VMware Verify (Intelligent Hub)

In this lab we will setup MFA using VMware's own Intelligent hub. This authentication method does not require a phone number (GSM) to be registration, but rather will use the already deployed intelligent hub as "soft token" during the authentication process.

Prerequisites:

- Workspace ONE Access integrated with Workspace ONE UEM
- Hub Services activated with Notifications enabled.
- Workspace ONE Intelligent Hub app 20.05 or later installed on user devices.
- iOS or Android (physical or emulator) Device enrolled
- (Optional) Require device-level passcodes for managed devices and app-level passcode for registered devices.

NOTE: This authentication method is designed to be used in conjunction with another form of authentication, and should not be used as a stand alone authentication method.

NOTE: Please ensure you have a mobile device enrolled from the introduction labs from day 1. Currently VMware Verify (Intelligent Hub) is only supported on iOS & Android and does not support getting prompts on Windows devices.

Part 1: Configure Authentication method

rrs & Groups Catalog 👻 Identity & Acc	ess Management	
Providers Password Recovery Assistant	Authentication Methods	thentication Methods Magic Link
Authentication Methods for Bu	lilt-in Identity Providers	
Important: When you disable an authent authentication method.	lication method, the authentication method is removed as a	choice in the access policy rules page. Make sure you updat
Authentication Methods	Configure	Status
Login Risk Score	/	Disabled
FID02	,	Disabled
Verify (Intelligent Hub)	1	Disabled
VMware Verify	/	Disabled
Mobile SSO (for iOS)	1	Disabled

1. On your Workspace ONE Access administrator console

- Login using your custom admin account.
- Select the Identity & Access Management tab
- To the right of the page select Manage
- Select Authentication Methods
- Next to Verify (Intelligent Hub) select the pencil icon

Verify (Intelligent Hu	b)
Enable Verify (Intelligent Hub)	
MFA Action Timeout in Seconds*	This will enable Verify (Intelligent Hub) 60 Enter the number of seconds after which the MFA request expires. This value can be between 30 and 90 seconds.
Enhanced Verification on Managed Devices	
Enhanced Verification on Registered Devices	Users authenticating from Workspace ONE UEM managed devices will be prompted for biometric or passcode verification on approval.
Enhanced Verification on Requests from Mobile Devices	Users authenticating from Workspace ONE UEM registered devices will be prompted for biometric or passcode verification on approval.
	Requests initiating from a mobile device require biometric or passcode verification. You do not need to enable this if you've enabled enhanced verification on Managed and Registered devices.
	Gancel
	Gancer

- 2. On the pop-up Verify (Intelligent Hub) window
 - Select the box next to Enable Verify (Intelligent Hub)
 - Select the box next to Enhanced Verification on Managed Devices
 - Select **Save** at the bottom right

Dashboard	- Users	& Groups Catalo	og 👻 Identity & Ac	cess Management	Roles	
Directories	Identity Pro	viders Passwor	rd Recovery Assistant	Authentication I	Methods Policies	5
		Identity Provi	ders (3)			
		Identity Provi	Auth Methods	Directory	Network Ran	Connector(s)
		System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES	
		Built-in	Mobile SSO (for iOS) Certificate (cloud deployment)	LivefireSync UEMLocalDirecto sfmusk	ALL RANGES	ws1- connector.euc- livefire.com

- 3. In Workspace ONE Access console
 - Navigate to Identity Providers
 - Select the **Built-in** Identity provider.

Authentication Methods	Select which authentication methods the IdP	will use to authenticate users.
	Authentication Methods	Associate Authentication Method
	Verify (Intelligent Hub)	
	Password (Local Directory)	
	Certificate (cloud deployment)	✓
Network	Select which networks this IdP can be access	sed from. Choose from the available network ranges from the lis

- 4. In the **Built-in** Identity provider window
 - Scroll down until the Authentication methods area
 - Select the box next to Verify (Intelligent Hub)
 - Select **Save** at the bottom of the page.

Part 2: Configure Access Policy

8 w	/orkspace ONE™ Access		
Dashboa	ird 👻 Users & Groups 🛛 Catalog 👻 Id	entity & Access Management Roles	
Directorie	s Identity Providers Password Recovery	Assistant Authentication Methods Policies	
	ADD POLICY EDIT DELETE	EDIT DEFAULT POLICY NETWORK RANGES	
	Policy Name	Applies to	Rv
	<pre>default_access_policy_set</pre>	O Application(s)	2

- 1. In the Workspace ONE Access admin console
 - Navigate to Identity & Access Management.
 - Select Manage
 - On the left hand side and click on Policies
 - Click EDIT DEFAULT POLICY on the Policies page.

Edit Policy					
1 Definition 2 Configuration	You can create a list of rule of devices that can access application before reauthe	es to access the applications se the applications, the auth mether enticating.	lected. For each rule, select t hods, and the maximum numb	he IP network range, ber of hours users can	the type use the
3 Summary	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				

- 2. In the Edit Policy window
 - In the left hand navigation, select Configuration
 - Select ALL RANGES next to Device Type > Web Browser.

URATION	Edit Policy Rule	
If a user's network range is	ALL RANGES	~
and the user accessing content from *	Web Browser	× ©
and user belongs to group(s)	Q Select Groups	٩
	Rule applies to all users if no group(s) selected.	
Then perform this action	Authenticate using	~ (i)
then the user may authenticate using *	Certificate (cloud deployment)	~_ © 🌯
If the preceding method fails or is not applicable, then	Password (cloud deployment)	~ © 🕀
If the preceding method fails or is not applicable, then	Password (Local Directory)	⊻ ® ⊕ ×
	ADD FALLBACK METHOD	

3. In the **Edit Policy Rule** page click the + next to the first form of authentication.

This could be **Certificate (cloud deployment)** or it could be **Password (cloud deployment)**. *This could depend on previous labs or use-cases. The important concept is that we are using the "and" function in authentication rather than "or".*

If a user's network range is *	ALL RANGES ~	١
and the user accessing content from *	Web Browser ~	١
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	١
Then perform this action	Authenticate using ~	٩
then the user may authenticate using *	Certificate (cloud deployment)	() ()
and	✓ Select authentication method	×
the preceding method fails or is not applicable then	Password (Local Directory) Password (cloud deployment) Cartificate (cloud deployment)	() ()
	Verify (Intelligent Hub) Password	
	CANCEL	SAVE

[then the user may authenticate using * and	Certificate (cloud deployment) Verify (Intelligent Hub)	~ ~	() ⊕ ×	
If the precedin	g method fails or is not applicable, then	Password (cloud deployment)	×	٠ 🕀	
If the precedin	g method fails or is not applicable, then	Password (Local Directory)	<u> </u>	٩ 🕀	×
			CANCEL	SAV	E
				_	
OR	then the user may authenticate using *	Password (cloud deployment)	~		Ð
<u>OR</u>	then the user may authenticate using *	Password (cloud deployment) Verify (Intelligent Hub)	~	- - -	Ð
If the prece	then the user may authenticate using • and eding method fails or is not applicable, then	Password (cloud deployment) Verify (Intelligent Hub) Password (Local Directory)	~	- (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	€
If the prece	then the user may authenticate using • and	Password (cloud deployment) Verify (Intelligent Hub) Password (Local Directory)	~	_ (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	€

- 4. You should now get a new authentication method drop down next to "**and**"
 - a. Select Verify (Intelligent Hub)

b. Once you have confirmed that you either have Certificate (cloud deployment) and Verify (Intelligent Hub) or you have Password (cloud deployment) and Verify (Intelligent Hub) you can click **SAVE** at the bottom right

NOTE: Ensure you have password (local directory) still as the fallback authentication method to ensure you can get back in to the administrator console.

Edit Policy					×
1 Definition 2 Configuration	You can create a list of ru of devices that can acces application before reauth	les to access the applications se s the applications, the auth meth enticating.	lected. For each rule, select the nods, and the maximum numb	he IP network range, t er of hours users can	the type use the
3 Summary	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)	×
	ii ALL RANGES	Windows 10	Certificate (cloud depl	8 Hour(s)	×
	ADD POLICY RULE				
			c,	ANCEL BACK	NEXT

5. Click **NEXT** on the **Edit Policy** page

Edit Policy		×
1 Definition 2 Configuration 3 Summary	Definition Name default_access_policy_set Description Default access policy set Applications	
	4 Application(s) Configuration Policy Rule 1 If a user's network range is ALL RANGES and the user is accessing content from Web Browser and the user belongs to the group(s) All Users then the user may authenticate using Certificate (cloud deployment) & Verify (Intelligent Hub)	
	CANCEL BACK SA	VE

6. Click **SAVE** on the **Summary** page

Part 3: Test Verify (Intelligent Hub) Implementation

← → × ↑ 📙 > `	← → × ↑ 📙 > This PC > Desktop > Remote Desktops	
1	Name ^	Date modified
A Quick access	s Horizon.RDP	2/28/2021 11:29
Desktop 🖈	B RDSH01a.RDP	4/13/2018 7:13 /
🕂 Downloads 🖈	SQL.RDP	4/3/2018 11:20 /
🔮 Documents 🖈	STrueSSO.RDP	1/12/2020 7:36 /
💽 Pictures 🛛 🖈	W10Client01.RDP	3/16/2021 12:35
DesktopInfo	w10EXT01a.RDP	6/5/2020 10:29 /
hol	nto w10Parent01a.RDP	3/2/2021 10:47 /
📙 Remote Desktop	NS1-Connector.RDP	4/3/2018 11:27 4
System32		

1. Navigate to your on-premise lab environment and click into the **Remote Desktops** folder on the **Desktop** of the **ControlCenter** virtual machine.

a. **Double Click** the **W10Client01.RDP** to connect to the Windows 10 Client.

퉣 Rem	Remote Desktop Connection					
The publisher of this remote connection can't be identified. Do you want to connect anyway?						
This remo where thi	ote connection could ha s connection came from	m your local or remote computer. Do not connect unless you know or have used it before.				
	Publisher:	Unknown publisher				
<u>_</u>	Туре:	Remote Desktop Connection				
	Remote computer:	W10Client01.euc-livefire.com				
🗌 Don't	ask me again for conne w Details	ctions to this computer Connect Cancel				

2. Click **Connect** when the **Remote Desktop Connection** windows pops up.



3. On the Desktop of the **W10Client01** click **Google Chrome** on the desktop

Sew Tab	× +			
<> C û ♀ aw-e	emusk.vidmpreview.com			
III Apps 🗘 aw-c	emusk.vidmpreview.com			
Q, aw-e	musk.vidmpreview.com - Google Sea	arch		
Interpretion to the termination of terminatio of termination o	× +			- 🗆 ×
\leftrightarrow \rightarrow C \triangle \cong cas.vide	mpreview.com/cas/t/AW-EMUSK/API	I/1.0/REST/landing?E	AB_CALLBACK_URL=%2Fauth%2Flo	ogin%2Fe 🖈 🕒 :
Apps	Select a certificate		×	
	Select a certificate to which you want to	authenticate cas.vidmpr	review.com:443	
	Subject	lssuer	Serial	
	user32SCR	emusk	0195AB	
	Certificate information		OK Cancel	
OR Workspace UN	E			
user32TDS				
password				
euc-livefire.cor	m			
Sign in				
Forgot passwor	d?			
Change to a different	: domain			
vm ware:				

4. Type in the **Workspace ONE Access URL** for your tenant and click enter

a. if you have configured **Certificate (cloud deployment)** as your first authentication method you will be prompted to select a certificate click **OK.** (If you did the extra material on the previous lab you will not be prompted.)

b.**OR** If you have configured Password (cloud deployment) as your first authentication method select your domain and enter username and password.



5. If you have multiple devices configured for this user you will be asked to select your device. Confirm the device and click **Continue**.

NOTE: If you only have a single device configured you will not be prompted to select a device. This device becomes the default/preferred device and will be remember for future authentication requests. (See part 5 to reset)

\odot	Pri	ority	(36)
Today, 13:11			
Sign-in R	equested		
Your cred	entials are b	eing used	to sign in.
User	us	er32SCR	
Device Ty	pe W	indows Des	ktop
IP Address	5 20	8.91.1.201	
C	leny	41	
			piove
10:12 @		-	
10:12 ®	ty		
10:12 Priori A few seconds ap	ty 20	L	π⊿ 1 (39)
10:12 Priori A fee seconds a Sign-in Requir Your credentia	ty 20 ested Is are being used t	o sign in.	ne⊿∎ ⊛
10:12 Priori A fee seconds a Sign-in Reque Your credentia User :	ty 20 ested Is are being used t Mark	o sign in.	n:⊿ ∎ ③
10.12 Priori A fee seconds e Sign-in Reque Your credentia User : Device Type :	ty jo is are being used t Mark Windows Desk	o sign in.	n.⊿ ■ (3)
10.12 Priori A fee seconds eg Sign-in Reque Your credentia User : Device Type : IP Address :	ty ested Is are being used t Mark Windows Desk 66.170.98.245	o sign in. top	n⊿ ∎ (39)
10:12 Priori A few seconds ag Sign-in Reque Your credentia User : Device Type : IP Address :	ty ested Is are being used t Mark Windows Desk 66.170.98.245	o sign in.	n⊿∎ 33
10.12 @ Priori A few seconds av Sign-in Requ Your credentia User : Device Type : IP Address :	ty 20 Is are being used t Mark Windows Desk 66.170.98.245	o sign in.	an⊿ ∎ ③
10.12 © Priori Sign-ion Reque Your credentia User : IP Address :	ty ssted Is are being used t Mark Windows Desk 66.170.98.245	o sign in.	µµµve ⊛
10.12 Priori A fee records ag Sign-in Requ Your credentia User: Device Type : IP Address :	ty ested Is are being used t Mark Windows Desk 66.170.98.245	o sign in.	(a)
10.12 Priori A fee second a p Sign-in Reque Your credentia User: Device Type : IP Address :	ty 29 sted Is are being used to Mark Windows Desk 66. 170.98.245	o sign in.	n⊿∎ (€)
10.12 Priori Free records as Sign-in Reque Your credentia User: Device Type : IP Address :	ty jo sated Mark Windows Desk 66.170.68.245	o sign in.	n.⊿∎ ⊕
10.12 Priori From Priori Sign-In Requ Vour credentia User: Device Type : IP Address :	ty po stated Is are being used t Mark Windows Desk 46.170.08.245	o sign in.	and f
10.12 Priori Priori Siga-In Requ Voor credentu Usar: Device Type : IP Address : P Address :	ty parent Is are being used to Mark Windows Deak 64.170.08.245	o sign in. top	a a a a a a a a a a

6. The browser will now give you **60 seconds** to respond to the request on your mobile device. If notification are enabled from the Intelligent Hub you will see the notification on the lock screen, otherwise navigate to the **Intelligent Hub** and click **Approve** on the **Sign-in Request**.

Note: The screen shots are for both iOS and Android above depending on which platform you are using.



7. You will then be prompted for the device passcode (or Touch-ID/Face-ID) used to unlock the device if you have one.

Favo	rites							US User32 SCR	
								Account	
	w	0	.		ser\ nd	VICE		Sign out	Ð
1	Microsoft Word	Oi	utlook		Servic	eNow			
Web	site 🕠 👈	Website	(i) 🛨	Web	osite	(i)	•		

8. Once approved, you will be authenticated in the web browser to your Intelligent hub.

		For You	-	History
iority	0	1		
0				×
Sign Your User: Devic View r	-in Request credentials a user32SCR re Type: Win nore >	ted re being us dows Desk	ed to sign ir top	
	Deny		Approve	
17 mir	iutes ago			
		Histor	y	X
Sign Your	-in Reques	sted are being u	sed to sign	in.
Sign Your User Devia View	I-in Reques credentials a : user32SCF ce Type: Win more >	sted are being u R adows Des	sed to sign	in.
Sign Your User Devia View	I-in Reques credentials : user32SCF Type: Win more > oproved nutes ago	sted are being u adows Des	sed to sign	in.
Sign Your User Devid View 12 mi 12 mi Sign	I-in Request credentials : user32SCF by Will more > oproved nutes ago	sted are being u adows Des adows Des	sed to sign	in.
Sign Your User Devia View 12 mi 12 mi 12 mi Sign Your User Devia View	in Request credentials : user32SCF with the second second more	sted are being u tows Des ndows Des sted are being u tows Des	sed to sign ktop sed to sign ktop	in.

9. In the Intelligent Hub on the mobile device click on **For You.** Here you can view the current Notifications. Then click in the top right corner on **History**. Here you will see the Authentication requests that have been made.

Part 4: Troubleshooting / Reporting



Troubleshooting / Reporting step:

Let's have a look what events are created as a result of the authentication.

1. Navigate back to the **Workspace ONE Access** administration console and click on the **down arrow** next to Dashboard and select **Reports**.



2. Click on **Audit Events** from the Reports drop down and **Show**

Audit Events From 3 days a	✓ User: ago to 0 days ago	Type: All	✓ Action: A	II V Object:	
Audit Even	ts				Export as CSV
DATE, TIME (UTC+03:00)	USER (DOMAIN NAME)	EVENT		OBJECT	
Jan 21, 2021 1:33:24 PM	user32SCR (euc- livefire.com)	LOGIN (Certificate (cloud deployment), Verify (Intelligent Hub))		f8ef9d1d-64b1-4ccd-8399-1b318c0389cb	View Details

3. Click **View Details** on the the most current event labeled **LOGIN (Certificate (cloud deployment), Verify (Intelligent Hub))**

View audit events detail	8
<pre>"deviceId" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH7 like Gecko) Chrome/87.0.4280.141 Safari/537.36", "workspaceId" : "EFFA05C70C7B5648A453CC63E1A15757", "sourceIp" : "208.91.1.201", "objectType" : "LOGIN", "objectName" : null, "values" : ["isForceAuth" : "false", "tokenId" : "f9b72d0a-4f71-4896-ad6e-e6661531bdbd", "successAuthMethods" : "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.aut d.hubmfa", "success" : "true", "authMethods" : "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.aut d.hubmfa", "success" : "true", "authMethods" : "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.aut d.hubmfa", "authMethods" : "identityProvider.embedded.authMethod.certificate,identityProvider.embedded.aut d.hubmfa", "actorExternalId" : "20885284-bf5c-4bbe-9730-34c9e55d4196" } }</pre>	TML, thMetho

4. In the details view of the event, you should see that the **Authentication Method** is hubmfa and that **"success" : "true"**.

Part 5: Reset preferred device

What's New in the April 2021 Release

Verify (Intelligent Hub) New Features

- Geolocation in Hub Notification is included in Verify (Intelligent Hub). There is now geolocation information within Verify (Intelligent Hub) push MFA notifications. this will allow end users to see the geolocation of the device that is making the MFA request.
- Ability to reset user device selection for Verify (Intelligent Hub) Administrator Flow. Workspace ONE Access now has the ability for administrators to unlink a device that end users configured with Verify (Intelligent Hub) within the Workspace ONE Access console. After unlinking the device, the next time that an end user logs in, they will go through the initial Verify (Intelligent Hub) flow and re-select the device that they wish to link with Verify (Intelligent Hub). This allows administrators to service users that do not have access to the device that is linked to Verify (Intelligent Hub);

In a previous version of this lab you would have used an API string to reset the preferred device setting for the Verify (Intelligent Hub) as of April 2021, Access now has a GUI based reset action for administrator to reset end-users prior selected device for MFA.

8 Works	B Workspace ONE" Access Tenant Admin - AW-MANFRED						MANFRED	
Dashboard -	Users & Groups Catalog	 Identity & Access Ma 	anagement Roles			Q Sea	rch users, groups or applications	
sers Group	bs						People	Settings
	Users (12)						Add User	
	User Name	User ID	Domain	Directory	VMware Verify Phone Nu	Groups	Status	
	Admin,Tenant	manfred	System Domain	System Directory	N/A	ALL USERS	Enabled	
	Lebio,Mark	Mark	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@	Enabled	
	L Dusello, Fernando	Fernando	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@	Enabled	
	L empowerlisbon,Empo	empowerlisbon@gmail.c	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled	
	Likin,Kevin	Kevin	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Domain Us	Enabled	
	L manfred,manfred@eu	manfred@euc-livefire.com	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled	
	Arios,Tom	Tom	euc-livefire.com	LivefireSNC	N/A	ALL USERS, Marketing@	Enabled	
	L mark.mark@euc-livefir	. mark@euc-livefire.com	Auth0	Auth0-Directory	N/A	ALL USERS	Enabled	

- 1. In the WorkspaceONE Access admin console navigate to Users & Groups
 - In the Users tab click on the user Debio, Mark

<back list<="" th="" to="" user=""><th></th><th>Profile Groups Two-Factor Authentication Apps</th></back>		Profile Groups Two-Factor Authentication Apps
	First Name	Mark
	Last Name	Debio
Mark Debio	Username	Mark
(Mark) Domain: euc-livefire.com	Email	mark@euc-livefire.com
Directory: LivefireSNC Status: 🔮 User is enabled	Role	User
Principal Name: Mark@euc-livefire.com		To assign or unassign the admin role to the user, click here
Distinguished Name: CN=Mark Debio,OU=Marketing,OU=Corp,DC=euc- livefire,DC=com		
External ID: d7f0751c-b022-407c-b086- 8ba634c9f22c		

2. In the user view click on **Two-Factor Authentication**

<back list<="" th="" to="" user=""><th>Profile Groups Two-Factor Authentication Apps</th></back>	Profile Groups Two-Factor Authentication Apps						
	Intelligent Hub Verify Preferred device receives Intelligent Hub verify requests. Reset will reset the user's selection of preferred device.						
Mark Debio Mark)	Reset						
Domain: euc-livefire.com	Device Friendly Name: Mark Android Android 10.0.0 X3X0						
Directory: LivefireSNC Status: Suser is enabled	UDID: b304064d9a9c078bc47413095a28a2548bac23061b						
	Make/Model: google Android SDK built for x86_64						
Principal Name: Mark@euc-livefire.com							
Distinguished Name: CN=Mark Debio,OU=Marketing,OU=Corp,DC=euc- ivefire,DC=com	VMware Verify						
External ID: d7f0751c-b022-407c-b086- 3ba634c9f22c	No VMware Verify devices found. Looks like the user hasn't enabled VMware Verify yet.						
✓ Enable	FIDO2						
Delete User	Add up to ten FIDO2 security keys. Only USB security keys are allowed.						

3. You will now find the option under the title **Intelligent Hub Verity** to Reset. **Don't click** on Reset for this lab as we will continue to use this device as the preferred device for Hub MFA.

This concludes the VMware Verify - Intelligent Hub lab.

Authored by: Simeon Frank