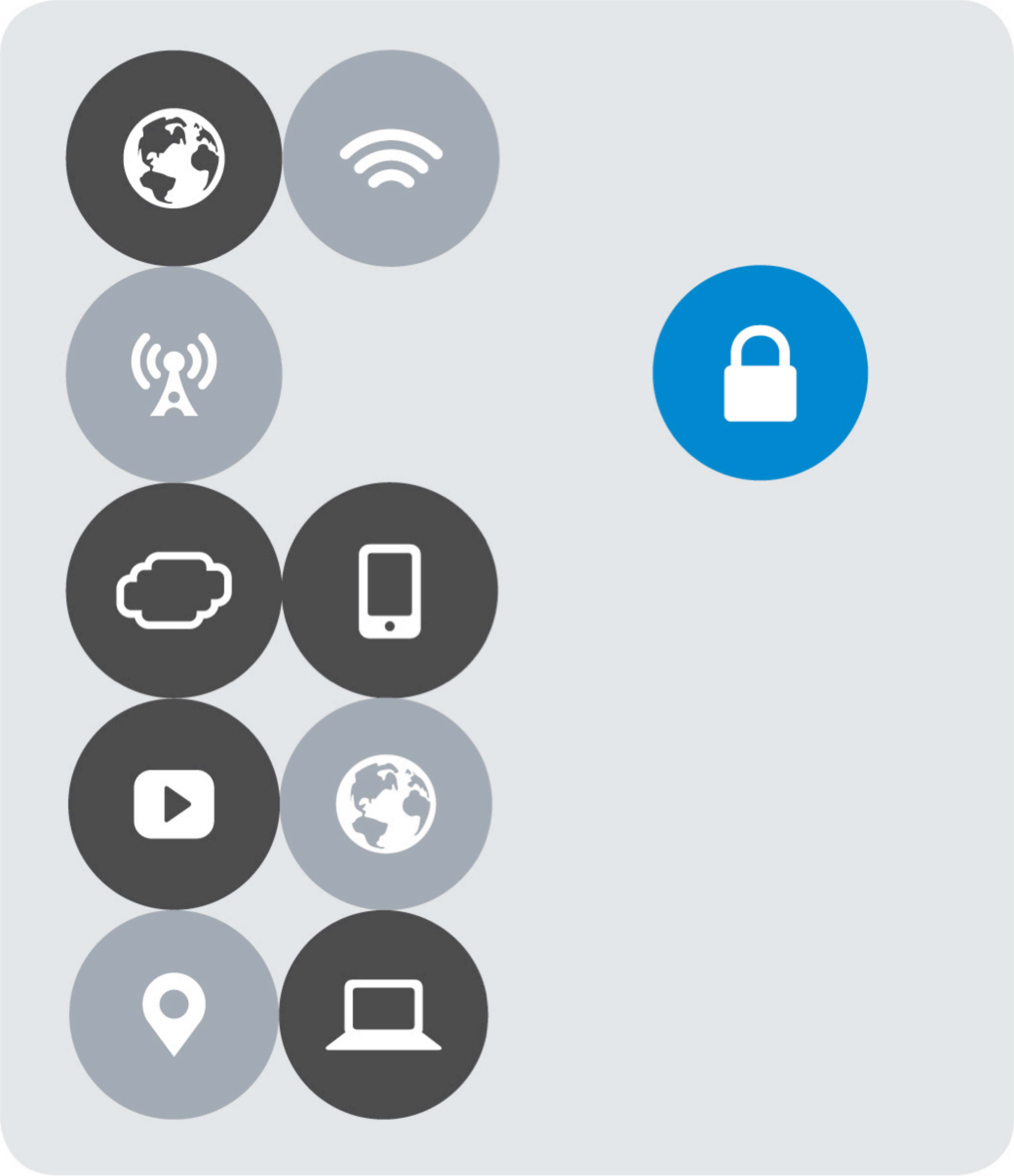
INTEGRATION GUIDE

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:

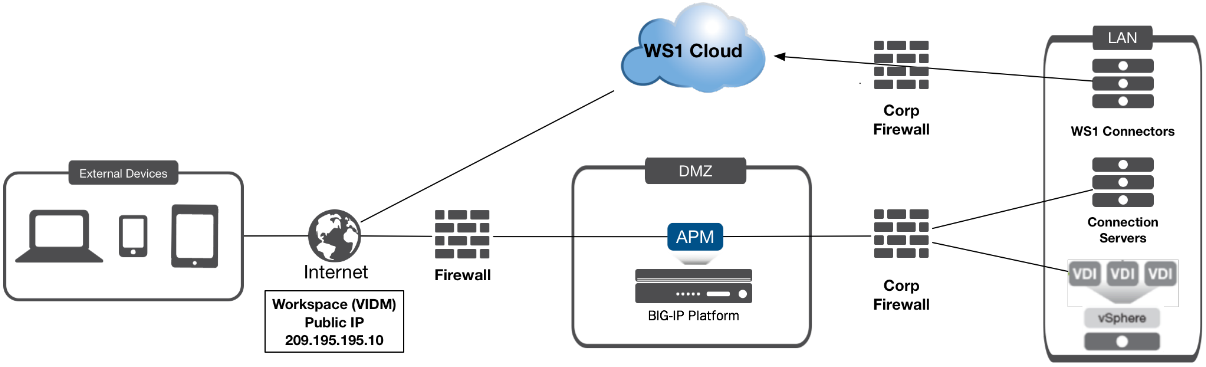
(1) The Version 1.0 Document only supports up to VMware Identity Manager 3.2.x and above, as joint features were added for the integration in 3.2.x that do not exist in previous versions.

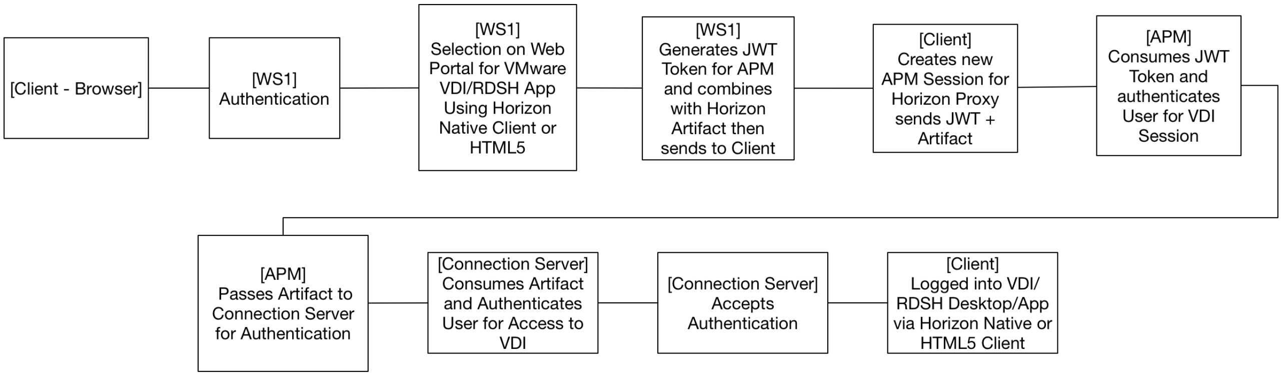
(2) Workspace One Cloud is compatible with this guide, as the VMware Workspace One Cloud edition has continual upgrading, any possible issues with the integration or after deployment issues might be considered a regression in our joint integration code.

Contents

Overview

Workspace One (WS1) - Cloud



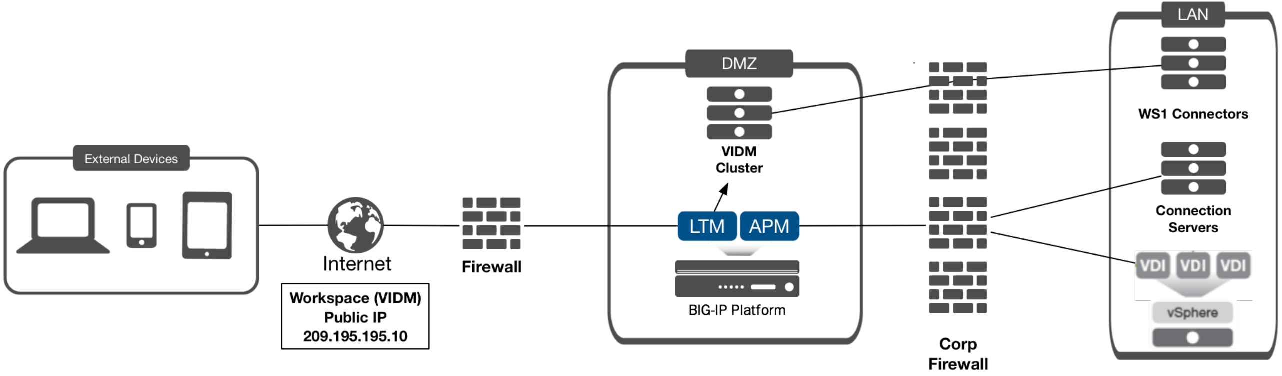

[Client - Browser]
[WS1] Authentication
[WS1] Selection on Web Portal for VMware VDI/RDSH App Using Horizon Native Client or HTML5
[WS1] Generates JWT Token for APM and combines with Horizon Artifact then sends to Client
[Client] Creates new APM Session for Horizon Proxy sends JWT + Artifact
[APM] Consumes JWT Token and authenticates User for VDI Session
[APM] Passes Artifact to Connection Server for Authentication
[Connection Server] Consumes Artifact and Authenticates User for Access to VDI
[Connection Server] Accepts Authentication
[Client] Logged into VDI/ RDSH Desktop/App via Horizon Native or HTML5 Client

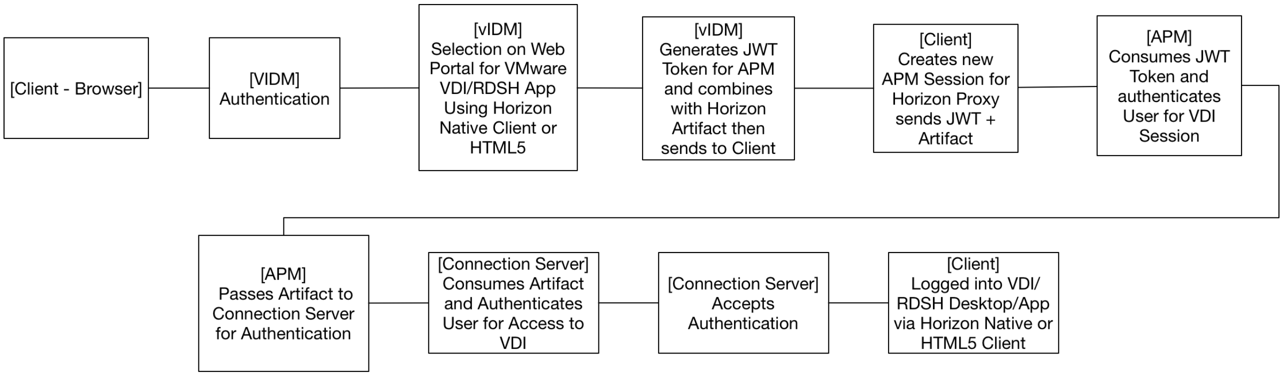
Workspace One combines applications and desktops in a single, aggregated workspace. Employees can then access the desktops and applications regardless of where they are based. With fewer management points and flexible access, Workspace One reduces the complexity of IT administration.

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




[Client - Browser]
[VIDM]
Authentication
[vIDM]
Selection on Web Portal for VMware VDI/RDSH App Using Horizon Native Client or HTML5
[vIDM]
Generates JWT Token for APM and combines with Horizon Artifact then sends to Client
[Client]
Creates new APM Session for Horizon Proxy sends JWT + Artifact
[APM]
Consumes JWT Token and authenticates User for VDI Session
[APM]
Passes Artifact to Connection Server for Authentication
[Connection Server]
Consumes Artifact and Authenticates User for Access to VDI
[Connection Server]
Accepts Authentication
[Client]
Logged into VDI/ RDSH Desktop/App via Horizon Native or HTML5 Client

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 Manger 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-by-step instructions for prerequisites are outside the scope of this document, see the BIG-IP documentation on support.f5.com for specific instructions.

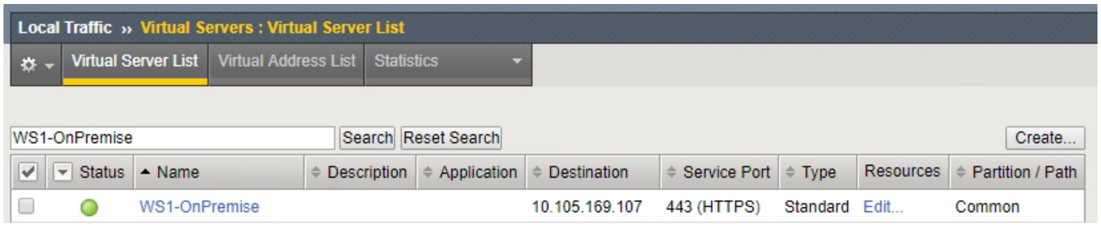
1. F5 requires running this configuration using BIG-IP APM/LTM version 13.1 with an Engineering Hotfix (F5 Support Service Request must be made with mention of RFE 683741-1, 684370-1 and 635509-1.)
   - This functionality will be integrated into version 14.0+, when released.
2. Create/import an SSL Certificate 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)

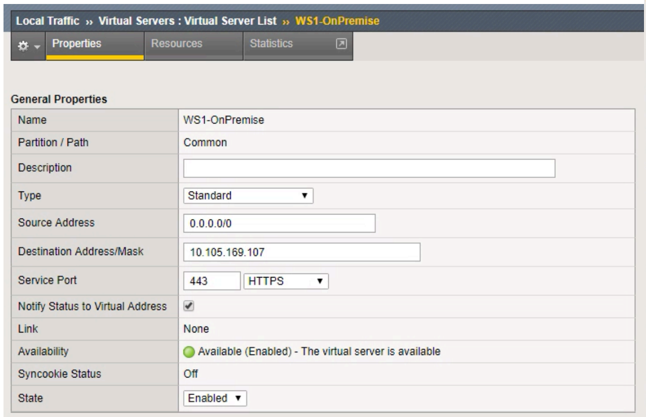
NOTE: If using Workspace One Cloud this prerequisite is not needed

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



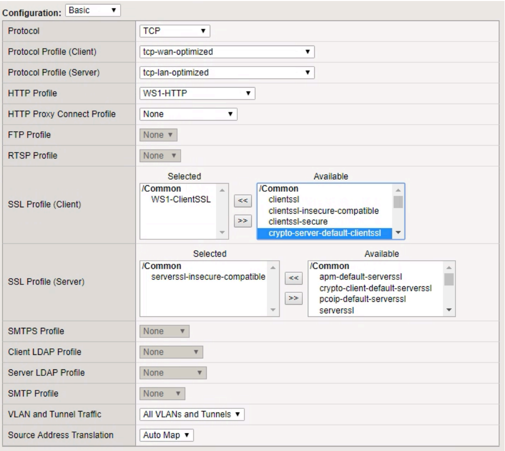
WS1-OnPremise

☑	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

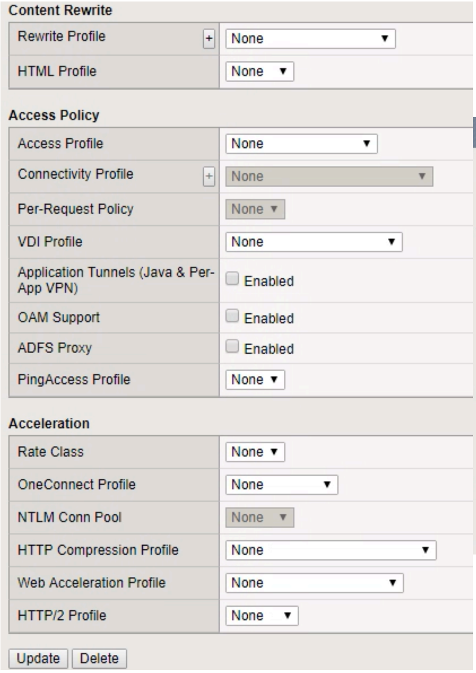
General Properties

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
Syncookie Status	Off
State	Enabled



Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp-wan-optimized
Protocol Profile (Server)	tcp-lan-optimized
HTTP Profile	WS1-HTTP
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected: /Common WS1-ClientSSL Available: /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: /Common serverssl-insecure-compatible Available: /Common apm-default-serverssl crypto-client-default-serverssl pcoip-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

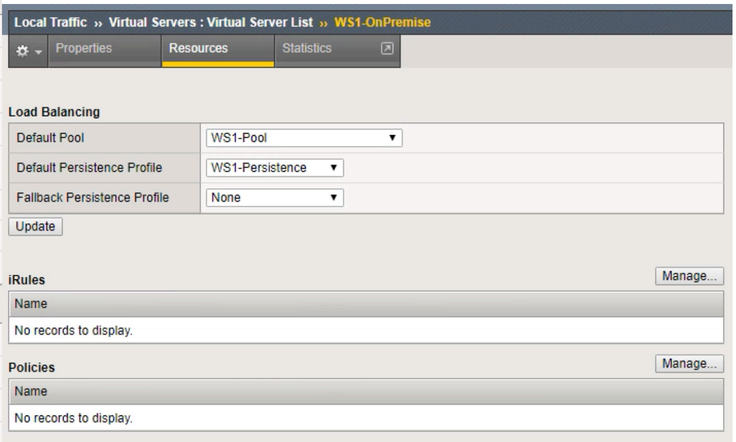
Rewrite Profile	None
HTML Profile	None

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


Local Traffic » Virtual Servers : Virtual Server List » WS1-OnPremise
Properties
Resources
Statistics
Update
Manage...
Manage...

Load Balancing

Default Pool	WS1-Pool
Default Persistence Profile	WS1-Persistence
Fallback Persistence Profile	None

iRules

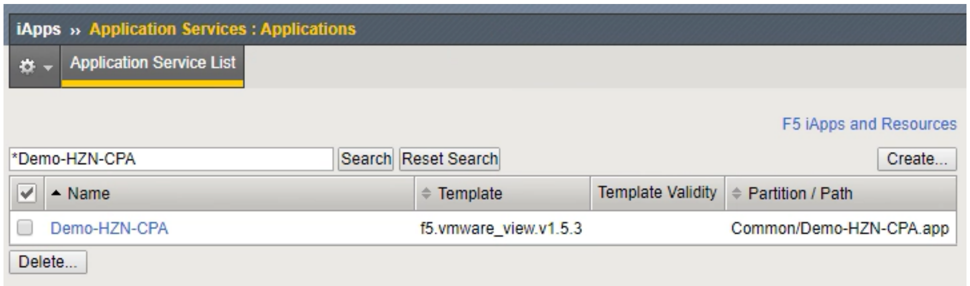
Name
No records to display.

Policies

Name
No records to display.

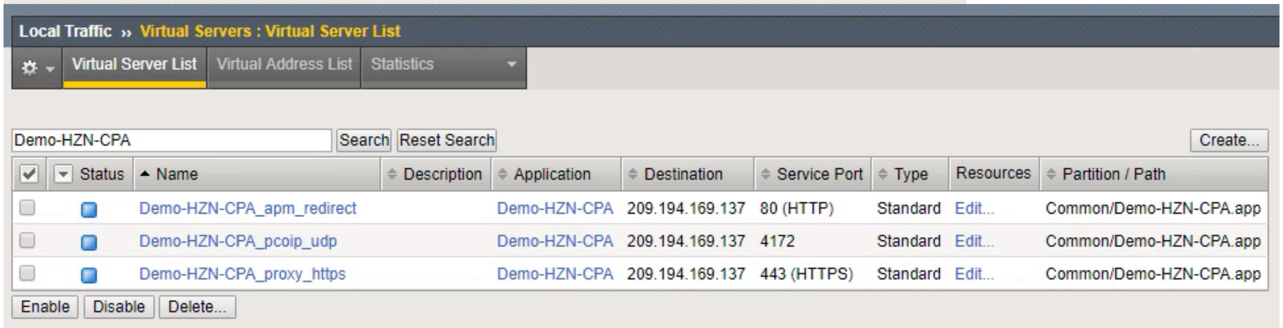
Prerequisite (Horizon APM Configuration)

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



*Demo-HZN-CPA

☑	Name	Template	Template Validity	Partition / Path
☐	Demo-HZN-CPA	f5.vmware_view.v1.5.3		Common/Demo-HZN-CPA.app



Demo-HZN-CPA

☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
☐	🟦	Demo-HZN-CPA_apm_redirect		Demo-HZN-CPA	209.194.169.137	80 (HTTP)	Standard	Edit...	Common/Demo-HZN-CPA.app
☐	🟦	Demo-HZN-CPA_pcoip_udp		Demo-HZN-CPA	209.194.169.137	4172	Standard	Edit...	Common/Demo-HZN-CPA.app
☐	🟦	Demo-HZN-CPA_proxy_https		Demo-HZN-CPA	209.194.169.137	443 (HTTPS)	Standard	Edit...	Common/Demo-HZN-CPA.app

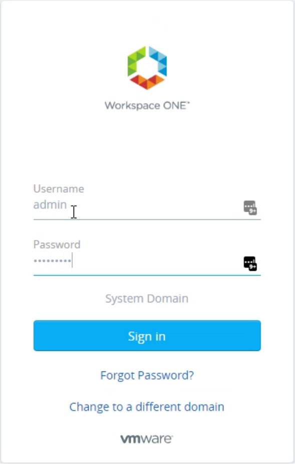
VIDM/WS1 Configurations

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

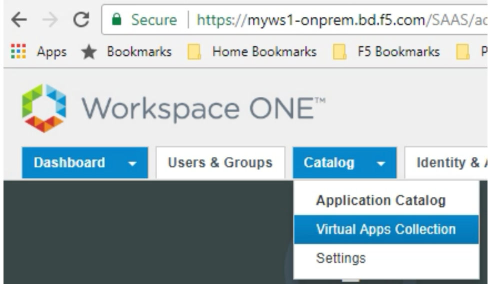
Log onto the VIDM/WS1 Portal Configuration Page

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

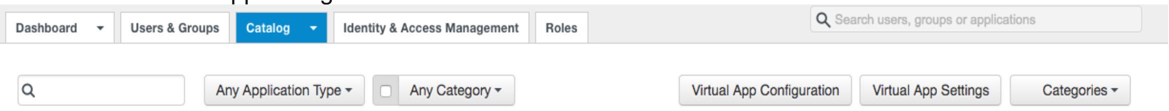


Username: admin
Password: •••••••••

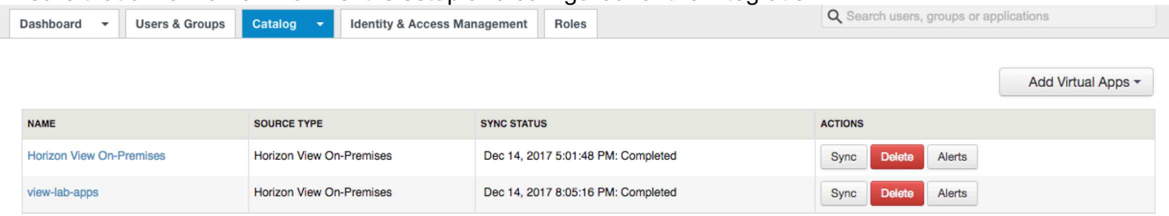
2. Select the down arrow next to Catalog and Select “Virtual Apps”



3. Click on the “Virtual App Configuration” button.

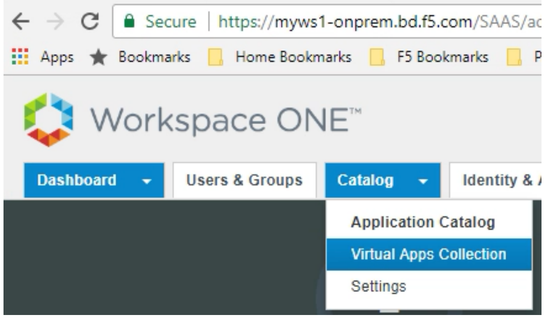


4. Ensure that a Horizon environment is setup and configured for the integration

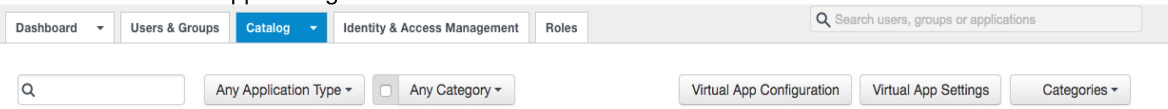

Dashboard
Users & Groups
Catalog
Identity & Access Management
Roles
Search users, groups or applications
Add Virtual Apps

NAME	SOURCE TYPE	SYNC STATUS	ACTIONS
Horizon View On-Premises	Horizon View On-Premises	Dec 14, 2017 5:01:48 PM: Completed	Sync Delete Alerts
view-lab-apps	Horizon View On-Premises	Dec 14, 2017 8:05:16 PM: Completed	Sync Delete Alerts

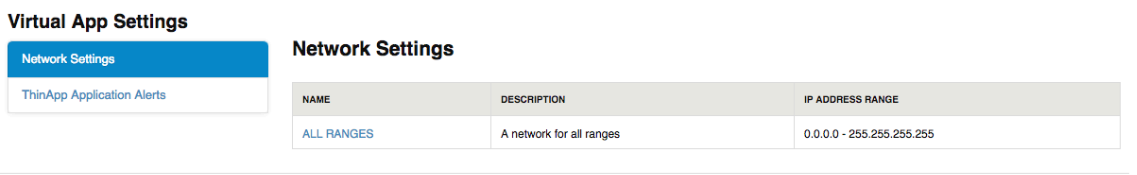
5. Select the down arrow next to Catalog and Select “Virtual Apps”



6. Click on the “Virtual App Settings” button.



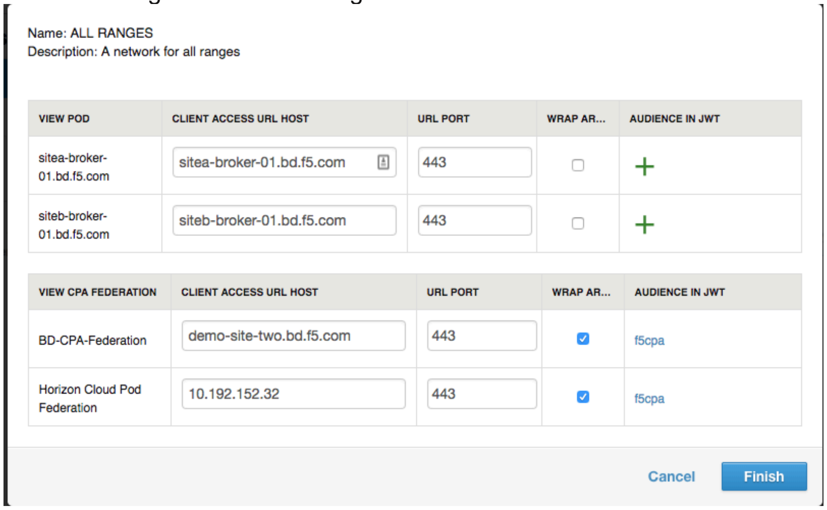
7. Select the Network Settings Tab and Select the “All Ranges” link



Network Settings

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



Name: ALL RANGES
Description: A network for all ranges

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
BD-CPA-Federation	demo-site-two.bd.f5.com	443	☑	f5cpa
Horizon Cloud Pod Federation	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)

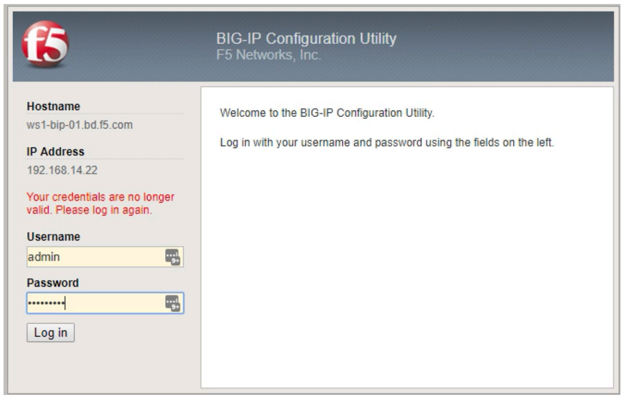
c. Click the Save Button.

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



Hostname: ws1-bip-01.bd.f5.com

IP Address: 192.168.14.22

Your credentials are no longer valid. Please log in again.

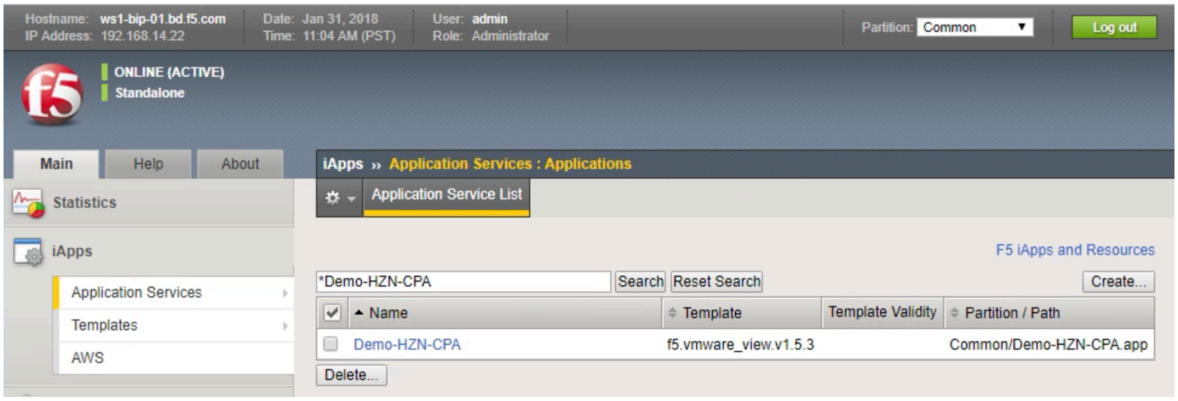
Username: admin

Password: ••••••••••

Welcome to the BIG-IP Configuration Utility.

Log in with your username and password using the fields on the left.

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

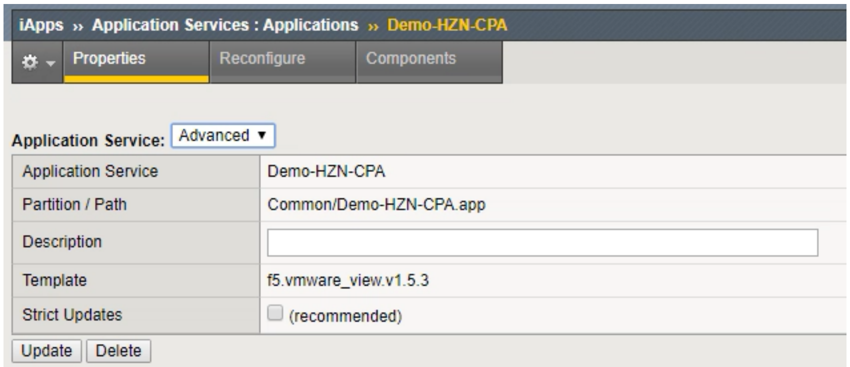


Hostname: ws1-bip-01.bd.f5.com
IP Address: 192.168.14.22
Date: Jan 31, 2018
Time: 11:04 AM (PST)
User: admin
Role: Administrator
Partition: Common

*Demo-HZN-CPA

☑	Name	Template	Template Validity	Partition / Path
□	Demo-HZN-CPA	f5.vmware_view.v1.5.3		Common/Demo-HZN-CPA.app

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



Application Service: Advanced

Application Service	Demo-HZN-CPA
Partition / Path	Common/Demo-HZN-CPA.app
Description	
Template	f5.vmware_view.v1.5.3
Strict Updates	□ (recommended)

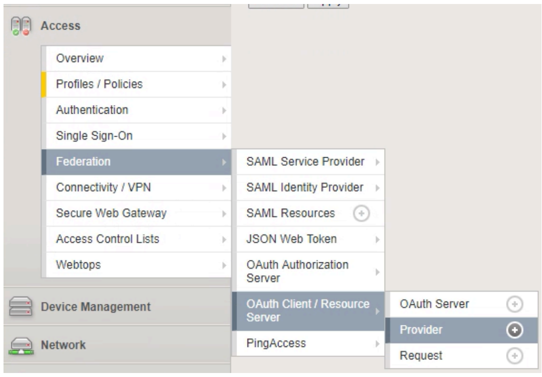
a. Change the pull-down menu from **Basic** to **Advanced**.

b. **Uncheck** the **Strict Updates** checkbox.

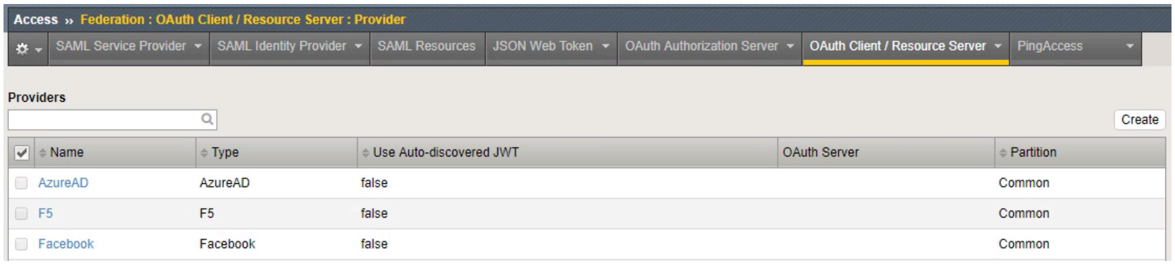
c. Click the **Update** button.

Create OAUTH Resources

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



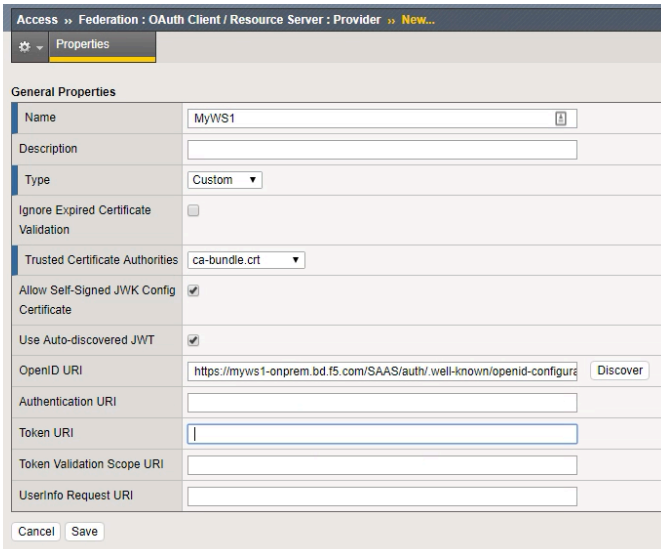
2. Click the Create Button


Access » Federation : OAuth Client / Resource Server : Provider
SAML Service Provider
SAML Identity Provider
SAML Resources
JSON Web Token
OAuth Authorization Server
OAuth Client / Resource Server
PingAccess
Create

Providers

☑	Name	Type	Use Auto-discovered JWT	OAuth Server	Partition
□	AzureAD	AzureAD	false		Common
□	F5	F5	false		Common
□	Facebook	Facebook	false		Common

3. In the OAuth Client / Resource Server Provider Menus


Access » Federation : OAuth Client / Resource Server : Provider » New...
Properties
Discover
Cancel
Save

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-configura
Authentication URI	
Token URI	
Token Validation Scope URI	
UserInfo Request URI	

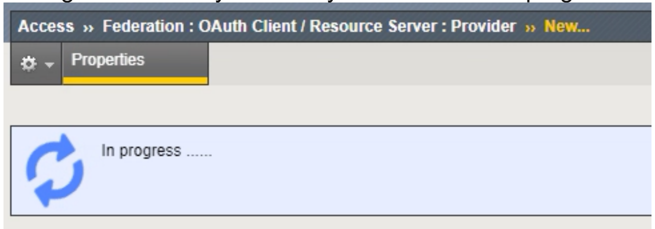
a. Enter a Unique Name

b. Change type to **Custom**

c. In the **OpenID URI** enter the following (**replacing <MyVIDMFQDN>** with your unique instance) *https://**<MyVIDMFQDN>**/SAAS/auth/.well-known/openid-configuration*

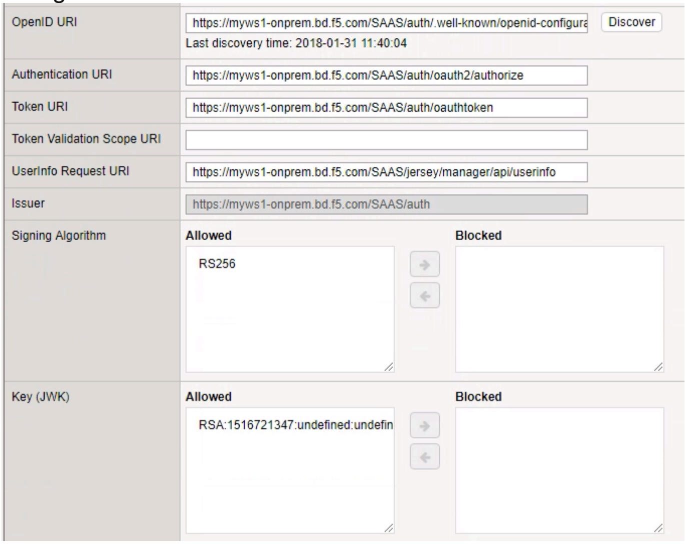
d. Click the Discover Button

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

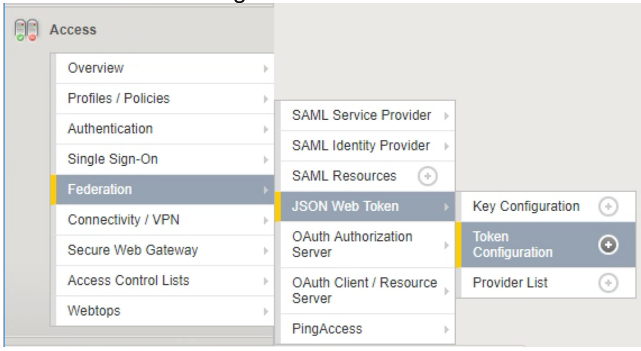
In progress ......

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 configuration.

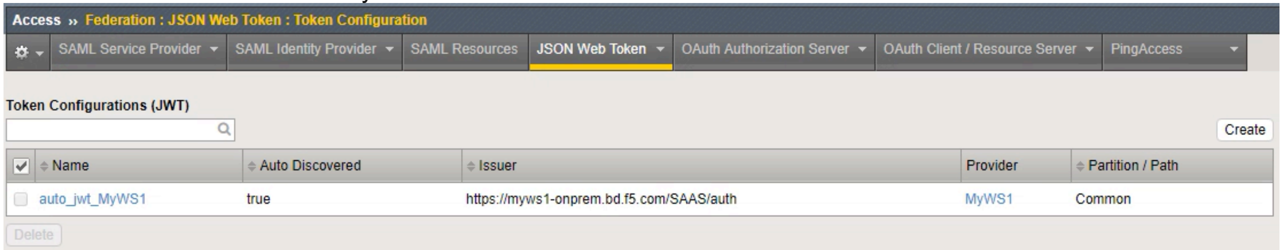


OpenID URI	https://myws1-onprem.bd.f5.com/SAAS/auth/.well-known/openid-configura Discover Last discovery time: 2018-01-31 11:40:04	
Authentication URI	https://myws1-onprem.bd.f5.com/SAAS/auth/oauth2/authorize	
Token URI	https://myws1-onprem.bd.f5.com/SAAS/auth/oauthtoken	
Token Validation Scope URI	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

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



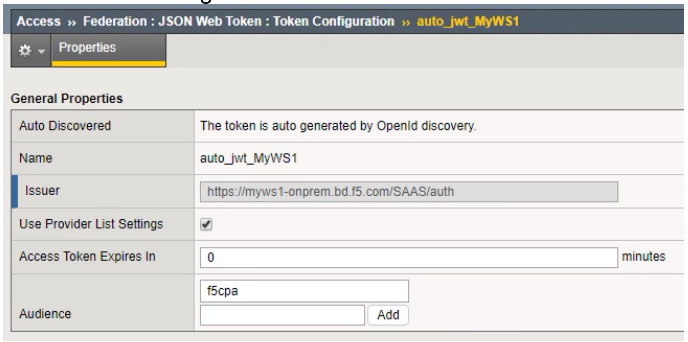
7. There should be an auto-created Token Configuration due to the discovery in the previous section, select the auto-created Token that contains your VIDM FQDN in the Issuer.


Access » Federation : JSON Web Token : Token Configuration
SAML Service Provider
SAML Identity Provider
SAML Resources
JSON Web Token
OAuth Authorization Server
OAuth Client / Resource Server
PingAccess
Create
Delete

Token Configurations (JWT)

☑	Name	Auto Discovered	Issuer	Provider	Partition / Path
□	auto_jwt_MyWS1	true	https://myws1-onprem.bd.f5.com/SAAS/auth	MyWS1	Common

8. In the Token Configuration


Access » Federation : JSON Web Token : Token Configuration » auto_jwt_MyWS1

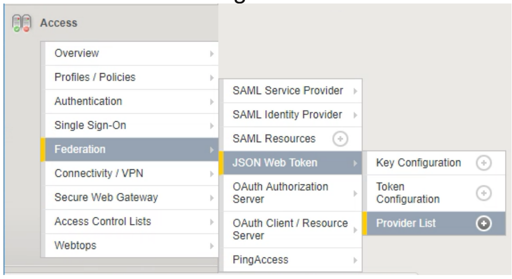
General Properties

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
Audience	f5cpa

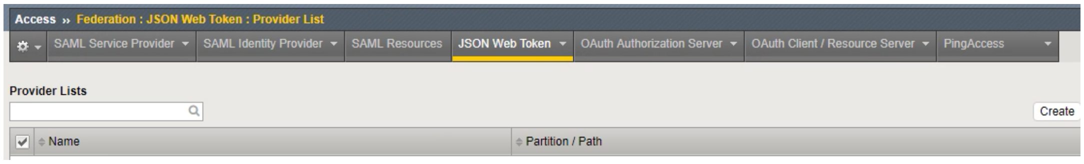
a. Type the name of your Audience (Created previously in the VIDM Configurations section) and Click the Add button.

b. Once the audience is added scroll to the bottom and click the save button.

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



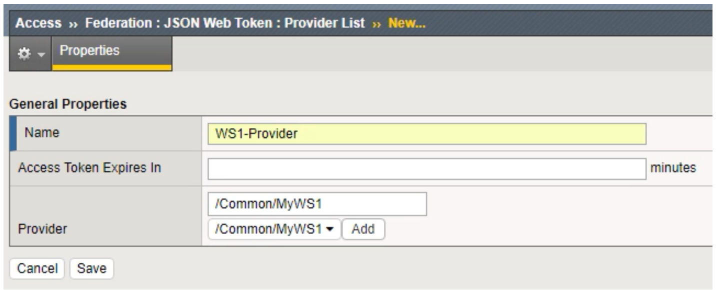
10. Click the Create Button


Access » Federation : JSON Web Token : Provider List

Provider Lists

☑	Name	Partition / Path

11. In the JSON Web Token Provider List


Access » Federation : JSON Web Token : Provider List » New...

General Properties

Name	WS1-Provider
Access Token Expires In	minutes
Provider	/Common/MyWS1 /Common/MyWS1

a. Enter a Unique Name

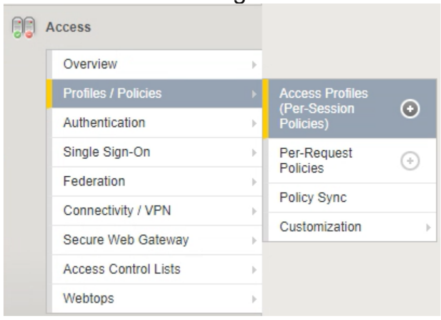
b. In the Provider pull down menus Select the OAUTH Client / Resource Server Provider previously created and click the Add button.

c. Click the Save button.

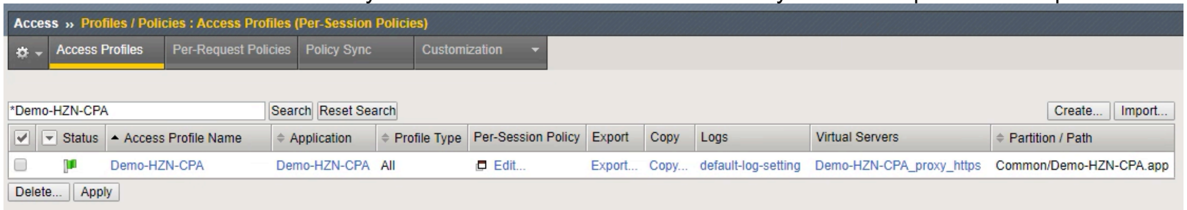
Once these Steps have been completed you can move forward to Modifying the Horizon APM Access Policy.

Modify Horizon Access Policy

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

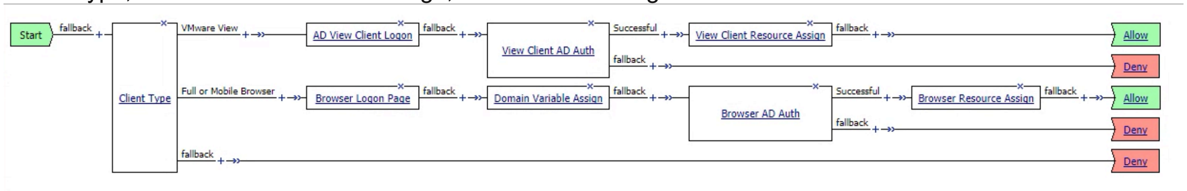


2. Click the Edit in Per-Session Policy under the Horizon APM Access Policy created as part of Prerequisites

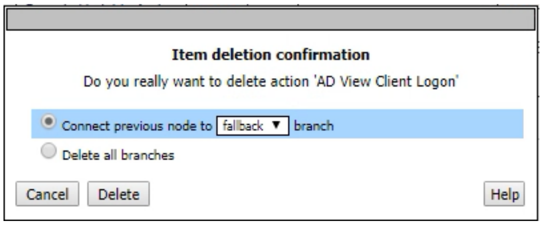


☑	Status	Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	Partition / Path
□		Demo-HZN-CPA	Demo-HZN-CPA	All	Edit...	Export...	Copy...	default-log-setting	Demo-HZN-CPA_proxy_https	Common/Demo-HZN-CPA.app

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.



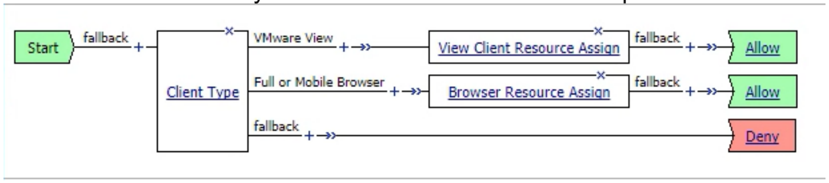
Item deletion confirmation

Do you really want to delete action 'AD View Client Logon'

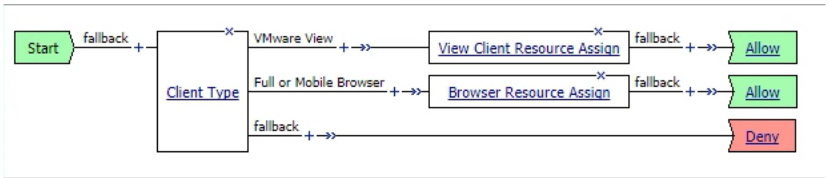
● Connect previous node to fallback ▼ branch

○ Delete all branches

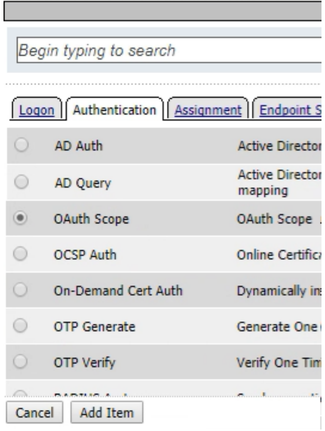
5. Once all of the objects except Client Type, View Client Resource Assign and Browser Resource Assign are deleted the Visual Policy Editor should look like the below picture.



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)



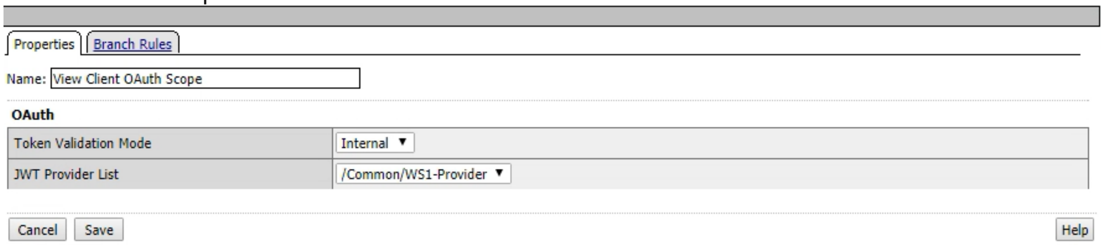
Begin typing to search

Logon | Authentication | Assignment | Endpoint S

○	AD Auth	Active Director
○	AD Query	Active Director mapping
●	OAuth Scope	OAuth Scope
○	OCSP Auth	Online Certifica
○	On-Demand Cert Auth	Dynamically in
○	OTP Generate	Generate One
○	OTP Verify	Verify One Tim

Cancel | Add Item

8. 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

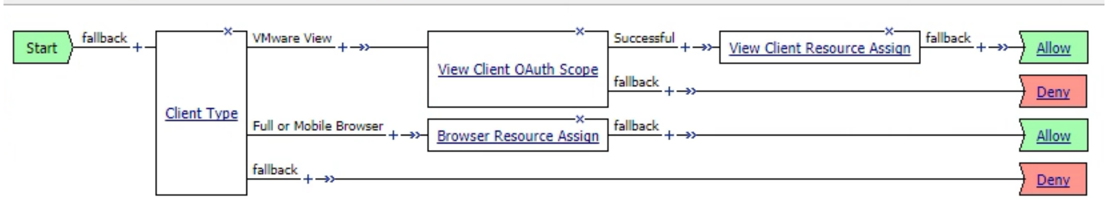
a. Provide a Unique Name (Since on the View Client Path we put View Client OAuth Scope)

b. Change the Token Validation Mode to Internal.

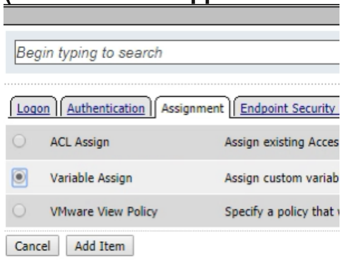
c. Select the JWT Provider previously created in F5 Configurations.

d. Click the Save Button.

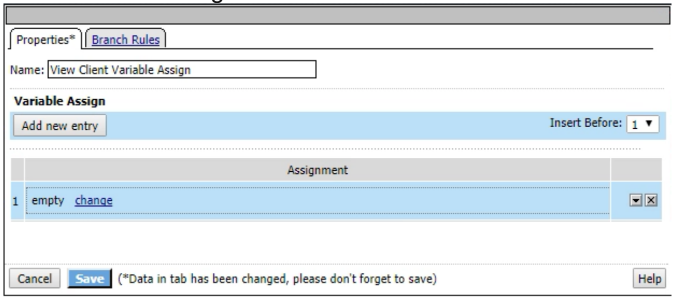
9. The Updated VPE should look like the below picture. Click on the + between View Client OAuth Scope and View Client Resource Assign in the Successful line to create an object between the two.



10. Select Variable Assign from the Assignment tab and click the Add Item button.
(Picture was cropped to take up less space)



11. In the Variable Assign



Name: View Client Variable Assign

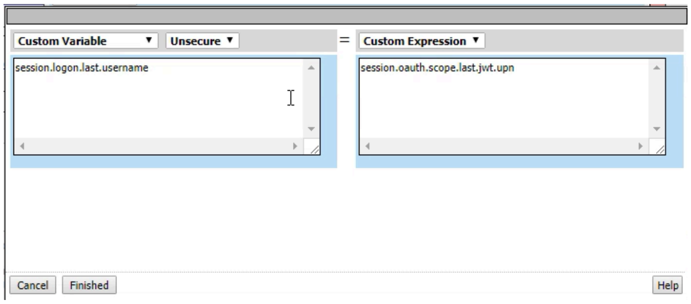
1 empty change

(*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



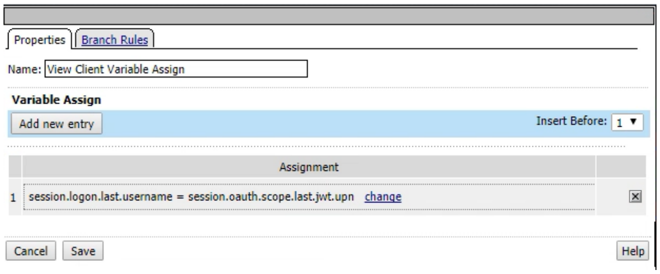
session.logon.last.username = session.oauth.scope.last.jwt.upn

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.

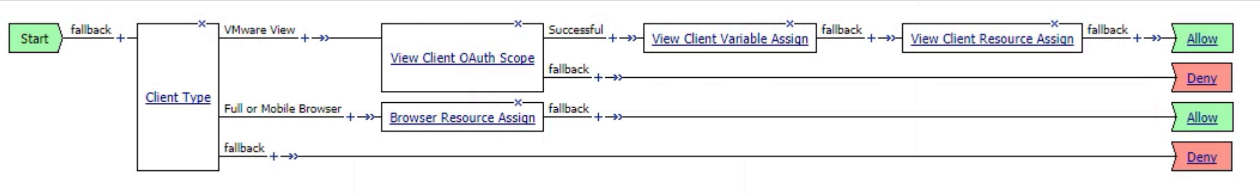
12. Click the Save button



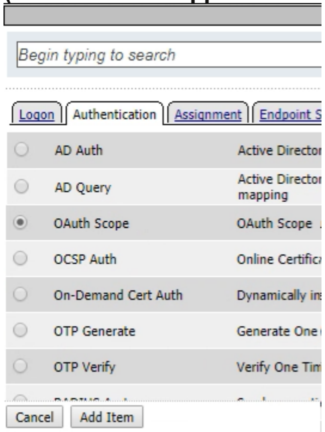
Name: View Client Variable Assign

1 session.logon.last.username = session.oauth.scope.last.jwt.upn change

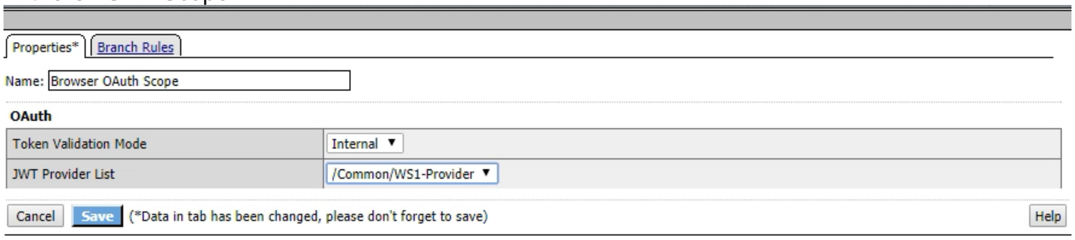
13. The Updated VPE should look like the below picture. Click on the + between Client Type on the Full or Mobile Browser line and Browser Resource Assign to create an object between the two.



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



Name: Browser OAuth Scope

OAuth

Token Validation Mode	Internal
JWT Provider List	/Common/WS1-Provider

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

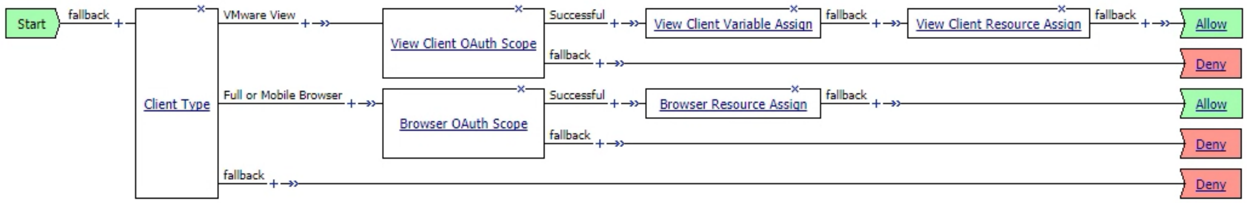
a. Provide a Unique Name (Since on the Browser Path we put Browser OAuth Scope)

b. Change the Token Validation Mode to Internal.

c. Select the JWT Provider previously created in F5 Configurations.

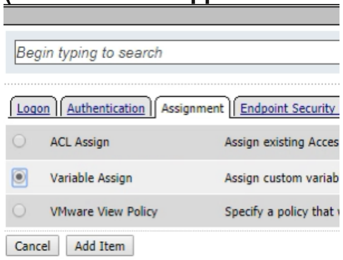
d. Click the Save Button.

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.

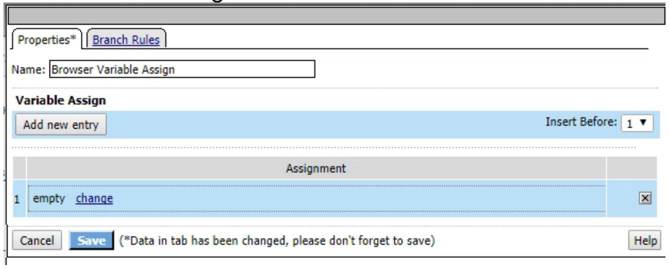


17. Select Variable Assign from the Assignment tab and click the Add Item button.

    (Picture was cropped to take up less space)



18. In the Variable Assign



Name: Browser Variable Assign

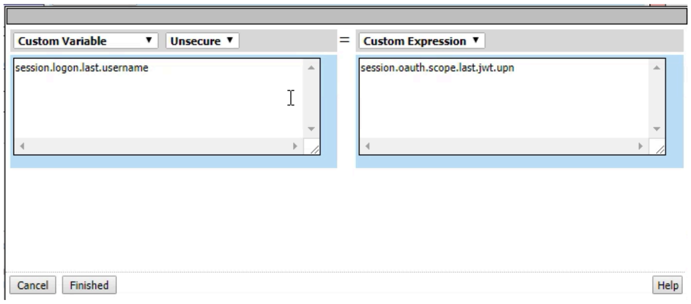
1 empty change

(*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



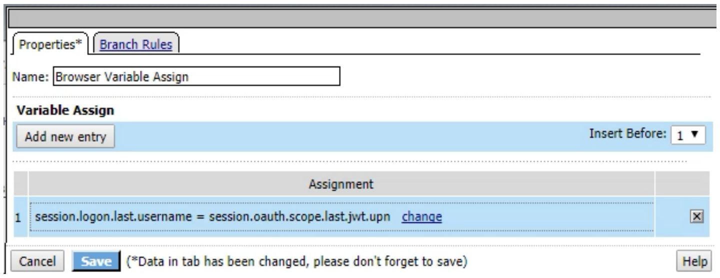
session.logon.last.username = session.oauth.scope.last.jwt.upn

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

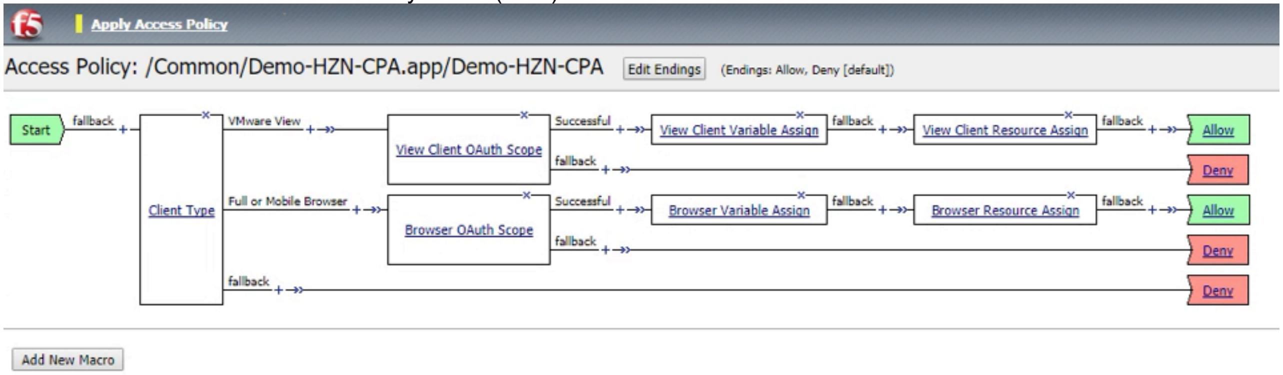


Name: Browser Variable Assign

1 session.logon.last.username = session.oauth.scope.last.jwt.upn change

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

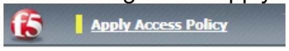
20. This is what the end state Visual Policy Editor (VPE) should look like.



Apply Access Policy

Access Policy: /Common/Demo-HZN-CPA.app/Demo-HZN-CPA Edit Endings (Endings: Allow, Deny [default])

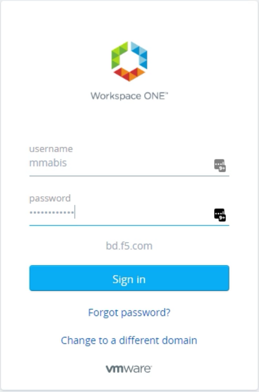
21. Once configuration is completed click on the “Apply Access Policy” link in the top left of the screen to save all of the changes and apply them.



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.

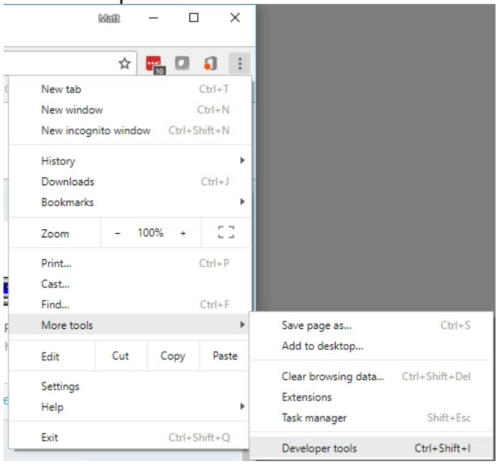
1. In VIDM/WS1 Portal login as a user with access to the horizon resources.



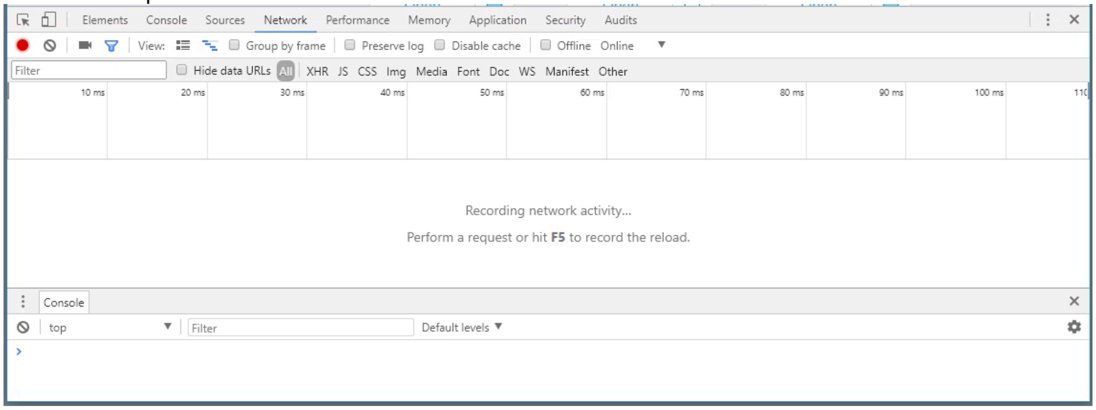
username
mmabis

password
••••••••••••

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.



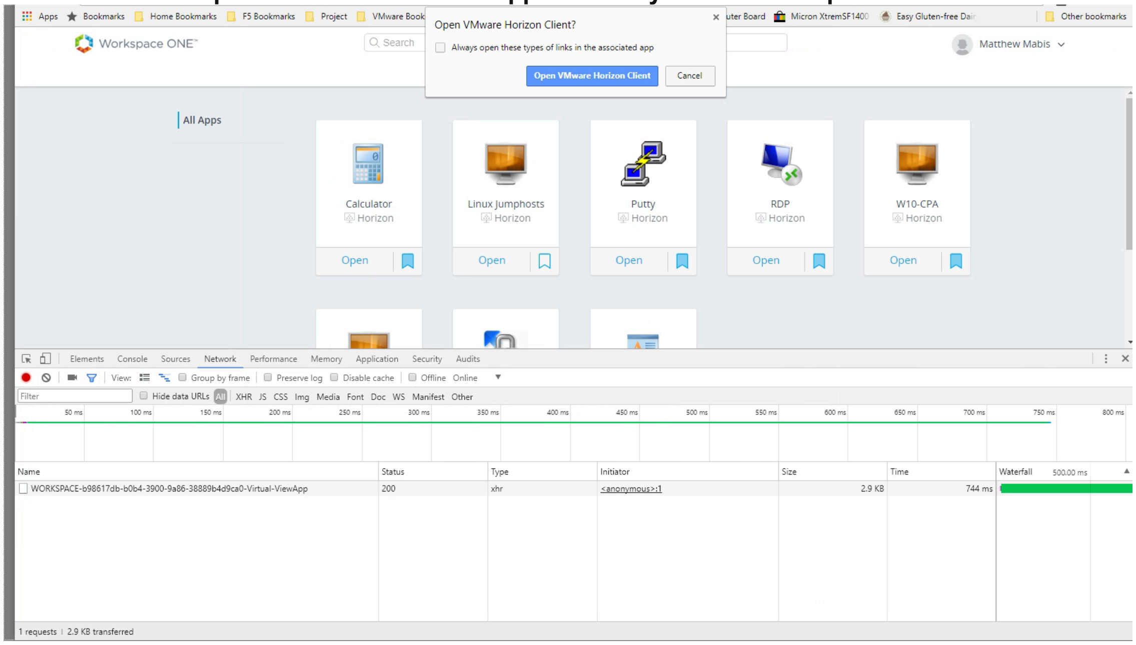
3. In the Developer Console select the "Network" tab



Recording network activity...

Perform a request or hit **F5** to record the reload.

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-****



Open VMware Horizon Client?

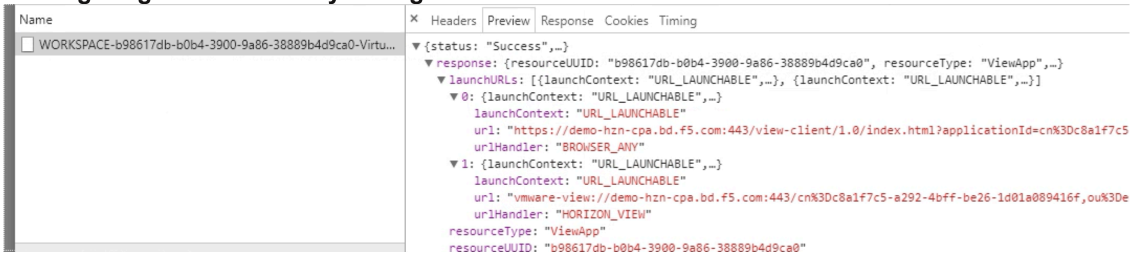
☐ Always open these types of links in the associated app

Open VMware Horizon Client | Cancel

Name	Status	Type	Initiator	Size	Time
WORKSPACE-b98617db-b0b4-3900-9a86-38889b4d9ca0-Virtual-ViewApp	200	xhr	<anonymous>:1	2.9 KB	744 ms

1 requests | 2.9 KB transferred

5. 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”



WORKSPACE-b98617db-b0b4-3900-9a86-38889b4d9ca0-Virtu...

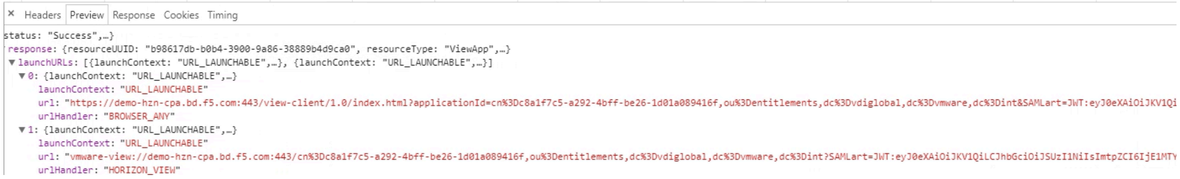
```
▼{status: "Success",…}
  ▼response: {resourceUUID: "b98617db-b0b4-3900-9a86-38889b4d9ca0", resourceType: "ViewApp",…}
    ▼launchURLs: [{launchContext: "URL_LAUNCHABLE",…}, {launchContext: "URL_LAUNCHABLE",…}]
      ▼0: {launchContext: "URL_LAUNCHABLE",…}
          launchContext: "URL_LAUNCHABLE"
          url: "https://demo-hzn-cpa.bd.f5.com:443/view-client/1.0/index.html?applicationId=cn%3Dc8a1f7c5
          urlHandler: "BROWSER_ANY"
      ▼1: {launchContext: "URL_LAUNCHABLE",…}
          launchContext: "URL_LAUNCHABLE"
          url: "vmware-view://demo-hzn-cpa.bd.f5.com:443/cn%3Dc8a1f7c5-a292-4bff-be26-1d01a089416f,ou%3De
          urlHandler: "HORIZON_VIEW"
    resourceType: "ViewApp"
    resourceUUID: "b98617db-b0b4-3900-9a86-38889b4d9ca0"
```

   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.

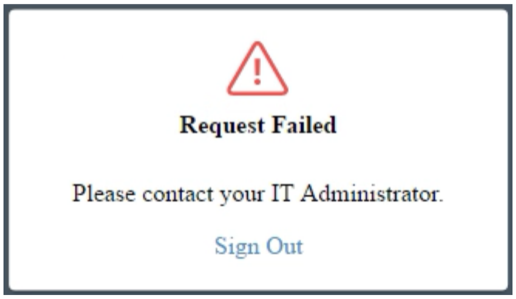
6. In the Launch URL Strings there will be a section called “SAMLart=” if the line looks like “SAMLart=JWT:” then VMware Identity Manger is wrapping the JWT token within the SAML artifact field for the F5 to Decrypt. If the “SAMLart=” field does not contain JWT: then the Horizon Environment that you are trying to access is not configured for JWT Wrapping as per previous section “Configuring VMware Identity Manager”



```
status: "Success",…}
response: {resourceUUID: "b98617db-b0b4-3900-9a86-38889b4d9ca0", resourceType: "ViewApp",…}
▼launchURLs: [{launchContext: "URL_LAUNCHABLE",…}, {launchContext: "URL_LAUNCHABLE",…}]
  ▼0: {launchContext: "URL_LAUNCHABLE",…}
      launchContext: "URL_LAUNCHABLE"
      url: "https://demo-hzn-cpa.bd.f5.com:443/view-client/1.0/index.html?applicationId=cn%3Dc8a1f7c5-a292-4bff-be26-1d01a089416f,ou%3Dentitlements,dc%3Dvdiglobal,dc%3Dvmware,dc%3Dint&SAMLart=JWT:eyJ0eXAiOiJKV1Qi
      urlHandler: "BROWSER_ANY"
  ▼1: {launchContext: "URL_LAUNCHABLE",…}
      launchContext: "URL_LAUNCHABLE"
      url: "vmware-view://demo-hzn-cpa.bd.f5.com:443/cn%3Dc8a1f7c5-a292-4bff-be26-1d01a089416f,ou%3Dentitlements,dc%3Dvdiglobal,dc%3Dvmware,dc%3Dint?SAMLart=JWT:eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjE1MTY
      urlHandler: "HORIZON_VIEW"
```

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.



Request Failed

Please contact your IT Administrator.