# 2. Using Dynamic Environment Manager as part of a Workspace ONE solution for usability and security.

Horizon and Dynamic Environment Manager (DEM) provide a great combination of capabilities to apply DLP controls depending on a range of endpoint parameters and location information.

There are some features that might be used in the context of security, in our research. we have discovered some constraints with certain parameters and we will address the potential and the downside to this functionality

## Part 1: Identifying registry based configurations as a basis for the Conditional elements we could possibly use when using Horizon Smart Policies

This section will serve as an introduction to registry based configurations and what we choose from in the registry if we are wanting to use this configuration with Horizon Smart Policies

# Identifying registry based configurations for the Condition based elements in Horizon Smart Policies

You might still be logged in from a previous lab on the Horizon Client with the Craig accounts.

If you are you might be able to move down immediately to Step 9 in Part 1



- 1. On your **ControlCenter** server
  - from the **Desktop**
    - Open the Remote Desktops \ Site 1 folder
    - Launch the W11Client-01a.rdp shortcut

Windows Security	×			
Your credentials did no	t work			
Your system administrator does not allow the use of saved credentials to log on to the remote computer 172.16.30.40 because its identity is not fully verified. Please enter new credentials.				
w11client-01a\craig				
Password				
The logon attempt failed				
More choices				
ОК	Cancel			

#### 2. In the **Windows Security** page

- ensure Craig is the username
- in the **password** area
  - enter VMware1!
- select OK



- 3. On your **W11Client-01a** desktop
  - From the **taskbar** or **Desktop** 
    - launch your VMware Horizon Client
    - In the VMware Horizon Client window
      - select corp.euc-livefire.com broker URL

Microsoft	
Sign in	
craig@corpXXX.euc-livefire	e.com
Can't access your account?	
	Next

- 4. In the Microsoft Sign in window
  - enter Craig@corpXXX.euc-livefire.com
    - where XXX is your assigned Domain identifier
  - select Next



- 5. In the Microsoft Enter password window
  - enter VMware1!
  - select Sign in



- 6. In the Microsoft Stay signed in?
  - select Yes

https://corp.euc-livefire.com/port X	+			
← → C ☆ @ corp.euc-livefire.com/portal/nativeclient				
	Open VMware Horizon Client? https://corp.euc-livefire.com wants to open this application. Always allow corp.euc-livefire.com to open links of this type in the associated app Open VMware Horizon Client Cancel			
	Launching Horizon client <u>Click here</u> if the client is not launched automatically.			

#### 7. On your **W11Client-01a** desktop

- on the Open VMware Horizon Client? window
  - select Open VMware Horizon Client

VMwa	re Horizon Clie	ent				
	🖒 https://	corp.euc-liv	efire.com			
	Develo	pers	Enterprise_Deskto	>	Calc	ulator
	☆		ф ···		습	

- 8. In the VMware Horizon Client login window
  - select the Enterprise\_Desktop entitlement

Settings
File Explorer
Search
Run
Shut down or sign out >
Desktop
tent

- 9. On your Horizon Desktop session
  - from the **taskbar** 
    - select and right-click the **START** button
    - from the **inventory** 
      - select Run

(c	Notepad reated by		
	💷 Run	×	
		Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
	Open:	regedit.exe v	
		OK Cancel Browse	

#### 10. In the **Run** window

- next to **Open**:
  - enter regedit.exe
- select OK

N11Client-01a - 172.16.30.40 - Remote Desktop Connection						
	Registry Editor		Enterprise_Des	[L] Ctrl+Alt+Del 🕴 USB Devi		
Recy File	Edit View Favorites Help					
Cor	mputer/HKEY_LOCAL_MACHINE\SO	FTWARE\VMware, Inc.\\	Mware VDM\Session	nData\1		
	- 🚞 VMware Unity	Name	Туре	Data		
	VMware UsbRedii	(Default)	REG_SZ	(value not set)		
	VMware VDM	ViewClient_Age	REG_SZ	1683103515		
Mici	- Agent	ViewClient_Brok	REG_SZ	Horizon-01a.euc-livefire.com		
	Daiss Agent	ViewClient_Brok	REG_SZ	EUC-LIVEFIRE		
	Dump	ViewClient_Brok	REG_SZ	w10-bir-inst		
	> KeyVaultCNG	ViewClient_Brok	REG_SZ	172.16.20.10		
	- Log	MiewClient_Brok	REG_SZ	corp.euc-livefire.com		
VM Horize	> 🚞 Node Manage	ViewClient_Brok	REG_SZ	External		
	- Performance S	MiewClient_Brok	REG_SZ	uag-hzn-01a.euc-livefire.com		
G	> 📁 Plugins	MiewClient_Brok	REG_SZ	AP		
	> 🚞 PrintRedir	ViewClient_Brok	REG_SZ	172.16.30.40		
	- RdpVcBridge	ViewClient_Brok	REG_SZ	172.16.30.40, 172.16.20.20, 172.16.		
Calc	- RemoteExperix	ViewClient_Brok	REG_SZ	false		
teres	> RTAV	ViewClient_Brok	REG_SZ	https://horizon-01a.euc-livefire.co		
	- ScannerRedire	ViewClient_Brok	REG_SZ	Craig		

#### 11. In the Registry Editor window

- from the *left Inventory pane*
- select and expand HKEY\_LOCAL\_MACHINE > SOFTWARE > VMware, Inc. > VMware VDM > SessionData > 1

Y_LOCAL_MACHINE\SC	DFTWARE\VMware, Inc.\VMware VDM\SessionData\1	
VMware Drivers	Name	T
VMware GEORED	ViewClient Displays.SystemDpi	R
VMware HzMon	ab View Client Displays Topology	R
VMware Logon N	WiewClient Displays Topology//2	
VMware Optimiza	ab View Client Displays Topology/2	
VMware Remote	ab View Client Info ID	p
VMware SDRTran:	WiewClient_ID_Address	D
VMware Tools	WewClient_IP_Address	
VMware TSDR	WiewClient_Keyboard.KeyDelaylokepeat	
VMware TSMMR	ViewClient_Keyboard.Keykepeatkate	R.
VMware UEM	ViewClient_Keyboard.Language	к
VMware Unity	* ViewClient_Keyboard.Layout	R
VMware UsbRedii	ViewClient_Keyboard.NumFuncKeys	R
VMware VDM	ViewClient_Keyboard.NumIndicators	R
- Agent	ViewClient_Keyboard.NumKeys	R
DaaS Agent	ViewClient_Keyboard.ScanCodeMode	R
> DeviceRedirec	ViewClient_Keyboard.SubType	R
- Dump	ViewClient_Keyboard.Type	R
> KeyVaultCNG	ViewClient_Language	R
Log	ab ViewClient_Launch_ID	R
> Node Manage	ViewClient_Launch_SessionType	R
Performance S	ab ViewClient_LoggedOn_Domainname	R
> Plugins	ViewClient_LoggedOn_Username	R
> PrintKedir	ab ViewClient_MAC_Address	R
Карусвладе	ab ViewClient Machine Domain	R
KemoteExperie	ViewClient Machine FODN	R
Second RIAV	ViewClient Machine Name	R
Scannerkedire	ab ViewClient MDMDeviceID	R
ScriptEvents	ab ViewClient Mouse Identifier	R
Security	ab ViewClient Mouse NumButtons	R
	ab ViewClient Mouse SampleBate	P
TSMMR	ab View Client Protocol	P
	A View Client Trop	
VirtualChanne	Mary Client TZID	R D
virtuarchanne	wiewclient_120	к
	Viewclient_Windows_limezone	B

#### 12. In the **SessionData \ 1** folder

- Note the registry based ViewClient\_ parameters that are available. These can serve as part of a Conditional Element in Horizon Smart Policies
- Other than **Risk Scoring** functionality, with **DEM Conditions**, Its important to note, these are the only parameters we might consider using to manage and control the endpoint session in Dynamic Environment Manager.

- In the next Parts we will look at example parameters like and evaluate how secure this approach ACTUALLY is
  - ViewClient\_MDMDeviceID : enrolled devices
  - ViewClient\_Broker\_GatewayLocation or Client Location: which has the value of Internal or External
  - Other examples of contributing to endpoints being Secured and Usable when accessing resources using Horizon in an Organization could be
    - ViewClient\_ Machine\_Domain: the remote Windows 10/11 clients domain name
    - ViewClient\_Machine\_Name: the remote Windows 10/11 clients PC name

+	all	172.25.4.43	- 8
0.40 - Remote Desktop (	Connection		
}•• 주 ∐	Enterprise_Des 🖺	] Ctrl+Alt+Del 🕴 USB Devices > 🕂 Exit Fullscreen	)-
er		Help	
e		About VMware Horizon Client	
		Return to Desktop and Application Selection Screen	
e		Settings	
		🕞 Logoff Desktop	
d		X Disconnect	
Disconnect and	log off desktop?		
This desktop will be di	isconnected and logged	off. Any unsaved work will be lost.	
OK	- +-	Concei	

- 13. In the Horizon Client VDI session
  - next to **Exit Fullscreen** 
    - select the more options icon
      - select Logoff Desktop
    - In the Disconnect and log off desktop? window
      - select OK

# Part 2: Setting up VMware Horizon Smart Policies with VMware Dynamic Environment Manager

This part is divided up into two sections.

Section 1: We will create a Horizon Smart Policy for external endpoints that are Managed by Workspace ONE UEM

Section 2: We will create a Horizon Smart Policy for external endpoints that are UnManaged by Workspace ONE UEM

# Section 1: Setting up a Smart Policy for Trusted Devices using the ManagedDevices property



- 1. On your ControlCenter server Desktop
  - from the Taskbar
    - select and launch, the *DEM management Console* shortcut



- 2. In the Dynamic Environment Manager Console
  - Select the User Environment tab

VMware	Dynamic En	nvironment Manager - Management Consol
Personal	ization	User Environment Condition Sets
Refresh Group By Tag	Create Ed	dit Duplicate Import Export Remove
List		Horizon Smart Policies
ADMX-based Se App Volumes Application Bloc Drive Mappings Environment Va File Type Assoc Files and Folder Folder Redirecti Charles Folder Redirecti	ettings king riables iations s on	Horizon Smart Policies       Find       Name
Logon Tasks	Create	te Horizon Smart Policies setting
<ul> <li>Logoff Tasks</li> <li>Printer Mapping</li> <li>Privilege Elevati</li> <li>Revietor Setting</li> </ul>	s on	

- 3. In the Dynamic Environment Manager Console
  - In the User Environment Inventory
    - Select Horizon Smart Policies,

• Right-click and select Create Horizon Smart Policies setting...

Horizon Smart Policies ×						
Settings	Conditions Comments					
Genera	Settings					
Name:	Compliant Endpoints					
Label:	USB, Clipboard and Client drive	USB, Clipboard and Client drive				
Tag:	Managed					
Horizor	Smart Policy Settings					
V Aud	io playback	Enable	- ^			
🗸 Ban	dwidth profile	Broadband WAN	-			
Blast Ex	treme protocol:					
🖻 B	last codec	Enable	~			
V H	1.264	Enable				
EH	1.264 high color accuracy	Enable	*			
EH	1.264 maximum quality		0			
E H	1.264 minimum quality	36	0			
EH	IEVC/H.265	Enable	-			
V J	PG	Enable				
E J	PG image quality - Low		0			
E J	PG image quality - Mid		- 0			
E J	PG image quality - High	90	0			
V N	fax frame rate	30				
🖾 N	fax session bandwidth		0			
🗖 N	lax session BW megapixel slope	6200	• •			
		Save	<u>C</u> ancel			
E 5	witch encoder	Disable	•			
V Drag	and drop	Allow all				
V Print	ing	Enable				
Redirect	ion:					
V C	lient drive	Allow all				
VC	lipboard	Allow all				
VU	SB	Enable				
V Web	and Chrome file transfer	Allow upload from client t	to ager 👻 🤟			
<u>P</u> revio	ous <u>N</u> ext	Save	<u>C</u> ancel			

- 4. In the Horizon Smart Policies, window
  - Under the **Settings** tab
    - enter the following:-
      - Under **General** Settings, enter the following, next to:
        - Name: Compliant Endpoints
        - Label: USB, Clipboard and Client drive
        - Tag: Managed
      - In the Horizon Smart Policy Settings, enable the following checkboxes, next to:
        - Audio Playback : Enable
        - Bandwidth Profile : Broadband WAN
        - Blast Extreme protocol
          - H.264: Enable
          - JPG: Enable
          - Max frame rate : 30
      - Drag and drop : Allow all
      - Printing : Enable
      - In the **Redirection** settings, enable the following checkboxes and associated settings, next to:
        - Client drive : Allow all
        - Clipboard : Allow all
        - USB : Enable
      - Web and Chrome file transfer: Allow all

Horizon Smart Polici	es			
Settings Condition	s Comme	ents		
- Conditions				
Add 🔹	Edit	-	Remove	
No conditions are configured				

- 5. In the **Horizon Smart Policies** window
  - Select the Conditions tab
  - Under Conditions, select the dropdown next to Add



#### 6. In the **Add Condition** dropdown

- Select Horizon Client Property
- Note: By default, if you connect directly to a View Connection Server,
  - the gateway location is Internal

- If you connect to an Unified Access Gateway Server,
- the gateway location is **External** by default.

Horizon Client Property					×
Settings -					
Property:	Client location	*	Is equal to:	External	•
				<u>0</u> K	<u>C</u> ancel

- 7. In the Horizon Client Property, add the following:
  - next to Property,
    - from the **dropdown** 
      - select Client location
  - next to **Is equal to**,
    - from the **dropdown** 
      - select External
  - To close the Horizon Client Property
    - select OK

Horizon Smart Policies						
Settings Conditions Comments						
Conditions						
Add - Edit Remove						
Horizon client property 'Client location' is equa						

- 8. In the Horizon Smart Policies window
  - In the **Conditions** tab
    - next to **Add** 
      - select the dropdown



- 9. In the **Add Condition** dropdown
  - Select Horizon Client Property

Horizon Client Property						
- Settings -						
Property:	Broker_GatewayType	<ul> <li>Is equal to</li> </ul>	- AP			
			<u>O</u> K	<u>C</u> ancel		

- 10. In the Horizon Client Property window,
  - next to **Property**:
    - enter Broker\_GatewayType
  - next to Broker\_GatewayType
    - from the dropdown
      - select is equal to
  - In the box area, to the right of Is equal to
    - enter AP
  - select OK

Horizon Smart Policies						
Settings Conditions Comments						
Conditions						
Add - Edit Remove 📥 🔻						
Horizon client property 'Client location' is equal to 'External'						
AND Horizon client property 'Broker_GatewayType' is equal to 'AF						

- 11. In the Horizon Smart Policies window
  - In the **Conditions** tab
    - next to Add
      - select the dropdown



- 12. In the **Add Condition** dropdown
  - Select Horizon Client Property

Horizon Clie	ent Property			×
Property:	MDMDeviceID	▼ Exists	•	
			<u>O</u> K <u>C</u> ancel	

- 13. In the Horizon Client Property window,
  - next to **Property**:
    - enter **MDMDeviceID**
  - next to **MDMDeviceID** 
    - ensure **Exists** is selected
  - select OK

Horizon Smart Policies	×
Settings Conditions Comments	
Conditions       Add     •       Edit     •       Remove	
Horizon client property 'Client location' is equal to 'External' AND Horizon client property 'Broker_GatewayType' is equal to 'AP' AND Horizon client property 'MDMDeviceID' exists	
<u>Save</u> <u>C</u> ancel	

- 14. In the Horizon Smart Policies window
  - Select Save

# Section 2: Setting up a Smart Policy for UnTrusted Devices using the ManagedDevices property

VMware Dynamic Env	ironment Manager - Management Cons	ole	
Personalization	User Environment Condition Sets	Application Migration	
Refresh Group By Tag List	Duplicate Import Export Remove	Configure	
ADMX-based Settings	Horizon Smart Policies		
<ul> <li>Drive Mappings</li> </ul>	Name	Label	
Environment Variables	Compliant Endpoints	USB, Clipboard and Client Drive	
File Type Associations			
a Folder Redirection			
Range Horizon Smart Policies			
Logon Tasks Create	Horizon Smart Policies setting		
Logoff Tasks			
Printer Mappings			
Privilege Elevation			

- 1. In the **User Environment** Inventory
  - Select Horizon Smart Policies,
  - Right-click and select Create Horizon Smart Policies setting...

ttings Conditions Comments					
General Settings					
Name: Non Compliant Devices					
abel: USB, Clipboard and Client driv	e disabled				
Tag: UnManaged			-		
Iorizon Smart Policy Settings					
IPG	Enable	-	^		
JPG image quality - Low	25	\$			
JPG image quality - Mid	35	÷			
🔲 JPG image quality - High	90	÷			
Max frame rate	30	:			
Max session bandwidth	1000000	÷			
Max session BW megapixel slope	6188	÷			
Min session bandwidth	256	÷			
Switch encoder	Disable	*			
Drag and drop	Disable	*			
Printing	Enable	*			
Redirection:					
Client drive	Disable	*			
Clipboard	Disable	-			
USB	Disable	-			
Web and Chrome file transfer	Disable	*	~		

- 2. In the Horizon Smart Policies, Settings tab enter the following:-
  - Under **General** Settings, enter the following, next to:
    - Name: Non Compliant Endpoints
    - Label: USB, Clipboard and Client drive disabled
    - Tag: UnManaged
  - In the Horizon Smart Policy Settings, enable the following checkboxes, next to:
    - Audio Playback : Enable
    - Bandwidth Profile : Broadband WAN
    - Blast Extreme protocol
      - H.264: Enable
      - Max frame rate : 30
  - Drag and drop : Disable
  - In the **Redirection** settings, enable the following checkboxes and associated settings, next to:
    - Client drive : Disable
    - Clipboard : Disable
    - USB : Disable
  - Web and Chrome file transfer: Disable

Horizon Smart Policies							
Settings Conditions Comments							
Conditions							
Add -	Edit	-	Remove				
No conditions are configured							

- 3. In the Horizon Smart Policies window
  - Select the Conditions tab
  - Under Conditions, select the dropdown next to Add



- 4. In the **Add Condition** dropdown
  - Select Horizon Client Property

Horizon Client Property					×
Property:	Client location	*	ls equal to:	External	•
				<u>о</u> к	<u>C</u> ancel

- 5. In the Horizon Client Property, add the following:
  - next to **Property**,
    - from the **dropdown** 
      - select Client location
  - next to **Is equal to**,
    - from the dropdown
      - select External
  - To close the **Horizon Client Property** 
    - select OK

Horizon Smart Policies						
Settings Conditions Comments						
Conditions						
Add - Edit Remove						
Horizon client property 'Client location' is equa						

- 6. In the Horizon Smart Policies window
  - In the Conditions tab
    - next to **Add** 
      - select the dropdown



- 7. In the **Add Condition** dropdown
  - Select Horizon Client Property

Horizon Client Property						
- Settings -						
Property:	Broker_GatewayType	<ul> <li>Is equal to</li> </ul>	- AP			
			<u>O</u> K	<u>C</u> ancel		

- 8. In the Horizon Client Property window,
  - next to **Property**:
    - enter Broker\_GatewayType
  - next to Broker\_GatewayType
    - from the dropdown
      - select is equal to
  - In the box area, to the right of Is equal to
    - enter AP
  - select OK

Horizon Smart Policies
Settings Conditions Comments
Conditions
Add - Edit Remove 📥 🔻
Horizon client property 'Client location' is equal to 'External'
AND Horizon client property 'Broker_GatewayType' is equal to 'AF

- 9. In the Horizon Smart Policies window
  - In the **Conditions** tab
    - next to Add
      - select the dropdown



- 10. In the **Add Condition** dropdown
  - Select Horizon Client Property

Horizon Clie	ent Property			×
- Settings - Property:	MDMDevicelD	▼ Exists	•	
			<u>O</u> K	<u>C</u> ancel

- 11. In the Horizon Client Property window,
  - next to **Property**:
    - enter **MDMDeviceID**
  - next to MDMDeviceID
    - ensure **Exists** is selected
  - select OK

Unmanaged Devices - Horizon Smart Policies
Settings Conditions Comments
Conditions
Add • Edit • Remove
Horizon client property 'Client location' is equal to 'Exte AND Horizon client property 'Broker_GatewayType' is ea
AND Ho Add
OR
AND NOT
OKINU
Movella
Unmanaged Devices - Horizon Smart Policies
Satting Constants Comments
Conditions Comments
Add - Edit - Remove
Horizon client property 'Client location' is equal to 'External'
AND Horizon client property 'Broker_GatewayType' is equal to 'AP'
AND NOT Horizon client property 'MDMDeviceID' exists

- 12. In the Horizon Smart Policies window
  - next to AND Horizon client property 'MDMDeviceID' exists
    - select & right-click and from the dropdown
      - select AND NOT
  - Select Save

# Part 3 : Testing your Smart Policies.

- · We will demonstrate the following in this exercise
  - That being **Drag and Drop** functionality.
  - **USB redirection** (limited functionality here)
  - We will use the Dynamic Environment Manager Logs, to see if the settings are effective.
- We will use a Managed and UnManaged device to test this setup
  - W11Client-01a is our managed device
  - W11EXT-01a is our unmanaged device
- We will use the *Sales User Mark* to test this functionality

### Step 1: Testing the Smart Policies for a Managed device



- 1. On your ControlCenter server desktop
  - Open the Remote Desktop \ Site 1 folder
  - launch W11Client-01a.RDP

WE-days Consider	
windows security	~
Your credentials did no	t work
Your system administrator does credentials to log on to the remo- because its identity is not fully ve credentials.	not allow the use of saved ote computer 172.16.30.40 erified. Please enter new
w11client-01a\craig	
•••••	୕
The logon attempt failed More choices	
ОК	Cancel

- 2. In the **Windows Security** page
  - using the W11client-01a\craig as username
  - in the **password** area
    - enter VMware1!
  - select OK



- 3. On your **W11Client-01a** desktop
  - From the **taskbar** or **Desktop** 
    - launch your VMware Horizon Client

- In the VMware Horizon Client window
  - select corp.euc-livefire.com broker URL

sign in	
craig@corpXXX.euc-livefire.	com
Can't access your account?	
	Next

- 4. In the **Microsoft Sign in** window
  - enter Craig@corpXXX.euc-livefire.com
    - where XXX is your assigned Domain identifier
  - select Next

Microsoft	
← craig@corp24r.euc-livefire.com	
Enter password	
Forgot my password	
	Sign in
	Sign in

- 5. In the Microsoft Enter password window
  - enter VMware1!
  - select Sign in



- 6. In the Microsoft Stay signed in?
  - select Yes



#### 7. On your W11Client-01a desktop

- on the Open VMware Horizon Client? window
  - select Open VMware Horizon Client

Ċ	https://	/corp.euc-liv	efire.com		•	
	Develo	opers	Enterpris	se_Deskto p		
	☆		습			

- 8. In the VMware Horizon Client login window
  - select the Enterprise\_Desktop entitlement

mote Desktop	Connection		
≣ ጾ →	- Enterprise_Des	🔛 Ctrl+Alt-Del	😫 USB Devices > 🗧 Exit Fullscreen \cdots — 🗙
			Automatically Connect at Startup Automatically Connect when Inserted No suitable USB devices available

- 9. In the VMware Horizon Client
  - next to USB Devices
    - select the dropdown arrow,
    - Note, **No suitable USB devices available**, is the message you get.
      - Therefore if there were physical devices connected to the endpoint, its most likely that USB redirection would work
    - select Exit Fullscreen



- 10. From your W11Client-01a desktop
  - With your mouse, select the Google Chrome shortcut
    - Drag it over into the Horizon Client session
      - Note that you will get a + **type Icon** , just below your cursor.
  - Release your mouse button to **Drop the Console** within the Horizon Session



- 11. In the Horizon Client session
  - From the **Taskbar**,
    - select the File Explorer folder shortcut



- 12. In the File Explorer Window
  - Select This PC in the left Inventory
  - To the right, scroll down and observe, there are network locations configured. ie the Z: drive



# Step 2: Observing the Logs

- 1. On the **ControlCenter** server
  - Open your File Explorer Icon, from the Taskbar
  - On the C:\, open your UEMProfiles\YOUR Custom Test User\Logs folder

#### Click to copy



- 2. In File Explorer C:\UEMProfiles\user1\Logs
  - Select and right-click FlexEngine.log
  - Select Edit with Notepad++

845	2023-03-30 16:59:24.641 [INFO ] Processing path-based DEM undo actions and/or creation of
846	2023-03-30 16:59:24.656 [INFO ] Done (480 ms) [< <ifp#2b062380-82a29]< th=""></ifp#2b062380-82a29]<>
847	2023-03-30 16:59:09.384 [INFO ] Starting FlexEngine VI0.8.0.1064 [IFP#31/ab01e-1a2d42>>]
848	2023-03-30 16:59:09.384 [INFO ] Running from service (NoAD)
849	2023-03-30 16:59:09.385 [INFO ] Performing path-based import
850	2023-03-30 16:59:09.424 [INFO ] Skipping Horizon Smart Policies settings due to condition
851	2023-03-30 16:59:09.430 [INFO ] Applied Horizon Smart Policies settings:
852	2023-03-30 16:59:09.430 [INFO ] Bandwidth profile is set to 'Dedicated WAN'
853	2023-03-30 16:59:09.430 [INFO ] Audio playback is enabled
854	2023-03-30 16:59:09.430 [INFO ] Blast Extreme: H.264 is enabled, JPG is enabled, Max
855	2023-03-30 16:59:09.430 [INFO ] Drag and drop is allowed
856	2023-03-30 16:59:09.430 [INFO ] Printing is enabled
857	2023-03-30 16:59:09.430 [INFO ] Client drive redirection is allowed
858	2023-03-30 16:59:09.430 [INFO ] Clipboard redirection is allowed
859	2023-03-30 16:59:09.430 [INFO ] USB redirection is enabled
860	2023-03-30 16:59:09.430 [INFO ] Web and Chrome file transfer is allowed
861	2023-03-30 16:59:09.755 [INFO ] Configured message for trigger 'Workstation unlocked' ('
862	2023-03-30 16:59:09.770 [INFO ] Configured user environment settings refresh for trigger
863	2023-05-50 16:59:09.766 [INFO ] CONTIGUIED USED ENVIRONMENT SECTINGS TELLESN FOR CHIGGED
064	2002 02 20 16.66.11 204 (TMED 1 Config file 1) control contor and livefive com/HomConfig/C

#### 3. In the **Notepad++** session

- Reload your logs, by selecting File > Reload from Disk
- Scroll down, right to the bottom of your logs,
  - Scroll up until you find the YOUR Custom Test User and the Performing pathbased import logs starting
  - Observe that each configuration is processed and logged as disabled / enabled or True / False
  - Note its the Internal Policy that is being applied
  - Note what features are **allowed** or **enabled**

				-		×	
<u>=</u>	Ctrl+Alt+Del	USB Devices	>	[တြ] Fulls	screen		
+	Help						
Al A In A Sort →	About	VMware Horizo	on Client	t			
	Return	n to Desktop an	d Applic	ation Sele	ection S	creen	
~ C Q Se	🔞 Settin	gs					
nd drives	🕞 Logof	f Desktop					
:al Disk (C:)	X Disco	nect	)				8
b GB free of 95.2 GB							
twork Drive (Z:)							
1 GB free of 95.2 GB							
Disconnect and log off desktop?							
This desktop will be disconnected and logged off.	Any unsaved wor	k will be lost.					
ОК	Cancel						

- 4. On the **ControlCenter** server
  - switch back to your Horizon Client session
  - next to Fullscreen,
    - next to **Options**,
      - select the See more (3 buttons),
    - select Log Off Desktop
      - On the Disconnect and log off desktop? window
    - select OK

### Step 3: Testing the Smart Policies for an UnManaged device



- 1. On the **ControlCenter** server
  - Open the Remote Desktops \ Site1 folder
  - Open w11EXT-01a.RDP

Windows Security	×
Your credentials did no	t work
Your system administrator does n credentials to log on to the remo because its identity is not fully ve credentials.	not allow the use of saved ote computer 172.16.30.30 prified. Please enter new
w11ext-01a\nancy	
•••••	ି
The logon attempt failed More choices	
ОК	Cancel

- 2. On the **Windows Security** window
  - Ensure w11ext-01a\nancy is the username
  - In the **password** area
    - enter VMware1!
  - select OK



- 3. On the W11Ext-01a desktop
  - Launch the VMware Horizon Client shortcut
    - In the VMware Horizon Client
      - select + Add Server

lame of the Conne	ction Server		
corp.euc-livefire.c	om		×
Cancel		Connect	

- 4. On the **W11Ext-01a** desktop
  - In the Name of the Connection Server window
    - enter corp.euc-livefire.com
    - select Connect

WICIOSOIL	
Sign in	
nancy@corpXXX.euc-liv	efire.com
Can't access your account?	
	Next

#### 5. In the **Microsoft Sign in** window

- enter nancy@corpXXX.euc-livefire.com
  - where XXX is your assigned Domain identifier
- select Next



- 5. In the **Microsoft Enter password** window
  - enter VMware1!
  - select Sign in

Microsoft	
nancy@corp24r.euc	livefire.com
Stay signed	in?
Do this to reduce th to sign in.	e number of times you are a
Don't show this	again
	No. Var

- 6. In the Microsoft Stay signed in?
  - select Yes

https://corp.euc-livefire.com/port X	+
← → C ☆ @ corp.euc-li	vefire.com/portal/nativeclient
	Open VMware Horizon Client? https://corp.euc-livefire.com wants to open this application. Always allow corp.euc-livefire.com to open links of this type in the associated app Open VMware Horizon Client
	Launching Horizon client <u>Click here</u> if the client is not launched automatically.

#### 7. On your **W11Client-01a** desktop

- on the Open VMware Horizon Client? window
  - select Open VMware Horizon Client

<				
	https:/	//corp.euc-liv	efire.com	
	Develo	opers	Enterprise_Deskto	Calculator
	☆		☆ …	ф <b></b>

- 8. In the VMware Horizon Client login window
  - select the Enterprise\_Desktop entitlement



#### 9. In the Horizon Client

- In the top bar, next to Connect USB Device, select the drop-down
  - Notice that **USB is "Initializing"** is the state of USB (a change of state)

Corp Sales			
		臣 Ctrl+Alt+Del	USB Devices
8	This PC	× +	Automatica
Recycle Bin S	🕀 New ~ 🐰	[0] [1] [2] [2] [1] [1] [2] [2] [2] [2] [2] [2] [2] [2] [2] [2	Automatica
			USB Unavai
	$\leftrightarrow \rightarrow \checkmark \uparrow$	This PC      C     Q     Search This PC	
Microsoft Edge E	Documents *	~ Devices and drives	
	Downloads 🖈	Local Disk (C:) 76.6 GB free of 95.2 GB	
	Music *	_	
VMware Horizon Pe	Videos 📌		
7	> 💻 This PC		
Calculator (created by (c	> 🚈 Network		Activate V
	2 items		Go to Setting

• We will read the logs to validate

#### 10. In the Horizon Client Desktop

- On the title bar,
  - select the File Explorer Icon
- Ensure **This PC is** selected in the left inventory
  - Scroll down on the right side to the bottom of the window.

- Notice that you have **no** Network drive Mappings
- In the Horizon W11 desktop session
  - Close all windows



#### 11. In the W11EXT-01a Desktop

- Attempt to drag the VMware Horizon shortcut into the Horizon Desktop session.
- From the Horizon Desktop session
  - attempt to drag the Google shortcut to the W11EXT-01a desktop



#### 12. On the W11EXT-01a desktop

- Switch back to your Horizon Client session
  - to the right of **FullScreen** 
    - select ... (see more)
    - select the drop down,
    - select Log Off Desktop
    - In the Disconnect and log off desktop? window
      - Select OK

### Step 4: Observing the Logs

- 1. On the **ControlCenter** server
  - From the Taskbar
    - open your File Explorer Icon,
  - On the C:\
    - Browse to UEMProfiles > nancy > Logs folder

Click to copy

📕   🛃 📕 🖛   G	\UEMProfiles\r	ancy\Logs						
File Home	Share Vi	w						
Pin to Quick Copy access	Paste	<b>y path</b> e shortcut	Move to •	Copy to •	Delete	■] Rename	New folder	¶ ₹
Cli	pboard			Org	anize			I
← → • ↑ [	→ This PC →	Local Disk	:(C:) → l	JEMProf	iles → r	nancy →	Logs	
Site1	^ Nan	ie	^			Da	ite modif	ied
Site2		FlexEngine.l	og			3/	31/2023 8	3:23
System32		FlexEngine-	async.log			3/	31/2023 7	7:56
This PC		FlexEngine-	DefaultAp	plicatio	ns.log	3/	31/2023 7	7:56
3D Objects								

- 2. In File Explorer C:\UEMProfiles\nancy\Logs
  - select and right-click FlexEngine.log
  - select Edit with Notepad++

[INFO ] Done (589 ms) [< <ifp#05alceb5-4c86bf]< td=""></ifp#05alceb5-4c86bf]<>
[INFO ] Starting FlexEngine v10.8.0.1064 [IFF#2c57349d-531ae2>>]
[INEQ ] Running from service (NoAD)
Performing path-based import
[INFO ] Skipping Horizon Smart Policies settings due to conditions ('Compliant Endpoints.xml')
[INFO ] Applied Horizon Smart Policies settings:
[INFO ] Bandwidth profile is set to 'Dedicated WAN'
[INFO ] Blast Extreme: Max frame rate is set to 30
[INFO ] Drag and drop is disabled
[INFO ] Client drive redirection is disabled
[INFO ] Clipboard redirection is disabled
[INFO ] USB redirection is disabled
[INFO ] Web and Chrome file transfer is disabled
[INFO ] Configured message for trigger 'Workstation unlocked' ('Message at unlock.xml')
[INFO ] Configured user environment settings refresh for trigger 'Workstation unlocked' ('Refresh Ag
[INFO ] Configured user environment settings refresh for trigger 'Session reconnected' ('Refresh Pr:
[INFO ] Config file '\\controlcenter.euc-livefire.com\UemConfig\General\Applications\Acrobat Reader
[INFO ] No profile archive to import for config file '\\controlcenter.euc-livefire.com\UemConfig\Ge:
[INFO ] Config file '\\controlcenter.euc-livefire.com\UemConfig\General\Applications\Chrome.INI' add

#### 3. In the Notepad++ session

- Reload your logs, by selecting File > Reload from Disk
- Scroll down, right to the bottom of your logs,
  - Scroll up until you find the Performing path-based import logs starting
  - Note the Compliant Endpoints.xml is skipped due to conditions
  - Note the Applied Horizon Smart Policies
    - Drag and drop is disabled
    - Client drive redirection is disabled
    - Clipboard redirection is disabled
    - USB redirection is disabled
    - Web and Chrome file transfer is disabled
  - Note what features are **allowed** or **enabled**

### Step 5 : The Unvarnished Truth

So far everything looks amazing. However we have discovered the following regarding this configuration



#### 1. On your ControlCenter desktop

- switch to your Chrome Browser
  - open a **new tab**

- from the **Favourites** bar
  - launch the Workspace ONE **UEM** shortcut

Workspace ONE <sup>™</sup> UEM
Username Donnie.brookstone@gmail.com
Trendument
Next
Trouble logging in
Password
Log In
Log in as a different user Trouble logging in

- 2. In the Workspace ONE UEM login
  - under Username
    - enter your Registered course Username
    - select Next
  - under **Password** 
    - enter VMware1!
  - select Log In

🛃 vSphere - W11EXT-01a - Summa 🗙 🛛 🚱 W11EXT-01a					
← → C ☆ 🔒 dw-livefire.awmdm.com/AirWatch/					
😙 my-ip.livefire.lab/ip 🔤 Horizon©Site 1 👿 UAG-HZN-01a					
🖏 Works	pace ONE UEM	Re			
Ê					
GETTING STARTED	Dashboard				
$\sim$	List View				
MONITOR	Device Updates				
	Lifecycle	>			
DEVICES	Profiles & Resources	>			
음 ACCOUNTS	Compliance Policies	>			
	Certificates	>			
	Drovisioning	、 、			

- 3. In the Workspace ONE UEM Admin console
  - select **DEVICES**
  - under Dashboard
    - select List View

Devices		_	
List View			
Filters >> 💽 AD	DEVICE	LAYO T 🗸 🕑	) EX
QUERY SEND	LOCK C REBOOT DEVICE	MORE ACTIONS V 1 item :	selected
Last Seen 🔺	General Info	Management	ser
	Craig W11CLIENT-01A VMware7,1 a b	Enterprise Wipe	aig@l
<b>3</b> m	ReinhartMarchTEST UEM Managed   Corporate - Dedicate	criterprise keset	alg alg St
	Jackie W11CLIENT-02A VMware7,1 a ba	Admin	ckie@
🧹 🚮	ReinhartMarchTEST	Manage Tags	ckie P
	Commanaged   Colporate - Dedicate	Change Organization Group	

- 4. In the Workspace ONE UEM Admin console
  - List View console
    - Next to Craig W11CLIENT-01A
      - select the checkbox
    - In the **middle of the pane**

#### MORE ACTIONS

- select the **dropdown**
- In the **dropdown** 
  - select Enterprise Wipe

Keep Ap Device	ps On 🗌 🤅	)				
Last Seen	Friendly Name	C/E/S	User	Platform	Keep Apps On De	Model
🔺 4m	Craig W11CLIENT	С	Craig	Windows Desktop	Supported	Desktop
						,
urity PIN:						
got Security	PIN?					

- 5. In the **Restricted Action Enterprise Wipe** window
  - below Security Pin
    - enter your PIN
  - switch back to your W11Client-01a session



- 6. On your **W11Client-01a** desktop
  - On Taskbar / Search box
    - enter intelligent hub
      - notice that all you see is AirwatchAgent.msi



- 7. On your **W11Client-01a** desktop
  - On Taskbar / Search box

- enter Control Panel
- from the **Best Match** 
  - select Control Panel
- In the Control Panel app
  - under Programs
    - select Uninstall a program



- 8. In the Programs and Features section
  - Note there is no Workspace ONE Intelligent HUB on this endpoint



- 9. On your **W11Client-01a** desktop
  - launch the VMware Horizon client shortcut
  - In the VMware Horizon Client
    - select the corp.euc-livefire.com broker url

https://corp.euc-livefire.com/port X	+
$\leftrightarrow$ $\rightarrow$ C $\triangle$ $\stackrel{\text{\tiny B}}{}$ corp.euc-liv	efire.com/portal/nativeclient
	Open VMware Horizon Client? <ul> <li>https://corp.euc-livefire.com wants to open this application.</li> <li>Always allow corp.euc-livefire.com to open links of this type in the associated app</li> </ul> Open VMware Horizon Client Cancel
	Launching Horizon client
	<u>Click here</u> if the client is not launched automatically.

#### 10. On your **W11Client-01a** desktop

- on the Open VMware Horizon Client? window
  - select Open VMware Horizon Client



- 11. In the VMware Horizon Client login window
  - select the Enterprise\_Desktop entitlement

Corp Sales						
						Ë
8	This PC	×	-			
Recycle Bin S	⊕ New - 🔏 🖸		) ©	Û	$\uparrow \downarrow$	Sort ~
	$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\blacksquare$ > This	PC >		Ý	С	Q Se
Microsoft	Documents * V Dev	ices and d	rives			
Euge E	🚽 Downloads 🖈	Local Di	sk (C:)			
	🔀 Pictures 🖈	76.6 GB	free of 95.2 G	B		DVD
	🕖 Music 🔹 🗸 🗸 🖓 Net	work locat	ions			
VMware Horizon Pe	🔀 Videos 🖈	Network	Drive (Z:)			
_		71.6 GB	free of 95.2 G	βB		
<b>,</b>	> 📃 This PC					
Calculator (created by (c	> 🖆 Network					
	3 items					
			Search	1.0		-

- 12. In the VMware Horizon Client session
  - from the **taskbar** 
    - select the Folder icon
    - In the **Quick Access** pane
      - select This PC

- In This PC area
  - Note you have a drive mapping
- Feel free to attempt to drag and drop

x
- 🗆 X
E Ctrl+Alt+Del 🛱 USB Devices > 🔁 Fullscreen
Help
About VMware Horizon Client
Return to Desktop and Application Selection Screen
Settings
<b>0</b> ₽ Logoff Desktop
X Disconnect
Disconnect and log off desktop?
This desktop will be disconnected and logged off. Any unsaved work will be lost.
OK Cancel
VMware Horizon Client
tps://corp.
https://corp.euc-livefire.com
Log off server?
You will be logged off the server.
OK Cancel

- 13. In the **Horizon Client** session
  - next to Fullscreen
    - select the dropdown
      - select Logoff Desktop
  - In the Disconnect and log off desktop?
    - select OK
  - In the VMware Horizon Client
    - top left corner
      - select the **back arrow**
    - In the Log off server? window
      - select OK
  - minimize the w11Client-01a session



- 14. On the **ControlCenter** server
  - From the Taskbar
    - open your File Explorer Icon,
  - On the C:\
    - Browse to UEMProfiles > mark > Logs folder

#### Click to copy

📕 ) 🖓 🛄 🖛 I	C:\UEMPr	ofiles\mark\Logs						
File Home	Share	View						
Pin to Quick Copy access	Paste	从 Cut Copy path ₽ Paste shortcut	Move to ~	Copy to ~	Delete	Rename	New folder	대 New it 한 Easy ac
1	Clipboard			Org	anize			New
$; \leftarrow \rightarrow \cdot \cdot \uparrow$	<mark>}</mark> → Th	is PC → Local Disk	:(C:) → l	JEMProf	iles → r	mark ⇒	Logs	
. Site1	^	Name	^			E	)ate modif	ied
Site2		FlexEngine.le	og			3	/31/2023 1	11:39 AM
System32		FlexEngine-a	async.log			3	/31/2023 9	9:45 AM
💻 This PC		FlexEngine-I	DefaultAp	plication	ns.log	3	/31/2023 9	9:45 AM
j 🗊 3D Objects	;							
. Desktop								

#### 15. In File Explorer C:\UEMProfiles\mark\Logs

- select and right-click FlexEngine.log
- select Edit with Notepad++

D	[INFO	]	Processing path-based DEM undo actions and/or creation of 'run once' flag files
7	[INFO	]	Done (764 ms) [< <ifp#317a99cd-la2d42]< td=""></ifp#317a99cd-la2d42]<>
1	[INFO	]	Starting FlexEngine v10.8.0.1064 [IFF#39f6elc9-23ee30>>]
2	[INFO	]	Running from service (NoAD)
2	1711	]	Performing path-based import
4	[INFO	]	Skipping Horizon Smart Policies settings due to conditions ('Non Compliant Devices.xml')
L	[INFO	]	Applied Horizon Smart Policies settings:
L	[INFO	]	Bandwidth profile is set to 'Dedicated WAN'
1	[INFO	]	Audio playback is enabled
1	[INFO	]	Blast Extreme: H.264 is enabled, JPG is enabled, Max frame rate is set to 30
1	[INFO	]	Drag and drop is allowed
1	[INFO	]	Printing is enabled
1	[INFO	1	Client drive redirection is allowed
1	[INFO	1	Clipboard redirection is allowed
1	[INFO	1	USB redirection is enabled
1	[INFO	1	Web and Chrome file transfer is allowed
7	[INFO	1	Configured message for trigger 'Workstation unlocked' ('Message at unlock.xml')
1	[INFO	]	Configured user environment settings refresh for trigger 'Workstation unlocked' ('Refresh 2
3	[INFO	]	Configured user environment settings refresh for trigger 'Session reconnected' ('Refresh Pi

#### 16. In the **Notepad++** session

- Reload your logs, by selecting File > Reload from Disk
- Scroll down, right to the bottom of your logs,
  - Scroll up until you find the Performing path-based import logs starting
  - Note the Non Compliant Endpoints.xml is skipped due to conditions
  - Note the Applied Horizon Smart Policies
    - Drag and drop is allowed
    - Client drive redirection is allowed
    - Clipboard redirection is allowed
    - USB redirection is allowed
    - Web and Chrome file transfer is allowed

() We will now investigate why this is happening

• Switch back to your W11Client-01a RDP session



- 17. On the **W11Client-01a** desktop session
  - From the taskbar
    - In the **Search** area
      - enter registry Editor
    - In the **Best Match** area
      - select Run as administrator

User Account Control	×
Do you want to allow this app to make changes to your device?	
🌼 Registry Editor	
Verified publisher: Microsoft Windows	
Show more details	
To continue, enter an admin username and password.	
admin	
•••••••	
W11CLIENT-01A\admin	
More choices	
Yes No	

- 18. In User Account Control window
  - Below admin
    - enter VMware1! as the password
  - select Yes



#### 19. In the **Registry editor**

- In the **Inventory** 
  - browse to
    - HKEY\_LOCAL\_MACHINE > SOFTWARE > Microsoft > Provisioning > OMADM > MDMDeviceID
  - Notice that you still have a **DeviceClientId** value in the registry
- In the **Inventory** 
  - select & right-click the MDMDeviceID folder
    - select **Delete**



- 20. On your **W11Client-01a** desktop
  - launch the VMware Horizon client shortcut
  - In the VMware Horizon Client
    - select the corp.euc-livefire.com broker url

https://corp.euc-livefire.com/port X	+
← → C ☆ @ corp.euc-lin	vefire.com/portal/nativeclient
	Open VMware Horizon Client?
	https://corp.euc-livefire.com wants to open this application.
	Always allow corp.euc-livefire.com to open links of this type in the associated app
	Open VMware Horizon Client Cancel
	Launching Horizon client
	Click here if the client is not launched automatically.
	CICK HELE II THE CHERT IS NOT IMUICHED AUTOMATICALLY.

#### 21. On your **W11Client-01a** desktop

- on the **Open VMware Horizon Client?** window
  - select Open VMware Horizon Client

< گ ا	ttps://corp.eud	-livefire.com				
۱ 🔂	ttps://corp.eud	-livefire.com				
t	Developers	Enterpr	ise_Deskto p	Calcu	ulator	
습		습				

- 22. In the **VMware Horizon Client** login window
  - select the Enterprise\_Desktop entitlement



#### 23. In the VMware Horizon Client session

- from the **taskbar** 
  - select the Folder icon
  - In the Quick Access pane
    - select This PC
    - In This PC area
      - Note that you now dont have a drive mapping
  - Feel free to attempt to drag and drop

#### 1 In Summary

Using the registry element for Conditions within Dynamic Environment Manager is more a usability solution than a security solution and we are not able to rely on this alone.

Other Client System Information that is registry based that we might consider for Conditions might be

- Machine\_Domain: the remote Windows 10 clients domain name
- Machine\_Name: the remote Windows 10 clients PC name
- Broker\_GatewayLocation or Client Location which has the value of Internal or External

In a later lab we will look at a 3rd Party solution called OPSWAT that will allow us to provide a broad range of rules to ensure compliant