4. Unified Access Gateway / VMware Horizon integration into Workspace ONE Access

Overview

- Traditional Federation with VMware Horizon and Workspace ONE Access has been a popular approach and is used my many organizations.
- Organizations with High Security requirements do not like and SAML artifacts being validated internally
- In this session we look at the option to validate the SAML artifact on the Unified Access Gateway instead of forwarding the artifact internally.

Part 1. Enabling SAML federation with the VMware Unified Access Gateway for Workspace ONE Access as the IDP

The Federation of Unified Access Gateway and VMware Horizon with Workspace ONE Access will be done in three phases

- Phase 1. We enable and configure the SAML federation on 4 VMware Unified Access Gateway servers in a multi-site scenario
- Phase 2. We enable and configure the SAML Integration as a Web App in Workspace ONE Access
- Phase 3. We will create deep links in Workspace ONE Access for our Desktop entitlements

Step 1. Preparing to Federate the Unified Access Gateway with Workspace ONE Access



Note exporting the IDP.XML was accomplished on Day 1. Step 1 is here to remind you of the process. If you have an IDP.xml file downloaded in your Downloads folder on your ControlCenter server.

Move on to Step 2.

Workspace ONE*	ì
Username administrator	
Password	
System Domain	
Sign in	
Forgot Password?	
Change to a different domain	

- 1. On your ControlCenter server
 - Open your Workspace ONE Access, Admin console URL
 - Under Username
 - enter Administrator
 - Under Password
 - enter VMware1!
 - Select Sign In



- 2. In the Web Intelligent Hub Console
 - To the right,
 - select TA
 - From the dropdown
 - select Workspace ONE Access Console

← → C ☆ ● aw	-livefirernelmarchdev.vidmpreview.com/ws1adminui/#/workspace/resour	rces/web-apps/list
S my-ip.livefire.lab/ip 🔤 H	orizon ® Site 1 🛛 ym UAG-HZN-01a ym UAG-HZN-01b 🛛 🕅 Avi Vantage Contro	i 🔫 HZN Cloud 🚱 vi
Unsupported VMware Identity M New updates available. Learn with the second	lanager Connectors (versions 19.03.0.1 and earlier) will be discontinued soon. Action Requi hat's new in <u>Workspace ONE Access SaaS release notes</u> . Learn what's new in <u>Hub Services</u>	red if your organization is using release notes.
(R) Workspace ONE Acce	Q Search for users, groups, or applications	
Monitor Accounts Reso	urces containe secondgs	
Web Apps	Web Apps	
Virtual Apps	Add and configure web applications.	
Virtual Apps Collections		
Policies	NEW EDIT ASSIGN DELETE CATEGORIES V MORE V	SETTINGS
Global Launcher Preferences	Application	Туре
	Historoft Fusal	Mich Application Link

- 3. In the Workspace ONE Access Console
 - Select Resources
 - Under the Resources > WEB Apps area
 - Select SETTINGS

Settings	
Global Approvals SaaS Apps	Approvals Manage access to applications that require approval from your organization before applications can be used. Requiring approval automatically enables the Licensing
SAML Metadata	option within SaaS app configuration. When enabled users will need to request access to those applications from the Workspace ONE catalog.
	Enable Approvals
	No No
	SAVE
h	

- 4. In the **Settings** window
 - below SaaS Apps
 - select SAML Metadata

Settings						
Global Approvals	Download SAML Metadate	Gene	rate CSR			
SaaS Apps	This is your organization's logins from Workspace ON	SAML-signi E Access t	ing certificate o relying app	e. It is used to plications, su	o authent ch as Wel	
SAML Metadata	Google Apps. Copy and pa	ste the cer	tificate belov	v and send i	t to the re	
Application Sources	applications so they can ac integrating with other relyin metadata URLs below.	cept login: ng applicat	s from Works ions utilizing	pace ONE A SAML 2.0, y	ccess. Fo ou can us	
	Identity Provider (IdP) me					
	Service Provider (SP) met	Open li	nk in new tab	0		
	Signing Certificate ()	Open li Open li	nk in new wir nk in incogni	ndow to window		
	Expires	C				
	March 10, 2033	Copy lin	nk as nk address			
	Issuer	Incoact				
	Manager	inspect			nuty	
G Save As				A. Smarth Decord	in sole	~
Organize • New folder				C Controlling	(iii •	0
	n Maper (Land Approx and Concess and		Date modified 22/9222-950-244 22/9222-950-244 22/72203 6450 954 22/72203 6450 954 5/77/2203 640 954	Type File folder 34th Decoument 34th Decoument 34th Decoument 34th Decoument	Size 33.83 34.83 6.83 14.83	
File name idp.aml Save as type: XML Document (".aml)						
				- Com	Correct	

- 5. In the **Settings** window
 - in the right pane
 - below SAML Metadata
 - select & right click Identity Provider (IdP) metadata
 - in the drop down menu
 - select Save link as...
 - in Flle Explorer Save As window
 - ensure **Downloads** is selected **Quick Access** (default)
 - at the bottom of the window
 - select Save

Step 2. Enabling SAML Federation on Site 1, UAG-HZN-01a



- 1. On your **Site 1 Browser** profile
 - In the Favourites bar

• select the UAG-HZN-01a shortcut

- Coo VMware	
Unified Access Gateway	
admin	
Login	

- 2. In the VMware Unified Access Gateway login
 - in the **Username** area
 - enter admin
 - in the **Password** area
 - enter VMware1!
 - select Login



- below Configure Manually
 - click Select

Identity Bridging Settings	
Upload Identity Provider Metadata	
Upload Keytab Settings	4
Realm Settings	4
OCSP Settings	4

- 4. In the VMware Unified Access Gateway admin console
 - scroll down to Identity Bridging Settings
 - to the right of Upload Identity Provider Metadata
 - select the **GEAR** icon

Upload Identity Provider Metadata				
Entity ID	Workspace ONE Access	0		
* IDP Metadata	Select	0		
Encryption Certificate Type	None	· 0		
Always force SAML auth	\otimes	0		
	Save Cancel			

- 5. In the **Upload Identity Provider Metadata** window
 - next to Entity ID
 - enter Workspace ONE Access
 - next to IDP Metadata
 - click Select



- 6. In the **File Explorer Open** window
 - Quick Access > Downloads folder
 - (this should be the default)
 - select idp.xml
 - in the bottom right corner
 - select Open

Upload Identity Provider Metadata				
Entity ID	Workspace ONE Access	Ū		
* IDP Metadata	idp.xml	Change (j)		
Encryption Certificate Type	None	~ (i)		
Always force SAML auth		Ū		
	Save Cancel			

- 7. In the Upload Identity Provider Metadata window
 - next to Always force SAML auth
 - switch the Toggle from OFF to ON
 - select Save
 - scroll back up to the top of UAG admin console

Edge Service Settings	Active Sessions: 0	
• >	Horizon Settings	•
0	Reverse Proxy Settings	0
o	Tunnel Settings	٥

- 8. In the VMware Unified Access Gateway admin console
 - In the **General Settings** area
 - next to Edge Service Settings
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Horizon Settings		
Enable Horizon		0
Connection Server URL	https://horizon-01a.euc-livefire.com	0
Connection Server URL Thumbprint		0
Honor Connection Server Redirect	8	0
Connection Server IP mode	IPv4 v	0
Client Encryption Mode	ALLOWED 🗸	0
Re-Write Origin Header	8	0
Enable PCOIP		0
Disable PCOIP Legacy Certificate	8	0
PCOIP External URL	172.16.20.11:4172	0
Enable Blast	\bigcirc	0
Blast External URL	https://uag-hzn-01a.euc-livefire.com:443	0
Enable UDP Tunnel Server	\bigcirc	0
Blast Proxy Certificate	Select	0
Blast Allowed Host Header Values		0
Enable Tunnel	8	0
More V		
	Save Cancel	

- 9. In the **Horizon Settings** window
 - scroll down to the bottom
 - next to More
 - select the **expand** icon

Horizon Settings		
Enable Horizon		Ū
Connection Server URL	https://horizon-01a.euc-livefire.com	(i)
Minimum SHA Hash Size	Default 🗸	١
Connection Server URL Thumbprint		Ū
Honor Connection Server Redirect	\otimes	١
Connection Server IP mode	IPv4 🗸	١
Client Encryption Mode	ALLOWED 🗸	١
Auth Methods	Select 🗸	Ū
Health Check URI Path	Passthrough SAML	Ū
Re-Write Origin Header	SAML and Passthrough SAML and Unauthenticated	٦
Enable PCOIP	\bigcirc	١

- next to **Auth Methods**
 - from the **dropdown**
 - select SAML

(0
	Client Encryption Mode	ALLOWED 🗸			Œ
	Auth Methods	SAML	~		Œ
	Identity Provider *			~	0
		Workspace ONE Access			ta
	SAMI Audiences	Add new SAML Audience		0	a

- 11. In the Horizon Settings window
 - below Auth Methods
 - next to Identity Provider*
 - from the **dropdown**
 - select Workspace ONE Access

Client Encryption Mode	ALLOWED 🗸	Φ
Auth Methods	SAML 🗸	Ū
Identity Provider *	Workspace ONE Access	v 0
	Download SAML service provide	er metadata
SAML Audiences	Add new SAML Audience	• 0
Health Check URI Path	/favicon.ico	Ū

- 12. In the Horizon Settings window
 - below Identity Provider*
 - select Download SAML service provider metadata

Download SAML service provider metadata		
Identity Provider *	Workspace ONE Access	Ū
External Host Name	corp.euc-livefire.com	0
	Download Cancel	

- 13. In the **Download SAML service provider metadata** window
 - next to External Host Name

- enter corp.euc-livefire.com
- select Download

Client Custom Executables	Select 🗸	0
Host Port Redirect Mappings	Source Host:P Redirect Host:Port	0
Host Entries	Add new host entry	0
Disable HTML Access	\otimes	
Less *		
	Save Cancel	

- 14. In the **Horizon Settings** window
 - scroll down to the bottom of the window
 - select Save

Step 3. Enabling SAML Federation on Site 1, UAG-HZN-01b

0	x @) Wa	orkspace ONE	Acc	ess	×	6	🔊 Ne	w Tab
Horizo	n®Site 1	M	UAG-HZN-0	a	M	UAG-HZN-0	1Ь		Avi Vantag

- 1. On your **Site 1 Browser** profile
 - In the Favourites bar
 - select the UAG-HZN-01B shortcut

- Contraction of the second se
Unified Access Gateway
admin Login

- 2. In the VMware Unified Access Gateway login
 - in the **Username** area
 - enter admin
 - in the **Password** area
 - enter VMware1!
 - select Login



- below Configure Manually
 - click Select

Identity Bridging Settings	
Upload Identity Provider Metadata	
Upload Keytab Settings	4
Realm Settings	4
OCSP Settings	4

- 4. In the VMware Unified Access Gateway admin console
 - scroll down to Identity Bridging Settings
 - to the right of Upload Identity Provider Metadata
 - select the **GEAR** icon

Upload Identity Provider Metadata		
Entity ID	Workspace ONE Access	0
* IDP Metadata	Select	0
Encryption Certificate Type	None	· 0
Always force SAML auth	\otimes	0
	Save Cancel	

- 5. In the Upload Identity Provider Metadata window
 - next to Entity ID
 - enter Workspace ONE Access
 - next to IDP Metadata
 - click Select



- 6. In the **File Explorer Open** window
 - Quick Access > Downloads folder
 - (this should be the default)
 - select idp.xml
 - in the bottom right corner
 - select Open

Upload Identity Provider Metadata		
Entity ID	Workspace ONE Access	0
* IDP Metadata	ldp.xml	Change (j)
Encryption Certificate Type	None	✓ i)
Always force SAML auth		Ū
	Save Cancel	

- 7. In the Upload Identity Provider Metadata window
 - next to Always force SAML auth
 - switch the Toggle from OFF to ON
 - select Save
 - scroll back up to the top of UAG admin console

Edge Service Settings	Active Sessions: 0	
• >	Horizon Settings	•
0	Reverse Proxy Settings	0
o	Tunnel Settings	٥

- 8. In the VMware Unified Access Gateway admin console
 - In the **General Settings** area
 - next to Edge Service Settings
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Blast Proxy Certificate	Select (D
Blast Allowed Host Header Values		Ð
Enable Tunnel		Ð
More *		
	Save Cancel	
1		

- 9. In the Horizon Settings window
 - scroll down to the bottom
 - next to **More**
 - select the **expand** icon

Client Encryption Mode	ALLOWED ~
Auth Methods	Select 🗸
Health Check URI Path	Select Passthrough SAML
Re-Write Origin Header	SAML and Passthrough SAML and Unauthenticated
Enable PCOIP	

- next to **Auth Methods**
 - from the **dropdown**
 - select SAML

Client Encryption Mode	ALLOWED V
Auth Methods	SAML 🗸
Identity Provider *	~ (
	Workspace ONE Access ta
SAMI Audiences	Add new SAML Audience

- 11. In the **Horizon Settings** window
 - below Auth Methods
 - next to Identity Provider*
 - from the **dropdown**
 - select Workspace ONE Access

Client Custom Executables	Select	0
Host Port Redirect Mappings	Source Host:P Redirect Host:Port	•
Host Entries	Add new host entry	•
Disable HTML Access	\otimes	
Less *		
	Save Cancel	

- 12. In the Horizon Settings window
 - scroll down to the bottom of the window
 - select Save

Step 4. Enabling SAML Federation on Site 2, UAG-HZN-02a



- 1. On your ControlCenter server
 - switch to your Site 2 Browser profile
 - In the Favourites bar
 - select the UAG-HZN-02a shortcut

- Contraction of the second se
Unified Access Gateway
admin Login

- 2. In the VMware Unified Access Gateway login
 - in the **Username** area
 - enter admin
 - in the **Password** area
 - enter VMware1!
 - select Login



- below Configure Manually
 - click Select

Identity Bridging Settings	
Upload Identity Provider Metadata	
Upload Keytab Settings	4
Realm Settings	4
OCSP Settings	4

- 4. In the VMware Unified Access Gateway admin console
 - scroll down to Identity Bridging Settings
 - to the right of Upload Identity Provider Metadata
 - select the **GEAR** icon

Upload Identity Provider Me	etadata	
Entity ID	Workspace ONE Access	0
* IDP Metadata	Select	0
Encryption Certificate Type	None	• 0
Always force SAML auth	\otimes	0
	Save Cancel	

- 5. In the **Upload Identity Provider Metadata** window
 - next to Entity ID
 - enter Workspace ONE Access
 - next to IDP Metadata
 - click Select



- 6. In the **File Explorer Open** window
 - Quick Access > Downloads folder
 - (this should be the default)
 - select idp.xml
 - in the bottom right corner
 - select Open

Upload Identity Provider Me	etadata	
Entity ID	Workspace ONE Access	Ū
* IDP Metadata	idp.xml	Change (j)
Encryption Certificate Type	None	~ (i)
Always force SAML auth		Ū
	Save Cancel	

- 7. In the Upload Identity Provider Metadata window
 - next to Always force SAML auth
 - switch the Toggle from OFF to ON
 - select Save
 - scroll back up to the top of UAG admin console

Edge Service Settings	C C Active Sessions: 0	
• >	Horizon Settings	٢
0	Reverse Proxy Settings	•
0	Tunnel Settings	۰

- 8. In the VMware Unified Access Gateway admin console
 - In the **General Settings** area
 - next to Edge Service Settings
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Blast Proxy Certificate	Select	0
Blast Allowed Host Header Values		0
Enable Tunnel		0
Tunnel External URL	https://uag-hzn-01a.euc-livefire.com:443	0
Tunnel Proxy Certificate	Select	(i)
	Save Cancel	

- 9. In the Horizon Settings window
 - scroll down to the bottom
 - next to More
 - select the **expand** icon

Client Encryption Mode	ALLOWED ~	
Auth Methods	Select 🗸	
Health Check URI Path	Select Passthrough SAML	
Re-Write Origin Header	SAML and Passthrough SAML and Unauthenticated	
Enable PCOIP		

- next to **Auth Methods**
 - from the **dropdown**
 - select SAML

		0
Client Encryption Mode	ALLOWED 🗸	0
Auth Methods	SAML 🗸	Œ
Identity Provider *		~ (
	Workspace ONE Access	ta
SAMI Audiences	Add new SAML Audience	00

- 11. In the **Horizon Settings** window
 - below Auth Methods
 - next to Identity Provider*
 - from the **dropdown**
 - select Workspace ONE Access

Client Custom Executables	Select 🗸	0
Host Port Redirect Mappings	Source Host:P Redirect Host:Port	0
Host Entries	Add new host entry	0
Disable HTML Access	\otimes	
Less *		
	Save Cancel	
l		_

- 12. In the **Horizon Settings** window
 - scroll down to the bottom of the window
 - select Save

Step 5. Enabling SAML Federation on Site 2, UAG-HZN-02b



- 1. On your ControlCenter server
 - on your **Site 2 Browser** profile
 - In the Favourites bar
 - select the UAG-HZN-02b shortcut

- Contraction of the second se
Unified Access Gateway
admin Login

- 2. In the VMware Unified Access Gateway login
 - in the **Username** area
 - enter admin
 - in the **Password** area
 - enter VMware1!
 - select Login



- below Configure Manually
 - click Select

Identity Bridging Settings	
Upload Identity Provider Metadata	
Upload Keytab Settings	4
Realm Settings	4
OCSP Settings	4

- 4. In the VMware Unified Access Gateway admin console
 - scroll down to Identity Bridging Settings
 - to the right of Upload Identity Provider Metadata
 - select the **GEAR** icon

Upload Identity Provider Metadata				
Entity ID	Workspace ONE Access	0		
* IDP Metadata	Select	0		
Encryption Certificate Type	None	• 0		
Always force SAML auth	\otimes	0		
	Save Cancel			

- 5. In the Upload Identity Provider Metadata window
 - next to Entity ID
 - enter Workspace ONE Access
 - next to IDP Metadata
 - click Select



- 6. In the **File Explorer Open** window
 - Quick Access > Downloads folder
 - (this should be the default)
 - select idp.xml
 - in the bottom right corner
 - select Open

Upload Identity Provider Metadata				
Entity ID	Workspace ONE Access	Ū		
* IDP Metadata	idp.xml	Change (j)		
Encryption Certificate Type	None	~ (i)		
Always force SAML auth		Ū		
	Save Cancel			

- 7. In the Upload Identity Provider Metadata window
 - next to Always force SAML auth
 - switch the Toggle from OFF to ON
 - select Save
 - scroll back up to the top of UAG admin console

Edge Service Settings	Active Sessions: 0	
• >	Horizon Settings	•
0	Reverse Proxy Settings	0
o	Tunnel Settings	٥

- 8. In the VMware Unified Access Gateway admin console
 - In the **General Settings** area
 - next to Edge Service Settings
 - turn the **TOGGLE** from **OFF** to **ON**
 - to the right of **Horizon Settings**
 - select the **GEAR** icon

Blast Proxy Certificate	Select	0
Blast Allowed Host Header Values		0
Enable Tunnel		0
Tunnel External URL	https://uag-hzn-01a.euc-livefire.com:443	0
Tunnel Proxy Certificate	Select	0
	Save Cancel	

- 9. In the Horizon Settings window
 - scroll down to the bottom
 - next to More
 - select the **expand** icon

Client Encryption Mode	ALLOWED ~	
Auth Methods	Select 🗸	
Health Check URI Path	Select Passthrough SAML	
Re-Write Origin Header	SAML and Passthrough SAML and Unauthenticated	
Enable PCOIP		

- next to **Auth Methods**
 - from the **dropdown**
 - select SAML

				9
Client Encryption Mode	ALLOWED 🗸		(1
Auth Methods	SAML	*	(1
Identity Provider *			~	1
	Workspace ONE Access		t	а
SAMI Audiences	Add new SAML Audience		0	ø

- 11. In the **Horizon Settings** window
 - below Auth Methods
 - next to Identity Provider*
 - from the **dropdown**
 - select Workspace ONE Access

Client Custom Executables	Select 🗸	0
Host Port Redirect Mappings	Source Host:P Redirect Host:Port	0
Host Entries	Add new host entry	0
Disable HTML Access	\otimes	
Less *		
	Save Cancel	

- 12. In the Horizon Settings window
 - scroll down to the bottom of the window
 - select Save

Part 2. Configuring the SAML Federation for Horizon

For TrueSSO to work the Horizon SAML authenticator is required. We configure this on both Site 1 and Site 2

Step 1. Configuring the SAML federation with VMware Horizon on Site 1

	Арр	s 🔇 my-ip.livefire.	.lab/ip vm VMware	Horiz	on® NSX ma	anager 🜵 App	Volumes Mana	S UAG	S vCenter
	vmw	VMware Ho	rizon®		Pod Clu	uster-HORIZON	N Q	User Sea	irch
	C Update	ed 01/13/2022, 4:50 I	PM 🗸						
ľ	Sessio	ns	<u>0</u>	Ser	rvers				
I	Proble	em vCenter VMs	Q	vc	enter Servers	Gateways	Connection	Servers	
l	Proble	em RDS Hosts	1						
N	Events	;	<u>4309</u>	Ad	d Edit	Remove	More ~		
I	Syster	n Health	<u>0</u>						
	Ma	chines	^						
I.	Settin	gs	× 🗲						
Ľ	Ser	vers	-		vCenter Server				VM Disk Spa
	Dor	nains		0	vcenter.euc-livef	ire.com(adminis	strator@vsphere.	local)	\oslash

- 1. On your ControlCenter server
 - Site 1 Browser
 - In the Horizon Admin Console
 - In the **Inventory**
 - expand Settings,
 - select Servers
 - In the Servers area
 - select the Connection Servers tab

Servers
vCenter Servers Gateways Connection Servers
Enable Edit Backup Now
Connection Server Version
HORIZON-01A 8.8.0-21073694

- 2. Under Servers
 - Select the radio button to next HORIZON-01a
 - Select Edit

	General	Authentication
Tags		
Tags can be up	sed to restrict which deskto	op pools can be accessed through this Connection
10.52 0011 00 01		

- 3. On the Edit Connection Server Settings page
 - Select the Authentication tab.

Edit Conn	ection Server Set	tings			
	General	Authentication			
Delegation of	authentication to VMware	Horizon (SAML 2.0 Authenticator):			
Disabled					
Disabled					
Allowed Required					
Delegation	General				
Allowed					
SAML Auth	nenticator				
No Enable	d Authenticator config	gured			
Manage	SAML Authenticators				
Create at le	east one SAML Auther	nticator and enable it, fi			

- 4. On the Authentication tab
 - below **Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):**
 - On the **Drop down Arrow**
 - Select Allowed,
 - Select the Manage SAML Authenticators box

	Manage SAML Authenticators				
(SAML Auth	enticators Edit	configured in Remove	n this Horizon e	
	Name		Descriptio	on St	
	No record	ds availabl	e.		

- 5. On the Manage SAML Authenticators box
 - Select Add

* Type	 Dynamic 	 Static 	
* Label			
Workspace ONE Access			
Description			
* Metadata URL			
https://aw-livefirewwkorn.vid	mpreview.com/SAAS/API/1.0/GET/me	tadata/idp.xml	
Administration URL			
* TrueSSO Trigger Mode 🛞			
Enabled		~	
 Enabled for Connection 	Server		

- 6. In the Add SAML 2.0 Authenticator window.
 - Ensure Dynamic radio button is selected,
 - Enter the following:
 - Under Label:
 - type Workspace ONE Access
 - Under Metadata URL : enter
 - https://YOUR CUSTOM Access URL/SAAS/API/1.0/GET/metadata/idp.xml
 - e.g. https://aw-euclivefirefran.vidmpreview.com/SAAS/API/1.0/GET/metadata/ idp.xml
 - Under * TrueSSO Trigger Mode
 - from the dropdown
 - select Enabled
 - Select OK

Manage S/	AML Authentica	itors			\times	
SAML Authentica	L Authenticators configured in this Horizon environment					
Add Edit	Remove					
Name	Description	Status	Туре	Admin URL		
Workspace ON Access	E	Enabled	Dynamic		*	
					v	
				Cancel	ОК	

7. In the Manage SAML Authenticators window

• Select **OK** to close

	Authentication	Backup
Delegation of authentication to VMwar	e Horizon (SAML 2.0 Authenticator):	
Allowed	~	
SAML Authenticator		
Workspace ONE Access		
Manage SAML Authenticators		
* Workspace ONE Server Hostname		
Block connections from clients that	don't support Workspace ONE mode 🛛	
Horizon Authentication		
Changes to authentication settings will ta	ane errett om next user logan.	
smart card authentication for users:		
Optional	~	

- 8. In the Connection Server Settings
 - Select OK

Step 2. Configuring the SAML federation with VMware Horizon on Site 2



- 1. On your ControlCenter server
 - Site 2 Browser
 - In the Horizon Admin Console
 - Inventory pane
 - expand Settings,
 - select Servers
 - In the middle pane
 - select the Connection Servers tab
| - | |
|---------------|---|
| ~
<u>0</u> | Servers |
| <u>0</u> | vCenter Servers Gateways Connection Servers G |
| <u>0</u> | |
| <u>6</u> | Enable Disable Edit Now |
| <u>0</u> | |
| ^ | |
| | Connection Server Version PC |
| | HORIZON-02A O.0.0-21073094 Ins |
| | |

- 2. Under Servers
 - select the radio button to next HORIZON-02a
 - select Edit

	General	Authentication
Tags		
Tags can be	e used to restrict which deskto	op pools can be accessed through this Connection

- 3. On the Edit Connection Server Settings page
 - select the Authentication tab.

General	Authentication
Delegation of authentication to V	Mware Horizon (SAML 2.0 Authenticator):
Disabled	*
Disabled	
Allowed	
Reduired	
Manage SAML Authenticators	
Manage SAML Authenticators	Settinas
Manage SAML Authenticators Edit Connection Server	Settings
Manage SAML Authenticators Edit Connection Server General	Settings
Manage SAML Authenticators Edit Connection Server General	Settings
Manage SAML Authenticators Edit Connection Server General Asterisk (*) denotes required field	Settings
Manage SAML Authenticators Edit Connection Server General Atterisk (*) denotes required field Delegation of authentication to VMw	Authentication vare Horizon (SAML 2.0 Authenticator)
Manage SAML Authenticators Edit Connection Server General Asterisk (*) denotes required field Delegation of authentication to VMw Allowed	Authentication vare Horizon (SAML 2.0 Authenticator)
Manage SAML Authenticators Edit Connection Server General Asterisk (*) denotes required field Delegation of authentication to VMw Allowed SAML Authenticator	Settings Authentication vare Horizon (SAML 2.0 Authenticator)
Manage SAML Authenticators Edit Connection Server General Asterisk (*) denotes required field Delegation of authentication to VMw Allowed SAML Authenticator Workspace ONE Access	Settings Authentication Authenticator)
Manage SAML Authenticators Edit Connection Server General Asterisk (*) denotes required field Delegation of authentication to VMw Allowed SAML Authenticator Workspace ONE Access Manage SAML Authenticators	Settings Authentication vare Horizon (SAML 2.0 Authenticator)

- 4. In the **Edit Connection Server Settings** window
 - on the Authentication tab,
 - under Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):
 - from the Drop down Arrow
 - select Allowed,
 - below SAML Authenticator
 - select the Manage SAML Authenticators box

Manage	Manage SAML Authenticators		
SAML Auther	Edit Remove	in this Horizon e	
Name	Descript	ion St	
No records	available.		

- 5. On the Manage SAML Authenticators box
 - Select Add

* Туре	 Dynamic 	 Static 		
• Label				
Workspace ONE Access				
Description				
* Metadata URL				
https://aw-livefirewwkorn.vidr	npreview.com/SAAS/API/1.0/GE	T/metadata/idp.xm		
Administration URL				
 TrueSSO Trigger Mode ① 				
Enabled			~	
 Enabled for Connection S 	erver			

- 6. In the Add SAML 2.0 Authenticator window.
 - ensure **Dynamic** radio button is selected,
 - enter the following:

- under Label:
 - type Workspace ONE Access
- Under Metadata URL : enter
 - https://YOUR CUSTOM Access URL/SAAS/API/1.0/GET/metadata/idp.xml
 - e.g. https://aw-euclivefirefran.vidmpreview.com/SAAS/API/1.0/GET/ metadata/idp.xml
- under * TrueSSO Trigger Mode
 - from the dropdown
 - select **Enabled**
- select OK

Manage SAML Authenticators				\times	
SAML Authenticat	tors configured in this Ho	orizon environment			
Name	Description	Status	Туре	Admin URL	
Workspace ON Access	E	Enabled	Dynamic		^
					~
				Cancel	ОК

- 7. In the Manage SAML Authenticators window
 - Select **OK** to close

General	Authentication	Backup	
Delegation of authentication to VMware Ho	rizon (SAML 2.0 Authenticator):		
Allowed	~		
SAML Authenticator			
Workspace ONE Access			
Manage SAML Authenticators			
Enable Workspace ONE mode 🛈			
Workspace ONE Server Hostname			
Block connections from clients that don	't support Workspace ONE mode 🔘		
Horizon Authentication			
Changes to authentication settings will take e	effect on next user login.		
Smart card authentication for users:			
Optional	¥		
Disconnect user sessions on smart card	removal		

- 8. In the Connection Server Settings
 - Select OK

Part 3. Configuring Workspace ONE Access for VMware Unified Access as the Service Provider

In this section perform the Workspace ONE Access part of the SAML Federation process with VMware Unified Access Gateway

Configuring Workspace ONE Access for VMware Unified Access as the Service Provider

Workspace ONE*	
Username administrator	
Password	
System Domain	
Sign in	
Forgot Password?	
Change to a different domain	

- 1. On your ControlCenter server
 - Open your **Workspace ONE Access**, Admin console URL
 - Under Username
 - enter Administrator
 - Under Password
 - enter VMware1!
 - Select Sign In

	TA
TA Tenant Admin	
Workspace ONE Access Console	
Manage Hub Experience	
Account	
Sign out	\ominus

- 2. In the **Web Intelligent Hub** Console
 - To the right,
 - select TA
 - From the dropdown
 - select Workspace ONE Access Console

← → C 🏠 🔒 aw-livefirernelmarchdev.vidmpreview.com/ws1adminui/#/workspace/resources/web-apps/list				
S my-ip.livefire.lab/ip 🧰 H	lorizon®Site 1 🛛 🚾 UAG-HZN-01a	uag-HZN-01b	🔼 Avi Vantage Control	🔫 HZN Cloud 🛛 🐼 🗤
Unsupported VMware Identity M New updates available. Learn w	Manager Connectors (versions 19.03.0.1 a hat's new in <u>Workspace ONE Access Sa</u>	and earlier) will be discor aS release notes. Learn v	ntinued soon. Action Required i what's new in <u>Hub Services rele</u>	f your organization is using ase notes.
(R) Workspace ONE Acc	ess Q Search for users, grou	ups, or applications		
Monitor Accounts Reso	ources actions actiongs			
Web Apps	Web Apps			
Virtual Apps	Add and configure web application	ns.		
Virtual Apps Collections	_			
Policies	NEW	DECETE CATE		SETTINGS
Global Launcher Preferences	Application		Туре	•
	Hissocoft Even		14(-)4(-)	Application Link

- 3. In the Workspace ONE Access Console
 - select Resources
 - Under the Resources > WEB Apps area
 - select NEW

New SaaS Application	
1 Definition	Definition
2 Configuration 3 Access Policies 4 Summary	Search () Q OR BROWSE FROM CATALOG Name * () Unified Access Gateway SAML SP
CANCEL NEXT	Description ()
	Ģ

- 4. In the **New SaaS Application** window
 - 1. In the Definition area
 - under Name
 - enter Unified Access Gateway SAML SP
 - Under Icon
 - select **SELECT FILE** ...



- 5. In the **File Explorer > Open** window
 - In the Quick Access pane
 - select Desktop
 - in the **Desktop** area
 - select software > UAG > Icons
 - in the **Icons** folder
 - select UAG.png
 - select Open

New SaaS Application	>
	OR BROWSE FROM CATALOG
1 Definition	Name *①
2 Configuration	Unified Access Gateway SAML SP
3 Access Policies	Description (j)
4 Summary	
	Letter &
	Icon ()
	SELECT FILE
	Unified Access Gateway
	Category ①
	¥
	Selected Categories
	CANCEL NEXT

- 6. In the **New SaaS Application** window
 - 1. In the **Definition** area
 - Select NEXT



- 7. On the **ControlCenter** server
 - from the **Taskbar**
 - select the Folder icon



- 8. In the File Explorer window
 - from the **Quick Access** pane
 - select Downloads

📕 🔄 🧧 🖛 🛛 Downloads	5						
File Home Share	View						
Pin to Quick Copy Paste	✓ Cut	Move to •	Copy to •	Delete Renar	ne New folder		
Clipboard			Org	anize			
← → ~ ↑ ↓ > This	← → ~ ↑ 🕹 > This PC > Downloads						
A Quick access	Name	C			^		
🕂 Downloads 🚿	ide yml	enre.com	0	Open			
🔮 Documents 🖈	e sp.xml			-114			
📰 Pictures 🛷	🔄 VidmAirWat	chRoot	E 📔 E	dit with Notepa	ad++		
icons	Workspace (ONE Acce	l de la	1			
Site1				Open with			
Site2			(Give access to	versions		

- 9. In the **File Explorer** window
 - Downloads folder

- select corp.euc-livefire.com
 - select & right-click Edit with Notepad++

fle Edi	Searc	1 View	Encoding	Lang	uage	Settings	Tools	Macro	Run	Plugi	ins \	Windov	v ?									
a 🚽 B		8 🐚 🖥	à ⊀ %i		2 d	100	ha 🔍	ي چ	53	Ξ2 1	請	a [1	£1 🖿	۲	۲	•					
new 1	🛛 🔚 Fix	Engine Jo	g 🖂 🔚 cor	p.euc-liv	vefire.co	m.xmi 🖾	1															
1		1 vers	ion="1.0)" en	codir	ig="UT	P-8"?>	<md:en< th=""><th>tity</th><th>lesor</th><th>ipto</th><th>r xn</th><th>lnsiz</th><th>d="ur</th><th>n:oa</th><th>s1s:</th><th>name</th><th>site</th><th>SAML</th><th>:2.0:</th><th>netada</th><th>ta" e</th></md:en<>	tity	lesor	ipto	r xn	lnsiz	d="ur	n:oa	s1s:	name	site	SAML	:2.0:	netada	ta" e
2	BhM	ROIxGa	AZBgNVB/	lg TEk	dyZWE	OZXI9	TWPuY2	hlc3R1	cjBQ	4A4GA	1UEE	XMHU:	2FsZs	9yZDE	YMBY	G						
3	A10	ChMPU2	VjdGlnby	BMaW	1pdGN	KMTCW	NOYDVO	QDEy57	ZWNOa	WdvI	FJT	SBED	21haW	4gVmF	saWR	h						
4	dGl	biBTZW	N1cnUgU:	2Vydm/	VyIEN	IBMB4X	DTIzMD	IxNzAw	MDAM!	(FoXD	TION	(DMx0)	TINT	'k10Vo	WHILE	b						
5	MBk	ALUEAN	wSK151d	MtbG	12ZW7	penUu	Y29tMI	ICIJAN	Bgkql	ki09	WOB/	QEFA	AOCAg	BAMII	CCgR	C						
6	AgE	sMiON/	zb635Jb	njFfq	SexF1	tui76	q9LbRd	D/ynR3	01RV	:NoOb	Yxe)	HAPO	4qFp0	+E+Ih	fB9H	9						
7	Ajs	41eZ11	Zj6yHNV	TbIX8	a8Lri	IRTE	GFbZtw	WB/yTo	97Rn9	9Iyp1	ERAU	Jr1oA	K02d1	9XUBh	W7uT	5						
8	Lo+	2+RX+1	J4GnjRfs	BROB	8doM]	[a/RT4	+R3e6e	24wT5F	xlxz)	lQnAn	8Z1n	DNOR	8Qk9Y	mxGdg	GaGe	4						
9	1000	taI+81	C/OLnln	/6uYf	1JzAt	kkTgf	LQ1JZs	zF3DRc	nOlL	t5nx	7ng5	VsdR	nzP9E	CXGKA	Yriw	s						
10	YMC	tNvBs6	ipNd4xCvi	D7TiE	NpSal	pITLM	TOUgvy	106FI0	P65R	/Bex0	LUpy	C6pX	YZWr5	PfqWt	fZ+r	4						
11	B5X	1AoTS4	5T4fXU1/	lxOR/	RtlZr	synCf	QqMhSB	du7ALg	0/031	YQou	GBFS	505HCI	RPBmV	QMskV	E6zd	D						
12	107	it2kV4	CgZkzava	ayn7y	1pBB4	3rdee	RLHoms.	YGKSTW	arrM,	a2FU/	9VJ6	Pxbf	vp3g/	Ah+a6	+zcf	z						
13	//X	JPQH8t	wtBPSj5M	liBvh	F5QNS	gqXiU	HSOomG	kyg0T+	fpJ6	NpRH	EVW	ERq9	tSNCT	07VXu	09jJ	v						
14	Pc5	k2taCE	Wa5MS4ni	df04	nksxp	pJH01	Evi1t2	t6bMB9	nFA9t	IfDI	tC4p	W7Nr	70c+0	k8pzu	hmVK	n						
15	M+84	AWEAAS	OCANONG	MEMB	8GA10	JdIwQY	MBaAFI	2MXsR0	rYrh	1+mb+	ZsF(lbgBjl	WIII MI	DGA10	dDgQ	N.						
16	BBR	o9wCX/	E496akdi	CVV09	2041	(3wzAO	BgNVBQ	BBA18E	BAMCE	BaAwD	AYD'	ROTA	QH/BA	IWADA	dBgN	v						
17	HSU	FjAUBq	grBgEFB(2cDAQ	YIKW	BBQUH	AwIwSQ	YDVR0g	BEIW	DADE	gsrl	geea	bIxAQ	ICBZA	1MCM	G						
18	CCa	AQUFBA	IBFhdodi	Rwez	ovL38	11Y3Rp	Z28uY2	9tLONQ	UZAII	3gZng	QwB/	/dgs/di	rocco	SCAQU.	FBWE	в						
19	BBg	djBPBq	grBgEFB(2cmAo	ZDallF	RocDov	L2Nyd0	5zZWN0	aWdvi	.mNvb	S9T2	WNOal	WdvU1	MBRG9	tYW1	а.						
20	VnF:	aWRhd0	lvblNlY:	svyzv	Nlcn2	lckNB	LaNydD	AjBggr	BgEFI	3QcwA	YYX	HROci	DovL2	9jc3A	uc2V	1						
21	dG1	by5jb2	OwLwYDVE	RORBO	gwJo]	SK151	dMMtbG	12ZWZp	cnUu)	(29tg	hB1c	WMtb	G12ZW	ZpemU	uY29	t						
22	MIII	TOXER	(YBBAHWe)	lEAg	SCAW	EggPp	AWcAdg	B2/4g/	Crb71	VECY	cził	17o0t1	KTNuy	ncaEI	Kn+Z	n						
23	TFO	daaaay	Zfoe2EAJ	AEAw	BHME	CIQDG	zxddKE	JZHZFI	2WbV	Joe+p	ZLPO	DLD	bwpv/	hXaNC	logI	σ						
24	byP	mNTD63	CzMDhV1I	RC 6NK	AYRC	EhJOL	6ogar6	GqYnQA	dQDat	r9rP	7W21	(p+bw	rtca	hwkXF	su1G	R						
ensible	Markun	annuan	file	_	_						le	nath • 3	1456	lines + 33		_		n · 1	Col-1	Pos-	1	

- 10. In the **Notepad++** application
 - with your keyboard
 - enter CTRL + A
 - enter CTRL + C
 - switch back to the New SaaS Application wizard



- 11. In the **New SaaS Application** window
 - 2. In the **Configuration** area
 - the box below URL / XML
 - paste your corp.euc-livefire.com.xml metadata
 - scroll down the Configuration area to the bottom
 - below Show in User Portal
 - change the Toggle from ON to OFF
 - select NEXT

New SaaS Application		×
1 Definition 2 Configuration 3 Access Policies 4 Summary	Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.	2
	CANCEL BACK NEX	

- 12. In the New Saas Application window,
 - 3. In the Access Policies section
 - Select NEXT

New SaaS Application	n I	×
1 Definition 2 Configuration 3 Access Policies 4 Summary	Definition Name Unified Access Gateway SAML SP Description - Kon @== Categories - Categories - Configuration	
	Authentication Type SAML 2.0 Configuration URL/XML URL/XML xml version="1.0" encoding="UTF-8"? <md:entitydescriptor <br="" xmlns:md="umcoasis:names:tc:SAML:2.0metadata">Relay State URL ADVANCED PROPERTIES ~</md:entitydescriptor>	
	CANCEL BACK SAVE & ASSIGN SAV	/E

- 13. In the New Saas Application window,
 - 4. In the **Summary** section
 - Select SAVE & ASSIGN

) Application: 'Unified Access Gateway SAML SP added successfully Selected App(s): Unified Access Gateway SAML SP Jess / User Groups C, sale A: SalestReuc-livefire.com		l
Selected App(s): Unified Access Gateway SAML SP Jaes / User Groups C, said & SalestRuc-livefire.com		
seected App(s): United Access Gateway SAML SP Liser / User droups C. see Sales@euclivefire.com		
Q. said & SalessReuc-livefine.com		
충 Sales#euc-livefire.com &		
	Deployment Type	
	No assignments found.	
Assign		
) Application: "Unified Access Gateway SAML SP' a	dded successfully.	
Selected App(s): Unified Access Gat	eway SAML SP	
Isers / User Groups	,	
O Dev		
0,000		
Selected Users / User Groups		Deployment Type
쑴 Sales@euc-livefire.com		Automatic
영 Developers@euc-livefire.com	_	Automatic
_		
CANCEL SAVE		

- 14. In the **Assign** window
 - Under Users / Groups

- Enter Sales
 - Select Sales@euc-livefire.com
- Enter **Devel**
 - Select Developers@euc-livefire.com
- Under **Deployment** type
 - From the dropdowns
 - Ensure both Sales and Developers are set to
 - Automatic
- In the bottom right corner
 - select SAVE

lateway ®	X (8) Workspace ONE Access X M Unified Access Gateway	◎ X 🏧 VMware Hor
🔒 aw-	livefirernelmarchdev.vidmpreview.com/ws1adminui/#/workspace/resource	es/web-apps/list
ip 🚾 Ho	rizon®Site 1 🛛 🏧 UAG-HZN-01a 🐜 UAG-HZN-01b 🔣 Avi Vantage Control	🔫 HZN Cloud 🛛 🛃 vcenter
re Identity Ma ple. Learn wha	anager Connectors (versions 19.03.0.1 and earlier) will be discontinued soon. Action Required at's new in <u>Workspace ONE Access SaaS release notes</u> . Learn what's new in <u>Hub Services re</u>	i if your organization is using older (lease notes.
ONE Acce	ss Q Search for users, groups, or applications	
ts Resou	rces Integrations Settings	
pns	Web Apps Add and configure web applications.	SETTINGS
ierences	Application	туре
		Web Application Link
	Kicrosoft Outlook	Web Application Link
	Microsoft Powerpoint	Web Application Link
	Microsoft Word	Web Application Link
		SAML 2.0

- 15. In your **Workspace ONE Access** Console
 - Web Apps interface
 - Note your Unified Access Gateway SAML SP Web APP

Part 4. Deploying VMware Horizon Deep Links for entitlements

As we are not using the Workspace ONE Access Connector to sync entitlements, we will create Deep Links for our Entitlements and assign these to our Security Groups

Step 1. Deploying a Deep link for the Enterprise Corp Instant Clone Global Entitlement



- 1. On your ControlCenter server
 - Open your Workspace ONE Access, Admin console URL
 - Under Username
 - enter Administrator
 - Under Password
 - enter VMware1!
 - Select Sign In

	TA
TA Tenant Admin	
Workspace ONE Access Console	
Manage Hub Experience	
Account	
Sign out	\ominus

- 2. In the **Web Intelligent Hub** Console
 - To the right,
 - select TA
 - From the dropdown
 - select Workspace ONE Access Console

← → C ① ⓐ av	v-livefirernelmarchdev.vidmprevi	ew.com/ws1adminu	ii/#/workspace/resources	:/web-apps/list
S my-ip.livefire.lab/ip 🧰 H	lorizon®Site 1 🛛 🚾 UAG-HZN-01a	uag-HZN-01b	🔼 Avi Vantage Control	🔫 HZN Cloud 🛛 🐼 🗤
Unsupported VMware Identity M New updates available. Learn w	Manager Connectors (versions 19.03.0.1 a hat's new in <u>Workspace ONE Access Sa</u>	and earlier) will be discor aS release notes. Learn v	ntinued soon. Action Required i what's new in <u>Hub Services rele</u>	f your organization is using ase notes.
(R) Workspace ONE Acc	ess Q Search for users, grou	ups, or applications		
Monitor Accounts Reso	ources actions actiongs			
Web Apps	Web Apps			
Virtual Apps	Add and configure web application	ns.		
Virtual Apps Collections	_			
Policies	NEW	DECETE CATE		SETTINGS
Global Launcher Preferences	Application		Туре	•
	Hissocoft Even		14(-)4(-)	Application Link

- 3. In the Workspace ONE Access Console
 - select Resources
 - Under the Resources > WEB Apps area
 - select NEW

1 Definition	Definition
2 Configuration	Name * (1)
3 Summary	Enterprise Instant Clone Windows 11 Desktops
	Description (j)
	lcon (j)
	SELECT FILE

- 5. In the New SaaS Application window
 - 1. In the Definition area
 - under Name
 - enter Enterprise Instant Clone Windows 11 Desktops
 - under Icon
 - select SELECT FILE ...

Organize • New folde					8	
A	Name	Date modified	Tune	Gra	E.c.	
🖈 Quick access		Date modified	170~	565		
Desktop 🖈	Enterprise Desktop.jpg	4/17/2023 5:02 PM	JPG File	8 KB		
- Downloads 🖈	Excel_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Documente et	Microsoft Teams_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
Documents y	OneDrive_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
Pictures x	OneNote_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Dump	Outlook_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
lcons	PowerPoint_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
Site1	SharePoint_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
Site2	Skype_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
	📧 uag.png	3/22/2023 11:07 AM	PNG File	6 KB		
This PC	Word_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
3D Objects	Yammer_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Desktop						
Documents						
Downloads						
h Music						
E Dictures						
Videos						
Local Disk (C:)						
Network						
horizon-01a.euc						
treliant						
- content v						

- 6. In the **File Explorer** > **Open** window
 - In the Quick Access pane
 - select **Desktop**
 - in the **Desktop** area
 - select software > software > lcons
 - in the **Icons** folder
 - select Enterprise Desktop.jpg
 - select Open

New SaaS Application		×
1 Definition	OR BROWSE FROM CATALOG	
2 Configuration 3 Access Policies 4 Summary	Name * () Enterprise Full Clone Windows 11 Desktops Description () Kon () SELECT FILE	• •
	Category () 	хт

- 7. In the **New SaaS Application** window
 - 1. In the **Definition** area
 - Select NEXT

New SaaS Application	
1 Definition	Single Sign-On
2 Configuration	Authentication Type • 🛈
3 Access Policies	SAML 2.0 OpenID Connect SAML 1.1 SAML 2.0
4 Juninary	Web Application Link

- 8. In the **New SaaS Application** window
 - 2. In the **Configuration** area
 - below Authentication Type *
 - from the **dropdown**
 - select Web Application Link

New SaaS Application	
1 Definition 2 Configuration 3 Summary	Single Sign-On Authentication Type • Web Application Link Target URL • https://corp.euc-livefire.com/portal/nativeclient Open in Workspace ONE Web No
CANCEL	BACK

- 9. In the New SaaS Application window
 - 2. In the **Configuration** area
 - below Target URL *
 - enter the following URL

https://corp.euc-livefire.com/portal/nativeclient/ Enterprise_Desktop?action=startsession&desktopProtocol=BLAST&launchMinimized=false

- In the bottom right corner
 - select **NEXT**

New SaaS Application		×
1 Definition 2 Configuration 3 Summary	Definition Name Enterprise Full Clone Windows 11 Desktops Description - Icon Categories - Configuration	
	Authentication Type None Target URL https://corp.euc-livefire.com/portal/nativeclient/Enterprise_Desktop?action=start-session&desktopProtocol=BLAST Access Policies Open in Workspace ONE Web No	1
	CANCEL BACK SAVE & ASSIGN SAV	/E

- 10. In the **New Saas Application** window,
 - 3. In the **Summary** section
 - Select SAVE & ASSIGN

Assign		
Selected App(s): Enterprise Full Clo	one Windows 11 Desktops	5
Users / User Groups O, dev		
路 Developers@euc-livefire.com	loyment Type	Entitlement Type
容 Developers@euc-livefire.com	<u>Autom</u> etic ~	Include

11. In the **Assign** window

- Under Users / Groups
 - Enter Devel
 - Select Developers@euc-livefire.com

sers / User Groups		
Q sales 쫅 Sales@euc-livefire.com		
	loyment Type	
路 Developers@euc-livefire.com	Automatic	
Selected Users / User Groups	Deployment Type	
路 Developers@euc-livefire.com	Automatic	~
중 Sales@euc-livefire.com	Automatic	\sim
쭑 Developers@euc-livefire.com 쭑 Sales@euc-livefire.com	Automatic	_

12. In the **Assign** window

- Under Users / Groups
 - Enter sales
 - select sales@euc-livefire.com
- Under **Deployment** type
 - From the **dropdowns**
 - Ensure both Sales and Developers are set to
 - Automatic
- In the bottom right corner
 - select SAVE

Acces	s	Q Search for users, groups, or applications	
Resour	ces	Integrations Settings	
	Add	eb Apps and configure web applications.	TTINGS
ces		Application	Туре
		Enterprise Instant Clone Windows 11 Desktops	Web Application Link
	O	Microsoft Excel	Web Application Link
		Microsoft Outlook	Web Application Link
	0	<u>Microsoft Powerpoint</u>	Web Application Link
		<u>Microsoft Word</u>	Web Application Link
		+ Unified Access Gateway SAML SP	SAML 2.0
			,

- 13. In your **Workspace ONE Access** Console
 - Web Apps interface
 - Note your Enterprise Instant Clone Windows 11 Desktops Web Application Link

Step 2. Deploying a Deep link for the Enterprise Full Clone Global Entitlement



- 1. In the Workspace ONE Access Console
 - under the Resources > WEB Apps area
 - select NEW

New SaaS Application	
1 Definition	Definition
2 Configuration 3 Access Policies 4 Summary	Search C OR BROWSE FROM CATALOG Name *
	Enterprise Full Clone Desktops
	Icon () SELECT FILE

- 2. In the **New SaaS Application** window
 - 1. In the Definition area
 - under Name
 - enter Enterprise Full Clone Desktops
 - under Icon
 - select **SELECT FILE** ...

T	> Netw	vork > nonzon-uta.euc-liverire.com > s	ortware > icons	~ C	Search icons		
Organize 🔻 🛛 N	ew folder					E 🔹 🔲	•
A Quick accord	^	Name	Date modified	Туре	Size		
Decident		e desktop-developer.jpg	4/17/2023 6:22 PM	JPG File	14 KB		
Desktop	*	Enterprise Desktop.jpg	4/17/2023 5:02 PM	JPG File	8 KB		
Downloads	*	Excel_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Documents	*	Microsoft Teams_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
Pictures	*	OneDrive_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
- Dump		OneNote_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Icons		Outlook_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
Site1		PowerPoint_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB		
Cite?		SharePoint_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
Sitez		Skype_128x128.png	3/6/2023 2:28 PM	PNG File	5 KB		
💻 This PC		🖻 uag.png	3/22/2023 11:07 AM	PNG File	6 KB		
3D Objects		Word_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
Desktop		Yammer_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB		
B Documents							
Downloads	~						
	File nam	e: desktop-developer.ing		~	All Files (*.*)		,

- 3. In the **File Explorer** > **Open** window
 - In the Quick Access pane
 - select **Desktop**
 - in the **Desktop** area
 - select software > software > lcons
 - in the **Icons** folder
 - select desktop-developer.jpg
 - select Open

New SaaS Application		×
	OR BROWSE FROM CATALOG	-
1 Definition	Name *①	
2 Configuration	Enterprise Full Clone Desktops	
3 Access Policies	Description ()	
4 Summary		1
		6
	lcon (j)	
	SELECT FILE	
	Developer.	
	Category ①	
	Selected Categories	
	CANCEL	хт

- 4. In the **New SaaS Application** window
 - 1. In the **Definition** area
 - Select NEXT

New SaaS Application	
1 Definition	Single Sign-On
2 Configuration	Authentication Type • (j)
3 Access Policies	SAML 2.0 OpenID Connect SAML 1.1
4 Summary	SAML 2.0 Web Application Link

- 5. In the **New SaaS Application** window
 - 2. In the **Configuration** area
 - below Authentication Type *
 - from the **dropdown**
 - select Web Application Link

New SaaS Application	
1 Definition 2 Configuration 3 Summary	Single Sign-On Authentication Type • Web Application Link Target URL • https://corp.euc-livefire.com/portal/nativeclient
CANCEL	Open in Workspace ONE Web () No BACK NEXT

- 6. In the **New SaaS Application** window
 - 2. In the **Configuration** area
 - below Target URL *
 - enter the following URL

https://corp.euc-livefire.com/portal/nativeclient/ Developers?action=startsession&desktopProtocol=BLAST&launchMinimized=false

- In the bottom right corner
 - select **NEXT**

New SaaS Application		×
1 Definition 2 Configuration 3 Summary	Definition Name Enterprise Full Clone Desktops Description - Icon Categories - Configuration Authentication Type None Target URL https://corp.euc-livefire.com/portal/nativeclient/Developers?action=start-session&desktopProtocol=BLAST&launch.ktopProtocol=BLAST&la	
	CANCEL BACK SAVE & ASSIGN SAV	E

- 7. In the New Saas Application window,
 - 3. In the **Summary** section
 - Select SAVE & ASSIGN

Assign		
Selected App(s): Enterprise Full Clo	ne Windows 11 Desktops	
Users / User Groups Q. dev		
路 Developers@euc-livefire.com	loyment Type	Entitlement Type
格 Developers@euc-livefire.com	<u>Autom</u> etic ~	Include

- 8. In the **Assign** window
 - Under Users / Groups
 - Enter Devel
 - Select Developers@euc-livefire.com

Assign	
Application: 'Enterprise Full Clone Desktops' added successfully.	
Selected App(s): Enterprise Full Clone Desktops	
Users / User Groups	
Q Search for Users or Groups	
Selected Users / User Groups	Deployment Type
器 Developers@euc-livefire.com	Automatic
CANCEL	SAVE

- 9. In the **Assign** window
 - Under **Deployment** type
 - From the dropdown
 - Developers are set to
 - Automatic
 - In the bottom right corner
 - select SAVE

my-ip.iivetire.iab/ip	iorizon®Site i 💆 UAG-HZN-UTa 🦉 UAG-HZN-UTD 📉 Avi vantage Control 🦇	HZN Cloud 🕜 vcenter-0		
Unsupported VMware Identity Manager Connectors (versions 19.03.0.1 and earlier) will be discontinued soon. Action Required if your organization is using older con New updates available. Learn what's new in <u>Workspace ONE Access SaaS release notes</u> . Learn what's new in <u>Hub Services release notes</u> .				
(R) Workspace ONE Acc	Q Search for users, groups, or applications			
Monitor Accounts Reso	ources Integrations Settings			
Web Apps Virtual Apps Virtual Apps Collections Policies Global Launcher Preferences	Web Apps Add and configure web applications.	SETTINGS		
(Enterprise Full Clone Desktops	Web Application Link		
	Enterprise Instant Clone Windows 11 Desktops	Web Application Link		
	<u>Microsoft Excel</u>	Web Application Link		

- 10. In your Workspace ONE Access Console
 - Web Apps interface
 - Note your Enterprise Full Clone Desktops Web Application Link

Part 5. Testing the Horizon desktop sessions in Workspace ONE Access

Part 5 brings everything we have done on Day 2 together.

We will look at 3 primary testing scenarios



Step 1: Testing Site 1 based network traffic

- 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 not 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

VMware Horizon Client	
corp.euc-livefire.	

- 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.com	
Can't access your account?	

- 4. In the **Microsoft login** login window
 - in the **username** area
 - enter craig@corpXXX.euc-livefire.com
 - XXX is your assigned domain name
 - select Next

← craig@corp21r.euc-livefire.com Enter password	← craig@corp21r.euc-livefire.com Enter password Password	Craig@corp21r.euc-livefire.com Enter password Password Forgot my password	Microsoft	
Enter password	Password	Password Forgot my password	← craig@corp21r.euc-livetire.con	n
Decement	Passworu	Forgot my password		

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



- 6. In the **Microsoft login** login window
 - below Stay signed in?
 - select No

Open	VMware Horizon Client?	
http	s://corp.euc-livefire.com wants to open this application.	
	Always allow corp.euc-livefire.com to open links of this type in the associate	ed app
	Open VMware Horizon Client	Cancel

- 7. In the **Open VMware Horizon Client?** window
 - select Open VMware Horizon Client



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

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

- 9. On your Horizon Desktop session
 - from the **taskbar**
 - select and right-click the **START** button
 - from the **inventory**
 - select Run
| 😑 Run | × |
|-------|--|
| | Type the name of a program, folder, document, or Internet
resource, and Windows will open it for you. |
| Open: | cmd.exe ~ |
| | OK Cancel Browse |

- 10. In the **Run** window
 - next to **Open**:
 - enter cmd.exe
 - select OK

Therefore Desktop		_		×
딸 Ctrl+Alt+Del 쯷 USE	B Devices >	(c) Ful	lscreen	
Select C:\Windows\System32\cmd.exe		-		×
Microsoft Windows [Version 10.0.22621.1105] (c) Microsoft Corporation. All rights reserved.				I
C:\Windows\System32>hostname BLR-Inst-2				
C:\Windows\System32>_				

- 11. In the **CMD.exe** window
 - In the **prompt area**:
 - enter hostname
 - with your **keyboard**
 - select ENTER
 - Notice that you have a **Horizon virtual desktop** with the **BLR** naming convention representing **Bangalore**

Step 2: Testing Site 2 based network traffic



- 1. On your **ControlCenter** server
 - from the **Desktop**
 - Open the Remote Desktops \ Site 2 folder
 - Launch the W11Client-02a.rdp shortcut

Windows Security	\times
Your credentials did not work	
Your system administrator does not allow the use of saved credentials to log on to the remote computer 172.16.40.40 because its identity is not fully verified. Please enter new credentials.	
w11client-02a\jackie	
••••••	
The logon attempt failed More choices	
OK Cancel	

- 2. In the **Windows Security** page
 - ensure **Jackie** is the username
 - in the **password** area
 - enter VMware1!
 - select OK

VMware Horizon Client	
corp.euc-livefire.	

- 3. On your **W11Client-02a** 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	
jackie@corpXXX.euc-livefire.com	
Can't access your account?	

- 4. In the **Microsoft login** login window
 - in the **username** area
 - enter jackie@corpXXX.euc-livefire.com
 - XXX is your assigned domain name
 - select Next

← iackie@corp19r.euc-livefi	ire com
Enter password	inc.com
Password	
Forgot my password	
	Sign in

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



- 6. In the **Microsoft login** login window
 - below Stay signed in?
 - select No

Open VMware Horizon	lient?
https://corp.euc-livefire.c	om wants to open this application.
Always allow corp.eu	livefire.com to open links of this type in the associated app
	Open VMware Horizon Client Cancel

- 7. In the **Open VMware Horizon Client?** window
 - select Open VMware Horizon Client



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

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

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

😑 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	cmd.exe ~
	OK Cancel Browse

- 10. In the **Run** window
 - next to **Open**:
 - enter cmd.exe
 - select OK

N11Clie	nt-02a - 172.16.40.40 - Remote Desktop Connection
0	₩ ++ Enterprise Desk E Ctrl+A
Recycle Bin	
2	C:\Windows\system32\cmd.exe
Microsoft	Microsoft Windows [Version 10.0.22621.1413] (c) Microsoft Corporation. All rights reserved.
edge	C:\Users\jackie>hostname SEA-Inst-3
2 VMware	C:\Users\jackie>_
Horizon Pe	

- 11. In the **CMD.exe** window
 - In the **prompt area**:
 - enter hostname
 - with your **keyboard**
 - select ENTER
 - Notice that you have a Horizon virtual desktop with the SEA naming convention representing Seattle

Step 3. Testing Horizon integration with Workspace ONE Access

using CPA Global Entitlements



- 1. On your Control Center server
 - On your **Chrome browser**
 - Open up an **Incognito** session
 - In the address bar enter your Workspace ONE Access tenant url

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

- 2. In the **Microsoft Sign in** window
 - enter
 - craig@corpXXX.euc-livefire.com

- where **XXX** is your assigned domain
- select Next

Microsoft	
← craig@corp19	r.euc-livefire.com
Enter password	
Microsoft	
craig@corp19r.eu	c-livefire.com
Stay signed	d in?
Do this to reduce to sign in.	the number of times you are aske
Do this to reduce to sign in.	the number of times you are aske nis again

- 3. In the Microsoft Sign in window
 - Under Enter password
 - enter VMware1!
 - select Sign in
 - In the Stay signed in? window
 - select NO



4. In the web Intelligent Hub

Select Apps



5. In the web Intelligent Hub

- Under New Apps
 - select Enterprise Desktop



- 6. In the **Open VMware Horizon Client?** window
 - select Open VMware Horizon Client

	settings
	File Explorer
	Search
	Run
	Shut down or sign out >
	Desktop
	Search
_	

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

📟 Run	×
12	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	cmd.exe ~
	OK Cancel Browse

- 8. In the **Run** window
 - next to **Open:**

- enter cmd.exe
- select OK

MS Paint VLC media (created by player	
C:\Windows\system32\cmd.exe	
Notepac _M icrosoft Windows [Version 10.0.22621.1105] (created b (c) Microsoft Corporation. All rights reserve	ed.
C:\Users\craig>hostname W11-BLR-FC-1	
READMIC:\Users\craig>_	
Self-Supp	
UEM Use	

- 9. In the CMD.exe window
 - In the **prompt area**:
 - enter hostname
 - with your **keyboard**
 - select ENTER
 - Notice that you have a **Horizon virtual desktop** with the **BLR** naming convention representing **Bangalore**

1 Conclusion

To summarize. The started off the labs for Day 2 with first configuring

- 1. On both Site 1 and Site 2 using VMware AVi Local load-balancing of 4 UAG servers
- 2. Using a VMware AVi . You configured a Global Load balancing solution across site 1 and site 2
- 3. We then enabled and configured VMware Horizon Cloud Pod Architecture across site 1 and site 2
- 4. We then enabled a Federation of Workspace ONE access with Unified Access Gateway and VMware Horizon
 - From our ControlCenter server. We launched a Web based Intelligent Hub session

- From the Intelligent Hub we did a Horizon Desktop launch and our GLSB redirected us to Site 1
- Feel free to repeat the same steps on a Site 2 based desktop for Intelligent Hub