Session Protection with VMware Horizon

Introduction

This chapter has 3 primary objectives

- Securing a Horizon Blast sessions using HTML Access
- Securing the HTML Blast functionality when Origin Blocking refuses connections via the Unified Access Gateway
- Securing Workspace ONE Access and VMware Horizon Sessions with JWT TOKEN

Overview

When launching an entitlement using the HTML client with Horizon Blast either through Workspace ONE Access or as a Direct connection with the broker **by default** one might observe the following:

You might notice that the Browser constantly gets stuck even though our Connection server had trusted CA signed certificates from a public source.

The problem also occurs wheen using HTML blast via Workspace ONE Access, even though Workspace ONE Access is using CA-signed certificates.

The result is an unsatisfactory User-Experience, a user would have to accept what appears to be an Invalid certificate, leaving them with concerns about the resource they are consuming



Background

In earlier versions of Horizon, if we wanted to solve this problem we had to perform two primary operations.

1st an edit had to made on the Broker to the LDS database using ADSIEDIT. The reason for this is as follows and it entails understanding how the transport works. The 2nd step entailed replacing the Agents self-signed cert with a CA signed cert. In a non-persistant environment the most practical way to do this was to use a wild-card certificate.

This exercise is divided into two parts.

- Part 1 will cover understanding this issue with the Transport
- Part 2 we will use the latest approach to configuring Horizon Blast with Workspace ONE Access and you will notice how much better it works.

Introduction: Validating the default configuration on the Blast transport



- 1. On the **ControlCenter** server.
 - Launch an **Incognito session** on your **Chrome browser** session
 - In the address bar enter your custom URL for Workspace ONE Access
 - Below **Select your domain**, ensure **euc-livefire.com** is the selection.
 - Select Next

- Under the **username** area
 - Enter the user name Mark
- In the **password** area
 - Enter VMware1! as the password
- Select Sign in

Favorites App	People For Yo	ou Support	
	Q Search Apps		
		New Apps All Apps Categories ~	
New Apps			
0	\bigcirc	🥩 🖳	
Calculator	Internet Explorer	Paint W10INST	

- 2. In the Workspace ONE Access Console
 - Select Apps
 - Under Categories, select Virtual
 - Select and launch, Calculator



- 3. In the Password Request window
 - In the **Password** area Enter VMware1! as the password
 - Select Sign In
 - In the address bar, notice you have an IP address, also you will notice it says the certificate is not Valid.

CN=	-Common Properties ? X
Attribute Editor	
Attributes:	
Attribute	Value ^
pae-NumNUCountHig	<not set=""></not>
pae-NumSessionsHigh	<not set=""></not>
pae-NumSessionsHig	<not set=""></not>
pae-NumSviSessions	<not set=""></not>
pae-NumUnmanaged	<not set=""></not>
pae-OVDIKeyCipher	<not set=""></not>
pae-PCoIPBandwidth	<not set=""></not>
pae-PortalPath	<not set=""></not>
pae-PreferDNS	<not set=""></not>
pae-PreForcedLogoff	Your desktop is scheduled for an important u
pae-PreLoginMessage	<not set=""></not>
pae-ProtectionLevel	2
pae-ProtoRedirKp1	\01\00\00\00\24\01\00\00\08\00\00\00\
pae-ProtoRedirKp2	\01\00\00\00\24\01\00\00\08\00\00\0
<	>
Edit	Filter
OK	Cancel Apply Help

- 4. So there are two problems here, our Agent is using a self-signed cert, but even if we had a CA signed cert it would not be trusted as by default Horizon prefers to use IP address rather than domain name.
 - In the past this was a two part process, where we had to edit the LDS database using ADSIEDIT (above screenshot of the config) and we would have configure Horizon to Prefer using a FQDN rather than an IP Address. The reason for this was, even if we had a valid certificate it would not be recognized as the address in the certificate would not map to the address in the browser.
 - 2. On the virtual desktop we would replace the self-signed cert with a CA signed Wild CARD cert .
 - And that was a problem as no one liked that, it was not secure, it gave the impression of being secure, but it was an open door waiting to be exploited.
 - 3. Thankfully this issue has been rectified and we will look at Part 2 on how secure our Horizon environment properly when we integrate with Access using the Blast Protocol
 - 4. Log off from Workspace ONE Access and Close any open Browsers
 - 5. Reference
 - https://kb.vmware.com/s/article/2088354
 - https://docs.vmware.com/en/VMware-Horizon-7/7.5/horizon-installation/ GUID-8E7FBB9D-F2DB-4787-B11B-7506126DEB7F.html
 - 6. We will also in the next lab teach an implement TRUESSO for a single sign-on experience

Part 1. Securing a Horizon Blast sessions using HTML Access.

What the Product development team have done is give us the ability to Tunnel HTML Blast traffic through the Broker.

- This has a two advantages. The Broker can use its own CA signed certificate when launching the session with the client and we do not have to configure the Broker to prefer to use DNS as the client is connecting directly with the Broker.
- Best practice now is to configure the HTML BLAST SECURE GATEWAY on the Broker for internal Horizon Clients. In the past we would not configure Blast to Tunnel through the Horizon Connection Server if we wanted to use the Unified Access Gateway.
- With this new configuration we are able to use this Connection Server for both Internal and External use.
 - We will now implement this configuration on the Horizon Connection server and then test this configuration out in this Part

🔅 VMware - Workspace ONE 🛛 🙁 VMware Horiz	on X
← → C 🛈 â aw-livelite-markusmi444 vidm	preview.com/authc
S my-ip.livefir 2.lab/ip 🚾 VMware Horizon® 😰 Cente	r 🔇 UAG-HZN 🤇
Version 2012 administrator	
•••••	
EUC-LIVEFIRE ~	
Remember user name	
Sign in	

- 1. On your **ControlCenter** server,
 - Launch the Chrome Browser,
 - Select the VMware Horizon shortcut in the Favourites Bar
 - Login as Administrator
 - For password us VMware1!
 - Select Sign in

← → C ☆ 🔒 horizon.euc-livefire	.com/admin/#/main/servers/virtualCenterServers
Apps 🕤 my-ip.livefire.lab/ip 🔽 VMware	Horizon® 🔇 UAG-HZN 🔇 UAG-UEM 🌆 NSX manager 🌵 App
VMware Horizon*	Pod Cluster-HORIZON
C Updated 11/22/2021, 11:53 AM	
Sessions <u>0</u>	Servers
Problem vCenter VMs 0	vCenter Servers Gateways Connection Servers
Problem RDS Hosts 0	
Events <u>4</u>	Add Edit Remove More ~
System Health 0	
Machines	
Settings ~	
Servers	vCenter Server VM
Domains	 vcenter.euc-livefire.com(administrator@vsphere.local)
Product Licensing and Usage	
Global Settings	

2. In the Horizon Console

- Expand Settings
- Under Settings select Servers

← → C 🏠 🔒 horizon.euc	-livefire.com/admin/#/main	/servers/virtualCe	nterServers
🚻 Apps 🔇 my-ip.livefire.lab/ip 🔽	VMware Horizon® 🔇 UAG-	HZN 🔇 UAG-UE	M 💀 NSX manager 🛭 🖕 A
VMware Horizon*	_	Pod C	luster-HORIZON
C Updated 11/22/2021, 11:53 AM	~		
Sessions	Servers		
Problem vCenter VMs	vCenter Servers	Gateways	Connection Servers
Problem RDS Hosts	<u>D</u>		
Events	4 Add Edit	Remove	More ~
System Health	0		
Machines	•		
Settings ×			1
Servers	vCenter Serve	r	VI
Domains	 vcenter.euc-liv 	efire.com(administ	trator@vsphere.local) 🤤
Product Licensing and Usage			
Global Settings			

- 3. Under Servers,
 - Select the Connection Servers tab

~ <u>0</u>	Servers		
<u>0</u>	vCenter Servers Gateways	Connection Servers	
<u>0</u>		-	-
4	Enable Disable Edit	Backup Now	
<u>0</u>			
^			
	Connection Server	Version	PCoIP Secur
	HORIZON	8.3.0-18294467	Installed

- 4. On the **Connection Servers** tab,
 - Select the radio button next to Horizon
 - Select Edit

Use Blast Secure Gateway for all Blast connections to machine ③	
O Use Blast Secure Gateway for only HTML Access connections to machine ③	
💿 Do not use Blast Secure Gateway 🕥	
* Blast External URL:	
https://cs1-pd1.euc-livefire.com:8443	(
Example: https://myserver.com:8443	

- 5. Notice that the existing configuration
 - This issue occurs when the setting **Do not use Blast Secure Gateway** is selected
 - This configuration was a default with Horizon 7,
 - In Horizon 8, the default configuration when Horizon is fresh-installed is **Use Blast** Secure Gateway for all Blast Connections to machine

🔾 Use Blast Secure Gateway for all Blast connections to machine 🛈	
Use Blast Secure Gateway for only HTML Access connections to machine 🔘	
🔵 Do not use Blast Secure Gateway 🛈	
Blast External URL:	
https://cs1-pd1.euc-livefire.com:8443	0
xample: https://myserver.com:8443	

- 6. In the Edit Connection Server Settings window
 - Select the radio button next to Use Blast Secure Gateway for only HTML Access Connections to machine
 - Close the Edit Connection Server Settings by selecting OK

Part 2. Validating our Horizon HTML Blast Configuration and configuring Single Sign-On for password based Authentication.

VMware - Workspace ONE × Interview - Workspace ONE × New Tab
← → C 🏠 🗎 aw-livefire-markusrn444.vidmpreview.com/authcontrol/auth/request
🕥 my-ipJivefireJab/ip 🔤 VMware Horizon® 🔗 vCenter 📀 UAG-HZN 🥥 UAG-UEM 🔤 NS
^
Workenaca ONE*
THUR REPORTED
Select Your Domain
euc-livefire.com 🗸
Remember this setting
Next
vmware
*
Workspace ONE"
username
password
euc-livefire.com
Sinn in
- Ogn m
Forgot password?
Change to a different domain
vmmware:

- 1. On the **ControlCenter** server.
 - From your Chrome browser Open an Incognito browser se new tab

- In the address bar enter your custom Workspace ONE Access URL
- In the Select your domain, ensure euc-livefire.com is the selection. Select Next
- Enter the username Mark and the password VMware1! Select Sign in

♦ Apps VMware Intelligent Hub ♦ Apps VMware Intelligent Hub	× 🔤 Vi	/ware Horizon	®: Cluster	-HORIX	New Tab	(apps	+
S my-ip.livefire.lab/ip VMwa	are Horizon⊗	🕑 vCenter	🕤 UAG	-HZN 🔇	UAG-UEM	NSX NSX	manag
		Favorites	A	pps	People	For \	/ou
					Q s	earch App	os
	New A	pps				ħ	
		0					
	📮 Hori	zon		Horiz	on	•••	Ç (
Password Reques We need your password to sin Password	st gn in to Calcu	lator.				×	
				Cancel	Si	gn In	

- 2. In the Workspace ONE Access Console
 - Select Apps
 - Under Categories, select Virtual
 - Select and launch, Calculator
 - In the Password Request window, enter VMware1!
 - Select Sign In

Cal	cul Edit H			×	
				0	
МС	MR	MS	M+	M-	
←	CE	с	±	4	
7	8	9	/	%	
4	5	6	*	1/x	
1	2	3	-	_	
0 . + =					

- 3. On your **Chrome Browser**, a new tab should be launch
 - Close your Incognito Chrome Browser session
 - As mentioned earlier, we will address the single Sign-On issue for password based Authentication

(8) Workspace ONE [™] A	Access	
Dashboard 👻 Users & Grou	ups Catalog 👻 Identity & Act	cess Management Roles
Directories Identity Providers	Password Recovery Assistant	Authentication Methods Policies
	Directories (2)	
	Directory Name	Туре
Tenant Admin • AW-LIVEFIR Q Search users, groups or appli Reset Virtual App Usage dentity & Access Management User Attributes Terms of Us	E-MARKUSRN444 cations Manage Setup es re Preferences Auto Dis	
Worker	Iden	

- 4. On your **ControlCenter** server
 - Switch to your Chrome browser and select your custom Workspace ONE Access URL session tab
 - If necessary log in again with your custom System Admin credentials
 - In the Workspace ONE Access admin Console
 - Select the Identity & Access Management tab
 - To the right of the Identity & Access Management console,
 - Select Setup
 - Under Setup,
 - Select Preferences

allowed	
Password Caching	✓ Enable
	If enabled, a user's password is cached when first logging in to Workspace ONE Access using password-based authentication. If using an alternate method of authentication (such as a third-party IdP, RADIUS, certificate-based, etc.), a user's password is cached when they are challenged with password-based authentication during the first launch of a virtual app.
	Enable this to provide single sign-on for users running Horizon, Horizon Cloud, and Citrix virtual apps from the Workspace ONE Catalog. For Horizon and Horizon Cloud, for better user experience and security set up True SSO instead of caching passwords.
	Save

5. In the **Preferences** area

- Scroll right down, to the bottom of the Preferences area
- Next to Password Caching, select the check-box next to Enable
- Select Save
- The Password Caching check box in Preferences will only provide single sign-on for Password based authentication.
 - The Caching of Password for Horizon is a feature that was disabled In December 2019 and this check box was re-introduced for those customers that wanted to accept the security risks of password based caching.
 - This solution does not work for 3rd-Party auth methods

Conclusion

In this session we have seen how we secure internal HTML Blast traffic

If we were external our traffic would tunnel through the Blast Secure Gateway on the UAG. However, when external we would not then tunnel again through the Horizon Connection server. The Unified Access Gateway would come into play. In the next part we will look at how we configure the Unified Access Gateway for secure the HTML Blast Transport for external Access.

Part 3: Securing the HTML Blast functionality when Origin Blocking refuses connections via the Unified Access Gateway



- 1. On your **ControlCenter** Server
 - Open your Remote Desktop folder, launch W10EXT01a.RDP
 - Login as Administrator@euc-livefire.com
 - With the password VMware1!
 - On the W10Ext01a desktop, open your Chrome browser, in the address bar, type uaghzn.euc-livefire.com or select the UAG-Client shortcut
 - Select the VMware Horizon HTML Access shortcut



- 2. Notice you have a Failed to connect to the Connection Server issue
 - Select **OK** to close the **Error** message
 - This is not a UAG issue and nothing is broken. This due to a new secure feature that has been enabled in Horizon 7 called *Origin checking* which is enabled by default and is a new standard defined in RFC 6454
 - <u>https://docs.vmware.com/en/VMware-Horizon-7/7.1/com.vmware.horizon-view.security.doc/GUID-AA5D0A57-51A7-4FC1-A79B-AFD15A72499A.html</u>
 - Close all Windows, minimise your W10Ext01a.RDP session

File Home Shar	e View					
Pin to Quick Copy Paste	✓ Cut Image: Copy path Image: Paste shortcut	Move Copy to •	Delete Rename	New folder	access • Properties	Sopen ▼ Compared and the set of
Clipboard	I	Org	anize	New	Op	en
$\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow R$	emote Desktops					
🔹 Quick access	Name	^	Da	te modified	Туре	Size
Deskton	norizon.RDF	F	2/2	28/2021 11:29 PM	Remote Desktop	3 KB
	nd RDSH01a.RD	P	4/1	3/2018 7:13 AM	Remote Desktop	3 KB
Uownloads 🖈	Note: Solid Solid Solid States Solid States Solid States S		4/3	3/2018 11:20 AM	Remote Desktop	3 KB
🚆 Documents 🛛 🖈	NueSSO.RDI	0	1/1	2/2020 7:36 AM	Remote Desktop	3 KB
📰 Pictures 🛛 🖈	N10Client01	.RDP	3/1	9/2021 6:33 AM	Remote Desktop	3 KB
DesktopInfo	Notexa and with the second sec	RDP	6/5	5/2020 10:29 AM	Remote Desktop	3 KB
Remote Desktops	ntoparent01 💀	a.RDP	3/2	2/2021 10:47 AM	Remote Desktop	3 KB
System32	NS1-Conne 💀	ctor.RDP	4/3	3/2018 11:27 AM	Remote Desktop	3 KB

- 3. On your **ControlCenter** server Desktop
 - In the Remote Desktops folder
 - Launch Horizon.RDP
 - Login as username Administrator@euc-livefire.com
 - Password is VMware1!



- 4. On your **Horizon Connection server**, go to your **logs** folder to validate this is the issue.
 - On the Task bar launch File Explorer
 - Go to c\:ProgramData\VMware\VDM\logs
 - Open the most current debug log and
 - Search for a keyword "unexpected origin"
 - This validates the issue we are having. To solve this proceed with the following step

	· · ·			-
horizo	n.euc-livefire.com/adm	nin/#/main/serv	ers/connection	Servers
.lab/ip	vm VMware Horizon®	S UAG-HZN	UAG-UEM	NSX NSX r
			a dat	
rizor	28		Pod Clu	ster-HOR
	~	(Mware		
	Unified A	ccess G	Gateway	,
	admin	Login		

- 5. On your **ControlCenter** server Desktop
 - Open your Chrome Browser, open a new tab and select the UAG_HZN shortcut
 - In the UAG Admin login, type
 - In the **Username** area type : admin
 - In the **Password** area type: VMware1!
 - Select Login



- 6. On the **Unified Access Gateway Appliance** admin console
 - Under Configure Manually
 - Click on, Select

ay Appliance v21.06	
Edge Service Settings	x ∂ x
Advance	d Settings

- 7. On the Unified Access Gateway Appliance v20.12 Admin console
 - Under **General** Settings
 - Next to Edge Service Settings, move the toggle next to Edge Service Settings from Left to Right

y Appliance v21.06		
Edge Service Settings		
	 Horizon Settings 	٢
	O Reverse Proxy Settings	٥

- 8. To the right of Horizon Settings,
 - Select the gear wheel

Enable Honzon	(i)
Connection Server URL https://horizon.euc-livefire	e.com
Connection Server URL Thumbprint	0
Connection Server IP mode IPv4 🗸	٦
Re-Write Origin Header NO	٦
Enable PCOIP YES	0
Disable PCOIP Legacy Certificate ONO	0
Convection Server Dimose Pol	

- 9. In the Horizon Settings, next to
 - **Re-write Origin Header**, move the **toggle** from **No** on the left to **Yes** on the right.
 - Select **Save** at the bottom of the window.
 - Logout from the UAG Admin console



- 10. Switch back to your W10Ext01a server,
 - Launch your Chrome Browser
 - Enter UAG-HZN.euc-livefire.com in the Address Bar
 - Select VMware Horizon HTML Access

VMware Horizon	ŝ
Mark	
Login	
Cancel	

11. In the Login window type in the following:

- Username: Mark
- Password: VMware1!
- Select Login



- 12. In the Horizon HTML entitlements,
 - Launch Paint

🗟 w10EXT01a - w10EXT01a.euc-liv	efire.com - Remote Desktop Connection	,
0	VMware Horizon	× +
asysta Bin	← → O	euc-livefire.com/portal/webclie
0	Horizon	
n life Souseje Souseje	Q. Search	A Snushes
	Running	
like se	💞 Paint 🛛	
llain.	Windows Calcul 😒	
e	Available	
Bilge	W10INST	* 11
	Calculator	*
konistan)	Internet Explorer	*
	Paint	*
- Horizon		@ Mark
-		Mark
Q Search		Settings
Running	4	- Fullscreen
		About
Paint		Log out
Log Out		
Are you sure you Server?	u want to log out of th	e Horizon Connection
		Cancel OK

- 13. Notice your entitlement launches without any further prompts
 - Select Log out
 - On the **Log Out** window select **OK**
 - Close your Browser
 - Minimize your W10Ext01a.RDP Session

Conclusion

This concludes this part

We have Configured HTML Blast for external access using the Unified Access Gateway and the HTML Blast Secure Gateway

Part 4: Configuring secure sessions when Integrating Workspace ONE Access with VMware Horizon and the Unified Access Gateway.

Introduction

When configuring the Transport integration with Workspace ONE Access a customer might have deployed an On-premises, LAN deployed Workspace ONE Access server or DMZ deployed Workspace ONE Access server or the customer might have subscribed to a SAAS deployment of Workspace ONE Access.

VMware Horizon will always be on a Microsoft Active Directory Domain joined LAN connected network. The Unified Access Gateway will be deployed in the DMZ to facilitate all external access for Horizon Based resources and will not be domain joined.

Internal Users should / could connect and tunnel directly through the Connection Server with HTML Blast or have a direct session to the Horizon Agent on the LAN.

External Users should always connect and tunnel via the Unified Access Gateway and should never have a Direct session on the Transport from an external network to a domain joined desktop.

In this scenario all we are doing is securing North / South traffic. To ensure East / West traffic within networks are secure we would use the Micro-segmentation feature of VMware NSX

The objective of this session is demonstrate the Networking configuration requirements when Workspace ONE Access integrates with VMware Horizon and the VMware Unified Access Gateway.

Workspace ONE*
Select Your Domain System Domain
Remember this setting
Next
vm ware [.]

- 1. On your **ControlCenter** server,
 - On your **Google Chrome** browser,
 - Open a new tab
 - Enter your custom Workspace ONE Access URL
 - Ensure that in the Select your Domain window,
 - You have System Domain selected in the dropdown
 - Select Next

	Workspace ONE"
	Username administrator
1	Password
	System Domain
	Sign in
	Forgot Password?
	Change to a different domain
	vmware [.]
	ТА
,	TA Tenant Admin
	Administration Console
	Account
	Sign out

- 2. In the Workspace ONE Sign-In page
 - Under Username type administrator,
 - Under Password type enter your custom password
 - Select Sign In
 - In the right-hand corner, select **TA** > **Administration Console**



- 3. In the Workspace ONE Access console
 - Select Catalog > Virtual Apps Collection

🗰 Apps 🛛 Morizon 🔅 WS1-Connect	or 🕤 Horizon c	loud conn 🚾 Hor
(8) Workspace ONE ^{**} Acce	SS	
Dashboard 👻 Users & Groups	Catalog 👻	Identity & Access
Virtual Apps		ONS
Name		Source Type
Horizon		Horizon
1 - 1 of 1 item(s)		

- 4. In the Virtual Apps Collections window,Double-Click Horizon

Dasht	board - Users & Groups Catalog - Identity & Access Management Roles
	< BACK
	Horizon
	Overview Network Ranges
	EDIT SYNC DELETE
	Connector
	Connector Name
	ws1-connector.euc-livefire.com

- 5. In the **Horizon** window,
 - Select the Network Ranges tab

8 Workspace ONE™ Access								
Das	Dashboard - Users & Groups Catalog - Identity & Acc							
	< ВАСК							
	Horizon							
	Overview Network Ranges							
	ADD							
	Name							
	ALL RA	NGES			Þ			

6. In Network Ranges window

Select ALL RANGES

Applications will be accessible by all users it no groups are assigned.						
Pod and Federation						
Pod	Client Access FQDN (j)	Port	Wrap Artifact in JWT	Audience in JWT ①		
Horizon.euc-livefire.com	uag-hzn.euc-livefire.com	443	Yes	https://aw-livefire-markusrr		
				ADD		

- 7. In the Assign Pods to Network Ranges window
 - Scroll down to Pod and Federation
 - Under Client Access FQDN
 - Enter uag-hzn.euc-livefire.com
 - Under Wrap Artifact in JWT
 - Switch the **Toggle** to **Yes**
 - Under Audience in JWT

- Type your custom **Workspace ONE Access URL**. e.g. https://aw-livefiremarkusrn444.vidmpreview.com
- Select ADD
- Select **SAVE**

Part 5: Configuring Unified Access Gateway and VMware Horizon Sessions with JWT TOKEN



- 1. On the **ControlCenter** server
 - On your **Chrome** browser, Open a **new Tab**, select the **UAG-HZN** admin shortcut session
 - In the **Username** area, login as admin
 - In the **password** area, enter VMware1!,
 - Select Login



- 2. In the UAG ADMIN Console
 - Under Configure Manually, select the Blue Select button

Advanced Settings	
System Configuration	0
Network Settings	0
High Availability Settings (Not Configured)	٥
TLS Server Certificate Settings	٥
SAMI, Settings	٥
Endpoint Compliance Check Provider Settings	٥
JWT Settings	٥
Account Settings	0

3. In the UAG ADMIN Console

- Under Advanced Settings
 - Select the Gear to the right of JWT Settings

JWT Settings	
	Add
	No JWT setting has been added.
	Close

- 4. In the UAG ADMIN Console
 - In the **JWT Settings** window, select Add

JWT Settings		
Name *	Workspace ONE Access	0
Issuer	Workspace ONE Access]0
Dynamic Public key URL	https://aw-livefire-markusrn444.vidmpreview.com/	0
Public key URL thumbprints		0
Trusted Certificates	No trusted certificate is added.	()
Public key refresh interval	86400	0
Static Public Keys	No public key is added for this setting.	1
	Save Cancel	
JWT Settings		
		Add
Name		
Workspace ONE Access	\$ ×	
	Close	

- 5. In the **JWT Settings** window, enter the following, next to
 - Name: Workspace ONE Access
 - Dynamic Public key URL: https://YOUR CUSTOM ACCESS FQDN/SAAS/API/1.0/REST/ auth/token?attribute=publicKey&format=pem
 - Public key refresh interval: 86400
 - Select Save
 - Select Close

Unified Access Gateway Ap	bliance v20.09
General Settings	
	Edge Service Settings SHOW C Active Sessions: 0
	Authentication Settings
Edge Service Settings	HIDE 🔵 🗲 Active Sessions: 0
•	> Horizon Settings
0	Reverse Proxy Settings
0	Tunnel Settings

6. In the UAG Admin Console

- In the General Settings area
 - Next to Edge Service Settings, select and move the toggle to the right
 - To the right of Horizon Settings, select the GEAR

Enable Blast	0	
Blast External URL https://uag-hzn.euc-livefire.com:443	0	
Enable UDP Tunnel Server	(i)	
Blast Proxy Certificate Select	0	
Enable Tunnei 🖉 🕫 🌒	0	
Tunnel External URL https://uag-hzn.euc-livefire.com:443	Ū	
Tunnel Proxy Certificate Select	0	
More ¥		
Gateway Location * External V		(i)
JWT Settings Select		~ (i)
JWT Audiences	J	i
Trusted Certificates No trusted certificate is addec	d.	o (j
onse Security Headers Name Value		o (i)
Strict-Transport-Security: max-age=315360	·· / •	
Disable HTML Access		
Less *		
Save Cancel		

7. In the **Horizon Settings** window

- At the bottom of the page, select More
- To the right of JWT Settings select the dropdown and select Workspace ONE Access
- Scroll to the bottom of the window and select Save

Part 6: Validating Workspace ONE Access Transport Configurations with VMware Horizon

INTRODUCTION

All Horizon sessions configured to communicate with Workspace ONE Access have been configured to be secure. We will now test the session

			- (_ ;	×
			☆	θ (:
vCenter	New tab			Ctrl+T	
	New windo	New window			
	New incog	nito windo	w Ctrl+	Shift+N	
	History				Þ
Search users,	Download	s		Ctrl+J	
	Bookmarks	5			Þ
	Zoom	- 100)% +	53	
	Print			Ctrl+P	
	Cast				
	Find			Ctrl+F	
	More tools	;			Þ
	Edit	Cut	Сору	Paste	
ist Attempt Sync	Settings				
ay 31, 2020, 9	Help				Þ
	Exit				

1. On your **ControlCenter** server

- On your **Chrome Browser** in the top right hand corner,
- Select the 3 DOTS
- Select New incognito window



2. On your Chrome Browser

• Enter your custom Workspace ONE Access URL

Workspace ONE*
Select Your Domain
euc-livefire.com 🗸
Remember this setting
Next
vm ware [.]

- 3. In the **Select Your Domain** window.
 - Validate that the default domain **euc-livefire.com** is selected
 - Select Next

	Workspace ONE*	
username Mark		
password		
	euc-livefire.com	₽.
	Sign in	
	Forgot password?	
Cha	nge to a different domain	
	vm ware ⁻	

- 4. In the **Log in** window
 - Under username enter Mark,
 - Under password enter VMware1!,
 - Select Sign in



- 5. Next to Favorites,
 - Select Apps

aw-livefire-markusrn444.vidr	mpreview.com/catalog-portal/ui#	//apps		
🔤 VMware Horizon® 💋 vCent	iter 🥱 UAG-HZN 🥱 UAG-UEM	NSX manager		
	Pavorites	Apps People Fo	r You Support	
		Q Search A	pps	
			New Apps	All Apps Categories
	New Apps			
	e			
	Calculator	Internet Explorer	Paint	W10INST
	- Horizon	📮 Horizon 🛛 🚥	- Horizon ····	- Horizon ····
			\	

6. In the **Apps** area

Select Internet Explorer

	-livefire.com/portal/webclient/#/d	lesktop			
🔇 my-ip.livefire.Jab/ip 🔤 VMware Hori	izon® 🕜 vCenter 🔇 UAG-HZN	S UAG-UEM 💿 NSX manager			
Horizon					
Q Search			- March 1984		
Running		MSN Outlook, Office, Sky ×	N tocia=tenp		
Internet Explorer 💿 🔀		a	et new wallpapers	every day fror ar desktop with dai	n Microsoft ly backgrounds
Available					
W10INST +		powered b	1 y Microsoft News		
Calculator		Outli	yok.com 😽 Wa	vfair 💼	Microsoft Store
Internet Explorer			e d		Viter
ng Paint					Easy-to-follow RECIPES DONE in 35 minutes
		CORONAN	IRUS NEWS 🕴 📿 AUSTI	N / 62*F 🖋 👘 Try	MSN in Microsoft Edge NE
 C	-livefire.com/portal/webclient/#/d izon® ② vCenter ③ UMG-HZN ③ Mark ③ Settings ④ Fullscreen ③ About	iesttop was (<u>></u>) (ARX A SARAH MA ARXING A SARAH A SARAH
🧑 Internet Explorer 💿 🔀	E Log out				
Log Out Are you sure you want to log out of Server?	of the Horizon Connection				
	Cancel OK				
_	► MD				
MD Mark Debio					
Account					
Sign out	Ð				

- 7. Notice the Address in the Browser is our **Horizon Connection** server.
 - In this example, We have launched a Virtual Application from **Workspace ONE ACCESS** and our secure session is Tunneling through the Unified Access

- Select Log out
- On the **Log Off** window select **OK**
- In the top right hand corner, select your account Icon. In this example its MD, right-click, select Sign Out
- Close the browser



Conclusion

In Summary we looked at Best practice with the regard to configuring the Blast protocol for using with HTML Client. It is important to note that Native Client by default offers the same and possibly better user experience and we do not necessarily, see the errors we see with the HTML client. However best practices and configurations we saw in this exercise apply to both the Native and the HTML client

Acknowledgements and References

As author of this material, I wish to thank Graeme Gordon from TechMarketing for their continued support and guidance on getting this lab right

Some useful resource links to continue your development

https://techzone.vmware.com/resource/understand-and-troubleshoot-horizonconnections#HTML_Client_Access

https://techzone.vmware.com/resource/zero-trust-secure-access-traditional-applicationsvmware

https://docs.vmware.com/en/VMware-Horizon-7/7.1/com.vmware.horizon-view.security.doc/ GUID-AA5D0A57-51A7-4FC1-A79B-AFD15A72499A.html https://kb.vmware.com/s/article/2088354

https://theidentityguy.ca/2021/02/25/workspace-one-access-best-practices-in-policymanagement/

About the Author: Reinhart Nel

https://www.livefire.solutions/meet-the-team/reinhartnel/

For any questions related to this session, email Reinhart at RACE-Livefire-EUC@vmware.com