## Unified Access Gateway / VMware Horizon integration into Workspace ONE Access

## **Overview**

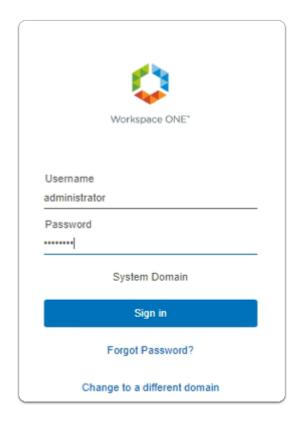
- Traditional Federation with VMware Horizon and Workspace ONE Access has been a popular approach and is used by many organizations.
- Organizations with high security requirements do not like a SAML Artifact being validated internally
- In this session we look at the option to validate the SAML Artifact 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



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

	ТА
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 ☆ ● av	v-livefirernelmarchdev.vidmpreview.com/ws1adminui/#/workspace/resour	ces/web-apps/list
S my-ip.livefire.lab/ip 🔤 H	korizon ®Site 1 🛛 🐜 UAG-HZN-01a 🐜 UAG-HZN-01b 🛛 🕅 Avi Vantage Contro	l 🔫 HZN Cloud 😰 v
	Manager Connectors (versions 19.03.0.1 and earlier) will be discontinued soon. Action Requir hat's new in <u>Workspace ONE Access SaaS release notes</u> . Learn what's new in <u>Hub Services</u>	
(R) Workspace ONE Acc	ess Q Search for users, groups, or applications	
Monitor Accounts Reso	urces	
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
	Microsoft Even	Moh Application Link

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

Settings	×
Global	Americals
Approvals	Approvals Manage access to applications that require approval from your organization before
SaaS Apps	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

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

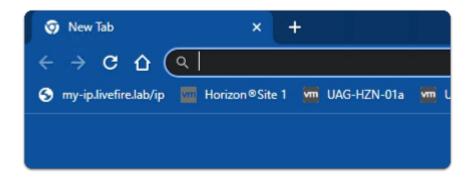
P • • • • • • • • • • • • • • • • •	Approvals SaaS Apps SaAML Metadata Application Sources SAML Aetadata Application Sources SAML Metadata Application Sources SAML Metadata Application Sources SAML Metadata Application Sources SAML Metadata Coople Apps Copy and paste the certificate below and send it to the re logications source on accept logications such as Wel Coople Apps Copy and paste the certificate below and send it to the re logications Sources SAML Metadata Application Sources SAML Metadata Cople Apps Copy and paste the certificate below and send it to the re logications sources SAML Metadata Cople Apps Copy and paste the certificate below and send it to the re logications sources SAML Metadata Detadata Q Service Provider (SP) me Service Provider (SP) me Service Provider (SP) me Copen link in new tab Open link in corognito window Signing Certificate Explices March 10, 203 ISSUE Copy link address ISSUE Copy li	Global						
SaaS Apps SAML Metadata Applications Sources Applications Sources SAML Metadata Applications Sources SAML Metadata Applications Sources SAML Metadata Bapelications Sources SAML Metadata Copy Link Additions Signing Certificate Down and past the certificate blow and set the territicate blow and set the certificate blow and set the set the set the certificate blow and set the certificate blow and set the certificate blow	Stands Apps SAML Metadata Applications Sources Applications sources Applications sources Applications sources SAML Metadata Application Sources SAML Metadata Application Sources SAML Metadata Definition of the source of the so	Approvals		Download SAML Metadata	Gener	rate CSR		
SAML Metadata Application Sources Application Applications Application Sources Application Applications Application Sources Application Applications Applications Application Applications Application Applications A	SAML Metadata Application Sources  Application Sources  Coogle Apps. Copy and paste the certificate below and send it to the re application so they can access to lights from Workspace ONE Access. Fe interacting with other relying applications utilizing SAML 2.0, you can us metadata URLs below.  SAML Metadata ©  Identity Frovider (GP) me Service Provider (GP) me Service Provider (GP) me Copy link in new vindow Copy link in new vindow Copy link in the service  C=US, O=AW-LIVEFIRE Inspect  Name to  Service Provider (GP) me Copy link address  Servi	SaaS Apps			-	-		
Application Sources applications so they can accept logins from Workspace ONE Access. Fc integrating with other relying applications utilizing SAML 2.0, you can us metadata URLs below. SAML Metadata @ Ladentix Provider (GP) me Service Provider (GP) me Service Provider (GP) me Cells Or AW-LIVERIRE Denk  To the file  Denk  Den	Application Sources applications so they can accept logins from Workspace ONE Access. Fc integrating with other relying applications utilizing SAML 2.0, you can us metadata URLs below. SAML Metadata @ Identity Provider (SP) met Service Provider (SP) met Service Provider (SP) met Service Provider (SP) met Service Structure Dentity To the former of the service Integrating with other relying applications utilizing SAML 2.0, you can us metadata URLs below. SaML Metadata @ Identity Provider (SP) met Service Structure Dentity To the former of the service Integrating with other relying applications utilizing SAML 2.0, you can us metadow Service Provider (SP) met Service Provider (SP) met Service Structure Dentity To the former of the service Integrating with other service Dentity To the former of the service Integrating with the service Integrating wit	SAML Meta	data					
Identity Provider (IdP) me Service Provider (IdP) me Service Provider (IdP) me Service Provider (IdP) me Service Provider (IdP) me Open link in new tab Open link in new tab Open link in new tab Open link in incognito window       Signing Certificate (i) Expires March 10, 2033 ISSUER Copy link address     Open link in new tab Open link in incognito window       Swe ink as Copy link address     Swe ink as Copy link address       Determine Determine Determine Service Service Service Determine Service Service Service Determine Service Service Service Determine Service Service Determine Service Service Determine Service Determine Service Determine Service Service Determine Service Service Determine Service Service Determine Service Determine Service Determine Service Service Determine Service Determine Service Determine Service Determine Service Determine Service Determine Service Determine Service Determine Service Determine Service Determine Determine Service Determine Determine Service Determine Determine Service Determine Determine Determine Service Determine Dete	Lidentity, Provider (SP) me Service Provider (SP) me Service Provider (SP) me Service Provider (SP) me Open link in new tab Open link in incognito window Save link as Copy link address Issuer Cuts, 0=AW-LIVEFIRE Determine Determ	Application	Sources	applications so they can ac integrating with other relyin	cept logins	from Works	pace ONE A	ccess. Fo
Signing Certificate () Expires March 10, 2033 ISSUE? Copy link address ISSUE? Description	Signing Certificate () Expires March 10, 2033 ISSUER Copy link address ISSUER Copy link address ISSUER Copy link address Inspect			Identity Provider (IdP) me'				
Save link as Copy link address Issuer C-US, 0=AW-ILVEPIRE Inspect Mananer Mananer Cuts, 0=AW-ILVEPIRE Inspect Mananer Cuts, 0=AW-ILVEPIRE Inspect Insp	March 10, 2033     Save link as       Issuer     Cutly, 0=AW-IUVE/IRE     Inspect       Mananar     Inspect     Inspect       Outcomer     0     Save link as       Optimize None March     Improvide     Improvide       Optimize None     Improvide     Improvide       Improvide     Improvide     I			Signing Certificate ()				
I BAUET CLUS, O=AW-LIVEFIRE Manaturer Bande	I data Control Contro							
ServeA. b → + 0 € + harK > Decelorate + Decelorate + Decelor	Serie A b = + + 0 + hBr K - Donklade			Issuer	Copy lin	nk address		
à la ruí A Opprior • None Mar Opprior • None Mar Opprior • None Mar Opprior • None Mar Opprior • None Mar Debatys e Debatys	Bank              w             w							
Opposite         Nore         Date montified         Part         Date montified         Part         Solution	Oppetier     New-Yahr     Difference     Difference <thdifference< th="">     Difference     Difference</thdifference<>				Inspect			ntity
None         Description         State           Delates come	Nome         Description         Space			Manager	Inspect			
	🥏 Network 🗸			Manager	Inspect	v	🕹 🛛 Search Downl	loads

#### 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

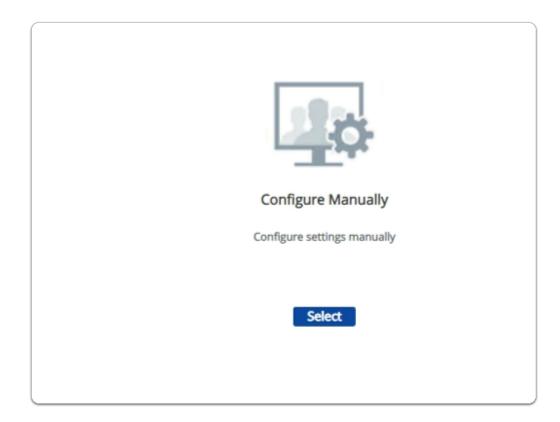


- 1. On your **Site 1 Browser** profile
  - In the Favourites bar
    - select the UAG-HZN-01a shortcut

- 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



#### 3. In the VMware Unified Access Gateway admin console

- below Configure Manually
  - click Select

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

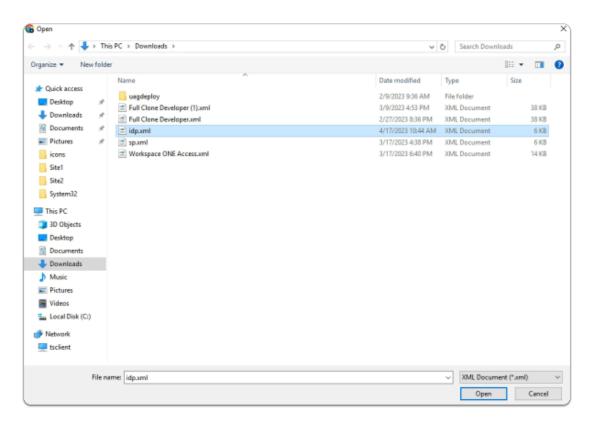
4. In the VMware Unified Access Gateway admin console

## 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 ()		
Encryption Certificate Type	None	✓ ①		
Always force SAML auth		(i)		
	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	•

- 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 <b>v</b>	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		0
Blast External URL	https://uag-hzn-01a.euc-livefire.com:443	0
Enable UDP Tunnel Server		٥
Blast Proxy Certificate	Select	0
Blast Allowed Host Header Values		0
Enable Tunnel	8	0
More ¥		
	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	<b>(</b> )
Minimum SHA Hash Size	Default 🗸	١
Connection Server URL Thumbprint		Ū
Honor Connection Server Redirect	$\otimes$	0
Connection Server IP mode	IPv4 🗸	٩
Client Encryption Mode	ALLOWED 🗸	0
Auth Methods	Select V	Ū
Health Check URI Path	Passthrough SAML	0
Re-Write Origin Header	SAML and Passthrough SAML and Unauthenticated	١
Enable PCOIP		٩

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

				0
Client Encryption Mode	ALLOWED 🗸			6
Auth Methods	SAML	~		Œ
Identity Provider *			~	Œ
	Workspace ONE Access			ta
SAMI Audiences	Add new SAML Audience		0	æ

- 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	<b>v</b> 0
	Download SAML service provide	er metadata
SAML Audiences	Add new SAML Audience	• 1
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

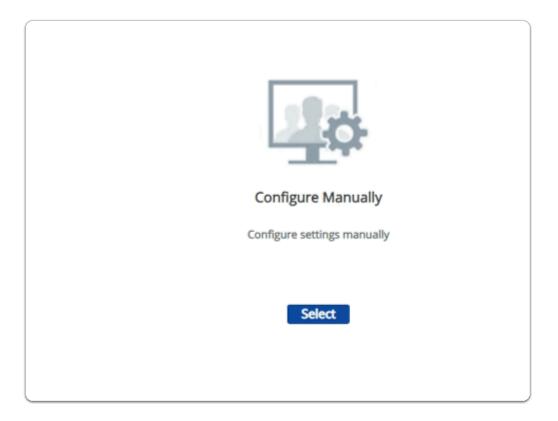
## Step 3. Enabling SAML Federation on Site 1, UAG-HZN-01b

۲	×   0	Workspace ON	E Ac	cess		×	🔊 Ne	w Tab
Horizo	on®Site 1	🚾 UAG-HZN-0	a	M	UAG-HZ	№-01Ь		Avi Vantag
			L					

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

- Colored With Ware
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



### 3. In the VMware Unified Access Gateway admin console

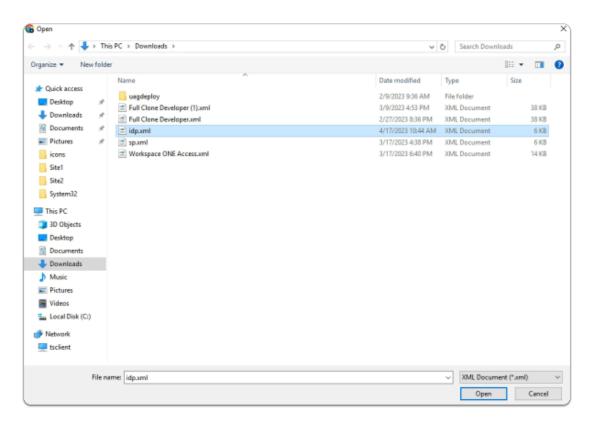
- below Configure Manually
  - click Select

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	<b>~</b> (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	•

- 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		D
Enable Tunnel		D
More >		
	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

Client Encryption Mode	ALLOWED V
Auth Methods	SAML 🗸
Identity Provider *	<b>~</b> ]0
	Workspace ONE Access
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	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

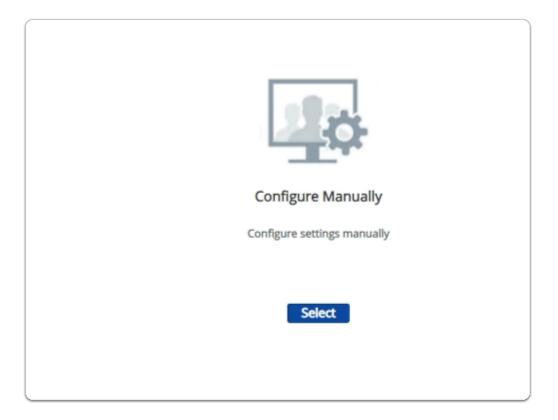
Step 4. Enabling SAML Federation on Site 2, UAG-HZN-02a



- 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



### 3. In the VMware Unified Access Gateway admin console

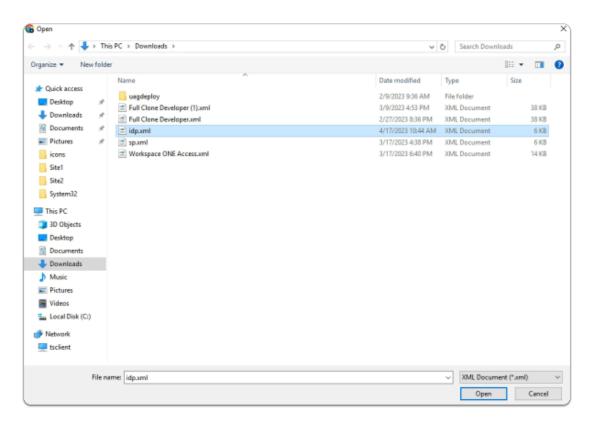
- below Configure Manually
  - click Select

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	<b>~</b> (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	•

- 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		D
Enable Tunnel		D
More >		
	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

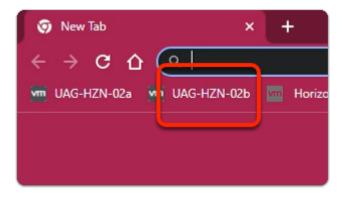
		Þ.
Client Encryption Mode	ALLOWED V	Ð
Auth Methods	SAML V	Ð
Identity Provider *	<b>~</b>	D
	Workspace ONE Access	3
SAMI Audiences	Add new SAMI Audience	D

- 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

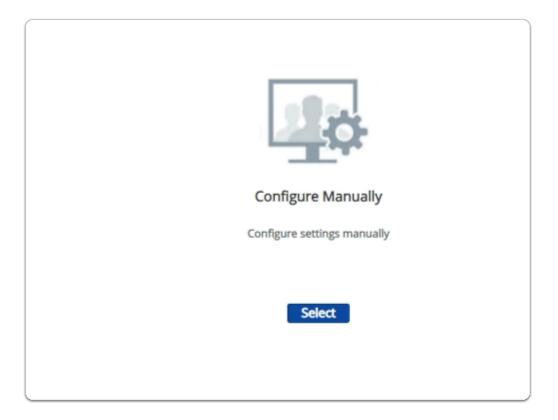
Step 5. Enabling SAML Federation on Site 2, UAG-HZN-02b



- 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



## 3. In the VMware Unified Access Gateway admin console

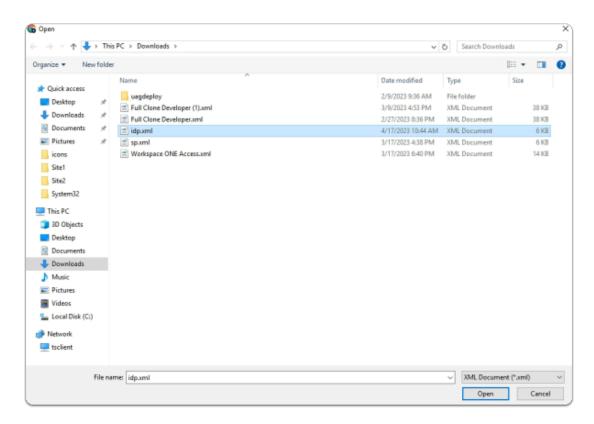
- below Configure Manually
  - click Select

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	<b>~</b> (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	•

- 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		D
Enable Tunnel		D
More >		
	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

		Þ.
Client Encryption Mode	ALLOWED V	Ð
Auth Methods	SAML V	Ð
Identity Provider *	<b>~</b>	D
	Workspace ONE Access	3
SAMI Audiences	Add new SAMI Audience	D

- 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	

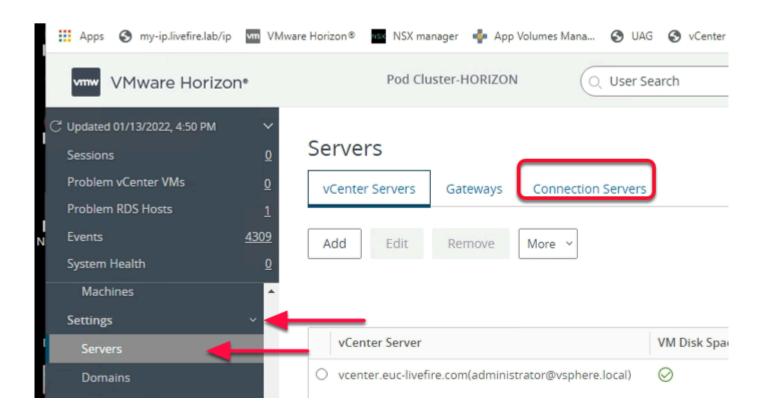
- 12. In the **Horizon Settings** window
  - scroll down to the bottom of the window
    - select Save

## 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

Intelligent Hul: X 💽 Apps   VMware Intelli X 🔛 Worl C 👔 intrizon-01a.eut-Yivefire.com/admin/#/lo vefire.la vip 🔤 Horizon® 🌀 v Senter-01a 🐳 App Vol
VMware Horizon* Version 2212
administrator
EUC-LIVEFIRE ~
Remember user name
Sign in

- 1. On your **ControlCenter** desktop
  - On your Site 1 Chrome Browser
    - Open a new tab
  - In the Favourites bar
    - Select the Horizon shortcut
  - In the User Name area
    - enter administrator
  - In the **Password a**rea
    - enter VMware1!
  - Select Sign in



- 2. 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 Disable Edit	Backup Now
Connection Server	Version
HORIZON-01A	0.0.0-21075694

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

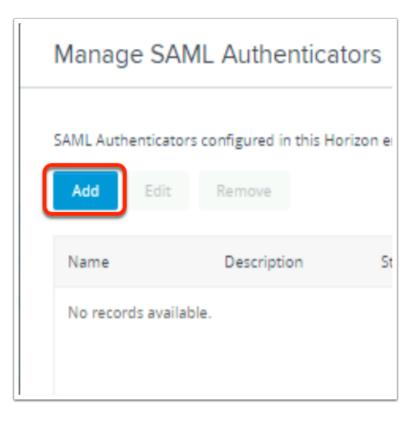
	General	Authentication
Tags		
Tags can be	e used to restrict which deskto	op pools can be accessed through this Connectio
-		

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

dit Connection Server Sett	ings
General	Authentication
elegation of authentication to VMware H	lorizon (SAML 2.0 Authenticator):
Disabled	
Disabled	
Allowed Required	
General	
Delegation of authentication to	VMware Horizon (SAI
5AML Authenticator No Enabled Authenticator config	ured
Manage SAML Authenticators	
Create at least one SAML Authen	ticator and enable it, fo

- 5. 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



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

* Type	<ul> <li>Dynamic</li> <li>Static</li> </ul>	
* Label		
Workspace ONE Access		
Description		
* Metadata URL		
https://aw-livefirewwkorn.vid	Impreview.com/SAAS/API/1.0/GET/metadata/idp.xml	
Administration URL		
* TrueSSO Trigger Mode ④		
Enabled	~	
	Server	
<ul> <li>Enabled for Connection</li> </ul>		

- 7. 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

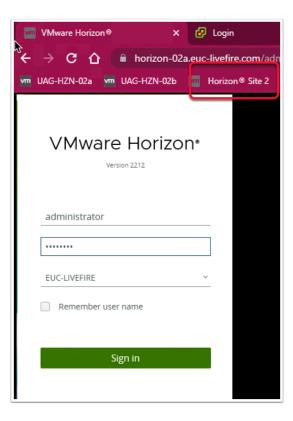
Manage SA	AML Authentica	tors			$\times$
_	tors configured in this H	orizon environment			
Add Edit	Remove	Status	Туре	Admin URL	
Workspace ON Access		Enabled	Dynamic	Autorit	*
					v
				Cancel	ОК

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

General	Authentication	Backup	
Delegation of authentication to VMware Ho	orizon (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 dor	i't support Workspace ONE mode 🔘		
Horizon Authentication			
Changes to authentication settings will take	effect on next user login.		
Smart card authentication for users:			
Optional	*		
Disconnect user sessions on smart card	l removal		

- 9. In the Connection Server Settings
  - Select OK

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

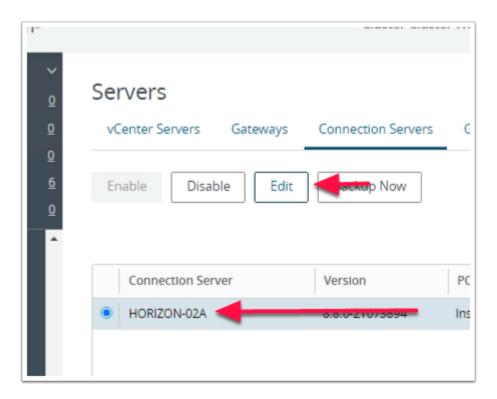


- 1. On your **ControlCenter** desktop
  - switch to your **Site 2** Chrome browser
    - Open a new tab
  - from the Favourites bar
    - select the Horizon Site 2 shortcut
  - In the User Name area
    - login as administrator
  - In the **Password a**rea
    - type VMware1!
  - Select Sign in

VMware Horizon®: Cluste	er-HORI ×	t.	lle 🕂	
← → C ● horizo	on-02a.euc-live	fire.com/admin/#	#/main/servers/o	connectionServers
🐖 UAG-HZN-02a 🛛 🐖 UAG	Б-НZN-02ь 🔤	Horizon® Site 2	🚾 HZN Cloud	🔼 Avi Vantage Co
VMware Horizon*				
C Updated 03/17/2023, 10:44 AM	~			
Sessions	Server	rs.		
Problem vCenter VMs		Servers Gatewa	ys Connection	Servers Cateway C
Problem RDS Hosts	<u>0</u>		<u> </u>	
Events	6 Enable	Disable	Edit Backup N	ow
System Health	1			
Applications	*			
Farms	Con	nection Server	Version	PCoIP Secure
Machines	• HOF	IZON-02A	8.8.0-210738	194 Installed
Global Entitlements				
Horizon Agents				
Settings V				
Servers				
Domains				
Certificate Management				

### 2. In the Horizon Admin Console

- Inventory pane
  - expand Settings,
    - select Servers
    - In the middle pane
      - select the Connection Servers tab



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

Edit Connection Server Settings					
General	Authentication				
Tags Tags can be used to restrict which deskto	p pools can be accessed through this Connectior				
Tags					
Separate tags with ; or ,					

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

Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):	
Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator):	
Disabled	~
Disabled	
Allowed Required	
-	
Manage SAML Authenticators	
Edit Connection Server Settings	
	٦
Edit Connection Server Settings General Authentication	]
	]
	]
General Authentication	]
General Authentication Asterisk (*) denotes required field	]
General Authentication Asterisk (*) denotes required field Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)	]
General Authentication Asterisk (*) denotes required field Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) Allowed	

- 5. 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

	Manag	e SAM	L Authe	nticators	
	SAML Auth	enticators	configured in	this Horizon	e
l	Add	Edit	Remove		
	Name		Descriptio	on	St
	No recor	ds availabl	e.		

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

• Туре	<ul> <li>Dynamic</li> <li>Static</li> </ul>	
Label		
Workspace ONE Access		
Description		
Metadata URL		
https://aw-livefirewwkorn.vidm	preview.com/SAAS/API/1.0/GET/metadata/idp.xml	
Administration URL		
<ul> <li>TrueSSO Trigger Mode ①</li> </ul>		
Enabled	~	
<ul> <li>Enabled for Connection Se</li> </ul>	rver	
_		

- 7. 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					
SAML Authenticat	ors configured in this H	orizon environment			
Add Edit	Remove				
Name	Description	Status	Туре	Admin URL	
Workspace ONE Access		Enabled	Dynamic		•
				Cancel	

### 8. In the Manage SAML Authenticators window

• Select **OK** to close

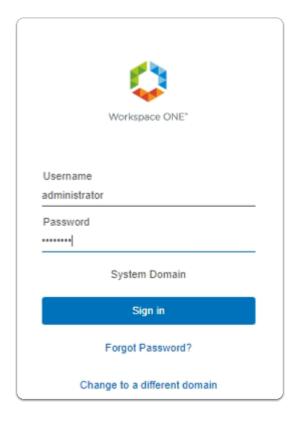
	Authentication	Backup
Delegation of authentication to VMwar	a Karina (CAMI 20 Authenticator)	
Allowed	e nonzon (some zo notinenticator).	
SAML Authenticator		
Workspace ONE Access		
Manage SAML Authenticators		
Enable Workspace ONE mode		
* Workspace ONE Server Hostname 🤇		
Block connections from clients that	don't support Workspace ONE mode 💿	
Horizon Authentication		
Changes to authentication settings will to	ake effect on next user login.	
Smart card authentication for users:		
Optional	~	
o provide		

- 9. 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



- 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 Tenant Admin Workspace ONE Access Console Manage Hub Experience Account Sign out	ТА			
Manage Hub Experience Account	Tenant Admin	Tenant		ТА
Account	kspace ONE Access Console	pace ONE	рас	Works
	age Hub Experience	ge Hub Exp	ge H	Manag
Sign out	unt	nt	nt	Accou
	out 🕞	ut	ut	Sign o

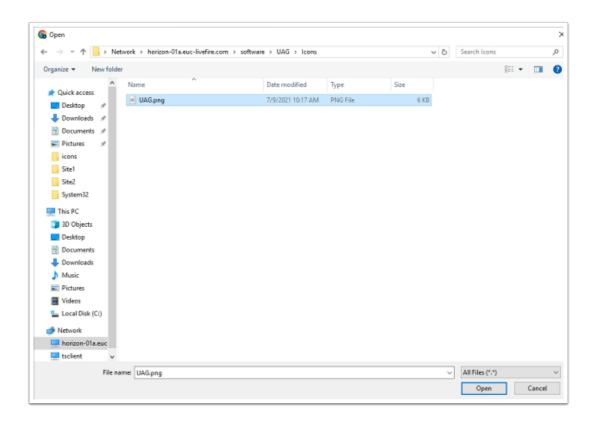
- 2. In the **Web Intelligent Hub** Console
  - To the right,
    - select TA
  - From the dropdown
    - select Workspace ONE Access Console

← → C ☆ ● av	v-livefirernelmarchdev.vidmprevi	ew.com/ws1adminu	i/#/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 🛛 😥 🗤
	Manager Connectors (versions 19.03.0.1 a hat's new in <u>Workspace ONE Access Sa</u>			
(R) Workspace ONE Acc	ess Q Search for users, grou	ips, 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	Decere Care		SETTINGS
Global Launcher Preferences	Application		Туре	•
	Hissocoft Even		1Alok	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 Description ()
CANCEL NEXT	

- 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** ...



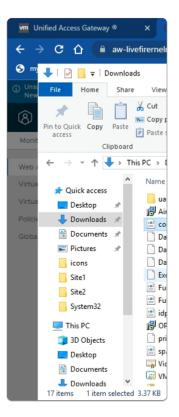
- 5. In the **File Explorer > Open** window
  - In the Quick Access pane
    - select Desktop
    - in the **Desktop** area
      - select software > UAG > Icons
        - in the Icons folder
          - select UAG.png
        - select Open

New SaaS Application		×
New SaaS Application          1 Definition         2 Configuration         3 Access Policies         4 Summary	OR BROWSE FROM CATALOG Name *  Unified Access Gateway SAML SP Description  Icon  SELECT FILE	×
	Category	
	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

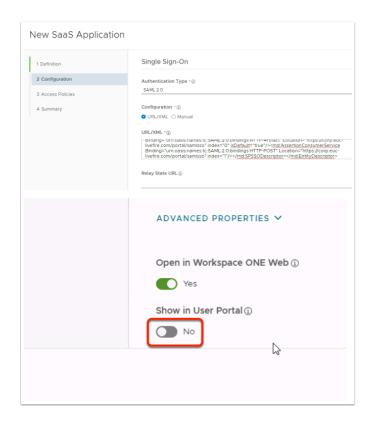
🕹   🛃 📒 🖛   Downloads	5				
File Home Share	View				
Pin to Quick Copy Paste	✓ Cut ✓ Copy path ✓ Paste shortcut	Move to •	Copy to •	Delete Rename	New folder
Clipboard			Org	anize	
← → × ↑ 🕹 > This	s PC > Download	s			
A Quick access	Name			^	
🕂 Downloads 🖈	e corp.euc-liv corp.euc-liv	efire.com		Open	
🔮 Documents 🖈	🖹 sp.xml			-lia	
📰 Pictures 🛛 🖈	🔄 VidmAirWat	chRoot		dit with Notepad	++
icons	Workspace	ONE Acce	d a	h	
Site1				Open with	
Site2				oive access to	

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

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

e Edi	
	H & & & & & & & & & & & & & & & & & & &
new 1	🗵 🔜 RexEngine log 🗵 🔚 corp.euc-livefire.com.xml 🔀
1	<pre>C?xml version="1.0" encoding="UTF-8"?&gt;</pre>

- 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 - Configuration	
	Configuration Authentication Type SAML 2.0 Configuration URL/XML URL/XML URL/XML xml version="1.0" encoding="UTF-8"? <md:entitydescriptor -="" advanced="" properties="" relay="" state="" td="" url="" xmlns:md="umroasis:names:tc:SAML:2.0metadata" ~<=""><td></td></md:entitydescriptor>	
	CANCEL BACK SAVE & ASSIGN SAV	/E

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

Assign					
Application: 'Unified Access Gateway SAML SP' added succe	ssfully.				
Selected App(s): Unified Access Gateway SAML SP					
Users / User Groups					
े. said कि SailessReuc-livefire.com	Deployment Type No assignments found.				
Assign					
Application: "Unified Access Gateway SAM	IL SP' added successfully.				
Selected App(s): Unified Acces	s Gateway SAML SP				
Q. Dev					
Q Dev					
Selected Users / User Groups		Deployment Type			
器 Sales@euc-livefire.com		Automatic			
용 Developers@euc-livefire.com		Automatic			
	$\sim$				
CANCEL SAVE					

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

- Enter Sales
  - Select Sales@euc-livefire.com
- Enter **Devel** 
  - Select Marketing@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

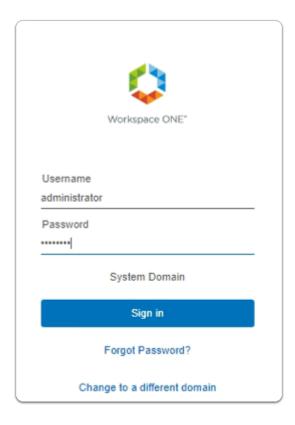
lateway ®	X (8) Workspace ONE Access X M Unified Access Gateway	◎ X   🏧 VMware Hor
🔒 aw-	livefirernelmarchdev.vidmpreview.com/ws1adminui/#/workspace/resource	es/web-apps/list
ip 🚾 Ho	rizon®Site 1 🛛 🏧 UAG-HZN-01a 🐜 UAG-HZN-01b 🔣 Avi Vantage Control	🛛 🛁 HZN Cloud 🛛 🛃 vcenter
	anager Connectors (versions 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>	
ONE Acce	ss Q Search for users, groups, or applications	
ts Resou	rces Integrations Settings	
pns	Web Apps         Add and configure web applications.         NEW       EDIT         ASSIGN       DELETE         CATEGORIES Y       MORE Y	SETTINGS
ierences	Application	туре
		Web Application Link
	Kicrosoft Outlook	Web Application Link
	Microsoft Powerpoint	Web Application Link
	Microsoft Word	Web Application Link
	+ Unified Access Gateway SAML SP	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

	ТА
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 ☆ ● av	v-livefirernelmarchdev.vidmprevi	ew.com/ws1adminu	i/#/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 🛛 😥 🗤
	Manager Connectors (versions 19.03.0.1 a hat's new in <u>Workspace ONE Access Sa</u>			
(R) Workspace ONE Acc	ess Q Search for users, grou	ips, or applications		
Monitor Accounts Reso	ources actions actiongs			
Web Apps	Web Apps			
Virtual Apps Add and configure web applications.				
Virtual Apps Collections				
Policies	NEW	Decere Care		SETTINGS
Global Launcher Preferences	Application		Туре	•
	Hissocoft Even		1Alok	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 ...

	Network > horizon-01a.euc-livefire.com >	software > icons		~	ð Search icon	1	
Organize 👻 New fo	older					111 -	
<ul> <li>A Quick access</li> </ul>	Name O	Date modified	Туре	Size			
	Enterprise Desktop.jpg	4/17/2023 5:02 PM	JPG File	8 KB			
Desktop 🖈	Excel_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB			
🕂 Downloads 🖈	Microsoft Teams_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB			
🗎 Documents 🖈	OneDrive_128x128.png	3/6/2023 2:28 PM	PNG File	4 KB			
📰 Pictures 🛛 🖈	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			
Icons	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			
Sitez	🖻 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							
> 🁌 Music							
> 📰 Pictures							
> 📑 Videos							
> 🛓 Local Disk (C:)							
<ul> <li>Metwork</li> </ul>							
> 💶 horizon-01a.euc							
> 💻 tsclient	~						
	e name: Enterprise Desktop.jpg				✓ All Files (%)		

- 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 @ Lon @ SELECT FILE. Category @	
	Selected Categories	
	CANCEL NEX	r

- 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 * ①				
3 Access Policies 4 Summary	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	Definition	
2 Configuration	Name Enterprise Full Clone Windows 11 Desktops	
3 Summary	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	
	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

Jsers / User Groups				
Q sales 쫅 Sales@euc-livefire.com				
		loyment	Туре	
器 Developers@euc-livefire.c	com	Automatic		
Selected Users / User Group	s	Deployment	Туре	
路 Developers@euc-livefire.c	com	Automatic		$\sim$
쯍 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

(R) Workspace ONE Acces	Q Search for users, groups, or applications	
Monitor Accounts Resour	ces Integrations Settings	
Web Apps Virtual Apps Virtual Apps Collections	Web Apps Add and configure web applications.	
Policies	NEW EDIT ASSIGN DELETE CATEGORIES ~	MORE - SETTINGS
Global Launcher Breferencer	Application	Туре
	Enterprise Instant Clone Windows 11 Desktops	Web Application Link
	Inified 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

← → C ☆ ● av	w-livefirernelmarchdev.vidmpreview.com/ws1adminui/#/wc
S my-ip.livefire.lab/ip 🔤 H	łorizon®Site 1 🧰 UAG-HZN-01a 媡 UAG-HZN-01b 📉 Av
	Manager Connectors (versions 19.03.0.1 and earlier) will be discontinued s /hat's new in <u>Workspace ONE Access SaaS release notes</u> . Learn what's ne
(8) Workspace ONE Acc	ess Q Search for users, groups, or applications
Monitor Accounts Reso	ources Integrations Settings
Web Apps Virtual Apps Virtual Apps Collections	Web Apps Add and configure web applications.
Policies Global Launcher Preferences	
	Enterprise Instant Clone Windows 11 Desktops
	Microsoft Excel

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

New SaaS Application	
1 Definition	Definition
<ul><li>2 Configuration</li><li>3 Access Policies</li><li>4 Summary</li></ul>	Search C OR BROWSE FROM CATALOG Name * Enterprise Full Clone Desktops Description
	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 ....

	> Netw	ork > horizon-01a.euc-livefire.com > se	oftware > icons	~ Ū	Search icons	مر
Organize 🔻 🛛 N	ew folder					H 🔹 🔟 🧯
📌 Quick access	^	Name	Date modified	Туре	Size	
Desktop	*	e desktop-developer.jpg	4/17/2023 6:22 PM	JPG File	14 KB	
	1.1	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	
Site2		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		Vammer_128x128.png	3/6/2023 2:28 PM	PNG File	3 KB	
Documents						
- Uownloads	~					
	File nam	e: desktop-developer.jpg		~	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	Single Sign-On
2 Configuration	Authentication Type 🕻
3 Summary	Web Application Link
	Target URL •
	https://corp.euc-livefire.com/portal/nativeclient
	Open in Workspace ONE Web ()
	No No
CANCEL	BACK

- 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.k   Access Policies   Open in Workspace ONE Web   No	
	CANCEL BACK SAVE & ASSIGN SAV	E

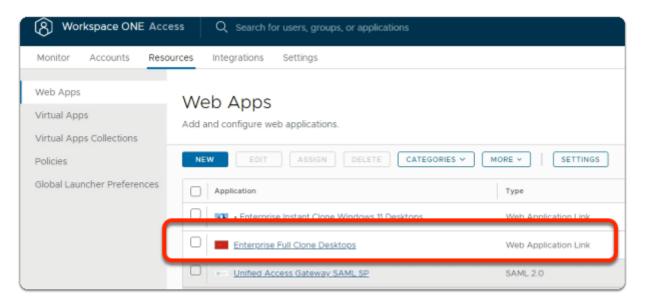
- 7. In the New Saas Application window,
  - 3. In the **Summary** section
    - Select SAVE & ASSIGN

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
쯍 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



- 10. In your Workspace ONE Access Console
  - Web Apps interface

Note your Enterprise Full Clone Desktops Web Application Link