

APM Proxy with Workspace One





Version History

Date	Version	Author	Description	Compatible Versions
Mar 2018	1.0	Matt Mabis	Initial Document	VMware Identity Manager 3.2.x and Above (1) Workspace One Cloud (2)

NOTES:

(1) The Version 1.0 Document only supports up to VMware Identity Manager 3.2.x and above, as joint features were added for the integration in 3.2.x that do not exist in previous versions.

(2) Workspace One Cloud is compatible with this guide, as the VMware Workspace One Cloud edition has continual upgrading, any possible issues with the integration or after deployment issues might be considered a regression in our joint integration code.



Contents

Version History
Overview
Workspace One (WS1) - Cloud4
VMware Identity Manager (VIDM) - On-Premise5
Caveats
Prerequisites7
Prerequisite (VIDM LTM Configuration)8
Prerequisite (Horizon APM Configuration)9
VIDM/WS1 Configurations 10
Enable JWT Functionality in VIDM/WS110
F5 BIG-IP Configurations
Disable Strict Updates on APM Configuration12
Create OAUTH Resources
Modify Horizon Access Policy
Verifying JWT Token Functioning
Troubleshooting

Overview

Workspace One (WS1) - Cloud



Workspace One combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Workspace One reduces the complexity of IT administration.

Workspace One Cloud instead of being deployed on-premise within a datacenter is now deployed in the Cloud. Organizations can centralize assets, devices, and applications and manage users and data securely while gaining access to upgrades instantly and not having to take maintenance outages during upgrades.

VMware and F5 have developed an integration to add additional layers of security and provide gateway access with Workspace One Cloud. This document provides step-by-step instructions for setting up Workspace One Cloud as an Identity Provider (IDP) in front of F5 APM as a Service Provider (SP) utilizing APM as a Gateway for VMware Horizon. These configurations will provide the Single Pane of Glass that Workspace One provides with the DMZ Security and Scalability that F5 PCoIP/Blast Proxy provides with VMware Horizon.



VMware Identity Manager (VIDM) - On-Premise

VMware Identity Manager combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Identity Manager reduces the complexity of IT administration.

Identity Manager is delivered as a virtual appliance (VA) that is easy to deploy onsite and integrate with existing enterprise services or can be deployed on a Windows platform. Organizations can centralize assets, devices, and applications and manage users and data securely behind the firewall. Users can share and collaborate with external partners and customers securely when policy allows.

VMware and F5 have developed an integration to add additional layers of security and provide gateway access with VMware Identity Manager. This document provides step-by-step instructions for setting up VMware Identity Manager as an Identity Provider (IDP) in front of F5 APM as a Service Provider (SP) utilizing APM as a Gateway for VMware Horizon. These configurations will provide the Single Pane of Glass that VMware Identity Manager provides with the Security and Scalability that F5 PCoIP/Blast Proxy provides with VMware Horizon.

Caveats

These are the current caveats/restrictions in this version of the documentation

- 1. Workspace One Mobile (MobileSSO) is **NOT verified** in this version of the documentation/code.
- 2. Citrix Integration with Workspace One is **NOT verified** in this version of the documentation/code.
- 3. All Changes currently are done with Manual Configurations, iAPP update to come in future releases.

Prerequisites

The following are prerequisites for this solution and must be complete before proceeding with the configuration. Step-bystep instructions for prerequisites are outside the scope of this document, see the BIG-IP documentation on support.f5.com for specific instructions.

- 1. F5 requires running this configuration using BIG-IP APM/LTM version 13.1 with an Engineering Hotfix (F5 Support Service Request must be made with mention of RFE 683741-1, 684370-1 and 635509-1.)
 - This functionality will be integrated into version 14.0+, when released.
- Create/import an SSL Certificate that contains the load-balanced FQDN that will be used for Identity Manager Portal. (VIDM Deployments Only)
- 3. Upload the following to the BIG-IP system: (VIDM Deployments Only)
 - The SSL Certificate must be uploaded to the BIG-IP.
 - The Private Key used for the load-balanced FQDN certificate.
 - The Primary CA or Root CA for the SSL Certificate you uploaded to the BIG-IP.
 NOTE: The Primary or Root CA for the FQDN Certificate will also be uploaded to the BIG- IP and are required to be loaded on each Identity Manager appliance.
- 4. Workspace One/VMware Identity Manager deployed and configured.
 - For VMware Identity Manager a (3-Node) behind a LTM FQDN VIP on the BIG-IP and VIDM is setup/configured to the domain and horizon environment.
 - For Workspace One Cloud the environment has been setup/configured with connectors to the domain and horizon environment.
- 5. VMware Horizon is completely setup and configured behind a APM VIP on the BIG-IP (in this document we are assuming that the VIP was deployed via the iAPP)

NOTE: VMware recommends the use of Certificates which support Subject Alternate Names (SANs) defining each of the node FQDNs (public or internal) within the load balanced VIP FQDN. Wildcard certificates may be used, but due to wildcard certificate formats, SAN support is typically not available with wildcards from public CAs - and public CAs may complain about supplying an internal FQDN as a SAN value even if they do support SAN values. Additionally, some VMware Identity Manager features may not be usable with wildcard certificates when SAN support is not defined.

Prerequisite (VIDM LTM Configuration)

NOTE: If using Workspace One Cloud this prerequisite is not needed

This section is to confirm prerequisites were completed prior to moving forward. If this configuration is not completed please use the F5 Integration guide "Load Balancing VMware Identity Manager" prior to moving forward. <u>https://f5.com/Portals/1/PDF/Partners/f5-big-ip-vmware-workspaceone-integration-guide.pdf</u>

Local	Traffic »	Virtual Servers : Virtu	ual Server List						
⇔ ⇒	Virtual S	erver List Virtual Add	ress List Statis	stics 🔻					
WS1-0	OnPremise		Search R	leset Search					Create
	 Status 	▲ Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
	•	WS1-OnPremise			10.105.169.107	443 (HTTPS)	Standard	Edit	Common

Local Traffic ** Virtual Server List ** WS1-OnPremise Protocal Componentia Componentia ************************************			Configuration: Basic V	
Properties Resource Statistics Product Product (Starter) Product Product (Starter) Product Product (Starter) General Properties MITP Product Product (Starter) MITP Product (Starter) MITP Product (Starter) Name WS1-OnPremise FTP Product (Starter) None Partition / Path Common RTSP Product (Starter) RTSP Product (Starter) Type Standard Standard Standard Source Address 0.0.0.0/0 Standard Starter) Service Port 443 HTTPS Starter) Starter) Nothy Status to Virtual Address Available (Enabled). The virtual server is available Starter Product Starter Product Starter Product Syncoke Status Off None None None Starter Product None Syncoke Status Off Starter Product None	Local Traffic » Virtual Servers	: Virtual Server List » WS1-OnPremise	Protocol	TCP
Image: Control Properties Produce Profile (Server) Image: Control Profile (Server) Image: Control Profile (Server) Name WS1-OnPremise MTTP Profile VS1-MTP Profile VS1-MTP Profile Pattion / Path Common Common Common Description Standard Vs1-Standard KrSP Profile Sected Vs1-Standard Type Standard Vs1-Standard Vs1-Standard Vs1-Standard Vs1-Standard Source Address 0.0.0.00 Standard Vs1-Standard Vs1-Standard Vs1-Standard Service Port 443 HTTPS \cdots Standard Standard Vs1-Standard	🚓 🚽 Properties 🛛 Reso	urces Statistics 🗵	Protocol Profile (Client)	tcp-wan-optimized •
General Portion MTTP Provide Mem MitTP Provide Mome Name WS1-OnPrenise Common RTSP Provide Some = - Description Common RTSP Provide Some = - Type Standard			Protocol Profile (Server)	tcp-lan-optimized •
General Properties HTTP Prov Connect Profile None Name WS1-OnPremise FTP Profile None Partition / Path Common FTP Profile None Description Image: Common Connect Con			HTTP Profile	WS1-HTTP V
Name WS1-OnPremise FTP Profile Set # Partition / Path Common RTSP Profile Set # Description Image: Common image: Commo	General Properties		HTTP Proxy Connect Profile	None
Pathon / Path Common RTSP Profile Some Description Image: Common register on compatible on common register on common register on common register on common register on com	Name	WS1-OnPremise	FTP Profile	None *
Description Sector Available Type Standard SSL Profile (Clerr) SSL Profile (Sarve)	Partition / Path	Common	RTSP Profile	None *
Type Standard Standard Type Standard Image: Standard Source Address 0.0.0.00 Image: Standard Destination Address/Mask 10.105.169.107 Image: Standard Service Port 443 Image: Standard Virtual Status to Virtual Address Image: Standard Status to Virtual Address Image: Standard Status to Virtual Address Link None Image: Status to Virtual Address Image: Status to Virtual Address Syncockie Status Off Image: Status to Virtual St	Description			Selected Available
Source Address 0.0.0.0/0 Destination Address/Mask 10.105.169.107 Service Port 443 HTPS ▼ Address/Mask Image: Common Service S	Туре	Standard	SSL Profile (Client)	WS1-ClientSSL Clientssl Clientssl Clientssl
Destination Address/Mask 0.105.169.107 Available Service Port 443 HTPS • SSL Profile (Server) SSL Profile (Server) SSL Profile (Server) SSR Profile (Server) </td <td>Source Address</td> <td>0.0.0/0</td> <td></td> <td>cientssi-secure crypto-server-default-clientssi</td>	Source Address	0.0.0/0		cientssi-secure crypto-server-default-clientssi
Service Port 443 HTTPS SSL Porties (server) Description (server) <thdescription (server)<="" th=""></thdescription>	Destination Address/Mask	10.105.169.107		Common Compatible Available
Notify Status to Virtual Address Image: Constraint of the Virtual Address I	Service Port	443 HTTPS V	SSL Profile (Server)	severss-insecure-companies xx approximation serverss crypto-client-default-serverss >> poip-default-serverss
Link None Index Index Availability Availabile (Enabled) - The virtual server is available Clent LDAP Profile None Syncode Status Off Syncode Status None None	Notify Status to Virtual Address	 Image: A state of the state of	011700 0-484	serverssi ·
Availability Availabile (Enabled) - The virtual server is available Cent Color Politie None * Syncookie Status Off Syncookie Status None *	Link	None	Oferst I DAD Deater	None +
Syncookie Status Off Status Off Status Statu	Availability	Available (Enabled) - The virtual server is available	Clent LDAP Profile	None T
State Enabled	Syncookie Status	Off	SHITE Braffa	None *
	State	Enabled T	SMIT FIGHE	
Vakaro Luneirance AlvZvs and Luneirance AlvZ	State	Lindbrou ·	VLAN and runnel framic	Automatical Automatica Automatical Automatical Automatica Automatica Automatica Automatica

Content Rewrite

Rewrite Profile +	None
HTML Profile	None 🔻
Access Policy	
Access Profile	None
Connectivity Profile +	None 🔻
Per-Request Policy	None V
VDI Profile	None
Application Tunnels (Java & Per- App VPN)	Enabled
OAM Support	Enabled
ADFS Proxy	Enabled
PingAccess Profile	None V
Acceleration	n
Rate Class	None V
OneConnect Profile	None 🔻
NTLM Conn Pool	None v
HTTP Compression Profile	None
Web Acceleration Profile	None
HTTP/2 Profile	None
Undata Delata	1

Local	Traffic » Virtual S	ervers : Virtu	al Server List	» W	/S1-OnPre
	Properties	Resources	Statis		
Load B	alancing				
Defaul	t Pool	WS	1-Pool		•
Defaul	t Persistence Profile	WS	1-Persistence	٠	
Fallba	ck Persistence Profi	le Non	e	۲	
Update	9				
iRules					
Name					
No rec	ords to display.				
Policies	5				
Name					
No rec	ords to display.				

Update Delete

Prerequisite (Horizon APM Configuration)

This section is to confirm prerequisites were completed prior to moving forward. If this configuration is not completed please use the F5 Deployment guide "Deploying F5 with VMware View and Horizon View" prior to moving forward. https://www.f5.com/pdf/deployment-guides/vmware-horizon-view-dg.pdf

iAnns Application Services · Applications						
Application Contract reprint						
			EE iAppo apr	d Deseures		
			F5 IApps and	d Resource	5	
*Demo-HZN-CPA Search	Reset Search			Create		
Name	Template	Template Validity \$	Partition / Path			
Demo-HZN-CPA	f5.vmware_view.v1.5.3	С	ommon/Demo-HZ	N-CPA.app		
Delete					-	
Local Traffic » Virtual Servers : Virtual Server List						
🔅 🗸 Virtual Server List Virtual Address List Stati	stics 🔫					
Demo-HZN-CPA Search	Reset Search					Create
🖌 💌 Status 🔺 Name 🗘	Description	Destination	Service Port	Type	Resources	Partition / Path
Demo-HZN-CPA_apm_redirect	Demo-HZN-CF	PA 209.194.169.137	7 80 (HTTP)	Standard	Edit	Common/Demo-HZN-CPA.app
Demo-HZN-CPA_pcoip_udp	Demo-HZN-CF	PA 209.194.169.137	4172	Standard	Edit	Common/Demo-HZN-CPA.app
Demo-HZN-CPA_proxy_https	Demo-HZN-CF	PA 209.194.169.137	443 (HTTPS)	Standard	Edit	Common/Demo-HZN-CPA.app
Enable Disable Delete						

VIDM/WS1 Configurations

Enable JWT Functionality in VIDM/WS1

After making sure that either the Workspace One Cloud environment is deployed and setup with connectors and VMware Horizon and/or the VIDM environment is setup behind the load balancer and configured for VMware Horizon we move along to configuring the VIDM/WS1 environment to work with the F5 APM

Log onto the VIDM/WS1 Portal Configuration Page

1. In a browser, login as an Admin to the VIDM/WS1 FQDN (in this example, https://myws1-onprem.bd.f5.com)



2. Select the down arrow next to Catalog and Select "Virtual Apps"



3. Click on the "Virtual App Configuration" button.

4.



Q Search users, groups or applications Dashboard 👻 Users & Groups Catalog 👻 Identity & Access Management Roles Add Virtual Apps -NAME SOURCE TYPE SYNC STATUS ACTIONS Horizon View On-Prei Horizon View On-Premises Dec 14, 2017 5:01:48 PM: Completed Alerts Sync Horizon View On-Premises Dec 14, 2017 8:05:16 PM: Completed view-lab-apps Sync Alerts

INTEGRATION GUIDE

6.

APM Proxy with VMware Workspace One

5. Select the down arrow next to Catalog and Select "Virtual Apps"

\leftrightarrow \rightarrow C Secure https://myws1-onprem.bd.f5.com/SAAS/ac	
🔢 Apps ★ Bookmarks 📙 Home Bookmarks 📙 F5 Bookmarks 📙 P	
🛟 Workspace ONE™	
Dashboard → Users & Groups Catalog → Identity & J	
Application Catalog	
Virtual Apps Collection	
Settings	
Click on the "Virtual App Settings" button.	
Dashboard - Users & Groups Catalog - Identity & Access Management Roles	Q Search users, groups or applications
Q Any Application Type - Any Category -	Virtual App Configuration Virtual App Settings Categories -

7. Select the Network Settings Tab and Select the "All Ranges" link

Virtual App Settings			
Network Settings	Network Settings		
ThinApp Application Alerts	NAME	DESCRIPTION	IP ADDRESS RANGE
	ALL RANGES	A network for all ranges	0.0.0.0 - 255.255.255.255

8. In the All Ranges Network Setting

VIEW POD	CLIENT ACCESS URL HOST	URL PORT	WRAP AR	AUDIENCE IN JWT
sitea-broker- 01.bd.f5.com	sitea-broker-01.bd.f5.com	443		+
siteb-broker- 01.bd.f5.com	siteb-broker-01.bd.f5.com	443		+
VIEW CPA FEDERATION	CLIENT ACCESS URL HOST	URL PORT	WRAP AR	AUDIENCE IN JWT
3D-CPA-Federation	demo-site-two.bd.f5.com	443		f5cpa
Horizon Cloud Pod	10.192.152.32	443		f5cpa

- a. Enable the checkbox for "Wrap Artifact in JWT" on the Horizon Environment that was configured in previous steps.
- b. Click the + under the "Audience in JWT" next to the checkbox and provide a unique name (our example is f5cpa)
- c. Click the Save Button.

Once Completed the configuration for VIDM/WS1 is now setup, you can now move to configuring the F5 APM.

F5 BIG-IP Configurations

Disable Strict Updates on APM Configuration

1. Login to your F5 BIG-IP Instance



2. Under the iAPPs Section → Application Services, select the iAPP Deployed for the Horizon APM Configuration

Hostname: ws1-bip-01.bd.f5.com Date: IP Address: 192.168.14.22 Time:	Jan 31, 2018 User: admin 11:04 AM (PST) Role: Administrator		Partition: Com	imon 🔻	Log out
ONLINE (ACTIVE) Standalone					
Main Help About	iApps » Application Services : Application	ns			
Statistics	Application Service List				
iApps				F5 iApps and	Resources
Application Services	*Demo-HZN-CPA	Search Reset Search			Create
Tomplatos	✓ ▲ Name	Template	emplate Validity	Partition / Path	
	Demo-HZN-CPA	f5.vmware_view.v1.5.3	(Common/Demo-HZN	-CPA.app
AWS	Delete				

3. In the Properties Tab (Advanced) of your Deployed IAPP for Horizon APM

iApps	» Application Ser	vices : Application	s » Demo-HZN-CPA
₩ -	Properties	Reconfigure	Components
	_		
Applica	ation Service: Adva	anced V	
Applic	ation Service	Demo-HZN	-CPA
Partiti	on / Path	Common/D	emo-HZN-CPA.app
Descri	iption		
Templ	ate	f5.vmware_	view.v1.5.3
Strict	Updates	(recomm	ended)
Updat	e Delete		

- a. Change the pull-down menu from Basic to Advanced.
- b. Uncheck the Strict Updates checkbox.
- c. Click the Update button.

Create OAUTH Resources

1. In the Access Menus go to Federation → OAuth Client / Resource Server → Provider

Access	
Overview	•
Profiles / Policies	Þ.
Authentication	×
Single Sign-On	×
Federation	SAML Service Provider >
Connectivity / VPN	> SAML Identity Provider >
Secure Web Gateway	SAML Resources
Access Control Lists	JSON Web Token
Webtops	OAuth Authorization Server
Device Management	OAuth Client / Resource OAuth Server
	Provider 📀
Network	Request (*)

2. Click the Create Button

Acc	Access » Federation : OAuth Client / Resource Server : Provider								
	, SAML Service Provider 👻	SAML Identity Provider	SAML Resources	JSON Web Token 👻		- OAuth Client / Resource Server	 PingAccess 	-	
Provi									
		Q						Create	
	Name	⇔ Type	Use Auto-discovered	JWT		OAuth Server	Partition		
	AzureAD false Common								
	F5 I	F5 false Common							
	Facebook	Facebook	cebook false Common						

3. In the OAuth Client / Resource Server Provider Menus

Access » Federation : OAuth	Client / Resource Server : Provider » New
🚓 👻 Properties	
General Properties	
Name	MyWS1
Description	
Туре	Custom
Ignore Expired Certificate Validation	
Trusted Certificate Authorities	ca-bundle.crt 🔻
Allow Self-Signed JWK Config Certificate	•
Use Auto-discovered JWT	
OpenID URI	https://myws1-onprem.bd.f5.com/SAAS/auth/.well-known/openid-configure Discover
Authentication URI	
Token URI	
Token Validation Scope URI	
UserInfo Request URI	
Cancel Save	

- a. Enter a Unique Name
- b. Change type to Custom
- c. In the **OpenID URI** enter the following (**replacing <MyVIDMFQDN>** with your unique instance) <u>https://<**MyVIDMFQDN>**/SAAS/auth/.well-known/openid-configuration</u>
- d. Click the Discover Button

APM Proxy with VMware Workspace One

4. During the Discovery Process you will see an "In progress" section this is expected behavior.

Access » Federation : OAuth Client / Resource Server : Provider » New						
🔅 🚽 Properties						
In progress						

5. If the Discovery is successful you will see that some of the previously empty areas are now populated with data and additional boxes have appeared. Scroll to the bottom and click the Save button to complete the

OpenID URI	https://myws1-onprem.bd.f5.com/SAAS/auth/.well-known/openid-configura					
	Last discovery time: 2018-01-31 11:40:04					
Authentication URI	https://myws1-onprem.bd.f5.com/SAAS/auth/oauth2/authorize					
Token URI	https://myws1-onprem.bd.f5.com/SAAS/auth/oauthtoken					
Token Validation Scope URI						
UserInfo Request URI	https://myws1-onprem.bd.	f5.com/SAAS/jersey/r	manager/api/userinfo			
Issuer	https://myws1-onprem.bd.	f5.com/SAAS/auth				
Signing Algorithm	Allowed		Blocked			
	RS256	*				
Key (JWK)	Allowed		Blocked			
	RSA:1516721347:undefi	ned:undefin 🗦				

6. In the Access Menus go to Federation \rightarrow JSON Web Token \rightarrow Token Configuration



7. There should be an auto-created Token Configuration due to the discovery in the previous section, select the auto-created Token that contains your VIDM EODN in the Issuer

Access » Federation : JSON Web Token : Token Configuration										
₿ -	SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	JSON Web Token 👻	OAuth Authorization Server 👻	OAuth Clien	t / Resource Serve	 PingAccess 	-	
Toker	Token Configurations (JWT)									
L									Create	
	≑ Name	Auto Discovered	⇒ Issuer				Provider	+ Partition / Path	Create	
	≑ Name auto_jwt_MyWS1	Auto Discovered true	≑ Issuer https://my	ws1-onprem.bd.f5.com/	SAAS/auth		Provider MyWS1	Partition / Path Common	Create	

INTEGRATION GUIDE

APM Proxy with VMware Workspace One

8. In the Token Configuration

	0	
Access » Federation : JSC	N Web Token : Token Configuration » auto_jwt_MyWS1	
🚓 👻 Properties		
General Properties		
Auto Discovered	The token is auto generated by OpenId discovery.	
Name	auto_jwt_MyWS1	
Issuer	https://myws1-onprem.bd.f5.com/SAAS/auth	
Use Provider List Settings		
Access Token Expires In	0	minutes
	f5cpa	
Audience	Add	

- a. Type the name of your Audience (Created previously in the VIDM Configurations section) and Click the Add button.
- b. Once the audience is added scroll to the bottom and click the save button.
- 9. In the Access Menus go to Federation \rightarrow JSON Web Token \rightarrow Provider List

Access				
Overview	×			
Profiles / Policies	+			
Authentication	+	SAML Service Provider >		
Single Sign-On		SAML Identity Provider >>		
Federation	Þ	SAML Resources 💮		
Connectivity / VPN		JSON Web Token >	Key Configuration	(\cdot)
Secure Web Gateway	-	OAuth Authorization Server	Token Configuration	\odot
Access Control Lists		OAuth Client / Resource	Provider List	\odot
Webtops	÷	Server Pingéccoss		
		T IIIgAccess		

10. Click the Create Button

Access » Federation : JSON Web Token : Provider List										
÷.	SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	JSON Web Token 👻	OAuth Authorization Server 👻	OAuth Client / Resource Server 👻	PingAccess	-		
Provid	Provider Lists									
	Q Create									
•	V Name O Partition / Path									

11. In the JSON Web Token Provider List

Access » Federation : JSON Web Token : Provider List » New						
🚓 👻 Properties						
General Properties						
Name	WS1-Provider					
Access Token Expires In		minutes				
	/Common/MyWS1					
Provider	/Common/MyWS1 - Add					
Cancel Save						

- a. Enter a Unique Name
- b. In the Provider pull down menus Select the OAUTH Client / Resource Server Provider previously created and click the Add button.
- c. Click the Save button.

Once these Steps have been completed you can move forward to Modifying the Horizon APM Access Policy.

Modify Horizon Access Policy

1. In the Access Menus go to Profiles / Polices → Access Profiles (Per Session Policies)

Access			
Overview	F		
Profiles / Policies	•	Access Profiles	
Authentication	÷	Policies)	•
Single Sign-On	Þ	Per-Request	(+)
Federation	F	Policies	
Connectivity / VPN	\rightarrow	Policy Sync	
Secure Web Gateway		Customization	•
Access Control Lists	F		
Webtops	÷		

2. Click the Edit in Per-Session Policy under the Horizon APM Access Policy created as part of Prerequisites

Access » Profiles / Policies : Access Profiles (Per-Session Policies)									
🚓 👻 Access Profiles	Per-Request Policies		Customization 👻						
*Demo-HZN-CPA	*Demo-HZN-CPA Search Reset Search Import								
Status 🔺 Acce	ss Profile Name 💠	Application + Pro	ofile Type Per-Session P	olicy Export	Сору	Logs	Virtual Servers	Partition / Path	
Demo-ł	IZN-CPA De	mo-HZN-CPA AII	Edit	Export	Copy	default-log-setting	Demo-HZN-CPA_proxy_https	Common/Demo-HZN-CPA.app	
Delete Apply									

3. In Visual Policy Editor this is a typical Horizon iAPP Deployment, we will remove ALL of the policies except Client Type, View Client Resource Assign, and Browser Assign.



4. To delete the other objects, click on the X within the box (usually top right corner) a popup dialog for deletion like the one below will appear. Keep the default selection of "Connect Previous node to fallback branch" and click the delete button.



5. Once all of the objects except Client Type, View Client Resource Assign and Browser Resource Assign are deleted the Visual Policy Editor should look like the below picture.

Start fallback +	×	VMware View + →→ <u>View Client Resource Assign</u> fallback + →→ <u>Alle</u>	ow
	Client Type	Full or Mobile Browser +	ow
		fallback +->>	ny

6. Click on the + between VMware View Client Type and View Client Resource Assign to create an object between the two.



7. Select OAUTH Scope from the Authentication tab and click the Add Item button. (Picture was cropped to take up less space)

Begin typing to search						
Logo	Logon Authentication Assignment Endpoint S					
	AD Auth	Active Director				
0	AD Query	Active Director mapping				
۲	OAuth Scope	OAuth Scope				
\odot	OCSP Auth	Online Certifica				
0	On-Demand Cert Auth	Dynamically in				
\bigcirc	OTP Generate	Generate One				
0	OTP Verify	Verify One Tim				
Canc	el Add Item	~ 1 · · · ·				

In the OAUTH Scope 8.

Properties Branch Rules	
Name: View Client OAuth Scope	
OAuth	
Token Validation Mode	Internal T
JWT Provider List	/Common/WS1-Provider 🔻
Cancel Save	Help

- ncel Save
 - Provide a Unique Name (Since on the View Client Path we put View Client OAuth Scope) a.
 - Change the Token Validation Mode to Internal. b.
 - Select the JWT Provider previously created in F5 Configurations. C.
 - d. Click the Save Button.
- 9. The Updated VPE should look like the below picture. Click on the + between View Client OAuth Scope and View Client Resource Assign in the Successful line to create an object between the two.

Start fallback +	VMware View + ->	Allow
Client Tyr	fallback + ->	Deny
<u>Circle 19</u>	Full or Mobile Browser +	Allow
	fallback + ->>	Deny

10. Select Variable Assign from the Assignment tab and click the Add Item button.

(Picture was cropped to take up less space)

Begin typing to search	
Logon Authentication Assign	ment Endpoint Security
O ACL Assign	Assign existing Acces
Variable Assign	Assign custom variab
O VMware View Policy	Specify a policy that
Cancel Add Item	

11. In the Variable Assign

Properties* Branch Rules	
Name: View Client Variable Assign	
Variable Assign	
Add new entry	Insert Berore: 1
Assignment	
1 empty <u>change</u>	
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help

- a. Enter a Unique Name (Since on the View Client Path we put View Client Variable Assign)
- b. Click the "Add new entry" button
- c. Click the "change" link on line 1

Custom Variable V Unsecure V		=	Custom Expression V	
ession.logon.last.username	I		session.oauth.scope.last.jwt.upn	*
	F //		(P
Cancel Finished				Hel

- d. in the left field enter "session.logon.last.username" (without quotes)
- e. in the right field enter "session.oauth.scope.last.jwt.upn" (without quotes)
- f. Click the Finished button.

12. Click the Save button

Properties Branch Rules	
Name: View Client Variable Assign	
Variable Assign	
Add new entry	Insert Before: 1 🔻
Assignment	
1 session.logon.last.username = session.oauth.scope.last.jwt.upn <u>change</u>	×
Cancel Save	Help

13. The Updated VPE should look like the below picture. Click on the + between Client Type on the Full or Mobile Browser line and Browser Resource Assign to create an object between the two.



14. Select OAUTH Scope from the Authentication tab and click the Add Item button.

(Picture was cropped to take up less space)

Beg	Begin typing to search				
	n Authentication Assignm	nent Endpoint S			
	AD Auth	Active Director			
0	AD Query	Active Director mapping			
۲	OAuth Scope	OAuth Scope			
\bigcirc	OCSP Auth	Online Certifica			
0	On-Demand Cert Auth	Dynamically in			
\bigcirc	OTP Generate	Generate One			
0	OTP Verify	Verify One Tim			
Canc	el Add Item				

15. In the OAUTH Scope

Properties* Branch Rules	
Name: Browser OAuth Scope	
OAuth	
Token Validation Mode	Internal T
JWT Provider List	/Common/WS1-Provider 🔻
Cancel Save (*Data in tab has been changed,	please don't forget to save) Help

- a. Provide a Unique Name (Since on the Browser Path we put Browser OAuth Scope)
- b. Change the Token Validation Mode to Internal.
- c. Select the JWT Provider previously created in F5 Configurations.
- d. Click the Save Button.
- 16. The Updated VPE should look like the below picture. Click on the + between Browser OAuth Scope and Browser Resource Assign in the Successful line to create an object between the two.



17. Select Variable Assign from the Assignment tab and click the Add Item button.

(Picture was cropped to take up less space)

Begin typing to search	
Logon Authentication Assign	ment Endpoint Security
O ACL Assign	Assign existing Acces
Variable Assign	Assign custom variab
O VMware View Policy	Specify a policy that
Cancel Add Item	

18. In the Variable Assign

Properties* Branch Rules	
Name: Browser Variable Assign	
Variable Assign	
Add new entry Insert Befo	re: 1 🔻
Assignment	
1 empty <u>change</u>	×
	Hala

- a. Enter a Unique Name (Since on the Browser Path we put Browser Variable Assign)
- b. Click the "Add new entry" button
- c. Click the "change" link on line 1

~		
+		*
		` II
	* 4	*

- d. in the left field enter "session.logon.last.username" (without quotes)
- e. in the right field enter "session.oauth.scope.last.jwt.upn" (without quotes)
- f. Click the Finished button.

19. Click the Save button

Properties* Branch Rules					
Name: Browser Variable Assign					
Variable Assign					
Add new entry Insert Before:	1 🔻				
Assignment					
1 session.logon.last.username = session.oauth.scope.last.jwt.upn <u>change</u>	×				
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help				

20. This is what the end state Visual Policy Editor (VPE) should look like.

	ess Policy
Access Policy: /	Common/Demo-HZN-CPA.app/Demo-HZN-CPA [Edit Endings] (Endings: Allow, Deny [default])
Start	X VMware View X Successful + ->> Yiew Client Variable Assign fallback + ->> Allow ent Type Full or Mobile Browser + ->> Successful + ->> Browser Variable Assign fallback + ->> Allow fallback + ->> Successful + ->> Browser Variable Assign fallback + ->> Allow fallback + ->> Browser Variable Assign fallback + ->> Allow fallback + ->> Browser Variable Assign fallback + ->> Allow fallback + ->> Browser Qauth Scope fallback + ->> Denv fallback + ->> Denv Denv Denv

Add New Macro

21. Once configuration is completed click on the "Apply Access Policy" link in the top left of the screen to save all of the changes and apply them.



Verifying JWT Token Functioning

Once fully configured there are ways to validate if a JWT token is being created and sent to the appropriate site. This validation will be done using Google Chrome as the browser.

1. In VIDM/WS1 Portal login as a user with access to the horizon resources.



2. In the browser click the 3 Dots in the upper right-hand corner → More Tools → Developer Tools. This will open the Developer Tools Console within the browser window.

	MER		×		
	☆	.	1		
New tab			Ctrl+T		
lew windo	w		Ctrl+N		
lew incogn	nito windov	w Ctrl+S	Shift+N		
istory			•		
ownloads			Ctrl+J		
Bookmarks			•		
		000			
loom	- 10	JU% +	1.4		
Print			Ctrl+P		
Print Cast			Ctrl+P		
Print Cast Find			Ctrl+P Ctrl+F		
Print Cast Find Viore tools			Ctrl+P Ctrl+F	Save page as	c
Print Cast Find Viore tools Edit	Cut	Сору	Ctrl+P Ctrl+F Paste	Save page as Add to desktop	c
Print Cast ind Aore tools dit	Cut	Сору	Ctrl+P Ctrl+F Paste	Save page as Add to desktop Clear browsing data	C Ctrl+Shift
Print Cast Find More tools Edit Settings	Cut	Сору	Ctrl+P Ctrl+F Paste	Save page as Add to desktop Clear browsing data Extensions	C Ctrl+Shift
Print Cast Find More tools Edit Settings Help	Cut	Сору	Ctrl+P Ctrl+F Paste	Save page as Add to desktop Clear browsing data Extensions Task manager	Ctrl+Shift Shift

3. In the Developer Console select the "Network" tab

R	Elements	Console Source	es Network P	erformance Memor	y Application	Security Audits					:	×
٠	0 🔳 🏹	View: 📰 🐂 🗆) Group by frame	Preserve log	Disable cache	Offline Online	W					
Filte	r	🗌 Hide data	a URLs 📶 🛛 XHR	JS CSS Img Media	Font Doc WS	Manifest Other						
	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms	70 ms	80 ms	90 ms	100 ms		11
	Recording network activity											
				Perior	n a request or n	it FS to record tr	le reload.					
:	Console											×
0	top	▼ Filter		Defa	ult levels 🔻							¢
>												

4. In the Catalog Section of the Workspace One Portal select an Application or Desktop and click the "Open" field for that App or Desktop that will trigger the event to launch either the HTML5 or Native Client.

Note in the Developer Console an item will appear usually named Workspace-****** VMware Book Open VMware Horizon Client? SF1400 🏾 🍐 Easy Gluten-free Dair Other bookmarks ard 🧰 M 🚺 Workspace ONE Matthew Mabis v Always open these types of links in the associated app Open VMware Horizon Client Cancel All Apps 2 RDP W10-CPA Calculator Linux lumpho Putty Open Open Open Open Open Elements Console : × 🖲 🔕 🖿 🗑 View: 📰 🛬 🗉 Group by frame Pre Disable cache Offline Online 🔲 Hide data URLs 🔊 XHR JS CSS Img Media Font Doc WS Manifest Other 400 ms 450 ms 500 ms 550 ms 600 ma 650 ms 750 m 800 m Туре Time WORKSPACE-b98617db-b0b4-3900-9a86-38889 2.9 KB requests | 2.9 KB transferred

Select the Object created in the previous section (Named Workspace-***<Some Long GUID>***).
 Note: that the url/uri string will have the FQDN of the horizon environment as per previous section

"Configuring VMware Identity Manager"

Name	× Headers Preview Response Cookies Timing
WORKSPACE-b98617db-b0b4-3900-9a86-38889b4d9ca0-Virtu	▼{status: "Success",…}
	<pre>v response: {resourceUUD: "b98617db-b084-3908-9886-38889b409ca0", resourceType: "ViewApp",-} v launchURLs: [launchContext: "URL_LAUNCHABLE",-,} {launchContext: "URL_LAUNCHABLE",-,}] v0: [launchContext: "URL_LAUNCHABLE",-,} launchContext: "URL_LAUNCHABLE",-,,] launchContext: "URL_AUNCHABLE",-,,] launchContext: "URL_AUNCHABLE,-,,] launchCo</pre>

- a. In the Preview Tab of the developer console expand the "Response:"
- b. Expand "launchURLs:"
- c. Expand both the "0:" and "1:" sections to reveal the launch URLs.
- 6. In the Launch URL Strings there will be a section called "SAMLart=" if the line looks like "SAMLart=JWT:" then VMware Identity Manger is wrapping the JWT token within the SAML artifact field for the F5 to Decrypt. If the "SAMLart=" field does not contain JWT: then the Horizon Environment that you are trying to access is not configured for JWT Wrapping as per previous section "Configuring VMware Identity Manager"

× Headers Preview Response Cookies Timing LaunchContext: "URL_LAUNCHABLE",...} unchContext: "URL_LAUNCHABLE",...} university: "https://domo-hzn-cpa.bd.f5.com:443/view-client/1.0/index.html2applicationId=cn%30c8a1f7c5-a292-4bff-be26-1d01a809416f,ou%3Dentitlements,dc%3Dvdiglobal,dc%3Dvmware,dc%3Dint&SAMLart=JWT:ey30eX4101XV2Qu unihande: "SaMCSER_WW" ▼ 1: {launchContext: "URL_LAUNCHABLE",...} launchContext: "URL_LAUNCHABLE" uninionita. uni_innormat. uni_innormat. uni: "mmare-view://dem/tn-cpa.bd.f5.com:443/cn%30c8a1f7c5-a192-4bff-be26-1d01a889416f,ou%30entitlements,dc%30vdiglobal,dc%30vmware,dc%30int75AMLert=3WT:ey30eXA1013KV1QLLC3hbGci013SUIINIIsImtp2C161jE1MT unihandier: "Mountanti (Marchandia) (Marchandia)

Troubleshooting

If the following error or something like it is seen check your DNS Settings on your VIDM Servers to ensure they are pointing at the LTM VIP not the APM VIP, if they do the following errors have been seen.

