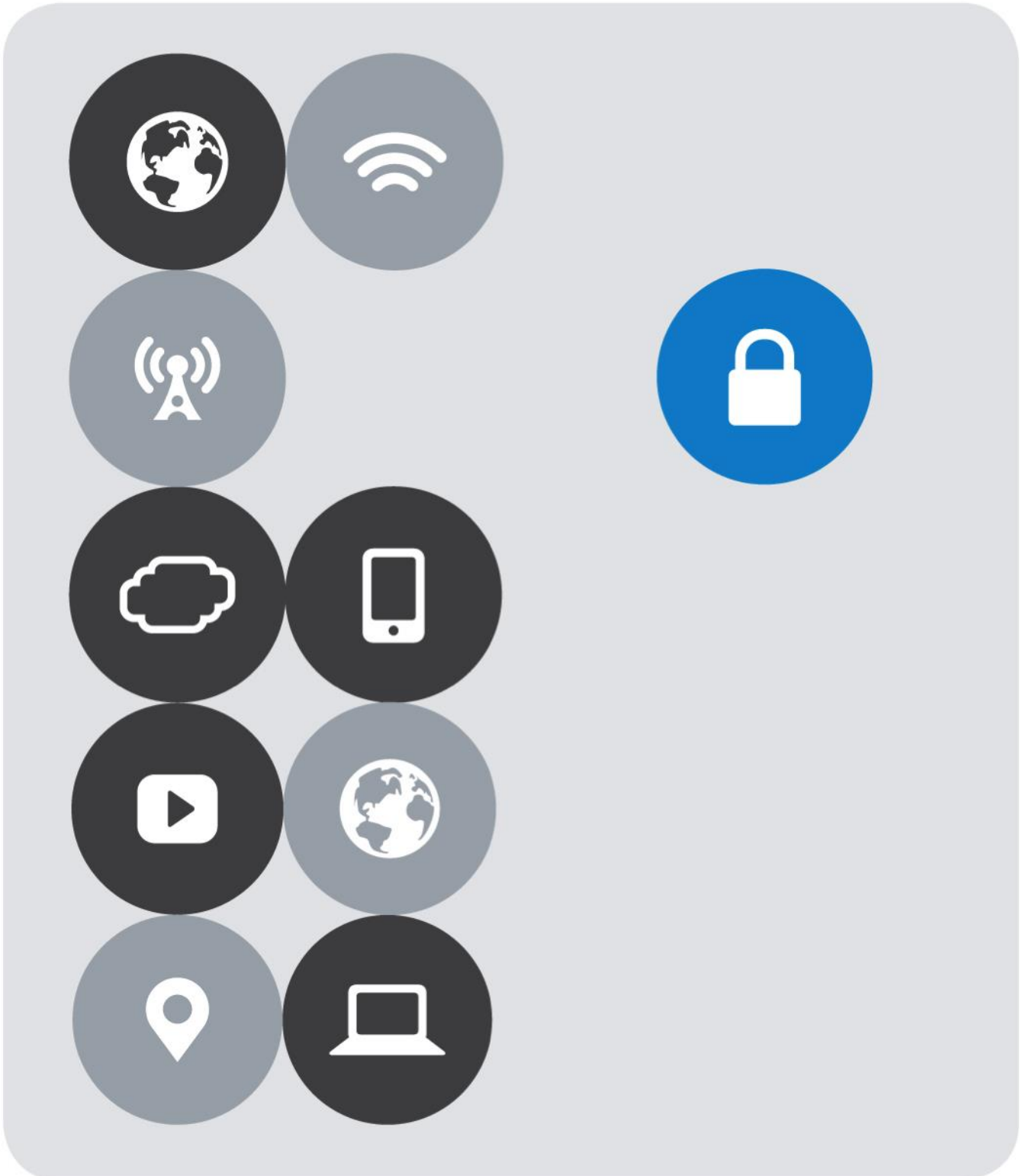




INTEGRATION GUIDE

vmware®

Access Policy Manager (APM) Proxy with Workspace ONE





Version History

Date	Version	Author	Description	Compatible Versions
Dec 2020	2.0	Matt Mabis	Updates to Documentation	Workspace ONE Cloud with Connector 19.03.x.x (2) (3)
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) 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 the joint solutions, its recommended to open a support case with VMware first.

(3) The current release of Workspace ONE Cloud and Workspace ONE Access as of December 2020 as per VMware still only supports the version of Workspace ONE Access Connector 19.03.x.x for Virtual Apps (Citrix, Horizon, Horizon Cloud and ThinApp) as per release notes and documentation.

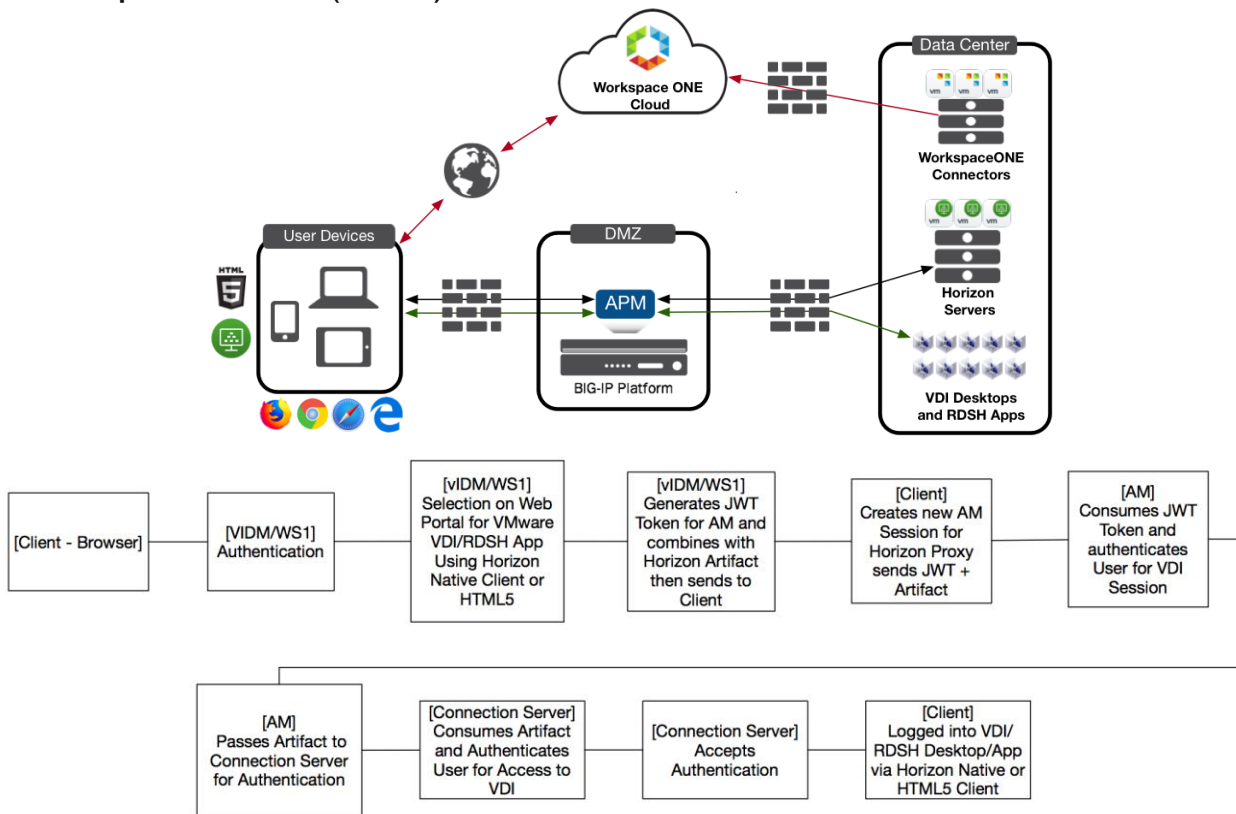


Contents

Version History	2
Overview	4
Workspace ONE (WS1) - Cloud	4
VMware Workspace ONE Access (VIDM) - On-Premises.....	5
Caveats.....	6
Prerequisites	7
Prerequisite - Workspace ONE Access (VIDM) LTM Configuration	8
Prerequisite (VMware Horizon APM Configuration)	9
Workspace ONE Configurations	10
Enable JWT Functionality in Workspace ONE.....	10
F5 BIG-IP Configurations.....	12
Disable Strict Updates on APM Configuration.....	12
Create OAUTH Resources	13
Modify Horizon Access Policy	16
Verifying JWT Token Functioning	22
Troubleshooting.....	24

Overview

Workspace ONE (WS1) - Cloud

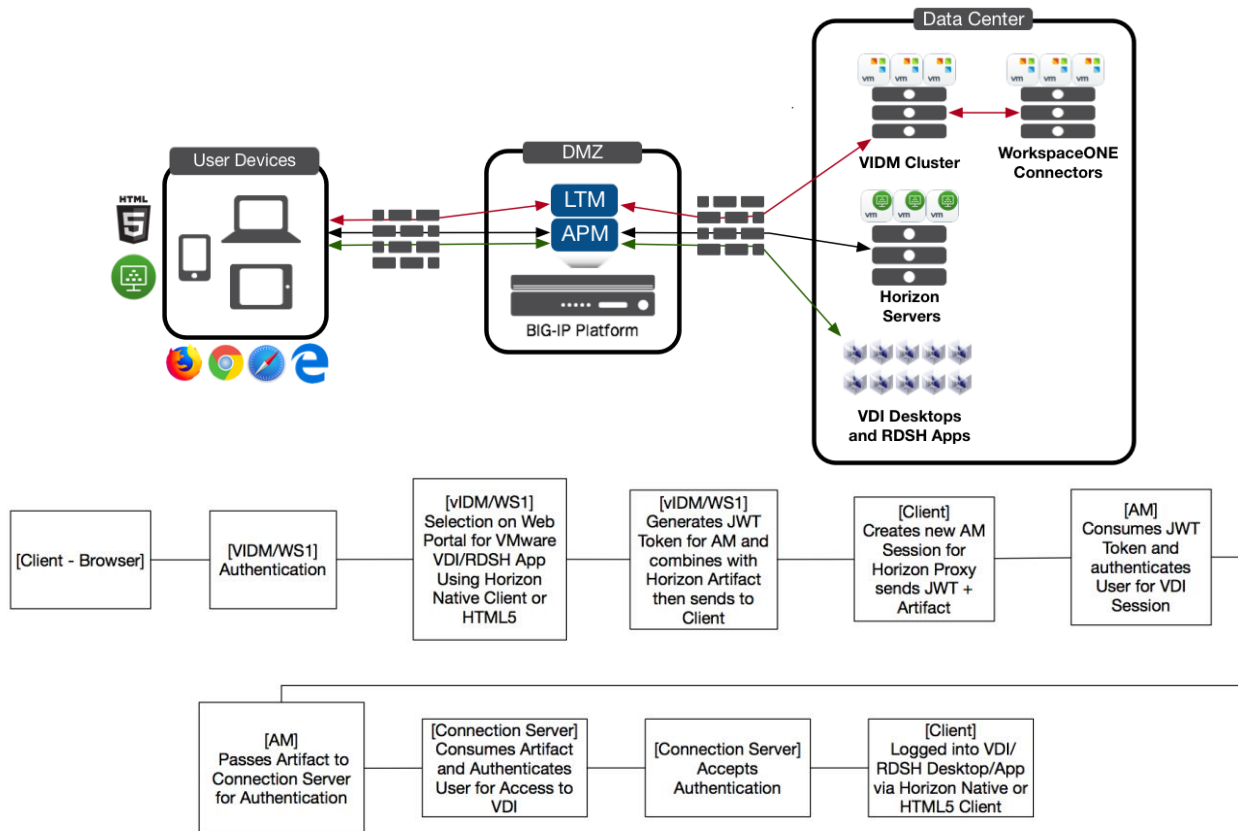


Workspace ONE combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Workspace ONE reduces the complexity of IT administration.

Workspace ONE Cloud instead of being deployed on-premises 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 Access Policy Manager (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 Workspace ONE Access (VIDM) - On-Premises



VMware Workspace ONE Access (VIDM) 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 Access reduces the complexity of IT administration.

Workspace ONE Access is delivered as a virtual appliance (VA) that is easy to deploy onsite and integrate with existing enterprise services and a Workspace ONE Access Connector will be installed on a Windows OS for integrations with Virtual Applications and Active Directory authentication. 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 Workspace ONE Access. This document provides step-by-step instructions for setting up Workspace ONE as an Identity Provider (IDP) in front of F5 Access Policy Manager (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 Workspace ONE 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. Internet Explorer 11 (IE11) and Microsoft Edge Browsers are only supported on Windows 10 Build 1703 and Later due to Microsoft 507-character limit in Application Protocol URL.
<https://blogs.msdn.microsoft.com/ieinternals/2014/08/13/url-length-limits/>
Microsoft will not fix this in previous builds of Windows 10 less than build 1703 nor backport to earlier versions of Windows as this is an OS limitation and not a Browser limitation.
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-by-step 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 13.1.1.3+ or newer.
2. Create/import an SSL Certificate that contains the load balanced FQDN that will be used for Workspace ONE Access Portal and Connectors.
3. Upload the following to the BIG-IP system: (Workspace ONE Access (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 Workspace ONE Access appliance.
4. Workspace ONE is deployed and configured.
 - For Workspace ONE Cloud the environment has been setup/configured with connectors to the domain and horizon environment.
 - For Workspace ONE Access (VIDM) a (3-Node) behind a LTM FQDN VIP on the BIG-IP and VIDM is setup/configured 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 Workspace ONE Access features may not be usable with wildcard certificates when SAN support is not defined.

Prerequisite - Workspace ONE Access (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. (Including MobileSSO)

<https://f5.com/Portals/1/PDF/Partners/f5-big-ip-vmware-workspaceone-integration-guide.pdf>

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List Virtual Address List Statistics

WS1-OnPremise Search Reset 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 Servers : Virtual Server List » WS1-OnPremise

Properties Resources Statistics

Configuration: Basic

General Properties

Name: WS1-OnPremise

Partition / Path: Common

Description:

Type: Standard

Source Address: 0.0.0.0/0

Destination Address/Mask: 10.105.169.107

Service Port: 443 HTTPS

Notify Status to Virtual Address: ☒

Link: None

Availability: ● Available (Enabled) - The virtual server is available

SyncCookie Status: Off

State: Enabled

SSL Profile (Client): Selected: WS1-ClientSSL Available: clientssl-clientssl-insecure-compatible-clientssl-secure-crypto-server-default-clientssl

SSL Profile (Server): Selected: serverssl-insecure-compatible Available: apm-default-serverssl-crypto-client-default-serverssl-pcop-default-serverssl-serverssl

SMTPS Profile: None

Client LDAP Profile: None

Server LDAP Profile: None

SMTP Profile: None

VLAN and Tunnel Traffic: All VLANs and Tunnels

Source Address Translation: Auto Map

Content Rewrite

Rewrite Profile: None

HTML Profile: None

Access Policy

Access Profile: None

Connectivity Profile: None

Per-Request Policy: None

VDI Profile: None

Application Tunnels (Java & Per-App VPN): ☐ Enabled

OAM Support: ☐ Enabled

ADFS Proxy: ☐ Enabled

PingAccess Profile: None

Acceleration

Rate Class: None

OneConnect Profile: None

NTLM Conn Pool: None

HTTP Compression Profile: None

Web Acceleration Profile: None

HTTP/2 Profile: None

Update Delete

Local Traffic » Virtual Servers : Virtual Server List » WS1-OnPremise

Properties Resources Statistics

Load Balancing

Default Pool: WS1-Pool

Default Persistence Profile: WS1-Persistence

Fallback Persistence Profile: None

Update

iRules Manage...

Name

No records to display.

Policies Manage...

Name

No records to display.

Prerequisite (VMware 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>

iApps » Application Services : Applications




Application Service List

F5 iApps and Resources

<input checked="" type="checkbox"/>	▲ Name	◆ Template	Template Validity	◆ Partition / Path
<input type="checkbox"/>	Demo-HZN-CPA	f5.vmware_view.v1.5.3		Common/Demo-HZN-CPA.app

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List
Virtual Address List
Statistics

<input checked="" type="checkbox"/>	▼ Status	▲ Name	◆ Description	◆ Application	◆ Destination	◆ Service Port	◆ Type	Resources	◆ Partition / Path
<input type="checkbox"/>		Demo-HZN-CPA_apm_redirect		Demo-HZN-CPA	209.194.169.137	80 (HTTP)	Standard	Edit...	Common/Demo-HZN-CPA.app
<input type="checkbox"/>		Demo-HZN-CPA_pcoip_udp		Demo-HZN-CPA	209.194.169.137	4172	Standard	Edit...	Common/Demo-HZN-CPA.app
<input type="checkbox"/>		Demo-HZN-CPA_proxy_https		Demo-HZN-CPA	209.194.169.137	443 (HTTPS)	Standard	Edit...	Common/Demo-HZN-CPA.app

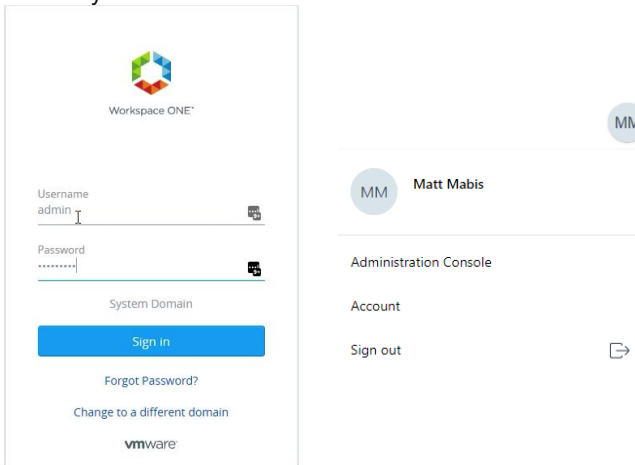
Workspace ONE Configurations

Enable JWT Functionality in Workspace ONE

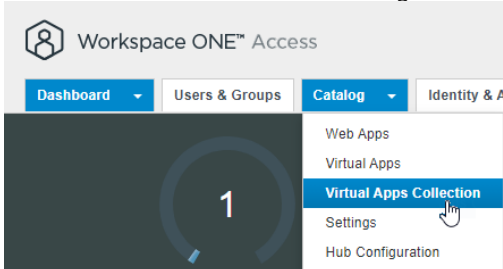
After making sure that either the Workspace ONE Cloud environment is deployed and setup with connectors and VMware Horizon and/or the VMware Workspace ONE Access (VIDM) environment is setup behind the load balancer and configured for VMware Horizon we move along to configuring the Workspace ONE environment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

Log onto the Workspace ONE Portal Configuration Page

1. In a browser, login as a Workspace ONE Admin to the Workspace ONE FQDN once Logged in click on the Icon for your authenticated user and select "Administration Console"



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



3. Ensure that a Horizon environment is setup and configured for the integration, select the Horizon Configuration in our Example its BD-Horizon.

Virtual Apps Collections

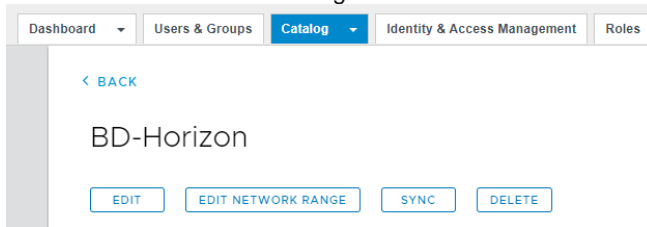
NEW
EDIT
SYNC
DELETE

	Name	Source Type	Sync Frequency	Sync Status
<input type="radio"/>	hyak	Horizon	Manual	Completed More
<input type="radio"/>	BD-Horizon	Horizon	Weekly	Completed More

INTEGRATION GUIDE

Access Policy Manager (APM) Proxy with Workspace ONE

- Click on the “Edit Network Range” button.



- Select the Appropriate Network Range link, in our use case “Web Browser” is the correct range.
Network Ranges

Assign pods to the following network ranges. If you cannot find the right network ranges for these pods, create a new one.

Name	Description	IP Address Range
ALL RANGES	A network for all ranges	0.0.0.0 - 255.255.255.255
Web Browser	d	0.0.0.0 - 255.255.255.255
+ CREATE NETWORK RANGE		

- In the selected range’s setting scroll to the bottom, if using VMware Cloud Pod Architecture, you will see a View CPA Federation, if not you will see just a Pod Configuration.

NOTE: Client Access FQDN’s must be filled out for POD and CPA Federation (if exists) to click Save.

[← NETWORK RANGES](#) Assign Pods to Network Ranges

IP Ranges ⓘ

To

[+ ADD IP RANGE](#)

Pod	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT ⓘ
hzn-broker-01.bd.f5.com	horizon-internal.bd.f5.co	443	<input type="checkbox"/> No	+ ADD

View CPA Federation	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT
Hzn-CPA-Main	horizon-cpa.bd.f5.com	443	<input checked="" type="checkbox"/> Yes	f5cpa × + ADD

[CANCEL](#) [SAVE](#)

- Click the slider to enable (Green) for “Wrap Artifact in JWT” on the Horizon Environment (Federation or Pod) depending on the external access that was configured in previous steps.
- Click the (+) ADD button under the “Audience in JWT” next to the slider and provide a unique name (our example is f5cpa)
- Click the Save Button.

Once Completed the configuration for Workspace ONE 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

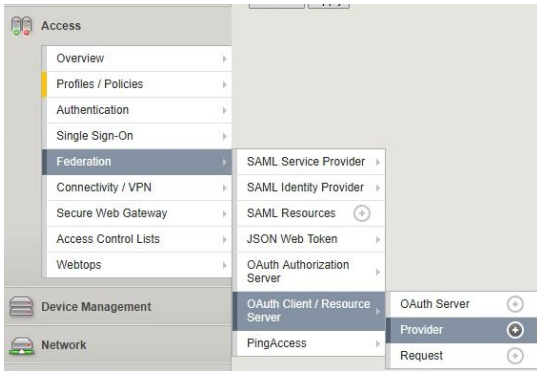
2. Under the iApps Section → Application Services, select the iApp Deployed for the Horizon APM Configuration

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

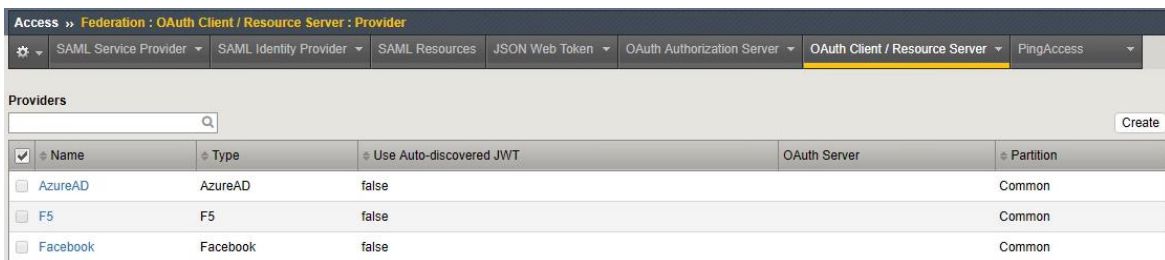
- a. Change the pull-down menu from **Basic** to **Advanced**.
- b. **Uncheck** the **Strict Updates** checkbox.
- c. Click the **Update** button.

Create OAUTH Resources

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



2. Click the Create Button



3. In the OAuth Client / Resource Server Provider Menus

Access > Federation : OAuth Client / Resource Server : Provider > New...

Properties

General Properties

Name: MyWS1

Description:

Type: 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-configuration Discover

Authentication URI:

Token URI:

Token Validation Scope URI:

UserInfo Request URI:

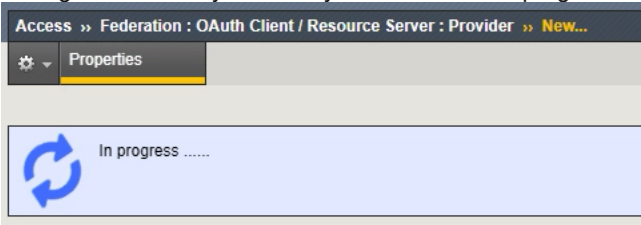
Cancel Save

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

INTEGRATION GUIDE

Access Policy Manager (APM) Proxy with Workspace ONE

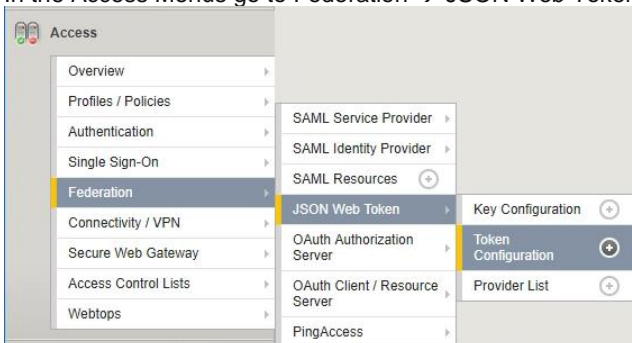
4. During the Discovery Process you will see an “In progress” section this is expected behavior.



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 configuration.

OpenID URI	<input type="text" value="https://myws1-onprem.bd.f5.com/SAAS/auth/.well-known/openid-configuration"/> <input type="button" value="Discover"/>	
Authentication URI	<input type="text" value="https://myws1-onprem.bd.f5.com/SAAS/auth/oauth2/authorize"/>	
Token URI	<input type="text" value="https://myws1-onprem.bd.f5.com/SAAS/auth/oauth2/token"/>	
Token Validation Scope URI	<input type="text"/>	
Userinfo Request URI	<input type="text" value="https://myws1-onprem.bd.f5.com/SAAS/jersey/manager/api/userinfo"/>	
Issuer	<input type="text" value="https://myws1-onprem.bd.f5.com/SAAS/auth"/>	
Signing Algorithm	<div>Allowed RS256</div>	<div>Blocked</div>
Key (JWK)	<div>Allowed RSA:1516721347:undefined:undefined</div>	<div>Blocked</div>

6. In the Access Menu go to Federation → JSON Web Token → 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 Workspace ONE FQDN in the Issuer.

Access >> Federation : JSON Web Token : Token Configuration				
	SAML Service Provider	SAML Identity Provider	SAML Resources	JSON Web Token
Token Configurations (JWT)				
<input checked="" type="checkbox"/>	Name	Auto Discovered	Issuer	Partition / Path
<input type="checkbox"/>	auto_jwt_MyWS1	true	https://myws1-onprem.bd.f5.com/SAAS/auth	MyWS1 Common
<input type="button" value="Delete"/>				

INTEGRATION GUIDE

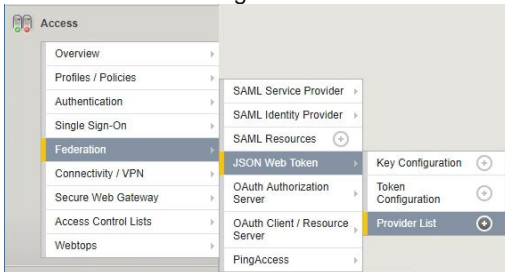
Access Policy Manager (APM) Proxy with Workspace ONE

8. In the Token Configuration

The screenshot shows the 'Properties' tab of the 'auto_jwt_MyWS1' configuration. Under 'General Properties', the 'Auto Discovered' checkbox is checked, and the 'Name' is 'auto_jwt_MyWS1'. The 'Issuer' field contains 'https://myws1-onprem.bd.f5.com/SAAS/auth'. The 'Use Provider List Settings' checkbox is checked. The 'Access Token Expires In' field is set to '0' minutes. The 'Audience' field contains 'f5cpa' and has an 'Add' button next to it.

- Type the name of your Audience (Created previously in the Workspace ONE Configurations section) and Click the Add button.
- Once the audience is added scroll to the bottom and click the save button.

9. In the Access Menus go to Federation → JSON Web Token → Provider List



10. Click the Create Button

The screenshot shows the 'Provider List' page. The 'Create' button is highlighted in the top right corner.

11. In the JSON Web Token Provider List

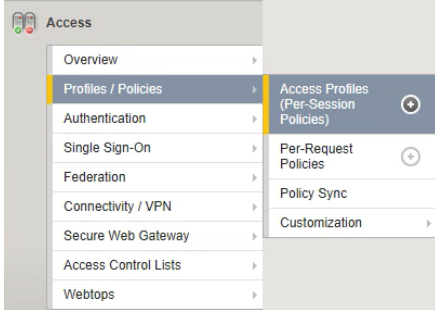
The screenshot shows the 'New...' form for adding a new provider. The 'Name' field is 'WS1-Provider'. The 'Access Token Expires In' field is empty. The 'Provider' field has a dropdown menu showing '/Common/MyWS1' and an 'Add' button. At the bottom, there are 'Cancel' and 'Save' buttons.

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

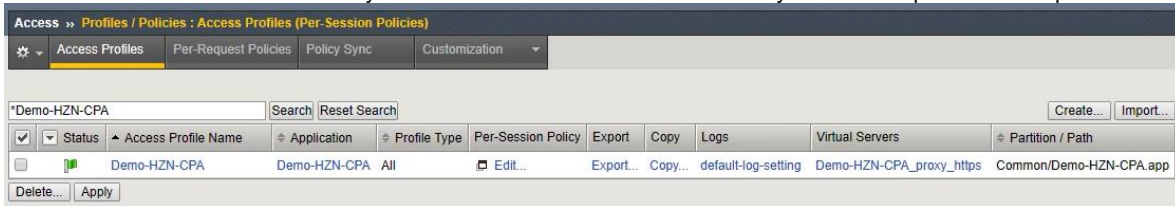
Once these Steps have been completed you can move forward to Modifying the Horizon APM Access Policy.

Modify Horizon Access Policy

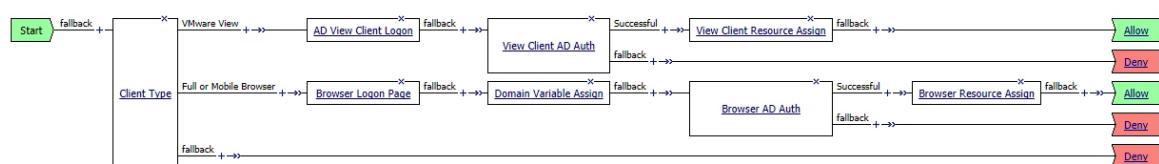
1. In the Access Menus go to Profiles / Polices → Access Profiles (Per Session Policies)



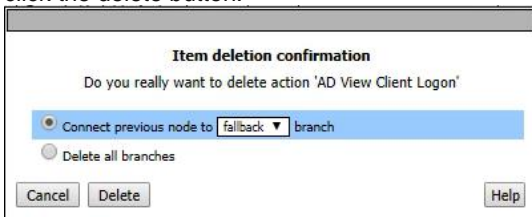
2. Click the Edit in Per-Session Policy under the Horizon APM Access Policy created as part of Prerequisites



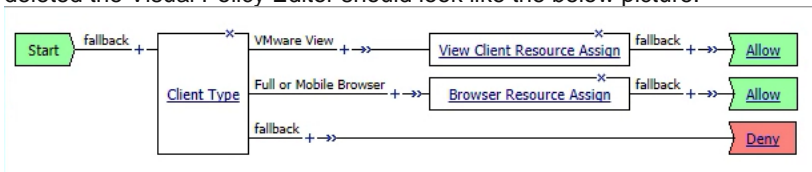
3. In Visual Policy Editor this is a typical Horizon iApp Deployment, we will remove all the policies except Client Type, View Client Resource Assign, and Browser Assign.



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.



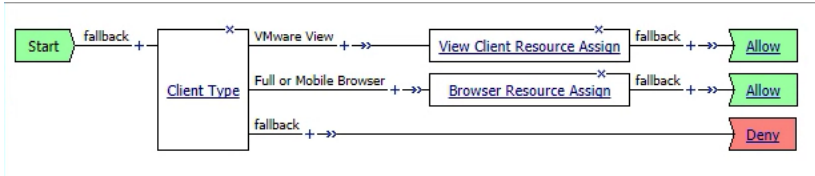
5. Once all the objects except Client Type, View Client Resource Assign and Browser Resource Assign are deleted the Visual Policy Editor should look like the below picture.



INTEGRATION GUIDE

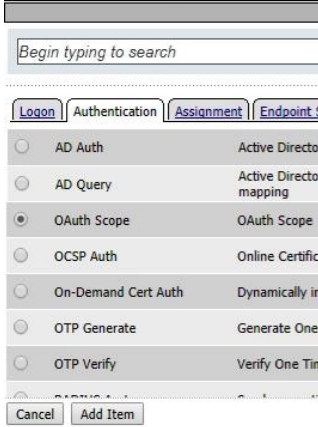
Access Policy Manager (APM) Proxy with Workspace ONE

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



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

(Picture was cropped to take up less space)



- In the OAUTH Scope

Properties Branch Rules

Name: View Client OAuth Scope

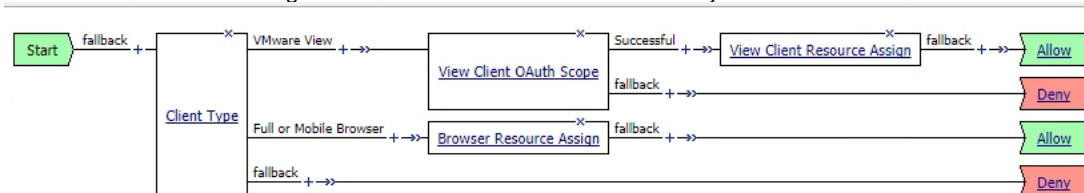
OAuth

Token Validation Mode Internal

JWT Provider List /Common/WS1-Provider

Cancel Save Help

- Provide a Unique Name (Since on the View Client Path we put View Client OAuth Scope)
 - Change the Token Validation Mode to Internal.
 - Select the JWT Provider previously created in F5 Configurations.
 - Click the Save Button.
- 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.



INTEGRATION GUIDE

Access Policy Manager (APM) Proxy with Workspace ONE

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

(Picture was cropped to take up less space)

The screenshot shows the 'Assignment' tab selected. It contains three radio button options: 'ACL Assign' (Assign existing Access), 'Variable Assign' (Assign custom variable), and 'VMware View Policy' (Specify a policy that). The 'Variable Assign' option is selected. Below the options are 'Cancel' and 'Add Item' buttons.

11. In the Variable Assign

The screenshot shows the 'Variable Assign' configuration window. The 'Name' field is 'View Client Variable Assign'. The 'Variable Assign' section has an 'Add new entry' button and an 'Insert Before' dropdown set to '1'. Below is a table with one row: '1 empty change'. At the bottom are 'Cancel', 'Save', and 'Help' buttons. A message says: '(*Data in tab has been changed, please don't forget to save)'.

- 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

The screenshot shows the variable assignment configuration. On the left, under 'Custom Variable', is the expression 'session.logon.last.username'. On the right, under 'Session Variable', is the expression 'session.oauth.scope.last.jwt'. At the bottom are 'Cancel', 'Finished', and 'Help' buttons.

- d. in the left field enter “session.logon.last.username” (without quotes)
- e. in the right field change “Custom Expression” to “Session Variable” and enter “session.oauth.scope.last.jwt.upn” (without quotes)
- f. Click the Finished button.

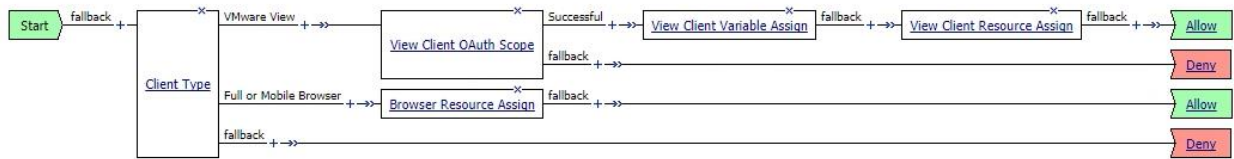
12. Click the Save button

The screenshot shows the 'Variable Assign' configuration window. The 'Name' field is 'View Client Variable Assign'. The 'Variable Assign' section has an 'Add new entry' button and an 'Insert Before' dropdown set to '1'. Below is a table with one row: '1 session.logon.last.username = session.oauth.scope.last.jwt.upn change'. At the bottom are 'Cancel', 'Save', and 'Help' buttons.

INTEGRATION GUIDE

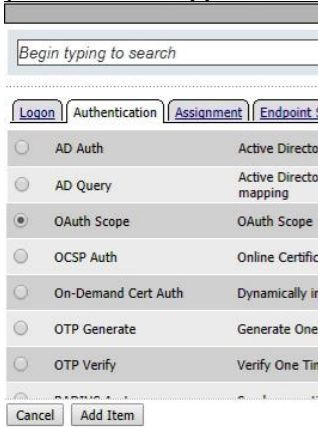
Access Policy Manager (APM) Proxy with Workspace ONE

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)



15. In the OAUTH Scope

Properties* Branch Rules

Name: Browser OAuth Scope

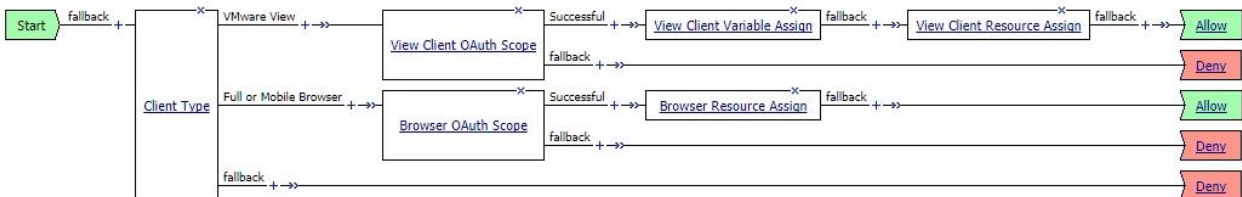
OAuth

Token Validation Mode: Internal

JWT Provider List: /Common/WS1-Provider

Cancel Save (*Data in tab has been changed, please don't forget to save) Help

- Provide a Unique Name (Since on the Browser Path we put Browser OAuth Scope)
 - Change the Token Validation Mode to Internal.
 - Select the JWT Provider previously created in F5 Configurations.
 - 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.



INTEGRATION GUIDE

Access Policy Manager (APM) Proxy with Workspace ONE

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

(Picture was cropped to take up less space)

The screenshot shows the 'Assignment' tab selected. It contains three radio button options: 'ACL Assign' (Assign existing Access), 'Variable Assign' (Assign custom variable), and 'VMware View Policy' (Specify a policy that). The 'Variable Assign' option is selected. Below the options are 'Cancel' and 'Add Item' buttons.

18. In the Variable Assign

The screenshot shows the 'Variable Assign' configuration window. The 'Name' field is 'Browser Variable Assign'. The 'Variable Assign' section has an 'Add new entry' button and an 'Insert Before' dropdown set to '1'. Below is a table with one row: '1 empty change'. At the bottom are 'Cancel', 'Save' (disabled), and 'Help' buttons. A message says '(*Data in tab has been changed, please don't forget to save)'.

- 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

The screenshot shows the variable assignment configuration. On the left, under 'Custom Variable', is the expression 'session.logon.last.username'. On the right, under 'Session Variable', is the expression 'session.oauth.scope.last.jwt.upn'. The 'Unsecure' checkbox is checked.

The screenshot shows the bottom of the configuration window with 'Cancel', 'Finished', and 'Help' buttons.

- d. in the left field enter “session.logon.last.username” (without quotes)
- e. in the right field change “Custom Expression” to “Session Variable” and enter “session.oauth.scope.last.jwt.upn” (without quotes)
- f. Click the Finished button.

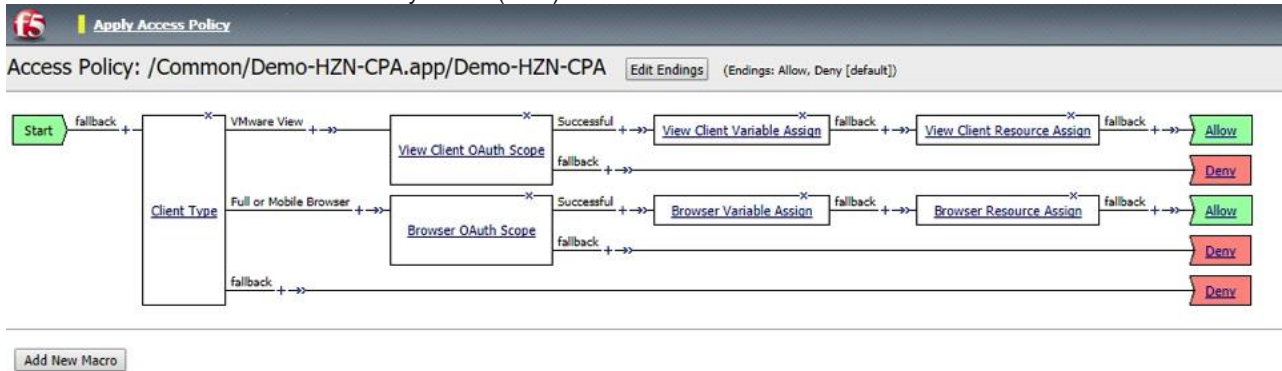
19. Click the Save button

The screenshot shows the 'Variable Assign' configuration window after saving. The 'Assignment' table now contains the expression 'session.logon.last.username = session.oauth.scope.last.jwt.upn' followed by a 'change' link. The 'Save' button is now enabled.

INTEGRATION GUIDE

Access Policy Manager (APM) Proxy with Workspace ONE

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



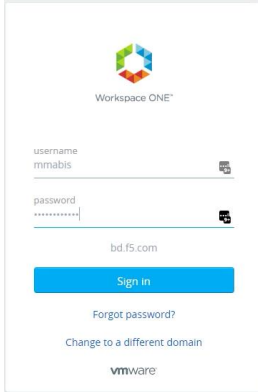
21. Once configuration is completed click on the "Apply Access Policy" link in the top left of the screen to save all the changes and apply them.



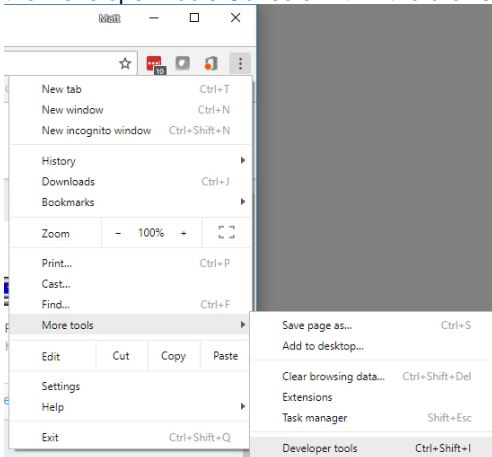
Verifying JWT Token Functioning

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.

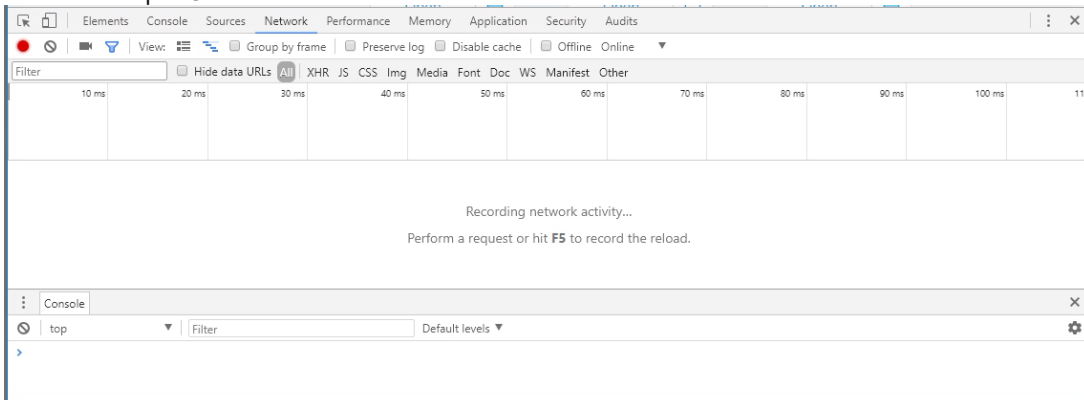
1. In VIDM/WS1 Portal login as a user with access to the horizon resources.



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.



3. In the Developer Console select the “Network” tab



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.

