Agility 2018 Hands-on Lab Guide

Contents:

1	Class 1: SAML Federation with F5 5 1.1 Getting Started 5 5
	1.2Lab 1: SAML Service Provider (SP) Lab71.3Lab 2: SAML Identity Provider (IdP) Lab201.4Lab 3: Kerberos to SAML Lab441.5Lab 4: [Optional] SaaS Federation iApp Lab581.6Conclusion66
2	Class 2: OAuth Federation with F5 73 2.1 Lab Environment 73 2.2 Lab 1: Social Login Lab 74 2.3 Lab 2: API Protection 129 2.4 Lab 3: Reporting and Session Management 167 2.5 Lab 4: Troubleshooting 171 2.6 Conclusion 173
3	Class 3: SWG - Securing Outbound Internet Access1753.1Lab Environment1753.2Lab 1: SWG iApp – Explicit Proxy for HTTP and HTTPS1773.3Lab 2: URL Category-based Decryption Bypass1913.4Lab 3: Explicit Proxy Authentication – NTLM1933.5Lab 4: SWG Reporting with BIG-IQ1963.6Lab 5: SWG iApp - Transparent Proxy for HTTP and HTTPS1983.7Lab 6: Captive Portal Authentication2003.8Lab 7: SSL Visibility for DLP (ICAP)2023.9Conclusion203
4	Class 4: SAML Identity Provider (IdP) Lab2054.1Lab Topology & Environments2054.2BIG-IP Basics (optional)2074.3Module 1: SAML Identity Provider2094.4Module 2: Access Control227
5	Class 5: AD FS Proxy Lab2335.1Getting Started2335.2Module: Connect and Validate Environment234

	5.3 5.4 5.5 5.6	Module: Deploy ADFS Load Balancing Services 23 Module: Deploy ADFS Proxy Services 24 Module: Additional Information and Troubleshooting Tips 24 Conclusion 24	40 46
6	Clas 6.1 6.2 6.3 6.4 6.5 6.6 6.7	s 6: Federating Common Services24Welcome24Lab 1: SAML Service Provider (SP) Lab24Lab 2: IDaaS SAML Identity Provider (iDP) Lab (OKTA)25Lab 3: oAuth and OpenID Connect Lab (Google)27Lab 4: oAuth and AzureAD Lab28Conclusion30Appendix30	49 58 73 88 07
7	Clas 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8	s 7: Introduction to Universal Access31Lab Information31Lab 1 - Deploy a simple reverse proxy service31Lab 2 - Create My First Policy32Lab 3 - Configuring a VPN Policy32Lab 4 - Configuring an APM Webtop33Lab 5 - FORMS Based Authentication33Lab 6 - BASIC Authentication34Lab 7 - Single-Sign-On Across Authentication Domains34	15 19 27 30 33 41
8	Clas 8.1 8.2 8.3 8.4 8.5 8.6 8.7 8.8	s 8: Troubleshooting Universal Access35Getting Started	54 56 69 72 85 11
9	Clas 9.1 9.2 9.3 9.4 9.5 9.6 9.7	s 9: Multi-Factor Auth for Cloud Applications43Getting Started43Pre-Work Activities43Lab 1: Create a basic APM Policy44Lab 2: Setup an AWS Connector44Lab 3: Setup a Salesforce Connector44Lab 4: Set up Google Authenticator (GA)44Lab 5: Set up DUO44	38 48 56 69 81
10	10.1 10.2	s 10: Privileged User Access49Lab Network Setup49Lab 1: WebSSH and APM49Validation49	96

Class 1: SAML Federation with F5

1.1 Getting Started

1.1.1 Lab Network Setup

In the interest of focusing as much time as possible configuring and performing lab tasks, we have provided some resources and basic setup ahead of time. These are:

- · Cloud-based lab environment complete with Jump Host, Virtual BIG-IP and Lab Server
- Duplicate Lab environments for each student for improved collaboration
- The Virtual BIG-IP has been pre-licensed and provisioned with Access Policy Manager (APM)
- Pre-staged configurations to speed up lab time, reducing repetitive tasks to focus on key learning elements.

If you wish to replicate these labs in your environment you will need to perform these steps accordingly. Additional lab resources are provided as illustrated in the diagram below:

C	Lab AGILITY 2017 330 SAML Federation with F5 Lab Environment										
Stude Lapo	ent pp		onment	-(Jump H	app.partne 10.1.10.20 idp.partne 10.1.10.21 External 10.1.10.2/24 10.1.1 10.1.1.10.2/24 10.1.1	0/24 r.com 0/24	S/ BIG-IP	AML SP Partner AML iDP Partner Internal	er	Server
			BIG-IP (ve)	Q		ab Server.		🕑 SA	ML Partners	Alloc	ated VLANs
OS	Windows 7 (64bit)	TMOS	12.1		OS	Windows 2012		SP	SAML SP Partner app.partner.com	TMOS	IP Subnet
Internal	10.1.20.2/24	Internal	10.1.20.245/24 (Self)		Internal	10.1.20.254/24			10.1.10.200/24	Internal	10.1.20.0/24
External	10.1.10.2/24	External	10.1.10.245/24 (Self)		Services	Active Directory		iDP	SAML iDP Partner idp.partner.com	External	10.1.10.0/24
Mgmt.	10.1.1.2/24	Mgmt.	10.1.1.245/24			IIS			10.1.10.210/24	Mgmt.	10.1.1.0/24

1.1.2 Timing for labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. This can never be accurately predicted but we strived to provide an estimate based on several people, each having a different level of experience. Below is an estimate of how long it will take for each lab:

Lab Description	Time Allocated
LAB I (SAML Service Provider (SP))	25 minutes
LAB II (SAML Identity Provider (IDP))	25 minutes
LAB III (Kerberos to SAML)	25 minutes
LAB IV (SAAS Federation IAPP)	25 minutes

1.1.3 Authentication – Credentials

The following credentials will be utilized throughout this Lab guide.

Credential Use	User ID	Password
BIG-IP Configuration Utility (GUI)	admin	admin
BIG-IP CLI Access (SSH)	root	default
Jump Host Access	f5demo\user	Agility1
All User authentication for Labs/Tasks	user	Agility1

1.1.4 Utilized Browsers

The preferred browsers for this lab are Firefox and Internet Explorer. Shortcut links have been provided to speed access to targeted resources and assist you in your tasks. Except where noted, either browser can be used for all lab tasks.

1.1.5 General Notes

As noted previously, environment staging has been done to speed up lab time, reducing repetitive tasks to focus on key learning elements. Where possible steps that have been optimized have been called out with links and references provided in the *Additional Information* section for additional clarification. The intention being that the lab guide truly serves as a resource guide for all your future federation deployments.

1.2 Lab 1: SAML Service Provider (SP) Lab

The purpose of this lab is to configure and test a SAML Service Provider. Students will configure the various aspects of a SAML Service Provider, import and bind to a SAML Identity Provider and test SP?Initiated SAML Federation.

Objective:

- · Gain an understanding of SAML Service Provider(SP) configurations and its component parts
- · Gain an understanding of the access flow for SP-Initiated SAML

Lab Requirements:

• All Lab requirements will be noted in *f* the tasks that follow

Estimated completion time: 25 minutes

1.2.1 TASK 1 ? Configure the SAML Service Provider (SP)

SP Service

- 1. Begin by selecting: Access -> Federation -> SAML Service Provider -> Local SP Services
- 2. Click the **Create** button (far right)

Acces	Access » Federation : SAML Service Provider : Local SP Services							
* -	SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Server 👻			PingAccess •	
Local SP Services						Create		
	External IdP Connectors		SAML IdP C	ennedere		Description	Partition	
	Connector Automation		SAME IOP CO	onnectors		Description	Paruuon	
	Authentication Context Class	es						

3. In the **Create New SAML SP Service** dialog box click **General Settings** in the left navigation pane and key in the following as shown:

Name:	app.f5demo.com
Entity ID:	https://app.f5demo.com

4. Click **OK** on the dialogue box

Create New SAML SP	Service	
General Settings Carlot Settings Security Settings Authentication Context Advanced Settings	Name*: app.f5demo.com Entity ID*: https://app.f5demo.com SP Name Settings Scheme : Host : https Description : Relay State :	
	OK Cancel	

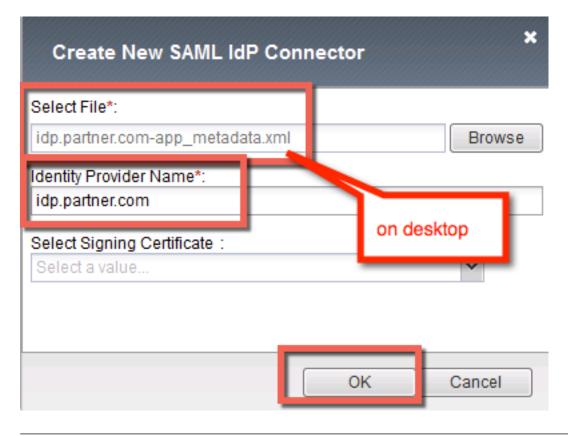
Note: The yellow box on Host will disappear when the Entity ID is entered.

IdP Connector

- Click on Access ?> Federation ?> SAML Service Provider ?> External IdP Connectors or click on the SAML Service Provider tab in the horizontal navigation menu and select External IdP Connectors
- 2. Click specifically on the Down Arrow next to the Create button (far right)
- 3. Select From Metadata from the drop down menu

1	Acces	s » Federation : SAML Service	e Provider : External Id	P Connectors								
	* -	SAML Service Provider 👻 SA	ML Identity Provider 👻	SAML Resources	OAuth Authorization Server 👻		e Server 👻 PingAccess	•				
	Usett	Local SP Services	connectors. When	you use this BIG-IP s	ystem as a SAML service provid	er, it sends authenticatio	n requests to the IdP and in turr	receives assertions from	m the IdP. You can create, edit and de	ete IdP conn	ections by	
	clicki	External IdP Connectors										
	1	Connector Automation									Create	h
		Authentication Context Classe	9S		- 4							Н,
		Vallio A		SAML SP Se	rvices	Desc	ription		Partition	Cust	om	al.
										From	n Metadata	I
										From	Template a	л

- 4. In the Create New SAML IdP Connector dialogue box, click Browse and select the idp.partner.com?app_metadata.xml file from the Desktop of your jump host.
- 5. In the Identity Provider Name field enter idp.partner.com:
- 6. Click **OK** on the dialog box



Note: The idp.partner.com-app_metadata.xml was created previously. Oftentimes, IdP providers will have a metadata file representing their IdP service. This can be imported to save object creation time as it has been done in this lab

- 7. Click on the Local SP Services from the SAML Service Providers tab in the horizontal navigation menu
- 8. Click the checkbox next to the previously created *app.f5demo.com* and click **Bind/Unbind IdP Con**nectors at the bottom of the GUI

Acces	Access » Federation : SAML Service Provider : Local SP Services						
* -	SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Server 👻	OAuth Client / Res		
	Local SP Services						
	External IdP Connectors						
	Connector Automation						
	Authentication Context Classes						
	Name 🔺		SAML IdP C	onnectors	[
	app.f5demo.com						
	Edit Delete	Bind/Unbind IdP Connect	tors Export Meta	idata			

9. In the Edit SAML IdP's that use this SP dialogue box, click the Add New Row button

10. In the added row, click the Down Arrow under SAML IdP Connectors and select the /Com-

mon/idp.partner/com SAML IdP Connector previously created

11. Click the **Update** button and the **OK** button at the bottom of the dialog box

Edit SAML IdP's that use this SP	×
IdP Connectors associated with this SP Service	
	Add New Row Create New IdP Connector 👻
SAML IdP Connectors Matching Source	Matching Value
/Common/idp.partner.c 👻	×
Update	Cancel
Edit Delete	
	OK Cancel

12. Under the Access ?> Federation ?> SAML Service Provider ?> Local SP Services menu you should now see the following (as shown):

Name:	app.f5demo.com
SAML IdP Connectors:	idp.partner.com

Access » Federation : SAML Service Provider : Local SP Services							
⇔ ÷	SAML Service Provider 👻	SAML Identity Provider 👻	SAML	Resources	OAuth Aut		
	✓ Name ▲ SAML IdP Connectors						
	☑ app.f5demo.com idp.partner.com						

1.2.2 TASK 2 ? Configure the SAML SP Access Policy

- 1. Begin by selecting Access ?> Profiles/Policies ?> Access Profiles (Per?Session Policies)
- 2. Click the Create button (far right)

Access » Profiles / Policies : Access Profiles (Per-Session Policies)								
Access Profiles Per-Request Policies Policy Sync Customization -								
* Search	* Search Create. In					reate Import		
Status Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
access		All	(none)	(none)	(none)			Common

3. In the New Profile window, key in the following:

Name:	app.f5demo.com?policy
Profile Type:	All (from drop down)
Profile Scope:	Profile (default)

- 4. Scroll to the bottom of the New Profile window to the Language Settings
- 5. Select *English* from the **Factory Built?in Languages** on the right, and click the **Double Arrow (<<)**, then click the **Finished** button.

Access » Profile	es / Policies : A	ccess Profiles	(Per-Session Policies) » New Profile.				
General Propertie	s						
Name		app.f5demo	app.f5demo.com-policy				
Parent Profile		access	access				
Profile Type		All	All				
Profile Scope	Profile Scope		<u>~</u>				
Language Settings							
Additional Languages	Afar (aa)	~ Add					
Languages	Acc English (en)	epted Languages	Factory BuiltIn Languages Japanese (ja) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-lw) Korean (ko) Spanish (es) French (fr) German (de)				
Default Language	English (en) 🖂						
Cancel Finished							

6. From the Access ?> Profiles/Policies ?> Access Profiles (Per?Session Policies) screen, click the Edit link on the previously created app.f5demo.com?policy line

Acce	Access » Profiles / Policies : Access Profiles (Per-Session Policies)								
☆ -	Access F	Profiles	Per-Request Policies	Policy Sync	Customization	*			
*			Searc	:h					
•	 Status 	Access	Profile Name				Application	Profile Type	Per-Session Policy
]#	access						All	(none)
	P	app.f5der	mo.com-policy					All	🗗 Edit

7. In the Visual Policy Editor window for /Common/app.f5demo.com?policy, click the Plus (+) Sign between Start and Deny

Access Policy: /Common/app.f5demo.com-policy	Edit Endings
Start	
Add New Macro	

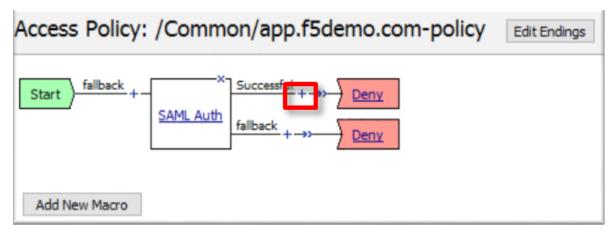
- 8. In the pop?up dialog box, select the **Authentication** tab and then click the **Radio Button** next to **SAML Auth**
- 9. Once selected, click the Add Item button

Logo	Authentication Assign	ment] [Endpoint Security (Server-Side)] [Endpoint Security (Client-Side)] [General Purpose]	-
0	AD Auth	Active Directory authentication of end user credentials	
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping	
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
0	HTTP Auth	HTTP authentication of end user credentials	
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
0	LDAP Auth	LDAP authentication of end user credentials	
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping	,
0	LocalDB Auth	Local Database Authentication	
0	NTLM Auth Result	NTLM authentication of end user credentials	
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication	
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	
0	OTP Generate	Generate One Time Passcode (OTP)	
0	OTP Verify	Verify One Time Passcode (OTP)	
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off	
0	RADIUS Auth	RADIUS authentication of end user credentials	
0	RSA SecurID	RSA SecurID two-factor authentication of end user credentials	
0	SAML Auth	SAML Auth using SAML Service Provider Interface	
0	TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off	
<u> </u>	cel Add Item	TACACC: A. M	He

- 10. In the SAML Auth configuration window, select /Common/app.f5demo.com from the AAA Server drop down menu
- 11. Click the **Save** button at the bottom of the window

Properties* [Branch Rules]				
Name: SAML Auth				
SAML Authentication SP				
AAA Server	/Common/app.f5demo.com 💌			

12. In the Visual Policy Editor window for /Common/app.f5demo.com?policy, click the Plus (+) Sign on the Successful branch following SAML Auth



- 13. In the pop-up dialog box, select the **Assignment** tab, and then click the **Radio Button** next to **Variable Assign**
- 14. Once selected, click the Add Item buton

Logor	Authentication Assignmen	ndpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
0	ACL Assign	Assign existing Access Control Lists (ACLs)
0	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership
0	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs
0	BWC Policy	Assign Bandwidth Controller policies
0	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop
0	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP
0	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership
0	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections
0	Pool Assign	Assign a Local Traffic Pool
0	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway
0	Resource Assign	Assign Connectivity Resources
0	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings
0	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables
0	Variable Assign	Assign custom variables, configuration variables, or predefined session variables
0	VMware View Policy	Specify a policy that will apply to VMware View connections
Cano	Add Item	

15. In the Variable Assign configuration window, click the Add New Entry button

- 16. Under the new Assignment row, click the Change link
- 17. In the pop?up window, configure the following:

Left Pane	
Variable Type:	Custom Variable
Security:	Unsecure
Value:	session.logon.last.username

Right Pane	
Variable Type:	Session Variable
Session Variable:	<pre>session.saml.last.attr.name.emailaddress</pre>

- 18. Click the Finished button at the bottom of the configuration window
- 19. Click the Save button at the bottom of the Variable Assign dialog window

V Properties* Branch Rules	
Name: Variable Assign	
ack + Haninkiniana	
Add new entry	Insert Before:
Assignm	ent
1 empty change	X
Custom Variable	Session Variable
session.logon.last.username	Session Variab last.attr.name.emailaddress
-	
<	testing and an effect data as
session.sami.las	t.attr.name.emailaddress
Cancel Finished	Help

20. In the Visual Policy Editor select the Deny ending along the fallback branch following the Variable Assign

Access Policy: /Common/app.f5demo.com-policy Edit Endings				
Start fallback +				
Add New Macro				

21. From the Select Ending dialog box, select the Allow button and then click Save

Select End	ing:		
Allow E			
O Deny [
Cancel	Save		Help

22. In the Visual Policy Editor click Apply Access Policy (top left) and close the Visual Policy Editor

6	Apply Access Policy
Acces	s Policy: /Common/app.f5demo.com-policy Edit Endings
Start) fallback + - Successful + → <u>Variable Assign</u> fallback + → <u>Allow</u> SAML Auth fallback + → <u>Deny</u>
Add N	lew Macro

1.2.3 TASK 3 ? Create the SP Virtual Server & Apply the SP Access Policy

- 1. Begin by selecting Local Traffic -> Virtual Servers
- 2. Click the Create button (far right)

🔅 🚽 Virtual Server List 🛛 /irtual Address Li	ist Stat	istics 👻						
	Search	Reset Search						Create
Status A Name		• Description	Application	• Destination	Service Port	• Туре	Resources	Partition / Path
No records to display.								

3. In the New Virtual Server window, key in the following as shown:

General Properties	
Name:	app.f5demo.com
Destination Address/Mask:	10.1.10.100
Service Port:	443

Configuration	
HTTP Profile:	http (drop down)
SSL Profile (Client)	app.f5demo.com?clientssl

Access Policy	
Access Profile:	app.f5demo.com?policy

Resources		
iRules:	application?irule	

4. Scroll to the bottom of the configuration window and click Finished

Local Traffic » Virtual Servers	Virtual Server List » New Virtual Server	***
General Properties		
Name	app.f5demo.com	
Description		
Туре	Standard	
Source Address		
Destination Address/Mask	10.1.10.100	
Service Port	443 HTTPS 🔽	
Notify Status to Virtual Address		
State	Enabled 🗸	
Configuration: Basic 🗸		
Protocol	TCP	
Protocol Profile (Client)	tcp 🗸	
Protocol Profile (Server)	(Use Client Profile)	
HTTP Profile	http 🗸	
FTP Profile	None 🗸	
RTSP Profile	None 🗸	
SSH Proxy Profile	None	
	Selected	Available
SSL Profile (Client)	/Common app.f5demo.com-clientss <	clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl wom-default-clientssl

Access Policy	
Access Profile	app.f5demo.com-policy
Connectivity Profile +	None 🗸
Per-Request Policy	None 🗸
VDI Profile	None
Application Tunnels (Java & Per-App VPN)	Enabled
OAM Support	Enabled

Resources			
Г	Enabled	Available sýs_auth_ssl_cc_ldap	•
iRules	application-irule <<	_sys_auth_ssl_crldp _sys_auth_ssl_ocsp _sys_auth_tacacs _sys_https_redirect	-
	Up Down		
	Enabled	Available	
Policies	<		
		~	
Default Pool +	None 💌		
Default Persistence Profile	None		
Fallback Persistence Profile	None 💌		
Cancel Repeat Finished			

Note: The iRule is being added in order to simulate an application server to validate successful access.

1.2.4 TASK 4 ? Test the SAML SP

1. Using your browser from the jump host, navigate to the SAML SP you just configured at https://app.f5demo.com (or click the provided bookmark)

https://app.f5demo.com/ × +	
(i) iii https://app.f5demo.com	
🚯 Big-IP 📃 idp.f5demo.con 📃 app.f5dem	o.com 🗉 idp.partner.com 🗏 app.partner.com 🗏 saas.f5demo.com

- 2. Did you successfuly redirect to the IdP?
- 3. Log in to the IdP. Were you successfully authenticated?

Note: Use the credentials provided in the Authentication section at the beginning of this guide (user/Agility1)

- 4. After successful authentication, were you returned to the SAML SP?
- 5. Were you successfully authenticated to the app in the SAML SP?
- 6. Review your Active Sessions (Access ?> Overview ?> Active Sessions)
- 7. Review your Access Report Logs (Access ?> Overview ?> Access Reports)

1.3 Lab 2: SAML Identity Provider (IdP) Lab

The purpose of this lab is to configure and test a SAML Identity Provider. Students will configure the various aspect of a SAML Identity Provider, import and bind to a SAML Service Provider and test IdP-Initiated SAML Federation.

Objective:

- · Gain an understanding of SAML Identity Provider(IdP) configurations and its component parts
- · Gain an understanding of the access flow for IdP-Initiated SAML

Lab Requirements:

• All Lab requirements will be noted in the tasks that follow

Estimated completion time: 25 minutes

1.3.1 TASK 1 ? Configure the SAML Identity Provider (IdP)

IdP Service

- 1. Begin by selecting: Access ?> Federation ?> SAML Identity Provider ?> Local IdP Services
- 2. Click the Create button (far right)

Access >> Federation : SAML Identity Provider : Local IdP Services									
🔅 👻 SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Ser	ver 👻 🤇	OAuth Client / Resource		PingAccess	•	
Local IdP Services									
	External SP Connectors								Create
Name 🔺 SAML SP Cor	Artifact Resolution Services	s Portal Acc	cess Resources	Log	Description	Partition			
				-		-			

3. In the **Create New SAML IdP Service** dialog box, click **General Settngs** in the left navigation pane and key in the following:

IdP Service Name:	idp.f5demo.com?app
IdP Entity ID:	https://idp.f5demo.com/app

Create New IdP Servi	ce	×
General Settings SAML Profiles Findpoint Settings SASertion Settings SAML Attributes Security Settings	IdP Service Name*: idp.f5demo.com-app IdP Entity ID*: https://idp.f5demo.com/app IdP Name Settings Scheme : Host : https Description : Log Setting : From Access Profile Create	
	OK Cance	

Note: The yellow box on "Host" will disappear when the Entity ID is entered

4. In the **Create New SAML IdP Service** dialog box, click **Assertion Settings** in the left navigation pane and key in the following:

Assertion Subject Type:	Persistent Identifier (drop down)
Assertion Subject Value:	<pre>%{session.logon.last.username} (drop down)</pre>

Create New IdP Servi	ce X
General Settings SAML Profiles Endpoint Settings	Assertion Subject Type : Persistent Identifier
SAML Attributes	Assertion Subject Value*: %{session.logon.last.username}
	Authentication Context Class Reference : urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
	Assertion Validity (in seconds) : 600
	Encryption Strength : AES128
	OK Cancel

- 5. In the Create New SAML IdP Service dialog box, click SAML Attributes in the left navigation pane and click the Add button as shown
- 6. In the Name field in the resulting pop-up window, enter the following: emailaddress
- 7. Under Attribute Values, click the Add button
- 8. In the Values line, enter the following: %{session.ad.last.attr.mail}
- 9. Click the Update button
- 10. Click the **OK** button

Create New IdP Servi	ice	×
General Settings SAML Profiles Proposition Settings	SAML Attributes	Add
SAML Attributes	Name - Value(s)	Encrypt Type
	Edit	
		OK Cancel

Create Ne	w SAML Attribute
Name*:	
Name*: emailaddress	
Attribute Value(s	5)

	Add
Value(s)	
%{session.ad.last.attr.mail}	
Update Cancel	
Edit Delete	
Encrypt	
Type: AES128 ~	
ОК	Cancel

11. In the **Create New SAML IdP Service** dialog box, click **Security Settings** in the left navigation pane and key in the following:

Signing Key:	/Common/SAML.key (drop down)
Signing Certificate:	/Common/SAML.crt (drop down)

Note: The certificate and key were previously imported

12. Click **OK** to complete the creation of the IdP service

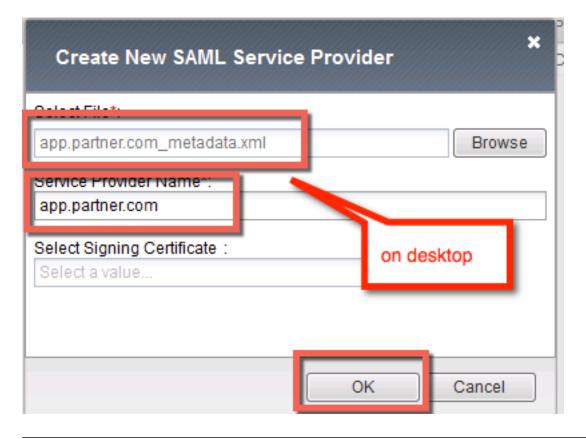
Create New IdP Serv	ice			×
General Settings SAML Profiles Endpoint Settings	Signing Key : /Common/SAML.key	~		
SAML Attributes	Signing Certificate: /Common/SAML.crt	Y		
]		OK	Cancel

SP Connector

- 1. Click on **External SP Connectors** (under the **SAML Identity Provider** tab) in the horizontal navigation menu
- 2. Click specifically on the Down Arrow next to the Create button (far right)
- 3. Select From Metadata from the drop down menu

Access » Federation : SAML Ide	entity Provider : External SP Con	aectors				
🔅 🗸 SAML Service Provider 👻	SAML Identity Provider 👻 SAM	IL Resources OAuth Authorization Server -		PingAccess -		
This application is used to manag Users can create, edit and delete		alG-IP (this device), in its role as a SAML Identi respective buttons.	ity Provider, receives an authentication	n request from a service a	and in turn authenticates the user and sends an as	sertion back to the service.
Users can create, euit and delete	External SP Connectors	respective buttons.				
	Artifact Resolution Services					Create
🗐 Name 🔺		SAML IdP Services	Description		Partition	Custom
saml_office365			Predefined SP co	nnector object for Office 3	65 Common	From Metadata
						From Template

- 4. In the **Create New SAML Service Provider** dialogue box, click **Browse** and select the *app.partner.com_metadata.xml* file from the Desktop of your jump host
- 5. In the Service Provider Name field, enter the following: app.partner.com
- 6. Click **OK** on the dialog box



Note: The app.partner.com_metadata.xml file was created previously. Oftentimes SP providers will have a metadata file representing their SP service. This can be imported to save object creation time as has been done in this lab.

- 7. Click on Local IdP Services (under the SAML Identity Provider tab) in the horizontal navigation menu
- 8. Select the Checkbox next to the previously created idp.f5demo.com and click the Bind/Unbind SP Connectors button at the bottom of the GUI

Access » Federation : SAML Identity Provider : Local IdP Services								
\$ -	SAML Service Provider 🔻	SAML Identity Provider 👻	SAML	Resources	OAuth Authorizatio	n Server 👻	OAuth Client / Res	
		Local IdP Services						
	-	External SP Connectors						
		Artifact Resolution Services						
	lame 🔺	SAML SP Connectors		Access Profile	s	Portal Access	Resources	
V io	dp.f5demo.com-app							
	Edit Delete	Bind/Unbind IdP Connect	tors	Export Meta	data			

9. In the Edit SAML SP's that use this IdP dialog, select the /Common/app.partner.com SAML SP Connection Name created previously

10. Click the **OK** button at the bottom of the dialog box

Edit SAML SP's that use this I	dP		*
SP Connectors associated with this IdP	Service		
		Create S	P Connector 👻
SAML SP Connection Name			
/Common/app.partner.com			
Common/saml_office365			
		_	
		ок	Cancel

11. Under the Access ?> Federation ?> SAML Identity Provider ?> Local IdP Services menu you should now see the following (as shown):

Name:	idp.f5demo.com-app
SAML SP Connectors:	app.partner.com

Access » Federation : SAML Identity Provider : Local IdP Services							
₩ -	SAML Service Provider 👻	SAML	Identity Provider 👻	SAML Resource			
	Name 🔺		SAML SP Connecto	rs			
	idp.f5demo.com-app		app.partner.com				

1.3.2 TASK 2 ? Create SAML Resource, Webtop, and SAML IdP Access Policy

SAML Resource

- 1. Begin by selecting Access ?> Federation ?> SAML Resources
- 2. Click the Create button (far right)
- 3. In the New SAML Resource window, enter the following values:

Name:	partner?app
SSO Configuration:	idp.f5demo.com?app
Caption:	Partner App

4. Click **Finished** at the bottom of the configuration window

Access » Federation : SAML Re	sources					
🔅 🗸 SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Server \prec	OAuth Client / Resource Server 👻	PingAccess	•
)			_
					Crea	te
🖌 🕈 Name 💠 SSO Configurati	on				Partition / F	Path
No records to display.						
Delete						

Access >> Federation : SAML Resources >> New SAML Resource...

General Properties

Name	partner-app	
Description		
Publish on Webtop	Enable	
Configuration		
SSO Configuration	idp.f5demo.com-app 🗸	
Customization Settings for E	Inglish	
Language	English	
Caption	Partner App	
Detailed Description		
Image	Browse No file selected.	View/Hide

Webtop

1. Select Access ?> Webtops ?> Webtop List

Cancel Repeat Finished

2. Click the Create button (far right)

Acces	s » Webtops : We	btop Lists						
⇔ ⇒	Webtop Lists	Webtop Link List	Webtop Section List	Hosted Content	•			
								Create
•	Name				1	Type	Access Profiles	Partition / Path

3. In the resulting window, enter the following values:

Name:	full_webtop
Type:	Full (drop down)

4. Click Finished at the bottom of the GUI

Access » Webtops: Webtop Lists » New Webtop						
General Properties	_					
Name	full_webtop					
Туре	Full 🗸					
Configuration						
Minimize To Tray	Enabled					
Show a warning message when the webtop window close	Enabled					
Show URL Entry Field	Enabled					
Show Resource Search	Enabled					
Fallback Section						
Initial State	Expanded 🗸					
Cancel Repeat Finished						

SAML IdP Access Policy

- 1. Select Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)
- 2. Click the **Create** button (far right)

Access » Profiles / Policies : Access Profiles (Per-Session Policies)								
Access Profiles Per-Request Policies Policy Sync Customization -								
* Search							c	eate Import
Status Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
🗆 🏴 access		All	(none)	(none)	(none)			Common

3. In the **New Profile** window, enter the following information:

Name:	idp.f5demo.com?policy
Profile Type:	All (drop down)
Profile Scope:	Profile (default)

- 4. Scroll to the bottom of the New Profile window to the Language Settings section
- 5. Select *English* from the **Factory Built?in Languages** menu on the right and click the **Double Arrow** (<<), then click the **Finished** button.
- 6. The **Default Language** should be automatically set

General Properties	
Name	idp.f5demo.com-policy
Parent Profile	access
Profile Type	
Profile Scope	Profile

Additional Languages	Afar (aa)	
	Acce pted Languages	Factory BuiltIn Languages
Languages	English (en)	Japanese (ja) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-tw) Korean (ko) Spanish (es) French (fr) German (de)
Default Language	English (en)	

7. From the Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies) screen, click the Edit link on the previously created idp.f5demo.com?policy line

Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
Access Profiles Per-Reques		t Policies	Policy S	ync C	ustomization	•				
	_									
				0						
_				Search						
~	Status	 Name 		÷ A	pplication	Profile Type	Access Policy	Export	Сору	Logs
]#	access				All	(none)	(none)	(none)	
	0.0	idp.f5demo.	com-policy			All	Edit	Export	Copy	default-log-setting
		rup.iouerno.	componey			7.94				

8. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign between Start and Deny

Access Policy: /Common/idp.f5demo.com-policy	Edit Endings
Start fallbac	
Add New Macro	

- 9. In the pop-up dialog box, select the **Logon** tab and then select the **Radio** next to **Logon Page**, and click the **Add Item** button
- 10. Click **Save** in the resulting Logon Page dialog box

Begin typing to search		9
	ment Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
O Citrix Logon Prompt	Configure logon options for Citrix clients	
O External Logon Page	Redirect user to externally hosted form-based web logon page	
O HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication	
O HTTP 407 Response	HTTP 407 Response for Basic or SPNEGO/Kerberos authentication	
Logon Page	Web form-based logon page for collecting end user credentials (used with most deployments)	
 Virtual Keyboard 	Enables a virtual keyboard on the logon page for entering credentials	
O VMware View Logon Page	Display logon screen on VMware View dients	
Cancel Add Item		Help

11. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign between Logon Page and Deny

Access Policy: /Common/idp.f5demo.com-policy	Edit Endings
Start	
Add New Macro	

12. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Auth**, and click the **Add Item** button

D	AD Auth	Active Directory authentication of end user credentials	
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping	
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
0	HTTP Auth	HTTP authentication of end user credentials	
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
0	LDAP Auth	LDAP authentication of end user credentials	
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping	
0	LocalDB Auth	Local Database Authentication	
0	NTLM Auth Result	NTLM authentication of end user credentials	
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication	
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	
0	OTP Generate	Generate One Time Passcode (OTP)	
0	OTP Verify	Verify One Time Passcode (OTP)	
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off	
0	RADIUS Auth	RADIUS authentication of end user credentials	
0	RSA SecurID	RSA SecurID two-factor authentication of end user credentials	
0	SAML Auth	SAML Auth using SAML Service Provider Interface	
0	TACACS+ Acct	Send accounting messages to a TACACS + server when users log on and off	
\sim	TA 1800 1 8.46	TEREPORT A. M E J	

- 13. In the resulting AD Auth pop-up window, select /Common/f5demo_ad from the Server drop down menu
- 14. Click **Save** at the bottom of the window

Properties Branch Rules				
Name: AD Auth				
Active Directory				
Туре	Authentication 🚽			
Server	/Common/f5demo_ad 💌			
Cross Domain Support	Disabled 💌			
Complexity check for Password Reset	Disabled 💌			
Show Extended Error	Disabled 💌			
Max Logon Attempts Allowed	3 💌			
Max Password Reset Attempts Allowed	3 💌			

15. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign on the successful branch between AD Auth and Deny

Access Policy: /Common/idp.f5demo.com-policy	Edit Endings
Start fallback + Successf + * AD Auth fallback + * AD Auth fallback Add New Macro Add New Macro * * *	Deny Deny

16. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button

0	AD Auth	Active Directory authentication of end user credentials	
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping	
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
0	HTTP Auth	HTTP authentication of end user credentials	
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
0	LDAP Auth	LDAP authentication of end user credentials	
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping	
0	LocalDB Auth	Local Database Authentication	
0	NTLM Auth Result	NTLM authentication of end user credentials	
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication	
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	
0	OTP Generate	Generate One Time Passcode (OTP)	
0	OTP Verify	Verify One Time Passcode (OTP)	
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off	
0	RADIUS Auth	RADIUS authentication of end user credentials	
0	RSA SecurID	RSA SecurID two-factor authentication of end user credentials	
0	SAML Auth	SAML Auth using SAML Service Provider Interface	
0	TACACS+ Acct	Send accounting messages to a TACACS + server when users log on and off	

17. In the resulting AD Query pop-up window, select /Common/f5demo_ad from the Server drop down menu

Properties* Branch Rules					
Name: AD Query	Name: AD Query				
Active Directory					
Туре					
Server	/Common/f5demo_ad 🔍				
SearchFilter					
Fetch Primary Group	Disabled 💌				
Cross Domain Support	Disabled 💌				
Fetch Nested Groups	Disabled 💌				
Complexity check for Password Reset	Disabled 💌				
Max Password Reset Attempts Allowed	3 🗨				
Prompt user to change password before expiration	none 💌 0				

- 18. In the AD Query pop?up window, select the Branch Rules tab
- 19. Change the Name of the branch to Successful.
- 20. Click the Change link next to the Expression

Properties Branch Rules*	
Add Branch Rule	Insert Before: 1: Successful 💌
Nar : Successful	
Expression: User's Primary Group ID is	100 <u>change</u>
Name: fallback	

21. In the resulting pop-up window, delete the existing expression by clicking the **X** as shown

Simple Advanced	
User's Primary Group ID is 100	×
AND Add Expression	
OR	
Add Expression	

22. Create a new Simple expression by clicking the Add Expression button

Simple* Advanced
Add Expression

23. In the resulting menu, select the following from the drop down menus:

Agent Sel:		-	
Condition:	AD	Query	Passed

24. Click the **Add Expression** Button

Simple*		
Agent Se	AD Query	-
Condition	AD Query Passed	
Active Dir	rectory Query has Passed	
Cancel	Add Expression	

25. Click the Finished button to complete the expression

Simple Advanced	
Active Directory Query has Passed 🗸	x
AND Add Expression	
OR	
Add Expression	
Cancel Finished	
Cancel Prinsned	Help
	Help
Properties Branch Rules*	Help
	Help
Properties Branch Rules*	Help
Properties Branch Rules*	Help
Properties Branch Rules* Add Branch Rule Name: Successful	Help

- 26. Click the **Save** button to complete the **AD Query**
- 27. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign on the successful branch between AD Query and Deny

Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, De	ny [de
Start fallback + Logon Page fallback + Successful + > AD Query fallback + > Deny AD Auth fallback + > Deny fallback + > Deny fallback + > Deny fallback + > Deny	2
Add New Macro	

28. In the pop-up dialog box, select the **Assignment** tab and then select the **Radio** next to **Advanced Resource Assign**, and click the **Add Item** button

1e

000	n Authentication Assignmen	Endpoint Security (Server-Side) Endpoint Security (Clent-Side) General Purpose	
)	ACL Assign	Assign existing Access Control Lists (ACLs)	
	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
	BWC Policy	Assign Bandwidth Controller policies	
	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	
	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership	
	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections	
	Pool Assign	Assign a Local Traffic Pool	
	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
	Resource Assign	Assign Connectivity Resources	
	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
	VMware View Policy	Specify a policy that will apply to VMware View connections	

- 29. In the resulting Advanced Resource Assign pop-up window, click the Add New Entry button
- 30. In the new Resource Assignment entry, click the **Add/Delete** link

Properties* Branch Rules
Name: Advanced Resource Assign
Resource Assignment
Add new entry
1 Add/Delete

31. In the resulting pop-up window, click the SAML tab, and select the Checkbox next to /Common/ partner-app

Q	Begin typing to searc	ch] in [Current Tab 💌
Static	: ACLs 0/0 SAML 1/1*	Webtop 1/1*	Show 7 more tabs		
/Common/partner-app					

32. Click the Webtop tab, and select the Checkbox next to /Common/full_webtop

Begin typing to search in Current Tab ~
Static ACLs 0/0 SAML 1/1* Webtop 1/1* Static Pool 0/3 Show 6 more tabs
O None
Ommon/full_webtop

- 33. Click the Update button at the bottom of the window to complete the Resource Assignment entry
- 34. Click the Save button at the bottom of the Advanced Resource Assign window

35. In the Visual Policy Editor, select the Deny ending on the fallback branch following Advanced Resource Assign

itart falback + Logon Page falback	AD Auth fallback f
) Deny

36. In the Select Ending dialog box, selet the Allow radio button and then click Save

Select Endi	ng:	
Allow		
🔿 Deny 🗖		
Cancel	Save	Help

37. In the Visual Policy Editor, click Apply Access Policy (top left), and close the Visual Policy Editor

5 Apply Access Policy
Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])
Start fallback + - X Successful + - Advanced Resource Assign fallback + - Allow Start fallback + - AD Query fallback + - Allow AD Auth fallback + - - - Allow - fallback + - - - - - - Deny - - - - - - -
Add New Macro

1.3.3 TASK 3 - Create the IdP Virtual Server and Apply the IdP Access Policy

- 1. Begin by selecting Local Traffic ?> Virtual Servers
- 2. Click the Create button (far right)

Local Traffic ->> Virtual Servers : Virtual Server List									
₩ -	Virtual Server List	/irtual Address List							
				-					
		Sea	rch Reset Search						Create
2	 Status Name 		Description	Application	• Destination	Service Port	• Туре	Resources	Partition / Path
No re	cords to display.								
Enal	ble Disable De	elete							

3. In the New Virtual Server window, enter the following information:

General Properties	
Name:	idp.f5demo.com
Destination Address/Mask:	10.1.10.110
Service Port:	443

Configuration	
HTTP Profile:	http (drop down)
SSL Profile (Client)	idp.f5demo.com?clientssl

Access Policy	
Access Profile:	idp.f5demo.com?policy

General Properties		
Name	idp.f5demo.com	
Partition / Path	Common	
Description		
Туре	Standard	
Source Address	0.0.0.0/0	
Destination Address/Mask	10.1.10.110	
Service Port	443 HTTPS 💌	
Notify Status to Virtual Address		
Availability	📴 Unknown (Enabled) - The children po	ol member(s) either don't have service che
Syncookie Status	Off	
State	Enabled 💌	
Configuration: Basic 💌		
Protocol	ТСР 💌	
Protocol Profile (Client)	tcp	
Protocol Profile (Server)	(Use Client Profile)	
HTTP Profile	http 💌	
FTP Profile	None 👻	
RTSP Profile	None 👻	
SSH Proxy Profile	None	
SSL Profile (Client)	Selected /Common idp.f5demo.com-clientssl	Available
	Selected	Available

	1
Access Policy	
Access Profile	idp.f5demo.com-policy
Connectivity Profile	None 🗸 😽
Per-Request Policy	None 💌
VDI Profile	None
Application Tunnels (Java & Per-App VPN)	Enabled
	—

4. Scroll to the bottom of the configuration window and click Finished

1.3.4 TASK 4 - Test the SAML IdP

1. Using your browser from the jump host, navigate to the SAML IdP you just configured at https://idp.f5demo.com (or click the provided bookmark)

https://idp.f5demo.com	× (+
🗲 🕕 🔒 🛛 https://idp.f5dem	o.com
🕼 Big-IP 🔲 idp.f5demo.com 🗉	app.f5demo.com 🗉 idp.partner.com 🗉 app.partner.com

2. Log in to the IdP. Were you successfully authenticated? Did you see the webtop with the SP application?

Note: Use the credentials provided in the Authentication section at the beginning of this guide (user/Agility1)

- 3. Click on the Partner App icon. Were you successfully authenticated (via SAML) to the SP?
- 4. Review your Active Sessions (Access ?> Overview ?> Active Sessions)
- 5. Review your Access Report Logs (Access ?> Overview ?> Access Reports)

1.4 Lab 3: Kerberos to SAML Lab

The purpose of this lab is to deploy and test a Kerberos to SAML configuration. Students will modify a previous built Access Policy and create a seamless access experience from Kerberos to SAML for connect-

ing users. This lab will leverage the work performed previously in Lab 2. Archive files are available for the completed Lab 2.

Objective:

- Gain an understanding of the Kerberos to SAML relationship its component parts.
- Develop an awareness of the different deployment models that Kerberos to SAML authentication opens up

Lab Requirements:

• All Lab requirements will be noted in the tasks that follow

Estimated completion time: 25 minutes

1.4.1 TASK 1 – Modify the SAML Identity Provider (IdP) Access Policy

 Using the existing Access Policy from Lab 2, navigate to Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies), and click the Edit link next to the previously created *idp.f5demo.com-policy*

Acces	ss » Pr	ofiles / Polic	ies : Access	Profiles (F	Per-Sessi	on Policies)				
Access Profiles Per-Request		t Policies	Policy S	ync C	Customization	-				
				Search						
				ocarcin						
	Status	 Name 		\$ A	pplication	Profile Type	Access Policy	Export	Сору	Logs
]	access				All	(none)	(none)	(none)	
] #	idp.f5demo.	com-policy			All	📮 Edit	Export	Сору	default-log-setting
Delete	ə Ap	ply Access P	olicy							

2. Delete the Logon Page object by clicking on the X as shown

Access Policy: /Common/idp.f5d	emo.com-policy Edit Endings (Endings: Allow, Deny [default])
Start falback + Logon Page black + →>-	AD Auth fallback + ->> fallback + ->> fallback + ->> Deny
Add New Macro	

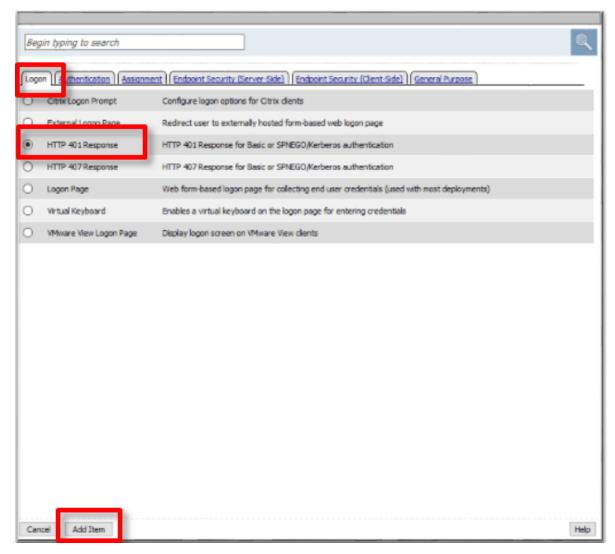
3. In the resulting **Item Deletion Confirmation** dialog, ensure that the previous node is connect to the **fallback** branch, and click the **Delete** button

Item deletion confirmation	
Do you really want to delete action 'Logon Page'	
Connect previous node to fallback v branch	
O Delete all branches	
Cancel Delete	Help

4. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign between Start and AD Auth

Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])
Start fallback +-+ AD Auth Successful +-+ Advanced Resource Assign fallback +-+> Allow AD Auth fallback +-+> Deny Deny
Add New Macro

5. In the pop-up dialog box, select the **Logon** tab and then select the **Radio** next to **HTTP 401 Response**, and click the **Add Item** button



6. In the HTTP 401 Response dialog box, enter the following information:

Basic Auth Realm:		
HTTP Auth Level:	basic+negotiate (drop down)	

7. Click the Save button at the bottom of the dialog box

Properties* Branch Rules				
Name: HTTP 401 Response				
401 Response Settings				
Basic Auth Realm	f5demo.com			
HTTP Auth Level	basic+negotiat	:e 🗸		
Customization				

Language	en 🗸 Reset all defaults
Logon Page Input Field #1	Username .::
Logon Page Input Field #2	Password
HTTP response message	Authentication required to access the resources.
Logon Page Original URL	Click here if already logged in

- 8. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign on the Negotiate branch between HTTP 401 Response and Deny
- 9. In the pop-up dialog box, select the Authentication tab and then select the Radio next to Kerberos Auth, and click the Add Item button

Begin typing to search	
Logon Authentication Assig	ment Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
AD Auth	Active Directory authentication of end user credentials
AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
 Client Cert Inspection 	Check the result of client certificate authentication by the Local Traffic Client SSL profile
CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
HTTP Auth	HTTP authentication of end user credentials
Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
LDAP Auth	LDAP authentication of end user credentials
LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
O LocalDB Auth	Local Database Authentication
O NTLM Auth Result	NTLM authentication of end user credentials
 OCSP Auth 	Online Certificate Status Protocol (OCSP) dient certificate authentication
On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
OTP Generate	Generate One Time Passcode (OTP)
OTP Verify	Verify One Time Passcode (OTP)
O RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
C RADIUS Auth	RADIUS authentication of end user credentials
RSA SecurID	RSA SecurID two-factor authentication of end user credentials
SAML Auth	SAML Auth using SAML Service Provider Interface
O TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off
O	TARARE A SHARE AND A CARACTERIA

10. In the Kerberos Auth dialog box, enter the following information:

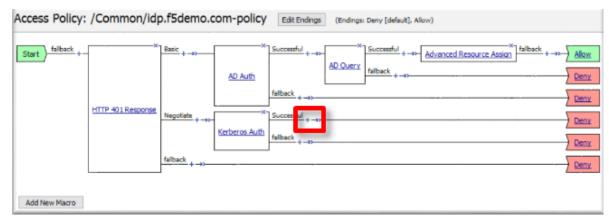
AAA Server:	/Common/apm-krb-aaa (drop down)	
Request Based Auth:	Disabled (drop down)	

11. Click the Save button at the bottom of the dialog box

Properties Branch Rules				
Name: Kerberos Auth				
KERBEROS				
AAA Server	/Common/apm-krb-aaa 🗸			
Request Based Auth	Disabled 🗸			
Max Logon Attempts Allowed	3 🗸			

Note: The *apm-krb-aaa* object was pre-created for you in this lab. More details on the configuration of Kerberos AAA are included in the Learn More section at the end of this guide.

12. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign on the Successful branch between Kerberos Auth and Deny



13. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button

Log	Authentication Assig	nment) Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
0	AD Auth	Active Directory authentication of end user credentials
D.	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) dient certificate authentication
0	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
0	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
0	LocalDB Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
0	RADIUS Auth	RADIUS authentication of end user credentials
0	RSA SecurID	RSA SecurID two-factor authentication of end user credentials
0	SAML Auth	SAML Auth using SAML Service Provider Interface
~	TACACS+ Acct	Send accounting messages to a TACACS + server when users log on and off

- 14. In the resulting AD Query(1) pop-up window, select /Commmon/f5demo_ad from the Server drop down menu
- 15. In the SearchFilter field, enter the following value: userPrincipalName=%{session.logon.
 last.username}

Properties Branch Rules	
Name: AD Query(1)	
Active Directory	
Туре	Query
Server	/Common/f5demo_ad 🗸
SearchFilter	userPrincipalName=%{session.logon.last.username}
Fetch Primary Group	Disabled 🗸
Cross Domain Support	Disabled V
Fetch Nested Groups	Disabled V
Complexity check for Password Disabled V	
Max Password Reset Attempts Allowed	3 🗸
Prompt user to change password before expiration	none v 0

- 16. In the AD Query(1) window, click the Branch Rules tab
- 17. Change the Name of the branch to Successful.
- 18. Click the Change link next to the Expression

Properties Branch Rules*	
Add Branch Rule	Insert Before: 1: Successful 💌
Nan : Successful	×
Expression: User's Primary Group ID is 100 change	
Name: fallback	-

19. In the resulting pop-up window, delete the existing expression by clicking the ${f X}$ as shown

Simple Advanced	
User's Primary Group ID is 100	×
AND Add Expression	
OR	
Add Expression	

20. Create a new Simple expression by clicking the Add Expression button

Simple* Advanced
Add Expression

21. In the resulting menu, select the following from the drop down menus:

Agent Sel:		-	
Condition:	AD	Query	Passed

22. Click the Add Expression Button

Simple*		
Agent Se	AD Query	
Condition	AD Query Passed	
Active Dir	ectory Query has	Passed 💌
Cancel	Add Expression	

23. Click the **Finished** button to complete the expression

Simple Advanced	_
Active Directory Query has Passed 🗸	×
AND Add Expression	
OR	
Add Expression	
Cancel Finished	Help

24. Click the Save button to complete the AD Query

Properties Branch Rules*
Add Branch Rule
Name: Successful
Expression: Active Directory Query has Passed
Name: fallback
~~~

- 25. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Plus (+) Sign on the Successful branch between AD Query(1) and Deny
- 26. In the pop-up dialog box, select the **Assignment** tab and then select the **Radio** next to **Advanced Resource Assign**, and click the **Add Item** button

Rea	in typing to search		Q
Deg	in opping to source		
Logo	n Authentication Assignmen	Endpoint Security (Server-Side) Endpoint Security (Clent-Side) General Purpose	
0	ACL Assign	Assign existing Access Control Lists (ACLs)	
0	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
۲	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
0	BWC Policy	Assign Bandwidth Controller policies	
0	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
0	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	
0	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership	
0	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections	
0	Pool Assign	Assign a Local Traffic Pool	
0	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
0	Resource Assign	Assign Connectivity Resources	
0	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
0	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
0	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
0	VMware View Policy	Specify a policy that will apply to VMware View connections	
Can	cel Add Item		Help

- 27. In the resulting Advanced Resource Assign(1) pop-up window, click the Add New Entry button
- 28. In the new Resource Assignment entry, click the  ${\bf Add}/{\bf Delete}$  link

Properties* Branch Rules
Name: Advanced Resource Assign
Resource Assignment
Add new entry
1 Add/Delete

29. In the resulting pop-up window, click the SAML tab, and select the Checkbox next to /Common/partner-app

	gin typing to sear	in	Current Tab 💌		
Static ACL	s 0/C	Webtop 1/1*	Show 7 more tabs		
/Common/partner-app					

30. Click the Webtop tab, and select the Checkbox next to /Common/full_webtop

Begin typing to search in Current Tab ~							
Static ACLs 0/0 SAML 1/1* Webtop 1/1* Static Pool 0/	3 Show 6 more tabs						
O None							

- 31. Click the **Update** button at the bottom of the window to complete the Resource Assignment entry
- 32. Click the Save button at the bottom of the Advanced Resource Assign(1) window

33. In the Visual Policy Editor, select the Deny ending on the fallback branch following Advanced Resource Assign

Start       falback       +	Access Policy:	/Common/id	D.f5demo.com-policy Edit Endings: Allow, Deny [default])
			AD Auth falback + -=>- Negotiate + -=>- Kerberos Auth falback + -=>- AD Query falback + -=>- Deny falback + -=>- Deny

34. In the Select Ending dialog box, selet the Allow radio button and then click Save

Select En	ding:	
Allow		
O Deny		
Cancel	Save	Help

35. In the Visual Policy Editor, click Apply Access Policy (top left), and close the Visual Policy Editor

Apply Access Policy		
Access Policy: / Common	ndp.f5demo.com-policy	Edit Endings (Endings: Allow, Deny [default])
Start felback +	Negotiale + -e>	Successful +
Add New Macro		

## 1.4.2 TASK 2 - Test the Kerberos to SAML Configuration

**Note:** In the following Lab Task it is recommended that you use Microsoft Internet Explorer. While other browsers also support Kerberos (if configured), for the purposes of this Lab Microsoft Internet Explorer has been configured and will be used.

1. Using Internet Explorer from the jump host, navigate to the SAML IdP you previously configured at *https://idp.f5demo.com* (or click the provided bookmark)

https	s://idp.f5demo.com × +
€ 0 ₽	https://idp.f5demo.com
🕼 Big-IP 🗉	] idp.f5demo.com 🗏 app.f5demo.com 🗏 idp.partner.com 🗏 app.partner.com 🗏 saas.f5demo.com

- 2. Were you prompted for credentials? Were you successfully authenticated? Did you see the webtop with the SP application?
- 3. Click on the Partner App icon. Were you successfully authenticated (via SAML) to the SP?
- 4. Review your Active Sessions (Access ?> Overview ?> Active Sessions)
- 5. Review your Access Report Logs (Access ?> Overview ?> Access Reports)

# 1.5 Lab 4: [Optional] SaaS Federation iApp Lab

The purpose of this lab is to familiarize the Student with the new SaaS Federation iApp. Students will use the iApp to create a federation relationship with a commonly used SaaS provider. This lab will leverage the work performed previously in Lab 3. Archive files are available for the completed Lab 3.

Objective:

- Gain an understanding of the new SaaS Federation iApp and its features.
- · Deploy a working SaaS federation using the iApp to a commonly used SaaS provider

Lab Requirements:

All lab requirements will be noted in the tasks that follow

Estimated completion time: 25 minutes

#### 1.5.1 TASK 1 – Create a new SaaS SAML Service Provider (SP)

- 1. Navigate to Access ?> Federation ?> SAML Identity Provider ?> External SP Connectors
- 2. Click specifically on the **Down Arrow** next to the **Create** button (far right)
- 3. Select From Metadata from the drop down menu

Access » Federation: SAML Identity Provider: External SP Connectors										
🔅 🗸 SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Server 👻	OAuth Client / Re	esource Server 👻	PingAccess 🗸				
This application is used to manag Users can create, edit and delete		alG-IP (this d	evice), in its role as a SAML Ident	ity Provider, receiv	es an authenticatio	n request from a servi	ce and in turn authentio	cates the user and sends	s an assertion ba	ck to the service.
Users can create, euit and delete	External SP Connector		Juliona.							
	Artifact Resolution Serv	vices								Create
Name 🔺		SAML IdP S	ervices		Description			Partition		Custom
saml_office365					Predefined SP co	nnector object for Offic	ce 365	Common		From Metadata
										From Template 🕨

- 4. In the Create New SAML Service Provider dialogue box, click Browse and select the SAMLSP-00D36000000jjkp.xml file from the Desktop of your jump host
- 5. In the Service Provider Name field, enter: salesforce
- 6. Click **OK** on the dialog box

Create New SAML Service	× Provider
Select File*:	
SAMLSP-00D36000000jjkp.xml	Browse
Service Provider Name*:	
salesforce	
Select Signing Certificate :	
Select a value	on desktop
	OK Cancel

## 1.5.2 TASK 2 - Deploy the SaaS Federation iApp

1. Navigate to iApps ?> Application Services -> Applications and click on the Plus (+) Sign as shown

iApps		This application is used to man authentication request from a s delete their SP connects by				m a ser	
	Application Services	۰.	Applications			,	
	Templates	ŀ			Name 🔺	_	
	AWS				app.partner	.com	
-					saml_office	365	

- 2. In the resulting New Application Service window, enter saas as the Name
- 3. Select f5.saas_idp.v1.0.rc1 from the Template drop down menu

iApps » Application Services : Applications » New Application Service					
Template Selection: Basic	<b>•</b>				
Name	saas				
Template	f5.saas_idp.v1.0.0rc1	•			

**Note:** The iApp template has already been downloaded and imported for this lab. You can download the latest iApp templates from https://downloads.f5.com/

4. Configure the iApp template as follows:

SaaS Applications					
Application:	New federation relationship with salesforce.com				
SP:	salesforce				
Display Name:	SalesForce				
SP Initiated:	No				

SaaS Application	S							
Which SaaS application (and SP Connector) are you using?	Application Add	New federation relationship with Salesford	e.con • \$P	salesforce	Display Name	SalesForce	SP Initiate	

BIG-IP APM Configuration	
What EntityID do you want to use for your SaaS applica-	https://idp.f5demo.com/
tions?	idp/f5/
Should the iApp create a new AAA server or use an existing	f5demo_ad
one?	

BIG-IP APM Configuration	
How is your EntityID formatted?	My EntityID is a URL
	Select appropriate format used to identify provider (APM) to federation partners (SaaS applications).
What EntityID do you want to use for your SaaS applications?	https://idp.f5demo.com/idp/f5/
	Specify the globally unique, persistent URL or URN that will be used to identify this Identity Provider 1
Should the iApp create a new AAA server or use an existing one?	f5demo_ad
	Choose whether you want the iApp template to create a new AAA server object, or select the custom specific requirements, we recommend allowing the iApp to create a new AAA server for the deploym
Which APM logging profile do you want to use?	default-log-setting
	Select the APM logging profile to use for the Access Policy created by this iApp deployment.

BIG-IP Virtual Server	
What is the IP address clients will use to access the BIG-IP IdP Service?	10.1.10.120
What port do you want to use for the virtual server?	443
Which certificate do you want this BIG-IP system to use for client authen-	idp.f5demo.com.
tication?	crt
What is the associated private key?	idp.f5demo.com.
	key

BIG-IP IdP Virtual Server	
What is the IP address clients will use to access the BIG-IP IdP Service?	10.1.10.120
	Specify the IP address for the BIG-IP virtual server. Clients will resolve the FQDN of the I
What port do you want to use for the virtual server?	443
	Specify the associated service port. The default port is 443.
Which certificate do you want this BIG-IP system to use for client authentication?	idp.f5demo.com.crt
	Select the name of the certificate the system uses for client-side SSL processing. The c
What is the associated private key?	idp.f5demo.com.key
	Select the name of the associated SSL key.

**Note:** We are deploying the iApp on a different IP so that you can see how everything is built out; however, this IdP will not work, as the *idp.f5demo.com* FQDN resolves to another IP. We are going to use the iApp to create the SAML resource that we will assign to our existing access policy from Lab 3.

IdP Encryption Certificate and Key	
Which certificate do you want to use to encrypt your SAML Assertion?	SAML.crt
What is the associated private key?	SAML.key

Which certificate do you want to use to encrypt your SAML Assertion?	SAML.crt
	Select the name of the certificate you imported select it. To select any new certificates and ke
	The certificate can be either self-signed certificate a wildcard certificate to sign SAML assert
What is the associated private key?	SAML.key
	Select the name of the associated SSL key.

- 5. Scroll to the bottom of the configuration template and click Finished
- 6. Once deployed, you can review the built out SaaS Federation iApp at iApps ?> Application Services ?> Applications ?> saas

iApps » Application Services : Applications » sass							
🗙 🚽 Properties	Reconfigure	Components	Security	Analytics			
	,	,					
Name				Availability	Туре		
🖃 🚞 BIG-IP							
🖃 🚞 sass					Application Service		
🖃 📑 🔲 sa	SS_VS			Unknown	Virtual Server		
10	.1.10.120				Virtual Address		
sa	ss_http				Profile		
🖃 📃 sa	ss_client-ssl				Profile		

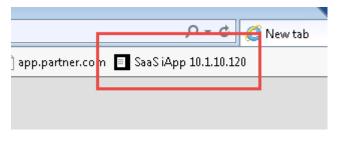
7. Review the new virtual servers created by the iApp at Local Traffic ?> Virtual Server ?> Virtual Server List

Local Traffic » Virtual Servers : Virtual Server List						
🗱 👻 Virtual Server List 🛛 Virtual Address List		Statistics	-			
* Search						
Status 🔺 N	lame	Description	Application	Destination		
🔲 🔲 app.	).f5demo.com			10.1.10.100		
🔲 🔲 idp.f	.f5demo.com	_		10.1.10.110		
🔲 💼 saa:	as_redir_vs		saas	10.1.10.120		
🔲 🔲 saa:	as_vs		saas	10.1.10.120		
Enable Disable Delete						

8. Review the new Access Policy built by the iApp at Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies) and select the Edit link next to the saas Access Policy

<b>#</b> -	Access	Profiles Per-Reques	t Policies Poli	icy Sync	Customization	-
		,				
			Search			
•	Status	▲ Name	Application	Profile Type	Access Policy	Ехро
	p#	access		All	(none)	(none
	<b>]#</b>	app.f5demo.com-policy		All	🗖 Edit	Ехро
	p#	idp.f5demo.com-policy		All	🗩 Edit	Expor
	0.0	saas	saas	All	Edit	Ехро

9. Test the SaaS iApp by clicking on the bookmark in your browser.



Note: Navigating to the virtual server by IP will produce a certificate warning. This is expected. Click

#### 1.5.3 TASK 3 - Modify the SAML IdP Access Policy

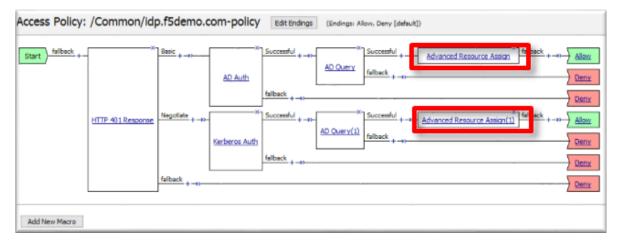
The previous task, Task 2, was to provide you an understanding of how the SaaS Federation iApp can automatically build a configuration for you.

In this task we will be modifying the existing Webtop from prior labs to add the SaaS SalesForce application. The purpose of the task is so you can see the F5Demo App and SalesForce in the same Webtop.

 Using the same Access Policy from Lab 3, navigate to Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies) and click the Edit link next to the previously created idp.f5demo. com-policy

Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
₽	- Access	s Profiles	Per-Reques	st Policies	Policy S	ync C	ustomization	-		
				Search						
•	<ul> <li>Status</li> </ul>	<ul> <li>Name</li> </ul>		\$ J	Application	Profile Type	Access Policy	Export	Сору	Logs
	<b>]</b> #	access				All	(none)	(none)	(none)	
	-	idp.f5demo.	com-policy			All	Edit	Export	Сору	default-log-setting
		rup.ioueinio.	com ponej							

2. In the Visual Policy Editor window for /Common/idp.f5demo.com?policy, click the Advanced Resource Assign object.



3. Click the Add/Delete link on the Resource Assignment item

Na	me: Advanced Resource Assign(1)
R	esource Assignment
C	Add new entry
	Expression: Empty change
1	SAML: /Common/partner-app
1	Webtop: /Common/full_webtop
	Add/Delete

4. Click the SAML tab, and select the checkbox next to /Common/saas.app/ saas_SalesForce_saml_resource_sso

SAML 2/2* Webtop 1/2 Show 7 more tabs	2		
/Common/partner-app			
/Common/saas.app/saas_SalesForce_saml_resource_sso			

- 5. Click the **Update** button at the bottom of the window to complete the Resource Assignment entry
- 6. Click the Save button at the bottom of the Advanced Resource Assign window
- 7. Repeat steps 2 6 with the Advanced Resource Assign (1) object
- 8. In the Visual Policy Editor, click Apply Access Policy (top left), and close the Visual Policy Editor

	ccess Policy /Common/idp	o.f5demo.c	om-policy	Edit Endings (Endings: Allow, Deny [default])
Start		Basic + -+>	AD Auth	Successful +
	HTTP 401 Response	Negotiate + -+>-	Kerberos Auth	felbeck + →>     Deny       Successful + →>     AD Query(1)       felbeck + →>     Advanced Resource Assign(1)       felbeck + →>     Alow
		fallback +		falback + -22
Add New Macro		,		

## 1.5.4 TASK 4 - Test the SaaS Federation Application

1. Using your browser from the jump host, navigate to the SAML IdP previously configured at https://idp.f5demo.com (or click the provided bookmark)



- 2. Were you prompted for credentials? Were you successfully authenticated? Did you see the webtop with the new SaaS SP application?
- 3. Click on the SalesForce icon. Were you successfully authenticated (via SAML) to the SP?
- 4. Review your Active Sessions (Access ?> Overview ?> Active Sessions)
- 5. Review your Access Report Logs (Access ?> Overview ?> Access Reports)

# **1.6 Conclusion**

Thank you for your participation in the 301 Access Policy Manager (APM) Federation Lab. This Lab Guide has highlighted several notable features of SAML Federation. It does not attempt to review all F5 APM Federation features and configurations but serves as an introduction to allow the student to further explore the BIG-IP platform and Access Policy Manager (APM), its functions & features.

#### 1.6.1 Learn More

The following are additional resources included for reference and assistance with this lab guide and other APM tasks.

#### Links & Guides

- Access Policy Manager (APM) Operations Guide: https://support.f5.com/content/kb/en-us/ products/big-ip_apm/manuals/product/f5-apm-operations-guide/_jcr_content/pdfAttach/download/ file.res/f5-apm-operations-guide.pdf
- Access Policy Manager (APM) Authentication & Single Sign on Concepts: https://support.f5. com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0.html

#### • SAML:

- Introduction: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-sso-13-0-0/28.html#guid-28f26377-6e10-42c9-883a-3ac65eab9092
- F5 SAML IdP (Identity Provider with Portal): https://support.f5.com/kb/ en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/29.html# guid-42e93e4b-e4fc-4c3d-ae53-910641d5755c
- F5 SAML IdP (Identity Provider without Portal): https://support.f5.com/kb/ en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/30.html# guid-39ffed07-65f2-40b8-85ae-c80073cc4e82
- F5 SAML SP (Service Provider): https://support.f5.com/kb/en-us/ products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/31.html# guid-be2cf224-727e-4a0f-aa68-676fdedba37b
- F5 Federation iApp (Includes o365): https://www.f5.com/pdf/deployment-guides/ saml-idp-saas-dg.pdf
- F5 o365 Deployment Guide: https://www.f5.com/pdf/deployment-guides/ microsoft-office-365-idp-dg.pdf

#### • Kerberos

- Kerberos AAA Object: (See Reference section below)
- Kerberos Constrained Delegation: http://www.f5.com/pdf/deployment-guides/ kerberos-constrained-delegation-dg.pdf
- Two-factor Integrations/Guides (Not a complete list)
  - RSA Integration: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-single-sign-on-12-1-0/6.html#conceptid
  - DUO Security:
    - * https://duo.com/docs/f5bigip
    - * https://duo.com/docs/f5bigip-alt
  - SafeNet MobilePass: http://www.safenet-inc.com/resources/integration-guide/data-protection/ SafeNet_Authentication_Service/SafeNet_Authentication_Service_RADIUS_Authentication_ on_F5_BIG-IP_APM_Integration_Guide
  - Google Authenticator: https://devcentral.f5.com/articles/two-factor-authentication-with-google-authenticator-ar
- Access Policy Manager (APM) Deployment Guides:
  - F5 Deployment Guide for Microsoft Exchange 2010/2013: https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2010-and-2013-big-ip-v11
  - F5 Deployment Guide for Microsoft Exchange 2016: https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2016-big-ip-v11-v12-ltm-apm-afm

- F5 Deployment Guide for Microsoft SharePoint 2010/2013: <a href="https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2010-and-2013-new-supported-iapp-big-ip-v114-ltm-apm-asm-aam">https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2010-and-2013-new-supported-iapp-big-ip-v114-ltm-apm-asm-aam</a>
- F5 Deployment Guide for Microsoft SharePoint 2016: https://f5.com/solutions/ deployment-guides/microsoft-sharepoint-2016-big-ip-v114-v12-ltm-apm-asm-afm-aam
- F5 Deployment Guide for Citrix XenApp/XenDesktop: https://f5.com/solutions/ deployment-guides/citrix-xenapp-or-xendesktop-release-candidate-big
- F5 Deployment Guide for VMWare Horizon View: https://f5.com/solutions/deployment-guides/ vmware-horizon-view-52-53-60-62-70-release-candidate-iapp-big-ip-v11-v12-ltm-apm-afm? tag=VMware
- F5 Deployment Guide for Microsoft Remote Desktop Gateway Services: <a href="https://f5.com/solutions/deployment-guides/microsoft-remote-desktop-gateway-services-big-ip-v114-ltm-afm-apm">https://f5.com/solutions/deployment-guides/microsoft-remote-desktop-gateway-services-big-ip-v114-ltm-afm-apm</a>
- F5 Deployment Guide for Active Directory Federated Services: <a href="https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm">https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm</a>

#### 1.6.2 Reference: Kerberos AAA Object

The following is an example of the AAA Server object used in Lab 3: Kerberos to SAML Lab (the /Common/apm-krb-aaa used in Task 1).

#### **AD User and Keytab**

- 1. Create a new user in Active Directory
- 2. In this example, the User Logon Name kerberos has been created

	New Object - User	x		
Create in:	acme.com/acme-users			
First name:	Kerb Initials:			
Last name:	Eros			
Full name:	Kerb Eros			
User logon name:				
kerberos	@acme.com v			
User logon name (pre-Windows 2000):				
ACME\	kerberos			
	< Back Next > Cance	el		

3. From the Windows command line, run the KTPASS command to generate a keytab file for the previously created user object

ktpass /princ HTTP/kerberos.acme.com@ACME.COM /mapuser acme\kerberos /
ptype KRB5_NT_PRINCIPAL /pass password /out c:\file.keytab

FQDN of virtual server:	kerberos.acme.com
AD Domain (UPN format):	@ACME.COM
Username:	acme\kerberos
Password:	password

4. Review the changes to the AD User object

Kerb Eros Properties ? X						
Organization	Published Certificates	Membe	r Of Passw	ord Replication		
Dial-in	Object Securi	ty E	nvironment	Sessions		
Remote contro		ervices Prof	ile COM+	Attribute Editor		
General A	ddress Account	Profile	Telephones	Delegation		
User logon na	me:					
HTTP/kerbe	ros.acme.com	@acme.c	om	~		
User logon na	me (pre-Windows 2000	):				
ACME\		kerberos				
Log On To         ✓ Unlock account         Account options:         □ User must change password at next logon						
□ User cannot change password         ✓ Password never expires         □ Store password using reversible encryption						
Account expires Never C End of: Tuesday, August 9, 2016						
OK Cancel Apply Help						

## Kerberos AAA Object

- 1. Create the AAA object by navigating to Access ?> Authentication -> Kerberos
- 2. Specify a Name

- 3. Specify the Auth Realm (Ad Domain)
- 4. Specify a Service Name (This should be HTTP for http/https services)
- 5. Browse to locate the Keytab File
- 6. Click Finished to complete creation of the AAA object

Access » Authentication » New Server					
General Properties					
Name	Kerberos_SSO				
Туре	Kerberos				
Configuration					
Auth Realm	ACME.COM				
Service Name	HTTP				
Keytab File	Browse No file selected.				
Cancel Repeat Finished					

7. Review the AAA server configuration at Access ?> Authentication

# **Class 2: OAuth Federation with F5**

# 2.1 Lab Environment

All lab prep is already completed if you are working in the UDF or Ravello blueprint. The following information will be critical for operating your lab. Additional information can be found in the ***Learn More*** section of this guide for setting up your own lab.

Lab Credentials

Host/Resource	Username	Password
Windows Jump Host	user	user
Big-IP 1, Big-IP 2 GUI (Browser Access)	admin	admin
Big-IP 1, Big-IP 2 CLI (SSH Access)	root	default

Lab Network & Resource Design

2

GAGILITY 2017 331 OAuth Federation with F5 En										Lab vironment		
and the second second	Big-IP 1 OAuth (C/RS) 10.1.4/24 Lab Server Lab Server Lab Server Lab Server Lab Server Lab Server Lab Server Lab Server Lat Serv											
Ju	ump Host	3IG	G-IP-1 (VE) 🚳 31G-IP-2 (VE) 🧃				Lal	b Server	1	/LANs		
OS	Windows 7	TMOS	13.0.0	5	TMOS	13.0.0	R	OS	Ubuntu	TMOS	IP Subnet	
External	10.1.20.210	Internal	10.1.10.10/24	1	Internal	10.1.10.11/24		Internal	10.1.10.100/24	Internal	10.1.10.0/24	
Mgmt.	10.1.1.6	External	10.1.20.10/24	00	External	10.1.20.11/24		Services	Web Services	External	10.1.20.0/24	
2)-2,-2	1-21-21-2	Mgmt.	10.1.1.4/24	2	Mgmt.	10.1.1.5/24		Services	web services	Mgmt.)	10.1.1.0/24	
8 8	8 8 8 8	8 8	8 8 8	No.	Wax	8 8) A	Y	a) (f	60	6 0		

# 2.2 Lab 1: Social Login Lab

Note: The entire module covering Social Login is performed on BIG-IP 1 (OAuth C/RS)

## 2.2.1 Purpose

This module will teach you how to configure a Big-IP as a client and resource server enabling you to integrate with social login providers like Facebook, Google, and LinkedIn to provide access to a web application. You will inject the identity provided by the social network into a header that the backend application can use to identify the user.

# 2.2.2 Task 1: Setup Virtual Server

1. Go to Local Traffic -> Virtual Servers -> Create

Local Traffic » Virtual Servers : Virtual Server List										
🛪 🗸 Virtual Server List 🛛 Virtual Address List Stati				-						
*		Se	arch							Create
💌 💌 Status	▲ Name			Description	Application	Destination	♦ Service Port	⇔ Type	Resources	Partition / Path
	dns_host_	resolver				10.1.20.99	53	Standard	Edit	Common
Enable Disable Delete										

- 2. Enter the following values (leave others default)
  - Name: social.f5agility.com-vs
  - Destination Address: 10.1.20.111
  - Service Port: 443
  - HTTP Profile: http
  - SSL Profile (Client): f5agility-wildcard-self-clientssl
  - Source Address Translation: Auto Map

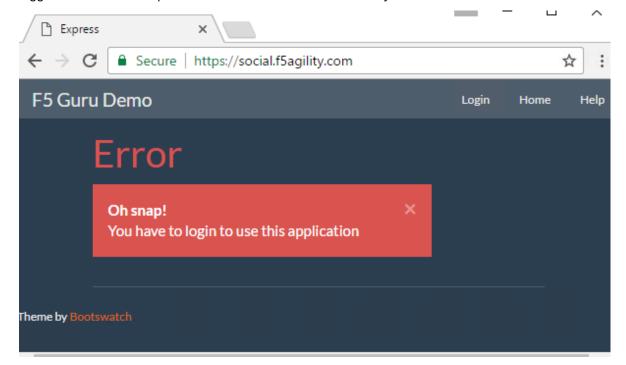
General Properties	
Name	social.f5agliity.com-vs
Description	
Туре	Standard V
Source Address	
Destination Address/Mask	10.1.20.111
Service Port	443 HTTPS V
Notify Status to Virtual Address	
State	Enabled V
Configuration: Basic 🗸	
Protocol	TCP
Protocol Profile (Client)	tcp ~
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	[http 💙]
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None V
RTSP Profile	None 🗸
SSL Profile (Client)	Selected Available Centrast-insecure-compatible Clentsis-insecure-compatible Clentsis-secure crypto-server-default-clientssi splitession-default-clientssi wom-default-clientssi
SSL Profile (Server)	Selected Available
SMTPS Profile	None 🗸
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None 🗸
VLAN and Tunnel Traffic	All VLANs and Tunnels V
Source Address Translation	Auto Map 🗸

3. Select webapp-pool from the Default Pool drop down and then click **Finished** 

Resources		
iRules	Enabled	Available _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main _sys_APM_Office365_SAML_BasicAuth _sys_APM_activesync _sys_auth_krbdelegate
Policies	Enabled	Available
Default Pool +	webapp-pool 🗸	
Default Persistence Profile	None ~	
Fallback Persistence Profile	None ~	
Cancel Repeat Finished		

4. Test access to https://social.f5agility.com from the jump host's browser.

You should be able to see the backend application, but it will give you an error indicating you have not logged in because it requires a header to be inserted to identify the user.



## 2.2.3 Task 2: Setup APM Profile

1. Go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) -> Create



- 2. Enter the following values (leave others default) then click Finished
  - Name: social-ap
  - Profile Type: All
  - **Profile Scope:** Profile

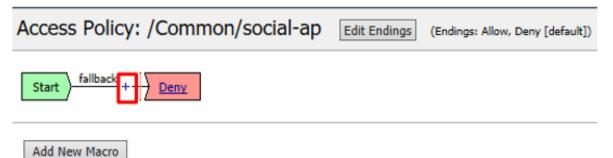
• Languages: English

Access » Profiles / Policies : Access Profiles (Per-Session Policies) » New Profile						
General Pro	operties					
Name		social-ap				
Parent Pro	ofile	access				
Profile Ty	pe	All				
Profile Sc	cope	Profile V				
Language Settings						
Additional Languages	Afar (aa)					
Languages		Factory Builtin Languages       Chinese (Simplified) (2h-ch)       Chinese (Traditional) (2h-thv)       Korean (No)       Spansta (es)       Prench (ft)       German (de)				
Default Language	English (en) V					
Cancel Finished						

3. Click Edit for social-ap, a new browser tab will open

Access is: Profiles / Policies : Access Profiles (Par Session Policies)							
O - Access Prolies Per-Request Policies Policy Sync Customization +							
P Search Create Import.							
V Status * Access Profile Name	· Application	· Profile Type	Per-Bession Policy	Export Co	py Logs	Virtual Bervers	· Partition / Path
D M access		All	(none)	(none) (no	ma)		Common
🗆 🏴 secial-ap		All	Ø Edt	Export Co	py default log-setting		Common
Delete Apply							

4. Click the + between Start and Deny, select OAuth Logon Page from the Logon tab, click Add Item



Beg	gin typing to search		Q
Logo	Mathentication Assignm	ent Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
С	Citrix Logon Prompt	Configure logon options for Citrix clients	
С	External Logon Page	Redirect user to externally hosted form-based web logon page	
D	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication	
C	HTTP 407 Response	HTTP 407 Response for Basic or SPNEGO/Kerberos authentication	
)	Logon Page	Web form-based logon page for collecting end user credentials (used with most deployments)	
۲	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication	
D	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials	
)	VMware View Logon Page	Display logon screen on VMware View clients	
Canc	el Add Item		He

5. Set the Type on Lines 2, 3, and 4 to none

1	Properties* Branch Rules							
,	Name: OAuth Logon Page							
ľ	Logon Page Age	nt						
1	Split domain from		No	~				
lł	CAPTCHA Configu	ration	None					
Ľ								
	Type	Post Variable Nar	ne	Session Variable Name	Clean Variable	Values	Read Only	
	1 radio $\checkmark$	oauthprovidertype		oauthprovidertype	No 🗸	F5;Google;Facebook;Ping;Cus	No $\sim$	
	2 none 🗸	oauthprovidertypero	pc	oauthprovidertyperopc	No 🗸		No $\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!$	
	3 none 🗸	username		username	No 🗸		No 🗸	
	4 none 🗸	password		password	No 🗸		No $^{\vee}$	
	5 none 🗸	field5		field5	No 🗸		No 🗸	

6. Change the Logon Page, Input Field #1 to "Choose a Social Logon Provider"

Customization	Import	t				
Language	en ⊻ Reset all defaults					
Form Header Text	Secure Logon for F5 Networks					
Logon Page Input Field #1	Choose a Social Logon Provider	]				
Input Field #1 Values	=>F5;Google=>Google;Facebook=>Facebook;Ping=>Ping Identity;Custom=>Custom;ROPC=>ROPC dit]					

7. Click the Values column for Line 1, a new window will open.

	Туре	Post Variable Name	Session Variable Name	Clean Variable	Values	Read Only
1	radio 🔻	oauthprovidertype	oauthprovidertype	No 🔻	F5;Google;Facebook;Ping;Cus	No 🔻
					Click Here	

Alternatively, you may click [Edit] on the Input Field #1 Values line. Either item will bring you to the next menu.

Customization	In	nport			
Language	en V Reset all defaults				
Form Header Text	Secure Logon for F5 Networks				
Logon Page Input Field #1	Choose a Social Logon Provider				
Input Field #1 Values F5=>F5;Google=>Google;Facebook=>Facebook;Ping=>Ping Identity;Custom=>Custom;ROPC=>ROPC [cdit]					

8. Click the X to remove F5, Ping, Custom, and ROPC

Lan	guge:		en 🗸
Ad	d Option	Insert after last o	ne 🗸
1	Value F5	Text (Optional)	
2	Google	Google	
	Facebook	Facebook	
4	Ping	Ping Identity	
5	Custom	Custom	
6	ROPC	ROPC	
Ca	ncel Finished		Help

9. Click Finished

Languge:	en 🗸
Add Option	Insert after last one
Value 1 Google 2 Facebook Cancel Finished	Text (Optional) Google Facebook
Properties       Branch Rules         Name:       OAuth Logon Page         Logon Page Agent       Split domain from full Username         Split domain from full Username       No ▼         CAPTCHA Configuration       None ▼         Type       Post Variable Name       Session Variable Name         1 radio       © oauthprovidertype       No ▼	Values Read Only e;Facebook No V

Note: The resulting screen is shown

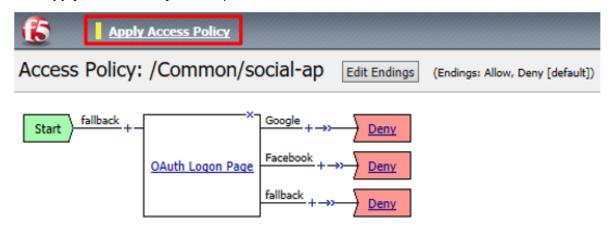
10. Go to the Branch Rules tab and click the X to remove F5, Ping, Custom, F5 ROPC, and Ping ROPC

	Insert Before: 1: F5 V
Name: F5	
Expression: OAuth provider is F5 change	
Name: Google	
Expression: OAuth provider is Google change	
Name: Facebook	• • X
Expression: OAuth provider is Facebook change	
Name: Ping	
Expression: OAuth provider is Ping change	
Name: Custom	
Expression: OAuth provider is Custom change	
Name: F5 ROPC	
Expression: OAuth provider is ROPC AND OAuth ROPC provider is F5ROPC change	
Name: Ping ROPC	
Expression: OAuth provider is ROPC AND OAuth ROPC provider is PingROPC change	
Name: fallback	

#### 11. Click Save

*	
Properties* Branch Rules*	
Add Branch Rule	Insert Before: 1: F5 🛛 🗸
Name: F5	undo
Name: Google	
Expression: OAuth provider is Google change	
Name: Facebook	- • X
Expression: OAuth provider is Facebook change	
Name: Ping	undo
Name: Custom	undo
Name: F5 ROPC	undo
Name: Ping ROPC	undo
Name: fallback	
Cancel Save ("Data in tab has been changed, please don't forget to save)	Help

12. Click Apply Access Policy in the top left and then close the browser tab



# 2.2.4 Task 3: Add the Access Policy to the Virtual Server

1. Go to Local Traffic -> Virtual Servers -> social.f5agility.com-vs

Local Traffic » Virtual Servers : Virtual Server List								
🗱 🚽 Virtual S	erver List	Virtual Add	Iress List	Statist	tics	-		
						_		
*			Sea	arch				
💌 💌 Status	🗕 Name			4	Description	÷		
	dns_host_	resolver						
	social.agil	ity.com-vs						

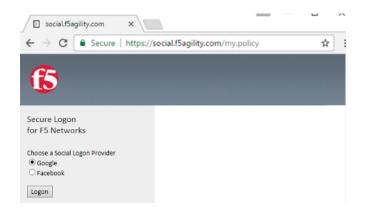
2. Modify the Access Profile setting from none to social-ap and click Update

Access Policy	
Access Profile	social-ap 🗸
Connectivity Profile +	None V
Per-Request Policy	None ~
VDI Profile	None ~
Application Tunnels (Java & Per- App VPN)	Enabled
OAM Support	Enabled
PingAccess Profile	None ~

3. Test access to https://social.f5agility.com from the jump host again, you should now see a logon page requiring you to select your authentication provider. Any attempt to authenticate will fail since we have only deny endings.

Update

Delete



# 2.2.5 Task 4: Google (Built-In Provider)

#### Setup a Google Project

1. Login at https://console.developers.google.com

G Geegle Cloud Platform X +									-	
+ https://console.developers.google.com	C Q, Search	☆ 0	۵	+	÷ C	- 9	<b>n</b> 1-	41.14	ø	-
	Google									
	Sign in to continue to Google Cloud Plat	form								
	Email or phone									
	More options			NEXT						
Englis	ih (United States) 👻	He	p 1	Privacy	Term					

**Note:** This portion of the exercise requires a Google Account. You may use an existing one or create one for the purposes of this lab

2. Click Create Project and give it a name like "OAuth Lab" and click Create

Google APIs	Q,
← Manage Resources 📑 CREATE PROJECT 🗑 DELETE	
No projects match the filter	
Resources pending deletion	

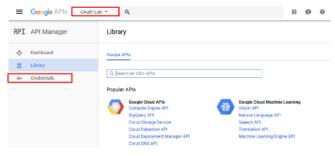


# New Project

Project name 🕜								
OAuth Lab								
Your project ID will be oaut	Your project ID will be oauth-lab-168918 🕜 Edit							
Create Cancel								
Note: You may have existing pro	ojects so the menus may be slightly different.							

Note: You may have to click on Google+ API under Social APIs

3. Go to the Credentials section on the left side.



**Note:** You may have navigate to your OAuth Lab project depending on your browser or prior work in Google Developer

4. Click OAuth Consent Screen tab, fill out the product name with "OAuth Lab", then click save

≡	Google APIs	OAuth Lab 🔻	٩
API	API Manager	C	redentials
¢	Dashboard	c	redentials OAuth consent screen Domain verification
쁐	Library	E	nail address 💿
0+	Credentials	Ē	<this account="" be="" google="" id="" will="" your=""></this>
		P	roduct name shown to users 🛞
			OAuth Lab
		н	omepage URL (Optional)
			https:// or http://
		P	roduct logo URL (Optional)
			http://www.example.com/logo.png
		P	This is how your logo will look to end users Max size: 120x120 px
		0	ptional until you deploy your app
			https:// or http://
			erms of service URL (Optional)
			https:// or http://
			Save Cancel

5. Go to the **Credentials** tab (if you are not taken there), click **Create Credentials** and select **OAuth Client ID** 

≡	Google APIs	0Auth Lab 💌	۹		12	ø
API	API Manager		Credentia	als		
٩	Dashboard	[	redentials	OAuth consent screen Domain verification		
#	Library					
0+	Credentials			APIs Credentials		
				oreactions		
				You need credentials to access APIs. Enable the APIs you plan to use and then create the credentials they require. Depending on the		
				APL you need an API key, a service account, or an CAuth 2.0 client ID. Refer to the API documentation for details.		
				Create credentials *		
				API key Identifies your project using a simple API key to check quota and access		
				OAuth client ID Requests user consent so your app can access the user's data		
				Service account key Enables server-to-server, app-level authentication using robot accounts		
				Help me choose Asiss a few questions to help you decide which type of credential to use		

- 6. Under the Create Client ID screen, select and enter the following values and click Create
  - Application Type: Web Application
  - Name: OAuth Lab
  - Authorized Javascript Origins: https://social.f5agility.com
  - Authorized Redirect URIs: https://social.f5agility.com/oauth/client/ redirect

≡	Google APIs	OAuth Lab 🔻	٩	11	ø
API	API Manager	<del>&lt;</del>	Create client ID		
¢	Dashboard				
#	Library	. v	Veb application		
C*	Credentials	Co. Name	Norder Learn more Signation and an annow Signation and an annow signation and an annow signation and an annow and an a	o after the	× y have

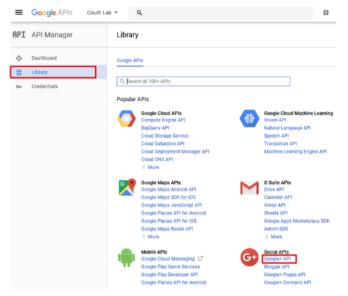
 Copy the Client ID and Client Secret to notepad, or you can get it by clicking on the OAuth Lab Credentials section later if needed. You will need these when you setup Access Policy Manager (APM).

# OAuth client

Here is your client ID

<this be="" client="" id="" specific="" will="" your=""></this>	× 🖸
Here is your client secret	
<this be="" client="" secret="" specific="" will="" your=""></this>	ū

- ок
- 8. Click Library in the left-hand navigation section, then select Google+ API under Social APIs or search for it



9. Click Enable and wait for it to complete, you will now be able to view reporting on usage here

≡	Google APIs aun u	ab *	٩		**	ø	0		I	
API	API Manager	← Goog	le+ API							
φ.	Dashboard	About this				_				~
12	Library			Daca	mentation	Try Inia	API In A	Pile Exp	larer	
Ow.	Credentials	The Googler	API enables developers to build on top of the Google+ platform.							
		Using cred	entials with this API							
		You can acce 2.0 client10.	er dala with OAATh 2.0 na care dala with this APL On the Dredentials page, create an OAath A Celent Di Housets ager consent so that your ago can access user that client ID when making your API call to Receipt Learn more	2-	<b>~</b>			•	2	
				Your app	User con	pert			Uter d	ate.
		You can applic a web applic enables app-	we interaction this API to perform server-to-ear we interaction, for example between alon and disagle benice. You'r need a device account leg, wrich wei assimenticate You'r sito one a nevice account leg, wrich is	• ••		0		•	1	••
		used to autho	stas your API call to Geogle. Learn more	Your service	Authorita	stics		00	ide se	ervice

≡	Google APIs ONLIN La	u- 0, 11 (0 (0	e = (	D
API	API Manager	Coogle+ API Distant		
Φ	Dashboard	Drawlaw Quittas		
33 0~	Library trodentials	About this API Decementation Trythe API in	APts Diplow	×
		If Adhermones     If Adhermones     If Adhermones     If the process in the proceses in the process in the proce	14 days   36 d	1215

10. For Reference: This is a screenshot of the completed Google project:

nr1	API Manager	÷	Client ID for Web ap	plication	2 DOWNLOAD JSON	C RESET SEC
Φ	Dashboard					
쌦	Library	Clien	t ID	<this be<="" td="" will=""><td>our specific client ID&gt;</td><td></td></this>	our specific client ID>	
		Clien	t secret	<this be="" td="" will="" y<=""><td>our specific client secret&gt;</td><td></td></this>	our specific client secret>	
0+	Credentials	Crea	tion date May 27	2017, 12:07:25 PM		
		Restric Enter J	tions exaScript origina, redirect URIs, o	r both		
		Enter J Aut For (htt) the	enaScript origina, redirect URIa, o horized JavaScript origina use with requests from a brows	er. This is the origin UR	of the cleant application. It can't cont by). If you're using a nonatendeed port	
		Enter J Aut For (htt) the	enaScript origina, redirect URIs, o <b>ihorized JavaScript origins</b> use with requests from a brows p.(*.sournple.com) or a path (hi origin URI.	er. This is the origin UR		, you must include it in
		Enter J Acc For (htt the Tr C Acc The The C C C C C C C C C C C C C C C C C C C	wadenpt origne, redivect URIs, et herized JawaStript origine user with request from a brows gu ² /savargle com or a path (No origin URI, bios/Josefal / Sagit My.com http://www.example.com herized redirect UIIIa user with requests from a web herized redirect UIIIa user with requests from a web guit. The path motionate urit. Sagit was on the motionate urit.	er. This is the origin UR tp://www.mple.com/aub erver. This is the path is n will be appended with lative paths. Cannot b	(b) If you're using a nonstandard port your application that users are red in the authorization code for access. M	, you must include it is 
		Enter J Acc For (htt the Tr C Acc The The C C C C C C C C C C C C C C C C C C C	existicant origins, reclevent URIs, e herited JavaScript origins use with requests from a brows up," sample com) or a path (h origin URI. http://social.r5agility.com http://www.example.com herized redirect URIs use with requests from a web s herized redirect URIs	er. This is the origin UR tp://www.mple.com/aub erver. This is the path is n will be appended with lative paths. Cannot b	(b) If you're using a nonstandard port your application that users are red in the authorization code for access. M	, you must include it i

#### Configure Access Policy Manager (APM) to authenticate with Google

1. Configure the OAuth Server Object: Go to Access -> Federation -> OAuth Client / Resource Server -> OAuth Server and click Create

Acce	Access a Foderstion : Okath Cheet I Benzeree Server : Okath Server									
٥.					OAuth Client / Resource Server 👻	PingAccess +				
_										
•		- Search								Create
¥ .	- Name						* Mode	+ Provider	* Application	· Portition / Path
None	cords to display.									
Delet	N									

- 2. Enter the values as shown below for the OAuth Server and click Finished
  - Name: Google
  - Mode: Client + Resource Server
  - Type: Google
  - OAuth Provider: Google
  - **DNS Resolver:** oauth-dns *(configured for you)*
  - Client ID: <Client ID from Google>
  - Client Secret: <Client Secret from Google>
  - Client's ServerSSL Profile Name: apm-default-serverssl
  - Resource Server ID: <Client ID from Google>
  - Resource Server Secret: <Client Secret from Google>

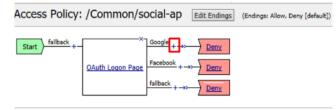
• Resource Server's ServerSSL Profile Name: apm-default-serverssl

Access » Federation : OAuth C	lient / Resource Server : OAuth Server » New OAuth Server Configuration
General Properties	
Name	Google
Description	
Mode	Client + Resource Server V
Туре	Google V
OAuth Provider +	Google ~
DNS Resolver +	oauth-dns V
iRules	Selected Available
Token Validation Interval	60 minutes
Client Settings	·
Client Id	This will be your specific Google client ID>
Client Secret	<this be="" client="" google="" secret="" specific="" will="" your=""></this>
Client's ServerSSL Profile Name	apm-default-serverssl
Resource Server Settings	
Resource Server ID	This will be your specific Google client ID>
Resource Server Secret	<this be="" client="" google="" secret="" specific="" will="" your=""></this>
Resource Server's ServerSSL Profile Name	apm-default-serverssi
Cancel Repeat Finished	

3. Configure the VPE for Google: Go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) and click Edit on social-ap, a new browser tab will open

e - Aconsi	Prolies									
		× See	arts.							wate Import
🗸 💌 Status	* Access			· Application	· Profile Type	Per-Session Policy	Export	Copy	Logs	· Partition / Path
o 🕨	access				All	(none)	(none)	(seec)		Common
D 🕨	secial-ap				All	Ø Edt.	Export	Copy	default-log-setting	Common
Dekta App	ly.									

4. Click the + on the Google provider's branch after the OAuth Logon Page



Add New Macro

5. Select OAuth Client from the Authentication tab and click Add Item

Log	an Authentication Assignm	est) [Endpoint Security (Server-Side)] [Endpoint Security (Client-Side)] [Seneral Purpose]
0	AD Auth	Active Directory authentication of end user credentials
	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
0	LocalDB Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
۲	GAuth Client	OAuth Client
0	OAuth Scope	OAuth Scope
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
0	RADIUS Auth	RADIUS authentication of end user credentials
Cano	Add Item	Ref for the following of a formation of a formation of the formation of th

- 6. Enter the following in the OAuth Client input screen and click Save
  - Name: Google OAuth Client
  - Server: /Common/Google
  - Grant Type: Authorization Code
  - Authentication Redirect Request: /Common/GoogleAuthRedirectRequest
  - Token Request: /Common/GoogleTokenRequest
  - Refresh Token Request: /Common/GoogleTokenRefreshRequest
  - Validate Token Request: /Common/GoogleValidationScopesRequest
  - Redirection URI: https://%{session.server.network.name}/oauth/client/ redirect
  - Scope: profile

Name: Google OAuth Client	
OAuth	
Туре	Client 🗸
Server	/Common/Google 🗸
Grant Type	Authorization code 🗸
Authentication Redirect Request	/Common/GoogleAuthRedirectRequest
Token Request	/Common/GoogleTokenRequest
Refresh Token Request	/Common/GoogleTokenRefreshRequest 🖂
Validate Token Request	/Common/GoogleValidationScopesRequest
Redirection URI	https://%{session.server.network.name}/oauth/client/redirect
Scope	profile

7. Click + on the Successful branch after the Google OAuth Client

	Access Policy			
Access Policy:	/Common/so	ocial-ap	Edit Endings	(Endings: Allow, Deny [default])
Start fallback +-	OAuth Logon Page	Google + →>- Facebook + fallback + ->>	Google OAuth	Client Successful + → <u>Deny</u> fallback + → <u>Deny</u> <u>Deny</u> <u>Deny</u>



8. Select OAuth Scope from the Authentication tab, and click Add Item

Log	Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
0	AD Auth	Active Directory authentication of end user credentials
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
	LocalD6 Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
0	OAuth Client	OAuth Client
۲	OAuth Scope	OAuth Scope
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
0	RADIUS Auth	RADIUS authentication of end user credentials
Cano	el Add Item	MPA Provide loss fastes and collarities of and some and destate.

- 9. Enter the following on the **OAuth Scope** input screen and click **Save** 
  - Name: Google OAuth Scope
  - Server: /Common/Google
  - Scopes Request: /Common/GoogleValidationScopesRequest
- Click Add New Entry
  - Scope Name: https://www.googleapis.com/auth/userinfo.profile
  - Request: /Common/GoogleScopeUserInfoProfileRequest

Properties* Branch Rules			
Name Google GAuth Scope			
OAuth			
Type	Scope 🖂		
Server	/Common/Google 🖂		
Scopes Request	/Common/GoogleValidationSco	zesRequest 💟	
Add new entry			Insert Before: 1 🖂
	Scope Name	Request	
1 [ps://www.googl	eapis.com/auth/userinfo.profile	/Common/GoogleScopeUserinfoProfileRequ 💟	×
Cancel Save *Data in tab ha	s been changed, please don't forget to save)		Help

1. Click the + on the Successful branch after the Google OAuth Scope object



Add New Macro

2. Select Variable Assign from the Assignment tab, and click Add Item

Logo	n Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
0	ACL Assign	Assign existing Access Control Lists (ACLs)	
0	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
0	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
0	BWC Policy	Assign Bandwidth Controller policies	
0	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
0	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	
	LDAP Group Resource Assign	Map AOLs and resources based on user LDAP group membership	
0	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections	
0	Pool Assign	Assign a Local Traffic Pool	
0	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
	Resource Assign	Assign Connectivity Resources	
0	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
۲	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
	VMware View Policy	Specify a policy that will apply to VMware View connections	
Cano	Add Item		Help

3. Name it Google Variable Assign and click Add New Entry then change

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

4. Enter the following values and click Finished

Left Side:

• Type: Custom Variable

- Security: Unsecure
- Value: session.logon.last.username

Right Side:

- Type: Session Variable
- Session Variable: session.oauth.scope.last.scope_data.userinfo.profile. displayName

Custom Variable 🛛 🗸 Unsecure 🗸	= Session Variable V	
ession.logon.last.username	Session Variable Lession.oauth.scope.las	
c	>	

5. Review the Google Variable Assign object and click Save

ſ	roperties") Branch Rules	
Na	me: Google Variable Assign	
v	ariable Assign	
	Add new entry Insert Before	: 1 ×
	Assignment	
1	session.logon.last.username = Session Variable session.oauth.scope.last.scope_data.userinfo.profile.displayN ame <a href="change">change</a>	×
(	ancel Save (Data in tab has been changed, please don't forget to save)	Hel

6. Click **Deny** on the **Fallback** branch after the **Google Variable Assign** object, select **Allow** in the pop up window and click **Save** 

Access Policy; /Common/social-ap Edit Endings (Cridings Allow, Every (default))							
Start Alback +	~	Google + -+o-	Google QAuth Client	1 1	Google DAuth Scope	Search + -++- Google Variable Assign	ack + -++ Deny
	OAuth Logon Page			fallback + -+>			Dany
		Facebook			Select Ending:	_	Deny
		fallback			Allow		
		+-+>			O Deny 🖬		Deny
					Cancel Save	Help	

7. Click Apply Access Policy in the top left and then close the tab

6	Apply Access Policy	
Access	Policy: /Common/se	OCial-ap Edit Endings (Endings: Allow, Deny (default))
Start )-	Oluth Legan Page	Google +

#### **Test Configuration**

1. Test by opening Chrome in the jump host and browsing to https://social.f5agility.com, select the provider and attempt logon.

social.f5agility.com	x ×	_	
← ⇒ C   Sec	ure https://social.f5agility.com/my	y.policy	☆ :
	G Sign in - Google Accounts × +		, u
Secure Logon for F5 Networks Choose a Social Logon Prov © Google Facebook Logon Logon	The http://xxxurit.google.     C Q, Search      Google      Sign in     to continue to flagsify.com      trace r prove      More options	<u></u>  ₩CXT	

**Note:** You are able to login and reach the app now, but SSO to the app has not been setup so you get an application error.

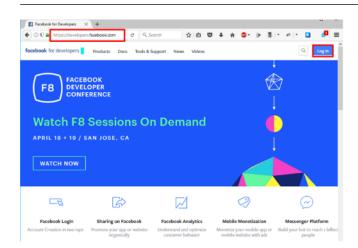
**Note:** You may also be prompted for additional security measures as you are logging in from a new location.

## 2.2.6 Task 5: Facebook (Built-In Provider)

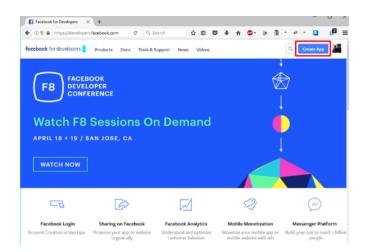
#### Setup a Facebook Project

1. Go to https://developers.facebook.com and Login

**Note:** This portion of the exercise requires a Facebook Account. You may use an existing one or create one for the purposes of this lab



2. If prompted click, Get Started and accept the Developer Policy. Otherwise, click Create App



3. Click **Create App** and name (**Display Name**) your app (Or click the top left project drop down and create a new app, then name it). Then click **Create App ID**.

**Note:** For example the **Display Name** given here was "OAuth Lab". You may also be prompted with a security captcha

Create a New App ID Get started integrating Facebook into your app or website	
Display Name OAuth Lab Contact Email	
< Your Facebook Account ID >	
By proceeding, you agree to the Facebook Platform Policies	Cancel Create App ID

4. Click **Get Started** in the **Facebook Login** section (*Or click + Add Product and then Get Started for Facebook*)

🚯 OAuth Lab 🔹	APPID: < Your App ID > -* View Analytics	
	Let us help you find new ways to grow your app. Click term to talk to our support to	an x
Settings		
	Product Setup	
App Review	Facebook Login The work's revenue ne social logic product Read Decommendation	Get Started
+ Add Product	Audience Network Manthe par make apper worker with ratio advisers 3 million Facebook advisitions. Raid Discenterial	Get Started
	Analytics Undertand the propile support with your business across apps, devices, platforms and waterbass. Read Occumentation	Get Started

5. From the "Choose a Platform" screen click on WWW (Web)



6. In the *"Tell Us about Your Website"* prompt, enter https://social.f5agility.com for the Site URL and click Save then click Continue

iOS	Android	Web	Other
1. Tell Us about You	ır Website		
Tell us what the URL	of your site is.		
Site URL			
https://social.f5a	gility.com		
			Save
			Continue

7. Click Next on the "Set Up the Facebook SDK for Javascript" screen

nstalled, instead yo	for JavaScript doesn't have any standalone files that need u simply need to include a short piece of regular JavaScript d the SDK into your pages. The async load means that it do ge.	t in your HTML that will
ommon defaults. Y	et of code will give the basic version of the SDK where the ou should insert it directly after the opening body> tag on	
		•
<script></td><td></td><td>Copy Code</td></tr><tr><td></td><td><pre>ncInit = function() {</pre></td><td>Copy Code ^</td></tr><tr><td>window.fbAsy FB.init({</td><td></td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId</td><td>: '178071772721497',</td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId cookie</td><td>: '178071772721497', : true,</td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId cookie xfbml</td><td>: '178071772721497', : true, : true,</td><td>Copy Code 💧</td></tr><tr><td>window.fbAsy FB.init({ appId cookie</td><td>: '178071772721497', : true, : true,</td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId cookie xfbml</td><td>: '178071772721497', : true, : true,</td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId cookie xfbml</td><td>: '178071772721497', : true, : true,</td><td>Copy Code</td></tr><tr><td>window.fbAsy FB.init({ appId cookie xfbml</td><td>: '178071772721497', : true, : true,</td><td>Copy Code</td></tr></tbody></table></script>		

8. Click Next on the "Check Login Status" screen

Note: Additional screen content removed.

#### 3. Check Login Status

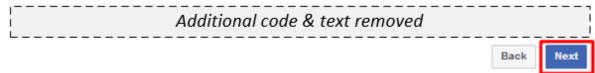
The first step when loading your web page is figuring out if a person is already logged into your app with Facebook login. You start that process with a call to FB.getLoginStatus. That function will trigger a call to Facebook to get the login status and call your callback function with the results.

Taken from the sample code above, here's some of the code that's run during page load to check a

Additional code & text removed		
dialog with FB.login() or show them the Login Button.		
	Back	Next

- 9. Click Next on the "Add the Facebook Login Button" screen
  - 4. Add the Facebook Login Button

Including the Login Button into your page is easy. Visit the documentation for the login button and set the button up the way you want. Then click Get Code and it will show you the code you need to display the button on your page.



10. Click **Facebook Login** on the left side bar and then click **Settings** 

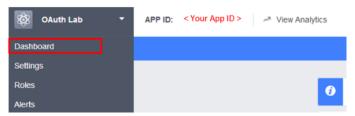
Your App ID X 🥔 View Analytics		
	Let us help you find new ways to graw your app. Click here to talk to our i	upport leases as
	IOS Android Web	Othe
		_
	1. Tell Us about Your Website	
	2. Set Up the Facebook SDK for Javascript	
	3. Check Login Status	
	4. Add the Facebook Login Button	
	5. Next Steps	
	3. Here soge	
	Congrats, you've added Facebook Login to year website! Be sure to check ex documentation pages for more advanced guides.	tourother
	Login Gialog 😳	
	Invoke the Login Citalog using your own botton instead of the Facebook Login	button.
	Access Tokens 🖾	
	Use the Access Tokens generated by Facebook Login for your website.	
	Permissions (3	
	Manage what data your app has access to through Facebook Login.	
	App Beview 🖸	
	Submit your app for review to ensure the best possible Facebook experience audience.	for your app's

11. For the Client OAuth Settings screen in the Valid OAuth redirect URIs enter https://social. f5agility.com/oauth/client/redirect and then click enter to create it, then Save Changes

ient OAuth	Settings
Yes	Client OAuth Login Enables the standard OAuth client token flow. Secure your application and prevent abuse by locking down which token refered URIs are allowed with the options below. Disable globally if not used. (19
Yes	Web OAuth Login         Force Web OAuth Reauthentication           Enables web based OAuth client login for building custem login flows. [7]         No
No	Embedded Browser OAuth Login Enables browser control redirect un for OAuth client login. (?)
/alid OAuth i	redirect URIs
https://social	.f5agility.com/oauth/client/redirect ×
No	Login from Devices Enables the Okuth client login flow for devices like a smart TV (*)
authorize	
Deauthorize	Callback URL

12. Click Dashboard in the left navigation bar

Dashboard



13. Here you can retrieve your App ID and App Secret for use in Access Policy Manager (APM).

	OAuth La This app is in developm API Version [?]	b O ent mode and can only be used by app admins, developers and testers 1?1 App ID
	v2.9	< Your App ID >
	App Secret	Show

Screenshot of completed Facebook project

**Note:** If you want Facebook Auth to work for users other than the developer you will need to publish the project

#### Configure Access Policy Manager (APM) to authenticate with Facebook

1. Configure the OAuth Server Object: Go to Access -> Federation -> OAuth Client / Resource Server -> OAuth Server and click Create

	ARCENS IN EINERSTON CONTROL CONTROL OF STREET									
۰.					ONUT CIERT Resource Server -					
Ŀ.,		< Search								Create
0	<ul> <li>Name</li> </ul>						* Mode	+ Provider	Application	Paration / Path
	Geogle						Client - Resource Server	Geogle		Common
Deb	ita									

- 2. Enter the values as shown below for the OAuth Server and click Finished
  - Name: Facebook
  - Mode: Client + Resource Server
  - Type: Facebook
  - OAuth Provider: Facebook
  - DNS Resolver: oauth-dns (configured for you)
  - Client ID: <App ID from Facebook>
  - Client Secret: <App Secret from Facebook>
  - Client's ServerSSL Profile Name: apm-default-serverssl
  - Resource Server ID: " App ID from Facebook>"
  - Resource Server Secret: <App Secret from Facebook>
  - Resource Server's ServerSSL Profile Name: apm-default-serverssl

Access » Federation : OAuth Client / Resource Server : OAuth Server » New OAuth Server Configuration...

General Properties	
Name	Facebook
Description	
Mode	Client + Resource Server V
Туре	Facebook V
OAuth Provider +	Facebook
DNS Resolver +	oauth-dns 🗸
iRules	Selected     Available       Image: Constraint of the system of th
Token Validation Interval	60 minutes
Client Settings	
Client Id	< This will be your specific Facebook App ID >
Client Secret	< This will be your specific Facebook App Secret >
Client's ServerSSL Profile Name	apm-default-serverssl
Resource Server Settings	
Resource Server ID	< This will be your specific Facebook App ID >
Resource Server Secret	< This will be your specific Facebook App Secret >
Resource Server's ServerSSL Profile Name	apm-default-serverssl 🗸
Cancel Repeat Finished	

3. Configure the VPE for Facebook: Go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) and click Edit on social-ap, a new browser tab will open

Access 14 Profiles ( Policies : Access Profiles (Per-Session Policies)								
Access Probles Per-Request Policies Policy Sync Customization +								
	-							
× Search							C	reale Import
v'  Status  Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Cepy	Logs	Virtual Servers	· Partition / Path
🗅 🏴 acons		All	(see)	(seet)	(none)			Common
🔰 🕨 social-ap		All	Ø Edt.	Export	Copy	default-log-setting		Common
Delote Apply								

4. Click the + on the Facebook provider's branch after the OAuth Logon Page

Access Policy: /Common/s	ocial-ap Edit Endings (Endin	ings: Allow, Deny [default])
QAuth Logen Page	Geogle GAuth Client	Socreeful + -e- Socreeful + -e- Social Olub Scale Solited + -e- Debod + -e- Debod Social Vaciable Aussi Solited + -e- Debod Social Vaciable Aussi Social Vacial Vaciable Auss

Add New Macro

5. Select OAuth Client from the Authentication tab and click Add Item

Logo	an Authentication Assignm	nent) Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
)	AD Auth	Active Directory authentication of end user credentials
)	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
0	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
0	LocalDB Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
۲	OAuth Client	OAuth Client
0	OAuth Scope	OAuth Scope
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcade (OTP)
	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
0	RADIUS Auth	RADIUS authentication of end user credentials
Canc	el Add Item	BPA Franklin kan faster antikenkline of and anno an deskele

- 6. Enter the following in the OAuth Client input screen and click Save
  - Name: Facebook OAuth Client
  - Server: /Common/Facebook
  - Grant Type: Authorization Code
  - Authentication Redirect Request: /Common/FacebookAuthRedirectRequest
  - Token Request: /Common/FacebookTokenRequest
  - Refresh Token Request: None
  - Validate Token Request: "/Common/FacebookValidationScopesRequest"
  - Redirection URI: https://%{session.server.network.name}/oauth/client/ redirect
  - Scope: public_profile (Note underscore)

Properties* Branch Rules	
Name: Facebook OAuth Client	
OAuth	
Туре	Client V
Server	/Common/Facebook 🗸
Grant Type	Authorization code \vee
Authentication Redirect Request	/Common/FacebookAuthRedirectRequest $ \smallsetminus $
Token Request	/Common/FacebookTokenRequest 🗸
Refresh Token Request	None 🗸
Validate Token Request	/Common/FacebookValidationScopesRequest \vee
Redirection URI	https://%{session.server.network.name}/oauth/client/redirect
Scope	public_profile
Cancel Save (#Data in tab bas bas	an channed please don't forget to save)

7. Click + on the Successful branch after the Facebook OAuth Client

Access Policy: /Common/social-ap EditEntings (Groups Deers (default), Alos)								
Start	Conde 1-00- Conde							
QAUCH Las	tallaud: p-et-							
	ALDRAK Brontout +							
	falladi, o - p							

8. Select OAuth Scope from the Authentication tab, and click Add Item

Logo	n Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
0	AD Auth	Active Directory authentication of end user credentials
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 101 Response action
0	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
	LocalD6 Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
0	OAuth Client	OAuth Client
۲	OAuth Scope	OAuth Scope
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
0	RADIUS Auth	RADIUS authentication of end user credentials
Cance	el Add Item	MPA ParentPoliser Baston and antication of an discussion and addate

- 9. Enter the following on the OAuth Scope input screen and click Save
  - Name: Facebook OAuth Scope
  - Server: /Common/Facebook
  - Scopes Request: /Common/FacebookValidationScopesRequest
  - Click Add New Entry

Add New Macro

- Scope Name: public_profile
- Request: /Common/FacebookScopePublicProfile

Properties* Branch Rules							
Name: Facebook QAuth Scope							
OAuth							
Туре	Scope 🖂						
Server	Server //Common/Facebook >/						
Scopes Request	/Common/FacebookValidationS	copesRequest 🗹					
Add new entry			Insert Before: $\underline{1 \lor}$				
Scope Name		Request					
1 public_profile		/Common/FacebookScopePublicProfile V	×				
Cancel Save ("Data in tab has been changed, please don't forget to save)							

10. Click the + on the Successful branch after the Facebook OAuth Scope object



11. Select Variable Assign from the Assignment tab, and click Add Item

	ACL Assign	Assign existing Access Control Lists (ACLs)
)	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership
)	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs
)	BWC Policy	Assign Bandwidth Controller policies
D	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop
D	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP
D	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership
D	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections
С	Pool Assign	Assign a Local Traffic Pool
D	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway
С	Resource Assign	Assign Connectivity Resources
D	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings
D	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables
•	Variable Assign	Assign custom variables, configuration variables, or predefined session variables
0	VMware View Policy	Specify a policy that will apply to VMware View connections

12. Name it Facebook Variable Assign and click Add New Entry then change

Properties* Branch Rules						
Names Facebook Variable Assign						
Variable Assign						
Add new entry Insert Before:	1 ~					
Assignment						
1 empty change	×					
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help					

13. Enter the following values and click Finished

Left Side:

- Type: Custom Variable
- Security: Unsecure
- Value: session.logon.last.username

Right Side:

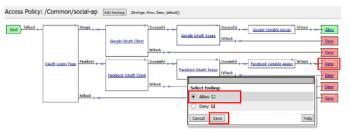
- Type: Session Variable
- Session Variable: session.oauth.scope.last.scope_data.public_profile.name

Custom Variable VInsecure V	= Session Variable
session.logon.last.username	Session Variable
Cancel Finished	Help

14. Review the Facebook Variable Assign object and click Save

Vame: Facebook Variable Assign		
Variable Assign		
Add new entry	Insert Befor	re: 1 ~
	Assignment	
session.logon.last.username = Session Va change	riable session.oauth.scope.last.scope_data.public_profile.name	2
Cancel Save T*Data in tab has been ch	anged, please don't forget to save)	H

15. Click **Deny** on the **Fallback** branch after the **Facebook Variable Assign** object, select **Allow** in the pop up window and click **Save** 



16. Click Apply Access Policy in the top left and then close the tab

6	Apple	Access Policy						
Acces	Access Policy: /Common/social-ap Edit Endings (Endings Alien, Deny [default])							
Start	failback + _	OAuth Logen Page	Google +	Google DAuth Client 	Successful + -++- falback + -+) Successful + -++- falback + -+0	Geogle OAuth Scope	Scould +	

# 2.2.7 Test Configuration

1. Test by opening Chrome in the jump host and browsing to https://social.f5agility.com, select the provider and attempt logon.

	I Log into Facebook   Facebook   Facebook
<b>f</b>	(€) ① ① ▲ https://www.facebook.com/ ○ ○ ♀ Search ☆ □ □ ↓ ★ ◎ ▼
	facebook 📟
Secure Logon for F5 Networks	
Choose a Social Logon Provi	Log into Facebook
<ul> <li>Google</li> <li>Facebook</li> </ul>	Email or Phone Number
Logon	Log In
	Create New Account
1	Not now

Note: You are able to login and reach the app now, but SSO to the app has not been setup so you

get an application error.

**Note:** You may also be prompted for additional security measures as you are logging in from a new location

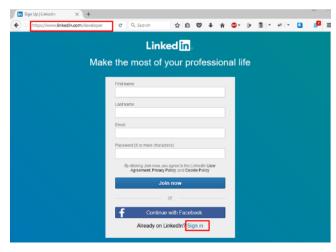
Note: You may need to start a Chrome New Incognito Window so no session data carries over.

You should be prompted to authorize your request. Click Continue as <Account> (Where <Account> is your Facebook Profile name)



## 2.2.8 Task 6: LinkedIn (Custom Provider)

1. Login at https://www.linkedin.com/secure/developer



**Note:** This portion of the exercise requires a LinkedIn Account. You may use an existing one or create one for the purposes of this lab*

2. Click Create Application

			- Handling
		reate Ap	plication
			Create Ap

Manage your desktop and mobile applications that leverage Linkedin APIs.

3. In the Create a New Application screen fill in the required values and click Submit

Create a New Application
Company Name:
My Company
Name:
OAuth Lab
Description:
QAuth Lab Exercise
a.
Application Logo:
Select File to Upload
Application Use: * Other
Website URL:
https://www.mycompany.com/info
Business Email:
user@mycompany.com
Business Phone:
5555551212
have read and agree to the LinkedIn API Terms of Use.
Submit

Note: Generic values have been shown. You may use the values you deem appropriate

Note: An Application logo has been provided on your desktop 'OAuth2.png'

- 4. In the "Authentication Keys" screen, check the boxes for r_basicprofile and r_emailaddress. In the Authorized Redirect URLs, enter https://social.f5agility.com/oauth/client/ redirect
- 5. Click Add. Finally, click Update at the bottom of the screen.

Authentication K	eys
------------------	-----

Client ID:	< Your Client ID >						
Client Secret:	< Your Client Secret >						
Default Applic r_basicprofile w_share	ation Permissions <mark>©r_</mark> emailaddress	<pre>rw_company_admin</pre>					
OAuth 2.0							
Authorized Redirect U	RLs:						
https://social.f5agility.co	om/oauth/client/redirect	Add					
OAuth 1.0a							
Default "Accept" Redir	ect URL:						
Default "Cancel" Redir	ect URL:						
Update	I						

#### Configure Access Policy Manager (APM) to authenticate with LinkedIn

1. Configure the OAuth Server Object: Go to Access -> Federation -> OAuth Client / Resource Server -> Provider and click Create

ľ	Access in Federation : Ukath Chand Hassiance Server : Premiter									
ľ		SAML Service Provider      SAML Identity Provider      1	14ML Recourses OAuth Authoriz	zation Server =	OAwth Client / Resource Server	<ul> <li>PingAccess</li> </ul>				
		Bearch								Create
Ì	1	+ Narro					© Type	OAuth Servers	* Application	· Parties / Path
	1	F5					FS			Common
		Facebook					Facebook	Facebook		Common
		Google					Google	Google		Common
		Fire					Ping			Common
j	hale	eba								

#### Note: You are creating a "Provider"

- 2. Enter the values as shown below for the OAuth Provider and click Finished
  - Name: LinkedIn
  - Type: Custom
  - Authentication URI: https://www.linkedin.com/oauth/v2/authorization
  - Token URI: https://www.linkedin.com/oauth/v2/accessToken
  - Token Validation Scope URI: https://www.linkedin.com/v1/people/~

Access » Federation : OAuth Client / Resource Server : Provider » New Provider						
General Properties						
Name	LinkedIn					
Description						
Туре	Custom V					
Authentication URI	https://www.linkedin.com/oauth/v2/authorization					
Token URI	https://www.linkedin.com/oauth/v2/accessToken					
Token Validation Scope URI	https://www.linkedin.com/v1/people/~					
Cancel Repeat Finished						

3. Configure the OAuth Redirect Request Profile Object: Go to Access -> Federation -> OAuth Client / Resource Server -> Request and click Create

Access + Federation : Glady Client / Bencence Server : Request					
SAME Service Provider + SAME Identity Provider + SAME Resources Oxfuth Authorization Server + OAuth Client / Resource Server + ProjAccess					
				_	
- Easth				Create	
✓ A Kane	Copy	+ Type	* Application	+ Partition / Pat	
C FAutrAndrechtegunt	Capy .	auth-redirect-request		Common	
C F50conReawst	Cepy	validation-scopes-request		Common	
FSTokenRatheshRequest	Capy	token-refresh-request		Common	
E FSTokerRequestRyNuthzCode	Copy .	token-request		Common	
0 EXTechnicate and the Comment	1000	taken excused		Common	

- 4. Enter the values as shown for the OAuth Request and click Finished
  - Name: LinkedInAuthRedirectRequest
  - HTTP Method: GET
  - Type: auth-redirect-request

## Access » Federation : OAuth Client / Resource Server : Request » New Request...

General Properties	
Name	LinkedInAuthRedirectRequest
Description	
Request Settings	
HTTP Method	GET V
Туре	auth-redirect-request
Add values here.	Parameter Type: custom  Parameter Name: Parameter Value: Add Custom   response_type   code client-id   client_id redirect-uri   redirect_uri scope   scope Edit Delete
Request Headers	Header Name: Header Value: Add Edit Delete
Cancel Repeat Finished	

- 5. Add the following request parameters and click **Add** after entering the values for each:
  - Parameter Type: custom
  - Parameter Name: response_type
  - Parameter Value: code

- Parameter Type: client-id
- Parameter Name: client_id
- Parameter Type: redirect-uri
- Parameter Name: redirect_uri
- Parameter Type: scope
- Parameter Name: scope

Note: LinkedIn requires a state parameter, but we already insert it by default.

Parameter Type:	custom ~
Parameter Name:	response_type
Parameter Value:	code
Add	
Parameter Type:	client-id ~
Parameter Name:	client_id
Add	
Parameter Type:	redirect-uri ~
Parameter Name:	redirect_uri
Add	
Parameter Type:	scope ~
Parameter Name:	scope
Add	

6. Configure the OAuth Token Request Profile Object: Go to Access -> Federation -> OAuth Client /

# Resource Server -> Request and click Create



- 7. Enter the values as shown for the OAuth Request and click Finished
  - Name: LinkedInTokenRequest
  - HTTP Method: POST
  - Type: token-request

Access » Federation : OAuth (	Client / Resource Server : Request » New Request
General Properties	
Name	LinkedInTokenRequest
Description	
Request Settings	
HTTP Method	POST V
Type Add	token-request V
Request Parameters	Parameter Type: Client-secret
Request Headers	Header Name: Header Value: Add Edit Delete
Cancel Repeat Finished	

- 8. Add the following request parameters and click Add after entering the values for each:
  - Parameter Type: grant-type
  - Parameter Name: grant_type
  - Parameter Type: redirect-uri
  - Parameter Name: redirect_uri

- Parameter Type: client-id
- Parameter Name: client_id
- Parameter Type: client-secret
- Parameter Name: client_secret

Parameter Type: grant-type 🗸								
Parameter Name: grant_type								
Add								
Parameter Type: redirect-uri V								
Parameter Name: redirect_uri								
Add								
Parameter Type: client-id ~								
Parameter Name: client_id								
Add								
Deservation Transv. Infrant as wet								
Parameter Type: client-secret ~								
Parameter Name: client_secret								
Add								

9. Configure the OAuth Validation Scopes Request Profile Object: Go to Access -> Federation -> OAuth Client / Resource Server -> Request and click Create

	Access + Federation : OAldh Chent / Research Server : Request									
	SAML Senice Provider + SAML detilly Provider + SAML Resources OAuth Autorization Server + OAuth Client / Resource Server + ProgAccess +									
					_					
1	- David				Create.					
4	* Kare	Copy	+ Type	* Application	+ Pattion / Patt					
	F&ut#IndextReport	Copy	auth-redirect-request		Common					
	EStoonPresent	Cepy	validation-scopes-request		Common					
	FSTokenReheahRequest	Copy	token-refresh-request		Common					
	FSTokenRequestRyAuttzCode	Capy	token-request		Common					
	EST-classifier and and the second	1000	Initian concept		Common					

- 10. Enter the values as shown for the **OAuth Request** and click **Finished** 
  - Name: LinkedInValidationScopesRequest
  - HTTP Method: GET
  - Type: validation-scopes-request

Access » Federation : OAuth O	Client / Resource Server : Request » New Request
General Properties	
Name	LinkedInValidationScopesRequest
Description	
Request Settings	
HTTP Method	GET 🗸
Туре	validation-scopes-request ~
Add values here.	Parameter Type: custom ✓ Parameter Name: Parameter Value: Add Custom   oauth2_access_token   %{session.oauth.client.last.access_toke^ custom   format   json
Request Headers	Header Name: Header Value: Add Edit Delete
Cancel Repeat Finished	

- 11. Add the following request parameters and click **Add** after entering the values for each:
  - Parameter Type: custom
  - Parameter Name: oauth2_access_token
  - Parameter Value: %{session.oauth.client.last.access_token}
  - Parameter Type: custom

- Parameter Name: format
- Parameter Value: json

Parameter Type:	custom 🗸
Parameter Name:	oauth2_access_token
Parameter Value:	%{session.oauth.client.last.access_token}
Add	
Parameter Type:	custom ~
Parameter Name:	format
Parameter Value:	json
Add	

12. Configure the OAuth Scope Data Request Profile Object: Go to Access -> Federation -> OAuth Client / Resource Server -> Request and click Create

Access in Federative : Otath Chert / Researce Server : Request.									
🗴 x SAML Service Provider * SAML Identity Provider * SAML Descurses OAuth Authorization Server * OAuth Client / Resource Server * Prophocess *									
- Easth				Create.					
A Nore	Copy	+ Tipe	* Application	Parttion / Path					
E FAshfordinghapant	Copy .	auth-redirect-request		Common					
E FS5coosRequest	Copy	validation-scopes-request		Common					
E FSTokenRatheahRequest	Copy	token-refresh-request		Common					
E FSTokenRequedEpAultsCode	Copy	token-request		Common					
C EFfetenitement	Para	Initian associate		Common					

- 13. Enter the values as shown for the OAuth Request and click Finished
  - Name: LinkedInScopeBasicProfile
  - HTTP Method: GET
  - URI: https://api.linkedin.com/v1/people/~
  - Type: scope-data-request

Access » Federation : OAuth Client / Resource Server : Request » New Request							
General P	roportion						
Name	Topernes	LinkedInScopeBasicProfile					
Descripti	on						
Request S	ottinge						
HTTP Me		GET 🗸					
Туре		scope-data-request					
URI		https://api.linkedin.com/v1/people/~					
Request	Add values here.	Parameter Type: custom  Parameter Name: Parameter Value: Add custom   oauth2_access_token   %{session.oauth.client.last.access_toke custom   format   json Edit Delete					
Request		Header Name: Header Value: Add Edit Delete					
Cancel	Repeat Finished						

- 14. Add the following request parameters and click **Add** after entering the values for each:
  - Parameter Type: custom
  - Parameter Name: " oauth2_access_token"
  - Parameter Value: %{session.oauth.client.last.access_token}

- Parameter Type: custom
- Parameter Name: format
- Parameter Value: json

Parameter Type:	custom V
Parameter Name:	oauth2_access_token
Parameter Value:	%{session.oauth.client.last.access_token}
Add	
Parameter Type:	custom 🗸
Parameter Name:	format
Parameter Value:	json
Add	

15. Configure the OAuth Server Object: Go to Access -> Federation -> OAuth Client / Resource Server -> OAuth Server and click Create



- 16. Enter the values as shown below for the OAuth Server and click Finished
  - Name: LinkedIn
  - Mode: Client + Resource Server
  - Type: Custom
  - OAuth Provider: LinkedIn
  - **DNS Resolver:** oauth-dns * (configured for you) *
  - Client ID: <App ID from LinkedIn>
  - Client Secret: < App Secret from LinkedIn >
  - Client's ServerSSL Profile Name: apm-default-serverssl
  - Resource Server ID: <App ID from LinkedIn >
  - Resource Server Secret: <App Secret from LinkedIn >
  - Resource Server's ServerSSL Profile Name: apm-default-serverssl

Access » Federation : OAuth C	lient / Resource Server : OAuth Server » New OAuth Server Configuration
General Properties	
Name	LinkedIn
Description	
Mode	Client + Resource Server V
Туре	Custom
OAuth Provider +	Linkedin V
DNS Resolver +	oauth-dns 🗸
iRules	Selected Available //CommonSys_APM_ExchangeSupport_OA_BasicAuthSys_APM_ExchangeSupport_Nelper
Token Validation Interval	60 minutes
Client Settings	
Client Id	< This will be your specific LinkedIn App ID >
Client Secret	< This will be your specific LinkedIn App Secret >
Client's ServerSSL Profile Name	apm-default-serverssl
Resource Server Settings	
Resource Server ID	< This will be your specific LinkedIn App ID >
Resource Server Secret	< This will be your specific LinkedIn App Secret >
Resource Server's ServerSSL Profile Name	apm-default-serverssi 🗸
Cancel Repeat Finished	

17. Configure the VPE for LinkedIn: Go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) and click Edit on social-ap, a new browser tab will open

Access a Profiles (Policies : Access Profiles (Per Session Policies)													
	Acons	Probles											
•			× Sec	ar ch								4	Create Import
¥	* Status	* Access	Profile Name			+ Application	· Profile Type	Per-Session Policy	Export	Cepy	Logs	Virtual Servers	Partition / Path
	<b>H</b>	access					All	(see)	(seec)	(none)			Common
	14	social-ap					All	Edt.	Export	Copy	default-log-setting		Common
Dele	12 A00	xy .											

18. Click on the link OAuth Logon Page as shown



19. Click on the Values area of Line #1 as shown. A pop-up window will appear

	Туре	Post Variable Name	Session Variable Name	Clean Variable	Values	Read Only
1	$radio \sim$	oauthprovidertype	oauthprovidertype	No 🗸	Google;Facebook	No $\checkmark$
2	none $\checkmark$	oauthprovidertyperopc	oauthprovidertyperopc	No 🗸		No $\sim$
3	none $\checkmark$	username	username	No 🗸		No 🗸
4	none $\checkmark$	password	password	No 🗸		$[\rm No~ \checkmark]$
5	none $\checkmark$	field5	field5	No \vee		$\rm No~ \simeq$

20. Click Add Option. In the new Line 3, type LinkedIn in both the Value and Text (Optional) fields and click Finished

Languge: en ∨				
Add	Add Option Insert after last one			
	Value	Text (Optional)		
1	Google	Google	V X	
2 3	Facebook	Facebook		
3	LinkedIn	LinkedIn		
Cancel Finished Help				

21. Click on the Branch Rules tab of the OAuth Logon Page screen

ſP	roperties* Bra	nch Rules				
Na	me: OAuth Logo	n Page				
Ŀ	ogon Page Age	nt				
S	Split domain from full Username No 🗸					
c	CAPTCHA Configuration None V					
	Туре	Post Variable Name	Session Variable Name	Clean Variable	Values	Read Only
1		oauthprovidertype	oauthprovidertype	No V	Google;Facebook;LinkedIn	No V
2	none 🗸	oauthprovidertyperopc	oauthprovidertyperopc	No 🗸		No 🗸

22. Click Add Branch Rule. In the resulting new line enter LinkedIn for the Name field and click the Change link on the Expression line

Properties* Branch Rules*	
Add Branch Rule	Insert Before: 1: LinkedIn 🛛 🗠
Name	×
Name: Google	A V X
Expression: OAuth provider is Google <u>change</u> Name: Facebook	A X
Expression: OAuth provider is Facebook change Name: fallback	
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help

23. Click Add Expression on the Simple tab

Simple Advance	d	
Add Expression		

24. Select OAuth Logon Page in the **Agent Sel:** drop down. Select OAuth provider type from the **Condition** drop down. In the **OAuth provider** field enter LinkedIn and then click **Add Expression** 

Simple	
Agent Sel:	OAuth Logon Page
Condition:	OAuth provider type 🗸 🗸
	wider is LinkedIn
Cancel	Add Expression

25. Click Finished on the Simple Expression tab

Simple* Advanced	
OAuth provider is LinkedIn	x
AND Add Expression	
OR	

Add Expression	
Cancel Finished	Help

26. Click Save on the completed Branch Rules tab

Properties* Branch Rules*		_
Add Branch Rule	Insert Before: 1: LinkedIn	$\sim$
Name: LinkedIn		×
Expression: OAuth provider is LinkedIn change		
Name: Google		×
Expression: OAuth provider is Google <u>change</u>		
Name: Facebook		×
Expression: OAuth provider is Facebook change		
Name: fallback		
Cancel Save *Data in tab has been changed, please don't forget to save)	ŀ	lelp

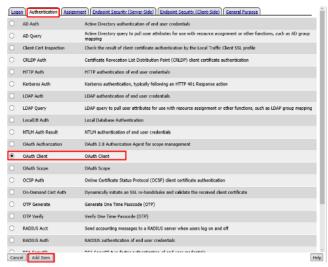
27. Click the + on the LinkedIn provider's branch after the OAuth Logon Page



Note: If not still in the VPE: Go to Access -> Profiles / Policies -> Access Profiles (Per Session

Policies). Click Edit on social-ap, a new browser tab will open*

28. Select OAuth Client from the Authentication tab and click Add Item

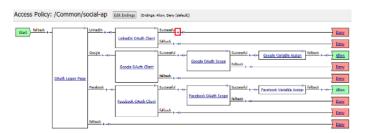


- 29. Enter the following in the OAuth Client input screen and click Save
  - Name: LinkedIn OAuth Client
  - Server: /Common/LinkedIn
  - Grant Type: Authorization Code
  - Authentication Redirect Request: /Common/LinkedInAuthRedirectRequest
  - Token Request: /Common/LinkedInTokenRequest
  - Refresh Token Request: None
  - Validate Token Request: /Common/LinkedInValidationScopesRequest
  - Redirection URI: https://%{session.server.network.name}/oauth/client/ redirect

<ul> <li>Scope: r_basicprofile</li> </ul>	*(Note	underscore)	*
-------------------------------------------	--------	-------------	---

Properties* Branch Rules	
Name: LinkedIn OAuth Client	
OAuth	
Туре	Client V
Server	/Common/LinkedIn 💟
Grant Type	Authorization code \vee
Authentication Redirect Request	/Common/LinkedInAuthRedirectRequest 🖂
Token Request	/Common/LinkedInTokenRequest
Refresh Token Request	None ~
Validate Token Request	/Common/LinkedInValidationScopesRequest \vee
Redirection URI	https://%{session.server.network.name}/oauth/client/redirect
Scope	r_basicprofile
Cancel Save (*Data in tab has been changed,	please don't forget to save)

30. Click + on the Successful branch after the LinkedIn OAuth Client



31. Select OAuth Scope from the Authentication tab, and click Add Item

Log	on Authentication Assignm	nent   Endpoint Security (Server-Side)   Endpoint Security (Client-Side)   General Purpose
0	AD Auth	Active Directory authentication of end user credentials
0	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile
0	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
0	HTTP Auth	HTTP authentication of end user credentials
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
0	LDAP Auth	LDAP authentication of end user credentials
0	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mappin
0	LocalDB Auth	Local Database Authentication
0	NTLM Auth Result	NTLM authentication of end user credentials
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
0	OAuth Client	QAuth Client
۲	OAuth Scope	OAuth Scope
0	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
0	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
	RADIUS Auth	RADIUS authentication of end user credentials
Cani	tel Add Item	MAR Presidenting for the antiparticular of and announced antiparticle

- 32. Enter the following on the OAuth Scope input screen and click Save
  - Name: LinkedIn OAuth Scope
  - Server: /Common/LinkedIn
  - Scopes Request: /Common/LinkedInValidationScopesRequest
  - Click Add New Entry
  - Scope Name: r_basicprofile
  - Request: /Common/LinkedInScopeBasicProfile

Properties* Branch Rules				
Name LinkedIn OAuth Scope				
OAuth				
Туре	Scope 🗸			
Server	/Common/LinkedIn 🗠			
Scopes Request	Scopes Request /Common/LinkedInValidationScopesRequest >>			
Add new entry				
Scope Name Request				
1 r_basicprofile		/Common/LinkedInScopeBasicProfile		
Cancel Save (*Data in tab has been changed, please don't forget to save)				

33. Click the + on the Successful branch after the LinkedIn OAuth Scope object



34. Select Variable Assign from the Assignment tab, and click Add Item

Logo	n Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
0	ACL Assign	Assign existing Access Control Lists (ACLs)	
0	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
0	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
0	BWC Policy	Assign Bandwidth Controller policies	
0	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
0	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as PADIUS or LDAP	
0	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership	
0	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections	
0	Pool Assign	Assign a Local Traffic Pool	
0	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
	Resource Assign	Assign Connectivity Resources	
0	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
0	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
۲	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
0	VMware View Policy	Specify a policy that will apply to VMware View connections	
Cano	Add Item		Help

35. Name it LinkedIn Variable Assign and click Add New Entry then change

Properties* Branch Rules	
Name: LinkedIn Variable Assign	
Variable Assign	
Add new entry	Insert Before: 1 🗸
Assignment	
1 empty change	×
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help

36. Enter the following values and click Finished

Left Side:

- Type: Custom Variable
- Security: Unsecure
- Value: session.logon.last.username

Right Side:

- Type: Session Variable
- Session Variable: session.oauth.scope.last.firstName

1		
	Custom Variable V Unsecure V	= Session Variable V
	session.logon.last.username	Session Variable session.couth.scope.last.fin
	Cancel Finished	Help

37. Review the LinkedIn Variable Assign object and click Save



38. Click **Deny** on the **Fallback** branch after the **LinkedIn Variable Assign** object, select **Allow** in the pop up window and click **Save** 

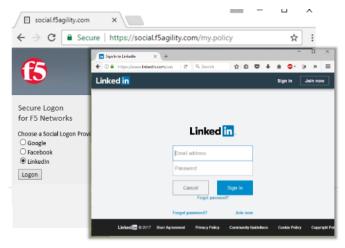


39. Click Apply Access Policy in the top left and then close the tab

Apply Acces	s Policy						
Access Policy: /Cor	mmon/so	cial-ap	idit Endings (Endings A	ilow, Deny (default)	)		
Start failback +-		LinkedIn +	LinkedIn OAuth Clent	Successful +	OAuth Scope	Buccessful +-to-Linkedin Variable Assists hilback +-to	) Allow ) Deny ) Deny
Déuth	Logan Page	Google +		Successful + -+0-	Google OAuth Scope	Second + +++ Gozale Variable Assist followk + ++++++++++++++++++++++++++++++++++	
		Facebook + -+t-	Facebook OAuth Client	Successful + -+>-	-×- Facebook QAuth Scope	Successful +	
		fallback					Denv

#### **Test Configuration**

1. Test by opening Chrome in the jump host and browsing to https://social.f5agility.com, select the provider and attempt logon.

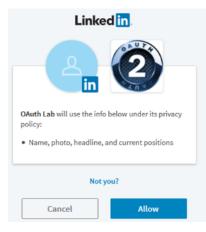


**Note:** You are able to login and reach the app now, but SSO to the app has not been setup so you get an application error.

**Note:** You may also be prompted for additional security measures as you are logging in from a new location.

Note: You may need to start a Chrome New Incognito Window so no session data carries over.

2. You will be prompted to authorize your request. Click Allow.



### 2.2.9 Task 7: Add Header Insertion for SSO to the App

In this task you will create a policy that runs on every request. It will insert a header into the serverside HTTP Requests that contains the username. The application will use this to identify who the user is, providing Single Sign On (SSO).

#### **Configure the Per Request Policy**

1. Go to Access -> Profiles/Policies -> Per Request Policies and click Create

Acces	is a Profiles ( Poli	cies : Per-Request Pol								
		Per-Request Policies			2					
					_					
· Search Create I import										
-	Per-Request Policy	Name				Per-Request Policy	Export	Сору	Virtual Servers	+ Partition / Pat
dynamic-prp						🕫 Edt	Export			Common

2. Enter prp-x-user-insertion the Name field and click Finished

Access » Profiles / Policies : Per-Request Policies					
Conoral Properties					
General Properties Name	prp-x-user-insertion				
Cancel Finished					

3. Click Edit on the prp-x-user-insertion policy line



4. Click the + symbol between Start and Allow

Per-Request Policy: /Common/prp-x-user-insertion

Start	fallback .	++-) 4	Allow
-------	------------	--------	-------

5. Under the General Purpose tab select HTTP Headers and click Add Item

Auth	nentication Assignment End	dpoint Security (Server-Side) General Purpose	
0	Application Filter Assign	Assign a Filter to lookup Applications	
0	Application Lookup	Application Lookup	
0	Category Lookup	Category Lookup	
$^{\circ}$	Empty	An Empty Action for constructing custom Branch Rules	
۲	HTTP Headers	Modify HTTP Headers	
$^{\circ}$	iRule Event	Raises an iRule ACCESS_PER_REQUEST_AGENT_EVENT event for use with custom iRules	
0	Logging	Log custom messages and session variables for reporting and troubleshooting	
$^{\circ}$	Protocol Lookup	Protocol Lookup	
0	Proxy Select	Proxy Select	
$^{\circ}$	Request Analytics	Request Analytics	
0	Response Analytics	Response Analytics	
0	SSL Bypass Set	SSL Bypass Set	
0	SSL Intercept Set	SSL Intercept Set	
$\bigcirc$	SSO Configuration Select	Selection of configured SSO Config	
0	URL Branching	Simple branching rules based on the URL	
$\bigcirc$	URL Filter Assign	Assign a Filter to lookup URLs	
Cano	el Add Item		Help

- 6. Under the HTTP Header Modify section, click Add New Entry to add the following two headers and then click Save
  - Header Operation: replace
  - Header Name: X-User
  - Header Value: %{session.logon.last.username}
  - Header Operation: replace
  - Header Name: X-Provider
  - Header Value: %{session.logon.last.oauthprovidertype}

P	Properties* Bran	ch Rules			
Na	ame: HTTP Heade	rs			
Н	ITTP Header Mod	lify			
	Add new entry			Insert Befor	re: 1 🗸
	Header Operation	Header Name	Header Value	Header Delimiter	
1	replace 🗸	X-Provider	%{session.logon.last.oauthproviderty		<b>I</b>
2	replace $\checkmark$	X-User	%{session.logon.last.username}		<b>A X</b>

#### **HTTP Cookie Modify**

Add new entry Insert Before: 🗸					
Cookie Operation	Cookie Name	Cookie Value			
Cancel Save (*Data in tab has been cha	anged, please don't forget to save	)	Help		

**Note:** Replace instead of Insert has been selected for Header Operation to improve security. A malicious user might insert their own X-User header. As using Insert would simply add another header. Using Replace will add a header if it does not exist, or replace one if it does.

You do not need to Apply Policy on per request policies. You may simply close the browser tab

# Per-Request Policy: /Common/prp-x-user-insertion



#### Add the Per Request Policy to the Virtual Server

1. Go to Local Traffic -> Virtual Servers and click on social.f5agility.com-vs

🌣 🗸 🗸 Vi	irtual Server List	Virtual Address List	Statistics -							
Search Create										
<b>v</b>   <b>v</b> s	Status 🔺 Name			Description	Application	Destination	Service Port	Type	Resources	Partition / Pat
	dns_host_resolver 10.1.20.99 53 Standard Edit Common									
	dns_host	resolver				10.1.20.99	53	Standard	Edit	Common

2. Scroll to the Access Policy section of the Virtual Server and select prp-x-user-insertion from the Per-Request Policy drop down. Scroll to the bottom of the page and click Update

Access Policy	
Access Profile	social-ap 🗸
Connectivity Profile +	None 🗸
Per-Request Policy	prp-x-user-insertion
VDI Profile	None ~
Application Tunnels (Java & Per- App VPN)	Enabled
OAM Support	Enabled
PingAccess Profile	None 🗸

|--|--|--|

#### **Test Configuration**

1. Go to https://social.f5agility.com in your browser and logon using one of the social logon providers. This time you should see your name appear in the top right corner. You can also click "Headers" in the webapp and look at the headers presented to the client. You will see x-user present here with your name as the value. You'll also see the x-provider header you inserted indicating where the data is coming from.

Demo	Webore Unitered	Hu
Graham Alde	rson's Tasks	
Home (5) Profile (1) H	laders 😁	
connection		
upgrade-insecure-requests		
user-agent		
referer		
accept-language		
	Contro Alianza	

# 2.3 Lab 2: API Protection

# 2.3.1 Purpose

This section will teach you how to configure a Big-IP (#1) as a Resource Server protecting an API with OAuth and another Big-IP (#2) as the Authorization Server providing the OAuth tokens.

# 2.3.2 Task 1: Setup Virtual Server for the API

Note: This task is performed on Big-IP #1 (RS)	
------------------------------------------------	--

#### **Create the Virtual Server**

1. Go to Local Traffic -> Virtual Servers and click on Create

Lo	Local Traffic » Virtual Servers : Virtual Server List											
¢	ŧ -	Virtual S	erver List	Virtual Address List		-						
*				Se	arch							Create
	1	<ul> <li>Status</li> </ul>	▲ Name			Description	Application	Destination	♦ Service Port	† Type	Resources	+ Partition / Path
			dns_host	resolver				10.1.20.99	53	Standard	Edit	Common
			social.agi	lity.com-vs				10.1.20.111	443 (HTTPS)	Standard	Edit	Common

- 2. Enter the following values (leave others default) then scroll down to Resources
  - Name: api.f5agility.com-vs
  - Destination Address: 10.1.20.112
  - Service Port: 443
  - HTTP Profile: http
  - SSL Profile (Client): f5agility-wildcard-self-clientssl
  - Source Address Translation: Auto Map

General Properties	
Name	api.f5agility.com-vs
Description	[
Туре	Standard V
Source Address	
Destination Address/Mask	10.1.20.112
Service Port	443 HTTPS V
Notify Status to Virtual Address	
State	Enabled V
Configuration: Basic V	
Protocol	TCP V
Protocol Profile (Client)	tcp ~
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http 🗸
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None 🗸
RTSP Profile	None 🗸
SSL Profile (Client)	Selected Available
SSL Profile (Server)	Selected Available Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (Common (C
SMTPS Profile	None 🗸
Client LDAP Profile	None 🗸
Server LDAP Profile	None
SMTP Profile	None 🗸
VLAN and Tunnel Traffic	All VLANs and Tunnels V
Source Address Translation	Auto Map 🗸

3. In the **Resources** section, select following value (*leave others default*) then click **Finished** 

# Default Pool: api-pool

#### Resources

iRules	Enabled	Available /Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Policies	Enabled	Available
Default Pool +	api-pool 🗸	
Default Persistence Profile	None 🗸	
Fallback Persistence Profile	None ~	
Cancel Repeat Finished		

#### **Test Configuration**

1. On the Jump Host, launch Postman from the desktop icon



2. The request should be prefilled with the settings below. If not change as needed or select **TEST API Call** from the **API Collection** and click **Send** 

Method: GET

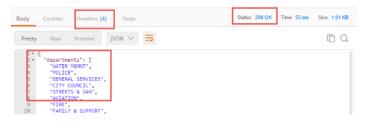
Target: https://api.f5agility.com/department

Authorization: No Auth

Headers: (none should be set)

b. https://epi./SegIlity. × +		No Environment	∨ © ‡
GET V b. https://api/5aglity.com/department		Params	nd 💙 Save 🗠
Authorization Headers Body Pre-request Script Tests			Cookies Code
Type No Auth 🗸			
Note: Headers Tab View			
Authorization Headers Body Pre-request Script Tests			Cookies Code
Key	Value		Bulk Edit Presets 🔻
New key	value		

3. You should receive a 200 OK, 4 headers and the body should contain a list of departments.



Note: This request is working because we have not yet provided any protection for the API.*

**Note:** If you get "Could not get any response" then Postman's settings may be set to verify SSL Certificates (default). Click File -> Settings and turn SSL Certificate Verification to Off.*

# 2.3.3 Task 2: Authorization Server

Note: This task is performed on Big-IP #2 (AS)

#### **Configure the Database Instance**

1. Go to Access -> Federation -> OAuth Authorization Server -> Database Instance and click Create



2. Enter oauth-api-db for the Name field and click Finished.

Access » Federation : OAuth	Authorization Server : Database Instance >> New Da
General Properties	
Name	oauth-api-db
Description	
Purge Schedule Settings	
Frequency	Daily V
Schedule At	02:00
Cancel Repeat Finished	

#### **Configure the Scope**

1. Go to Access -> Federation -> OAuth Authorization Server -> Scope and click Create



- 2. Enter the following values and and click Finished.
  - Name: oauth-scope-username
  - Scope Name: username
  - Scope Value: %{session.logon.last.username}
  - Caption: username

### Access » Federation : OAuth Authorization Server : Scope » New Scope...

#### General Properties

Name	oauth-scope-username	
Scope Name	username	
Scope Value	%{session.logon.last.username}	
Description		

#### Customization Settings for English

Language	English
Caption	username
Detailed Description	
Cancel Repeat Finished	

**Note:** This scope is requested by the Resource Server and the information here is provided back. You can hardcode a value or use a variable as we have here. So if the scope username is requested, we will supply back the username that was used to login at the Authorization Server (AS).*

#### **Configure the Client Application**

1. Go to Access -> Federation -> OAuth Authorization Server -> Client Application and click Create



#### 2. Enter the following values and click Finished.

- Name: oauth-api-client
- Application Name: HR API
- Caption: HR API
- Authentication Type: Secret
- Scope: oauth-scope-username
- Grant Type: Authorization Code

• Redirect URI(s): https://www.getpostman.com/oauth2/callback

#### Remember to click Add

eneral Properties		
Name	oauth-api-client	
Application Name	HR API	
Description		
Website URL		
Website Logo URL		
Contact		
ustomization Settings for Englis	- sh	
Language	English	
Caption	HR API	
Detailed Description		
ecurity Settings		
Authentication Type	O None  Secret  Certificate	
	Selected	Availab
Scope +	oauth-scope-usemame <	
	>>	
	Authorization Code	
Grant Type	L Implicit	
	Resource Owner Password Credentials	
	https://www.getpostman.com/oauth2/callback	
Redirect URI(s)		
	Edit Delete	
oken Management Configuration		
oken Management Configuration Use Profile Token Management Settings	Enabled	

**Note:** The Redirect URI above is a special URI for the Postman client you'll be using. This would normally be a specific URI to your client

#### **Configure the Resource Server**

1. Go to Access -> Federation -> OAuth Authorization Server -> Resource Server and click Create

Access » Federation : OAuth Authorization Server : Resource Server								
🔅 🔹 SAML Service Provider 👻 SAML Identity Provider 👻 SAML Resources OAuth Authorization Server 👻 OAuth Client / Resource Server 👻 PingAccess 💌								
Create								
Authentication Type     OAuth Profile     Partition /								
No records to display.								
Delete Download Resource Se	ervers							

- 2. Enter the following values and click Finished.
  - Name: oauth-api-rs
  - Application Type: Secret

Access » Federation : OAuth Authorization Server : Resource Server » New Resource Server						
General Properties						
Name	oauth-api-rs					
Authentication Type	◯ None	icate				
Description						
Cancel Repeat Finished						

# **Configure the OAuth Profile**

1. Go to Access -> Federation -> OAuth Authorization Server -> OAuth Profile and click Create

Access » Federation : OAuth Authorization Server : OAuth Profile									
- 10 v			SAML Resources	OAuth Authorization Server 👻			PingAccess	-	
*		× Search							Create
✓ ♦ Name Access Profiles Partition								tition / Path	
□ oauth Commo									nmon
Delete	ə								

- 2. Enter the following values and click **Finished**.
  - Name: oauth-api-profile
  - Client Application: oauth-api-client
  - Resource Server: oauth-api-rs
  - Database Instance: oauth-api-db

Access » Federation : OAuth	Authorization Server : OAuth Profile » N	New OAuth Profile
General Properties		
Name	oauth-api-profile	
Parent Profile	oauth	
Client Application	Selected //Common oauth-api-client	Available
Resource Server	Selected	Available
Database Instance	oauth-api-db	
Cancel Repeat Finished	Additional sections	ns removed

# Configure the APM Per Session Policy

1. Go to Access -> Profiles/Policies -> Access Profiles (Per Session Policies) and click Create

Access a Profiles / Policies : Access Profiles (Per -Session Policies)											
Access Prollies			Customization +								
	× Sear	rch								Cr	eate Import.
V Status * Access Profile Name				+ Application	· Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	· Partition / Patt
D M access					AI	(none)	(none)	(none)			Common
Delete Apply											

- 2. In the General Properties section enter the following values
  - Name: oauthas-ap
  - Profile Type: All
  - Profile Scope: Profile

# Access » Profiles / Policies : Access Profiles (Per-Session Policies) »

General Properties	
Name	oauthas-ap
Parent Profile	access
Profile Type	All
Profile Scope	Profile V

- 3. In the **Configurations** section select the following value from the **OAuth Profile** drop down menu.
  - OAuth Profile: oauth-api-profile

Configurations	
Logout URI Include	URI Add Edit Delete
Logout URI Timeout	5 seconds
Microsoft Exchange	None ~
User Identification Method	HTTP V
OAuth Profile	+ oauth-api-profile V

- 4. In the Language Settings section enter the following value and then click Finished.
  - Languages: English

Language Settings	
Additional Languages	Afar (aa)
Languages	Accepted Languages
Default Language	English (en) 🗸
Cancel Finished	

5. Click Edit on the oauthas-ap policy, a new browser tab will open.

Acce	ess » Pi	ofiles / Poli	cies : Access Profiles	(Per-Session Polici									
* •	Acces	s Profiles	Per-Request Policies		Customization								
*			× Sear	rch									Create Import
	💌 Statu	s Access	Profile Name			Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
C	1	access					All	(none)	(none)	(none)			Common
	1	oauthas-a	ip				All	🗗 Edit	Export	Сору	default-log-setting		Common

6. Click the + between Start and Deny

Access Policy: /Common/oauthas-ap	Edit Endings
Start fallback ++++	

7. Select Logon Page from the Logon tab, and click Add Item

Log	on Authentication Assignme	ent   Endpoint Security (Server-Side)   Endpoint Security (Client-Side)   General Purpose	
0	Citrix Logon Prompt	Configure logon options for Citrix clients	
$^{\circ}$	External Logon Page	Redirect user to externally hosted form-based web logon page	
0	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication	
0	HTTP 407 Response	HTTP 407 Response for Basic or SPNEGO/Kerberos authentication	
۲	Logon Page	Web form-based logon page for collecting end user credentials (used with most deployments)	
•	Logon Page OAuth Logon Page	Web form-based logon page for collecting end user credentials (used with most deployments) OAuth Logon Page used for OAuth Client authentication	
<ul><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>			
<ul> <li></li> <li><td>OAuth Logon Page</td><td>OAuth Logon Page used for OAuth Client authentication</td><td></td></li></ul>	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication	

8. Accept the defaults on the Logon Page and click Save

Properties Branch F	Rules					
Name: Logon Page			]			
Logon Page Agent Split domain from full	licername	No V				
CAPTCHA Configuratio		None V				
Туре	Post Va	riable Name	Session Variable Name	Clean Variable	Values	Read Only
1 text $\checkmark$	username		username	No 🗸		No 🗸
2 password $\checkmark$	password		password	No 🗸		No 🗸
3 none 🗸	field3		field3	No 🗸		No 🗸
4 none ~	field4		field4	No 🗸		No 🗸
5 none 🗸	field5		field5	No 🗸		No 🗸
Language	en ∨			1	Reset all de	Import
Form Header Text	Secure Lo	gon for F5 N	etworks			
Logon Page Input Fiel	d #1 Username	1				
Logon Page Input Fiel	d #2 Password					
Logon Button	Logon					
Front Image	[Replace I	mage] [Revert to D	efault]			
Save Password Check	Sava Pace					
New Password Prompt	New Pass	word				
Verify Password Prom	pt Verify Pas	sword				
Cancel Save						ł

9. Click the + between Logon Page and Deny



10. Select OAuth Authorization from the Authentication tab and click Add Item

Logo	on Authentication Assignme	ent Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	_
0	AD Auth	Active Directory authentication of end user credentials	
$\circ$	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping	
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	
$^{\circ}$	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
0	HTTP Auth	HTTP authentication of end user credentials	
0	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
0	LDAP Auth	LDAP authentication of end user credentials	
$^{\circ}$	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping	g
0	LocalDB Auth	Local Database Authentication	
$^{\circ}$	NTLM Auth Result	NTLM authentication of end user credentials	
۲	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management	
0	OAuth Client	OAuth Client	
0	OAuth Scope	OAuth Scope	
Cano	Add Item		Hel

11. Accept the defaults for the OAuth Authorization and click Save

Properties Branch Rules	
Name: OAuth Authorization	
OAuth Authorization	
Prompt for Authorization	Enabled V
Scope Assign	

#### Customization

Add new entry

Language	en V Reset all defaults
Authorize Message	Authorization request
Scope Message	requests permission to do the following:
Allow Message	Authorize
Deny Message	Deny
Cancel Save	Help

12. Click Deny on the Successful branch after the OAuth Authorization object, select Allow, click Save

Insert Before:

Access Po	licy: /Common/oau	ithas-ap	Edit Endings	(Endings: Allo	ow, Deny [def:
Start - fallba	ck + Logon Page fallback	+	uthorization	uccessful +→>-	
				*>	Deny
	Select Ending:				
	● Allow □				
	🔘 Deny 🗖				
	Cancel Save			Help	

13. Click Apply Access Policy in the top left and then close the tab

6	Apply Access Policy			
Access	Policy: /Common/	/oauthas-ap	Edit Endings	(Endings: Allow, Deny [def
Start	allback + <u>Logon Page</u> fall	lback + →>- OAuth /	Authorization	lback +→> <u>Allow</u>

**Note:** We are not validating the credentials entered on the Logon Page, so you can enter anything you want. In a production deployment you would most likely include some process for validating credentials such as an LDAP Auth or AD Auth object, or perhaps limiting access by IP or client certificate

**Note:** This policy might also set some variables that get used as scope values. Thus, you could determine what the scope values are by utilizing the policy here.*

#### **Create the Authorization Virtual Server**

1. Go to Local Traffic -> Virtual Servers and click Create

Local Traffic » Virtual Servers : Virtual Server List											
☆ -	Virtual Server List	Virtual Address List									
*	• Search Create										
	🚽 Status 🔺 Name				Description	Application	Destination	Service Port	Type	Resources	Partition / Path
No records to display.											

- 2. Enter the following values for the Authorization Server Virtual Server
  - Name: oauthas.f5agility.com-vs
  - Destination Address: 10.1.20.110
  - Service Port: 443
  - HTTP Profile: http
  - SSL Profile (Client): f5agility-wildcard-self-clientssl
  - Source Address Translation: Auto Map

General Properties	
Name	oauthas.f5agility.com-vs
Description	
Туре	Standard ~
Source Address	
Destination Address/Mask	10.1.20.110
Service Port	443 HTTPS V
Notify Status to Virtual Address	
State	Enabled V
Configuration: Basic V	
Protocol	TCP V
Protocol Profile (Client)	tcp ~
Protocol Profile (Server)	(Use Client Profile) V
HTTP Profile	http 🗸
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None 🗸
RTSP Profile	None ~
SSL Profile (Client)	Selected Available Common ISagility-wilcard-self-clientssl <<  Clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl
SSL Profile (Server)	Selected     Available       Image: Constraint of the server sel of the server server sel of the server sel of the server server sel of the serv
SMTPS Profile	None 🗸
Client LDAP Profile	None 🗸
Server LDAP Profile	None 🗸
SMTP Profile	None 🗸
VLAN and Tunnel Traffic	All VLANs and Tunnels $\smallsetminus$
Source Address Translation	Auto Map 🗠

3. Scroll to the **Access Policy** section, select oauthas-ap from the **Access Profile** drop down menu and then click **Finished** at the bottom of the screen.

Access Policy									
Access Profile oauthas-ap 🔻									
	Additional sections removed								
Cancel Repeat	Finished								

#### 2.3.4 Task 3: Resource Server

Note: This task is performed on Big-IP #1 (RS)

#### **Configure the OAuth Provider**

1. Go to Access -> Federation -> OAuth Client/Resource Server -> Provider and click Create

Acce	Access » Federation : OAuth Client / Resource Server : Provider									
* -	SAML Service Provider 👻				ver 👻 (	OAuth Client / Reso	ourceServer 👻	PingAccess		
*		Search						Create		
	▲ Name				† Type	OAuth Servers	Application	Partition / Path		
	F5				F5			Common		
	Facebook				Faceboo	k Facebook		Common		
	Google				Google	Google		Common		
	LinkedIn				Custom	LinkedIn		Common		
	Ping				Ping			Common		

- 2. Enter the following values for the Authorization Server Virtual Server and then click Finished
  - Name: oauthas.f5agility.com-provider
  - **Type:** F5
  - Authentication URI: https://oauthas.f5agility.com/f5-oauth2/v1/authorize
  - Token URI: https://oauthas.f5agility.com/f5-oauth2/v1/token
  - Token Validation Scope: https://oauthas.f5agility.com/f5-oauth2/v1/ introspect

#### Access » Federation : OAuth Client / Resource Server : Provider » New Provider...

#### General Properties

ocheral Properties	
Name	oauthas.f5agility.com-provider
Description	
Туре	F5 <b>T</b>
Authentication URI	https://oauthas.f5agility.com/f5-oauth2/v1/authorize
Token URI	https://oauthas.f5agility.com/f5-oauth2/v1/token
Token Validation Scope URI	https://oauthas.f5agility.com/f5-oauth2/v1/introspect
Cancel Repeat Finished	

#### **Configure the OAuth Server**

1. Go to Access -> Federation -> OAuth Client/Resource Server -> OAuth Server and click Create

Access » Federation : 0Auth Client / Resource Server : 0Auth Server									
÷ -	SAML Service Provider 🔻	SAML Identity Provider 🝷	SAML Resources	OAuth Authorization Server 👻 OAuth			Client / Reso	PingAccess	
*		Search							Create
	Name				A Mode		+ Provider	Application	Partition / Path
F	acebook				Client + Resource	Server	Facebook		Common
	Google				Client + Resource	Server	Google		Common
	inkedIn				Client + Resource	Server	LinkedIn		Common

- 2. Enter the following values for the Authorization Server Virtual Server and then click Finished
  - Name: api-resource-server
  - Mode: Resource Server
  - **Type:** F5
  - OAuth Provider: oauthas.f5agility.com-provider
  - DNS Resolver: oauth-dns
  - **Resource Server ID:** (see step 5) <*Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization Server -> Resource Server -> oauth-api-rs>*
  - **Resource Server Secret:** (see step 5) <*Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization Server -> Resource Server -> oauth-api-rs>*
  - Resource Server's Server SSL Profile Name: apm-allowuntrusted-serverssl

#### Access » Federation : OAuth Client / Resource Server : OAuth Server » New OAuth Se

#### **General Properties**

Name	api-resource-server	
Description		
Mode	Resource Server 🔹	
Туре	F5 🔻	
OAuth Provider +	oauthas.f5agility.com-provider	<b>•</b>
DNS Resolver +	oauth-dns 🔻	
	Selected	Availab
iRules	<ul> <li>&lt;</li> <li>&gt;&gt;</li> </ul>	/ <b>Common</b> _sys_APM_ExchangeSup _sys_APM_ExchangeSup _sys_APM_ExchangeSup
Token Validation Interval	60 minutes	
Resource Server Settings		

Resource Server ID	Your oauth-api-rs ID from Big-IP 2					
Resource Server Secret	Your oauth-api-rs secret from Big-IP 2					
Resource Server's ServerSSL Profile Name	apm-allowuntrusted-serverssl					
Cancel Repeat Finished						

**Note:** We are using a custom serverssl profile to allow negotiation with an untrusted certificate. This is needed because our Authorization Server is using a self-signed certificate. In production for proper security you should leverage a trusted certificate (most likely publicly signed) and the apm-defaultserverssl profile (or other as appropriate)*

3. The values for step 4 above can be obtained by accessing Big-IP 2 and navigating to Access -> Federation -> OAuth Authorization Server -> Resource Server -> oauth-api-rs as shown.

Access » Federation : OAuth Authorization Server : Resource Server » oauth-api-rs					
🚓 🚽 Properties					
General Properties					
Name	oauth-api-rs				
Resource Server ID	Your oauth-api-rs ID				
Partition / Path	Common				
Authentication Type	🔍 None 🖲 Secret 🔍 Certificate				
Secret	Your oauth-api-rs secret				
Description					

4. To configure the APM Per Session Policy go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) and then click Create

Acce	Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
÷ -	Access Profiles Per-Request Policies Policy Sync Customization 👻										
치	* Create Import										
	💌 Status	▲ Access	Profile Name	Application	on 🗢 Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	
	<b>]</b> ##	access			All	(none)	(none)	(none)			Common
	0	social-ap			All	🗖 Edit	Export	Сору	default-log-setting	social.agility.com-vs	Common

5. Enter the following values and then click Finished

## Access » Profiles / Policies : Access Profiles (Per-Session Policies) » New Profile

#### General Properties

Name	api-ap
Parent Profile	access
Profile Type	OAuth-Resource Server ▼
Profile Scope	Profile <b>T</b>

# Additional sections removed

#### Language Settings

Additional Languages	Afar (aa) 🔹 Add
Languages	Accepted Languages
Default Language	English (en) 🔻
Cancel Finished	

- Name: api-ap
- Profile Type: OAuth-Resource-Server
- Profile Scope: Profile
- Languages: English

#### Note: User Identification Method is set to OAuth Token and you cannot change it for this profile type.

6. Click Edit on the new api-ap policy and a new window will open

÷ -	Access I	Profiles	Per-Request I	^D olicies I	Policy Sync	cy Sync Customization 👻						
Create												
	<ul> <li>Status</li> </ul>	A 00000	Profile Name	♦ Applica	tion 🗢 Profile Type		Per-Session Policy	Export	Сору	Logs	Virtual Servers	
- I I	<ul> <li>Status</li> </ul>	- ALLES:	s Prome Name	<ul> <li>Abblica</li> </ul>	The state of the s	;	r er-dession r oncy	Export	Cobl	Logs	viitual Servers	
		access	Prome Name	<ul> <li>Applica</li> </ul>	All	,	(none)	(none)	(none)	Lugs	Viitual Gelvers	+ Partition Common
			Prolife Name	<ul> <li>Abbica</li> </ul>				(none)	(none)	default-log-setting	VIIIUAI Selveis	

7. Click Deny on the fallback branch after Start, select Allow and click Save

# Access Policy: /Common/api-ap

Start	Select Ending:	
	● Allow □	
	O Deny	
	Cancel Save	Help

8. Click Apply Access Policy in the top left and then close the tab

	Apply Access Policy			
Access Policy: /Common/api-ap				
Start	fallback + Allow			

9. To configure the APM Per Request Policy go to Access -> Profiles / Policies -> Per Request Policies and then click Create

Access » Profiles / Policies : Per-Request Policies								
🔹 🗸 Access Profiles	Per-Request Policies		Customization	-				
							_	
Create Import								
Per-Request Policy Name				Per-Request Policy	Export	Сору	Virtual Servers	Partition / Path
prp-x-user-insertion			Edit	Export	Сору	social.agility.com-vs	Common	

10. Enter api-prp for the Name and click Finished

# Access » Profiles / Policies : Per-Request Policies General Properties Name api-prp Cancel Finished

11. Click Edit on the api-prp policy and a new window will appear

Access » Profiles / Policies : Per-Request Policies							
☆ -	Access Profiles	Per-Request Policies	Policy Sync	Customization	-		
* Search							
Per-Request Policy Name Per-Request Policy Expo					Export		
api-prp Edit Expo					Export		
	prp-x-user-insertion Expo				Export		

12. Click Add New Subroutine

Per-Request Policy: /Common/api-prp	Edit Endings			
Start - Allow				
Add New Macro				
Add New Subroutine Add New Subroutine Macro				

13. Leave the Select Subroutine template as Empty. Enter RS Scope Check for the Name and then click Save

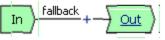
Select Subroutine template Empty
Name RS Scope Check Terminals: Out [default]
Empty subroutine with one terminal
In <i>fallback</i> Out
Cancel Save

14. Click the + next to the RS Scope Check



15. Click Edit Terminals on the RS Scope Check Subroutine

E Subroutine: RS Scope Check	Subroutine Settings / Rename	Edit Terminals	



16. First, rename Out to Success, then click Add Terminal and name it Failure

[Edit*]		
Add Terminal		1: Terminal 1 🔻
Name: Failure	#2 🎢	× ×
Name: Success	#1 🎢	🔳 default
Cancel Save (*Data in ta	b has been changed, please don't f	orget to save) Help

17. Go to the Set Default tab and select Failure then click Save

Edit* Set Default*	
• Failure	
Success	
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help

18. Click Edit Terminals again (it will ignore the order settings if you do this in one step without saving in between)

Subroutine: RS Scope Check	Subroutine Settings / Rename	Edit Terminals	
In fallback + Out			

19. Move Success to the top using the up arrow on the right side then click Save

<u>Out</u>

Edit* Set Default		
Add Terminal	1: Failu	ure ▼
Name: Failure 🛛 🐙 🎢	_	default
Name: Success #1 🎢		x
Cancel Save *Data in tab has been changed, please don't forge	t to save)	Help

20. Click the + between In and Success, a new window will appear



21. Select OAuth Scope from the Authentication tab and click Add Item

Log	on Authentication Assignm	ent (Endpoint Security (Server-Side) (General Purpose)			
0	AD Auth	Active Directory authentication of end user credentials			
$\bigcirc$	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication			
0	HTTP Auth	HTTP authentication of end user credentials			
$\bigcirc$	LDAP Auth	LDAP authentication of end user credentials			
0	LocalDB Auth	Local Database Authentication			
$\bigcirc$	OAuth Client	OAuth Client			
۲	OAuth Scope	OAuth Scope			
$\bigcirc$	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication			
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate			
$\bigcirc$	RADIUS Auth	RADIUS authentication of end user credentials			
Canc	Cancel Add Item				

- 22. Enter the following values and then click Save
  - Server: /Common/api-resource-server
  - Scopes Request: /Common/F5ScopesRequest

Properties* Branch Rules				
Name: OAuth Scope				
OAuth				
Туре	Scope 🔻			
Server	/Common/api-resource-server 🔻			
Scopes Request	/Common/F5ScopesRequest 🔹			
Add new entry				
Scope Name				
Cancel Save (*Data in tab has been changed, please don't forget to save)				

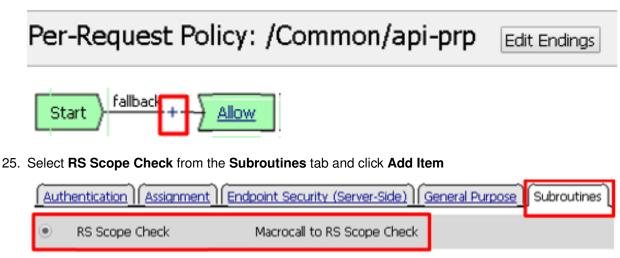
23. Verify that the **Successful** branch terminates in **Success** and the **Fallback** branch terminates in **Failure** 

Subrout	tine: RS So	cope Check	Subroutine Settings / Rer
In fallback +	X	Successful	Success
	OAuth Scope	+	Failure

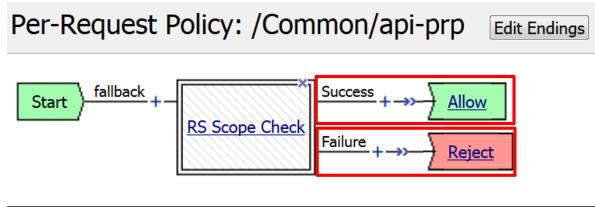
24. In the main policy, click + between the Start and Allow

Add Item

Cancel



26. Verify that the Success branch terminates in Allow and the Fallback branch terminates in Reject



Note: You do not need to "Apply Policy " on Per Request Policies*

27. To add the APM Policies to the API Virtual Server, go to Local Traffic -> Virtual Servers and click on api.f5agility.com-vs

*	Virtual S	erver List Virtual Ad	ldress List Statistics	-					
Search									
~	💌 Status	+ Nome			Description	Application	Destination		
•	Jaius	- ivame			• Description	<ul> <li>Application</li> </ul>	· Destination		
		api.f5agility.com-vs			* Description	Abblication	10.1.20.112		
_					* Description				

28. Scroll down to the Access Policy section. Change Access Profile from None to api-ap

Access Policy					
Access Profile	api-ap 🔻				
Connectivity Profile +	None <b>T</b>				
Per-Request Policy	api-prp 🔻				
VDI Profile	None <b>T</b>				
Application Tunnels (Java & Per- App VPN)	Enabled				
OAM Support	Enabled				
PingAccess Profile	None <b>T</b>				
Additional sections removed					
Update Delete					

#### 29. Change Per-Request Policy from None to api-prp and then click Update

#### 2.3.5 Task 3: Verify

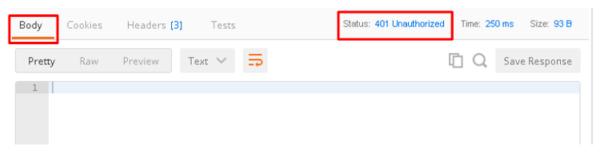
1. On the Jump Host, launch Postman from the desktop icon



2. The request should be prefilled with the settings below (same as earlier). If not change as needed or select **TEST API Call** from the **API Collection** and click **Send** 

b. https://epl.fSeglity. × +		No Environment	∨ ⊙ ³ / ₁
GET \vee b. https://api/5aglity.com/department		Params Send	✓ Save ✓
Authorization Headers Body Pre-request Script Tests			Cookies Code
Type No Auth 🗸			
Note: Headers Tab View			
Authorization Headers Body Pre-request Script Tests			Cookies Code
Кеу	Value	Bul	Edit Presets •
New key	value		
lesponse			

- Method: GET
- Target: https://api.f5agility.com/department
- Authorization: No Auth
- Headers: (none should be set)
- 3. You should receive a 401 Unauthorized and 3 headers, including WWW-Authenticate: Bearer. The body will be empty.



Note: Your API call failed because you are not providing an OAuth token. Both tabs shown

Body	Cookies	Headers (3)	Tests		Status: 401 Unauthorized	Time: 250 ms	Size: 93 B		
Connection   Close									
Content	Content-Length > 0								
WWW-A	uthenticate	e → Bearer							

4. Click the Authorization tab and change the Type from No Auth to OAuth 2.0

Test API Call X		No Environm	ent	∨ ⊙ ☆
▶ Test API Call				
GET 🗸 https://a	api.f5agility.com/department	Params	Send 🗸	Save ~
Authorization Headers	Body Pre-request Script Te	sts		Cookies Code
Туре	No Auth			
Body Cookies <b>Head</b>	No Auth	Status: 401 Unautho	prized Time: 250	ms Size: 93 B
Connection > Close	Digest Auth			
Content-Length > 0	OAuth 2.0			
WWW-Authenticate → Bear	Hawk Authentication AWS Signature			

5. If present, select any existing tokens on the left side and delete them on the right side. Click **Get New Access Token** 

Authorization	Headers		Pre-request S	cript	Tests
Туре		OAuth 2.0	~		
Existing Tokens		Get Ne	w Access Toker	,	Token Details
Get a new access token to add it to this list.					Select a token from the list to view details

- 6. In the Get New Access Token window, if the values do not match then adjust as needed, and click Request Token
  - Token Name: < Anything is fine here>

**Note:** If you're doing this lab on your own machine and using self signed certificates you must add the certs to the trusted store on your computer. If you've just done this, you must close Postman and reopen. You also need to go to File -> Settings in Postman and turn SSL certificate validation to off.

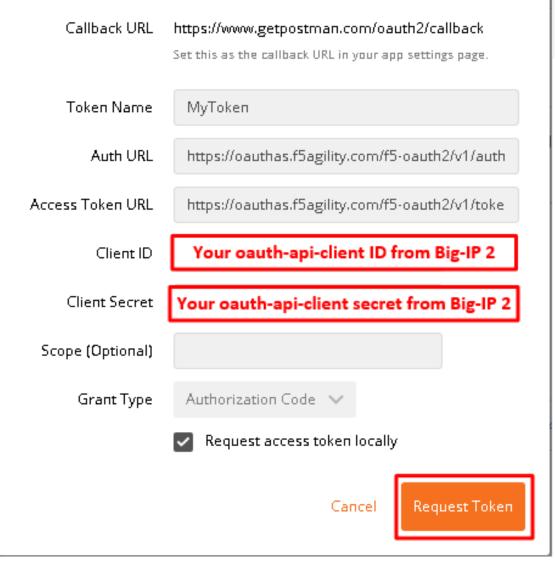
• Auth URL: https://oauthas.f5agility.com/f5-oauth2/v1/authorize

- Access Token URL: https://oauthas.f5agility.com/f5-oauth2/v1/token
- Client ID: <Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization Server -> Client Application -> oauth-api-client>
- Client Secret: <Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization Server -> Client Application -> oauth-api-client>
- Scope:
- Grant Type: Authorization Code
- Request access token locally: checked

### GET NEW ACCESS TOKEN

#### Request a new access token to add it to your list of tokens

On clicking Request Token, you will be redirected to the Auth URL where you can enter the user's credentials and request for a token

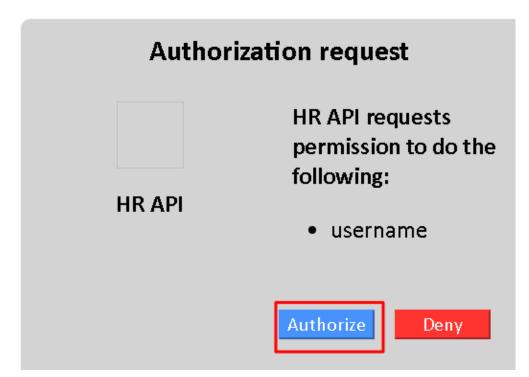


#### 7. Logon with any credentials, such as user/password

Secure Logon for F5 Networks
Username
Password
Logon

8. Authorize the HR API by clicking Authorize





9. You now have received an OAuth Token. Click the **name of your token** under **Existing Tokens** (left) and your token will appear on the right

Existing Tokens	Get New Access Token	MyToken		Delete Use Token
MyToken		Add token to	URL 🗸	
		access_toke n	3c9f4d3bdd9381104 9507c693a23c8629	la714c196289cb770a45 03a5bf770dd3
		expires_in	300	
		token_type	Bearer	

10. Change the **Add token to** drop down to Header and the click **Use Token**. You will note that the **Header** tab (in the section tabs just above) now has one header in the **Header** tab which contains your **Authorization Header** of type **Bearer** with a string value.

MyToken		Delete	Use Token
Add token to	Header 🗸		
access_toke n	3c9f4d3bdd938110 9507c693a23c862		
expires_in	300		
token_type	Bearer		
The Header tab data is	s shown in the screenshot		
Authorization Headers (	1) Body Pre-request Script	Tests	Cookies Code
Кеу		Value	Bulk Edit 🔹 Presets 🔻
<ul> <li>Authorization</li> </ul>		Bearer c89884a4df2e89f40	)d14939497bab069385c5410ba

11. Click Send at the top of the Postman screen

Get $$	https://api	i.f5agility.com	/department			Params	Se	nd 🗸	Save	~
Authorization	Headers (1)		Pre-request S	cript Tests					Cookies	Code
Туре		OAuth 2.0	$\sim$							
Existing Tokens		Get Ne	w Access Token	MyToke	n			Delete	Use T	oken
MyToken				Add toker	n to	Header	$\sim$			
				access_1 n	toke ec42165e10611860001db5bac66f8d6db 339f242a9f7d5824ec0ab7a93408				626	
				expires_i	n 3	:00				
				token_typ	e E	)earer				

12. You should receive a 200 OK, 5 headers and the body should contain a list of departments

			_		scone	licername		
Body	Cookies	Headers (5	) Tests			Status: 200 OK	Time: 350 ms	Size: 1.05 KB
Pretty	Raw	Previéw	JSON 🗸	₽				ΓQ
1 • K 2 • 3 4	"departme "WATER "POLICE "GENERA	MGMNT",	,					

**Note:** This time the request was successful because you presented a valid OAuth token to the resource server (the Big-IP), so it allowed the traffic to the API server on the backend.

#### 2.3.6 Task 4: Testing Session and Token States

**Note:** Parts of this task are performed on both Big-IP devices. Check each step to make sure you are working on the correct device.

#### Invalidate the Session

1. Go to **Big-IP 1 (OAuth C/RS) -> Access -> Overview -> Active Sessions**. Select the existing sessions and click **Kill Selected Sessions**, then confirm by clicking **Delete** 

Access » Overview : Active Sessions								
🚓 🚽 Active Sessions	Access Reports	OAuth Re	eports 🔫	SWG Reports 🛛 👻	Event Logs 🛛 👻			
Display Options								
Auto Refresh	Disabled	▼ Refr	resh					
Refresh Session Table	Refresh Session Table							
Total Active Sessions								
Active Session Count	1							
*	Se	earch						
💌 💌 Status 🗭 🕈 Se	ession ID Variables	▲ User	Client IP	≑ Start Time	Expiration			
📝 🥥 🗈 256f	10ed View	n/a	10.1.20.210	2017-05-31 13:22:24	2017-05-31 13:40:14			
Kill Selected Sessions								

2. Go back to **Postman** and click **Send** with your current OAuth token still inserted into the header. You should still receive a 200 OK, 5 headers and the body should contain a list of departments.

			_		srnna	licername		
Body	Cookies	Headers (5	) Tests			Status: 200 OK	Time: 350 ms	Size: 1.05 KB
Pretty	Raw	Preview	JSON 🗸	₽				ΓQ
1 * • 2 * 3 4	"departme "WATER "POLICE "GENERA	MGMNT",	,					

**Note:** You were still able to reach the API because you were able to establish a new session with your existing valid token*.

#### Invalidate both the Current Session and Token

1. Go Big-IP 2 (OAuth AS) -> Access -> Overview -> OAuth Reports -> Tokens. Change the DB Instance to oauth-api-db.

cess	s » Overview : OAuth Reports : Tok	ens					
		OAuth Reports 👻	SWG Reports 👻 E	vent Logs 🛛 👻			
0/	Auth Tokens					Revoke Refresh	
DB	Instance: Access T	oken Issued: 🔻					
'Cor	nmon/oauth-api-db 🔻 Last week	• U	ser or Client App	Search			
	User v	Client App 🛛 👻	Access Token Issued 😽	Access Token Expires ${}^{\prime}$	Access Token Status 🗸	Refresh Token Issued ~	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:45:38	2017-05-30 23:50:38	ACTIVE	2017-05-30 23:45:38	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:44:57	2017-05-30 23:49:57	ACTIVE	2017-05-30 23:44:57	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:39:16	2017-05-30 23:44:16	ACTIVE	2017-05-30 23:39:16	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:25:44	2017-05-30 23:30:44	EXPIRED	2017-05-30 23:25:44	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:15:13	2017-05-30 23:20:13	ACTIVE	2017-05-30 23:15:13	
	/Common/oauthas-ap.user	HR API	2017-05-30 23:09:48	2017-05-30 23:14:48	ACTIVE	2017-05-30 23:09:48	

2. Select all tokens, click **Checkbox** left in title bar and the click **Revoke** in the top right

Acces	s » Overview : OA	uth Reports : Toke	ns					
☆ -			OAuth Reports 🛛 🔫	SWG Reports 👻 E	event Logs 🛛 👻			
0	Auth Toker	าร					Revoke Refresh	
_	DB Instance:       Access Token Issued:       Image: state of the state o							
~	User	~	Client App 🗸 🗸	Access Token Issued 🛩	Access Token Expires 🗸	Access Token Status 🗸	Refresh Token Issued $\stackrel{\scriptstyle\scriptstyle{\vee}}{}$	R
~	/Common/oautha	s-ap.user	HR API	2017-05-30 23:45:38	2017-05-30 23:50:38	ACTIVE	2017-05-30 23:45:38	-
~	/Common/oautha	s-ap.user	HR API	2017-05-30 23:44:57	2017-05-30 23:49:57	ACTIVE	2017-05-30 23:44:57	
~	/Common/oautha	s-ap.user	HR API	2017-05-30 23:39:16	2017-05-30 23:44:16	ACTIVE	2017-05-30 23:39:16	
~	/Common/oautha	s-ap.user	HR API	2017-05-30 23:25:44	2017-05-30 23:30:44	EXPIRED	2017-05-30 23:25:44	
*	/Common/oautha	s-ap.user	HR API	2017-05-30 23:15:13	2017-05-30 23:20:13	ACTIVE	2017-05-30 23:15:13	

3. Go to **Big-IP 1 (OAuth C/RS) -> Access -> Overview -> Active Sessions**. Select the existing sessions and click **Kill Selected Sessions**, then confirm by clicking **Delete** 

Access » Overview : Active Sessions									
🚓 🚽 Active Sessions	Access Reports	OAuth Re	eports 🔫	SWG Reports 🛛 👻	Event Logs 🛛 👻				
		_							
Display Options	Display Options								
Auto Refresh	Disabled	▼ Refr	resh						
Refresh Session Table	Refresh Session Table								
Total Active Sessions									
Active Session Count	1								
*	Se	earch							
💌 💌 Status 🛨 🗢 Se	ession ID Variables	▲ User		Start Time	Expiration				
🗹 🥥 🗈 256f	10ed View	n/a	10.1.20.210	2017-05-31 13:22:24	2017-05-31 13:40:14				
Kill Selected Sessions									

4. Go back to **Postman** and click Send with your *current OAuth token still inserted* into the header. You should receive a 401 Unauthorized, **3 headers**, no body, and the WWW-Authenticate header will provide an error description indicating the token is not active.

Body Cookies (1)	Headers (3)	Tests	Status	: 401 Unauthorized	Time: 735 ms	Size: 155 B
Connection > Close						
Content-Length → 0						
WWW-Authenticate 🕠	Bearer error="invalio	l_token",error_descript	ion="Token is not	active"		

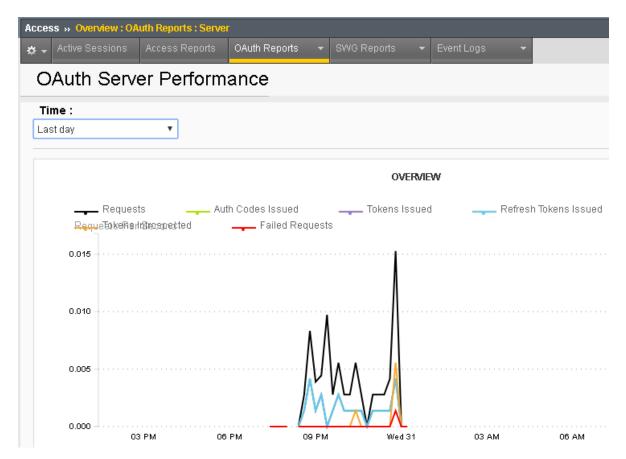
**Note:** You can remove the header, delete the token, and start over getting a new token and it will work once again.*

**Note:** This time you were no longer able to reach the API because you no longer had a valid token to establish your new session with. Getting a new token will resolve the issue.

# 2.4 Lab 3: Reporting and Session Management

#### 2.4.1 Task 1: Big-IP as Authorization Server (Big-IP 2)

1. You can see reporting on OAuth traffic at Access -> Overview -> OAuth Reports -> Server



 You can see the session logs by going to Access-> Overview-> Active Sessions and click on the active session, or for past sessions under Access -> Overview -> Access Reports -> All Sessions Report (it runs by default and asks for a time period)

Access » Overview : Acc	cess Reports						
🚓 🗸 Active Sessions	Access Reports	OAuth Reports 🛛 👻	SWG Report		Event Logs	-	
Reports Browser	<b>«</b>	All Sessions 🛞			·		
Favorites	+	😣 Export to CSV File	🔣 Show in Pop	oup Windov	🖉 🔄 View Repo	ort Constraints   🗼 Set	to default repo
Built In Reports	-	Local Time	Session ID	Logon	Active	Session Variables	State
💫 Favorite	💽 Run	2017-05-30 23:45:27	975c3806	user	N	View Session Variable	<u>s</u>
ACE Details (Air Sessions)		2017-05-30 23:44:45	<u>12b6d17e</u>	user	N	View Session Variable	<u>s</u>
ACL Summary (Session ID)	<b>^</b>	2017-05-30 23:39:02	e0804cb9	user	N	View Session Variable	<u>s</u>
ACL Summary(All Sessions		2017-05-30 23:29:31	4e9abf2f		N	View Session Variable	<u>s</u>
Allowed ACL Details (Sessi		2017-05-30 23:25:34	<u>92218414</u>	user	N	View Session Variable	<u>s</u>
Allowed ACLs (All Sessions	s)	2017-05-30 23:14:59	<u>c5c2800e</u>	user	N	View Session Variable	<u>s</u>
Denied ACL Details (Session	n ID)	2017-05-30 23:09:36	75eed6b0	user	N	View Session Variable	<u>s</u>
Denied ACLs (All Sessions)		2017-05-30 22:53:17	0c6b03d2	user	N	View Session Variable	<u>s</u>
Browser/App Reports		2017-05-30 22:24:41	<u>c851f7ad</u>	user	N	View Session Variable	<u>s</u>
		2017-05-30 22:19:38	5a3c7d6b		N	View Session Variable	<u>s</u>
Application and OS Distribut	.001	2017-05-30 22:12:10	9008d848	user	N	View Session Variable	<u>s</u>

#### 2.4.2 Task 2: Big-IP as Client / Resource Server (Big-IP 1)

1. After logging in Go to Access -> Overview -> Active Sessions and note that the "User" field is populated with the name from your social account (from social account labs). This happens because we took the relevant variable from the OAuth response and put it into the variable session.logon.last.username.

	uve 563	ssions												
🚓 👻 Active Sessions	Acces	s Reports	OAuth Report		SWG Rep	oorts 🔫	Event Log	js 🔻						
Display Options														
Auto Refresh		Disabled	Refrest	1										
Refresh Session Table														
Total Active Sessions														
Total Active Sessions Active Session Count		1												
			earch											
	¢ Se		earch Variables	▲ Use	r	Client IP		<ul> <li>Start T</li> </ul>						
Active Session Count	¢ Se: df4a5	Sion ID		▲ Use Chas L	_	<ul> <li>Client IP</li> <li>192.168.18</li> </ul>		<ul> <li>Start Tr 2017-05-</li> </ul>						

 There are more session variables retrieved from the provider you can examine. To see them click on View under Variables for the session. Search for variables that start with "session.oauth.scope.last". The scope will determine what the Authorization Server returns to you.

Access » Overview : /	ctive Se	ssions						
🔅 👻 Active Sessions	Acce	ss Reports	OAuth Rep	orts 👻	SWG Reports		Event Log:	
Display Options								
Auto Refresh		Disabled	Refre	sh				
Refresh Session Table	1							
	_							
Total Active Sessions								
Active Session Count		1						
*		S	earch					
Status H	• Se	ession ID	Variables	▲ Use	r ¢	Client IP		Start Ti
	3 df4a	5200	View	Chas L	esley 19	2.168.18	7.169	2017-05-
Kill Selected Sessions	]							

Note: You can terminate this session if desired at the Active Sessions screen*

df4a5200. <mark>session.oauth.scope.last</mark> .scope_data.public_profile.first_name	Chas
df4a5200.session.oauth.client./Common/social-ap_act_oauth_client_1_ag.state	
df4a5200.session.oauth.scope./Common/social-ap_act_oauth_scope_1_ag.scope	public_profile

3. You can see reporting on OAuth traffic at Access -> Overview -> OAuth Reports -> Client / Resource Server

Acce	cess » Overview : OAuth Reports : Client / Resource Server							
÷.	Active Sessions		OAuth Reports	▼ SWG Re	eports 👻	Event Logs ,		
С	Auth Clier	nt / Resour	ce Server	Perforr	nance			
Ti	me:							
La	st hour	T						
					OVERVIE	W		
	Requests Per	Second	Auth C	odes	Tokens	Refr	esh Tokens	Scope:
	0.03							
	0.02							
	0.01						$\Lambda$	
	0.00 01 PM	01:05 01:1	0 01:15	01:20	01:25	01:30 01:35	01:40	01:45

 You can see the session logs by going to Access-> Overview-> Active Sessions and click on the active session, or for past sessions under Access -> Overview -> Access Reports -> All Sessions Report (it runs by default and asks for a time period)

Access » Overview : Ac	cess Reports		
🗱 👻 Active Sessions	Access Reports	OAuth Reports 🛛 👻	SWG Reports - Event Logs -
Reports Browser	~	Session Details	- df4a5200 🛞
Favorites	-	😣 Export to CSV File	词 Show in Popup Window 🛐 View Report Constraints Current default report name: "All Sessions"
눩 Delete Favorite	💽 Run	Local Time	Log Message
Report Name		2017-05-31 13:49:19	/Common/social-ap:Common:df4a5200: Received User-Agent header: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53
		2017-05-31 13:49:19	/Common/social-ap:Common:df4a5200: New session from client IP 192.168.187.169 (ST=/CC=/C=) at VIP 192.168.187
		2017-05-31 13:49:24	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_client_1_ag: OAuth Client: authorization_code
		2017-05-31 13:49:24	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_client_1_ag: OAuth Client: User redirected to
		2017-05-31 13:50:10	/Common/social-ap:Common:df4a5200: New OAuth Authorization Code received
		2017-05-31 13:50:10	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_client_1_ag: OAuth Client: Requesting new to
		2017-05-31 13:50:14	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_client_1_ag: OAuth Client: succeeded for ser
		2017-05-31 13:50:14	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_scope_1_ag: OAuth Scope: getting list of sco
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_scope_1_ag: OAuth Scope: succeeded for s
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200: Username 'Chas Lesley'
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200: Following rule 'fallback' from item 'Facebook Variable Assign' to ending 'Allow
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200: Access policy result: LTM APM_Mode
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200: Received client info - Hostname: Type: Mozilla Version: 5 Platform: Win10 CP
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200:   Start (fallback)   OAuth Logon Page (Facebook)   Facebook OAuth Client (S

# 2.5 Lab 4: Troubleshooting

#### 2.5.1 Task 1: Logging Levels

 You can turn up the logging levels specific to OAuth at Access -> Overview -> Event Logs -> Settings. Often times *Informational* is enough to identify issues. It is recommended to start there before going to debug. In particular pay attention *session.oauth.client.last.errMsg* as it contains the errors the other side reported back to you.

<del>*</del> -	Active Sessions	Access Reports	OAuth F	Reports 🔫	SWG Rep	oorts 👻	Event Logs	-
	Name 🔺	Description		Access Syst	em Logs	URL Requ	iest Logs	Access

Edit APM Log Setting		^
<ul> <li>General Information</li> <li>Access System Logs</li> <li>URL Request Logs</li> <li>Access Profiles</li> <li>SSO Objects</li> </ul>	Publisher*: /Common/sys-db-access-publis Access Policy : Notice ACL : Notice Secure Web Gateway : Notice OAuth : Notice VDI : Notice	sher Create Per-Request Policy : Notice SSO : Notice ECA : Notice PingAccess Profile : Notice Endpoint Management System : Notice
		OK Cancel

#### 2.5.2 Task 2: Traffic Captures

1. You can actually examine what Big-IP has sent out when acting as a client/resource server. First, capture the traffic on the tmm channel:

tcpdump -i tmm:h -s0 -w /tmp/oauth.dmp

[root@bigip1:Active:Standalone] config # tcpdump -i tmm:h -s0 -w /tmp/oauth.dmp
cpdump: listening on tmm:h, link-type EN10MB (Ethernet), capture size 65535 bytes
C212 packets captured
12 packets received by filter
) packets dropped by kernel
[root@bigip1:Active:Standalone]

2. Then attempt your login using OAuth and ctrl-c the capture to end it. Now you need to ssldump the output:

ssldump -dr /tmp/oauth.dmp | more

[root@bigip1:Active:Standalone] config # ssldump -dr /tmp/oauth.dmp   more New TCP connection #3: 10.1.20.210(52064) <-> localhost.localdomain(10001) 0.0010 (0.0010) C>S
POST / HTTP/1.1
cache-control: no-cache
Postman-Token: 7d18ae0a-9335-4aba-98af-33797749aced
Authorization: Bearer a5f563285d005630134cd94330d23dcf9b33c615fffa01a30b25065afe45f285
User-Agent: PostmanRuntime/3.0.11-hotfix.2
Accept: */*
Host: api.f5agility.com
accept-encoding: gzip, deflate
Connection: keep-alive
client-session-id: abeb0683b03ea3beeecf069e272d3d36
session-key: abeb0683b03ea3beeecf069e272d3d36
profile-id: /Common/api-ap
partition-id: Common
session-id: 272d3d36

**Note:** Your SSL Ciphers must support ssldump utility. Refer to the following link for further details https://support.f5.com/csp/article/K10209

#### 2.5.3 Information: Logging at the Other Side

Sometimes the issue is not at your end and some providers have their own logging and reporting you can leverage. As an example, Google has a dashboard that reports errors.

#### 2.5.4 Information: The Browser

Although a lot of the critical stuff is passed back and forth directly without your browser being involved, you can at least validate the browser portions of the transaction are good (e.g. are you passing all the values you should, example below for Google).

# 2.6 Conclusion

#### 2.6.1 Learn More

#### Links & Information

• Access Policy Manager (APM) Operations Guide:

https://support.f5.com/content/kb/en-us/products/big-ip_apm/manuals/product/ f5-apm-operations-guide/_jcr_content/pdfAttach/download/file.res/f5-apm-operations-guide.pdf

Access Policy Manager (APM) Authentication & Single Sign On Concepts:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0. html

OAuth Overview:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/35.html#guid-c1b617a7-07b5-4ad6-9b84-29d6ecd789b4

#### OAuth Client & Resource Server:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/36.html#guid-c6db081e-e8ac-454b-84c8-02a1a282a888

#### OAuth Authorization Server:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/37.html#guid-be8761c9-5e2f-4ad8-b829-871c7feb2a20

#### • Troubleshooting Tips

#### - OAuth Client & Resource Server:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-sso-13-0-0/36.html#guid-774384bc-cf63-469d-a589-1595d0ddfba2

#### - OAuth Authorization Server:

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-sso-13-0-0/37.html#guid-8b97b512-ec2b-4bfb-a6aa-1af24842ee7a

#### 2.6.2 Lab Reproduction

If you are building your own, here is some important information about the environment not covered in the lab. This lab environment requires two Big-IPs. One will act as an OAuth Client and Resource (Client/RS) Server. The other will act as an OAuth Authorization Server (AS). Both must be licensed and provisioned for Access Policy Manager (APM).

On the OAuth Client/RS Big-IP you will need backend pools for the two virtual servers, the lab expects a webapp behind the Social VS that accepts a header named x-user and reposts it back to the user. The lab expects an API behind the API VS that can respond with a list of departments to a request to /department. Also, a DNS Resolver must be configured on this Big-IP, in our case we don't have a local DNS server to respond for the names used, so we are also leveraging an iRule and VS to answer DNS requests for specific names. You will need a browser for testing the social module and Postman for testing the API module.

# **Class 3: SWG - Securing Outbound Internet Access**

Welcome to the APM 231: SWG - Securing Outbound Internet Access lab. These lab exercises will instruct you on configuring F5 Secure Web Gateway (SWG) for typical use cases. This guide is intended to complement lecture material provided during the course and to serve as a reference guide when configuring SWG in your own environment. Expected time to complete: **3 hours** 

# 3.1 Lab Environment

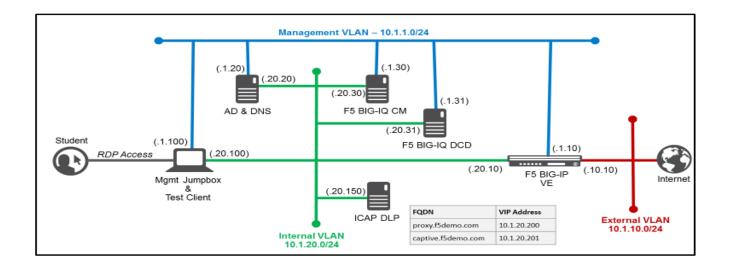
In the interest of time, the following components have been set up with basic configurations for you in a cloud-based virtual lab environment with:

- Windows Jump Host Provides remote access the virtual lab environment via RDP (note: you
  will need to connect to it using your Remote Desktop Client for Windows/Mac). This will also be
  your test client.
- BIG-IP Virtual Edition (VE) Pre-licensed and provisioned for Access Policy Manager (APM) and Secure Web Gateway (SWG)
- BIG-IQ Centralized Management (CM) VE BIG-IQ console
- BIG-IQ Data Collection Device (DCD) VE BIG-IQ logging node
- Windows Server Active Directory and DNS services
- DLP Server ICAP mode

Each student's lab environment is independent.

#### 3.1.1 Lab Environment Diagram

The following diagram illustrates the lab environment's network configuration and will be useful if you wish to replicate these exercises in your personal lab environment:



#### 3.1.2 Timing for Labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. Below is an estimate of how long it will take for each lab:

Lab Timing

Lab name (Description)	Time Allocated
Use Case: Enterprise Web Filtering	
Lab 1: SWG iApp - Explicit Proxy for HTTP and HTTPS	30 minutes
Lab 2: URL Category-based Decryption Bypass	25 minutes
Lab 3: Explicit Proxy Authentication - NTLM	25 minutes
Use Case: Access Reporting	
Lab 4: SWG Reporting with BIG-IQ	15 minutes
Use Case: Guest Access Web Filtering	
Lab 5: SWG iApp – Transparent Proxy for HTTP and HTTPS	15 minutes
Lab 6: Captive Portal Authentication	25 minutes
Use Case: SSL Visibility	
Lab 7: SSL Visibility for DLP (ICAP)	15 minutes

#### 3.1.3 General Notes

Provisioning Secure Web Gateway (SWG) requires Access Policy Manager (APM to also be provisioned.

When working with iApp templates for the first time, you should change the BIG-IP Configuration Utility's default "**Idle Time Before Automatic Logout**" setting to a larger value. This has already been done for you in the lab environment to save time.

### 3.1.4 Accessing the Lab Environment

To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces using HTTPS and SSH. You will also be using the Jump Host as a test client.

You class instructor will provide additional lab access details.

- 1. Establish an RDP connection to your Jump Host and login with the following credentials:
- User: JUMPBOX\external_user
- · Password: password
- 1. Use Firefox to access the BIG-IP GUI (https://10.1.1.10).
- 2. Login into the BIG-IP Configuration Utility with the following credentials:
- · User: admin
- · Password: admin

# 3.2 Lab 1: SWG iApp – Explicit Proxy for HTTP and HTTPS

In this lab exercise, you will learn how to automate and simplify a deployment of SWG using an iApp template.

Estimated completion time: 30 minutes

#### **Objectives:**

- · Create an Explicit Proxy configuration by deploying the SWG iApp template
- · Test web browsing behavior

#### Lab Requirements:

- BIG-IP with SWG licensed
- · BIG-IP must have access to the public Internet
- · BIG-IP must have access to a DNS server that can resolve queries for public Internet web site names
- The latest iApp for SWG can be downloaded from https://downloads.f5.com/ (browse to BIG-IP iApp Templates) Note: The iApp has already been downloaded and imported for you.

Before you can deploy the SWG iApp template, you must have the following objects configured:

- AD AAA server
- SWG-Explicit Access Policy
- Custom URL Filter
- Per-Request Access Policy

#### 3.2.1 Task 1 – Create an "SWG-Explicit" Access Policy for Authentication

#### Create an AD AAA Server

- Create an AD AAA server by selecting Access >> Authentication >> Active Directory and clicking on Create...
- Change the Name to AD_F5DEMO
- Change the Domain Name to **f5demo.com**
- Change Server Connection to Direct
- Change the Domain Controller to **10.1.20.20**
- Click Finished

🛪 🚽 Properties Gro	ups			
topenaes Gio	ups			
eneral Properties				
Name	AD_F5DEMO			
Partition / Path	Common			
Туре	Active Directory	Active Directory		
configuration				
-				
Domain Name	f5demo.com			
Server Connection	🔘 Use Pool 🖲 Direct			
Domain Controller	10.1.20.20			
Admin Name				
Admin Password				
Verify Admin Password				
Group Cache Lifetime	30	Days Clear Cache		
Password Security Object Cache Lifetime	30	Days Clear Cache		
Kerberos Preauthentication Encryption Type	None			
Timeout	15	seconds		

#### **Create a Per-Session Access Policy**

- Browse to Access >> Profiles / Policies >> Access Profiles (Per-Session Policies) and click Create...*
- Name the profile AP_Explicit_Auth
- Change the Profile Type to SWG-Explicit
- · Add English to the Accepted Languages list
- · Accept all other default settings and click Finished
- · Click on the Edit... link for the appropriate Access Policy created above

<b>#</b> -	Access I	Profiles	Per-Request	Policies	Policy Sync	Customization -				
Search										
1				Searc	n					
	<ul> <li>Status</li> </ul>	▲ Access	Profile Name	Search Applica		Per-Session Policy	Export	Сору	Logs	Virtual Se
	✓ Status	<ul> <li>Access</li> <li>AP_Explic</li> </ul>					Export Export			Virtual Se

• Select the + between Start and Deny and Add an HTTP 407 Response object

<u>(5</u>	Help Close
Access Policy: /Common/AP_Explicit_Auth Allow, Deny [default])	Edit Endings (Endings:
Start fallback + Deny	
Add New Macro	

Change the HTTP Auth Level to basic

Properties* Branch Rules	2				
Name: HTTP 407 Response					
407 Response Settings					
Basic Auth Realm					
HTTP Auth Level	basic 🔻				
Customization	1				
Language	en 🔻				
Logon Page Input Field #1	Username				
Logon Page Input Field #2	Password				
HTTP response message	Authentication required to access the resources				
Yes	Yes				
No	No				

- Click Save
- On the Basic branch of the HTTP 407 Object, Add an AD Auth Object

Beg	Begin typing to search				
	on Authentication Assi	anment Endpoint Security (S			
0	AD Auth	Active Directory authen			
$\bigcirc$	AD Query	Active Directory query t mapping			
0	CRLDP Auth	Certificate Revocation L			
$\bigcirc$	HTTP Auth	HTTP authentication of			
0	Kerberos Auth	Kerberos authenticatior			

Change the Server to /Common/AD_F5DEMO and change Show Extended Error to Enabled

Properties* Branch Rules				
Name: AD Auth				
Active Directory				
Туре	Authentication <b>T</b>			
Server	/Common/AD_F5DEMO V			
Cross Domain Support	Disabled 🔻			
Complexity check for Password Reset	Disabled <b>T</b>			
Show Extended Error	Enabled 🔻 👝			
Max Logon Attempts Allowed	3 🔻			
Max Password Reset Attempts Allowed	3 🔻			

Click Save

- On the Successful branch of the AD Auth Object, click on the Deny Ending and change it to Allow
- Click Save
- Click on the Apply Access Policy link

Apply Access Policy	
Access Policy: /Common/AP_Explicit_Auth Edit Endings	(Endings: Allow, Deny [default])
Start $fallback$ + $ X$ $Basic$ + $\rightarrow$ $AD Auth$ $fallback$ + $\rightarrow$ $fallback$ + $\rightarrow$	
HTTP 407 Response Negotiate	
	Select Ending
fallback + ->>	Allow
	Deny
Add New Macro	
An access policy consists of a start point, actions, and one or more endings. To ins right edge of the box. Click the <b>Add Macro</b> button to add a purpose-built set of pr	

## 3.2.2 Task 2 – Create a custom URL Filter

- Browse to Access >> Secure Web Gateway >> URL Filters and click Create...
- Name your filter LAB_URL_FILTER and click Finished
- Click on the first check box to select all categories

Hostname: bigip1 Date: Jun 8, 2017 IP Address: 10.1.1.10 Time: 9:44 AM (PD	User: <b>admin</b> T) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	Access » Secure Web Gatewa	y:URL Filters » LAB_URL_FILTER
Mage Statistics	🔅 👻 Properties	
iApps	General Properties	
🔋 Wizards	Name	LAB_URL_FILTER
SSL Orchestrator	Partition / Path	Common
SSL Orchestrator	Description	
Local Traffic	Update Delete	1
Traffic Intelligence	Associated Categories	
Acceleration		
Acceleration	Category	Sub-Category
Access	Custom Categories	
Overview	Abortion	
Profiles / Policies	🔽 🖸 Adult Material	
	Advocacy Groups	
Authentication	Bandwidth	
Single Sign-On	M Bandwidth	

• Click Allow at the bottom of the page



 Click the check box to select Social Web – Facebook and then click Block (for this lab, our URL filter will only block Facebook)

	Ð	Religion	6
		Security	0
		Shopping	Ð
	۵	Social Organizations	Ð
<b>V</b>		Social Web - Facebook	8
		Social Web - LinkedIn	Ð
		Social Web - Twitter	Ð
	۵	Social Web - Various	Ð
		Social Web - YouTube	Ð
	۵	Society and Lifestyles	Ð
		Special Events	0
		Sports	O
		Tasteless	O
		Travel	Ð
		Vehicles	٢
		Violence	٢
		Weapons	•
Allo	<b>w</b> [	Confirm Block	

## 3.2.3 Task 3 – Create a "Per-Request" Access Policy

- Browse to Access >> Profiles / Policies >> Per-Request Policies and click Create...
- Name your policy Lab_Per_Request
- Click Finished
- Click on the **Edit...** link for the appropriate Per-Request Policy created above, then go back to the VPE tab in your browser

Access » Profiles / Policies : Per-Request Policies							
🚓 🚽 Access Profiles 🛛 P	Per-Request Policies	Policy Sync	Customizat				
			_	_			
*	Searc	h 🚺			C	reate Import	
Per-Request Policy Na	ame	Per-Request Polic	y Export	Сору	Virtual Servers	Partition / Path	
Lab_Per_Request		🗗 Edit	Export	Сору		Common	
Delete							

- Click on the + symbol between Start and Allow
- Go to the General Purpose tab and add a Protocol Lookup object

6			
er-Request	: Poli	icy: /Common/Lab	Per Request Edit Endings (Endings: Allow, Reject [default])
Startfallback	Beg	in typing to search	
Add New Macro	Auth	nentication Assignment End	point Security (Server-Side)
	0	Application Filter Assign	Assign a Filter to lookup Applications
Add New Subrou	$\bigcirc$	Application Lookup	Application Lookup
	0	Category Lookup	Category Lookup
An access policy of an action, click or	$\bigcirc$	Empty	An Empty Action for constructing custom Branch Rules
You can get start	0	HTTP Headers	Modify HTTP Headers
access policy that Please see the O	$\bigcirc$	iRule Event	Raises an iRule ACCESS_PER_REQUEST_AGENT_EVENT event for use with cust
Please see the <u>Ol</u>	0	Logging	Log custom messages and session variables for reporting and troubleshooting
$\rightarrow$	۲	Protocol Lookup	Protocol Lookup
	0	Proxy Select	Proxy Select

- Click Add Item
- Click Save
- On the HTTPS branch, click the + and Add a Category Lookup object (General Purpose tab)

6				
Per-Request Pol	icy:	/Common/Lab_Per_	Request Edit Endings (Endings: Allow, Rej	ject [de
Start fallback +-	otocol	${\frac{1}{1}} + \frac{1}{1} +$		
Add New Macro				
Add New Subroutine	Beg	in typing to search		
	Auth	entication Assignment End	point Security (Server-Side) General Purpose	
An access policy consist action, click on the <b>x</b> on	0	Application Filter Assign	Assign a Filter to lookup Applications	
You can get started with access policy that you ca	$\bigcirc$	Application Lookup	Application Lookup	
Please see the Oplice H		Category Lookup	Category Lookup	
	$\bigcirc$	Empty	An Empty Action for constructing custom Branch	Rules
	0	HTTP Headers	Modify HTTP Headers	
		iRule Event	Raises an iRule ACCESS PER RECUEST AGENT	EVENT

- · Select Use SNI in Client Hello for Categorization Input
- Click Save
- After the Category Lookup, Add a URL Filter Assign Object (from the General Purpose tab) and choose URL Filter /Common/LAB_URL_FILTER

<b>f5</b>	
*Per-Request Policy: /Comm	on/Lab_Per_Request Edit Endings (Endings: Allow, Reject [default])
Start fallback + - X HTTP	+→> <u>Category Lookup</u> +→> * <u>URL Filter Assign</u> Confirm +→> <u>Reject</u> fallback +→> <u>Reject</u>
Add New Macro	Properties*     Branch Rules       Name:     URL Filter Assign
Add New Subroutine Add New Subrou An access policy consists of a start point, acti	URL Filter         /Common/LAB_URL_FILTER ▼           Note: To supply categories, a Category Lookup item must occur in the per-request policy before

Important: Change the Ending of the Allow outcome on the "fallback" branch from "Reject" to Allow

<u>(6</u>	
Per-Request Policy: /Com	mon/Lab_Per_Request [Edit Endings] (Endings: Allow, Reject [default])
Start fallback +	Category Lookup feilback + →→ URL Filter Assign Confirm + →→ Reject feilback + →> Reject feilback + →> Allow Allow

## 3.2.4 Task 4 – Create Explicit Proxy Configuration using the SWG iApp

Import the SWG iApp template into the BIG-IP – Note: This has been done for you.

- In the BIG-IP Management UI, browse to iApps >> Templates and click Import...
- Click **Choose File** or **Browse...** and select the iApp file (at the time of writing the current version is 1.1.0rc4 (f5.secure_web_gateway.v1.1.0rc4.tmpl).
- Click Open and Upload

#### Create a SWG proxy configuration

- Browse to iApps >> Application Services
- Click Create...
- · Change the name to SWG
- Change the Template to f5.secure_web_gateway.v1.1.0rc4 (your version may be newer)

1. Answer the questions as follows:

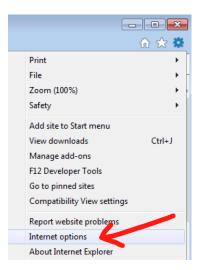
Question   Answer	
Do you want to see inline help?   Yes, show inl	ine help
Do you want to enable advanced options?	No, do not enable advanced options
Which type of SWG configuration do you want to deploy	Explicit Proxy
Do you want to use ICAP to forward requests for inspection by DLP servers?	No, do not use ICAP for DLP
What IP address and port do you want to use for the virtual server?	<ul><li>– IP Address: 10.1.20.200</li><li>– Port: 3128</li></ul>
What is the FQDN of this proxy?	proxy.f5demo.com. The local hosts file on your Jump Host has already been modified to resolve this FQDN to the correct IP address indicated above.
On which ports should the system accept HTTP traffic?	80
On which ports should the system accept HTTPS traffic?	443
Which SWG-Explicit Access Policy do you want to use?	AP_Explicit_Auth
Which Per-Request Access Policy do you want to use?	Lab_Per_Request
Do you want the system to forward all name requests?	Yes, forward all name requests
Which DNS servers do you want to use for forwarding?	– IP: 10.1.20.20 – Port: 53
Which SSL profile do you want to use for client-side connections?	Create a new Client SSL profile
Which Subordinate CA certificate do you want to use?	f5agility.crt
Which CA key do you want to use?	f5agility.key
Does the key require a password? If so, type it here	F5labs
Which SSL profile do you want to use for server-side connections?	Create a new Server SSL profile

2. Click Finished – you will see a large number of objects created for you on the Components tab.

## 3.2.5 Task 5 – Verify that the "F5 Agility CA" certificate is trusted

A Windows Domain Group Policy was configured to deploy the CA certificate that SWG uses to forge new certificates (on behalf of the origin server) to domain-joined machines.

- Open Internet Explorer on your Jump Host client machine
- Click the gear icon or hit Alt-X and select Internet options



- Go to the Content tab and click Certificates
- Click on the **Trusted Root Certification Authorities** tab and scroll down. You should see the **F5 Agility CA** certificate in the list.

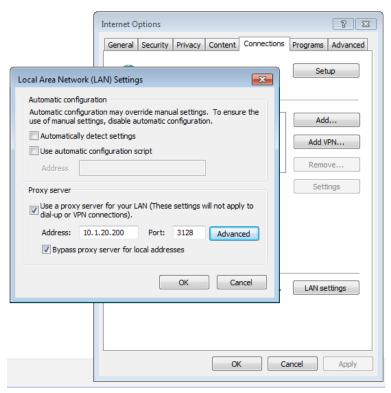
	ty Privacy Content Connec certificates for encrypted conne SL state Certificates		Ed		
AutoComplete Au on for Feeds and We	Certificates Intended purpose:				

• Double-click on the certificate to view its properties, then close this window and the Certificates window.

## 3.2.6 Task 6 – Testing

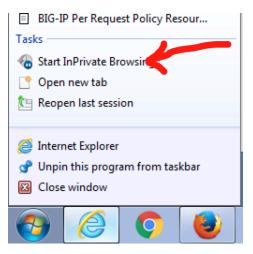
#### Configure your browser with a "Proxy Server"

- · Go to the Connections tab and click LAN settings
- Enable the checkbox for Use a proxy server for your LAN and enter:
  - Address: 10.1.20.200
  - Port: 3128
- Click OK twice.



#### Test 1:

- · Open a new Internet Explorer "InPrivate" browser window on your Jump Host client machine
- Browse to https://www.google.com

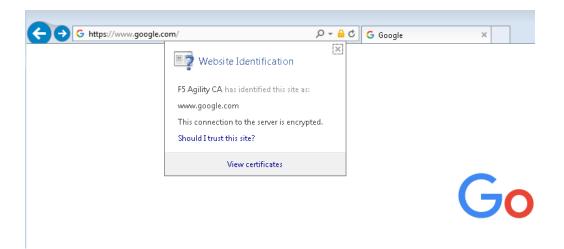


- The browser should prompt you for authentication. Submit your credentials:
  - User: user1
  - Password: AgilityRocks!
- · Verify defined user has an Access Session ID
- Browse to Access > Overview > Active Sessions

Access » Overview : Active Sessions					
🔅 🚽 Active Sessions	Access Reports	OAuth Re	eports <del>-</del>	SWG Reports 🛛 👻	Event Logs 🛛 👻
Display Options					
Auto Refresh	Disabled	▼ Re	fresh		
Refresh Session Table					
Total Active Sessions					
Active Session Count	1				
*	Se	arch			
Status 🛨 🗢 Se	ession ID Variables	▲ User	Client IP	Start Time	Expiration
🔲 🥥 🗈 a5a0	aa83 View	user1	10.1.20.100	2017-06-19 01:26:21	2017-06-19 01:43:02
Kill Selected Sessions					

#### Test 2:

• Using an InPrivate browser window from the client test machine, go to https://www.google.com and verify the SSL certificate is signed by the F5 Agility CA you configured in Lab 1



• Using an InPrivate browser window from the client test machine, go to https://www.wellsfargo.com and examine the certificate to verify that it is signed by the same **F5 Agility CA** you configured in Lab 1

	0 0 1
o.com/	Ø-∎c
Website Identification	×
F5 Agility CA has identified this site as:	
www.wellsfargo.com	
This connection to the server is encrypt	ed.
Should I trust this site?	
View certificates	

#### Test 3:

• Using an InPrivate browser window from the client test machine, go to https://www.facebook.com and verify that you are instead delivered a SWG Block Page, in accordance to the URL Filter you configured above.



# 3.3 Lab 2: URL Category-based Decryption Bypass

In this lab exercise, you will bypass SSL decryption based on requests to URLs categorized as financial services web sites.

Estimated completion time: 25 minutes

#### **Objectives:**

- · Apply a new Per-Request Policy to bypass SSL decryption for specific URL categories
- · Test web browsing behavior

#### Lab Requirements:

· Lab 1 previously completed successfully (working SWG iApp deployment)

## 3.3.1 Task 1 – Copy and configure new Per-Request Policy

- Copy the Lab_Per_Request Per Request Policy by browsing to Access Policy > Per-Request Policies and click Copy
- Name the copy Lab_Per_Request_SSL_Bypass
- Edit the new Per-Request Policy by clicking Edit, then go to the VPE tab in your browser
- Modify the Encrypted Category Lookup object to include a branch for SSL Bypass:
- · Click on the existing Category Lookup object
- On the Properties tab, change the name to Encrypted Category Lookup
- · Click to access the Branch Rules tab
- · Click Add Branch Rule and name it Banks
- · Click Change to modify the Expression of this new Branch Rule
- Click Add Expression
- Change Agent Sel: to Category Lookup
- Change Category is: to Financial Data and Services
- Click Add Expression
- Click Finished
- Click Save
- Add an SSL Bypass Set object (from the General Purpose tab) on the Banks branch of the Encrypted Category Lookup
- Click Save
- Add an SSL Intercept Set object (from the General Purpose tab) on the "fallback" branch of the Encrypted Category Lookup
- Click Save
- Add a URL Filter object on the SSL Bypass Branch; select the LAB_URL_FILTER URL filter previously created in Lab1
- Click Save

• Change the Allow branch to an ending of Allow

<b>(5</b> )		
Per-Request Policy: /Com	mon/Lab_Per_Request_SSL_Bypass Edit Endings (Endings: Reject [default], Allow)	
Start - fallback +	HTTPS +	->
	Bypass URL Filter	+→>→ <u>Reject</u>
	Fallback	+→>→ <u>Reject</u>
Protocol Lookup	fallback + ->>- SSL Intercept Set Fallback + ->>-	
	SSL Filter Assign	+->>
	fallback	+->>
	fallback + ->>	Allow

Add New Macro

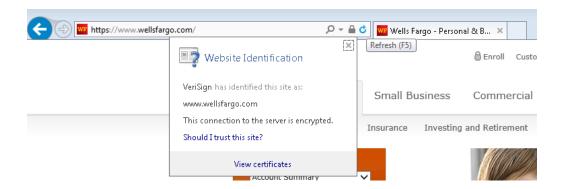
## 3.3.2 Task 2 – Reconfigure SWG iApp to assign New Per-Request Policy

- Browse to iApps >> Application Services > Applications"
- Click on SWG
- Click Reconfigure
- · Find the section Which Per-Request Access Policy do you want to use?
- Change the per-request policy to Lab_Per_Request_SSL_Bypass
- Scroll to the bottom and click finished

## 3.3.3 Task 3 – Testing

#### Test 1:

- Open Internet Explorer on your Jump Host client machine
- Browse to http://www.wellsfargo.com
- The browser should prompt you for authentication. Submit your credentials.
- User: user1
- **Password**: AgilityRocks!
- Verify the site loads correctly and inspect the SSL certificate to confirm that it is originated from Wells Fargo and SSL Bypass was enabled



# 3.4 Lab 3: Explicit Proxy Authentication – NTLM

In this lab exercise, you will reconfigure authentication for seamless login of AD domain-joined client using NTLM.

Estimated completion time: 25 minutes

#### **Objectives:**

- · Enable APM client-side NTLM authentication for the SWG explicit proxy
- · Test web browsing behavior

#### Lab Requirements:

· Lab 1 previously completed successfully (working SWG iApp deployment)

## 3.4.1 Task 1 – Logout and log back in as domain user

- · Logout of the windows remote desktop.
- · Login as a domain user with the following credentials (Switch User/Other User):
  - Username: F5DEMO\\user1
  - Password: AgilityRocks!

## 3.4.2 Task 2 – Join BIG-IP to Domain

- Use Firefox to access the BIG-IP GUI (https://10.1.1.10, admin/admin)
- · Browse to Access >> Authentication : NTLM : Machine Account
- Click Create
- · Fill out the fields as follows:
  - Name: agility-ntlm
  - Machine account: bigip1
  - Domain FQDN: f5demo.com
  - Domain controller FQDN: f5demo-dc.f5demo.com
  - Admin user: admin
  - Admin password: AgilityRocks!

Access » Authentication : NTLM : Machine Account » New Machine Account						
General Properties						
Name	agility-ntlm					
Configuration						
Machine Account Name	bigip1					
Domain FQDN	f5demo.com					
Domain Controller FQDN	f5demo-dc.f5demo.com					
Admin User	admin					
Admin Password	•••••					
Cancel Join						

- Click Join
- Create a new NTLM Auth Configuration
- Browse to Access >> Authentication : NTLM : NTLM Auth Configuration
- Click Create

Name: agility-ntlm

Machine Account Name: agility-ntlm

Domain controller FQDN: f5demo-dc.f5demo.com

#### Click Add

Access » Authentication : NTLM : NTLM Auth Configuration » New NTLM Auth Configuration			
General Properties			
Name	agility-ntlm		
Configuration			
Machine Account Name 🗧 🕂	agility-ntlm 💌		
Domain Controller FQDN List	Add f5demo-dc.f5demo.com		
Cancel Finished			

Click Finished

## 3.4.3 Task 3 – Create a new Access Policy

- Browse to Access >> Profiles / Policies >> Access Profiles (Per-Session Policies) and click Create...
- Name the profile AP_Explicit_NTLM
- Change the Profile Type to SWG-Explicit

Under Configurations:

Modify User Identification Method to Credentials

#### Modify NTLM Auth Configuration to agility-ntlm

- · Add English to Accepted Languages
- · Accept all other default settings and click Finished
- Click on the Edit... link for the appropriate Access Policy created above
- On the VPE browser tab, select the + between Start and Deny and Add a NTLM Auth Result object (from the Authentication tab)
- Click Save
- On the Successful branch of the NTLM Auth Result Object, click on the Deny Ending and change it to Allow
- Click Save
- Click Apply Access Policy

6	
Access Policy: /Common/AP_Explicit_NTLM	Edit Endings
Start fallback + Successful + - Allow <u>NTLM Auth Result</u> fallback + - Deny	

## 3.4.4 Task 4 – Reconfigure SWG iApp to apply NTLM Access Policy

- Browse to "iApps >> Application Services > Applications
- Click on SWG
- Click Reconfigure
- · Find the section Which SWG-Explicit Access Policy do you want to use?
- Change the per-request policy to AP_Explicit_NTLM
- Browse to the bottom and click Finished

## 3.4.5 Task 5 – Testing

Before testing, close all browser sessions and kill all session in the GUI under Access > Overview > Active Sessions

- Open Internet Explorer on your Jump Host client machine
- Browse to https://www.f5.com. The browser should not prompt you for authentication since NTLM authentication is happening in the background (transparent to the user).
- Examine the user session details under Access > Overview > Active Sessions. Click on the session ID for details. You can see that NTLM authentication was performed.



#### Display Opti

Auto Refres

Access » Overview : Ac	cess Reports			
🔅 🚽 Active Sessions	Access Reports	OAuth Reports 🛛 🔫	SWG Reports - Event Logs -	Total Active
Reports Browser	«	Session Details	bfde395c 🗵	Active Ses
Favorites	Ξ	🛞 Export to CSV File	🔟 Show in Popup Window 📳 View Report Constraints Current default report name: "All Sessions"	
눩 Delete Favorite	💽 Run	Local Time	Log Message	*
Report Name		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: User user1@F5DEMO from JUMPBOX is authenticated	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Received User-Agent header: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko.	🛛 🔽 🔽 St
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: New session from client IP 10.1.20.100 (ST=/CC=/C=) at VIP 10.1.20.200 Listener /Common/SWG.app/SWG_proxy_vs (Reput	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Following rule 'Successful' from item 'NTLM Auth Result' to ending 'Allow'	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Access policy room: SWG-Explicit	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Received client info - Hostname: Type: E Version: 11 Platton, vin7 CPU: unknown UI Mode: Full Javascript Support: 1 Active	Kill Select
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c:   Start (fallea v)   NTLM Auth Result (Successful)   Allow   Engine is: Allow	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Per-request policy, with trace:   Start (fallback)   Protoest workup (fallback)   Allow  , Ending is: Allow	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Source IP:10.1.20.100: Destination URL:https://f5.com/: User:user1: SSL bypass.0: UrlCategory is:/Common/Information_Tech	

# 3.5 Lab 4: SWG Reporting with BIG-IQ

In this lab exercise, you will explore SWG Reporting with Big-IQ Access.

Estimated completion time: 15 minutes

#### **Objectives:**

- · View SWG activity reports using BIG-IQ Access
- · Test web browsing behavior

#### Lab Requirements:

· Lab 3 previously completed successfully (working SWG iApp deployment)

#### 3.5.1 Task 1 – Generate New Web Browsing Traffic

 Open Internet Explorer on your Jump Host machine and browse to several web sites, including facebook.com and banking sites to generate reporting data for traffic that is allowed, decrypted, SSL bypassed, and blocked by SWG.

## 3.5.2 Task 2 – View SWG Reporting Data

- Using Firefox, browse to the BIG-IQ Management GUI **https://10.1.1.30**
- · Login with the following credentials:

Username: admin

Password: admin

- Browse to Monitoring > Dashboards > Access > Secure Web Gateway > Users to see the activity by users
- · Click on Categories to view category information,
- Adjust the time period to 30 days or less

🚯 BIG-IQ	🐠 Standalone   Hostname bigiq1,15ogility.com   IP.Address: 10.1.1.30   Time Jul 07,2017-20.59(PDT)   Administrator   admin 🛓-
Monitoring Configuration	Deployment Devices System
< ALERTS & NOTIFICATIONS	Summary
▶ AUDITLOGS	ACCESS GROUP/DEVICE: TIMEFRAME:
▼ DASHBOARDS	All Managed Devices (SWG) * Last O days *
▼ Access	
Application Summary	I Thu Fri9 Sat Sun Mon12 Tue Wed14 Thu Fri16 Sat Sun Mon19 Tue Wed21 Thu Fri23 Sat Sun Mon26 Tue Wed28 Thu Fri30 Sat1 Sun Mon3 Tue Wed5 Thu Fri7
▶ Federation	
▶ Sessions	REQUEST COUNTS PER ACTION OVER TIME
User Summary	AVG # requests / 11 days — Allowed — Blocked — Overall
▶ Logging Messages (AII)	d
Remote Logging Configuration	20,000
<ul> <li>Secure Web Gateway</li> </ul>	15,000
▶ Device	
DNS	10.000
▶ Local Traffic	
▶ REPORTS	5,000
▶ EVENTS	
	Thu 15 581.17 Mon 19 Wed 21 Fri 23 jun 25 Tue 27 Thu 29 july Mon 03 Wed 05 Fri 07 jul 09
	TOP 10 HOST NAMES BY REQUEST COUNT TOP 10 CATEGORIES BY REQUEST COUNT TOP 10 USERS BY REQUEST COUNT
	www.google.com         123         Search Engines and P         20856         student         21906           www.google-analytics         70         Information Technola         556         user1         316
	dlptest.com         51         Web Analytics         301         joe.hacker@yaho         83           pagead2.googlesyndic         35         Advertisements         226         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236         236
	Auvertisements 230

Click on SSL Bypass and view the breakdown between HTTPS Inspected and Bypassed Content

🚯 BIG-IQ	# Starosacore   Hostmarke biguit Soguity.com   # Address 1011.30   Hile Juli(),2017 (10100)   Addresstrator   addre
Monitoring Configuration	n Deployment Devices System
ALERTS & NOTIFICATIONS	SSL Bypass
▶ AUDIT LOGS	CSV Report Ref
▼ DASHBOARDS	ACCESS GROUP/DEVICE: TIMEFRAME:
▼ Access	Requests
Application Summary	u Fri9 Sat Sun Mon12 Tue Wed14 Thu Fri16 Sat Sun Mon19 Tue Wed21 Thu Fri23 Sat Sun Mon26 Tue Wed28 Thu Fri30 Sat1 Sun Mon3 Tue Wed5 Thu Fri
▶ Federation	
▶ Sessions	TOP 5 SSL BYPASS BY CONNECTION COUNT OVER TIME
User Summary	AVG # connections / 11 days HTTP/HTTPS inspected
▶ Logging Messages (All)	
Remote Logging Configurat	28,000
▼ Secure Web Gateway	
Applications	13,009
Application Families	10,000
Categories	
Client IP Addresses	5,000
Host Names	
SSL Bypass	Thu 15 Sat 17 Mon 19 Wed 21 Fri 22 jun 25 Tue 27 Thu 29 july Mon 03 Wed 05 Fri 07 jul 09
SWG Logs	4
URL Filters	Top 1000 SSL Bypass by Connection Count

Click on Host Name to look at the hosts your users are accessing

🏅   BIG-IÇ	?						Standalone   Hostname	: bigiq1.f5agiity.com	IP Address: 10.1.1.30			ator   admin
Monitoring	Configuration	Deployment	Devices	System								
ALERTS & NOTIFICA	ations	Host Names										
AUDIT LOGS											CSV Rep	port Re
DASHBOARDS		ACCESS GROUP/DE All Managed De		Last 30 days		Blocked						
▼ Access				,	Requests	s	111					
Application Sur	nmary	II Fri 9	Sat Sun M	on 12 Tue Wed 14	Thu Fri16 Sat	Sun Mon 19 Tue W		Sat Sun Mon 2	26 Tue Wed 28 Thu	ı Fri 30 Sat 1 Sun	Mon 3 Tue W	ed 5 Thu
▶ Federation												
▶ Sessions						TOP 5 HOST N	AMES BY REQUEST O	OUNT OVER TIME				
User Summary				-o- www.google.	om <u> </u>	google-analytics.com	-o- ssl.gstatic.	com <u></u>	bagead2.googlesyndica	tion.com —o— d	lptest.com	
User Summary ► Logging Messa	ges (All)	AVG # re	quests / 11 days		om ——— www			com <u></u>		tion.com —o— d	lptest.com	Overa
	E	AVG # re	quests / 11 days	—o— www.google.	om <u>-o-</u> www.			com — <del>o</del> — j		tion.com —o— d	lptest.com	-o- Overal
<ul> <li>Logging Messag</li> </ul>	g Configurat	1	iquests / 11 days	<b>→o</b> → www.google.	om <u> </u>			com —— j		tion.com ————— d	lptest.com	Overa
▶ Logging Messaj Remote Loggin	g Configurat	300 🔍	equests / 11 days	www.google.	om <u> </u>			com ———		tion.com —o— d	lptest.com	Overa
<ul> <li>Logging Messag</li> <li>Remote Logging</li> <li>Secure Web Gat</li> </ul>	g Configurat	300 <b></b> 250 200	iquests / 11 days	www.google.	om _o_ www					tion.com ————— d	lptest.com	Overa
<ul> <li>Logging Messag</li> <li>Remote Loggin</li> <li>Secure Web Gat</li> <li>Applications</li> </ul>	g Configurat	300 <b></b> 250 200 150	quests / 11 days	www.google.						tion.com —o— d	lptest.com	-o- Overa
<ul> <li>Logging Messau</li> <li>Remote Logging</li> <li>Secure Web Gat</li> <li>Applications</li> <li>Application F</li> </ul>	g Configurat	300 <b></b> 250 200	iquests / 11 days	www.google.	om			com —o—		tlon.com —o— d	lptest.com	Overa
Logging Messag Remote Logging     Secure Web Gat     Applications     Application F     Categories	g Configurat	300 <b></b> 250 200 150	iquests / 11 days		omwww.			com		tlon.com —o— d	lptest.com	Overa

• Click on **URLs** to get detail on what URLs your users are accessing

🚯 BIG-I	IQ						<ul> <li>Standalone</li> </ul>	Hostname: bi	giq1.f5agility.com	P Address: 10.1.1.3	I Time: Jul 07, 2017 21:03	2(PDT)   Administrat	tor   admin 👤
Monitoring	Configuration	Deployment	Devices	System									Q
ALERTS & NOTIF	CATIONS	URLs											
▶ AUDIT LOGS												CSV Rep	ort Refresh
▼ DASHBOARDS		ACCESS GROUP/D All Managed De		TIMEFRAME: Last 30 days		ow Blocked							
▼ Access					Requ			111					_
Application :	Summary	II Fri 9	Sat Sun N	lon 12 Tue Wed 14	Thu Fri 16 Sat	Sun Mon 19	Tue Wed 21 Th	i Fri 23 Sat	Sun Mon 26	Tue Wed 28 Thu	Fri 30 Sat 1 Sun M	Aon 3 Tue Wed 5	Thu Fri 7 II ف
▶ Federation													
▶ Sessions						т	OP 5 URLS BY REC	UEST COUNT	OVER TIME				
User Summa	iry		ttps://clients1.goog verall	le.com/	http://atf.msn.com/c,	gif? ——	https://www.google	.com/ _	<ul> <li>https://www.j</li> </ul>	google-analytics.com/	-o- https://www	w04.wellsfargomedia	3.C
▶ Logging Mes	ssages (All) =		equests / 11 days										
Remote Log	ging Configurat	م	_										
▼ Secure Web	Gateway	20,000 🟊											
Application	ns	15,000											
Application	n Families	13,000											
Categories	;	10,000											
Client IP A	ddresses												
Host Name	es	5,000											
SSL Bypas	s	o <b>o</b>									-0		0
SWG Logs		Thu 15	Sat 17	Mon 19	Wed 21	Fri 23	Jun 25	Tue 27	Thu 29	July N	ion 03 Wed 05	Fri 07	Jul 09
URL Filters	5												
URLs											✓ Filter		Y

# 3.6 Lab 5: SWG iApp - Transparent Proxy for HTTP and HTTPS

In this lab exercise, you will configure SWG in transparent proxy mode to support environments where clients do not leverage an explicit proxy. BIG-IP is deployed inline on the client's outbound path to the Internet to intercept the traffic.

Estimated completion time: 15 minutes

#### **Objectives:**

- Deploy SWG in transparent proxy mode
- · Test web browsing behavior

#### Lab Requirements:

- · Lab 1 previously completed successfully (working SWG iApp deployment)
- BIG-IP must be in path between the client workstation and the Internet (this has already been done for you in this lab)

## 3.6.1 Task 1 – Create a new Access Policy

- Use Firefox to access the BIG-IP GUI (https://10.1.1.10, admin/admin)
- Browse to Access >> Profiles / Policies >> Access Profiles (Per-Session Policies) and click Create...
- Name the profile AP_Transparent
- Change the Profile Type to SWG-Transparent
- Add English to Accepted Languages
- Accept all other default settings and click Finished
- Click on the Edit... link for the appropriate Access Policy created above
- Go to the VPE tab in your browser and on the **fallback** branch, click on the **Deny** Ending and change it to **Allow**
- Click Save
- Click Apply Access Policy

## 3.6.2 Task 2 – Reconfigure SWG iApp to apply Transparent Access Policy

- Browse to iApps >> Application Services > Applications
- Click on SWG
- Click Reconfigure
- · Change Configuration Type to Transparent Proxy
- Find the section Which SWG-Transparent Access Policy do you want to use?
- Change Access Policy to AP_Transparent
- · Find the section Which Per-Request Access Policy do you want to use?
- Change the per-request policy to Lab_Per_Request
- · Set Should the system translate client addresses to Yes...
- · Set Which SNAT mode do you want to use to use SNAT Auto Map
- Browse to the bottom and click Finished

## 3.6.3 Task 3 – Testing

- Open Internet Explorer on your Jump Host client machine
- Ensure Internet Explorer options are configured to *not* use an explicit proxy
- Browse to https://www.nhl.com. You should not be prompted for authentication.

# 3.7 Lab 6: Captive Portal Authentication

In this lab exercise, you will a captive portal to authenticate client connecting to the Internet through the SWG transparent proxy.

Estimated completion time: 25 minutes

#### **Objectives:**

- · Configure SWG with a Captive Portal to facilitate client authentication
- · Test web browsing behavior

#### Lab Requirements:

· Lab 5 previously completed successfully (working SWG transparent proxy deployment)

### 3.7.1 Task 1 – Create a new Access Policy

- Use Firefox to access the BIG-IP GUI (https://10.1.1.10, admin/admin)
- Browse to Access >> Profiles / Policies >> Access Profiles (Per-Session Policies) and click Create...
- Name the profile AP_Transparent_Captive_Portal
- · Change the Profile Type to SWG-Transparent
- Change Captive Portals to Enabled
- Set Primary Authentication URI to https://captive.f5demo.com
- · Add English to Accepted Languages
- · Accept all other default settings and click Finished
- · Click on the Edit... link for the appropriate Access Policy created above
- On the VPE browser tab, select the + and Add a Message Box object (from the General Purpose tab)
- For the Message, enter: Welcome to F5 Agility Guest Wifi Access. Please click the link to accept our terms and access the internet.
- For the Link enter Go
- Click Save
- · Select the + after the message box and Add a Logon Page object.
- Configure the Logon Page as shown below:

Properties Brand	h Rules					
Name: Logon Page						
Logon Page Ager	nt					
Split domain from fu	ull Username	No 🔻				
CAPTCHA Configure	ation	None <b>T</b>				
Туре	Post Vari	able Name	Session Variable Name	Clean Variable	Values	Read Only
1 text 🔻	username		username	No 🔻		No 🔻
none 🔻	password		password	No 🔻		No 🔻
3 none 🔻	field3		field3	No 🔻		No 🔻
4 none 🔻	field4		field4	No 🔻		No 🔻
5 none 🔻	field5		field5	No 🔻		No 🔻
Customization						Import
Language en T Reset all defau						efaults
Form Header Text	Secure Log	on for F5 Ne	tworks			
Logon Page Input Field # 11 ^{enter} email address						

- Click Save
- Click on the **Deny** ending and change it to **Allow**
- Click Apply Access Policy

<u>6</u>	
Access Policy: /Common/AP_Transparent_Captive_Portal	Edit Endings
$\begin{array}{ c c c c c c c c c c c c c c c c c c c$	

## 3.7.2 Task 2 – Reconfigure SWG iApp to enable Transparent Capture Portal

- Browse to iApps >> Application Services > Applications
- Click on SWG
- Click Reconfigure
- Find the section Which SWG-Transparent Access Policy do you want to use?
- Select AP_Transparent_Captive_Portal
- Change Configure the transparent proxy to relay to a Captive Portal to Yes, relay to a captive portal
- · Set the Captive Portal Configuration as follows:
  - IP Address: 10.1.20.201

- Port: 443
- SSL Certificate: captive.f5demo.com
- SSL Key: captive.f5demo.com
- Browse to the bottom and click Finished

## 3.7.3 Task 3 – Testing

- Open Internet Explorer on your Jump Host client machine
- Ensure Internet Explorer options are configured to NOT use an explicit proxy
- · Browse to https://www.nhl.com
- You should be redirected to the capture portal page, prompted to accept the policy by clicking **Go**, then prompted to provide your email address before being allowed through.

# 3.8 Lab 7: SSL Visibility for DLP (ICAP)

In this lab exercise, you will send decrypted traffic to an ICAP-based Data Loss Prevention (DLP) service for inspection. The DLP will block HTTP POSTs (uploads) of certain content such as credit cards numbers and documents with Top Secret data classification labels.

Estimated completion time: 15 minutes

#### **Objectives:**

- Re-configure the SWG iApp to send unencrypted HTTP and decrypted HTTPS traffic to an ICAP (DLP) server
- · Verify that the DLP service is able to see SWG proxy traffic and block if a policy violation occurs

#### Lab Requirements:

• Working SWG iApp deployment

## 3.8.1 Task 1 – Re-configure SWG iApp to enable ICAP inspection

- Browse to iApps >> Application Services > Applications
- Click on SWG
- Click Reconfigure
- · Scroll down to the ICAP Configuration section
- · Change the ICAP option to Yes, create a new ICAP DLP deployment
- Enter 10.1.20.150 as the IP address of the DLP server (the default port of 1344 is correct).

ICAP Configuration	
Do you want to use ICAP to forward requests for inspection by DLP servers?	Yes, create a new ICAP DLP deployment
	If you choose to create a new deployment, the iApp will configure the objects necessary to enable inspection of HTTP POST requests by one or more data loss prevention (DLP) servers.
To which DLP server(s) should this BIG-IP LTM forward HTTP POST requests?	IP Address: 10.1.20.150 Port: 1344 X Add
	Enter the IP address and port of the each DLP server. Click Add to create a new row. A gateway-icmp monitor will be configured on the DLP server pool.
Enter the size, in bytes, of the ICAP preview length:	1024
	ICAP preview length specifies how much of the request ICAP will inspect to determine whether to receive the remaining part of the message.

· Browse to the bottom and click Finished

## 3.8.2 Task 2 – Testing

- · Open Internet Explorer on your Jump Host client machine
- Browse to http://dlptest.com
- If you are prompted for authentication, login as user1 with password AgilityRocks!
- Click on the HTTP Post link at the top of the page.
- Fill in the **Subject** and **Message** fields with some random text and then add a credit card numbers such as **4111 1111 1111 1111**.
- Click on the **Submit** button to see if the DLP service detects this. ***Hint:** You should receive a blocking page message.*
- Go back to the previous page try submitting again but with the words **top secret**. Again, you should receive a blocking page from the DLP service.
- Now, go back to the previous page and click on the HTTPS Post link at the top of the page.
- Perform the credit card number and top secret submissions again. You should again see the blocking
  pages since SWG is decrypting the HTTPS connection and sending the decrypted POST data to the
  DLP service for inspection.
- If you want to see the DLP policy violations, browse to https://10.1.20.150/logs. Log in as mydlp with password mydlp.

# 3.9 Conclusion

## 3.9.1 Learn More

#### Links & Information

Secure Web Gateway Services Product Info:

https://f5.com/products/big-ip/secure-web-gateway-services-swgs

SWG Reference Architecture:

https://f5.com/solutions/enterprise/reference-architectures/secure-web-gateway

# Class 4: SAML Identity Provider (IdP) Lab

This lab covers the following topics:

- Configuring a SAML Identity Provider (IdP)
- · Configuring Group-based Access Control

Expected time to complete: 2 hours

To continue please review the information about the Lab Environment. Additionally, if you are new to the F5 BIG-IP Platform we've created an overview in the BIG-IP Basics section.

## 4.1 Lab Topology & Environments

All pre-built environments implement the Lab Topology shown below. Please review the topology first, then find the section matching the lab environment you are using for connection instructions.

#### **Using Your Lab Environment**

You will be using Ravello for this lab. We will be working with a Linux jumpbox, a BIG-IP Virtual Edition version 13.1, and a simulated SaaS application. We will be using the Linux desktop as our desktop for accessing the applications on the BIG-IP.

This diagram shows the topology of the network as it is currently configured:

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	Management IP	VLAN/IP Address(es)	Credentials
Linux	10.1.1.10	External: 10.1.10.10	f5student/f5DEMOs4u
Jumphost			
BIG-IP VE	10.1.1.245	External: 10.1.10.245	admin/admin
v13.1		Internal: 10.1.20.245	root/default
SaaS Appli-	10.1.1.55	Internal: 10.1.20.55	
cation			

#### How to Access the Labs

You will receive instructions from your proctor on how to access the workstation in the lab. On this workstation, you will have the following applications:

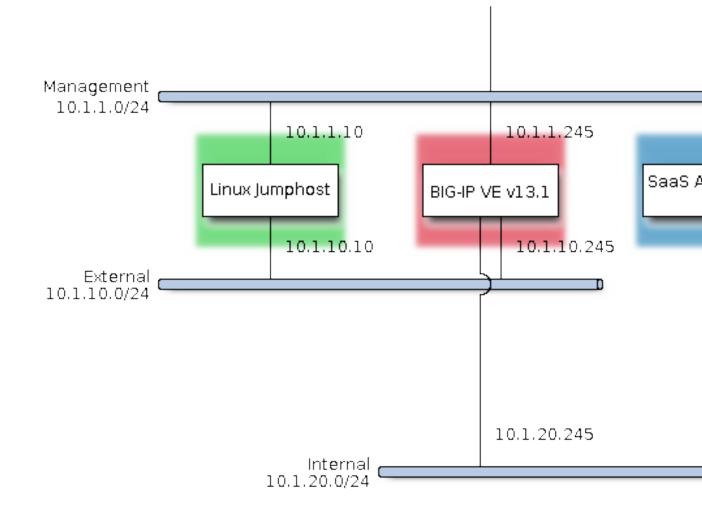


Fig. 4.1: Lab Topology

- Firefox Web Browser For testing the applications we create and BIG-IP management access. Links are bookmarked just below the address bar.
- Putty SSH Client For accessing the BASH and TMSH command line of the BIG-IP. The BIG-IP properties have been saved to the session labeled *BIG-IP*.

# 4.2 BIG-IP Basics (optional)

Just in case you're new to the F5 BIG-IP platform (or need a refresher) we've included some links and videos below that will help get you started.

## 4.2.1 What is BIG-IP

Source: https://devcentral.f5.com/articles/lightboard-lessons-what-is-big-ip-26793

## 4.2.2 BIG-IP Basic Nomenclature

Source: https://devcentral.f5.com/articles/lightboard-lessons-big-ip-basic-nomenclature-26144

### 4.2.3 F5 DevCentral BIG-IP Basics Articles

BIG-IP Basics Articles: https://devcentral.f5.com/articles?tag=devcentral+basics

#### 4.2.4 Using F5 in Various Environments

- Public Cloud:
  - AWS/Azure/GCP/etc.: http://clouddocs.f5.com/cloud/public/v1/
- Private Cloud:
  - OpenStack: http://clouddocs.f5.com/cloud/openstack/
  - VMware: https://f5.com/solutions/technology-alliances/vmware
- Container Ecosystems:
  - Cloud Foundry: http://clouddocs.f5.com/containers/latest/cloudfoundry/
  - Kubernetes: http://clouddocs.f5.com/containers/latest/kubernetes
  - Mesos Marathon: http://clouddocs.f5.com/containers/latest/marathon
  - RedHat OpenShift: http://clouddocs.f5.com/containers/latest/openshift/

#### 4.2.5 HA Proxy to BIG-IP Quick Start

If you're already familiar with HA Proxy, learning F5 BIG-IP is straightforward once you learn the associated F5 terminology.

Here is a list of common HA Proxy configuration terminology and its F5 equivalent:

HA Proxy	F5 BIG-IP
Frontend	Virtual Server (VIP)
Backend	Pool
Server	Member
mode http	HTTP Profile
default_backend	Default pool
use_backend	LTM policy
check port	Health monitor

## 4.2.6 NGINX to BIG-IP Quick Start

If you are already familiar with NGINX, learning F5 BIG-IP will be straightforward once you learn the F5 terminology.

NGINX administrators usually use multiple files and leverage the include command in their config to break down the config and make it easier to manage. F5 leverages *Profiles* which can be applied to a *Virtual Server*.

NGINX uses in-band (passive) health monitors which can be enabled on F5 through the creation of an *inband monitor*. BIG-IP also supports the use of active health monitors, which will poll the pool member periodically. Both can be used together for better monitoring of your services.

F5 BIG-IP supports control-plane and data-plane programmability with:

- Node.js through the use of iRulesLX, iControlLX and iAppsLX
- TCL through the use of iRules and iApp Templates

A lot of the manual configuration and scripting steps that are required with NGINX are supported more easily through various config parameters and profiles in BIG-IP. By leveraging the control-plane programmability features this class covers you can achieve full automation of your services with the BIG-IP platform.

F5 BIG-IP is designed to be a full proxy by default. In most cases there is no need to tune TCP & HTTP buffering like you would on NGINX (i.e. using proxy_buffering). This is because the default settings have been optimized and can adapt to most situations.

Here is a list of common NGINX configuration terminology and its F5 equivalent:

NGINX	F5 BIG-IP
listen	Virtual Server Port (VIP)
upstream	Pool
proxy_pass	Default Pool
server	Member
ssl_certificate	SSL Profile Option
return	LTM HTTP Policy Option
proxy_set_header X Forwarded For	HTTP Profile Option Insert X-Forwarded-For
proxy_set_header	LTM HTTP Policy Option
add_header	LTM HTTP Policy Option
location & proxy_pass	LTM HTTP Policy Option
Proxy Cache	Web Acceleration Policy

## 4.3 Module 1: SAML Identity Provider

In this lab we will learn the basics concepts required to use F5 Access Policy Manager as a SAML Identity Provider (IdP).

## 4.3.1 Lab 1.1: Create a SAML Identity Provider



#### Task 1 - Create a Local IdP Service

In this lab we will create the local Identity Provider service. This service is responsible for handling the authentication for the SaaS application.

**Note:** This guide may require you to Copy/Paste information from the guide to your jumphost. To make this easier you can open a copy of the guide by using the **Lab Guide** bookmark in Chrome.

- 1. Navigate to Access  $\rightarrow$  Federation  $\rightarrow$  SAML Identity Provider  $\rightarrow$  Local IdP Services
- 2. Click the + sign

Overview	F.		
Profiles / Policies	Þ		
Authentication	Þ		
Single Sign-On	Þ		
Federation	•	SAML Service Provider +	
Connectivity / VPN	÷	SAML Identity Provider >	Local IdP Services 📀
Secure Web Gateway	÷	SAML Resources 💮	External SP
			Connectors
Access Control Lists	+	JSON Web Token 🛛 🕨	Artifact Resolution

3. Configure the General Settings:

Property	Value
IdP Service Name	idp.f5demo.com
IdP Entity Id	https://idp.f5demo.com

Create New IdP Servi	ice X
General Settings SAML Profiles C Endpoint Settings Assertion Settings SAML Attributes Security Settings	IdP Service Name*:         idp.f5demo.com         IdP Entity ID*:         https://idp.f5demo.com         Name Qualifier :         IdP Hostname Settings         Scheme :       Host :         https       ✓         Description :          Log Setting :       From Access Profile         From Access Profile       ✓
	OK Cancel

4. Configure the Assertiion Settings:

Property	Value
Assertion Subject Value	%{session.logon.last.username}

Create New IdP Serv	ice	×
General Settings SAML Profiles Endpoint Settings SAssertion Settings SAML Attributes Security Settings	Assertion Subject Type : Email Address Assertion Subject Value*: %(session.logon.last.username) Authentication Context Class Reference : um:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport Assertion Validity (in seconds) : 600 Enable encryption of Subject Encryption Strength : AES128	×
	OK Car	ncel

5. Configure the *Security Settings*:

Property	Value
Signing Key	idp.f5demo.com.key
Signing Certificate	idp.f5demo.com.crt

Create New IdP Servi	ice	×
<ul> <li>General Settings</li> <li>SAML Profiles</li> <li>Endpoint Settings</li> <li>Assertion Settings</li> <li>SAML Attributes</li> <li>Security Settings</li> </ul>	Signing Key : /Common/idp.f5demo.com.key Signing Certificate : /Common/idp.f5demo.com.crt	
	ΟΚ	Cancel

6. Click the OK button.

## 4.3.2 Lab 1.2: Create an External SP Connector



Now that we have the Identity Provider configured, we need to configure the BIG-IP so it is aware of the Service Provider (the SaaS application). We do this by defining an External SP Connector using the metadata provided by the SaaS application, importing it into the BIG-IP, and setting the appropriate cryptographic controls.

#### Task 1 - Obtain the SAML Service Provider Metadata

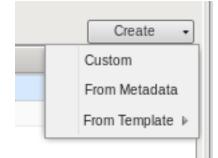
In a common deployment the metadata is provided by the application. This lab is no different, but the access method will vary. Follow the listed steps below to obtain the necessary XML file.

- 1. Open a browser and nagivate to https://app.f5demo.com/metadata.xml
- 2. Save the file as app.f5demo.com.xml

#### Task 2 - Create an External SP Connector

In this task we will create the External SP Connector object.

- 1. Navigate to Access  $\rightarrow$  Federation  $\rightarrow$  SAML Identity Provider  $\rightarrow$  External SP Connector
- 2. Click on the triangle on the right side of the Create button and select From Metadata



3. Enter the following information:

Property	Value
Select File	app.f5demo.com.xml
Service Provider Name	app.f5demo.com

Create New SAML Service Provider	×
Select File*:	
app.f5demo.com_metadataxml	Browse
Service Provider Name*: app.f5demo.com Select Signing Certificate : Select a value	~
OK	Cancel

4. Click the OK button

#### Task 3 - Modify the SP Connector Settings

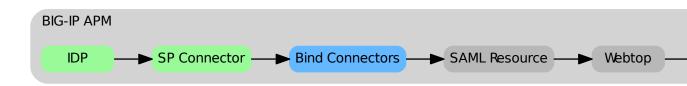
Finally, for security purposes, we'll configure the External SP Connector object to require that resposes are cryptographically signed. This prevents an attacker from manipulating the response and potentially gaining unauthorized access.

- 1. Click the checkbox next to app.f5demo.com and click the Edit button
- 2. Modify the following Security Settings:

	Property	Value		
	Response must be signed	checked		
Edit SAML SP Connel	Response must be signed       checked         ML SP Connector       al Settings         al Settings       Image: Require Signed Authentication Request         signing Certificate :       Signing Certificate :		metadata_sig_cert.( ~	×
	Encryption Type : AES128 Encryption Certificate : /Common/app.f5demo.co	m		_
			OK Cancel	

3. Click the OK button.

## 4.3.3 Lab 1.3: Bind SP Connectors



Once we have the Identity Provider and Service Provider objects configured, we need to link them together.

#### Task 1 - Bind the IdP and SP Connector

1. Navigate to Access  $\rightarrow$  Federation  $\rightarrow$  SAML Identity Provider  $\rightarrow$  Local IdP Services

<u> </u>	Access			
	Overview	Ŀ.		
	Profiles / Policies	÷.		
	Authentication	÷		
	Single Sign-On	Ŀ.		
	Federation	•	SAML Service Provider +	
	Connectivity / VPN	×.	SAML Identity Provider >	Local IdP Services 🧿
	Secure Web Gateway	÷	SAML Resources 💮	External SP
	Access Control Lists	÷.	JSON Web Token	Corricciois
	Webtops	÷	OAuth Authorization	Artifact Resolution

- 2. Check the radio button next to *idp.f5.demo.com*
- 3. Click on the Bind/Unbind SP Connectors button
- 4. Check the box next to /Common/app.f5demo.com

Edit SAML SPs that use this IdP	×
SP Connectors associated with this IdP Service	
	Create SP Connector 👻
SAML SP Connection Name 🔺	
/Common/app.f5demo.com	
Common/saml_office365	
	OK Cancel

5. Click the OK button.

## 4.3.4 Lab 1.4: Create SAML Resource



#### Task 1 - Create SAML Resource

1. Navigate to  $\textit{Access} \rightarrow \textit{Federation} \rightarrow \textit{SAML Resource}$  and click the + sign

•	Access		
	Overview	÷	
	Profiles / Policies	÷.	
	Authentication	÷	
	Single Sign-On	÷.	
	Federation	•	SAML Service Provider +
	Connectivity / VPN	÷	SAML Identity Provider >
	Secure Web Gateway	÷.	SAML Resources 💿
	Assess Control Lints		

2. Configure the following settings:

Property	Value
Name	app.f5demo.com
SSO Configuration	idp.f5demo.com
Caption	арр

Access » Federation : SAML Resources » New SAML Resource						
General Properties						
Name	app.f5demo.com					
Description						
Publish on Webtop	Publish on Webtop Senable					
Configuration						
SSO Configuration idp.f5demo.com						
Customization Settings for Eng	lish					
Language	English					
Caption	app					
Detailed Description	Detailed Description					
Image	Browse No file selected.	View/Hide				
Cancel Repeat Finished						

3. Click the *Finished* button.

## 4.3.5 Lab 1.5: Create a Webtop



## Task 1 - Create the SAML Webtop

- 1. Navigate to Access  $\rightarrow$  Webtops  $\rightarrow$  Webtop Lists
- 2. Click the + sign

Overview Profiles / Policies Authentication		
	÷	
Authentication	÷	
	÷	
Single Sign-On	ŀ	
Federation	ŀ	
Connectivity / VPN	÷	
Secure Web Gateway	Þ	
Access Control Lists		
Webtops	÷	

3. Configure the following settings:

Property	Value
Name	saml_webtop
Туре	full

Access » Webtops : Webtop Lists » New Webtop								
General Properties								
Name	saml_webtop							
Туре	Full							
Configuration	N							
Minimize To Tray	Enabled K							
Show a warning message when the webtop window close	Enabled							
Show URL Entry Field	Enabled							
Show Resource Search	Enabled							
Fallback Section								
Initial State	Expanded -							
Cancel Repeat Finished								

3. Click the *Finished* button.

## 4.3.6 Lab 1.6: Configure the Access Profile



The Access Profile defines the characteristics of how we authenticate and authorize a user using the BIG-IP platform. It controls things like what type logon page is presented to the user (if any at all), what language any dialog messages should be presented in, and – most importantly – the flow through which we limit access and assign resources.

F5 BIG-IP Access Policy Manager supports two types of Access Policies:

- 1. Per-Session access policies
- 2. Per-Request access policies

The difference centers around how frequently a policy is evaluated, either once at time of initial logon or after every single HTTP request.

### Task 1 - Create the Access Profile Object

- 1. Navigate to  $Access \rightarrow Profiles/Policies \rightarrow Access Profiles (Per-Session Policies)$
- 2. Click the + sign

Access			
Overview	ŀ		
Profiles / Policies	•	Access Profiles	0
Authentication	÷	(Per-Session Policies)	J.
Single Sign-On	÷	Per-Request	(+)

3. Configure the following settings:

Property	Value
Name	idp.f5demo.com-policy
Profile Type	All
Languages	English (en)

Access » Profiles / Policies	s : Access Profiles (Per-Session Policies) » New Profile						
General Properties							
Name	app.f5demo.com-policy						
Parent Profile	access						
Profile Type	A						
Profile Scope	Profile -						
Settinas							

Language Settings		
Additional Languages	Afar (aa)	
Languages	Accepted Languages	Factory BuiltIn Languages Japanese (ja) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-tw) Korean (ko) Spanish (es) French (fr) German (de)
Default Language	English (en) -	
Cancel Finished		

4. Click the *Finished* button.

### Task 2 - Configure the Access Policy Using the Visual Policy Editor

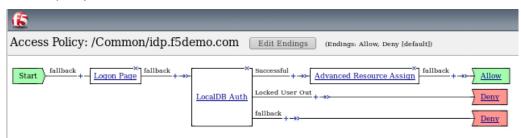
The Visual Policy Editor (VPE) is where the administrator configures the heart of the Access Policy. Using a flow chart methodology, it is easy to create robust policies without adding burdensome management overhead. Even significant policies can be easily read and understood.

### 1. Open the Visual Policy Editor

- (a) Navigate to  $Access \rightarrow Profiles/Policies \rightarrow Access Profiles (Per-Session Policies)$
- (b) Click the *Edit...* link and the VPE will open in a new window

₩ -	Access I	Profiles Per-Request Policies		zation 👻							
			Search							Create	. Import
~	✓ Status	▲ Access Profile Name		Application	+ Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	+ Partition / Pa
	jø –	access			All	(none)	(none)	(none)			Common
		idp.f5demo.com			A	Edit	_	-	default-log-setting		-

We'll build a policy like the one below:



### 2. Add a Logon Page

- (a) Click on the + link after the Start node
- (b) Select the Logon Page tab and click the Add Item button
- (c) Use the default settings and click the Save button

### 3. Add an Authentication Mechanism

- (a) Click on the + link after the Logon Page node
- (b) Select the Authentication tab and select LocalDB Auth then click the Add Item button

(c) Configure the following settings:

Property LocalDB Instance	Value /Common/agility						
Properties Branch Rules							
Name: LocalDB Auth							
/Common/a	gility -						
lowed 3 -							
	LocalDB Instance						

**Note:** The administrator can select from a variety of Authentication Mechanisms, including Active Directory and LDAP, among others. In this lab, the *LocalDB Auth* has been pre-configured.

(a) Click the *Save* button.

#### 4. Add Advanced Resource Assign

- (a) Click on the + link on the successful branch after the LocalDB Auth node
- (b) Select the *Assignment* tab and select *Advanced Resource Assign* then click the *Add Item* button
- (c) Click the Add New Entry button
- (d) Click the Add/Delete link
- (e) Select the Webtop tab and select the /Common/saml_webtop
- (f) Select the SAML tab and select the /Common/app.f5demo.com
- (g) Click the Update button, then click the Save button

(Proportion)	Branch Rules
Properties	branch Rules

Name: Advanced Resource Assign					
Resource Assignment					
Add new entry					

Expression: Empty change

- SAML: /Common/app.f5demo.com
- Webtop: /Common/SAML_webtop Add/Delete

N

1

### 5. Change the ending to Allow

- (a) Click on the Deny ending after the Advanced Resource Assign
- (b) Select Allow
- (c) Click Save

### 6. Apply Policy Changes

- (a) Click the Apply Access Policy in top left next to the F5 red ball
- (b) Close browser tab

## 4.3.7 Lab 1.7: Create the Virtual Server



In order to access almost anything through an F5 BIG-IP, you must define a Virtual Server. The Virtual Server listens on the specified address and handles the requests either by making a load balancing decision or prompting for a logon (or both!).

#### Task 1 - Create the Virtual Server

- 1. Navigate to Local Traffic  $\rightarrow$  Virtual Server List
- 2. Click the + sign

Local Traffic		
Network Map		
Virtual Servers	ŀ	Virtual Server List
Policies	·	Virtual Address List
Profiles		Statistics >

2. Configure the General Properties settings:

General Properties	
Property	Value
Name	idp.f5demo.com
Destination Address/Mask	10.1.10.101
Service Port	443

General Properties	
Name	idp.f5demo.com
Description	
Туре	Standard
Source Address	
Destination Address/Mask	10.1.10.101
Service Port	443 Select •
Notify Status to Virtual Address	
State	Enabled 🗾 😼

3. Configure the *Configuration* settings:

Configuration	
Property	Value
HTTP Profile	http
SSL Profile (Client)	idp.f5demo.com-clientssl
SSL Profile (Server)	serverssl

Configuration: Basic •	
Protocol	TCP
Protocol Profile (Client)	tcp 🔹
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http -
HTTP Proxy Connect Profile	None
FTP Profile	None 💌
RTSP Profile	None
	Coloriari
SSL Profile (Client)	Selected /Common idp.f5demo.com-clientssl >>
SSL Profile (Client) SSL Profile (Server)	/Common idp.f5demo.com-clientssl

4. Configure the *Access Policy* settings:

Access Policy	
Property	Value
Access Profile	idp.f5demo.com

Access Policy	
Access Profile	idp.f5demo.com 💌
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 -

5. Click the *Finished* button.

# 4.3.8 Lab 1.8: Test the SAML Configuration



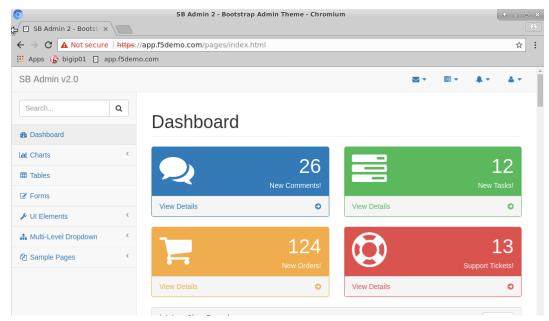
Now that we have all the pieces configured, the only thing left is to test and validate our setup to make sure it's working as expected.

### Task 1 - Test SAML IdP

- 1. Open Chromium and navigate to https://app.f5demo.com
- 2. Notice how we've been redirected to the authentication page at https://...
- 3. Login with the test credentials below:

Username	Password
alice	agility

4. You should now see a demo application. If not, please step back through the configuration and make sure you did not mistype one of the settings



5. Close the Chromium browser

# 4.4 Module 2: Access Control

In this lab we will limit access to SaaS resources based on group membership.

## 4.4.1 Lab 2.1: Modify the Access Profile

#### Task 1 - Launching the Visual Policy Editor

- 1. Navigate to  $Access \rightarrow Profiles/Policies \rightarrow Access Profiles (Per-Session Policies)$
- 2. Click the Edit... link

<del>*</del> -	Access I	Profiles Per-Request Policies	Policy Sync	Customi	zation 👻							
Search     Search												
<b>v</b>	✓ Status	▲ Access Profile Name			+ Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	+ Partition / Pat
						All	(none)	(none)	(none)			Common
		access				A		(10110)	(			Common

### Task 2 - Add a LocalDB Query

- 1. Click on the + sign after LocalDB Auth on the Successful branch
- 2. In the search field type local
- 3. Select Local Database and click the Add Item button

4. Configure the following settings:

Property	Value
LocalDB Instance	/Common/Agility

- 5. Click the Add new entry button
- 6. Configure the following settings:

Property	Value
Action	read
Destination	session.localdb.groups
Source	groups

7. Click the Save button

### Task 3 - Modify the Advance Resource Assignment

- 1. Click on Advance Resource Assign
- 2. Click on the *change* link

F	Properties Branch Rules
N	ame: Advanced Resource Assign
R	Resource Assignment
	Add new entry
	Expression: Empty change
1	SAML: /Common/app.f5demo.com
1	Webtop: /Common/saml webtop
	Add/Delete
1	SAML: /Common/app.15demo.com

- 3. Click the Add Expression button
- 4. Configure the following settings:

Property	Value
Agent Sel	LocalDB Group Check
Condition	LocalDB Query
User is a member of	Sales

5. Click the Add Expression button

Simple
Agent Sel: Local DB Group Check
Condition: LocalDB Query
User is a member of sales
Cancel Add Expression
Cancel Help

- 6. Click the Finished button
- 7. Click the Save button
- 8. Click the Apply Access Policy link in top left next to the F5 red ball

## 4.4.2 Lab 2.2: Test Access Control

Now that you have your IdP configured we need to test it to make sure it is working as expected.

### Task 1 - Test with an Authorized User

- 1. Open Chromium and navigate to https://app.f5demo.com
- 2. Login with the test credentials

Username	Password
alice	agility

3. You should now see a demo application.

♥ SB Admin 2 - Bootst →		SB Admin 2 - Bootstrap	Admin Theme - Chromiu	ım				+ = = ×
		/app.f5demo.com/pages/index.h	tml					☆ :
🔛 Apps 🚯 bigip01 🔲 a	app.f5dem	p.com						
SB Admin v2.0					₩ •	≣.+	<b>*</b> •	4.4
Search	۹	Dashboard						
Dashboard		Dashboard						
Lill Charts	<		26				1	2
I Tables			∠O New Comments!				L New Ta	
G Forms		View Details	o New Comments:	View Details			NCW IC	•
🗲 UI Elements	<	View Details	•	View Details				
🛔 Multi-Level Dropdown	<		124				1	13
쉽 Sample Pages	<		New Orders!				L Support Tic	
		View Details	O	View Details				Ð
		· · · · · · · · ·						

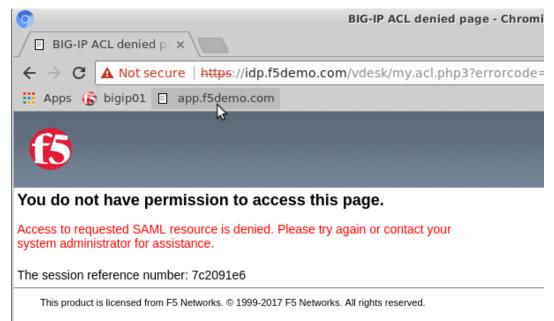
4. Click the user icon in the top right of the app and logout

### Task 2 - Test with an Unauthorized User

- 1. Navigate to https://app.f5demo.com (you can click the bookmark)
- 2. Login with the test credentials

Username	Password
john	agility

3. You should now see an error page since John is not a member of the sales group



8. Close the Chromium browser

# Class 5: AD FS Proxy Lab

This lab covers the following topics:

· Configuring AD FS Proxy Services on F5 BIG-IP

Expected time to complete: 2 hours

To continue please review the information about the Lab Environment.

# 5.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

**Note:** All work for this lab can be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

## 5.1.1 Lab Topology

The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE (v13.1)
- 5 x Windows Server 2016

### Lab Components

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials	Notes
BIGIP	<ul> <li>Management: 10.1.1.4</li> <li>Internal: 10.1.20.4</li> <li>External: 10.1.10.4</li> <li>ADFS Proxy Virtual Server IP: 10.1.10.100</li> <li>ADFS Load Balancing Virtual Server IP: 10.1.20.100</li> </ul>	• admin/ad • root/de:	Licensed with Best bundle, provisioned with LTM and APM. BIG-IP Version 13.1. fault
Client	• Internal 10.1.20.8	user/user	This is the client/jumphost used in the lab, it is domain joined. Windows Server 2016.
DC	• Internal 10.1.20.5	admin/admin	This is the domain controller and certificate authority. Win- dows Server 2016.
Арр	• Internal 10.1.20.10	admin/admin	Runs IIS with a claims app that is federated to ADFS. Windows Server 2016.
ADFS-1	• Internal 10.1.20.6	admin/admin	Primary ADFS farm node. Windows Server 2016.
ADFS-2	• Internal 10.1.20.7	admin/admin	Secondary ADFS farm node. Windows Server 2016.

# 5.2 Module: Connect and Validate Environment

In this module you will validate that ADFS and the application that requests ADFS authentication are functioning without the BIG-IP in the traffic flow.

# 5.2.1 Open an RDP session to the client machine

- 1. Open an RDP session to the client jumphost
- 2. Login with username: user and password: user

# 5.2.2 Change Client to Point at ADFS-1 Direct (BIG-IP not in traffic flow)

1. Double click the "ADFS-1 Direct" desktop shortcut



2. You should receive a notification that the HOSTS file now points adfs.vlab.f5demo.com directly at the ADFS-1 server.

Message from user 5/25/2018 5:42 PM	×
HOSTS file now points adfs.vlab.f5demo.com directly at ADI the traffic flow.	FS-1, BIG-IP is out of
	ОК

# 5.2.3 Open the BIG-IP Management Interface

- 1. Open Chrome
- 2. Click the BIG-IP shortcut



- 3. Login with username: admin and password: admin
- 4. Nothing needs to be done here now, you are only validating you can access the BIG-IP.

## 5.2.4 Verify ADFS and App are Functional

- 1. Close any open Chrome incognito windows
- 2. Open Chrome if not already open
- 3. Right click the "ADFS Demo App" shortcut and click "open in incognito window"

VERY IMPORTANT: For all testing in this lab, close all incognito windows first, then open a new one for your test. This will ensure you do not have issues related to cache or cookies.

ClaimsXRay 🗋	ADFS Demo App		
-		Open in new tab	
		Open in new window	
		Open in incognito window	
right click		Edit	
		Cut	
		Сору	

- 4. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com
- If the request failed and you do not see claims then the ADFS-1 Windows server may not have started correctly or Option 1: You can restart services on the ADFS servers from your client with the shortcut on the desktop. This is the fastest option.



Option 2: You can restart the ADFS-1 and then ADFS-2 servers. This is much slower.

You should now see the following:

# Welcome!

#### These are your claims:

Туре		
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	true	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user(a	f5dem
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.2	20.8
http://schemas.microsoft.com/claims/authnmethodsproviders	Wind	owsAu
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://	schem

- 5. Note that ADFS identified the user as inside the corporate network because they did not go through an MS-ADFSPIP compliant proxy.
- 6. What happened:
  - (a) You made a request to App
  - (b) App redirected you to ADFS for authentication
  - (c) ADFS authenticated you automatically with Windows Integrated Authentication with your domain joined computer
  - (d) ADFS redirected you back to App with a WS-Fed assertion
  - (e) App validated the assertion and displayed the claims it received from ADFS

You should close all browser windows in the client and repeat these steps to validate ADFS-2 using the desktop shortcut labeled "ADFS-2 Direct". If it fails, use the desktop shortcut to restart ADFS services as noted above.

# 5.3 Module: Deploy ADFS Load Balancing Services

In this module you will deploy simple load balancing of ADFS for internal users. No proxy services are needed for internal users.

## 5.3.1 Change Client to Point at BIG-IP Load Balancing Virtual Server

1. Double click the BIG-IP ADFS Load Balancer desktop shortcut



2. You should see that the HOSTS file now points ADFS at the load balancing virtual server (which is not yet created)

Message from user 5/25/2018 5:47 PM

HOSTS file now points adfs.vlab.f5demo.com at the ADFS load balancing Virtual Server, like an internal client.

- 3. Close any open Chrome incognito windows
- 4. Open a new Chrome window if not already open.
- 5. Right click the "ADFS Demo App shortcut" and open a new incognito window
  - (a) It should fail because you cannot access ADFS through the BIG-IP until you deploy the configuration.

OK

(b) If it is still working, you may need to close Chrome and/or retry the HOSTS file shortcut.

### 5.3.2 Deploy ADFS iApp for ADFS Load Balancing

- 1. Open the BIG-IP configuration interface
- 2. Open Local Traffic -> Virtual Servers and notice nothing is deployed
- 3. Open iApps -> Application Services -> Applications
- 4. Click Create

Accept all default values except for those listed below.

- 5. Name: adfs-lb
- 6. Template: f5.microsoft_adfs.v1.2.0rc7
- 7. SSL Encryption
  - (a) How should the BIG-IP system handle SSL traffic?

#### i. Encrypted traffic is forwarded without decryption (SSL pass-through)

SSL Pass-Through is chosen because Microsoft requires it for supported load balancing of ADFS. SSL Bridging breaks the connectivity between WAP servers and ADFS servers because client certificate authentication is required. You can use SSL Bridging if you will not point WAP servers at your deployment but following Microsoft's guidelines and using SSL Pass-Through is recommended.

### 8. High Availability

#### (a) What IP address do you want to use for the virtual server?

#### i. 10.1.20.100

10.1.20.x is the internal network in this environment.

### 1. Which FQDN will clients use to access AD FS?

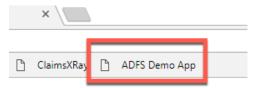
- (a) adfs.vlab.f5demo.com
- 2. Which servers should be included in this pool?
  - (a) 10.1.20.6
  - (b) Click Add
  - (c) 10.1.20.7

High Availability				
What IP address do you want to use for the virtual server?	10.1.20.100			
What service port do you want to use for the virtual server?	443			
Which FQDN will clients use to access AD FS?	adfs.vlab.f5demo.com			
Do you want to create a new pool or use an existing one?	Create a new pool		\$	
Which servers should be included in this pool?		Port 4 Port 4		Connection limit Connection limit
Do you want to configure support for client certificate authentication?	Yes, configure support for certificate authentication		¢	

9. Click Finished

# 5.3.3 Test the ADFS Load Balancing Functionality

- 1. Close any open Chrome incognito windows
- 2. Open a new Chrome window if not already open
- 3. Right click the "ADFS Demo App" shortcut and open in an incognito window



4. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

# Welcome!

#### These are your claims:

Туре		
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	true	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@	f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.2	0.4
http://schemas.microsoft.com/claims/authnmethodsproviders	Windo	wsAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	l http://s	chemas.microsoft.com/v
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-0	)5-25T20:03:21.959Z

Server time: 5/25/2018 8:03:22 PM

- 1. Note that ADFS is still identifying the user as inside the corporate network because the user did not go through an MS-ADFSPIP compliant proxy solution.
- 2. What happened:
  - (a) You made a request to App
  - (b) App redirected you to ADFS for authentication
  - (c) The BIG-IP received the request and load balanced it to one of the ADFS servers (this is the only change from last time)

- (d) ADFS authenticated you automatically with Windows Integrated Authentication with your domain joined computer
- (e) ADFS redirected you back to App with a WS-Fed assertion
- (f) App validated the assertion and displayed the claims it received from ADFS

## 5.3.4 Review the ADFS Load Balancing Configuration

- 1. Go to Local Traffic -> Virtual Servers
- 2. Notice there are two deployed, one on port 443 and one on port 49443
  - (a) 443 is for ADFS traffic
    - i. Pool members use port 443
  - (b) 49443 is for client certificate auth support
    - i. Pool members use port 49443

# 5.4 Module: Deploy ADFS Proxy Services

In this module you will deploy ADFS Proxy functionality. The BIG-IP will perform the same role in front of ADFS as a Web Application Proxy (WAP) server does, supporting the protocol MS-ADFSPIP.

## 5.4.1 Change Client to Point at BIG-IP ADFS Proxy Virtual Server

1. Double click the BIG-IP ADFS Load Balancer desktop shortcut



2. You should see that the HOSTS file now points ADFS at the load balancing virtual server (which is not yet created)

Message from user 5/25/2018 8:21 PM	×

HOSTS file now points adfs.vlab.f5demo.com at the ADFS Proxy Virtual Server, like	
an external client.	

- 3. Close any open Chrome incognito windows
- 4. Open a new Chrome window if not already open
- 5. Right click the "ADFS Demo App" shortcut and open a new incognito window
  - (a) It should fail because you cannot access ADFS through the BIG-IP until you deploy the configuration.

ок

(b) If it is still working, you may need to close Chrome and/or retry the HOSTS file shortcut.

# 5.4.2 Deploy ADFS iApp for ADFS Proxy (with MS-ADFSPIP support)

- 1. Open the BIG-IP configuration interface
- 2. Open iApps -> Application Services -> Applications
- 3. Click Create

Accept all default values except for those listed below.

- 4. Name: adfs-proxy
- 5. Template: f5.microsoft_adfs.v1.2.0rc7
- 6. Access Policy Manager (BIG-IP APM)
  - (a) Would you like to configure BIG-IP as an ADFS Proxy?
    - i. Yes, configure BIG-IP as an ADFS Proxy
  - (b) What is the account to be used for establishing proxy trust with ADFS?
    - i. admin@f5demo.com
  - (c) What is the password associated with that account?
    - i. admin

Establishing trust with ADFS requires username in UPN or domain\username format. This is true whether in the iApp or establishing trust manually.

- 7. SSL Encryption
  - (a) Which SSL certificate do you want to use?
    - i. internal-vlab.f5demo.com.crt
  - (b) Which SSL private key do you want to use?
    - i. internal-vlab.f5demo.com.key

Note that this time we are doing SSL Bridging. This is required for the ADFS Proxy. Client certificate authentication can still be performed because BIG-IP supports MS-ADFSPIP.

### 8. High Availability

- (a) What IP address do you want to use for the virtual server?
  - i. 10.1.10.100

10.1.10.x is the external/DMZ network in this environment. Notice this is .10 not .20 this time.

### 1. Which FQDN will clients use to access AD FS?

- (a) adfs.vlab.f5demo.com
- 2. Which servers should be included in this pool?
  - (a) 10.1.20.6
  - (b) Click Add
  - (c) 10.1.20.7
- 3. What Trusted CA would you like to use to validate the client certificate chain presented during certificate authentication?

#### (a) F5demo-DC-CA.crt

This is the AD Certificates Services CA certificate for this environment that was used to issue the client certificates so that the client certificate auth can be verified. It was pre-imported for you.

9. Click Finished

## 5.4.3 Test the ADFS Proxy Forms Authentication Functionality

- 1. Close any open Chrome incognito windows
- 2. Open a new Chrome window if not already open
- 3. Right click the "ADFS Demo App" shortcut and open a new incognito window

	× /	)		
ß	ClaimsXRay	ß	ADFS Demo App	
		_		-

If you do not get the ADFS logon page noted below wait 60-120 seconds for the ADFS servers to sync and try again. If you are still getting the error you may have cache problems. Double check that you have closed all other incognito windows before trying this, and you can clear cache and cookies by performing ctrl+shift+del and selecting "all time".

- 1. This time instead of automatically authenticating with Windows Integrated Authentication you are presented with a forms login page. This is because ADFS is configured to require Forms auth for external users.
  - (a) Username: user@f5demo.com
  - (b) Password: user
  - (c) Click Sign In

Sign in with your organizational account

@f5demo.com		
gn in		

Sign ii	n using	an	X.509	certificate
---------	---------	----	-------	-------------

1. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

# Welcome!

#### These are your claims:

Туре	Value
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy	APM
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	false
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10 1 20 4
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-i	10.1.1.8
http://schemas.microsoft.com/claims/authnmethodsproviders	FormsAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-05-25T21:15:05.387Z

Server time: 5/25/2018 9:15:05 PM

- 1. Note that ADFS now identifies the user as outside the corporate network, knows that APM acted as an ADFS Proxy, knows the user's true IP address, and that the user is now logging in with Form-sAuthentication instead of WindowsAuthentication.
- 2. What happened:
  - (a) You made a request to App
  - (b) App redirected you to ADFS for authentication
  - (c) The BIG-IP received the request and load balanced it to one of the ADFS servers, as well as communicated data about the traffic using MS-ADFSPIP.
  - (d) The ADFS server determined that you should be authenticated using the extranet policy and sent back a logon page which the BIG-IP forwarded on to you.
  - (e) You submitted the forms and ADFS authenticated with your credentials
  - (f) ADFS redirected you back to App with a WS-Fed assertion
  - (g) App validated the assertion and displayed the claims it received from ADFS

## 5.4.4 Test the ADFS Proxy Certificate Authentication Functionality

- 1. Close any open Chrome incognito windows
- 2. Open a new Chrome window if not already open
- 3. Right click the "ADFS Demo App" shortcut and open a new incognito window

× \				
🗋 ClaimsXRay	ß	ADFS Demo App		

1. Click Sign in using an X.509 certificate

Sign in with your organizational account

user@f5demo.com	
••••	
Sign in	
	1
Sign in using an X.509 certificate	

- 1. Note that you can configure ADFS extranet authentication settings to perform certificate authentication automatically. The ADFS server in this lab is setup to allow both forms and certificate authentication.
- 1. The certificate is already selected, click OK.

Select a certificate		×
Select a certificate to aut	henticate yourself to adfs.vlab.f5demo	o.com:49443
Users	f5demo-DC-CA	4A000000CFA27D41
Certificate informatio	n	OK Cancel

1. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

## Welcome!

These are your claims:

Туре	Value
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy	APM
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	false
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.20.4
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-in-	10.1.1.8
http://schemas.microsoft.com/claims/authnmethodsproviders	CertificateAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/x509
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-05-25T22:14:40.914Z

Server time: 5/25/2018 10:14:41 PM

- 1. Note that ADFS now ADFS has identified the authentication type as CertificateAuthentication
- 2. What happened:
  - (a) You made a request to App
  - (b) App redirected you to ADFS for authentication
  - (c) The BIG-IP received the request and load balanced it to one of the ADFS servers, as well as communicated data about the traffic using MS-ADFSPIP.

- (d) The ADFS server determined that you should be authenticated using the extranet policy and sent back a logon page which the BIG-IP forwarded on to you.
- (e) You selected the Certificate Authentication, which caused you to be redirected to port 49443 where the BIG-IP performed certificate authentication
- (f) BIG-IP forwarded on details about your authentication using MS-ADFSPIP to the ADFS server
- (g) ADFS redirected you back to App with a WS-Fed assertion
- (h) App validated the assertion and displayed the claims it received from ADFS

## 5.4.5 Review the ADFS Proxy Configuration

- 1. Go to Local Traffic -> Virtual Servers
- 2. Notice there are two adfs-proxy virtual servers deployed, one on port 443 and one on port 49443
  - (a) 443 is for ADFS traffic
    - i. Pool members use port 443
  - (b) 49443 is for client certificate auth support
    - i. Pool members use port 443
      - A. This is different from the load balancing only, which pointed to port 49443. This is because the certificate auth is not passing through, BIG-IP is performing the certificate auth, then sending the data along to ADFS using MS-ADFSPIP.
  - (a) Click on the virtual server adfs-proxy_adfs_vs_443
    - i. Scroll down and examine the Access Policy -> ADFS Proxy configuration item
      - A. Note that ADFS Proxy functionality is enabled and a trust is established. The BIG-IP will auto-renew this prior to expiration.
      - B. Note that no Access Profile is deployed. You can add one if desired for additional security. The iApp is capable of deploying it, along with the required bypass iRule for some URLs like the metadata sharing URL.
  - (b) Go to Local Traffic -> Profiles -> SSL -> Server and click adfs-proxy_server-ssl
    - i. Note that a certificate and key are used on the server side. These are created as part of establishing the trust with the ADFS server as noted in the previous step and then automatically input here.
    - ii. This is shared by both the 443 and the 49443 virtual servers because they need the same settings to communicate with ADFS.
  - (c) Change configuration mode to advanced
    - i. Note that the server name field contains adfs.vlab.f5demo.com. ADFS requires SNI and this is how you configure it on the serverssl profile.
  - (d) Go to Local Traffic -> Profiles -> SSL -> Client and click adfs-proxy_client-ssl-cert-auth
    - i. This is the SSL profile that provides certificate auth on the port 49443 virtual server.
    - ii. Note that Client Certificate is set to required and the Trusted Certificate Authorities is set to f5demo-DC-CA.

iii. You could use Advertised Certified Authority here if you wanted the client to only display certificates generated by a specific CA. This could be your primary CA, or even a specific subordinate CA if you wanted to issue client certificate auth user certificates from a specific CA to reduce the number shown to the user.

# 5.5 Module: Additional Information and Troubleshooting Tips

It is possible to implement an APM profile in front of the ADFS server. The deployment guide covers requirements, or you can select to deploy an APM profile in the iApp and it will handle everything including the required selective APM bypass iRule and SSO into ADFS.

When logging in to the default APM logon page, you do not need to specify the domain like you do on the ADFS logon page, just typing "user" (the samAccountName) will be sufficient. You can customize the APM logon page to accept samAccountName, UPN, or domain\username if desired.

The service that handles the MS-ADFSPIP trust relationship is adfs_proxy. You can restart this service if needed with the following CLI command: bigstart restart adfs_proxy.

If you cannot establish trust, it could be because the primary ADFS server is offline. The primary ADFS server in the farm must be functioning or new WAPs/Proxies cannot establish trust.

Microsoft provides a service called ClaimsXRay at https://adfshelp.microsoft.com that is very useful for troubleshooting ADFS related issues. There is a shortcut to it on your Chrome browser. The shortcut is configured to populate the values for ClaimsXRay for this lab environment so that you do not need to enter them into the webpage manually. It will redirect to your ADFS environment, where you can authenticate, then send you to ClaimsXRay where you can examine the claims.

For more information on this solution, go here: https://devcentral.f5.com/articles/ ad-fs-proxy-replacement-on-f5-big-ip-30191

For the deployment guide, go here: https://f5.com/solutions/deployment-guides/ microsoft-active-directory-federation-services-big-ip-v11-ltm-apm

# 5.6 Conclusion

## 5.6.1 Learn More

### Links & Information

Microsoft Active Directory Federation Services Deployment Guide:

https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm

• DevCentral: ADFS Proxy Replacement on F5 BIG-IP:

https://devcentral.f5.com/articles/ad-fs-proxy-replacement-on-f5-big-ip-30191

# **Class 6: Federating Common Services**

Welcome to the Common Federation lab at F5 Agility 2018

# 6.1 Welcome

Welcome to the 330 Access Policy Manager (APM) Federation Hands-on Lab Guide. The following labs and exercises will instruct you on how to configure and troubleshoot federation use cases based on the experience of field engineers, support engineers and clients. This guide is intended to complement lecture material provided during the 330 course as well as a reference guide that can be referred to after the class as a basis for configuring federation relationships in your own environment.

## 6.1.1 Lab Network Setup

In the interest of focusing as much time as possible configuring and performing lab tasks, we have provided some resources and basic setup ahead of time. These are:

- · Cloud-based lab environment complete with Jump Host, Virtual BIG-IP and Lab Server
- Duplicate Lab environments for each student for improved collaboration
- The Virtual BIG-IP has been pre-licensed and provisioned with Access Policy Manager (APM)
- Pre-staged configurations to speed up lab time, reducing repetitive tasks to focus on key learning elements.

If you wish to replicate these labs in your environment you will need to perform these steps accordingly. Additional lab resources are provided as illustrated in the diagram below:

<b>(5</b> ).	A	GILI 330 F	ed	<b>FY</b> eration	20 with F5	1	8	-	1	En	Lab ivironn	nent
Student Lapop		Cloud-ba Lab Enviror			Jump Ho		Externa	10.:	1.1.	Internal 245/24	Lab Ser	
PARA	🗩 Ji	ump Host		ه) ا(	-IP-1 (VE)		Lal	b Server		1	/LANs	
4 4 4 4	OS	Ubuntu		TMOS	13.1.0.3	8	os	Ubuntu		TMOS	IP Subnet	87-60-7
200	External	10.1.10.51/24		External	10.1.10.245/24		External	10.1.10.252/24		External	10.1.10.0/24	a m
	Internal	10.1.20.253/24		Internal	10.1.20.245/24		Internal	10.1.20.252/24		Internal	10.1.20.0/24	
4 4 4 4	Mgmt.	10.1.1.51/24		Mgmt.	10.1.1.245/24		Mgmt.	10.1.1.252/24		Mgmt.	10.1.1.0/24	
シシシシ	22	1222		XX	222	200				88 (	E	5

## 6.1.2 Timing for labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. This can never be accurately predicted but we strived to provide an estimate based on several people, each having a different level of experience. Below is an estimate of how long it will take for each lab:

Lab Description	Time Allocated
LAB 1 - SAML Service Provider (SP)	25 minutes
LAB 2 - SaaS SAML Identity Provider (IDP) (OKTA)	25 minutes
LAB 3 - oAuth & OpenID Connect (Google)	25 minutes
LAB 4 - oAuth and Azure AD Lab	25 minutes

## 6.1.3 Authentication – Credentials

The following credentials will be utilized throughout this Lab guide. All other credentials will be indicated at the time of use.

Credential Use	User ID	Password
BIG-IP Configuration Utility (GUI)	admin	admin
BIG-IP CLI Access (SSH)	root	default
Jump Host Access	f5student	f5DEMOs4u

## 6.1.4 Utilized Browsers

The preferred browser for this lab is Firefox. Shortcut links have been provided to speed access to targeted resources and assist you in your tasks. Except where noted, either browser can be used for all lab tasks.

## 6.1.5 General Notes

As noted previously, environment staging has been done to speed up lab time, reducing repetitive tasks to focus on key learning elements. Where possible steps that have been optimized have been called out with links and references provided in the *Additional Information* section for additional clarification. The intention being that the lab guide truly serves as a resource guide for all your future federation deployments.

## 6.1.6 Acknowledgements

This lab is built upon the work of prior F5 Agility's and the work of many individuals behind the scenes in addition the 2018 Agility Lab Team. Many thanks to the 2017 Agility Lab Team for the SAML & OAuth Federation Labs, Lucas Thompson for his OAuth/OIDC Lab and our lab testers Matt Harmon, Dave Lipowsky & Stu McMath.

## 6.1.7 Presented by

APM 330 Presented by: Steve Lyons, Chris Miller & Chas Lesley

# 6.2 Lab 1: SAML Service Provider (SP) Lab

The purpose of this lab is to configure and test a SAML Service Provider (SP). Students will configure the various aspects of a SAML Service Provider, import and bind to a SAML Identity Provider (IdP) and test SP-Initiated SAML Federation.

## 6.2.1 Objective:

- Gain an understanding of SAML Service Provider(SP) configurations and its component parts
- Gain an understanding of the access flow for SP-Initiated SAML

### 6.2.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- · Estimated completion time: 25 minutes

## 6.2.3 Lab 1 Tasks:

### TASK 1: Configure the SAML Service Provider (SP)

Refer to the instructions and screen shots below:

 Login to your lab provided Virtual Edition BIG-IP
 Begin by selecting: Access -> Federation -> SAML Service Provider -> Local SP Services
 Click the Create button (far right)

the left navigation • Name: app • Entity ID:	ew SAML SP Service dialogue box click General Settings in on pane and key in the following as shown: o.f5demo.com https://app.f5demo.com w box on Host will disappear when the Entity ID is entered.
Create New SAML SP	Service X
General Settings Carbont Settings Security Settings Authentication Context Requested Attributes Advanced Settings	Name*:   app.f5demo.com   Entity ID*: Inttps://app.f5demo.com   SP Name Settings   Scheme :   Host :   Inttps   Description :   Relay State :
	OK Cancel

- 5. Click on the **Security Settings** in the left navigation menu.
- 6. Check the Sign Authentication Request checkbox
- 7. Select /Common/SAML.key from drop down menu for the Message Signing Private Key
- 8. Select /Common/SAML.crt from drop down menu for the Message Signing Certificate
- 9. Click **OK** on the dialogue box

Create New SAML SF	? Service	×
General Settings Charlen Settings Security Settings Authentication Context Requested Attributes Advanced Settings	Authentication and Encryption Settings	
	OK Cancel	

### TASK 2: Configure the External SAML IdP Connector

Refer to the instructions and screen shots below:

- Click on the Access -> Federation -> SAML Service Provider ->
   External IdP Connectors or click on the SAML Service Provider tab in the horizontal navigation menu andselect External IdP Connectors.
- 2. Click specifically on the **Down Arrow** next to the **Create** button (far right)
- 3. Select From Metadata from the drop down menu

Acce	ess	·· Federation : SAML Servic	ce Provider : Local SP	Services				
÷ -		SAML Service Provider 👻 SA					PingAccess -	
	Ţ	Local SP Services						Create
	H-	External IdP Connectors	J	SAML IdP Connect	tors	Description	Partition	Custom
	4	Connector Automation					Common	 From Metadata
	1	Authentication Context Classes Attribute Consuming Services						From Template >
		Attribute Consuming Services					 	

4.	In the Create New SAML IdP Connector dialogue box, click Browse and select
	the <b>idp.partner.com-app_metadata.xml</b> file from the Desktop of your jump host.

5. In the Identity Provider Name field enter the following: idp.partner.com

6. Click **OK** on the dialogue box.

Note: The idp.partner.com-app_metadata.xml was created previously. Oftentimes, iDP providers will have a metadata file representing their IdP service. This can be imported to save object creation time as it has been done in this lab

Create New SAML IdP Co	nnector	×
Select File*:		
idp.partner.com-app_metadataxml		Browse
Identity Provider Name*:		On Desktop
idp.partner.com		
Select Signing Certificate :		
Select a value		*
	ОК	Cancel

### TASK: 3: Bind the External SAML IdP Connector to the SAML SP

Refer to the instructions and screen shots below:

- 1. Click on the **Local SP Services** from the **SAML Service Provider** tab in the horizontal navigation menu.
- 2. Click the **Checkbox** next to the previously created **app.f5demo.com** and select **Bind/Unbind IdP Connectors** button at the bottom of the GUI.

Access » Federation : SAML Service Provider : Local SP Services				
*      * SAML Service Provider      * SAML Service      * SAML Service      * SAML Service      * SAML Identity Provider      * SAML Re			-	
Local SP Services				
External IdP Connectors				
Connector Automation				
Authentication Context Classes				
Attribute Consuming Services			Create	
Name - SAML IdP	P Connectors Description	Partition		
app.fSdemo.com		Common		
Edit Delete Bind/Unbind IdP Connectors Exp	sport Metadata			

- 3. In the Edit SAML IdP's that use this SP dialogue box click the Add New Row button
- 4. In the added row click the **Down Arrow** under **SAML IdP Connectors** and select the /**Common/idp.partner.com** SAML IdP Connector previously created.
- 5. Click the **Update** button and the **OK** button at the bottom of the dialogue box.

Edit SAML IdPs that u	se this SP				×
IdP Connectors associated with	his SP Service				
		Add New Row	Crea	ate New IdP Connector	•
SAML IdP Connectors	Matching Source			Matching Value	
/Common/idp.partner.cc 💙			~		
	Update	Cancel			
Edit Delete					
				OK Cancel	

<ul> <li>6. Under the Access -&gt; Federa Local SP Services menu you</li> <li>Name: app.f5demo.co</li> <li>SAML IdP Connectors</li> </ul>	ou should now see the following <b>m</b>		
Access » Federation : SAML Service Provider : Local SP S	ervices		
SAML Service Provider - SAML Identity Provider -	SAML Resources JSON Web Token - OAuth Authoriza	on Server 👻	
	, , , , , , , , , , , , , , , , , , ,		
Name 🔺	SAML IdP Connectors	Description	
app.f5demo.com	idp.partner.com		

### TASK 4: Configure the SAML SP Access Policy

-	by selecting: <b>Access</b> -> <b>Prof</b> le <b>Create</b> button (far right)	iles/F	Polic	ies ->	Α	cc	ess l	Profile	s (Per-\$	Sessio	n Polici	es)
Main Help About	Access » Profiles / Policies : Access Profiles (Per-Session Policies)											
Statistics	🛪 🗸 Access Profiles 🛛 Per-Request Policies Policy Sync Customization 👻											
iApps	• Search							Create Import				
Wizards	V Status Access Profile Name						Logs Virtual Ser	vers © Partition / Path				
S DNS	Delete Apply	A	NI (	none)	(none)	(none)		Common				
Local Traffic												
Traffic Intelligence												
Acceleration												
Access												
Overview	Access Profiles (Per-Session •											
Profiles / Policies >	Policies)											
Single Sign-On	Per-Request  Policies											
Federation	Policy Sync											
Connectivity / VPN >	Customization											

- 3. In the **New Profile** window, key in the following as shown:
  - Name: app.f5demo.com-policy
  - **Profile Type**: **All** (from drop down)
  - Profile Scope: Profile (default)
- 4. Scroll to the bottom of the New Profile window to the Language Settings
- 5. Select **English** from the **Factory Built-in Languages** menu on the right and click the **Double Arrow** (<<), then click the **Finished** button.

Access >> Profiles / Polici	es : Access Profiles (Per-Session Policies) 🕠	New Profile	
General Properties			
Name	app.f5demo.com-policy		
Parent Profile	access		
Profile Type	All		
Profile Scope	Profile		
	Scroll to Language S	ettings	
Language Settings			
Additional Languages	Afar (aa)		
Languages	Accepted Languages	Factory BuiltIn Languages Japanese (ja) Chinese (Simplified) (zh-cn) Chinese (Traditional) (zh-tw) Korean (ko) Spanish (ces) French (fr) German (de)	
Default Language	English (en)		
Cancel Finished			

6. From the Access -> Profiles/Policies -> Access Profiles (Per-Session Policies), click the Edit link on the previously created app.f5demo.com-policy line.

	_															
Ac	cess															
*			Profiles													
							 	_								
r					Se	earch									Cr	eate Import
1	T	Status	Access	Profile N	lame				Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
0		pø	access				 			All	(none)	(none)	(none)			Common
8		pø –	app.f5der	no.com-p	olicy					All	Edit	Export	Copy	default-log-setting		Common
D	lete	Ap	ply													

7.	In the Visual Policy Editor window for the /Common/app.f5demo.com-policy, click	k
	the Plus (+) Sign between Start and Deny.	

8. In the pop-up dialogue box select the **Authentication** tab and then click the **Radio Button** next to **SAML Auth**. Once selected click the **Add Item** button.

Access Policy: /Common/app.f5demo.com-policy       Edit Endings         Start       fallback       Deny         Add New Macro       Add New Macro         Begin typing to search       Image: Common (app.f5demo) (Clear Side) (Clea
Start       Heny         Add New Macro         Begin typing to search         Iogon Authentication Assignment Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose         HTTP Auth         HTTP Auth         HTTP authentication of end user credentials         Kerberos Auth         Kerberos Auth         LDAP query         LDAP query         LDAP query         LDAP query         LocalDB Auth         Local Database Authentication         NTLM Auth Result         NTLM Auth Result         NTLM Auth Could Database Authentication of end user credentials         Outh Authorization         OAuth Authorization
Begin typing to search         Logon       Authentication         Authentication       Assignment         Endpoint Security (Server-Side)       Endpoint Security (Client-Side)         Image: Security Auth       HTTP authentication of end user credentials         Kerberos Auth       Kerberos authentication, typically following an HTTP 401 Response action         LDAP Auth       LDAP authentication of end user credentials         LDAP Query       LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping         LocalDB Auth       Local Database Authentication         NTLM Auth Result       NTLM authentication of end user credentials         Outh Authorization       OAuth 2.0 Authorization Agent for scope management
Logon       Authentication       Assignment       Endpoint Security (Server-Side)       Endpoint Security (Client-Side)       General Purpose         •       HTTP Auth       HTTP authentication of end user credentials         •       Kerberos Auth       Kerberos authentication, typically following an HTTP 401 Response action         •       LDAP Auth       LDAP authentication of end user credentials         •       LDAP Query       LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping         •       LocalDB Auth       Local Database Authentication         •       NTLM Auth Result       NTLM authentication of end user credentials         •       OAuth Authorization       OAuth 2.0 Authorization Agent for scope management
Logon       Authentication       Assignment       Endpoint Security (Server-Side)       Endpoint Security (Client-Side)       General Purpose         •       HTTP Auth       HTTP authentication of end user credentials         •       Kerberos Auth       Kerberos authentication, typically following an HTTP 401 Response action         •       LDAP Auth       LDAP authentication of end user credentials         •       LDAP Query       LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping         •       LocalDB Auth       Local Database Authentication         •       NTLM Auth Result       NTLM authentication of end user credentials         •       OAuth Authorization       OAuth 2.0 Authorization Agent for scope management
HTTP AuthHTTP authentication of end user credentialsKerberos AuthKerberos authentication, typically following an HTTP 401 Response actionLDAP AuthLDAP authentication of end user credentialsLDAP QueryLDAP query to pull user attributes for use with resource assignment or other functions, such as LDAPLocalDB AuthLocal Database AuthenticationNTLM Auth ResultNTLM authentication of end user credentialsOlduth AuthorizationOAuth 2.0 Authorization Agent for scope management
Kerberos AuthKerberos authentication, typically following an HTTP 401 Response actionLDAP AuthLDAP authentication of end user credentialsLDAP QueryCDAP query to pull user attributes for use with resource assignment or other functions, such as LDAPLocalDB AuthLocal Database AuthenticationNTLM Auth ResultNTLM authentication of end user credentialsOlauth AuthorizationOAuth 2.0 Authorization Agent for scope management
LDAP Auth       LDAP authentication of end user credentials         LDAP Query       LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP         LocalDB Auth       Local Database Authentication         NTLM Auth Result       NTLM authentication of end user credentials         O Auth Authorization       OAuth 2.0 Authorization Agent for scope management
LDAP QueryLDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mappingLocalDB AuthLocal Database AuthenticationNTLM Auth ResultNTLM authentication of end user credentialsOlauth AuthorizationOAuth 2.0 Authorization Agent for scope management
Index Y (uery group mapping       Index J (uery group mapping       Index J (uery group mapping)
·     Local DB Auth     Local Database Authentication       ·     NTLM Auth Result     NTLM authentication of end user credentials       ·     OAuth Authorization     OAuth 2.0 Authorization Agent for scope management
O OAuth Authorization OAuth 2.0 Authorization Agent for scope management
O Auth Client OAuth Client
O Auth Scope OAuth Scope
OCSP Auth         Online Certificate Status Protocol (OCSP) client certificate authentication
On-Demand Cert Auth Dynamically initiate an SSL re-handshake and validate the received client certificate
OTP Generate     Generate One Time Passcode (OTP)
O     OTP Verify     Verify One Time Passcode (OTP)
RADIUS Acct         Send accounting messages to a RADIUS server when users log on and off
RADIUS Auth     RADIUS authentication of end user credentials
RSA SecurID     RSA SecurID two-factor authentication of end user credentials
SAML Auth         SAML Service Provider Interface
TACACS+ Acct         Send accounting messages to a TACACS+ server when users log on and off
TACACS+ Auth     TACACS+ Authentication of end user credentials
Transparent Identity Import         Import Identity (user) information from IF-MAP server
Cancel Add Item Help

- 9. In the SAML Auth configuration window, select /Common/app.f5demo.com from the SAML Authentication, AAA Server drop down menu.
- 10. Click the **Save** button at the bottom of the configuration window.

Properties* Branch Rules	
Name: SAML Auth	
SAML Authentication SP	
AAA Server	/Common/app.f5demo.com
Attribute Consuming Service	None 🚽
Cancel Save (*Data in ta	ab has been changed, please don't forget to save) Help

- 11. In the **Visual Policy Editor** select the **Deny** along the **Successful** branch following the **SAML Auth**
- 12. From the **Select Ending** dialogue box select the **Allow Radio Button** and then click **Save**.

Access Policy: /Common/app.f5demo.co	om-policy Edit Endings (Endings: Allow, Deny [defa	
Start fallback + SAML Auth SAML Auth fallback + ->>> Deny	Select Ending: Allow  Only Cancel Save Help	

13. In the Visual Policy Editor click the Apply Access Policy (top left) and close the Visual Policy Editor.
Note: Additional actions can be taken in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access Policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case

 Image: Completing authentication in the Per Session policy (Access (Access Policy (Access (Access

### TASK 5: Create the SP Virtual Server & Apply the SP Access Policy

	r selecting: Local Traffic -> Virtual Servers • Create button (far right)
Main Help About	Local Traffic Virtual Servers: Virtual Server List
Statistics	•     Virtual Server List     Virtual Address List     Statistics
iApps	Create_
📔 Wizards	V I Status A Name © Description © Application © Description © Service Port © Type Resources © Partition / Path
S DNS	No records to display.
	Enable Disable Delete
Local Traffic	
Network Map	
Virtual Servers	Vinual Server Lat
Policies	V Virtual Address List
Profiles	b Statistics b

- 3. In the New Virtual Server window, key in the following as shown:
  - Name: app.f5demo.com
  - Destination Address/Mask: 10.1.10.100
  - Service Port: 443
  - HTTP Profile: http (drop down)
  - SSL Profile (client): app.f5demo.com-clientssl
  - Source Address Translation: Auto Map
- 4. Scroll to the Access Policy section
  - Access Profile: app.f5demo.com-policy
  - Per-Request Policy: saml_policy
- 5. Scroll to the Resource section
  - Default Pool: app.f5demo.com_pool
- 6. Scroll to the bottom of the configuration window and click Finished

Note: The use of the Per-Request Policy is to provide header injection and other controls. These will be more utilized later in the lab.

Local Traffic	: : Virtual Server List » New Virtual Server
General Properties	
Name	app.f5demo.com
Description	
Туре	Standard
Source Address	
Destination Address/Mask	10.1.10.100
Service Port	443 HTTPS •
Notify Status to Virtual Address	
State	Enabled
Configuration: Basic	
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
	Selected Available
SSL Profile (Client)	/Common     /Common       app.f5demo.com-clientssl        >>     /Common       clientssl     clientssl-insecure-compatible       clientssl-secure     crypto-server-default-clientssl
	Scroll to Source Address Translation
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map 🖌
Access Policy	Scroll to Access Policy Section
Access Profile	app.f5demo.com-policy
Connectivity Profile	+ None 1
Per-Request Policy	saml_policy
	Scroll to Default Pool
Default Pool +	app.f5demo.com_pool
Default Persistence Profile	None
Fallback Persistence Profile	None

257

### TASK 6: Test the SAML SP

Refer to the instructions and screen shots below:

- 1. Using your browser from the Jump Host click on the provided bookmark or navigate to https://app.f5demo.com . The SAML SP that you have just configured.

   Image: Strate of the strate of th
  - 2. Did you successfully redirect to the IdP?
  - 3. Login to the iDP, were you successfully authenticated? (use credentials provided in the Authentication Information section at the beginning of this guide)
    - Username: user
    - · Password: Agility1
  - 4. After successful authentication, were you returned to the SAML SP?
  - 5. Were you successfully authenticated (SAML)?
  - 6. Review your Active Sessions (Access Overview -> Active Sessions)
  - 7. Review your Access Report Logs (Access -> Overview Access Reports)

APPLICATION MATION		
Host	app.15demo.com	
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0	
Accept	text/html,application/xhtml+xml,application /xml;q=0.9,*/*;q=0.8	
Accept-Language	en-US,en;q=0.5	
Accept-Encoding	gzip, deflate, br	
Cookie	LastMRH_Session=6544be14; F5_ST=1212121531200137z604800	
DNT		
Connection	keep-alive	
Upgrade-Insecure-Requests		
SAMLResponselssuer	https://idp.partner.com/app	
SAMLIdentity	user	
ClientPlatform	Linux	
ClientIP		
EmailAddress	user@partner.com	

# 6.3 Lab 2: IDaaS SAML Identity Provider (iDP) Lab (OKTA)

The purpose of this lab is to configure and test a IDaaS SAML Identity Provider. Students will configure a IDaaS based SAML Identity Provider (in this case OKTA) and import and bind to a SAML Service Provider and test IdP-Initiated and SP-Initiated SAML Federation.

## 6.3.1 Objective:

- Gain an understanding of integrating a IDaaS SAML Identity Provider(IdP)
- · Gain an understanding of the access flow for IdP-Initiated SAML

# 6.3.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- · Estimated completion time: 25 minutes

# 6.3.3 Lab 2 Tasks:

### TASK 1: Sign Up for OKTA Developer Account

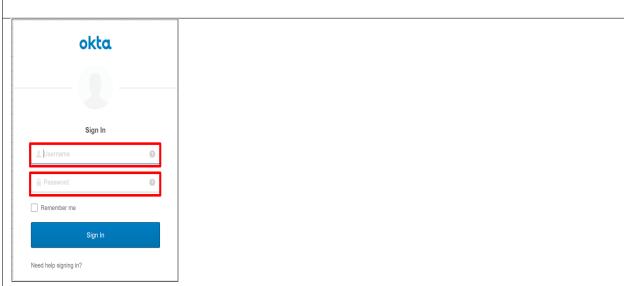
Refer to the instructions and screen shots below:

Note: The following steps provide instruction for setting up an OKTA developer account. If you already have one, you may elect to use that account. Understand, however, that the instructions below may need to be modified to match your environment.

- Sign Up for an OKTA developer account by navigating to: https://developer.okta.com/signup/ and using a VALID email and click Get Started
   Lippa registration, you will be directed to a bunching (bectmann) for your developer.
- 2. Upon registration, you will be directed to a hyperlink (hostname) for your developer account. This link should be saved for future use.
- 3. Additional instructions will be sent to the email address provided during account setup.

	BLOG DOCS SUPPORT	Q	
{okta} product pricing	BLOG DOCS SUPPORT	Ч	
	Start building on Okta		
	Email		
	First Name		
	Last Name		
	Company		
	GET STARTED		
	By clicking the button you agree to the lerms & conditions.		
	By clicking the batton you agree to the terms a concludes.		
We	elcome! You're ready t	o qo.	
	ے Follow the link in the email to begin accessing your new Ol!		
	Your Okta URL:		
	dev-XXXXX .oktapreview.co	m	
	Save this URL so you can access your account later		
	Have a question? We're here to help.		
	Post it in the Okta Developer Forums		
	Open a ticket by logging in to your account and clicking	Help'	
	Call us: 1-888-722-7871 To learn more about the Okta identity platform, check out o	ur docs	
	To real more about the Okta Identity plation in, check out o		

4. Following the instructions received from the generated email, sign into the OKTA development environment with your provided, temporary password.



- 5. Enter a New Password and the Repeat New Password
- 6. Use the drop down to select a Forgot Password Question and provide the Answer
- 7. Click a Security Image
- 8. Click Create My Account

Absword requirements: at least 8 characters, a lowercase letter, a number, no parts of your username.         Expert are parsword         Image: Constant of the work your of the work of		•••••
Choose a forgot password question Minere were you on New Year's Eve in the year 2000? Answer  Crovided answer> Cick a picture to choose a security Image Your security image gives you additional assurance that you are logging		
Choose a forgot password question     More were you on New Year's Eve in the year 2000?     Answe     Choose a security image     Click a picture to choose a security image     Your security image gives you additional assumance that you are logging		Repeat new password
		•••••
Answer	U	
<pre></pre>		
Click a picture to choose a security image Your security image gives you additional assurance that you are logging		
Your security image gives you additional assurance that you are logging		<provided answer=""></provided>
Your security image gives you additional assurance that you are logging		
Your security image gives you additional assurance that you are logging		
Your security image gives you additional assurance that you are logging		
Your security image gives you additional assurance that you are logging		
Your security image gives you additional assurance that you are logging		
		into Okta, and not a fraudulent website.
		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

## TASK 2: OKTA Classic UI

Refer to the instructions and screen shots below:

For the purposes of the lab and SAML development, we will be using the OKTA Classic UI which provides access to SAML configurations. (*Note: At lab publication, the Developer Console did not have SAML resources.*)
 In the top, left hand corner click the <> & select Classic UI from the drop down.

<>> Developer Console ▼				
Classic UI	Users	Applications	API	Customiz

### TASK 3: Enable OKTA Multi-Factor Authentication [OPTIONAL]

Refer to the instructions and screen shots below. This task will require a mobile app to enable a second factor.

<b>[OPTIONAL]</b> Note: Enabling MFA will require a Sma The step can be skipped if you prefer to 1. Click <b>Security</b> from the top navig	o just use UserID/Password	A client for your OS
okta Dashboard Directory Applications	Security Reports Settings	
🕖 Dashboard	General Authentication	
Status	Multifactor	

## [OPTIONAL]

- 2. Under OKTA Verify, change the dropdown from Inactive to Active
- 3. Click the Edit button next to *OKTA Verify Settings

Multifactor	Fector Enrollment Help	
Factor Types Factor Enrollment		
Okta Verify SMS Authentication Voice Call Authentication Google Authenticator	Okta Verify After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.	
Windows Hello (Web Authentication)		
U2F Security Key (FIDO 1.0)	Okta Verify Settings	
Yubikey Symantec VIP	Enable Push Notification	
On-Prem MFA RSA SecurID	Require Touchid for Okta Verify	
Security Question		

# [OPTIONAL]

- Check Enable Push Verification
   Check Require TouchID for OKTA Verify (optional)
- 6. Click Save

Multifactor	Factor Enrollment Hel
Factor Types Factor Enrollment	
Okta Verify 🔗	Okta Verify
Voice Call Authentication	After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit
Google Authenticator	number to gain access.
Windows Hello (Web Authentication)	
U2F Security Key (FIDO 1.0)	Okta Verify Settings Cancel
Yubikey	
Symantec VIP	Chable Push Notification
On-Prem MFA	Require Touchid for Okta Verify
RSA SecurID	
Security Question	Save

## TASK 4: Build SAML Application - OKTA

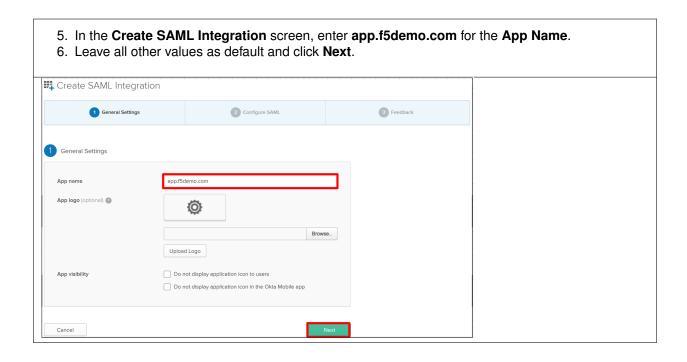
	the main o navigat		click <b>Appl</b>	ication	<b>is</b> , and .	Applica	<b>tions</b> from the dr	ropdown in the	;	
okta	Dashboard	Directory	Applications	Security	Reports	Settings	My Applications			
🕖 Dasht	board		Applications Self Service				S			

2. 0	2. Click Add Application in the Applications dialogue window.							N.
okta	Dashboard	Directory	Applications	Security	Reports	Settings	My Applications 🕣	Upgrade
Applic	cations							Help
👯 Add Appl	ication 🐺 As	sign Application	6					
Q þearch								
STATUS								
INACTIVE	0					1101110		

3. Click Crea	3. Click Create New App in the Add Application Menu							
okta Dashboard	Directory	Applications	Security	Reports	Settings	My	Applications 🔿	Upgrade
← Back to Applications								
Q Bearch for an application				All A B C	DEFGHI	JKLMNO	PQRSTU	v w x y z
Can't find an app? Create New App		<b>O</b> TELADOC	Teladoc Okta Verified					Add
Apps you created (0) $\rightarrow$		&frankly	<b>&amp;frankly</b> Okta Verified	✓ SAML				Add

- 3. In the **Create a New Application Integration** dialogue box, select **Web** from the drop down for **Platform**.
- 4. Select the SAML 2.0 radio button for Sign on Method and click Create.

Create a New Application Integration		×
Platform	Web v	
Sign on method	Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps.	
	SAML 2.0 Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.	
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
	Create	



- 7. In the **Create SAML Integration** screen, enter the following values
- 8. In the SAML Setting section
  - Single Sign on URL: https://app.f5demo.com/saml/sp/profile/post/acs
  - Audience URI (SP Entity ID): https://app.f5demo.com
- 9. Leave all other values as default and click Next.

Create SAML Integratio	on	
1 General Settings	2 Configure SAML	3 Feedback
SAML Settings		
		What does this form do?
GENERAL		This form generates the XML needed for the app's SAML request.
Single sign on URL 💿	https://app.f5demo.com/saml/sp/profile/post/acs	Where do I find the info this form needs?
	✓ Use this for Recipient URL and Destination URL	The app you're trying to integrate with should have its own documentation on
	Allow this app to request other SSO URLs	using SAML. You'll need to find that doc,
Audience URI (SP Entity ID)	https://app.f5demo.com	and it should outline what information you need to specify in this form.
Default RelayState 👔		Okta Certificate
	If no value is set, a blank RelayState is sent	Import the Okta certificate to your Identity Provider if required.
Name ID format	Unspecified v	1 Download Okta Certificate
Application username	Okta username v	
	Show Advanced Se	ettings
ATTRIBUTE STATEMENTS (OPTIONA	d.) LEARN	MORE
Name Name for	mat (optional) Value	
Unspe	cified v	×
Add Another		
Note:	Additional screen content removed.	
Previous Cancel	N	lext

"I'm an OKT Are you a cu 11. In the resultin	A custo ustomering expari nternal	Integration screen, mer adding an inter or partner? nded window, select app that we have o	ernal a	<b>pp</b> " radio button for
Create SAML Integrati	ion			
1 General Settings		2 Configure SAML		3 Feedback
3 Help Okta Support understand Are you a customer or partner?	I'm an Ok	ed this application ta customer adding an internal app ware vendor. I'd like to integrate my app with Okt	a	Why are you asking me this? This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.
The optional questions below	v assist Okta Suppor	t in understanding your app integration.		
App type 👔	✓ This is an	internal app that we have created		
Previous			Finish	

- 12. In the resulting application screen for **app.f5demo.com**, navigate to the **SAML 2.0 section**.
- Right Click the Identity Provider Metadata hyperlink and click Save Link As ...
   Save the metadata.xml to your jumphost desktop. We will be using it in a later step in the Lab.

General Sign On Import Assignments		
Settings Edit	About SAML 2.0 streamlines the end user experience by not requiring the user to	
SIGN ON METHODS The sign-on method determines how a user signs into and manages their credentials for an application. Some sign- on methods require additional configuration in the 3rd party application.	know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuretion in the 3rd party application may be required to complete the integration with Okta.	
© SAML 2.0	Application Username Choose a format to use as the default	
Default Relay State	username value when assigning the application to users.	
SAML 2.0 is not configured until you complete the setup instructions.      View Setup Instructions      Identity Provider metadata is available if this application supports dynamic configuration.      Open Link in New Jab	If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.	
Open Link in New Private Window Bookmark This Link Save Link As Save Link to Pocket		
Application username fo Search Google for "Identity Provid" Send Link to Device		
Update application user Inspect Element (Q)		

## TASK 5: Add User to SAML Application

Refer to the instructions and screen shots below:

<ol> <li>Within the app.f5demo.com applica and then Assign to People from the</li> </ol>		ssignments	then <b>Assign</b>
app.f5demo.com			
General Sign On Import Assignments			
Assign  Convert Assignments	Q Search	People 🔻	
Assign to People	Туре		
Assign to Groups			

 In the Assign app.f5demo.com to People dialogue box, select your User ID, click Assign, then Done.

Assign app.f5demo.com to People	×
Q Search	
Your selected user account	Assign
	Done

3. Click Save and	d Go Back.	
Assign app.f5demo.	com to People	×
User Name	Your selected user account	
	Save and Go Back	Cancel

4. Click <b>Done</b> .	
Assign app.f5demo.com to People	×
Q þearch	
Your selected user account	Assigned
	Done

## TASK 6: Add Multi-Factor Authentication Sign-On Policy [OPTIONAL]

Refer to the instructions and screen shots below. This section requires that **Task 3** be completed.

[OPTIONAL] 1. Within the app.f5demo.com application screen, Click Sign On	
app.f5demo.com	
General Sign On Import Assignments	

[OPTIO 2. Sc	NAL] rroll down to the Sign On P	olicy section and	d click Add	Rule	
Sign On	Policy				
Add I     Priority	Rule		Status	Actions	
Flionty	Rule Hallie		Status	Actions	
1	Default sign on rule		Active	Not editable	
	CONDITIONS		ACTIONS		
🤽 User	assigned this app	🔎 Allow access			
Anyv	vhere				

OPTIONAL]	
3. In the Add Sign On Rule dialog	gue box, enter MFA for the Rule Name.
4. Scroll down to the <b>Actions</b> sect	
	ccess, check the box for Prompt for factor.
6. Ensure Every Sign On radio bu	utton is selected.
7. Click <b>Save</b> .	
7. Onor Cave.	
	×
Rule Name MFA	
Disable rule	
CONDITIONS	
1 PEOPLE	
Who does this rule apply to?	
Users assigned this app     The following groups and users:	
LOCATION	
•	
If the user is located:      Anywhere	
O In Zone	
O Not in Zone	
ACTIONS	
ACCESS	
When all the conditions above are met, sign on to this application is: $\fbox{\label{eq:lowed_velocity}}$	
Prompt for re-authentication	
Prompt for factor - Multifactor Settings	
Every sign on     Once per session	
O Once a day	
Once a week     Once a month	
O Once per six months	
O Only once	
Sove	ancel

## TASK 7: Create the External IDP Connector

<ol> <li>Login to your lab pro</li> <li>Begin by selecting: <i>A</i></li> <li>External IdP Conne</li> </ol>	Access -> Federation -			Provid	der ->	
Access						
Overview	• •	_				
Profiles / Policies	SAML Service Provider	- F - 1	Local SP Services	÷	r - -	
	SAML Identity Provider	•	External IdP	(+)		
Authentication	SAMI Resources	ML Resources (*) Connectors	Connectors	U		
Single Sign-On	•		Connector	(+)	-	
Federation	JSON Web Token		Automation	0		
	OAuth Authorization		Authentication	(+)		
Connectivity / VPN	Server		Context Classes	0		
Secure Web Gateway	OAuth Client / Resource	e .	Attribute			
Access Control Lists	Server		Consuming	$\odot$		
	PingAccess		Services			
Webtops	Edit	Delete	e			

- 3. In the External IdP Connectors screen, click the downward arrow next to the word Create on the Create button (right side)
- 4. Select From Metadata from the drop down menu

_									
Access ·· Federation : SAML Service I	Provider : External IdF	P Connectors							
🚓 🗸 SAML Service Provider 👻 SAML									
Use this application to manage SAML IdP connections by clicking the respective butto	connectors. When you ons.	use this BIG-IP sys	tem as a SAML service	provider, it sends auther	tication	requests to the IdP and in turn recei	res assertions from the li	IP. You can create, edit	and delete IdP
Name 🔺		SAML SP Service	s	Desc	ription		Partition		Custom
idp.partner.com		app.f5demo.com					Common		From Metadata
									From Template ▶

- 5. In the **Create New SAML IdP Connector** dialogue box, use the **Browse** button to select the **metadata.xml** from the desktop (created in Task 4).
- 6. Name the Identity Provider Name: OKTA_SaaS-iDP.
- 7. Click OK.

Create New SAML IdP Connector	×
Select File*:	
metadata.xml	Browse
Identity Provider Name*:	
OKTA_SaaS-iDP	
Select Signing Certificate :	
Select a value	*
ОК	Cancel

### TASK 8: Change the SAML SP Binding

- 1. Begin by selecting: Access -> Federation -> SAML Service Provider -> Local SP Services
- 2. Select the checkbox next to app.f5demo.com and click Bind\UnBind IdP Connectors

_					
Acce	ss ··· Federation : SAML Service Provider : Local SP				
* •	SAML Service Provider - SAML Identity Provider -			PingAccess -	
	Local SP Services		,		
	External IdP Connectors				
	Connector Automation				
	Authentication Context Classes				
	Attribute Consuming Services				Create
	Name 🔺	SAML IdP Connectors	Description	Partition	
	app.f5demo.com			Common	
	Edit Delete Bind/Unbind IdP Connecto	rs Export Metadata			

3. Check the existing binding and	l click <b>Delete</b> .		
Edit SAML IdPs that use this SP		×	
IdP Connectors associated with this SP Service			
	Add New Row Cre	eate New IdP Connector 👻	
SAML IdP Connectors Matching Source		Matching Value	
Common/idp.partner			
Edit Delete			
		OK Cancel	

<ul> <li>4. Click Add New Row and use the following values <ul> <li>SAML IdP Connectors: /Common/OKTA_SaaS-iDP</li> <li>Matching Source: %{session.server.landinguri}</li> <li>Matching Value: /*</li> </ul> </li> <li>5. Click Update then OK.</li> </ul>	
Edit SAML IdPs that use this SP *	
IdP Connectors associated with this SP Service	
Add New Row Create New IdP Connector	
SAML IdP Connectors Matching Source Matching Value	
/Common/OKTA_SaaS· V %{session.server.landinguri} V /*	
Update     Cancel       Edit     Delete	
OK Cancel	

## **TASK 9: Apply Access Policy Changes**

Refer to the instructions and screen shots below:

1. Click the Apply Access Policy link in the top left corner of the Admin GUI									
Hostname: bigip01.f5demo.com IP Address: 10.1.1.245	Date: Jul 10, 2018 User: admin Time: 12:49 AM (PDT) Role: Admi								
ONLINE (ACTIVE Standalone Apply Access Pol									

2. Ensure app.f5demo.com-policy is checked and click Apply											
Access >> Profiles / Poli	Access										
🕁 🚽 Access Profiles	Per-Request Policies	Policy Sync	Customization	-							
*	Sea	rch									
Status Access	Profile Name										
🛛 📔 app.f5den	app.f5demo.com-policy										
Apply											

## TASK 10 – Test Access to the app.f5demo.com application

Refer to the instructions and screen shots below:

i https://app.f5demo.com

 Using your browser from the Jump Host click on the provided bookmark or navigate to: https://app.f5demo.com
 Bile Edit View History Bookmarks Tools Help
 BIG-IP® - bigip01.f5der × BIG-IP® - VPE - /Comm × New Tab × + 10. Destroy your Active Session by nagivating to **Access Overview** -> **Active Sessions** Select the checkbox next to your session and click the **Kill Selected Session** button.

Access » Overview : Active Se	ssions	
Active Sessions Acces	s Reports C	Auth Report
Display Options		
Auto Refresh	Disabled	<ul> <li>Refresh</li> </ul>
Refresh Session Table		
Total Active Sessions		
Active Session Count	1	
Active Session Count	1 Sea	rch
	Sea	nch] ▲User ♦
	Sea	

- 11. Close your browser and logon to your https://dev-<Dev-ID>.oktapreview.com account. Click on your app.f5demo.com application for IDP initiated Access.
- 12. After successful authentication, were you returned to the SAML SP?
- 13. Were you successfully authenticated (SAML)?
- 14. Review your Active Sessions (Access Overview -> Active Sessions).
- 15. Review your Access Report Logs (Access Overview -> Access Reports).

Work	+	
Ø		
app.f5demo.com		

# 6.4 Lab 3: oAuth and OpenID Connect Lab (Google)

The purpose of this lab is to better understand the F5 use cases OAuth2 and OpenID Connect by deploying a lab based on a popular 3rd party login: Google. Google supports OpenID Connect with OAuth2 and JSON Web Tokens. This allows a user to securely log in, or to provide a secondary authentication factor to log in. Archive files are available for the completed Lab 2.

# 6.4.1 Objective:

- Gain a better understanding of the F5 use cases OAuth2 and OpenID Connect.
- Develop an awareness of the different deployment models that OAuth2, OpenID Connect and JSON Web Tokens (JWT) open up

# 6.4.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- · Estimated completion time: 25 minutes

# 6.4.3 Lab 3 Tasks:

### **TASK 1: Setup Google's API Credentials**

Refer to the instructions and screen shots below:

	e Google/gMail account, you will need to set one up. Navigate to: velopers.google.com/apis/credentials & follow the directions for setup.*
Google	Coops
Sign in 10 continue to Google Cloue Platform	Create your Coople Account toon
Pergebana P	
Not provide an equal of the fit and contributing the prior help between the $\sigma$	Bernel Den Bernel Britsen Berne Bernel Bernel State Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Bernel Berne Bernel
Code several NDT	Algrammer No.

1. Navigate to https://console.developers.google.com/apis/credentials and log in with your developer account.

No.10	x +	5	s   00
(⊖) → @ @	<ul> <li>https://console.developers.google.com/kpis/credentisis</li> </ul>	→ D, Suppl N, Classification	=

- 2. You will be redirected to the Google API's screen. If you are previously familiar with Google API's you can create a new Project.
- 3. If you have not been you will be prompted to create a New Project.
- 4. Click **Create** in the dialogue box provided.

=	Google APIs Select a	project 👻 🔍		8	9	0	0	I	۲
RPI	APIs & Services	Credentials							
	Dashboard Library								
	condentrale.		Alto & Services						
			Credentials						
			To view hile program, select a project.						

5.	In the New Project window, provide a Project Name.	The suggested	value is:
	F5 Federation oAuth		

Note: If you have exceeded your project quota you may have to delete a project or create a new account

≡ Google APIs	Q	
New Project		
You have 10 projects remaining	g in your quota. Learn more.	
Project name 💿		
F5 Federation oAuth		
Your project ID will be f5-federation-oaut	h 🛞 Edit	
Create		

<ol> <li>In the next screen, select OAuth Client ID for the Credentials type and click Create Credentials</li> </ol>								
😑 Google APIs 🗧 Paredentian cauda 👻	۹. 🗱	9 0 🜔 i 😩						
RPI APIS & Services Credentiels								
de Deshtoard St Library Pe Crecientals	ich sonsent sensen – Sionnain verifiziellen							
	4/htep Installar root scored raises a simple advance work MAS GAY II Beginshows assumed to push applicate access the workfull Beginshows and May Databases server its server, applicing white advanced data states Databases server its server, applicing white advanced data states and advanced data states and advanced advanced advanced advanced advanced Databases server its server, applicing white advanced data states and advanced advanced advanced advanced advanced advanced advanced advanced advanced advanced advanced advanced ad	a						
	Hep the dhoose makes them paratises to help you disconnected type of conce Oriente opportunity							

<ol> <li>If you have not previously ac Click Configure Consent S</li> </ol>		Screen you may be prompte	ed to do so.
⊟ Google APIs ⇒ Ki Federation andt → ^Q	n e e 🔘 i 😩		
Create DAuth client ID			
$\hat{\mathbf{u}}_{i}$ to cerea an shuff client $\hat{\mathbf{u}}_{i}$ voumant that set a post-of name as the constant screen	Vietours cansert coren		
Application type			

- 8. On the OAuth Consent Screen tab, enter the email address of your developer account (pre-populated) for the Email Address.
   9. For the Product Name Shown to Users enter app.f5demo.com.
- 10. Click Save.

Ĺ.	RPI APIs & Services	Credentials	
	Outboard	Endertisis Outlin consent some Domain verification	
	E User	fead allers ()	
	<ul> <li>Orderäris</li> </ul>	remail address	
		app Mornaucon	
		Receipings (III. (Spland) (Spac) = 10 p./	The consent screep will be shown to
		Parties logs (0) ((pland) (0)	attest whohever you request access to their private data acception sheat. 5. If will be shown for all
		hilly /www.completion.children	applications registered in Itia preject.
		The information was reading with both and used Mexical topical ac	Processed provide on small address and product some for SAult to work.
		Privacy policy (No. Eprimed and you deploy your oper	
		https://wittp://	
		Teams of service (dit, (Contras)) Integral = Frig. (	
	a		
	-	2049 02001	

<ol> <li>In the Create OAuth Client ID⁴</li> <li>Application Type: Web Applie</li> <li>Name: app.f5demo.com</li> <li>Authorized JavaScript Engine</li> <li>Authorized Redirect URIs: ht</li> <li>Click Create.</li> </ol>	cation e: https://app.f5c	demo.com
Google APIs IP 15 Federation of with * 0,	ii 🖉 e 🕥 i 😩	
<ul> <li>Create Quith client ID</li> </ul>		
Mellocation con     Annual Constantian     Annual Constantian		
Autorized Autorize anglera Per ane with request a form a forward. This is the organ DP of the charts application. To any contrast a without Bifugut "Anamathicana", or a path (Mapacinaampin contraction), if you're uting a stantiant anglera', you matteriaabrit		
In the unique LAT. Inflyes: (https://talentine.com/		
Mige Very search and		
Autorized editors VIII. In each with square from some series, here it the generic pure tabletation that a serie editors that is then the summarized end to the square of the square of the square of the statement. Control called UII, here we are the state (Christian editor) and the statement. Integrating the from called the statement of the statement of the statement. Integration called the statement of the		

13. In the <b>OAuth Client</b> pop-up window copy an <b>Client Secret</b> in Gedit text editor provided or	
OAuth client	
Here is your client ID	
Kyour dient ID>	
Here is your client secret	
<your client="" secret=""></your>	¹ O
	ок

## TASK 2: Setup F5 OAuth Provider

	OAu	th Client/F			by navigating to <b>Access</b> -> <b>Federation</b> -> rver -> <b>Provider</b> and clicking <b>Create</b> .
		leri Fannen Sever-Foelder 1949, Moley Persie + 1948, Pe	anna 1936 (ch	Star + Chab A	notation fanor - Daub Clevi i Resson Row - Projector
Noviders				Cealer	
V I Have	1 Japan	1 One Auto-decoversource	OAUX Server	· Partition	
AsviA0	Asun40	taise		Gennos	
11 Hi	F6	tata -		Centrol	
E Faorbook	Facebook.	foit+		Germon	
TT Scoole	Google	tabe .		Centrol	
[]					
0.000	ORM	talar .		Germon	

- 2. Using the following values to complete the OAuth Provider
- Name: Google_Provider
- Type: Google
- Trusted Certificate Authorities: ca-bundle.crt
- Allow Self-Signed JWK Config: checked
- Use Auto-discovered JWT: checked
- 3. Click **Discover**.
- 4. Accept all other defaults.
- 5. Click Save.

eneral Properties Name	Google_Provider			
Description				
Туре	Google 🗸			
gnore Expired Certificate Validation				
Trusted Certificate Authorities	ca-bundle.crt	~		
Allow Self-Signed JWK Config Certificate				
Use Auto-discovered JWT				
OpenID URI	https://accounts.google.com/.well-know Last discovery time: 2018-06-05 18:41:2		Discover	
Authentication URI	https://accounts.google.com/o/oauth2/	v2/auth		
Token URI	https://www.googleapis.com/oauth2/v4	/token		
Token Validation Scope URI	https://www.googleapis.com/oauth2/v3	/tokeninfo		
UserInfo Request URI	https://www.googleapis.com/oauth2/v3	/userinfo		
issuer	https://accounts.google.com			
Signing Algorithm	Allowed RS256	Blocked		
		*	4	
Key (JWK)	Allowed	Blocked		
	RSA:1923397381d9574bb87320 RSA:3bcf0b3cc862a0ac77092f72	*		

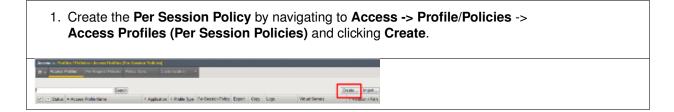
## TASK 3: Setup F5 OAuth Server (Client)

<ol> <li>Create the OAuth Server (Client) by navigating to A OAuth Client/Resource Server -&gt; OAuth Server ar</li> </ol>	
Access a Fabrician - Sector Care Fiberator Serve - Oden S	
Openant         Constru-           ~ # Hance         1 Mate:         1 Application:         Provide:         Provide:           No records to Stapling.         Deces.         Deces.         Deces.         Deces.	

- 2. Using the following values to complete the OAuth Provider
- Name: Google_Server
- Mode: Client
- Type: Google
- OAuth Provider: Google_Provider
- DNS Resolver: proxy_dns_resolver
- Client ID: <your client id>
- Client Secret: <your client secret>
- Client's Server SSL Profile Name: serverssl
- 3. Click Finished.

Google_Server
Cient
Google
Google_Provider
t proxy_dns_resolver .
Selected Available  //coarsev AM_Dppase APM_Coole_Remove ASM_Google_reCaptche_v2
60 minutes
< Your Client ID >

## TASK 4: Setup F5 Per Session Policy (Access Policy)



<ul> <li>Name:</li> <li>Profile</li> <li>Profile</li> </ul>	New Profile dialogue window enter the followir : Google_OAuth e Type: All e Scope: Profile uage: English Finished.
Access 10 Profiles /	/ Policies : Access Profiles (Per-Session Policies) - New Profile
General Properties	
Name	Google_OAuth
Parent Profile	access
Profile Type	All
Profile Scope	Profile
Language Settings	Scroll to the bottom of the screen
Additional Languages	Alar (we) m Add
	Accepted Languages Factory Bullin Languages
	English (m)
Languages	ks Samah (x)
	Serian (de)
Debuil Language	English (en) 💌
Carcal Finished	

4. Click Edit link of		e Google_OAuth A	ccess Poli
Access - Profiles (Publics : Access Profiles (Prefices on Porche)			
C - Arrens Publics Per Separal Publics Public Epice 2	Contradication		
Congin', Gilante (Search) (Search)			Cente Import
🧭 🖛 Status 🖛 Access Phalis Name	A Application & Profile Typ	ppe PardissionPolicy Exped Expy Logs	Vited Seven © Patton/Path
E 👂 Stogle_Chuin	M	D tot Expert Dogs detail togsaling	Common
Delta. Appy			

- 5. In the Google_OAuth Access Policy, click the "+" between Start & Deny6. Click the Authentication tab in the events window.
- 7. Scroll down and click the radio button for **OAuth Client**.
- 8. Click Add Item.

l	6		-				-
1	iccess Policy: /Common/Google_OAuth	1.	onto Pa	wine to search			۹,
	tabe 🗖	1	[	Andread and an Annual	ni ( <u>Brazal Assels: See, See</u> ) <u>Balani Seela Seela</u>	ac Sectors	
	Rash - Miter	Ċ.	151	MiA ther helfcature	IS MA per hefotan		
	Add New Posts	0	H	TP Auto	HTTP authentication of end user contention		
	AND PER MANY	0	Ref.	ter is Adh	Referror automization, typically following an WTTP 152. Response	alar	
			UM	AD AND.	URAP suchantication of and user credentals		
	An access policy consists of a start sumit, actions, and one or Ock the Add Harme butter to add a purpose-built set of pr		12/	AD Query	LEAV query is pull-use storic-be for use with ressure pargement methods.	t or other functions, such as 2049 group	l II
	You can get started with <u>Reside Mittach</u> . On the rain savigs	Ô.	Link	ditti Auth	Leaf Estable Authentication		
	Hamager: Wood Policy Full ar on line <u>Additionation</u> for me	0	нп	State Beach	1718 automization of real care contentials		
	Please see the <u>Orden Ests</u> for over Visal Policy Differ basics	0	08	ath authorities	Owath 2.8 Authorstoon Agent for some management		
		٠	08	NO DHE	Onut) these		
			05	all's Respon	Oliali: Seyer		IJ
		Gro	et [	AM Bark			Hala
			_				

- 9. In the ***OAuth_Client*** window enter the following values as shown:
- Server: /Common/Google_Server
- Grant Type: Authorization code
- OpenID Connect: Enabled
- OpenID Connect Flow Type: Authorization code
- Authentication Redirect Request: /Common/GoogleAuthRedirectRequest
- Token Request: /Common/GoogleTokenRequest
- Refresh Token Request: /Common/GoogleTokenRefreshRequest
- OpenID Connect UserInfo Request: /Common/GoogleUserinfoRequest
- Redirection URI: https://%{session.server.network.name}/oauth/client/redirect
- Scope: openid profile email
- 10. Click Save.

Properties* (Roods Rober)		
Neme: 04uth Olent		
OAuth		
Server	/Cananos/Scople_Server -	
Grant Type	Authoration rade -	
OpenID Connect	Crubled x	
OpenED Connect: Revin Type	Authorization code	
Authentication Redirect Request	/Common/GoopleAsthRedirectRequest x	
Token Republi	/Control/GoogleTakanTequest	
Refrech Taken Request	/Common/GoogleTakenRefreshRequest +	
OpenID Consect UserInfo Request	/Constant/GoogleLearnfold-quett -	
Advector UR:	https://%isester.server/retwork/renet/card//dent/redired.	Set Cellent
Scope	openid profile email	
Cancel Serve "Orto is tob has been o	tanged, please don't forget to save)	Hele

11. Click on the **Deny** link, in the **Select Binding**, select the **Allow** radio button and click **Save**.

Access Policy: /Common/Google_OAuth	dt Endings (Endings: Alow, Dwy (debailt))	
Start habet +- Chath Clent Sameral + t Dan	Salet Indag:	
Add New Marro		
	Cancel Save Heb	

12. Click on the <b>*Apply Access Policy</b> * link in the top left-hand corner. Note: Additional actions can be taken in the Per Session policy (Access Policy). The lab is simply completing authorization. Other access controls can be implemented based on the use case.
1 Apply Access Policy
Access Policy: /Common/Google_OAuth Edit Endings (Endings: Allow, Deny (default))
Start
Add New Macro

#### **TASK 5: Associate Access Policy to Virtual Server**

Refer to the instructions and screen shots below:

- 1. Navigate to Local Traffic -> Virtual Servers -> Virtual Server List and click on the app.f5demo.com Virtual Server link.
- 2. Scroll to the Access Policy section.

s : Virtual Server I	iat o app.15den	10.000	
			2
app./5demo.com			
Common			
1			
Standard			
0.0.0.0/0			
10.1.10.100			
443 HTT	PS 💌		
v			
None			
🔲 Unknown (Ena	oled) - The childre	n pool member(s	) either don't have servic
or			
Enabled +			
	app./5demo.com Common [] Standard 0.0.0.0/0 [10.1.10.100 [443 [HTT] [V] None [] Unknown (Enat Of	app /5demo.com Common [ ] Standard 0.0.0.0/0 [ 10.1.10.100 [ 443 HTTPS None Unknown (Enabled) The childre Of	app.#sdema.com Common [] Standard 0.0.0.0/0 [10.1.10.100 [10.1.10.100 [443] HTTPS None [] Unknown (Enabled) The children pool member(s

- 3. Use the Access Profile drop down to change the Access Profile to Google_OAuth
- 4. Use the **Per-Request Policy** drop down to change the **Per-Request Policy** to **Google_oauth_policy**
- 5. Scroll to the bottom of the Virtual Server configuration and click Update

Access Profile	Google_CAuth
Connectivity Profile	None
Per-Request Policy	Google_oauth_policy
VDI Profile	None
Application Tunnels (Java & Per- App VPN)	Enabled
OAM Support	Enabled
ADFS Proxy	Enabled
PingAccess Profile	None -

#### TASK 6: Test app.f5demo.com

1. Navigate in your provided b	rowser to https://app.f5demo.com	
Ondetionary X	m 7 12	
→ Q ^e A Q heperheadSerracer	9. Server 🗴 🛤 🖸 🛩 =	

2. Authenticate with the account you established your Google Developer account with.

🖸 Signila - Coogle Accour	• x +	
)⇒ <b>¢</b> ∆ ©	🕯 hljodemurlagioglemedojneto — 🖤 🛱 🗋 🔍 korek	N 10 - E
	G Signin with Roopie	
	Sign in	
	to continue to födema.com	
	Pargal anuli? Orada actour i NEXT	
	Higher (Helm Statist) - Higher (Helm Statistics)	

- 3. Did you successfully redirect to the Google?
- 4. After successful authentication, were you returned to the app.f5demo.com?
- 5. Did you successfully pass your OAuth Token?

Host     app.f5demo.com       User-Agent     Mozilla 5 0 (X11 Ubunity: Linux x86 -64; v/s6.0 (Userco2010011 Finetox56.0       Accept     Moxilhmit Application/Xhtmit xml, application xmxq.co.2/7.ep.0.8       Accept-Language     en-US.emq-0.5       Accept-Encoding     gz.p.6 delta.br       Referer     https://app.f5demo.com/admin/       Cookie     LastMHT_Sassion-07337676; r5_ST-11 z1 s2623065z04600       DNT     1       Connection     keap-alve       Upgrade-Insecure-Requests     1       AuthTyperhotEmail     eistery chas@gmail.com       OAuthUserhotEmail     eistery chas@gmail.com       OAuthUserhotEmail     costery	User-Agent     Mozilia & Q.K11: Ubunku: Linux x80. 64; vrs60. 00 dexe02010101 Filterox/s6.0       Accept     Moxthimi application/xhtmi +xmil application /xmix_10.06; r/p.40.8       Accept Language     nru US, gr.p.40.8       Accept Encoding     gzp, deflata, br       Referer     hbit X-gr.gp.64m       Cookie     Estimation Z25376; FS_ST-iz1z1z1528259965x604000       DNT     1       Connection     keep-allive       Upgrade-Inscure-Requests     1       Auth Type     outh       OAuthUserinfbeTiuliName     Chas Lestey					
User-Agent     Mozilia5 0 (A11) Ubunity Linux 806 (94; http://www.setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/obs/setabulity.com/o	User-Agent     Mozilla 50 (X1 1; Ubuntu Linux x80, 64; vr.56.0) Gekolo20100101 Firefox56.0       Accept     Moxilla Application:Xhm xml, application Xml; a-0.3, "r; a-0.3       Accept-Language     en U-U-Serry-Based       accept-Encoding     pzp, deflate, br       Referrer     https://spp.15demo.com/admin/       Cookie     IFS, ST=1 x1 x1 x1 52825985z604800       DNT     1       Connection     keep-allive       Upgnde-Inseure-Requests     1       AuthType     oauth       OAuthUserintoErual     selsy_chas@gmail.com       OAuthUserintoErual     felsey_chas@gmail.com       OAuthUserintoErual     Chas Leeley       OAuthUserintoErual     Chas Leeley					
Oservignin     \v>5.0.0     Gacka20100111     Findoux50.0       Accept     bx/th/thm/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/hith/thm/application/h	Valer Augenti     v/s6.0) Gecko 2010 01 01 Firefox/56.0       Accept     sn/thm/se0.9/*g-a0.8       Accept-Language     sn/Us nng-a0.5       Accept-Language     ssion-admin/       Cookie     F.5. ST-12 x1 z1 x152825995x70e*: F.5. ST-12 x1 z1 x152825995x604800       DNT     1       Connection     keup-alive       Upgrade-Insecure-Requests     1       AuthType     outh       OAuthUserintbErnali     leslay/chas@gmail.com       DAuthUserintbGreenName     Chas Lesley	Host	app.f5demo.com	-1		
Accept     ymlq_a0_0,"yq_a0_8       Accept_Encoding     gzip, deflate, br       Accept_Encoding     gzip, deflate, br       Referer     https://app.56mos.com/sadmin/       Cookie     Fs_ST=trtzts2659905z604800       DNT     1       Connection     keep-alve       Upgrade-Insecure Requests     1       Auft1Ype     pault       Could Learning     leasely_chas@gmail.com       Could Learning     hasiey_chas@gmail.com	Accept Language     en-US gr.nd-0.5       Accept Language     en-US gr.nd-0.5       Accept Language     gr.p. deflate, br       Referer     https://app.15demo.com/mdmin/       Referer     https://app.15demo.com/mdmin/       Cookie     FS_ST=1212121528259865x604800       DNT     1       Connection     keap-alive       Upgrade-insecure-Requests     1       AuthType     outh       OAuthUserintbErnall     festery chas@gmail.com       DAuthUserintbGreniName     Chas Lestey       OAuthUserintbGreniName     Chas Lestey	User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0	i i i		
AcceptEncoding         [pip, deflate, br           Referer         [https://app.55demo.com/admin//           Cockle         [s.5]/7576;           Cockle         [s.5]/7576;           DNT         1           Connection         [keep-alive           Upgrade-Insecure-Requests         1           AufhType         [oauth]           OutmUser/InfoEmail         [selsey, chas@gmail.com]           OutmUser/InfoEmail         [celsey]	Accept-Encoding     gzip, defitate, br       Referer     https://app.f5demo.com/admin/       Cookie     Instructure       DNT     fi       Connection     kesp-alive       Upgnde-Inseure-Requests     fi       AuthType     outh       OAuthUserIntoErmail     festery.chas@ymail.com       OAuthUserIntoErmail     festery.chas@ymail.com       OAuthUserIntoErmail     Chas Lesley       OAuthUserIntoErwanne     Chas Lesley	Accept		i i i		
Referer     Intps://app.t5demo.com/admin/       Cookie     LastMH-Session-0753767e; F5_ST=trtx1s2825995z604900       DNT     F       Connaction     keep-allve       Upgrade-Insecure-Requests     1       AuthType     oauth       OAuthUserthoFullName     ChasLestey	Indexeer         Index/NPL           Cookie         LasMMH_sesion-007337676;           FS_ST=1 x1 x1 x1562839965x04800           DNT         1           Connection         Keep-all/ve           Upgrade-Insecure-Requests         1           AuthType         pouth           QAuthUserIntErmail         leeley_chas@gmail.com           QAuthUserIntErmail         Chas Leeley	Accept-Language	en-US,en;q=0.5	-		
Cookie         LastMH1-Session-0753767e; F5_ST=121215282599652604000           DNT         1           Connection         keep-alive           Upgrade-Insecure-Requests         1           AuthType         oauth           OAtuItUsertinforElitiame         Fesley.chas.0ggmail.com           OAtuItUsertinforElitiame         Chas.Lestey	Cookie         LastMH-L Session-075376'e; P5_ST=iztatz1528259965x604800           DNT         1           Connection         Keep-allive           Upgrade-Insecure-Requests         1           AuthType         Gouth           OAuthUserIntoErunil         Keeley           OAuthUserIntoErunilace         Chas Leeley	Accept-Encoding	gzip, deflate, br	-		
Ubbit         F5_ST=121z1z1528259865z604800           DNT         1           Connection         Keep-alive           Upgrade-Insecure-Requests         1           AumTrype         oauth           OAumUserInfoEmail         Kesky-zhas@gmail.com           OAuthUserInfoEmail         Kesky-zhas@gmail.com	Lodoe (FS_ST=121t21t282829985x604800) DNT (1 Connection keep-alive Upgrade-Insecure-Requests 1 AuthType outh AuthType outh OAuthLeartingErmil lestery chas@ymail.com DAuthUserringErwinRame Chas Lestery OAuthUserringErwinRame Chas Lestery	Referer	https://app.f5demo.com/admin/			
Connection     keep-alive       Upgnde-Insecure-Requests     1       AuthType     oauth       OAuthUserInfoEmail     lesisy_chas@gmail.com       OAuthUserInfoFullName     Chas Lesiey	Gonnection     keep-alive       Upgnde-Inseure-Requests     1       AuftType     outh       OAuthUserIntDE-mail     estey.chas@ymail.com       OAuthUserIntDE-Willname     Chas Lestey       OAuthUserIntDE/Winame     Chas	Cookie		i i i i i i i i i i i i i i i i i i i		
Upgrade-Insecure-Requests     1       Auft/Type     oauth       OAuft/UserIntloEmail     Issiey.chas@gmail.com       OAuftUserIntDFullName     Chas Lesley	Upgrade-insecure-Requests     1       AufhType     Oauth       OAuthUserInfoEmail     leeky.chas@gmail.com       OAuthUserInfoFullName     Chas Leeley       OAuthUserInfoEvienName     Chas	DNT	1	-		
Auth Type South OAuth UsertholE mail [selsy chas@gmail.com OAuth UsertholE mail [selsy chas@gmail.com OAuth UsertholF utilName Chas Lesley	AuthType     oauth       OAuthUserInfoEmail     lesley.chas@gmail.com       OAuthUserInfoEulName     Chas Lesley       OAuthUserInfoEilVenName     Chas	Connection	keep-alive	-		
OAuhUserInioEmail         [esley.chas@gmail.com           OAuhUserInioFullName         Chas.Lesley	OAuthUserhibEmail     Iselay chas@gmail.com       OAuthUserhibEuliName     Chas Lealey       OAuthUserhibEvenName     Chas	Upgrade-Insecure-Requests		-		
OAuthUserInfoFullName Chas Lesley	OAuthUserIntoFullName Chas Lesley OAuthUserIntoGivenName Chas	AuthType	oauth	-		
	OAuthUserInfoGivenName Chas	OAuthUserInfoEmail	lesley.chas@gmail.com	-		
OAuthUserInfoGivenName Chas		OAuthUserInfoFullName	Chas Lesley			
	OAuthUserInfoFamilyName Lesley	OAuthUserInfoGivenName	Chas			
OAuthUserInfoFamilyName Lesley		OAuthUserInfoFamilyName	Lesley	-		
OAuthissuer https://Waccounts.google.com	OAuthissuer https://Waccounts.google.com	OAuthIssuer	https:///vaccounts.google.com			
		OAuthTokenType	Bearer			
	OAuthissuer https://Waccounts.google.com	OAuthUserInfoGivenName OAuthUserInfoFamilyName	Chas Lesley	-		
		OAuthTokenType	Bearer			

### **TASK 7: Per Request Policy Controls**

EMO APPLICATION		
Host	app.f5demo.com	
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; nr:56.0) Geoko/20100101 Firefox/56.0	
Accept	texthtml.application/khtml+xml,application /xml;g+0.9,*/*;g+0.8	
Accept-Language	en-US,en;q=0.5	
Accept-Encoding	gzip, deflate, br	
Referer	https://app./5demo.com/admin/	
Capitie	LastMRH_Session=0753767e; F5_ST=1z1z1z1528259965z604800	
DNT	1	
Cannection	keep-alive	
Upgrade-Insecure-Requests	1	
AuthType	oauth	
OAuthUserInfoEmail	lesley.chas@gmail.com	
OAuthUserInfoFullName	Chas Lesley	
OAuthUserInfoGivenName	Chas	
OAuthUserInfoFamilyName	Losioy	
OAuthissuer	https:////accounts.google.com	
OAuthTokenType	Bearer	

- 2. You will receive an Access to this page is blocked (customizable) message with a reference. You have been blocked because you do not have access on a per request basis.
- 3. Press the **Back** button in your browser to return to **https://app.f5demo.com**.



- 4. Navigate to Local Traffic -> iRules -> Datagroup List and click on the Allowed_Users datagroup.
- 5. Enter your Google Account used for this lab as the String value.
- 6. Click Add then Click Update.

Note: We are using a DataGroup control to minimize lab resources and steps. AD or LDAP Group memberships, Session variables, other user attributes and various other access control mechanisms can be used to achieve similar results.

Main Help About	Local Traffic >> iRules:	Data Group List -> Allowed_Users
Statistics	Properties	
J iApps	General Properties	
🔁 Wizards	Name	Allowed_Users
DNS	Partition / Path	Common
5 DNS	Type	String
Docal Traffic	Records	
Network Map		String: your@email.com
Virtual Servers		
Policies		Add Sdemo.com
Profiles		user2@f5demo.com
Ciphers	String Records	
iRules		
Pools		
Nodes		Edit Delete Record
Monitors ()		Los Lessie Hecord
Traffic Class 💿	Update Delete Da	a Group
Address Translation		

7. You should now be able to successfully to access the Admin Functions by clicking on the **Admin Link**.

Note: Per Request Policies are dynamic and do not require the same "Apply Policy" action as Per Session Policies.





9. The various Per-Request-Policy actions can be rev Note: Other actions like Step-Up Auth controls can be pe	
6	
Per-Request Policy: /Common/Google_oauth_policy Edit Endings (Endings: Allow, Reject [default])	
$\begin{array}{c} \textbf{Start} \end{array} \overset{\text{fallback}}{\underset{\text{fallback}}{\text{fallback}}} \ast - \underbrace{\textbf{ITTP Headers}}^{2} \overset{\text{fallback}}{\underset{\text{fallback}}{\text{fallback}}} \ast \rightarrow \underbrace{\textbf{Admin}}_{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{X}}{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{Admin Allowed}}{\underset{\text{fallback}}{\text{fallback}}} \ast \rightarrow \underbrace{\textbf{Admin}}_{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{X}}{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{Admin Allowed}}{\underset{\text{fallback}}{\text{fallback}}} \ast \rightarrow \underbrace{\textbf{Admin}}_{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{X}}{\underset{\text{fallback}}{\text{fallback}}} \overset{\text{X}}{\text{$	
Add New Macro	
Add New Subroutine Add New Subroutine Macro	

#### **TASK 8: Review OAuth Results**

- 1. Review your Active Sessions (Access -> Overview -> Active Sessions). 2. You can review Session activity or session variable from this window or kill the selected Session. Display Options And Refeed w second Destinat Refresh Seasten Table Intel Artise: Second Active Season Count Search Version Status • Season D Version • Vers • Cleat P • Velual Screen Skat Time 2010-05-00 17:06:56 G Solution Konmon/spp./ficierro.com View a) 0.1100.1
- 3. Review your Access Report Logs (Access -> Overview -> Access Reports).

Report Parameters
This report shows summary of all sections in the Kalabase , its which by These
Facert M 1 📩 Tour m
Na Argoni Con al

4. In the Report Parameters window click Run Report.

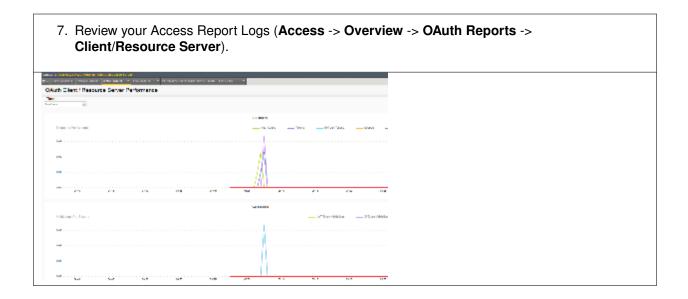
$\overline{\mathbf{P}}$	- 71	All Services II									
		Part of States of States									
4	1.	Show with the	la 🔯 Birel	Process Phylo		Rever Constant of Str.	Bellin Selection	seed Dames	the local sequences	and follows	
		Load Tree	Annies D	Lager	<b>heles</b>	Annual Installation	Size .	Country	Castron	Vision #	Class P.
6. P.	The second	2010/09/10 17:00	beloff to		× .	View Reader: Vielages				72.10.10	112.10.10
1 + 1	1 +										
-	1.			<b>.</b>							

5. Look at the SessionID report by clicking the Session ID Link.

6. Look at the **Session Variables** report by clicking the **View Session Variables** link. Pay attention to the OAuth Variables.

Note: Any of these session variables can be used to perform further actions to improve security or constrain access with logic in the Per-Session or Per Request VPE policies or iRules/iRulesLX.

And			
Statement President		consistent of share and share a	
Back Banks	Witness 7 Andre Catallan Cadalitie 7		
Anota al	Parales Terra	Waterland	Name & W
states 2	• Manuali		and a party
A front The	- 3 Jan		and a such that
	ومراهدات المعرب برياد الأربخو مكانت مسكرتها		وجراحة والمحراص لطائر باوحاك محداثا مطرعا فالمحاص
A franks	Colore and Starging Series		webs with the Researchingto Jame
No feature desired			THE STATE OF A REAL OF
OWNERS AND N	a Conservation		weight a set of set of the back in
de la seconda	E and	and a second	content and a second state in small
allowed and the first of the low of	C molt-railes	ter .	control provide a low text that is preadily realized
	The layers	initian and a second seco	control provide plane have been been been been been been been be
Hund You 24 Eaders	The second s		makes pack that he finds is partic
AND A VERY CARE A	Strangener	Tolean .	and a part of the last had being the group.
Read Pro (Blowne)	12 Look	**	water such that he finds is inclu-
Contraction many	E New	*******	stream parts that the Back is torta-
aptical cold field as	E have	The first is the second sec	and the state of the state of the state
Burner Banklum			
Bran Carlotter and			
i unad man	2 54/8	the strate of programmer and the strategy of the	Which have been been as an an and
	11 M	THE RECEIPTION OF THE RECEIPTI	CONTRACTOR OF A DESCRIPTION OF A DESCRIP
A CARGO A	Commission and		AND ADDRESS OF THE ADDRESS OF THE
Alternative (second second sec	DWINE	A REAL PROPERTY AND A REAL	
Burner, Warley Stranger		production desceptory Weddell and provide a provider and	
Aren Peuge		PART SPECIES AND PROVIDED AND ADDRESS OF	
No. of Acapa	Electrical and		sense have the sense of sense
A state has to	El ann		AND A DAME TO BE AND ADDRESS OF ADDRESS OF ADDRESS OF ADDRESS
diam'r.	Eleven and a second sec		AND A DAY OF BUILDING AND A
Build Barriel as Sectors	Exemple 1	1977	THE ALL MADE IN THE REPORT OF A
	A COMPANY AND A COMPANY		contract with a second state of the
GRADMA	The second se	48.041	content a work of an Arc Ac Adventise
Taxa di takan	1 Aug 1	- 1994 ( 10-00 ph/000 Ph/00	water parts that has highly been dealer
10 ALC: 198 199 2	(Teal)	MP IP IP IP IP I A CONTRACT A CONTRACT OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A	and a start of the last to be a start of the start
Review Sectority			



# 6.5 Lab 4: oAuth and AzureAD Lab

The purpose of this lab is to familiarize the Student with the using APM in conjunction with Microsoft Azure AD. Microsoft Active Directory Domain Services is offered by Microsoft Azure as a cloud service. This can be used together with OpenID to log in to APM.

# 6.5.1 Objective:

- · Gain an understanding of additional F5 OAuth features
- Deploy a working configuration using F5 APM and Microsoft Azure AD

# 6.5.2 Lab Requirements:

- All lab requirements will be noted in the tasks that follow
- · Estimated completion time: 25 minutes

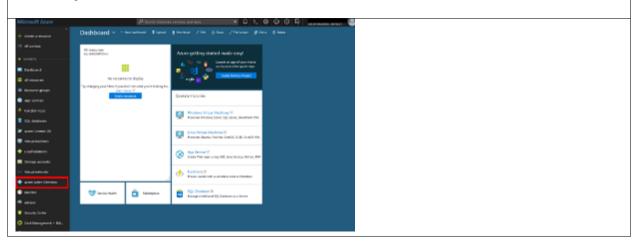
# 6.5.3 Lab 4 Tasks:

### TASK 1: Create/Review New Application Registration

Refer to the instructions and screen shots below:

Note: The following steps in this task can just be "REVIEWED". As setting up a free Azure account requires the entry of billing information, setting up an account and performing the steps below is a [REVIEW] task. For those desiring to set up an account refer to the "APPENDIX: Setting up an Azure Development Account". For those with existing accounts these steps may be followed if desired. For all others, simply review the steps in Task1 and proceed to Task 2.

1. Log into the Microsoft Azure Dashboard and click **Azure Active Directory** in the left navigation menu.



## [REVIEW]

2. Click on App Registration on the resulting menu and then New Application Registration on the flyout menu.

Manual Asar		Plantoneous artists white P A 1	6.0	
	Million and Mark Server			
12 Marchae	(X more a	The sphoto-sphoto-all blands & Troches.	_	
	Distance 15	To rise and manageptic appliedness for inner participations, places with the Record' Application Second		
<ul> <li>modeled</li> </ul>	al bolies	Tendris wave adapt		
	1000	New York Company of Co		
	4 mm	Taxa sama surviva, aplicators toris dances.		
🔹 agg Senatas	4 Inst	Then of gaph sizes		
	<ul> <li>Interior opticities</li> </ul>			
Signature	E Total			
	<ol> <li>Appropriate</li> </ol>			
Final mating	<ul> <li>taristerray</li> </ul>			
🗢 Last Malazaris	d term			
E Despensionite	konkting			
	2 holy 104 edite			
<ul> <li>Aller Active Sectors</li> </ul>	1 Insection			
<ul> <li>Market</li> </ul>	Inquestion of the			
🔹 uttar	• neutrop			
	If fragmin			
Costdesigness + Mil.	Reflective allege			
a maint second	10471			

- 3. In the pop menu for Create App Registration, enter the following values
- Name: app.f5demo.com
- Application Type: Web App /API
- Sign On URL: https://app.f5demo.com
- 4. Click Create.

Microsoft /	Azure				
		Home 3 Bloke www.			nations > Create
+ Create a re	source	Create	•	×	
E All services		* Name O			
+ ENVORITES -		app.f5demo.com	~		
🔲 Dashboard		Application type <b>0</b> Web app / API	~		
II resource	5	* Sign-on URL @ https://app/5demo.com	m 🗸		
😰 Resource g	roups	mips//approventicou	··· ·		
🔕 App Service	8				

- 5. In the resulting **app.f5demo.com Registered App** window, note & copy the **Application ID**. This will be used in a later setup step
- 6. Click Settings.

1	Aicrosoft Azure			
		<ul> <li>Hone &gt; Measurement (data.</li> </ul>	uit directory) - App registrations () app./Sdamo.com	
-	- Create a resource	app födemo.com Figurant igs		* • ×
Ξ	All services	🖨 Settings 🖌 Manifest	Colota	
	ENVORITES	Display norms, app fodemo.com	Application ID Physical action 129	
	Cashboard	Application type Web app / API Home page	Object ID • Object ID • Managed application in local direc	
:	All resources	Https://epp.f5dema.com	арр. Бестколого Э	.,
8	Resource groups			
•	App Services			
4	Function Apps			
	SQL databases			

[REVIEW]					
<ol><li>In the Settings f</li></ol>	lyout panel clic	ck Kevs			
	iyour parioi, oik				
Home > Robberdowsco (default directory) - App registration					
app.15demo.com	* ×	Settings		£	
Satings / Manifest B Delete		D Film utiling:			
Display name Application 1					
	Application (its	SENDRAL			
Application type Object ID Web app / API	e Calport I Ca	😥 Proportios	>		
Home page Managed ap https://app.f5demo.com app.f5demo.	plication in local directory	E Reply URLs	~		
×			<u></u>		
		🝰 Owners	>		
		#P1 400035			
		A Required permissions	>		
		📍 Keys	>		
			_		
		TROUBLISHOOTING - SUPPORT			
		X Troublesheet	>		
		New support request	>		
		-	-		

- 8. In the Keys flyout panel, enter the following values
  Description: app.f5demo.com
  Expires: In 2 Years
- 9. Click Save.

Keys		
Sove X Discard	Upload Public Key	
Passwords		
DESCRIPTION	EXCPLICAS.	VALUE
	V In 2 years	Value will be displayed on save
Key description	Duration V	Value will be displayed on save

10. Note the message provided by Azure in the Keys panel.         11. Copy the *Key Value* for use in a later setup step.         Keys         If Sees       X Deced         Y Deced       Typeed Public Key         A Copy the key value. You wont be able to retrieve after you kerve this black.         Passwords         BOOMPTON       KHIK
11. Copy the *Key Value* for use in a later setup step.         Keys         If Sere X Decerd Tuplead Public Key         Image: Copy the key value. You won't be able to retrieve after you leave this black.         Passwords         BOORPTION       VALUE
Image: Series       X Discard       The Upload Public Key         Image: Copy the key value. You won't be able to notifieve after you leave this blade.         Passwords         BISORPTION       CARRUS
Image: Series       X Discard       The Upload Public Key         Image: Copy the key value. You won't be able to notifieve after you leave this blade.         Passwords         BISORPTION       CARRUS
Copy the key value. You won't be able to native after you leave this blade. Passwords escommon permits value
Passwords elsowmon defaits value
DESCRIPTION DEPRES VALUE
app.5demo.com 64/2023 <ney.valan< th=""></ney.valan<>
Ray description Volume will be displayed on save
Public Keys
THURBERENT START DATE DOPERS

12. In the Settings flyout panel, click Reply URL.

-			
app.Edemo.com Replaced ap	* ×	Settings	
🗘 Settinge 🖌 Manifest 🛛 B. Dalets		,0 filmentinge	
Onplay name app.Edemo.com	Application ID supplication IDs	CININA.	
Application type With opp / API	Object ID <object id=""></object>	III Properties	>
Harne page https://app:f5demo.com	Managed application in local directory app./56eme.com	😑 Reply 184	>
	9	al Owners	$\rightarrow$
		AR 40000	
		🚠 Required provincions	$\rightarrow$
		9 Keye	>
		TAQUELING CTURE - IMPORT	
		X Instituted	<u> </u>
			~
		New support request	>

#### [REVIEW]

- 13. In the **Reply URL** flyout panel, enter https://app.f5demo.com/oauth/client/redirect
- 14. Click Save.

Reply URLs	
 Save X Discard	
https://app.15demo.com	
https://app.f5demo.com/oauth/client/redirect	

- 15. In the Settings flyout panel, click Required Permissions
- 16. In the Required Permissions flyout panel, click Grant Permissions



[REVIEW] 17. The following Required Permissions dialogu 18. Click Yes to proceed.	ie box may appear.
Required permissions ×	
Add Grant permissions	
Do you want to grant the permissions below for app./5demo.com for all accounts in current directory? This action will update any existing permissions this application already has to match what is listed below.	
Yes No	

- In the Required Permissions flyout panel, click Windows Azure Active Directory.
   In the Enable Access flyout panel, ensure the Sign In and Read User Profile.
- permission is checked.
- 21. Click Save.

Required permissions	×	Enable Access window load Access	
Not Companialars		E See Own	
	APROPERTURE: RECARD TOMO.	WTLEMENT FORMERED	1.0000
Mindows Room Active Directory	0 5	<ul> <li>Red directory dela</li> </ul>	e na
		Read and write domains	<b>0</b> fm
		Read and write directory data	0 Ni
		Read and write desires	0 m
		Red # Nddenmendenhips	• %
		Manage appricht (Na app artains ar artes.	0 m
		Read and write all applications	• ha
		Read and write down ins	0 fw
			1 No.44
		descent the discription for signal in any	4 km
		Red dradog data	0 Ni
		Read and write directory data	0 fm
		Read and write all provati	• Ni
		Read of groups	0 m
		Red et seec fui profile	• %
		Read of annex lineits profiles.	• 10
		Significant read and profile	👄 Mo

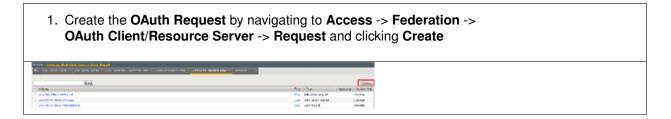
- 22. In the Registered Application panel, click Manifest.
- 23. In the **Edit Manifest** flyout panel, edit the **groupMembershipClaims** line (line 7) from **null** to "**All**" (note quotes are required).
- 24. Click Save.

Note: You can also update groupMembershipClaims to be "SecurityGroup".

agen Pachenni a com Nacional ant	N bi evadesi
Brann Provensky Andread Strand Province Harrison (1997) Harrison (1997) Harris	Rev X best X to The set & these           Image: The set of the set & these is the set of the

#### **TASK 2: Create OAuth Request**

Refer to the instructions and screen shots below:



- 2. Use the following values to create the Request
- Name: Azure_AD_Token
- HTTP Method: POST
- Type: token-request
- 3. Create the following Request Parameters using the Parameter Type drop down:
- Parameter Type: client-id
- Parameter Name: client_id (notice _ )
- Parameter Type: client-secret
- Parameter Name: client_secret (notice _ )
- Parameter Type: grant-type
- Parameter Name: grant_type (notice _ )
- Parameter Type: redirect-uri
- Parameter Name: redirect_uri (notice _ )
- Parameter Type: custom
- Parameter Name: resource
- Parameter Value: dd4bc4c7-2e90-41c9-9c41-b7eab5ab68b7
- 4. Click Finished.

Name	Azure_AD_Token
escription	
quest Settings	
(TTP Nethod	POST -
)pe	token-request
lequest Parameters	Parameter Type: custom Parameter Name: Parameter Name: Add Add Clent_id Clent_id Clent_id Clent_secret grant-type redired-uni custom   redured; uni Custom   reduced; Uni Custom
lequest Headers	Header Name: Header Value: Add

#### **TASK 3: Create OAuth Provider**

Refer to the instructions and screen shots below:

<ol> <li>Create the OAuth Provider by navigating to Access -&gt; Federation -&gt; OAuth Client/Resource Server -&gt; Provider and clicking Create.</li> </ol>					
		Bent i Tesecaro Server : Provider Edili, cando Provider V Edili, Des	ources	sian = Orioth Au	character Tener * Dilan Clart Fiscaure Care * Prophysion *
				CHER	
v chare	+ Type	<ul> <li>Use Auto-discovered JNC</li> </ul>	OAsth Gener	· Patition	
E AcureA0	Asys40	false .		Cennon	
11 M	18	latur		Centres	
E Facebook	Facebook	latur		Cennen	
T1 Geogle	Coogle	Refease .		Cennes	
E Obs	Otto	Nov		Cennes	
E Pro	Fing	tatuw		Cennen	

- 2. Use the following values to create the Request
- Name: f5demo_AzureAD_Provider
- Type: AzureAD
- OpenID URI: (replace _tennantID_ with the following tenantID f5agilitydemogmail.onmicrosoft.com )

Resulting URI should be as follows:

https://login.windows.net/f5agilitydemogmail.onmicrosoft.com/.well-known/openid-configuration

- 3. Click **Discover**.
- 4. Click Save.

Note: if using another account you can find you TenantID by navigating to the "Azure Portal" and clicking "Azure Active Directory". The tenant ID is the "default directory" as shown. The full name of the TenantID will be your "TenantID.onmicrosoft.com"

Access >> Federation : OA	uth Client / Resource S	kerver : Pr	ovider »	New		
Seneral Properties						
Name	15deme_AzureAD_Pro	ovider				
Description						
Туре	AzureAD -	_				
	10201010 V					
Ignore Expired Certificate Validation						
Trusted Certificate Authorities	ca-bundle.ort				•	
Allow Self-Signed JWK Config Certificate	2 💌					
Use Auto-discovered JWT	<b>V</b>					
OpenID URI	https://ogin.windows Last discovery time: 20			lonmicr	caoft.com/.well-know	Discover
Authentication URI	https://login.windows.net/219901d7-173a-4a71-aab6-2901606eb554/oau					
Teken URI	https://ogin.windows.net/219931d7-173a-4s71-aab6-2901966eb554/oau					
Token Validation Scope URI						1
	Alles desire and desire		at 171- 1			1
Userinto Request URI	https://ogin.windows					
bsuer .	https://sts.windows.n	ww219901d	7-173a-4a)	71-aab6	-2901060eb554/	
Signing Algorithm	Allowed			Bio	cked	
	R5256		•			• 
Key (JWK)	Allowed			Bło	oked	
	RSA 2545CVGx85g RSA BJL1Rozzhy4fj RSA:TioOywwhvdF	pxbxdZqohl	4			* •
Cancel Save						
licrosoft Azure				_		
	3 Replicies patient device References al Meta & Area		a árana			
Contraction of the second s	jitydenograal (delault dire					
	(and (lated)	d ^{ar} beitch d	feeloy 🛢 D	enta directo	Ŷ	
	Overview		itydemo		(default direct	(vno
	Ould rait	Asyn HO To		ymali	Caelault directi	ury)
All resources		Sign-ins				
	Even					
	Drangs Enterprise applications				Te sex sign in deta, your argan	vication meets Asure A
	Envices				PE er PE. Start a free trial	
	App registrations					
	Apple alter-proy					
	Litenses		w in Azere AD		mand biog ports.	
	Reure AD Conwect		nor February 15.2			
<ul> <li>Virbal educets</li> </ul>	Custom domain names	E Al sevi	15	(17)	Norfesture	
Annie Adive Deterling	Mobility (MDM and MMM)	0 608/802		00	82C - Concerner Identity Mane	gement - B28/92C
	And colored and the	1.66		an.		

#### TASK 4: Create OAuth Server

Refer to the instructions and screen shots below:

<ol> <li>Create the OAuth Server (Client) by navigating to A OAuth Client/Resource Server -&gt; OAuth Server* a</li> </ol>	
Access - Federation (Otel) Clear Placeana Server, Old Sanaer () - 2003 Networ Preside + 2003 Networ Preside + 2003 Networks, 2003 Web Sale + Shith Advancement Network - Math Carel Heaven Nation - Programmer	
Search         Course           = Name         = Hode         = Poster         = Pastors (Part           = Hinde         = Hode         = Poster         = Pastors (Part           = Brows         =         = Poster         = Pastors (Part	

<ul> <li>Name: f5d</li> <li>Mode: Clie</li> <li>Type: Azu</li> <li>OAuth Pro</li> <li>DNS Reso</li> <li>Client ID: 6</li> <li>Client Sec</li> <li>Client's Sec</li> <li>3. Click Finis</li> </ul>	reAD vider: f5demo_AzureAD_Provider lver: proxy_dns_resolver dd4bc4c7-2e90-41c9-9c41-b7eab5ab68b7 ret: YqHbzTosdBxdaGl9A/hXCs1ex1HWi+BTUSkgcfhbTwA= erver SSL Profile Name: serverssI-insecure-compatible
Name	I5demo_AzureAD_Server
Description	
Mode	Client
Туры	AzureAD
OAuth Provider	f5demo_AzureAD_Provider
DNS Resolver	proxy_dis_resolver
Rules	Selected Avalable           Common         A           APM_Bypass         APM_Coxie_Remove           APM_Coxie_Remove         ASM_Google_reCapitole_v2
Token Validation Interval	60 minutes
Client Settings	
Client Id	dd4bo4c7-2e90-41c9-5o41-b7eab5ab68b7
Client Secret	
Clent's ServerSSL Profile Name	serversel-insecure-compatible
Cancel Repeat Finished	

## TASK 5: Setup F5 Per Session Policy (Access Policy)

Refer to the instructions and screen shots below:

 Create the Per Session Policy by navigating to Access -> Profile/Policies -> Access Profiles (Per Session Policies) and clicking Create.

Access to Problem Phileles Cliccess Phillips (For A	innica Policinį				
C . Acami Palles Pre Experit Palsant Pals	y Ryna Custernization +				
f Seach					Grate Import
🔄 💌 Status in Access Polite Name	* Application + Profile Type, Pe	er-Section Policy Export	Copy Logo	Virtual General	P Patient Path

- 2. In the New Profile dialogue window enter the following values
- Name: AzureAD_OAuth
- Profile Type: All
- Profile Scope: Profile
- Language: English
- 3. Click Finished.

Name Parent Profile Profile Type Profile Scope		AzureAD_OAuth					
		access					
		All	-				
		Profile 💌					
Additional Languages	Afar (aa)	Add		Factory Builds Large ages			
Additional Languages	Afar (aa)	Accepted Languages		e (Simplified) (zh-cn) e (Traditional) (zh-bv) (ko) h (es) (h)	*		

4. Click Edit link on for the AzureAD_OAuth Access Policy				
Actorea sa Freilicea / Asiena / Avelaa				
g - Access Profiles - Pen-Neguest Folices - Pelicy Sync - Casemannos				
form [Samil] [Samil] [Samil]				
2 Strain A Access Politie Same I Application II Prefix Type Pro-Soviem Print, Pound Cours Lago Vision Soviem I Partices Path.				
III 🔰 Attaining_prices At 🗖 Lat. Lippert, Copy, astauting estate				
Lanse. Topole				

- 5. In the AzureAD_OAuth Access Policy, click the "+" between Start & Deny
- 6. Click the Authentication tab in the events window.
- 7. Scroll down and click the radio button for **OAuth Client**.
- 8. Click Add Item.

		_			_
l	6				_
	Access Policy: /Common/AcsumAD_GAuth	[in	in tuning to avaida		9
<u>9</u> .0		Log	Adverturies Arig	neral [Debuter-Security/Security] [Debuter-Security (Sect. Sold] [Debuter-Security]	
	Start Linco	0	R5 MA (ser Verflotten	P5-Wilk that numberoon	
	Add Sam Nacro		HTTP AUD	#719 authentication of end user predentals	
	Add New Race	0	Kalberts Auth	Ketleros authentizatori, typicale following an IETTP-401 Response action	
			USAP Auto	EMP authentication of end user credentals	
	An access policy spreams of a start point, actions, and one or Gain the Add Hanne institut to add a purpose hall set of pre-	0	UDAP Query	134P gamy to put user attributes for use with resource assignment or other functions, such as L34P group maging	1
			Localiti Auto	Local Database Authentication	
	Managers Mound Policy Littler on the Add/London for re-		NTUR Auth Result	NTUN authentication of and user profensials	
	Peace see the <u>Orden Role</u> for more Youri Policy Lifes Same.	0	GAUD Authorisation	6Auth 2.8 Authorization Apent for assoe management.	
		٠	GAUD-Deril	6Auth Dent	
		0	GAUD Scepe	EAuth Sospe	
					-
		Genes	Add Bern		inte
	-				

- 9. In the ***OAuth_Client*** window enter the following values as shown:
- Server: /Common/f5demo_AzureAD_Server
- Grant Type: Authorization code
- OpenID Connect: Enabled
- OpenID Connect Flow Type: Authorization code
- Authentication Redirect Request: /Common/AzureADAuthRedirectRequest
- Token Request: /Common/Azure_AD_Token
- Refresh Token Request: /Common/AzureADTokenRefreshRequest
- OpenID Connect UserInfo Request: None
- Redirection URI: https://%{session.server.network.name}/oauth/client/redirect
- 10. Click Save.

Properties" [Orange Dules]							
Name : Of ath Clent							
04/8							
Server .	/commany/fidewo_AdamaAda_berver						
Grant Tape	Authorization code						
OpenID Connect	Probled						
Open1D Connect New Type	Aufweisster ereb 💌						
Authentication Redirect Request	t /Common/HoursADAuthRedirectRequest 💌						
Token Request	/Common/Roure_AD_Token						
Rafradi Tokon Request	Common / Reunal Dital and Tradition Request w						
OpenED Connect DescEnilo Regi	und None w						
Reloctor UR	High / Major star was water of a same (in a diplotent/method)	ride il					
Nanjer							
Erent Sever Ports in t	tib has been changed, place don't forget to serv()	(Helpe)					

11. Click on the **Deny** link, in the **Select Binding**, select the **Allow** radio button and click **Save**.

Access Policy: /Common/AzureAD_OAuth	It Endings (endings: Allow, Deny (default()	
Surt taback +- OAuth Clent Successful +-air Denz	Select Fording:	
Add New Macro		
	Cancel Save Help	a di seconda

12. Click on the <b>Apply Access Policy</b> link in the top left Note: Additional actions can be taken in the Per Session p is simply completing authorization. Other access controls on the use case.	olicy (Access Policy). The lab
5 Apply Access Policy	
Access Policy: /Common/AzureAD_OAuth EditEndings (Endings Allow, Deny [default])	
Start ) falback +- QAuth Client Successful +	
Add New Macre	

## TASK 6: Associate Access Policy to Virtual Server

Refer to the instructions and screen shots below:

<ol> <li>Navigate to Local Traffic -&gt; Virtual Servers -&gt; Virtual Server List and click on the app.f5demo.com Virtual Server link</li> <li>Scroll to the Access Policy section.</li> </ol>						
Local Traffic » Virtual Servers : Virtual Server List » app.fidemn.com						
🚓 👻 Properties Reso	aces Security 🕶 Statistics 🕑					
General Properties						
Name	app.55dema.com					
Partition / Path	Common					
Description						
Туре	Standard					
Source Address	0.0.0.00					
Destination Address/Mask	10.1.10.100					
Service Port	443 HTTPS .					
Notify Status to Virtual Address	W					
Link	None					
Availability	Unknown (Enabled) The children pool member(s) either don't have service a					
Syncookie Status	or					
State	Labled •					

<ol> <li>Use the Access Profile drop down to change the Access Profile to AzureAD_OAuth.</li> <li>Use the Per-Request Policy drop down to change the Per-Request Policy to AzureAD_oauth_policy.</li> <li>Scroll to the bottom of the Virtual Server configuration and click Update.</li> </ol>
Access Policy
Access Profile AzureAD_OAuth
Connectivity Profile + None -
Per-Request Policy AzureAD_oauth_policy

## TASK 7: Test app.f5demo.com

Refer to the instructions and screen shots below:

1. Navigate in your provided brow	wser to https://app.f5demo.com	
Charlestown y X	w   T   22	
← → C ^a Q. https://postGeens.com	9, Secon 🗴 🕼 🖸 🛩 =	

٦

	demouser@f5a	ng AzureAD account: agilitydemogmail.on		
Burger by sale of the weathing of the line. No. 10, No. Ander Sec. No.	No. of Concession, Name			
-				
The state of the s	E Manuf	11		
R Barris	Sign in Frank prove Star			
and the second s	Leading of the	the shall		
A STATE OF STATE	Country Pressioner	and the states		
		ALL BURGER	to de-	

Г

- 3. Did you successfully redirect to the AzureAD?4. After successful authentication, were you returned to the app.f5demo.com?5. Did you successfully pass your OAuth Token?

Host	app.f5demo.com
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept	text/html,application/xhtml+xml,application /xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate, br
Referer	https://app.f5demo.com/admin/
Cookie	LastMRH_Session=e2cc5bf0; F5_ST=1z1z1z1528266325z604800
DNT	1
Connection	keep-alive
Upgrade-Insecure-Requests	1
AuthType	oauth
OAuthTokenUniqueName	demouser@f5agilitydemogmail.onmicrosoft.co m
OAuthTokenName	Demo User
OAuthissuer	https:////sts.windows.net///2f9931d7-173a- 4a71-aab6-290f666eb554//
OAuthTokenType	Bearer

#### **TASK 8: Per Request Policy Controls**

Refer to the instructions and screen shots below:

ED INFORMATION		
Host	app./5demo.com	
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0	
Accept	text html,application/xhtml+xml,application /xml;g=0.9,*/*;g=0.8	
Accept-Language	en-US,en;q=0.5	
Accept-Encoding	gzip, deflate, br	
Referer	https://app.f5demo.com/admin/	
Cocilia	LastMRH_Session=e2cc5bl0; F5_ST=12121215282663252604800	
DNT	1	
Connection	keep-alive	
Upgrade-Insecure-Requests	1	
AuthType	oauth	
OAuthTokenUniqueName	demouser@f5agilitydemogmail.onmicrosoft.co m	
OAuthTokenName	Demo User	
OAuthIssuer	https://///sts.windows.net///2/9931d7-173a- 4a71-aab6-290/666eb554\//	
OAuthTokenType	Bearer	

- 2. You will receive an **Access to this page is blocked** (customizable) message with a reference. You have been blocked because you do not have access on a per request basis.
- 3. Press the **Back** button in your browser to return to https://app.f5demo.com.

<b>f</b> 5	
-	
Access to this page is blocked.	
Access was denied by a per-request policy.	
The session reference number: 0753767e	
The category reference is: Uncategorized	_
This product is licensed from F5 Networks. © 1999-2017 F5 Networks. All rights reserved.	

- 4. Navigate to Local Traffic -> iRules -> Datagroup List and click on the Allowed_Users datagroup.
- 5. Enter your **demouser@f5agilitydemogmail.onmicrosoft.com** used for this lab as the **String** value.
- 6. Click **Add** then Click **Update**.

Note: We are using a DataGroup control to minimize lab resources and steps. AD or LDAP Group memberships, Session variables, other user attributes and various other access control mechanisms can be used to achieve similar results.

C	ONLINE (ACTIVE) Standalone	)		
Main Help About Statistics		Local Traffic IRules : Data Group List Allowed_Users		
			🔅 🗸 Properties	
			General Properties	
🗿 w	izards		Name	Allowed_Users
5 DI	10		Partition / Path	Common
<b>D</b> DI	15		Type	String
il La	cal Traffic		Records	
	Network Map			String: your@email.com
	Virtual Servers			
	Policies			Add 5demo.com
	Profiles			user2@f5demo.com
	Ciphers		String Records	
	iRules			
	Pools			
	Nodes			
	Monitors			Edit Delete Record
	Traffic Class		Update Delete Data G	roup
	Address Translation			
		_		

7. You should now be able to successfully to access the Admin Functions by clicking on the Admin Link.

Note: Per Request Policies are dynamic and do not require the same "Apply Policy" action as Per Session Policies.



8. To review the Per Request Policy, navigate to *Access -> Profiles/Policies -> Per Request Policies and click on the Edit link for the AzureAD_oauth_policy.

Standalone						
Main Help About	Access Profiles / Policies : Per-Request Policies					
Statistics	Access Profiles Per-Request Policies Policy Sync Customization +					
IApps	• Search				Creat	e Impor
Wizards	Per-Request Policy Name	Per-Request Policy	Export	Сору	Virtual Servers	Partition /
5 DNS	AzureAD_oauth_policy	🗖 Edit.	Export	Copy.	app.f5demo.com	Common
Local Traffic	Google_oauth_policy	Edt	Export	Copy.		Common
	sami_policy	🕫 Edt	Export	Copy.		Common
Traffic Intelligence	Delete					
Acceleration						
Access						
Overview						
Profiles / Policies						
Authentication						

9. The various Per-Request-Policy actions can be reviewed. Note: Other actions like Step-Up Auth controls can be performed in a Per-Request Policy					
fs Hep					
Per-Request Policy: /Common/AzureAD_oauth_policy Edit Endings: Allow, Reject [default])					
Start     fallback     +     Admin Allowed     +       Ittl:     Hunchese     Admin +     Admin Allowed       Ittl:     Hunchese     Admin +     Editors       Admin +     Ittl:     Admin +     Ittl:					
Add New Marro					

#### **TASK 9: Review OAuth Results**

Refer to the instructions and screen shots below:

Review your Active Sessions (Access -> Overview -> Active Sessions).
 You can review Session activity or session variable from this window or kill the selected Session.

Access to Overview Inferior Sensions						
👝 = Advertisestenen - Samer Frysch - Olich Frysch - PHI Frysch - Philippine - Phil						
An Province Transfer E. Reference						
Perinst Stream Links						
Tatal Active Versions						
Aufter Besater Gen 1 1						
<u> </u>						
Image: The Product of the Pr						
O C MARCON MANY ANY LELEVAL Community of Marcola and 2003/03/12/12     O Second Section						

<ol><li>Review your Access Report Logs (Access -&gt; Overview -&gt; Access Reports).</li></ol>					
Report Parameters X					
the report shows commerce of all seveness in the database Fourthalby Tama Report <u>v</u> 1 <u>v</u> Toure <u>v</u>					
Ran Report Cancel					

4. In the Report Parameters window click Run Report.

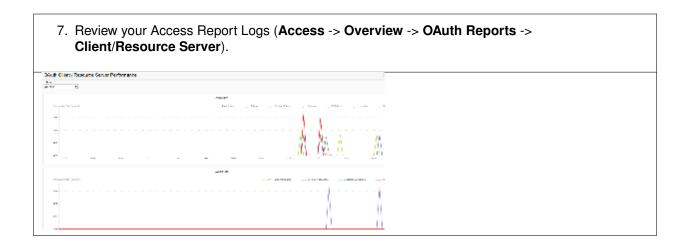
5. Look at the **SessionID** report by clicking the **Session ID** Link.

Andread McMarcaddell, Balan and Yamin Andread Annuella and Annuella and Andread Andread McMarcaddella. Balan and sense and an Annuella and an Annuella and Annuel

6. Look at the **Session Variables** report by clicking the **View Session Variables** link. Pay attention to the OAuth Variables.

Note: Any of these session variables can be used to perform further actions to improve security or constrain access with logic in the Per-Session or Per Request VPE policies or iRules/iRulesLX.

a 😳 seath	
a 😋 olant	
is 👝 Common Paramé C_Chick _ and _ and _ alone _ ag	
> Common/Scienc_AtereAD_Verver	
2 🔐 HC	
🔊 acces tokan	
E anti-addard	Logis and shows and 44 SUBPRESS OF STREET in all series fields and independent of the Sub- tional Street and Subsection (Sub-Sub-Sub-Sub-Sub-Sub-Sub-Sub-Sub-Sub-
	Nutriepostopento.com nutrientitativa en anter 11, PVI 31, Ottenporte publicação eman
Z autoradi	,
E winks	
E empires in	0600
Complete An	1000000000
😴 ent_mples_te.	0
# 🚖 4_3261	
22 alt	none -
S	part
ST And	distribution 2 Artificial Left And Alexandration Artificial
20 mm	1808000010
20 Hel	16060260740
📰 çərədə	60.100.140.01
2	https://www.endows.net/satis/site/riticae
Si nama	Geing User
S2 ***	1828226743
Contraction	Print ATTRONADON Print 647
20 ora	10VERS > 1010-468-5616-04VSTSIDEVST
2 80	OCKEMeng/190enjnEmisteng/194464La
2014 C	2000/ie7-170a-4a71-aao8-2006866ao85
50 M P	JWT
Contract processing	den en Stegiligden graft som ber



# 6.6 Conclusion

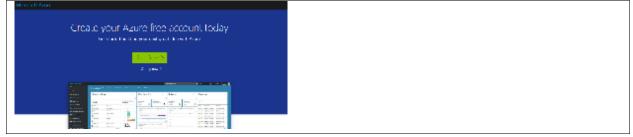
Thank you for your participation in the 330 Access Policy Manager (APM) Federation Lab. This Lab Guide has highlighted several notable features of SAML Federation. It does not attempt to review all F5 APM Federation features and configurations but serves as an introduction to allow the student to further explore the BIG-IP platform and Access Policy Manager (APM), its functions & features.

# 6.7 Appendix

## 6.7.1 Setting up an AzureAD Developer Account

The following steps are for informational purposes only and maybe subject to change based on Microsoft.

- 1. Navigate to the following URL to begin the process then follow the prompts as shown https://azure.microsoft.com/en-us/free/
- 2. The following images show the general flow to setup a free developer account
- Note: This process may change as dictated by Microsoft



3. Initial Setup		
Microsoft Sign in Troll, phone, or Gype Not Cart scene your account Netwoord 10 out and	Microsoft Create account Facilityservel coulizon Facilityservel band Data phone curber baned basis incercent address	
Microsoft Vorify email Unify email State the user work to Country of the series of the	Microsoft Create account Debis proceeding we need to race size a real prices knowing the arcs of a prices knowing the arcs of a need knowing the arcs of a n	-

#### 4. About You

Microsoft Azure	Top takes grant to a state of
Start with a \$210 credit for 30 day	ex and beep going for free
1 About you	
Country/Tropion	
Local Areas	<u>×</u>
Profession 1	
Latt Carte	
Beella Mess 8	
e hone	
Lang-6-40151,4000	
The conduction of the first line course descent	Property of the set
Vet	

Country code United States (+1) Phone number	dentity verification by phone			
United States (+1) Phone number	Country code			
Phone number	United States (+1)	~		
	hone number			

6. Identity Verification by Card	
3 Identity verification by card	
We beap price low by verifying that account holders are real people, not body or anonymous the demonstrate of the array year or at will not be charged a size or profile by one of the a people descent body provided for a temporary will be determined by the size of the si	
VISA 📷 📷 🐃	
Card number	
Explorion date CVV 0	
Nume on card	
Address Inc 1	
Address I on 2	
- Optional -	
C4y	
State ZIP code	

7. Agreement	
Agreement     I agree to the subscription agreement, offer details, privacy statement, and communications     policy     I will receive information, tips, and offers about Azure, including Azure Newsletter and pricing     updates, and other Microsoft products and services. <u>privacy statement</u> Sign up	-

## 6.7.2 Links & Guides

The following are additional resources included for reference and assistance with this lab guide and other APM tasks.

- Access Policy Manager (APM) Operations Guide: https://support.f5.com/content/kb/en-us/ products/big-ip_apm/manuals/product/f5-apm-operations-guide/_jcr_content/pdfAttach/download/ file.res/f5-apm-operations-guide.pdf
- Access Policy Manager (APM) Authentication & Single Sign on Concepts: https://support.f5. com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0.html
- SAML:
  - Introduction: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-sso-13-0-0/28.html#guid-28f26377-6e10-42c9-883a-3ac65eab9092
  - F5 SAML IdP (Identity Provider with Portal): https://support.f5.com/kb/ en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/29.html# guid-42e93e4b-e4fc-4c3d-ae53-910641d5755c
  - F5 SAML IdP (Identity Provider without Portal): https://support.f5.com/kb/ en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/30.html# guid-39ffed07-65f2-40b8-85ae-c80073cc4e82
  - F5 SAML SP (Service Provider): https://support.f5.com/kb/en-us/ products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/31.html# guid-be2cf224-727e-4a0f-aa68-676fdedba37b
  - F5 Federation iApp (Includes o365): https://www.f5.com/pdf/deployment-guides/ saml-idp-saas-dg.pdf
  - F5 o365 Deployment Guide: https://www.f5.com/pdf/deployment-guides/ microsoft-office-365-idp-dg.pdf
- OAuth
  - OAuth Overview: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-sso-13-0-0/35.html#guid-c1b617a7-07b5-4ad6-9b84-29d6ecd789b4
  - OAuth Client & Resource Server: https://support.f5.com/kb/en-us/ products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/36.html# guid-c6db081e-e8ac-454b-84c8-02a1a282a888
  - OAuth Authorization Server: https://support.f5.com/kb/en-us/products/ big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/37.html# guid-be8761c9-5e2f-4ad8-b829-871c7feb2a20
  - Troubleshooting Tips
    - * OAuth Client & Resource Server: https://support.f5.com/kb/en-us/ products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/36.html# guid-774384bc-cf63-469d-a589-1595d0ddfba2
    - * OAuth Authorization Server: https://support.f5.com/kb/en-us/products/ big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/37.html# guid-8b97b512-ec2b-4bfb-a6aa-1af24842ee7a

#### Kerberos

- Kerberos AAA Object: (See Reference section below)
- Kerberos Constrained Delegation: http://www.f5.com/pdf/deployment-guides/ kerberos-constrained-delegation-dg.pdf
- Two-factor Integrations/Guides (Not a complete list)
  - RSA Integration: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-authentication-single-sign-on-12-1-0/6.html#conceptid

#### - DUO Security:

- * https://duo.com/docs/f5bigip
- * https://duo.com/docs/f5bigip-alt
- SafeNet MobilePass: http://www.safenet-inc.com/resources/integration-guide/data-protection/ SafeNet_Authentication_Service/SafeNet_Authentication_Service_RADIUS_Authentication_ on_F5_BIG-IP_APM_Integration_Guide
- Google Authenticator: https://devcentral.f5.com/articles/two-factor-authentication-with-google-authenticator-ar
- Access Policy Manager (APM) Deployment Guides:
  - F5 Deployment Guide for Microsoft Exchange 2010/2013: https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2010-and-2013-big-ip-v11
  - F5 Deployment Guide for Microsoft Exchange 2016: https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2016-big-ip-v11-v12-ltm-apm-afm
  - F5 Deployment Guide for Microsoft SharePoint 2010/2013: https://f5.com/solutions/ deployment-guides/microsoft-sharepoint-2010-and-2013-new-supported-iapp-big-ip-v114-ltm-apm-asm-aam
  - F5 Deployment Guide for Microsoft SharePoint 2016: https://f5.com/solutions/ deployment-guides/microsoft-sharepoint-2016-big-ip-v114-v12-ltm-apm-asm-afm-aam
  - F5 Deployment Guide for Citrix XenApp/XenDesktop: https://f5.com/solutions/ deployment-guides/citrix-xenapp-or-xendesktop-release-candidate-big
  - F5 Deployment Guide for VMWare Horizon View: https://f5.com/solutions/deployment-guides/ vmware-horizon-view-52-53-60-62-70-release-candidate-iapp-big-ip-v11-v12-ltm-apm-afm? tag=VMware
  - F5 Deployment Guide for Microsoft Remote Desktop Gateway Services: <a href="https://f5.com/solutions/deployment-guides/microsoft-remote-desktop-gateway-services-big-ip-v114-ltm-afm-apm">https://f5.com/solutions/deployment-guides/microsoft-remote-desktop-gateway-services-big-ip-v114-ltm-afm-apm</a>
  - F5 Deployment Guide for Active Directory Federated Services: <a href="https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm">https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm</a>

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 Americas: info@f5.com Asia-Pacific: apacinfo@f5.com Europe/Middle East/Africa: emeainfo@f5.com Japan: f5j-info@f5.com ©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.

# **Class 7: Introduction to Universal Access**

#### Welcome to the F5 Identity and Access Management Solutions lab at F5 Agility 2018

The content contained here leverages a full DevOps CI/CD pipeline and is sourced from the GitHub repository at https://github.com/f5devcentral/f5-agility-labs-iam. Bugs and Requests for enhancements can be made by opening an Issue within the repository.

This class will cover APM concepts and will guide students through configuration steps for the following common use cases:

- Remote access VPN services
- Web portals (Webtops) for publishing internal applications
- · Using different authentication protocols
- · Single-Sign-On (SSO) functionality

# 7.1 Lab Information

#### 7.1.1 Login instructions

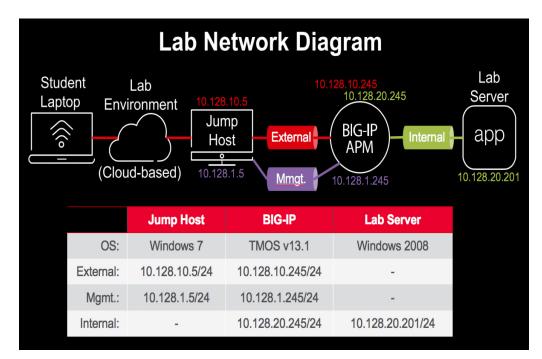
Please follow the instructions provided by the instructor to start your lab and access your jump host.

To access your dedicated student lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces (HTTPS, SSH).

- 1. Establish an RDP connection to your Jump Host and login with the following credentials:
  - User: user
  - Password: Agility1
- Access the BIG-IP GUI https://10.128.1.245 (you can double-click on the red "f5 Big-IP" shortcut icon on the Windows desktop).
- 3. Login into the BIG-IP Configuration Utility with the following credentials:
  - User: admin
  - Password: admin

**Note:** All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

## 7.1.2 Lab Topology



The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE v13.1 (provisioned for Local Traffic Manager and Access Policy Manager)
- 1 x Windows Server running Active Directory and Web services
- 1 x Windows Jumphost

Note: The following entries have been added in the local hosts file of your Jumphost:

- 10.128.10.10 www.f5demo.com
- 10.128.10.11 myvpn.f5demo.com
- 10.128.20.200 www2.f5demo.com
- 10.128.10.11 webtop.f5demo.com
- 10.128.10.12 forms.f5demo.com
- 10.128.10.12 forms.f5demo.com
- 10.128.10.13 basic.f5demo.com
- 10.128.10.13 app1.f5demo.com
- 10.128.10.13 app2.f5demo.com
- 10.128.10.13 app3.f5demo.com
- 10.128.1.245 bigip1.f5demo.com

## 7.1.3 Lab Components

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
BIG-IP	<ul> <li>Management: 10.128.1.245</li> <li>Internal: 10.128.20.245</li> <li>External: 10.128.10.245</li> </ul>	admin/admin
Jumphost	<ul> <li>Management: 10.128.1.5</li> <li>External: 10.128.10.5</li> </ul>	user/Agility1
Lab Server	• Internal: 10.128.20.201	administrator/Agility2018

## 7.1.4 Labs Timing/Duration

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. Below is an estimate of how long it will take for each lab:

Lab name (Description)	Time Allocated
Lab 1 - Deploy a simple reverse proxy service	10 minutes
Lab 2 – Create My First Policy	15 minutes
Lab 3 – Configuring a VPN Policy	20 minutes
Lab 4 – Configuring an APM Webtop	10 minutes
Lab 5 – FORMS Based Authentication	15 minutes
Lab 6 – BASIC Authentication	15 minutes
Lab 7 – Single-Sign-On Across Authentication Domains	20 minutes

# 7.2 Lab 1 – Deploy a simple reverse proxy service

This lab will teach you how to configure resources including Virtual Servers, Pools, and monitors that we will use as the foundation for subsequent labs.

**Note:** Lab Requirements:

- · BIG-IP with APM licensed and activated
- Web site up and running at 10.128.20.200:80, 10.128.20.201:80 and 10.128.20.202:80

## 7.2.1 Task – Create a pool

Follow these steps to complete this task:

- 1. Browse to Local Traffic > Pools and click the '+' next to Pools List to create a new pool.
- 2. Name the pool in "http_pool"
- 3. Assign the monitor "http" by selecting it and sliding it to the left.
- 4. Add the following "new node" members to the pool, then click Finished:
  - Node Name: server1, Address: 10.128.20.200, Service Port 80
  - Node Name: server2, Address: 10.128.20.201, Service Port 80
  - Node Name: server3, Address: 10.128.20.202, Service Port 80

Configuration: Basic 🗸	]
Name	http_pool
Description	
Health Monitors	Active     Available       //Common     gateway_icmp       http     ≤       >>>     https://tds.       >>>     https://tds.
Resources	
Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	New Node O New FQDN Node O Node List Node Name: server3     (Optional) Address: 10.128.20.202 Service Port: 80     HTTP     Add     R:1 P:0 C:0 server1 10.128.20.200 :80     R:1 P:0 C:0 server2 10.128.20.201 :80     R:1 P:0 C:0 server3 10.128.20.202 :80     Edit Delete
Cancel Repeat Finished	

## 7.2.2 Task - Create HTTP Virtual Server to redirect to HTTPS

- 1. Create a new Virtual Server by browsing to Local Traffic > Virtual Servers > Virtual Server List and click the '+' to create a new one.
- Name the Virtual Server in the following format http_vs_redir. For "Destination Address/Mask", use 10.128.10.10". For "Service Port", use 80.
- 3. For "HTTP Profile" choose the default http profile called http
- 4. Under iRules at the bottom of the screen, select the **sys_https_redirect** irule from the "Available" list and slide it over to the "Enabled" list and click **Finished**.

General Properties								
Name		http_vs_re	edir			1		
Description								
Туре		Standard		\$				
Source Address								
Destination Address/Ma	ask	10.128.10	10.128.10.10					
Service Port		80	HTT	Р 🗘				
Notify Status to Virtual A	ddress							
State		Enabled	\$					
Configuration: Basic	\$							
Protocol		ТСР	\$					
Protocol Profile (Client)		tcp			\$			
Protocol Profile (Server)		(Use Clien	t Profile	)	\$			
HTTP Profile		http		¢				
Resources								
iRules	/Commo sys_ht	Enabled n ttps_redirect	~~	_sys_auth_ra _sys_auth_ss _sys_auth_ss _sys_auth_ss _sys_auth_ta	I_cc_ldap I_crldp I_ocsp			
Policies		nabled	<	Available				
Policies Default Pool 🛨	Er	nabled	<	Available				
	Er	nabled	<	Available				

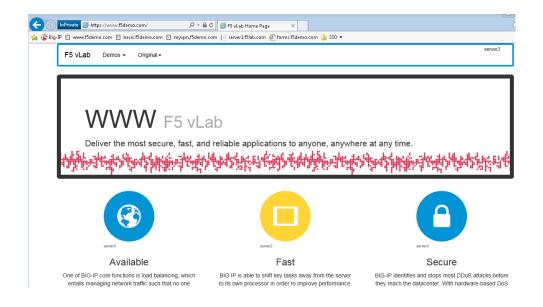
## 7.2.3 Task - Create HTTPS Virtual Server

- 1. Create a new Virtual Server by browsing to Local Traffic > Virtual Servers > Virtual Server List and click the '+' to create a new one.
- 2. Name the Virtual Server in the following format https_vs.
- 3. For "Destination Address/Mask", use 10.128.10.10. For "Service Port", use 443.
- 4. For "HTTP Profile", choose the default http profile
- 5. For "SSL Profile (Client)", choose the f5demo, slide it over to the "Selected" column
- 6. For "Source Address Translation", choose Auto Map
- 7. For "Default Pool", select the pool created earlier (http_pool) and click Finished.

General Properties	
Name	https_vs
Description	
Туре	Standard
Source Address	
Destination Address/Mask	10.128.10.10
Service Port	443 HTTPS 🔽
Notify Status to Virtual Address	
State	Enabled 🔽
Configuration: Basic 🔽	
Protocol	TCP
Protocol Profile (Client)	tcp 🔽
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http 🗸
SSL Profile (Client)	Selected Available           Common         clientssl           f5demo         <           >>>         clientssl-secure           crypto-server-default-clientssl
SSL Profile (Server)	Selected Available           Selected         Available           <
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
Default Pool	
Default Persistence Profile	None
Fallback Persistence Profile	None
Cancel Repeat Finished	

## 7.2.4 Task - Testing

You should now be able to browse to either Virtual Server (HTTP or HTTPs) and you should get the same page. Try: http://www.f5demo.com and https://www.f5demo.com



# 7.3 Lab 2 – Create My First Policy

In this lab, we will use the resources configured in the previous lab and configure a simple Access Profile using the Visual Policy Editor (VPE) to perform user authentication.

Note: Lab Requirements:

• Working HTTP and HTTPS Virtual Servers (from previous lab)

## 7.3.1 Task – Define an Authentication Server

Before we can create an access profile, we must create the necessary AAA server profile for our Active Directory.

Follow these steps to complete this task:

- 1. From the main screen, browse to Access > Authentication > Active Directory
- 2. Click Create... in the upper right-hand corner
- 3. Configure the new server profile as follows, then click Finished:
  - Name: Lab_SSO_AD_Server
  - Domain Name: f5demo.com
  - Server Connection: Direct
  - Domain Controller: 10.128.20.200

00							
00	Access		RADIUS	÷			
	Overview	+	LDAP	$( \cdot )$			
	Profiles / Policies	►	Active Directory	•	General Properties	[	_
	Authentication	Þ	SecurID	•	Name Type	Lab_SSO_AD_Server	
	Single Sign-On	÷	HTTP	$(\cdot)$	Configuration	/ care birectory	
	Federation	►	Oracle Access Mar	ager	Domain Name	f5demo.com	
	Connectivity / VPN	÷	OCSP Responder	$(\cdot)$	Server Connection	O Use Pool   Direct	
	Secure Web Gateway	►	CRLDP	$(\div)$	Domain Controller	10.128.20.200	
	Access Control Lists	►	TACACS+	÷	Admin Name		
	Webtops	►	Kerberos	$(\div)$	Admin Password		
			Local User DB	Þ	Verify Admin Password		
	Device Management		Endpoint		Group Cache Lifetime	30	Days
	Network		Management	$(\div)$	Password Security Object Cache Lifetime	30	Days
					Kerberos Preauthentication	None	
	System		Configurations	÷	Timeout	15	seconds
			NTLM	Þ		1	
	Device Management Network		Kerberos Local User DB Endpoint Management Systems CAPTCHA Configurations	<ul> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> </ul>	Verify Admin Password Group Cache Lifetime Password Security Object Cache Lifetime Kerberos Preauthentication Encryption Type Timeout	30 None	Days

## 7.3.2 Task – Create a Simple Access Profile

1. Navigate to Access > Profiles / Policies > Access Profiles (Per-Session Policies)

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

- 2. From the Access Profiles screen, click Create... in the upper right-hand corner
- 3. In the Name field, enter "MyAccessPolicy", and for "Profile Type", select the dropdown and choose All

General Properties					
Name	MyAccessPolicy				
Parent Profile	access				
Profile Type	All				
Profile Scope	Profile				

4. Under "Language Settings", choose **English** and click the "<<" button to slide over to the "Accepted Languages" column.

Language Settings		
Additional Languages	Afar (aa)	
Languages	Accepted Languages	Factory BuiltIn Languages       Japanese (ja)       Chinese (Simplified) (zh-cn)       Chinese (Traditional) (zh-tw)       Korean (ko)       Spanish (es)       French (fr)       German (de)
Default Language	English (en)	
Cancel Finished		

- 5. Click Finished, which will bring you back to the Access Profiles screen.
- 6. On the Access Profiles screen, click the **Edit** link under the Per-Session Policy column. The Visual Policy Editor (VPE) will open in a new tab.

Acc	Access » Profiles / Policies : Access Profiles (Per-Session Policies)												
*	, Access I	Profiles											
*			× Searc	:h			/	$\frown$				С	reate Import
	▼ Status	<ul> <li>Access</li> </ul>	Profile Name		Application	n 🗢 Profile Type	e Pe	er-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
	pe -	MyAccess	Policy			All	c	Edit	Export	Copy	default-log-setting		Common
	pe -	access				All	(n	one)	(none)	(none)			Common
Dele	te Appl	y											

7. On the VPE page, click the '+' icon on the "fallback" path, to the right of the Start object.

Access Policy: /Common/MyAccessPolicy	Б
Start fallback (+) Deny	
Add item	
Add New Macro	

8. On the popup menu, choose the Logon Page radio button under the Logon tab.

<b>6</b> 5			
Access Policy: /Com	nmoi	n/MyAccessPolicy	Edit Endings (Endings: Allow, Deny [default])
Start <u></u>	Be	gin typing to search	
Add New Macro	∫Log	on Authentication Assignm	ent Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
	0	Citrix Logon Prompt	Configure logon options for Citrix clients
An access policy consists of a	$^{\circ}$	External Logon Page	Redirect user to externally hosted form-based web logon page
on the upper right edge of the	0	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication
You can get started with <u>Devi</u> can later modify. See <b>BIG-IP</b>	0	HTTP 407 Response	HTTP 407 Response for Basic or SPNEGO/Kerberos authentication
Please see the <u>Online Help</u> fo	۲	Logon Page	Web form-based logon page for collecting end user credentials (used with most deployme
	0	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication
	0	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials
	$^{\circ}$	VMware View Logon Page	Display logon screen on VMware View clients

#### 9. Click Add Item.

Properties Branch Rule	s			
Name: Logon Page				~
Logon Page Agent				
Split domain from full Use	ername No 🔽			
CAPTCHA Configuration	None			
Туре	Post Variable Name	Session Variable Name	Values Read O	inly
1 text 🗸	username	username	No N	-
2 password V	password	password	No No	-
3 none 🗸	field3	field3	No No	-
4 none 🔽	field4	field4	No No	-
5 none 🗸	field5	field5	No No	-
Customization				_
Language	en 🗸		Reset all defaults	
Form Header Text	Secure Logon for F5 Networks			
Form Header Text				
Logon Page Input Field #1	Username			
Logon Page Input Field #2	Password			
Logon Button	Logon			=
				_
Front Image	[Replace Image] [Revert to Default]			
Save Password Checkbox	Save Password			
New Password Prompt	New Password			
Verify Password Prompt	Verify Password			~
Cancel Save				Help

## 10. Accept the defaults and click **Save**.

Now let's authenticate the client using the credentials to be provided via the "Logon Page" object.

11. Between the "Logon Page" and "Deny" objects, click the '+' icon.

licy

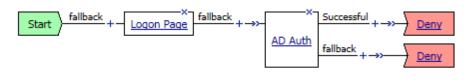
12. Select AD Auth found under the Authentication tab, and click the Add Item button.

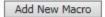
Log	on Authentication Assignme	ent Endpoint Security (Server-Side) Endpo
۲	AD Auth	Active Directory authentication of end user o
0	AD Query	Active Directory query to pull user attributes mapping
0	Client Cert Inspection	Check the result of client certificate authentic
$\circ$	CRLDP Auth	Certificate Revocation List Distribution Point
0	HTTP Auth	HTTP authentication of end user credentials
$^{\circ}$	Kerberos Auth	Kerberos authentication, typically following a
0	LDAP Auth	LDAP authentication of end user credentials
$^{\circ}$	LDAP Query	LDAP query to pull user attributes for use wit
0	LocalDB Auth	Local Database Authentication
$\circ$	NTLM Auth Result	NTLM authentication of end user credentials
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope man
$^{\circ}$	OAuth Client	OAuth Client
0	OAuth Scope	OAuth Scope
$^{\circ}$	OCSP Auth	Online Certificate Status Protocol (OCSP) clie
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and
$^{\circ}$	OTP Generate	Generate One Time Passcode (OTP)
0	OTP Verify	Verify One Time Passcode (OTP)
0	RADIUS Acct	Send accounting messages to a RADIUS serv
0	RADIUS Auth	RADIUS authentication of end user credentia
Can	cel Add Item	DCA Country Los forther all all strations of an

13. Accept the default for the **Name** and in the **Server** drop-down menu select the AD server created above: /**Common/LAB_SSO_AD_Server**, then click **Save**.

Properties* Branch Rules						
Name: AD Auth						
Active Directory						
Туре	Authentication <b>T</b>					
Server	/Common/Lab_SSO_AD_Server 🔻					
Cross Domain Support	Disabled 🔻					
Complexity check for Password Reset	Disabled					
Show Extended Error	Disabled 🔻					
Max Logon Attempts Allowed	3 🔻					
Max Password Reset Attempts Allowed	3 •					

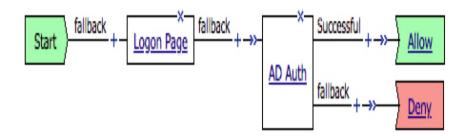
14. On the "Successful" branch between the **AD Auth** and **Deny** objects, click on the word **Deny** to change the ending.





15. Change the "Successful" branch ending to Allow, then click Save.

Select Ending:	
● Allow □	
◯ Deny ■	
Cancel Save	Help



16. In the upper left-hand corner of the screen, click on the **Apply Access Policy** link, then close the window using the **Close** button in the upper right-hand. Click **Yes** when asked "Do you want to close this tab?".



## 7.3.3 Task – Associate Access Policy to Virtual Servers

Now that we have created an access policy, we must apply it to the appropriate virtual server to be able to use it.

- 1. From the Local Traffic menu, navigate to the Virtual Servers List and click the name of the virtual server created previously: https_vs.
- 2. Scroll down to the "Access Policy" section, then for the "Access Profile" dropdown, select **MyAccessPolicy**.

Access Profile	MyAccessPolicy V
Connectivity Profile	+ None V
Per-Request Policy	None 🗸
/DI Profile	None 🔽
Application Tunnels (Java & Per App VPN)	- Enabled
DAM Support	Enabled
PingAccess Profile	None 🗸
celeration	
Rate Class	None 💌
	None V
Rate Class	
Rate Class DneConnect Profile	None 🔽
Rate Class DneConnect Profile NTLM Conn Pool	None  None
Rate Class DneConnect Profile ITLM Conn Pool ITTP Compression Profile	None None None

3. Click **Update** at the bottom of the screen.

## 7.3.4 Task – Testing

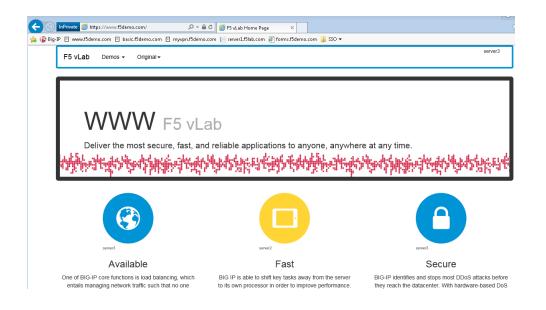
Now you are ready to test.

1. Open a new browser window and open the URL for the virtual server that has the access policy applied: https://www.f5demo.com. You will be presented with a login window.

Secure Logon
for F5 Networks
Username
Password
Logon

- 2. Enter the following credentials and click Logon:
  - Username: user
  - Password: Agility1

You will see a screen similar to the following:



# 7.4 Lab 3 – Configuring a VPN Policy

In this lab, we will use the Device Wizard to configure a new SSL VPN service with the necessary Network Access Resources on APM.

Note: Lab Requirements:

- · BIG-IP with APM licensed and activated
- · Server running AD and Web services
- · Local Host file entries on the Jump Host

#### 7.4.1 Task – Use the Wizard to create a new Remote Access service

The Wizard simplifies configuration tasks for specific use cases.

1. From the main menu on the left side of the screen, browse to the **Wizards > Device Wizards** and select the radio button for "**Network Access Setup Wizard for Remote Access**".

L iApps	Wizard Section	Wizard Section			
Wizards Device Wizards	Access Policy Manager Configuration				
S DNS	Description				
Local Traffic	Description	Configure a network access VPN connection for remote access. Creates an connection to internal resources.			
Traffic Intelligence	Next				

- 2. Click Next.
- 3. For the Policy Name field, enter **MyVPNPolicy**. This should auto populate the caption field. **Uncheck** the "**Enable Antivirus Check in Access Policy**" checkbox and click **Next**.

Policy Name	MyVPNPolicy
Default Language	en 🔻
Full Webtop	Enabled
Caption	MyVPNPolicy
Client Side Checks	Enable Antivirus Check in Access Policy
Cancel Next	

4. From the Select Authentication screen, choose the "**Use Existing**" radio button, select the AAA server "**Lab_SSO_AD_Server::Active Directory**" configured previously in Lab 2 and click **Next**.

Authentication Options	Create New  Use Existing		
Select AAA Server	Filter By Server Type: All Servers	▼ ] Lab_SSO_AD_Server::Active Directory	•
Cancel Previous Next			

5. Assign an IP Address Range to be used for the VPN connection on the "Configure Lease Pool" page. Click the radio button for "IP Address range" and enter the range "10.1.1.1-10.1.1.2", click Add and click Next.

Supported IP Version	IPV4
IPV4 Member List	Type: IP Address IP Address Range Start IP Address 10.1.1.1 End IP Address 10.1.1.2 Add 10.1.1.1 - 10.1.1.2
Cancel Previous Next	Edit Delete

6. On the "Configure Network Access" page, select "**Use split tunneling for traffic**" and for "IPV4 Lan Space", enter the network "**10.128.20.0**", mask "**255.255.255.0**", click **Add**, leave everything else default and click **Next**.

Client Settings	
Traffic Options	<ul> <li>Force all traffic through tunnel</li> <li>Use split tunneling for traffic</li> </ul>
IPV4 LAN Address Space	IP Address 10.128.20.0 × Mask 255.255.255.0 Add 10.128.20.0 / 255.255.255.0
	Edit Delete

7. Accept the default on the "Configure DNS Hosts for Network Access" page and click Next.

#### **Configure DNS Hosts for Network Access**

Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers are used by the client when performing name resolution for internal network resources.

These settings may be different than the BIG-IP system settings configured under **System :** the navigation pane.

IPV4 Primary Name Server	10.128.20.200	×
IPV4 Secondary Name Server		

 On the "Virtual Server (HTTPS connection)" page, enter "10.128.10.11" for the IP address of the Virtual Server that users will connect to for access to the VPN. Uncheck the "Create Redirect Virtual Server" option and click Next.

	Virtual Server IP Address	10.128.10.11
	Redirect Server	Create Redirect Virtual Server (HTTP to HTTPS)
[	Cancel Previous Next	

- 9. Verify your settings on the Review page and click Next when satisfied.
- 10. The Setup Summary page will display a list of the configuration objects that the Wizard created for you. Click **Finished**.

#### 7.4.2 Task – Testing

 Open a web browser to the virtual server created in the above step by navigating to https://myvpn.f5demo.com. You will be presented with a Logon page similar to the one from the last lab. |

Secure Logon for F5 Networks	
Username	
Password	
Logon	

2. Enter the following credentials:

Username: user

#### Password: Agility1

This will initialize, authenticate and establish a new VPN connection to the Network Resource that was configured. You will be presented with a new page that shows the connection details.

Traffic Type	Sent	Compression	Received	Compression
Network Access				
- Network Tunnel	5.42 KB	0%	324 B	0%
- Optimized Applications	0 B	0%	0 B	0%
Fotal	5.42 KB	0%	324 B	0%

3. Open a new browser tab and confirm that you are now connected to the internal network by browsing directly to the HTTP server used in the pool for the previous labs: http://server1.f5demo.com. You should see a page similar to the following:

F5 vLab Demos - Original - servert				
Deliver the most secure, fast, and	ab d reliable applications to anyone, anywher	e at any time.		
		And the second s		
Available	Fast	Secure		
One of BIG-IP core functions is load balancing, which entails managing network traffic such that no one server becomes eventwhether dhing holders alde. This improves application performance and availability.	BIG IP is able to shift key tasks away from the server to its own processor in order to improve performance. This can reduce the number of servers in a hybrical datacenter by as much as GD% and speed up the performance of the remaining servers.	BIG-IP identifies and stops most DDoS attacks before they reach the datacenter / With hardware-based DoS protections, BIG-19 detects DDoS attacks and rotates the connections away from critical servers, or rejects them outright.		
VE	•			

4. Close the page then click **Logout** on the F5 VPN page to terminate your VPN connection and close the browser window.

# 7.5 Lab 4 – Configuring an APM Webtop

In this lab, we will add a Webtop resource to the Access Policy created in the previous lab.

Note: Lab Requirements:

 Working HTTPS Virtual Server created in Lab 1 with Access Policy created in Lab 2 (Lab 2 successfully completed).

#### 7.5.1 Task – Create a Webtop resource

- 1. Expand the Access tab from the main menu on the left and navigate to Webtops > Webtop Lists.
- 2. Click Create to create a new Webtop called MyFullWebtop, select Type "Full", uncheck "Minmize To Tray" and click Finished.

General Properties		
Name	MyFullWebtop	
Туре	Full	
Configuration		
Minimize To Tray	Enabled	
Show a warning message when the webtop window close	Enabled	
Show URL Entry Field	✓ Enabled	
Show Resource Search	I Enabled	
Fallback Section		
Initial State	Expanded	

#### 7.5.2 Task – Enable "Content Rewrite" on the Virtual Server

- 1. Browse to Local Traffic > Virtual Servers > Virtual Server List and click on the name of your VPN Virtual Server called MyVPNPolicy_vs.
- 2. Scroll down to the "Content Rewrite" section, select "**rewrite**" for the "Rewrite Profile" field and click **Update**.

Content Rewrite	
Rewrite Profile +	rewrite
HTML Profile	None
Access Policy	
Access Profile	MyVPNPolicy V
Connectivity Profile +	MyVPNPolicy_cp
Per-Request Policy	None 🗸
VDI Profile	None
Application Tunnels (Java & Per- App VPN)	Enabled
OAM Support	Enabled

## 7.5.3 Task – Add Webtop resource to existing Access Policy

1. Browse to Access > Profiles / Policies > Access Profiles (Per-Session Policies), click on Edit for MyVPNPolicy. A new tab should open to the Visual Policy Editor for MyVPNPolicy.

<u>6</u>	
Access Policy: /Common/MyVPNPolicy Edit Er	ndings (Endings: Deny [default], Allow)
Start fallback + - Logon Page AD Auth fallback +	H + →→- <u>Advanced Resource Assign</u> fallback + →→- <u>Allow</u>

Add New Macro

- 2. Select the Advanced Resource Assign object.
- 3. Click Add/Delete.
- 4. Click on the **Webtop** tab, select the radio button for **MyFullWebtop**, then click the **Update** button at the bottom of the screen.



- 5. Click Save.
- 6. At the top left of the browser window, click on "Apply Access Policy", then close the tab.



#### 7.5.4 Task – Testing

- Open a web browser to the virtual server created in the previous lab by navigating to https://myvpn.f5demo.com. You will be presented with a Logon page similar to the one from the last lab.
- 2. Enter the following credentials:

Username: user

Password: Agility1

3. Click Logon.

This will open the APM Webtop landing page that shows the resources you are allowed to access. In this lab, we've only configured one resource: **Network Access**, but you can add as many as you want and they will appear on this Webtop page.

6		
Network Access		

# 7.6 Lab 5 – FORMS Based Authentication

In this lab, we will show you how to configure APM to leverage SSO functionality with an application server that uses forms based authentication.

Note: Lab Requirements:

- BIG-IP with APM licensed and activated
- · Server running AD and Web services
- · Local Host file entries on the Jump Host

## 7.6.1 Task – Create a Pool

- 1. Browse to Local Traffic > Pools and click the '+' next to Pools List to create a new pool.
- 2. Name the pool "forms_pool"
- 3. Assign the monitor "http" by selecting the monitor and moving it to the left.
- 4. Add the following new member/node to the pool and click Finished:
  - Node Name: forms, Address: 10.128.20.204, Service Port: 80

Configuration: Basic 🗸	
Name	forms_pool
Description	
Health Monitors	Active Available /Common Http <
Resources	
Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	New Node O New FQDN Node O Node List Node Name: forms     (Optional) Address: 10.128.20.204 Service Port: 80     HTTP     Add R:1 P:0 C:0 forms 10.128.20.204:80 Edit Delete
Cancel Repeat Finished	

## 7.6.2 Task – Create a Virtual Server

- 1. Browse to Local Traffic > Virtual Servers and click the '+' next to Virtual Server List to create a new one.
- 2. Use the following information to create the virtual server and leave the other settings at their default values, then click **Finished**:
  - Name the pool "forms_vs"
  - Destination Address/Mask: 10.128.10.12
  - Service Port: 443
  - HTTP Profile: http
  - SSL Profile (Client): f5demo
  - Source Address Translation: Auto Map
  - Default Pool: forms_pool

General Properties				
Name	forms_vs			
Description				
Туре	Standard			
Source			Selected	Available
Destination	Type:  Host Network Address: 10.128.10.12	SSL Profile (Client)	/Common f5demo <<< >>	clientssl
Service Port	443 HTTPS V		Selected	Available
Notify Status to Virtual Address		SSL Profile (Server)	<<	/Common apm-default-serverssl
State	Enabled V		>>	pcoip-default-serverssl
Configuration: Basic 🔻		SMTPS Profile	None 🗸	
Protocol	TCP	Client LDAP Profile	None	
Protocol Profile (Client)	tcp	Server LDAP Profile	None	
Protocol Profile (Server)	(Use Client Profile) V	SMTP Profile	All VLANs and Tunnels	
. ,		Source Address Translation	Auto Map V	
HTTP Profile	http 🔹			
Default Pool + for	rms_pool			
Default Persistence Profile No	one 🔻			
Fallback Persistence Profile	one 🔻			

## 7.6.3 Task – Testing without APM

Observe the current behavior of the login page without authentication enforced by APM.

1. Open your web browser and go to https://forms.f5demo.com. You should see a page that looks as follows:

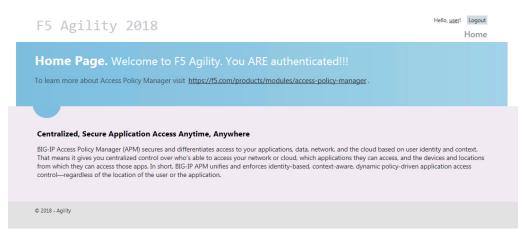
F5 Agility 2018	Log in
	Home
Log in.	
Use a local account to log in.	
User name	
Password	
□Remember me?	
Log in	
© 2018 - Agility	

2. Log in with the following credentials:

Username: user

Password: Agility1

Once successfully logged in you should see a web page similar to the following:



3. Logout using the link at the top right-hand corner of the page.

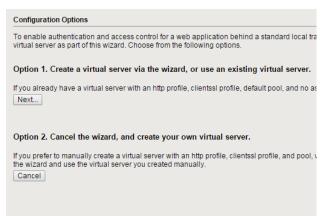
## 7.6.4 Task – Create Access Policy to use with Forms Based Authentication

- 1. Open the Wizards > Device Wizards page.
- 2. Select Web Application Access Management for Local Traffic Virtual Servers

Main Help About	Wizards » Device Wizards	
Mage Statistics	🔅 👻 Wizard List	
іАрр	Wizard Section	
Wizards Device Wizards	Access Policy Manager Configuration	Network Access Setup Wizard for Remote Access     Ortal Access Setup Wizard     Web Application Access Management for Local Traffic Virtual Servers
Local Traffic	Description	
Acceleration	Description	Configure authentication and access control for a web application behind a local traffic virtual server. C new or existing local traffic virtual server to provide authentication, access control, and endpoint security
Acceleration	Next	

#### 3. Click Next

4. Click Next for Option 1 on the Configuration Options page



- 5. Configure Basic Properties for the policy
  - (a) For Policy Name enter Forms_Access_Policy
  - (b) Uncheck Enable Antivirus Check in Access Policy

Policy Name	Forms_Access_Policy
Default Language	en 🔻
SSO Configuration	Configure SSO
Client Side Checks	Enable Antivirus Check in Access Policy
Cancel Previous Next	

- (c) Click Next
- 6. Configure the Authentication type used for this new policy
  - (a) Select Use Existing for the Authentication Options
  - (b) Select Lab_SSO_AD_Server::Active Directory

Select Authentication		
Please select the type of authe against a preconfigured externa		Ir access policy. When end users access the virtual server
	access policy without authentication, you a access policy and add an authentication a	are not authenticating users at all, or you will configure auth ction.
Authentication Options	O Create New  Use Existing	
Select AAA Server	Filter By Server Type: All Servers	Lab_SSO_AD_Server::Active Directory
Cancel Previous Next		

- (c) Click Next
- 7. Configure Single Sign On
  - (a) Select "Create New" for "SSO Options"
  - (b) Choose Form Based for the SSO Method
  - (c) Uncheck the option for "Use SSO Template"
  - (d) Enter /Account/Login* in the "Start URI" field
  - (e) Enter /Account/Login in the "Form Action" field
  - (f) Enter UserName in the "Form Parameter For User Name" field
  - (g) Enter Password in the "Form Parameter For Password" field

General Properties				
SSO Options	● Create New ○ Use Existing			
SSO Method	Form Based			
SSO Template	Use SSO Template			
SSO Method Configuration				
Start URI	/Account/Login*		>	0
Pass Through	Enable			
Form Method	POST			
Form Action	/Account/Login			
Form Parameter For User Name	UserName			
Form Parameter For Password	Password			
Hidden Form Parameters/Values	< >	$\langle \rangle$		
Successful Logon Detection Match Type	None			
Successful Logon Detection Match Value	<		>	0

- (h) Click Next
- 8. Configure Virtual Server
  - (a) Select Use Existing HTTPS Server
  - (b) Choose /Common/forms_vs for the Virtual Server

Options	<ul> <li>Create New HTTPS Server</li> <li>Use Existing HTTPS Server</li> </ul>
Virtual Server	/Common/forms_vs 🗸
Redirect Server	Create Redirect Virtual Server (HTTP to HTTPS)
Cancel Previous Next	

- (c) Click Next
- 9. Review configuration and click Next
- 10. Review the "Setup Summary", which shows all (existing and new) objects associated with this new policy and click **Finished**.
- 11. Add a logout URI Include to the new access policy
  - (a) Open the Access > Profiles / Policies > Access Profiles (Per-Session Policies) page
  - (b) Click on the name of the new policy Forms_Access_Policy
  - (c) Add "/Account/Logout" to the "Logout URI Include" field
  - (d) Change Logout URI Timeout to 1 second

Configurations		
Logout URI Include	URI Add /Account/Logout Edit Delete	
Logout URI Timeout	1 seconds	

- (e) Click Update
- 12. Enable SSO
  - (a) Click on the "SSO / Auth Domains" tab
  - (b) For "SSO Configuration", select Forms_Access_Policy_sso

Access Policy » Access Profiles : Access Profiles List » Forms_Access_Policy					
🔅 🗸 Properties	SSO	/ Auth Domains	Access Policy	Logs	
SSO Across Authentication Domains					
Domain Mode		Single Domain      Multiple Domains			
Domain Cookie					
Cookie Options		Secure Persistent HTTP Only			
SSO Configuration		Forms_Access	S_Policy_sso		
Update					

(c) Click Update

## 7.6.5 Task – Applying Access Policy Changes

After you create or change an access policy, the link Apply Access Policy appears in yellow at the top left of the BIG-IP Configuration utility screen. You must click this link to activate the access policy for use in your configuration.



- 1. Click the **Apply Access Policy** link, which will bring you to the Apply Access Policy screen, with a list of access policies that have been changed.
- 2. Select the new Access Policy and click the **Apply** button (by default, all access policies that are new or changed are selected).

Access Policy » Access Profiles : Access Profiles List					
÷	Access F	Profile List	Access Policy Sync	CAPTCHA Con	
	, , , , , , , , , , , , , , , , , , , ,				
×	* × Search				
	Status	<ul> <li>Name</li> </ul>			
Forms_Access_Policy					
Apply Access Policy					

After you apply the access policy, the Access Profiles list screen is displayed.

#### 7.6.6 Task – Testing with APM Authentication

Observe the behavior of the login page now that authentication is enforced by APM.

1. Open your web browser and go back to https://forms.f5demo.com. You should see a page that looks like the following:

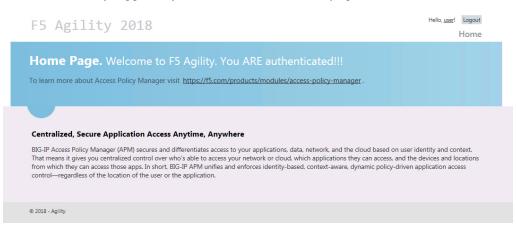
<b>(5</b> )	
Secure Logon for F5 Networks	
Username	
Password	
Logon	

2. Logon with the following credentials:

Username: user

Password: Agility1

Once successfully logged in you will see the same web page observed in task 2:



## 7.6.7 Task – Testing Logout

Earlier in Task 3, Step 9, we defined a **Logout URI Include** for this Access Policy. This is a list of logoff URIs that the access profile searches for in order to terminate the Access Policy Manager session. The URI we used was /Account/Logout, and the default logout delay is 5 seconds, which was modified to 1 second.

- 1. Logout using the **Logout** link at the top right-hand corner of the page.
- 2. Wait 1 second
- 3. Click the Home link in the banner at the top of the page
- 4. You should be redirected back to the F5 logon page

# 7.7 Lab 6 – BASIC Authentication

In this lab, we will show you how to configure basic authentication leveraging the SSO functionality of APM.

**Note:** Lab Requirements:

- BIG-IP with APM licensed and activated
- · Server running AD and Web services
- · Local Host file entries on the Jump Host

## 7.7.1 Task – Create a Pool

- 1. Browse to Local Traffic > Pools and click the '+' next to Pools List to create a new pool.
- 2. Name the pool "basic_pool"
- 3. Assign the monitor "http" by selecting the monitor and moving it to the left.
- 4. Add the following "New Member/Node" to the pool and click Finished:
  - Node Name: basic, Address: 10.128.20.203, Service Port: 80

Configuration: Basic			
Name	basic_pool		
Description			
Health Monitors	Active Available       Active     Available       /Common     gateway_icmp       http_head_f5     https       https_https_443     https_443		
Resources			
Load Balancing Method	Round Robin		
Priority Group Activation	Disabled		
New Members	New Node O New FQDN Node O Node List Node Name: basic     Address: 10.128.20.203 ×  Service Port: 80 HTTP Add		
	R:1 P:0 C:0 basic 10.128.20.203 :80		

## 7.7.2 Task 2: Create a Virtual Server

- 1. Browse to Local Traffic > Virtual Servers and click the '+' next to Virtual Server List to create a new one.
- 2. Use the following information to create the virtual server and leave other settings as default, then click **Finished**:
  - Name the pool "basic_vs"
  - Destination Address: 10.128.10.13
  - Service Port: 443
  - HTTP Profile: http
  - SSL Profile (Client): f5demo
  - Source Address Translation: Auto Map
  - Default Pool: basic_pool

General Properties			
Name	basic_vs		
Description			
Туре	Standard		
Source Address			
Destination Address/Mask	10.128.10.13		
Service Port	443 HTTPS 🗸		
Notify Status to Virtual Address			
State	Enabled V		
Configuration: Basic			
Protocol	TCP		
Protocol Profile (Client)	tcp 🗸		
Protocol Profile (Server)	(Use Client Profile)		
HTTP Profile	http 🗸		

	Selected	Available
SSL Profile (Client)	/Common f5demo	<ul> <li>clientssl</li> <li>clientssl-insecure-compatible clientssl-secure</li> <li>crypto-server-default-clientssl</li> </ul>
	Selected	Available
SSL Profile (Server)		<ul> <li>&lt; Apm-default-serverssl crypto-client-default-serverssl</li> <li>&gt; pcoip-default-serverssl</li> <li>✓</li> </ul>
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 🔽	

Default Pool +	basic_pool
Default Persistence Profile	None
Fallback Persistence Profile	None
Cancel Repeat Finished	

## 7.7.3 Task 3: Testing without APM

Observe the current behavior of the login page without APM authentication.

1. Open a private browsing window and go to **https://basic.f5demo.com**. You should receive a prompt that looks similar to the following screen shot:

inPrivate 🧟 abi	ローロ 図 outLinPrivate ・ クェン O Waiting for basic.f5demo.c × の な 袋
👍 🕞 Big-IP 🗉 www.f5den	10.com 🗿 basic.f5demo.com 🗏 myvpn.f5demo.com 📔 server1.f5lab.com 🗿 forms.f5demo.com
InPrivate is	Windows Security
When InPrivate Bi	The server reports that it is from basic f5demo.com.
InPrivate Browsing your browsing see history, and other See Help for more	Remember my credentials      OK Cancel
To turn off InPrivat	e Browsing, close this browser window.

- 2. Enter the following credentials:
  - Username: user
  - Password: Agility1
- 3. Once successfully logged in you will see a webpage similar to this one:

← 🕞 🗄 https://basic.f5de 오 ▾ 🔒 Ĉ 🗉 App #1 - F5 vLab 🛛 🗙	☆ 🔅
👍 🚯 Big-IP 📔 www.f5demo.com 🗏 basic.f5demo.com 🗏 myvpn.f5demo.com	📄 server1.f5lab.com 📔 forms.f5demo.com 길 SSO 🕶
🖸 F5 vLab	Hello, F5DEMO\user! Logout App #1
• 15 VEd0	
App #1.	
Hello	
Welcome. You ARE authenticated as F5DEMO\user	
© 2018 - F5	

4. Close the private browsing window.

## 7.7.4 Task 4: Create Access Policy to use with Basic Authentication

- 1. Open the **Wizards > Device Wizards** page.
  - (a) Select Web Application Access Management for Local Traffic Virtual Servers

	Main Help About	Wizards » Device Wizards	
Wizards         Wizard Section           Device Wizards         Access Policy Manager         Portal Access Setup Wizard for Remote Access           Device Wizards         Portal Access Setup Wizard         Portal Access Setup Wizard           Device Wizards         Description         Description           Description         Configure authentication and access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint access control for a web application behind a local traffic virtual server to provide authentication, access control for a web application behind a local traffic virtual server to provide authentication access control for a web application behind a local traffic virtual server to provide authentication access control for a web application behind a local traffic virtual server to provide authentication access control for a web application behind a local traffic virtual server to provide authentication access control for a web application behind a local traffic virtua	Statistics	🔅 👻 Wizard List	
Device Wizards       Oratal Access Setup Wizard         Device Wizards       Image: Configuration         Image: Device Wizards       Image: Device Wizards         Image: Device Wizards       Device W	іАрр	Wizard Section	
Device Wizards       Image: Configure authentication Access Management for Local Traffic Virtual Servers         Description       Description         Description       Configure authentication and access control for a web application behind a local traffic virtual server to provide authentication, access control, and endpoint server to provide authentication, access control, and endpoint server to provide authentication, access control, and endpoint server to provide authentication.	Wizards		O Portal Access Setup Wizard
Local Traffic     Description     Configure authentication and access control for a web application behind a local traffic virtual ser     new or existing local traffic virtual server to provide authentication, access control, and endpoint a	Device Wizards		Web Application Access Management for Local Traffic Virtual Servers
Configure authentication and access control for a web application behind a local traffic virtual ser new or existing local traffic virtual server to provide authentication, access control, and endpoint s	Local Traffic	Description	
		Description	Configure authentication and access control for a web application behind a local traffic virtual server. new or existing local traffic virtual server to provide authentication, access control, and endpoint security
	Acceleration	Next	

- (b) Click Next
- 2. Click Next for Option 1 on the Configuration Options page

Configuration Options
To enable authentication and access control for a web application behind a standard local tra virtual server as part of this wizard. Choose from the following options.
Option 1. Create a virtual server via the wizard, or use an existing virtual server.
If you already have a virtual server with an http profile, clientssl profile, default pool, and no as $\boxed{\text{Next}}$
Option 2. Cancel the wizard, and create your own virtual server.
If you prefer to manually create a virtual server with an http profile, clientssi profile, and pool, v the wizard and use the virtual server you created manually. Cancel

- 3. Configure Basic Properties for the policy
  - (a) For Policy Name enter **Basic_Access_Policy**
  - (b) Uncheck "Enable Antivirus Check in Access Policy"

Policy Name	Basic_Access_Policy
Default Language	en 🔽
SSO Configuration	Configure SSO
Client Side Checks	Enable Antivirus Check in Access Policy
Cancel Previous Next	

- (c) Click Next
- 4. Configure Authentication type used for policy
  - (a) Select Use Existing for the "Authentication Options"
  - (b) Select Lab_SSO_AD_Server::Active Directory

Please select the type of authors against a preconfigured extern	titication you would like to configure for your access policy. When end users access the virtual so I authentication server.	erver
f vou would like to test a basic	access policy without authentication, you are not authenticating users at all, or you will configure	e auth
	access policy and add an authentication action.	
	Create New  Use Existing	

- (c) Click Next
- 5. Configure SSO
  - (a) Select Create New for the "SSO Options"
  - (b) Choose HTTP Basic
  - (c) Click Next

General Properties	
SSO Options	Ocreate New ○ Use Existing
SSO Method HTTP Basic ÷	
SSO Method Configuration	
Username Conversion	
Cancel Previous Next	

- 6. Configure Virtual Server
  - (a) Select Use Existing HTTPS Server
  - (b) Choose /Common/basic_vs for the Virtual Server**

Options	○ Create New HTTPS Server
Virtual Server	/Common/basic_vs 🔽
Redirect Server	Create Redirect Virtual Server (HTTP to HTTPS)
Cancel Previous Next	

- (c) Click Next
- 7. Review configuration and click Next
- 8. Review the "Setup Summary", which shows all (existing and new) objects associated with this new policy.
- 9. Click Finished
- 10. Add a logout URI Include to the new access policy
  - (a) Open the Access > Profiles / Policies > Access Profiles (Per-Session Policies) page
  - (b) Click on the name of the new policy Basic_Access_Policy
  - (c) Add "/Home/Logout" to "Logout URI Include"
  - (d) Change Logout URI Timeout to 1 second

Configurations			
Logout URI Include	URI /Home/Logout Add /Home/Logout Edit Delete		
Logout URI Timeout	1 seconds		

- (e) Click Update
- 11. Enable the SSO Configuration
  - (a) Click on the SSO / Auth Domains tab
  - (b) For SSO Configuration, select Basic_Access_Policy_sso

Access Policy » Access Profiles : Access Profiles List » Basic_Access_Policy				
🔅 🚽 Properties	SSO /	/ Auth Domains	Access Policy	Logs
SSO Across Authenticatio	on Dom	ains		
Domain Mode		Single Doma	ain $\bigcirc$ Multiple Doma	ins
Domain Cookie				
Cookie Options		Secure Persistent HTTP Only		
SSO Configuration		Basic_Access	_Policy_sso 🗸	
Update				

(c) Click Update

## 7.7.5 Task 5: Applying Access Policy

After you create or change an access policy, the link Apply Access Policy appears in yellow at the top left of the BIG-IP Configuration utility screen. You must click this link to activate the access policy for use in your configuration.



- 1. Click the **Apply Access Policy** link, which will bring you to the Apply Access Policy screen, with a list of access policies that have been changed.
- 2. Select the Access Policy and click the **Apply** button (by default, all access policies that are new or changed are selected).

Access Policy » Access Profiles : Access Profiles List					
🚓 🗸 🗛 Access F	Profile List	Access Policy Sync	CAPTCHA Configuration		
*		× Sea	rch		
Status A Name					
Basic_Access_Policy					
Apply Access Policy					

After you apply the access policy, the Access Profiles list screen is displayed.

## 7.7.6 Task 6: Testing with APM Authentication

Observe the behavior of the login page with authentication enforced by APM.

1. Open a private browsing window and go to **https://basic.f5demo.com**. You should see a page that looks like the following:

<b>(5</b>	
Secure Logon for F5 Networks	
Username	
Password	
Logon	

2. Logon with the following credentials:

Username: user

Password: Agility1

Once successfully logged in you will see the same web page observed in task 3:

C       ○       Inttps://basic.f5de       P < ▲ C       □       App #1 - F5 vLab       ×       Inttps://basic.f5demo.com       Inttps:/	
E F5 vLab	ogout o #1
Арр #1.	
Hello Welcome. You ARE authenticated as F5DEMO\user	
© 2018 - F5	

## 7.7.7 Task 7: Testing Logout

Earlier in Task 3, Step 9, we defined a **Logout URI Include** for this Access Policy. This is a list of logoff URIs that the access profile searches for in order to terminate the Access Policy Manager session. The URI we used was /Home/Logout, and the default logout delay is 5 seconds which was modified to 1 second.

- 1. Click the Logout link located at the top right of the web pagee
- 2. Wait 1 second
- 3. Click the "App #1" link in the banner at the top of the page
- 4. You should be redirected back to the F5 logon page

# 7.8 Lab 7 – Single-Sign-On Across Authentication Domains

In this lab, we will show you how to provide SSO across multiple applications. Normally APM will require authentication each time an application is accessed. By using a Domain Cookie it is possible to re-use an existing APM session to access multiple applications.

Note: Lab Requirements:

• Previous Labs 5 and 6 successfully completed

#### 7.8.1 Task – Verify Authentication Required for different applications

- 1. Open a Private web browser or clear your browser cache and go to the Virtual Server used earlier https://basic.f5demo.com
- 2. You should be able to logon with the following credentials:
  - Username: **user**
  - Password: Agility1

- 3. Once successfully logged in, you will be presented with the same information page you observed earlier from basic.f5demo.com "App #1".
- 4. Now go to https://app2.f5demo.com you should be prompted to logon again.
- 5. You should be able to logon with the following credentials:
  - Username: **user**
  - Password: Agility1
- 6. Once successfully logged in, you will be presented with information about "App #2".
- 7. Logout and close the browser window.

#### 7.8.2 Task - Specify Domain Cookie

- 1. Open the Access > Profiles / Policies > Access Profiles (Per-Session Policies) page
- 2. Click on the name of the policy Basic_Access_Policy
- 3. Click on the SSO / Auth Domains tab
- 4. Enter f5demo.com to Domain Cookie

Access Policy » Access Profiles : Access Profiles List » Basic_Access_Policy					
<b>*</b> -	Properties	SSO	Auth Domains	Access Policy	Logs
		_			
SSO A	cross Authenticatio	on Dom	ains		
Doma	in Mode		Single Doma	ain 🔿 Multiple Doma	ins
Doma	in Cookie	f5demo.com			
Cookie Options		Secure Persistent HTTP Only			
SSO (	Configuration		Basic_Access	_Policy_sso 🗸	
Update	e				

- 5. Click Update
- 6. Don't forget to click on Apply Access Policy to put your changes in effect!

#### 7.8.3 Task - Testing Authentication across domains

- 1. Open a Private web browser or clear your browser cache and go to the Virtual Server used earlier https://basic.f5demo.com
- 2. You should be able to logon with Username: user Password: Agility1
- 3. Once successfully logged in, you will be presented with the same information page you observed earlier.
- 4. Now go to https://app2.f5demo.com. You should not be prompted to logon again!

## 7.8.4 Task 4 (Bonus) - Authentication across domains & virtual servers

Repeat the previous steps, but for Forms_Access_Policy instead of Basic_Access_Policy.

Are you prompted for authentication when going from https://forms.f5demo.com to https://basic.f5demo.com?

Try changing the value for "Profile Scope" for **Basic_Access_Policy** and **Forms_Access_Policy** from Profile to **Global** 

#### *Troubleshooting tips:

Did you forget to Apply Access Policy ?

Verify the Domain Cookie configured on the SSO page... for both policies?

# **Class 8: Troubleshooting Universal Access**

Welcome to the Troubleshooting Universal Access Lab. These lab exercises will instruct you on how to configure and troubleshoot common Access Policy Manager (APM) issues as experienced by field engineers, support engineers and customers. This guide is intended to complement lecture material provided during the course as well as a reference guide that can be referred to after the class as a basis for troubleshooting APM in your own environment.

Expected time to complete: 4 hours

# 8.1 Getting Started

## 8.1.1 Timing for Labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. This can never be accurately predicted but we strived to derive an estimate among several people each having a different level of experience. Below is an estimate of how long it will take for each lab:

#### LAB Timing

LAB Name (Description)	Time Allocated
LAB 1: APM Troubleshooting Lab Object Prep (C Do EITHER Lab 1 OR Lab 2 (not both)	20 minutes SUI)
LAB 2: APM Troubleshooting Lab Object Prep (1 Do EITHER Lab 1 OR Lab 2 (not both)	20 minutes MSH)
LAB 3: General Troubleshooting	5 minutes
LAB 4: Visual Policy Editor (VPE) and Session	20 minutes
Variables	
LAB 5: Command Line Tools	25 minutes

## 8.1.2 General Notes

Provisioning Access Policy Manager (APM) is not required for basic Access Policy uses cases although this has been provisioned for you ahead of time. This was done to save time as provisioning often requires services to restart which takes away valuable lecture/lab time.

## 8.1.3 How to use this Guide

For each section, follow the instruction of the class moderator on when to begin. Carefully read and implement each item step by step.

Archives have been provided for each completed section and can be loaded if necessary at the beginning of each section for prior labs. You can install the UCS archive by using the **tmsh no-license** option. For the command syntax, refer to the following example:

```
tmsh load sys ucs [ucs file name] no-license
```

# 8.2 Lab Environment

#### 8.2.1 Accessing the Lab Environment

To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces (HTTPS, SSH).

Your class instructor will provide additional lab access details.

#### 8.2.2 Lab Network Setup

In the interest of focusing as much time as possible configuring and troubleshooting APM, we have provided some resources and basic setup ahead of time. These are:

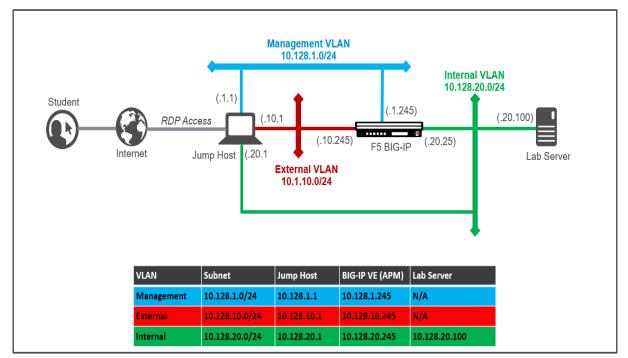
- · Cloud-based lab environment complete with Jump Host, Virtual BIG-IP (VE) and Lab Server
- Duplicate Lab environments for each student for improved collaboration
- Virtual BIG-IP has been pre-licensed and provisioned for Access Policy Manager (APM)

**Note:** All work for this lab will be performed exclusively from the Windows jump host. No installation or interaction with your local system is required.

If you wish to replicate these lab exercises in your own lab environment, you will need to perform these steps accordingly. Additional lab resources are provided as illustrated in the diagram below:

## 8.2.3 LAB Environment Diagram

# Lab Environment



#### 8.2.4 Lab Components

The following components have been included in your lab environment:

- 1 x Windows Jump Host
- 1 x F5 BIG-IP VE (v13.1)
- 1 x Windows Lab Server (AD/DNS/App)

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
Jump Host	<ul> <li>Management: 10.128.1.1</li> <li>Internal: 10.128.20.1</li> <li>External: 10.128.10.1</li> </ul>	agility/Agility1
BIG-IP VE	<ul> <li>Management: 10.128.1.245</li> <li>Internal: 10.118.20.245</li> <li>External: 10.118.10.245</li> </ul>	admin/admin
Lab Server	• Internal: 10.128.20.100	none

# 8.3 Lab 1: APM Troubleshooting Lab Object Preparation (GUI)

**Note:** You only need to perform EITHER Lab 1 OR Lab 2. They accomplish the same goal, but using different methods. Lab 2 gets the Lab Preparation using TMSH

The purpose of this lab is to preconfigure some objects that will be used throughout the other labs. These objects are as follows:

- Domain Name Services (DNS) Resolver
- Network Time Protocol (NTP) Server
- Access Policy (APM) AAA Server Active Directory
- Access Policy (APM) SSO Configuration NTLMv1
- Access Policy (APM) Access Profile
- · Local Traffic (LTM) Pool and Member
- · Local Traffic (LTM) Virtual Server

#### 8.3.1 Connect to the Lab

<b>(5</b> )	BIG-IP Configuration Utility F5 Networks, Inc.
Hostname bigip1.f5lab.com IP Address 10.128.1.245 Username	Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left.
admin Password	
Log in	

- 1. Establish an RDP connection to your Jump Host and double-click on the **BIG-IP** Chrome shortcut on the Windows desktop.
  - User: agility
  - · Password: Agility1
- 2. Ignore the certificate warning.
- 3. Login into the BIG-IP Configuration Utility with the desktop icon (or Favorite link in Chrome) with the following credentials:

- User: admin
- Password: admin

# 8.3.2 DNS Resolver for System Configuration

5 <b>•</b>	System		Setup Utility			
	Configuration	Þ	Device	×	General	dı
	File Management	•	Local Traffic	÷	NTP	
	Certificate Management		AWS	•	DNS	
	Disk Management		OVSDB		Hosts	
	Software Management		App IQ		SMTP 💮	
	License				SSHD	
	Resource Provisioning		Plug-ins		Upstream Proxy	

1. Create a DNS entry by selecting: System->Configuration->Device->DNS

System » Configuration : Device : DNS						
🔅 🗸 Device 🗸	Local Traffic 🛛 🔫	AWS 👻	OVSDB			
Properties			,			
DNS Lookup Server List	Address: 10.128. Add 10.128.20.100 Edit Delete	20.100	*			
BIND Forwarder Server List	Address: Add Edit Delete	Up Down	*			
DNS Search Domain List	Address: agilityla Add localhost agilitylab.com Edit Delete	b.com	*			
DNS Cache						
IP Version	IPv4 ▼					

- Update
- 2. In the Properties Section for DNS Lookup Server List, enter **10.128.20.100** in the Address field and click the **ADD** button.
- 3. Scroll down to the DNS Search Domain List section and enter **agilitylab.com** in the Address field and click the **ADD** button.
- 4. Click the **UPDATE** button at the bottom of the page to save the changes you just made.

## 8.3.3 NTP Server for System Configuration

100 <b>(</b>	System		Setup Utility			
	Configuration	×	Device		General	de
	File Management	- F	Local Traffic	- 1	NTP	
	Certificate Management	×.	AWS		DNS	
	Disk Management		OVSDB		Hosts	
	Software Management	- F	App IQ		SMTP (+)	
	License				SSHD	
	Resource Provisioning		Plug-ins		Upstream Proxy	

1. Create a NTP entry by selecting: System ? Configuration ? Device ? NTP

System » Configuration : Device : NTP								
⇔ -	Device	•	Local Traffic	•	AWS	-	OVSDB	
Proper	ties							
Time	Server List		Address: 1 Add 10.128.20.1		20.100		•	
Updat	te							

- 2. In the Properties Section for Time Server List, enter **10.128.20.100** in the Address field and click the **ADD** button.
- 3. Click the **UPDATE** button at the bottom of the page to save the changes you just made.

## 8.3.4 Access Policy (APM) AAA Server – Active Directory Object Creation

	Traffic Intelligence		RADIUS	÷
	Acceleration	LDAP	÷	
			Active Directory	•
	Access		SecurID	÷
	Overview	- 1-	HTTP	÷
Profiles / Policies		Oracle Access Man	ager	
	Authentication	•	OCSP Responder	÷
	Oinela Oine On		00100	

1. Create a new AAA Server Object of type Active Directory by selecting: Access ? Authentication ? Active Directory

			Create
Access Profiles	Per-Request Policy	Partition / Path	IP Address/Pool

2. Click the **CREATE** button on right side of page.

Access » Authentication »	lew Server	
General Properties		
Name	LAB_AD_AAA	
Туре	Active Directory	
Configuration		
Domain Name	agilitylab.com	×
Server Connection	◯ Use Pool   Direct	
Domain Controller		
Admin Name		
Admin Password		
Verify Admin Password		
Group Cache Lifetime	30	Days
Password Security Object Cache Lifetime	30	Days
Password Security Object Cache Lifetime	30	Days
Kerberos Preauthentication Encryption Type	None	
Timeout	15	seconds
Cancel Repeat Finished		

- 3. Under General Properties type LAB_AD_AAA in the name field.
- 4. In the Configuration Section, Click the radio button option next to **Direct** in the Server Connection row.
- 5. In the Domain Name field enter agilitylab.com
- 6. Leave the Domain Controller, Admin Name and Admin Password fields blank for now.
- 7. Click the **FINISHED** button at the bottom of the page to save your changes.

## 8.3.5 Access Policy (APM) SSO Configuration – NTLMv1

	Access		Use the follow configured the	-	
[	Overview	•	<ul> <li>System D</li> <li>DNS</li> </ul>	evice Ce	erti
	Profiles / Policies	•	NTP     SNMP		
	Authentication	×.	User Auth	enticatio	on
	Single Sign-On	► F	HTTP Basic	÷	
	Federation	► N	NTLMV1	€	a
	Connectivity / VPN	► <b>N</b>	NTLMV2	÷	ty

1. Create a new SSO Configuration Object of type NTLM by selecting: Access ? Single Sign-On ? NTLMV1

				Create
SSO Method	Access Profiles	Portal Access	Log	Partition / Path

2. Click the **CREATE** button on the right side of the page.

# Access » Single Sign-On » New SSO Configuration...

General Properties: Basic	~
Name	Agility_Lab_SSO_NTLM ×
SSO Method	NTLMV1
Log Settings	+ From Access Profile 🗸
Credentials Source	
Username Source	session.sso.token.last.username
Password Source	session.sso.token.last.password
Domain Source	session.logon.last.domain
SSO Method Configuration	
Username Conversion	Enable
NTLM Domain	
Cancel Finished	

- 3. In the Name field enter Agility_Lab_SSO_NTLM
- 4. Click the **FINISHED** button at the bottom.

#### 8.3.6 Access Policy (APM) Access Profile Creation

	Access			Use the following addition configured the system us
[	Overview	F		<ul> <li>System Device Certif</li> <li>DNS</li> </ul>
	Profiles / Policies	۰.		Access Profiles
	Authentication	÷	P	Per-Session 🕑 🖸 Policies)
	Single Sign-On	•		Per-Request

1. Create a new APM Profile Object of type ALL by selecting: Access ? Profiles/Policies ? Access Profiles (Per-Session Policies)

						C	reate Import
Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
	All	(none)	(none)	(none)			Common

2. Click the **CREATE** button on the right side of the page.

Access » Profiles / Policies : Ac	cess Profiles (Per-Session Policies) » New Profile
General Properties	
Name	Agility-Lab-Access-Profile
Parent Profile	access
Profile Type	All
Profile Scope	Profile <b>T</b>

- 3. In the Name field enter, Agility-Lab-Access-Profile
- 4. In the Profile Type drop down list select All
- 5. In the Profile Scope drop down list select Profile

Settings			Custom 🗆
Inactivity Timeout	900	seconds	
Access Policy Timeout	30	seconds	Ø
Maximum Session Timeout	604800	seconds	
Minimum Authentication Failure Delay	2	seconds	
Maximum Authentication Failure Delay	5	seconds	
Max Concurrent Users	0	[	
Max Sessions Per User	0	[	
Max In Progress Sessions Per Client IP	128	[	

6. In the Settings section click the checkbox to the right of Access Policy Timeout and change the value from 300, to **30**, seconds.

Additional Languages	Afar (aa)	<ul> <li>Add</li> </ul>			
	Accepte	ed Languages		Factory BuiltIn Languages	
Languages	English (en)		* << >> v	Spanish (es)	×
Default Language	English (en) 🔻				

- Scroll the bottom of the page and in the Language Settings section, click to highlight English in the Factory Builtin Languages box, then click the left << arrows to move it to the left box labeled Accepted Languages.
- 8. Click the **FINISHED** button at the bottom of the page to save your changes.

#### 8.3.7 Local Traffic (LTM) Pool and Member Creation

ocal Traffic			
Network Map			
Virtual Servers	Þ		
Policies	•		
Profiles	Þ		
Ciphers			
iRules			
Pools	•	Pool List	•
Nodes	+	Statistics	
	Network Map Virtual Servers Policies Profiles Ciphers iRules Pools	Network Map         Virtual Servers         Policies         Profiles         Oriphers         iRules         Pools	Network Map         Virtual Servers         Policies         Profiles         Ciphers         iRules         Pools

1. Create a new LTM Pool and Member by selecting Local Traffic ? Pools? Pools List

			Create
Description	Application	Members	Partition / Path

2. Click the **CREATE** button on the right side of the page.

Name	Agility-Lab-Pool
Description	
Health Monitors	Active Available       Active     Available       Image: Second state of the second
esources	
Load Balancing Method	Round Robin
Priority Group Activation	Disabled
New Members	New Node O New FQDN Node Node Name: (Optional) Address: 10.128.20.100  Service Port: 80 HTTP  Add
	Node Name Address/FQDN Service Port Auto Populate Priority
	10.128.20.100 10.128.20.100 80 0

- 3. In the Name field enter Agility-Lab-Pool
- 4. In the Resources section, in the New Members area, enter 10.128.20.100 in the Address field.
- 5. In the Service Port field, enter 80, or select HTTP from the drop-down menu.
- 6. Click the ADD button
- 7. Click the **FINISHED** button at the bottom to save your changes.

## 8.3.8 Local Traffic (LTM) Virtual Server Creation

This lab will walk you through creating the Virtual Server we will use during the course of the lab. This Virtual Server will be used to associate Access Policies which will be evaluated when authenticating users.

() ()	Local Traffic	Cancel Finished	
	Network Map		
	Virtual Servers	Þ	Virtual Server List 📀
	Policies	Þ	Virtual Address List
	Profiles	Þ	Statistics

1. Create an new Virtual Server by selecting Local Traffic ? Virtual Servers ? Virtual Server List

						Create
Description	Application	Destination	Service Port	Type	Resources	Partition / Path

2. Click the **CREATE** button on the right side of the page.

Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

#### General Properties

Name	Agility-LTM-VIP
Description	
Туре	Standard
Source Address	
Destination Address	10.128.10.100
Service Port	443 HTTPS V
Notify Status to Virtual Address	
State	Enabled

- 3. Under the General Properties section, in the Name field enter Agility-LTM-VIP
- 4. In the Destination Address field enter 10.128.10.100
- 5. In the Service Port fields enter 443, or select HTTPS from the drop-down menu

Configuration: Basic		
Protocol	TCP	
Protocol Profile (Client)	tcp	~
Protocol Profile (Server)	(Use Client Profile)	~
HTTP Profile	http 🔽	
HTTP Proxy Connect Profile	None	
FTP Profile	None 🗸	
RTSP Profile	None 🗸	
SSL Profile (Client)	Selected       //Common     <       clientssl     <       >>     ///>/	Available Common clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl
SSL Profile (Server)	Selected <<	Available Common apm-default-serverssl crypto-client-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 🗸	

- 6. Under the Configuration section, in the HTTP Profile field use the drop-down menu to select http
- 7. In the SSL Profile (Client) field select **clientssl** from the Available profiles then use the << left arrows to move it to the Selected box.
- 8. Ensure VLAN and Tunnel Traffic is set to All VLANs and Tunnels
- 9. In the Source Address Translation field select **Auto Map** from the drop-down menu.

Access Policy	
Access Profile	Agility-Lab-Access-Profile
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

10. Scroll down to the Access Profile section, select **Agility-Lab-Access-Profile** from the drop-down menu.

Default Persistence Profile	None	•
Fallback Persistence Profile	None	<b>~</b>
Cancel Repeat Finished		

11. Click the FINISHED button to save your changes.

## 8.4 Lab 2: APM Troubleshooting Lab Object Preparation (TMSH)

Note: You only need to perform one of Lab 1, 2, or 3. They accomplish the same thing only in different ways. Lab 2 gets the Lab Preparation using TMSH

The purpose of this lab is to preconfigure some objects that will be used throughout the other labs. These objects are as follows:

- Domain Name Services (DNS) Resolver
- Network Time Protocol (NTP) Server
- Access Policy (APM) AAA Server Active Directory
- Access Policy (APM) SSO Configuration NTLMv1
- Access Policy (APM) Access Profile
- Local Traffic (LTM) Pool and Member
- · Local Traffic (LTM) Virtual Server

## 8.4.1 Connect to the Lab via SSH

<b>(5</b> )	BIG-IP Configuration Utility F5 Networks, Inc.
Hostname bigip1.f5lab.com IP Address 10.128.1.245 Username admin	Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left.
Password ••••• Log in	

- 1. Establish an RDP connection to your Jump Host and double-click on the **BIG-IP** Chrome shortcut on the Windows desktop. User: agility Password: Agility1
- 2. Ignore the certificate warning.
- 3. Login into the BIG-IP via SSH using putty and the following credentials: User: root Password: default
- 4. Log in to tmsh by typing the following command: tmsh

## 8.4.2 DNS Resolver for System Configuration (TMSH)

1. To add a name server to your /etc/resolv.conf file, use the following command syntax, replacing <IP addresses> with your IP addresses:

#### modify sys dns name-servers add { <IP addresses> }

2. To add domains to your search list use the following command replacing <domains> with the domain you wish to add:

#### modify sys dns search add { <domains> }

3. Configure as follows:

modify sys dns name-servers add { 10.128.20.100 }

modify sys dns search add { agilitylab.com }

#### save sys config

4. To verify, use the following command: list sys dns

```
root@(bigipa)(cfg-sync Standalone)(Active)(/Common)(tmos)# 1
sys dns {
    name-servers { 10.128.20.100 }
    search { localhost agilitylab.com }
}
```

You should see the following reply:

## 8.4.3 NTP Server for System Configuration (TMSH)

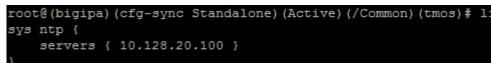
- 1. To configure one or more NTP servers for the BIG-IP system, use the following command syntax: modify sys ntp servers add {hostname hostname....}
- 2. Configure as follows:

modify sys ntp servers add { 10.128.20.100 }

save sys config

3. To verify, use the following command:

list sys ntp



You snould see the following reply:

#### 8.4.4 Access Policy (APM) AAA Server – Active Directory Object Creation (TMSH)

1. To configure an Active Directory AAA Server object, use the following command syntax:

create apm aaa active-directory <name> domain <domain-name> use-pool <disabled>

2. Configure as follows:

create apm aaa active-directory LAB_AD_AAA domain agilitylab.com use-pool disabled save sys config

3. To verify, use the following command:

list apm aaa

```
root@(bigipa)(cfg-sync Standalone)(Active)(/Common)(tmos)# 1
apm aaa active-directory LAB_AD_AAA {
domain agilitylab.com
use-pool disabled
```

You should see the following reply:

#### 8.4.5 Access Policy (APM) SSO Configuration – NTLMv1 (TMSH)

1. To configure an NTLMv1 SSO profile, use the following command syntax:

#### create apm sso ntlmv1 <profile_name>

2. Configure as follows:

create apm sso ntlmv1 Agility_Lab_SSO_NTLM

#### save sys config

3. To verify, use the command:

list apm sso

#### 8.4.6 Access Policy (APM) Access Profile Creation (see GUI steps)

**Note:** In order to gain familiarity with the Visual Policy Editor, please follow the GUI method of Access Policy creation: https://ua230-troubleshooting-2018-dev.readthedocs.io/en/latest/class4/module1/module1. html#access-policy-apm-access-profile-creation

#### 8.4.7 Local Traffic (LTM) Pool and Member Creation (TMSH)

1. To configure a LTM Pool and Pool members, use the following command syntax:

create ltm pool <pool-name> members add { <IP-addr>:<service-port> }

2. Configure as follows:

create Itm pool Agility-Lab-Pool members add { 10.128.20.100:80 } save sys config

3. To verify, use the following command:

list Itm pool

#### 8.4.8 Local Traffic (LTM) Virtual Server Creation (TMSH)

1. To configure a virtual server, use the following command syntax:

create ltm virtual Agility-LTM-VIP { destination 10.128.10.100:443 profiles add { clientssl http Agility-Lab-Access-Profile } vlans default source-address-translation { type automap } }

2. Configure as follows:

create ltm virtual Agility-LTM-VIP { destination 10.128.10.100:443 profiles add { clientssl http Agility-Lab-Access-Profile } vlans default source-address-translation { type automap } }

save sys config

3. To verify, use the following command:

list Itm virtual

## 8.5 Lab 3: General Troubleshooting

In this lab exercise, you will learn where to look and what to look at when an Access Policy is not successfully allowing access or not performing as intended.

## 8.5.1 Questions to ask yourself (LAB3)

- 1. Do we have proper Network Connectivity?
- 2. Are there any Upstream/Downstream Firewall Rules preventing APM to be reachable or to reach destination targets it requires to access?
- 3. Do we have DNS setup properly?
- 4. Do we have NTP setup properly?
- 5. Are we receiving any Warnings or Error messages when we logon?
- 6. Are there any missing dependencies?
- 7. Time to check on our Sessions under Manage Session Menu
  - (a) What can we see from the Manage Session Menu?
  - (b) If we click the Session ID link what more information is available?
  - (c) Is Authentication Successful or is it Failing?
  - (d) Is the user receiving the proper ENDING ALLOW from the Policy?
- 8. Time to Review the Reports information for the Session in question
  - (a) What information is available from the ALL SESSIONS REPORT?
  - (b) Can we review the Session Variables for the user's session from the ALL SESSION REPORT? If YES then Why however If NO then WHY?
- 9. Can the BIG-IP TMOS Resolve the AAA server by Hostname and by Hostname.Domain?
  - (a) Is the AAA reachable over the network, no Firewalls blocking communication from BIGIP Self-IP?

## 8.5.2 Verify DNS is setup from the CLI of the BIG-IP

Perform the following steps to verify DNS is correctly configured:

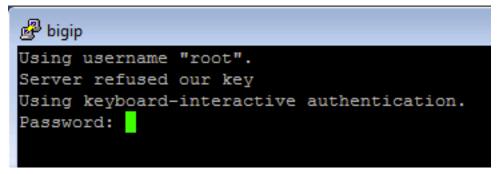


1. Click on the PuTTY (SSH client) to access the BIG-IP CLI

Section 2017 Putty Configuration		×
Category:		
Session	Basic options for your PuTTY se	ssion
Logging	Specify the destination you want to connect	et to
-Keyboard	Host Name (or IP address)	Port
Bell	10.128.1.245	22
─ Features ─ Window ─ Appearance	Connection type:	H 🔘 Se <u>r</u> ial
<ul> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	Load, save or delete a stored session Sav <u>e</u> d Sessions agilitylab Default Settings agilitylab	Load Saye Delete
	Close window on exit: Always Never Only on c	lean exit
About	<u>O</u> pen	<u>C</u> ancel

- 2. Click on the agilitylab Saved Session and click Load
- 3. The click on **OPEN**

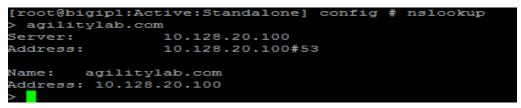
Alternatively, you can simply double-click on the agilitylab Saved Session to open the session



4. Logon as root with password default if necessary (you should logon automatically)

```
root@bigip1:Active:Standalone] config # dig agilitylab.com
 <<>> DiG 9.9.11-P1 <<>> agilitylab.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61961
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 4000
; QUESTION SECTION:
agilitylab.com.
                                        IN
                                                А
; ANSWER SECTION:
agilitylab.com.
                        600
                                IN
                                        А
                                                10.128.20.100
; Query time: 7 msec
; SERVER: 10.128.20.100#53(10.128.20.100)
; WHEN: Thu Jun 28 18:01:55 PDT 2018
; MSG SIZE rcvd: 59
[root@bigip1:Active:Standalone] config #
```

- 5. From the CLI type dig agilitylab.com and then press enter
- 6. The following results should be reviewed and verified.
- 7. If DNS is properly configured you should receive the returned IP address of 10.128.20.100



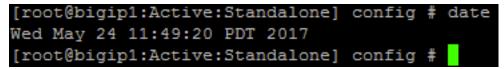
- 8. From the CLI type **nslookup** and then press enter.
- 9. Type agilitylab.com and then press enter
- 10. The following results should be reviewed and verified.
- 11. If DNS is properly configured you should receive the returned IP address of 10.128.20.100
- 12. Exit nslookup by typing exit

## 8.5.3 Verify NTP is setup from the CLI of the BIGIP

Perform the following steps to verify NTP is correctly configured:

[root@bigip:Activ remote	refid	st	t	when	poll	reach		
10.128.20.100							-8921.0	

- 1. From the CLI (via PuTTy –SSH Client) .... type ntpq –pn and then press enter.
- 2. The following results should be reviewed.



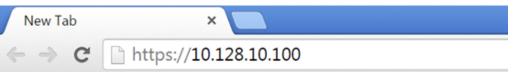
3. If time is out of sync by too much of an offset you can update the local time using the following command:

date MMDDhhmmYYYY

## 8.5.4 Manage Sessions within the Access Policy Manager menu

We use the Manage Sessions menu to view general status of currently logged in sessions, view their progress through a policy, and to kill sessions when needed.

SIEF I
--------



1. Open a USER session to APM through a new browser window by navigating to your first Virtual Server IP Address created in LAB I (10.128.10.100)

🗏 BIG-IP logout page 🛛 🗙 🦲	
← → C https://10.128.10.100	/vdesk/hangup.php3
Your session could not be established.	
The session reference number: ea45812d	
Access was denied by the access policy. This may be due to a failure to meet access policy requirements.	
If you are an administrator, please go to Access Policy >> Reports : All Sessions page and look up the session reference number displayed above.	
To open a new session, please click here.	

2. Did you receive an error message? If so, take note of the Session Reference Number

#### **TEST 1**

Access Policy » Manage Sess	ions			
🔅 🚽 Current Sessions				
Display Options				
Auto Refresh	Disabled   Refresh			
Refresh Session Table				
Total Active Sessions				
Active Session Count	0			
•	Search			
Status	Session ID	+ Logon	Client IP	¢
No records to display.				
Kill Selected Sessions				

- 1. In the browser window, you are using to manage the BIG-IP, navigate to Access ? Overview > Active Sessions menu.
- 2. Review the Manage Sessions screen, is there an Active Session? If not then why?

ST	EΡ	2

	Access		Use the following additio configured the system us	
[	Overview	F	System Device Certi     DNS	1
	Profiles / Policies	۱.	Access Profiles	
	Authentication	×.	(Per-Session 🕑 🗘 Policies)	
	Single Sign-On	÷	Per-Request	

1. Now open the APM Visual Policy Editor (VPE) for the policy created/loaded in LAB I by navigating to Access ? Profiles/Policies -> Access Profiles (Per-Session Policies) menu.

Acc	ess Policy		Profiles : Access Pr	offices List								
۰	- Access	Profile List										
_												
1			Sea	rch							C	reale Import
1	· Status	+ Name			Application	· Profile Type	Access Policy	Export	Copy	Logs	Virtual Servers	· Parttion / Path
8	1	Agility-Lab	Access-Profile			AI	D Edit	Export	Copy	default-log-setting	Agility-LTM-VIP	Common
	. (M. 1	access				Al	(none)	(none)	(none)			Common

2. Then click the Edit link in the row that has the name of your Access Profile you are working with currently. (Agility-Lab-Access-Profile)

<u>f5</u>		
Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start Deny		
Add New Macro		

3. This will either launch a new browser or new tab depending on your browsers settings to display the APM Visual Policy Editor (VPE). The first policy we created was never edited to add any additional tasks that would instruct APM on what Actions it would need to take/enforce throughout a Policy Execution for the user's Session. So we will now adjust the policy and retest to see if we receive some new results.

6		
Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start + Deny		
Add New Macro		

4. Click on the + symbol between the Start and ending Deny objects.

Beg	in typing to search		
∫ Logo	n Authentication Assignme	ent Fndpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
0	Citrix Logon Prompt	Configure logon options for Citrix clients	
$\odot$	External Logon Page	Redirect user to externally hosted form-based web logon page	
0	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication	
$\bigcirc$	HTTP 407 Response	HTTP 407 Response for Basic or SPNEGO/Kerberos authentication	
۲	Logon Page	Web form-based logon page for collecting end user credentials (used with most deployments)	
$\bigcirc$	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication	
0	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials	
$\bigcirc$	VMware View Logon Page	Display logon screen on VMware View clients	
Cano	Add Item	He	lp

5. This will pop up the Actions window where we can select from several Actions we wish to associate with our policy. On the Logon tab select the **Logon Page** radio button and then click the **ADD ITEM** button at the bottom of the page.

Properties Branch Rule	8			
Name: Logon Page				
Logon Page Agent				
Split domain from full Us	ername No 🔻			
CAPTCHA Configuration	None 💌			
Type	Post Variable Name	Session Variable Name	Values	Read Only
1 text 💌	username	username		No 💌
2 password 💌	password	password		No 💌
3 none 💌	field3	field3		No 💌
4 none 💌	field4	field4		No 💌
5 none 🔻	field5	field5		No 💌
5 Junie 🔛	liedo	lieus		1.00
Customization				
	en 💌		Reset all	defaults
Customization Language	en 💌		Reset all	defaults
Language	en  Secure Logon for F5 Networks		Reset all	defaults
	,		Reset all	defaults
Language Form Header Text	,		Reset all	defaults
Language	Secure Logon for F5 Networks		Reset all	defaults
Language Form Header Text Logon Page Input Field #1	Secure Logon for F5 Networks Username		Reset all	defaults 
Language Form Header Text Logon Page Input Field	Secure Logon for F5 Networks		Reset all	defaults 
Language Form Header Text Logon Page Input Field #1 Logon Page Input Field	Secure Logon br> for F5 Networks Username Password		Reset all	defaults
Language Form Header Text Logon Page Input Field #1 Logon Page Input Field	Secure Logon for F5 Networks Username		Reset all	defaults 
Language Form Header Text Logon Page Input Field #1 Logon Page Input Field #2	Secure Logon br> for F5 Networks Username Password		Reset all	defaults 
Language Form Header Text Logon Page Input Field #1 Logon Page Input Field #2	Secure Logon br> for F5 Networks Username Password		Reset all	defaults 
Language Form Header Text Logon Page Input Field #1 Logon Page Input Field #2 Logon Button	Secure Logon > for F5 Networks Username Password Logon		Reset all	defaults 

6. Click the **SAVE** button on the Logon Page properties window.

🚯 🕴 Apply Ac	ccess Policy		
Access Policy: /	Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start falback +- Lo	igon Page falback + →> Deny		
Add New Macro			
7. Then click t	he <b>Apply Access Policy</b> link on the to	op left of the	e page.
TEST 2			
New Tab	×		
$\  \   \leftrightarrow \  \   \mathbf{C}$	https://10.128.10.100		

1. Restart your session to APM. (https://10.128.10.100)

|--|

# Secure Logon for F5 Networks

Username	

Password

Logon

2. Did you receive and error this time? Or did you receive a Logon Page?

Acces	ss » Ove	rview	: Active Ses	sions								
₿ -	Active S	ession	s Access	Reports	OAuth R	leports 🔻	SWG Reports 🔹	F5 Adaptive Authentication	on (MFA) Reports	vent Logs	•	
Displa	y Options											
Auto	Refresh		[	5 seconds	▼ Sto	p Refresh						
Refre	sh Sessior	n Table	;									
Total A	ctive Ses	sions										
Active	e Session (	Count	1									
*				Se	earch							
	<ul> <li>Status</li> </ul>	•	Session ID	Variables	▲ User		Virtual Server	Start Time	Expiration	Bytes In	Bytes Out	≑ Se
		٥	700af5ea	View	n/a	10.128.10.1	/Common/Agility-LTM-VI	P 2018-06-28 18:11:53	2018-06-28 18:12:31	1 3020	5840	n/a
LIZE O			7									

- 3. Open your browser or tab for managing APM and open the Active Sessions menu again.
- 4. Is there now an Active Session displayed on the page? If you were already on this page you may need to click the Refresh Session Table button.
- 5. What does the Status Icon look like? Is it a Green Circle or a Blue Square?
- 6. Is your username displayed in the Logon column?
- 7. Click on the Session ID for your session, this will open up a Session Details window.

Session Details - f49bfabb 🛞							
😣 Export to CSV File	🔛 Show in Popup Window 🛐 View Report Constraints Current default report name: "All Sessions"						
Local Time	Log Message						
2017-05-24 12:58:46	/Common/Agility-Lab-Access-Profile:Common:f49bfabb: Received User-Agent header: Mozilla/5.0 (Windows NT 6.1; Win64; x64) Apple/WebKit/537.36 (KH						
2017-05-24 12:58:46	/Common/Agility-Lab-Access-Profile:Common:f49bfabb: New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener /Common/Ag.						

8. In the Session Details window, we can see some information about the session up to the point that the policy has executed so far.

•	•	
Built In Reports	+	
Custom Reports	+	4 4 Page 1 of 1 ▶ ▶   22

9. Further down there is a reports section titled **Built-In Reports**, click that to open the list of built in reports.

∃ Session Reports
All Sessions
Bad IP Reputation Sessions
Current Sessions
Session Details
Session Variables
Sessions by Geolocation

10. Scroll down to see the list of **Session Reports** and click the **Current Sessions** line and select **Run Report** from the pop up window.

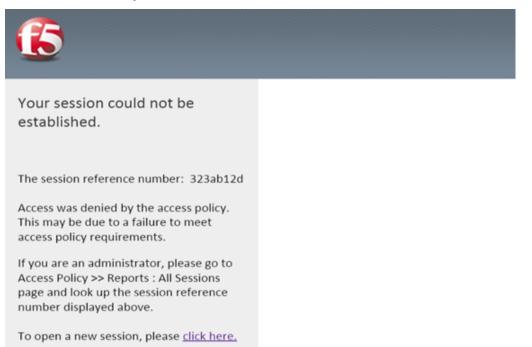
Session Details - 4f38124d 🗷 Current Sessions 🗷							
😣 Export to CSV File	Show in P	opup Window	View Report Constraint	S Current default re			
Local Time	Session ID	Logon	Session Variables	State			
2015-06-14 23:54:13	4F38124D		View Session Variables				

11. Do you see your Session ID displayed in the list of current sessions? If not then why?

**TEST 3** 

Secure Logon for F5 Networks	
Username	
student	
Password	
Logon	

- 1. Return to the browser or tab you are using for access to https://10.128.10.100. Restart a new session if necessary.
- 2. Next logon to the APM Logon page with:
  - Username: student
  - Password: password



3. Did you receive and error after logging on? If so note the Session Reference Number.

Access Policy » Manage Ses	sions			
🔅 👻 Current Sessions				
Display Options				
Auto Refresh	Disabled	Refresh		
Refresh Session Table				
Total Active Sessions				
Active Session Count	0			
*	Sear	ch		
🖌 💌 Status 🗭 🕈 Sess	ion ID Variable	es 🔺 User	Client IP	⇒ Star
No records to display.				
Kill Selected Sessions				

4. Review the Manage Sessions menu, is your session listed?

Access		Use the following a configured the syste	
Overview >	1	Active Sessions	tif
Profiles / Policies	1	Access Reports	
Authentication >	0	OAuth Reports  🖞	. ⊳ n
Cinala Cian On		N/C Baparta	

5. Navigate to Access -> Overview ? Access Reports. When prompted Click Run Report.

All Sessions									
😣 Export to CSV File   🧾 Show in Popup Window 🛐 View Report Constraints   🛼 Set to default report   Current default report name:									
Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent		
2015-06-15 06:17:55	323AB12D	student	N	View Session Variable	<u>s</u>				

6. Do you see your Session ID listed in the list of All Sessions? Is the username listed in the Logon column?

All Sessions 🗷	Session Details - 323AB12D
😣 Export to CSV File	🔝 Show in Popup Window 🛐 View Report Constraints   🛼 Set to default report   Cu
Local Time	Log Message
2015-06-15 06:17:55	Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%206.1%3b%20WOW)
2015-06-15 06:17:55	Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode: Fu
2015-06-15 06:17:55	New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener
2015-06-15 06:22:48	\N: Session deleted due to user logout request.
2015-06-15 06:22:48	Username 'student'
2015-06-15 06:22:48	Following rule 'fallback' from item 'Logon Page' to ending 'Deny'
2015-06-15 06:22:48	Access policy result: Logon_Deny
2015-06-15 06:23:26	Session statistics - bytes in: 8530, bytes out: 12420

- 7. Click the Session ID to open the Session Details window.
- 8. Do you now see more information in this Sessions Details compared to the previous one we reviewed?
- 9. Is the username listed in the details?
- 10. In the Session Details screen we can see some important troubleshooting information, for example just below the username row we see a line that states that the Policy followed a path or branch called Fallback out of the Logon Page object to an Ending "Deny" thus the Access Policy Result was Logon_Deny.

All Sessions	Session De	etails - 323A	812D 🗵				
😣 Export to CSV File	🧾 Show in P	opup Window	View R	eport Constraints   🛼	Set to default r	eport Current de	efault report name
Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent
2015-06-15 06:17:55	323AB12D	student	N	View Session Variables			

- 11. Now click back on the All Sessions tab at the top.
- 12. In the row for this session look to the right of the Logon column. You will see the next column states that the session is not Active. Now click the View Session Variables link in the next column.

All Sessions 🗷	Session Variables - 323ab12d	×
😣 Export to CSV File	🧾 Show in Popup Window 🗾 Vi	ew Report Constraints   🛼 Set to default report
Local Time	Session Variable Name	Session Variable Value

13. Do you see a lot of information recorded for Session Variables for this session? If not, then why?

## 8.6 Lab 4: Visual Policy Editor (VPE) & Session Variables

This lab will go a little deeper into understanding the Visual Policy Editor and Session Variables.

#### 8.6.1 Questions to ask yourself (LAB4)

• Does the VPE Flow look correct?

- Does the VPE have the proper ENDING assigned to the appropriate BRANCH?
- · Are your connection attempts following the intended VPE BRANCH/PATH during your test?
  - How could you alter the VPE to allow for better trouble shooting or pausing of a policy execution and termination?
- · How can I pause the Policy Execution or Termination to review the session variable in Reports?
- What are VPE Actions?
- · Are the Correct Session Variables being sent to the AAA Object?
- How can we GET or SET Session Variables in the VPE?
- How could I preserve the originally requested URI from the Client to pass to the internal server after APM authentication has complete?

#### 8.6.2 Visual Policy Editor (VPE) Workflow, Actions, Branches, Endings

The Visual Policy Editor (VPE) is a screen on which to configure an access policy using visual elements. We have used it a few times already throughout our previous labs. This is meant to both review and explain in a bit more detail what the available Visual Policy Editor conventions are.

This table provides a visual dictionary for the Visual Policy Editor (VPE).

#### Visual Policy Editor (VPE) Visual Dictionary

Element type	Description	Visual ele- ment
		Start falback + Deny
Initial Ac- cess Policy	When an access profile is created, usually an initial access policy is also created.	Add New Macro
Start	Every access profile contains a start.	Start -
Branch	A branch connects an action to another action or to an ending.	fallback
Add an ac- tion	Clicking this icon causes a screen to open with available actions for selec- tion.	-+-
Action	Clicking the name of an action, such as Logon Page, opens a screen with properties and rules for the action. Clicking the x deletes the action from the access policy.	- Logon Page
Action that requires some con- figuration	The red asterisk indicates that some properties must be configured. Click- ing the name opens a screen with properties for the action.	* <u>AD Auth</u>
Ending	Each branch has an ending: Allow or Deny.	Allow
Configure ending	Clicking the name of an ending opens a popup screen.	Select Ending: Allow  Oneny  Deny
Add a macro for use in the access policy	Opens a screen for macro template selection. After addition, the macro is available for configuration and for use as an action item.	Add New Macro
Macro added for use	Added macros display under the access policy. Clicking the plus (+) sign expands the macro for configuration of the actions in it.	Add New Macro + Macro: AD_Auth (Terminal
		Access Policy: / Common/plain Edit Endings (Endings: Abu Start / faback + (20. Auti) Oct + ->- Dear Add New Macro C Macro: AD_Auth Rename / Settings Edit Terminals
Macro- call in an Access Policy	Clicking the <i>Macrocall</i> name expands the <i>Macro</i> in the area below the <i>Access Policy</i> .	m (abock * 5002454) + → - 000 *AD3187 = → - 000

#### 8.6.3 Pausing the APM Policy Execution for Troubleshooting – The Message Box

Now that we have reviewed/refreshed our memory on VPE conventions lets edit our policy we were previously working on to add some more actions. This section we show a great tool for troubleshooting a policy that may have been reaching an ENDING DENY and closing the APM session too rapidly for proper inspection during the troubleshooting phase.

#### STEP 1

Acce	Access Policy # Access Profiles : Access Profiles List											
۰ م	Access F	hofile List Access Policy Sync	CAPTCHA Configuration List	NTLM -								
ŀ.		Se	arch							(	Create	import
4	· Status	- Name			• Application	• Profile Type	Access Policy	Export	Серу	Virtual Servers	· Par	tition / Path
	<b>P</b>	Agiity-Lab-Access-Profile				Al	Ø Edt.	Export	Copy	Agiity-LTM-VIP	Come	non

1. Navigate to Access ? Access Profiles ? Profiles/Policies -> Access Profiles (Per-Sessions Policies). Click Edit next to **Agility-Lab-Access-Profile** to open the Visual Policy Editor (VPE).

Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start fallback + - Logon Page fallback + ->>> Deny		

Add New Macro

2. After the Logon Page object, on the fallback branch, click the + symbol to open the Actions window.

[100	n Authentication Assignme	et ] [Endpoint Security (Server-Side) ] [Endpoint Security (Clent-Side) ] General Rurpose
	Decision Box	Oreste a custom decision page with two choices to display to the user
0	Email	Configure Email messages for reporting
	Empty	An Empty Action for constructing custom Branch Rules
	Rule Event	Raises an Rule ACCESS_POLICY_AGENT_EVENT event for use with custom Rules
	Local Detabase	Allows read/write access to a local on-box user database
0	Logging	Log custom messages and session variables for reporting and troubleshooting
•	Message Box	Create a custom message to display to the end user, with prompt to continue
Car	cel Add Zem	Help

3. Click on the **General Purpose** tab and then click the radio button next to **Message Box** and click the **ADD ITEM** button at the bottom of the page.

Properties Branch	1.Rules	
Name: Message Box		
Message Box		
Customization		
Language	en 💌	Reset all defaults
Message	Please click the link below to continue.	
Link	Click here to continue	
Cancel Save		Help

4. Click the SAVE button on the next window

Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start fallback + Logon Page fallback +	Deny	

- Add New Macro
- 5. Now client the ending Deny.

Select Ending:	
Allow □	
Deny	
Cancel Save	Help

6. In the pop-up window change it to Allow and click the **SAVE** button.

6	Apply Access Policy		
Access	Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Aloss, Deny [default])

7. Then click the Apply Access Policy link at the top left.

TEST 1

Secure Logon for F5 Networks	
Username	
student Password	
••••••	

- 1. Return to the browser or tab you are using for access to https://10.128.10.100. Restart a new session if necessary.
- Username: student
- Password: password



Logon

# Please click the link below to continue.

## Click here to continue

- 2. Did we receive an error this time after the logon page?
- 3. Did the Message Box display?

Access » Overview : Active Sessions									
🚓 🚽 Active Sessions					on (MFA) Reports Eve		-		
Display Options									
Auto Refresh	5 seconds	<ul> <li>Stop Refresh</li> </ul>							
Refresh Session Table									
Total Active Sessions									
Active Session Count	1								
* Search									
Status 🛨 🗢 Se	ession ID Variables	▲ User	♦ Virtual Server	Start Time	Expiration	Bytes In	Byte     Byte     Second seco		
🔲 💼 🖽 6e9e	e2b15 View	student 10.128.10.1	/Common/Agility-LTM-VIF	2018-06-28 18:18:48	2018-06-28 18:19:24	0	0		
Kill Selected Sessions									

- 4. Keep the message box display there and move to the other browser to review the Manage Sessions menu.
- 5. Does the Manage Sessions menu show the Username this time?
- 6. Is the Status showing a Blue Square or Green Circle? Why?

Session Details - 58098d87 🗵						
😣 Export to CSV File	I 🔝 Show in Popup Window 🛐 View Report Constraints Current default report name: "All Sessions"					
Local Time	Log Message					
2015-06-24 21:31:16	Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%206.1%3b%20WOW64)%20Apple					
2015-06-24 21:31:16	Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode: Full Javascript \$					
2015-06-24 21:31:16	New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener /Common/Agility-					
2015-06-24 21:31:31	Username 'student'					
2015-06-24 21:32:09	N: Session deleted due to user inactivity or errors.					

- 7. Click the session ID to review the details for any new messages.
- 8. If things worked correctly you should see a message in the details stating, "Session deleted due to user inactivity or errors"

```
k the link below to
```

#### Session Expired/Timeout

Due to user inactivity, your session expired. Click the following link to start a new session.

continue

> Start a new session

9. If you look back at the other browser window you should notice a Session Expired/Timeout message is being displayed.

#### STEP 2

Acc	scess Policy + Access Profiles : Access Profiles List													
0	Access I	Profile List Access Policy 5	iyne Cr	APTCHA Configuration List	NTLM +									
٢	Search Create import													
4	· Status	- Name				• Application	· Profile Type	Access Policy	Export	Сору	Virtual Servers	0	Partitio	on / Path
	<b>P</b>	Agiity-Lab-Access-Profile					Al	D Edt.	Export	Copy	Agility-LTM-VIP	c	ommor	1

1. Navigate back to Access ? Profiles/Policies ? Access Profiles (Per-Session Policies). Click on Agility-Lab-Access-Profile

Access Policy » Access Profiles : Access Profiles List » Agility-Lab-Access-Profile							
O - Properties	SSO / Auth Domains	Access Policy	Logs				
General Properties							
Name	Agility-Lab-Ac	cess-Profile					
Partition / Path	Common	Common					
Parent Profile	access						
Profile Type	AI						
Settings				Custom			
Inactivity Timeout	900	seconds					
Access Policy Timeout	30	seconds		V			

- 2. Access Policy Timeout from 30 seconds back to **300** seconds by removing the check from the custom column.
- 3. Click the **UPDATE** button at the bottom of the page.

	Apply Acces	s Policy									
Main	Help	About	Acces	Access Policy » Access Profiles : Access Profiles List » Agility-Lab-Access-Profile							
Magaza Statisti	cs		÷ -	Properties	SSO / Auth Domains	Access Policy	Logs				

4. Click Apply Access Policy link at the top left of the page.

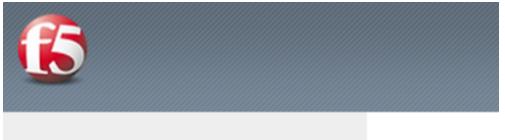
Access Policy » Access Profiles : Access Profiles List									
	Access F	Profile List	Access Policy Sync	CAPTCHA Configuration List	NTLM	•			
ŀ			Sea	arch					
	Status A Name								
-	Image: Agility-Lab-Access-Profile								
Apply Access Policy									

5. Finalize the update by confirming the box is checked next to the profile and clicking **APPLY ACESS POLICY** 

#### TEST 2

Secure Logon		
for F5 Networks		
Username		
student		
Password		
••••••		
Logon		

1. Now go back and restart the user session and logon.



# Please click the link below to continue.

## Click here to continue

- 2. Do NOT click the message box link "Click here to continue"
- 3. Leave the message box message displayed for the time.

fotal Ac	tive Sessions						
Active S	Session Count	1	1				
		Sea	rch				
~	<ul> <li>Status</li> </ul>	Session ID	▲ Logon	Client IP			
		4121b0a9	student	10.128.10.1			

4. Go to the other browser/tab and open the Manage Sessions menu.

- 5. Your session should be there but the Status icon should still be a Blue Square.
- 6. Click on your Session ID

Reports Browser		Session Details - 412100a9 ×
Fevorites		🕭 Export to CEV File 🛛 🔄 Show in Popup Window 📳 View Report Constraints: Current default report name: "All Sessions"
Delete Favorite	E Run	Local Time Log Message
		2015-06-24 21 57:10 Received User-Agent header: Mozille%26 0%20(Windows%20NT%206.1%30%20W0W64/%20Apple
		2015-06-24 21 57:10 Received client info - Type: Mobile Version: 5 Platform: Win7 CPU: unknown UI Mode: Pull Javascript
		2015-06-24 21 57:10 New session from client IP 10.128.10.1 (ST+/CC+/C+) at VIP 10.128.10.100 Listener /Common/Agility
		2015-06-24 21:57:16 Usemame 'student'
-		
Built In Reports		
Custom Reports		H ( Page toft) > H Ø

7. Click Built-in Reports

Session Reports			
All Sessions			
Bad IP Reputation Sessions			
Current Sessions			
Session Details	Ŧ		

8. Click on All Sessions report, then choose Run Report on the pop-up menu.

Session Details - 3	adaf206 📧	All Sessions	×				
😣 Export to CSV File	Show in F	opup Window	🛛 View R	eport Constraints Curren	t default repor	t name: "All Sessi	ons"
Local Time	Session ID	Logon	Active	Session Variables	State	Country	¢
2015-06-24 22:07:04	3ADAF206	student	Y	View Session Variables			

9. Click the Session Variables for your current session.

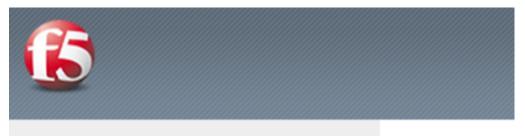
All Sessions 🗷 Session Var	iables - 10f1257e 🛞	
ariable Name	Variable ∀alue	√ariable ID
😑 session		session
⊳ 🧰 access		session.access
⊳ 🧰 client		session.client
⊒ createdfrom	ACCESS	session.createdfrom
E ha_unit	7e1185d64ff41bba33ba5dba81bde70b	session.ha_unit
inactivity_timeout	900	session.inactivity_timed
Iogon		session.logon
partition_id	Common	session.partition_id
policy		session.policy
⊳ 🧰 rest		session.rest
▷ 🧰 server		session.server
🚍 snapshotid	3fe322e12cc_400000000000000000000000000000000000	session.snapshotid
⊳ 🧰 stats		session.stats
📃 timeout	eval_timed_out	session.timeout
🗅 🧰 ui		session.ui
⊳ 🧰 user		session.user

10. Do you now have Session Variables being displayed for this session? If so why?

All Sessions 🛞 Session Variables - 10f1257e 🗵									
终 Export to CSV File   🧾 Show in Popup Window 🛐 View Report Constraints   🎠 Set to default report   Current default report name: "All Sessions"									
Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent	Virtual IP	Client IP
2017-05-24 13:38:35	10f1257e	student	Y	View Session Variables				10.128.10.100	10.128.10.1

11. Click the All Sessions tab and look at the column labeled Active. Does it show a Y or N in the column?

Note that session variables will only be displayed for Active sessions. Since you placed a message box in the VPE to pause policy execution the session is seen as active. This provides you the ability to now review Session Variables that APM has collected up to this point in the policies execution.



# Please click the link below to continue.

## Click here to continue

12. Now in the user browser click the link in the Message Box.

If it timed out then restart and this time click through the message box link.

T	Total Active Sessions													
	Active Ses	ssion (	Cour	t f	1									
*	* Search													
	🗸 🔽 St	tatus	٠	Session ID	Variables	▲ User	Client IP	Start Time	Expiration	Bytes In	Bytes Out	Session Type	Profile Name	\$
1			۵	10f1257e	View	student	10.128.10.1	2017-05-24 13:38:34	2017-05-24 13:56:13	2342	790	ltm_apm	/Common/Agility-Lab-Access-Profile	
	Kill Selected Sessions													

13. Now review the Active Sessions menu and note what icon is shown in the status column. Green Circle finally? Success!!

Session Details - 10f1257e 🛞						
😣 Export to CSV File	🔛 Show in Popup Window 📳 View Report Constraints Current default report name: "All Sessions"					
Local Time	Log Message					
2017-05-24 13:38:35	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Received User-Agent header: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KH					
2017-05-24 13:38:35	/Common/Agility-Lab-Access-Profile:Common:10f1257e: New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener /Common/A					
2017-05-24 13:38:58	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Username 'student'					
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Following rule 'fallback' from item 'Message Box' to ending 'Allow'					
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Access policy result: LTM APM_Mode					
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Received client info - Hostname: Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode					

14. If you now click the Session ID you will see that the Policy has reached an ending Allow thus the Access Policy Result is now showing we have been granted LTM+APM_Mode access.

ariable Name	Variable Value	Variable ID
🔁 session		session
⊳ 🧰 access		session.access
assigned		session.assigned
client		session.client
E createdfrom	ACCESS	session.createdfrom
📰 ha_unit	7e1185d64ff41bba33ba5dba81bde70b	session.ha_unit
inactivity_timeout	900	session.inactivity_timeo
Iogon		session.logon
partition_id	Common	session.partition_id
policy		session.policy
⊳ 🧰 rest		session.rest
b iserver		session.server
📰 snapshotid	3fe322e12cc_400000000000000000000000000000000000	session.snapshotid
≡ state	allow	session.state
⊳ 🧰 stats		session.stats
E timeout	estab_timed_out	session.timeout
▷ 🧰 ui		session.ui

15. Now open the All Sessions report once more to review the Session Variables collected.

4 😋 logon		session.logon
Common/Agility-Lab-Acces	s-Profile_ac	session.logon./Common/Agility-Lab-Access-Profile_ac
⊳ 🧰 last		session.logon.last
⊳ 🧰 page		session.logon.page
= partition id	Common	session partition id

16. Click the logon folder in the Session Variables page that opens for your session.

4 🔄 logon		session.logon
Common/Agility-Lab-Access-Profile_ac		session.logon./Common/Agility-Lab-Access-Profile_ac
4 🚞 last		session.logon.last
E logonname	student	session.logon.last.logonname
≡ result	1	session.logon.last.result
= username	student	session.logon.last.username
⊳ 🧰 page		session.logon.page
	· · · · · · · · · · · · · · · · · · ·	

17. Click the folder icon named *last* to expand its contents.

Notice on the left column labeled Variable Name above and to the right the next column is Variable Value and the third column is Variable ID. If you look at the Variable Name of username you will see to the right its value is recorded as student as you entered it in the logon page. The next column displays APM's matching session Variable ID for this information. You will see that the naming convention follows the session hierarchy starting with session. then the first folder logon. then the next folder last. then finally the Variable Name of Username.

We will use some session variables in the next lab to GET and SET information for the users session.

#### 8.6.4 Session Variables – Setting and Retrieving (Some Quick Information)

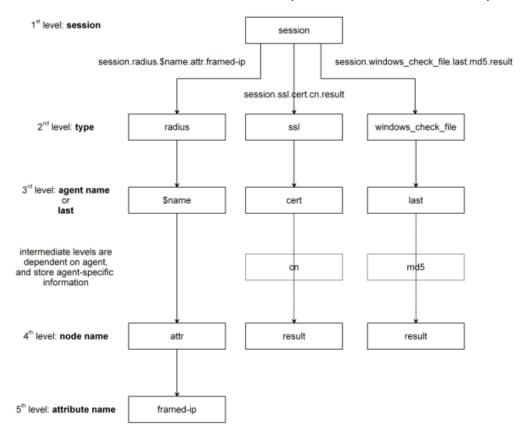
This section will provide some guidance on how to both retrieve and set session variables within a policy for a user's session. Session Variables are very useful in many areas of policy execution. They can be used to assist in areas like authentication or single sign-on or assigning resource items for users based on information APM can collect from the backend AAA server and its associated directory.

Currently cached session Variables are available in APM Reports for review by an administrator. Additional available variables can always be found in the APM Configuration Guides. What is really nice is that APM is not limited to only having awareness of Session Variable it collects from the user session establishment or from the AAA server, administrators can actually create or set their own custom session variables for

use within a policy. This means that an administrator could create new session variables via the VPE's Variable Assign action or session variables could even be set from an iRule attached to a virtual server. This means that information that the LTM VIP can see or be gathered via an iRule could then be set as a session variable that could then be retrieved and used within the VPE.

### **About Session Variable Names**

The name of a session variable consists of multiple hierarchical nodes that are separated by periods (.):



### **Session Variable Reference**

APM Session Variable references are provided in APM documentation. Current release information can be found at the following link: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/ apm-visual-policy-editor-13-0-0/5.html

### **Partial Session Variable list**

ACTION ITEM	SESSION VARIABLE	TYPE	DESCRIPTION
Denied Ending	session.policy.result	string	Access policy result: the access policy ended at Deny. The valu is access_denied.
Redirect Ending	session.policy.result	string	Access policy result: the access policy ended at Redirect. The value is redirect.
	session.policy.result.redirect.url	string	URL specified in the redirect, for example, http://www.siterequest.com.
llowed Ending	session.policy.result	string	Access policy result: the access policy ended at Allow. The valu is allowed.
	session.policy.result.webtop.network_access.autolaunch	string	Name of the resource that is automatically started for a network access webtop.
	session.policy.result.webtop.type	string	Type of webtop resource: network_access or web_application
ession management	session.ui.mode	enum	UI mode, as determined by HTTP headers.
	session.ui.lang	string	Language in use in the session, for example "en" (English).
	session.ui.charset	string	Character set used in the session.
	session.client.type	enum	Client type as determined by HTTP headers: portalclient or "Standalone".
	session.client.version	string	
	session.client.jailbreak	bool	Mobile device is jailbroken/rooted:
			• 0 - No • 1 - Yes
	session.client.js	bool	Client is capable of executing JavaScript:
	session.chenc.js	0001	• 0 - No
			• 1 - Yes
	session.client.activex	bool	Client is capable of running ActiveX Controls:
			• 0 - No
			• 1 - Yes
	session.client.plugin	bool	
	session.client.platform	string	Client platform as determined by HTTP headers:
			"Android"
			"ChromeOS"
			• "iOS""
			• "Linux""
			• "MacOS""
			• "Win10"
			• "Win2k"
			• "Win2k""
			• "Win7"
			<ul> <li>"Win8.1"</li> <li>"Win8"</li> </ul>
			"WindowsPhone"
			"WinLH"
			• "WinNT""
			"WinVI""

# Session Variable Categorization

While these are not formal categories, Session Variables fall under three general categories:

Category	Examples
Variables returned by Access Policy actions	<ul> <li>Active Directory query results</li> <li>Antivirus Check results</li> <li>Windows Info and Registry check results</li> </ul>
Special purpose user variables	<ul> <li>Lease Pools</li> <li>Client IP assigned to a client session</li> <li>Username and Password</li> </ul>
Network access resource variables and attributes	<ul> <li>Split tunneling</li> <li>DNS Settings</li> <li>Compression, etc.</li> </ul>

### Active Session Variables

Below is a short breakdown of information gathered and cached during an Active session. Additional information can be gathered from the results of End Point checks when they are put into a policy. These would display as folders like check_av or check_fw if the actions were added to the policy

Session Details - b8ac2b16 All Sessions Session	Variables - c35c7fd6 🙁				
Variable Name	Variable Value				Variable ID
D access					session.access
assigned		Client			session.assigned
Image: Contemport of the second se		Browser			session.client
n createdfrom	ACCESS	Information			session.createdfrom
nd and	timed_out				session.end
E ha_unit	f4b783582d1f19d75076daec1bc225dc				session.ha_unit
inactivity_timeout	900				session.inactivity_timeout
a 🔤 logon					session.logon
Common/Agility-Lab-Access-Profile_act_logon_page_ag			Name of	1	session.logon./Common/Agility-
a 😁 last			Variables for		session.logon.last
Iogonname	student		expressions		session.logon.last.logonname
result	1 K		orrules		session.logon.last.result
usemame	student				session.logon.last.username
> 🦳 page					session.logon.page
D Dicy					session.policy
Image: Provide the second s		T I			session.rest
Image: Server		Credentials &			session.server
snapshotid	f483479462f_40000000000000000000	SSO			session.snapshotid
n state	allow				session.state
Image: Stats					session.stats
Image: Second					session.ui
þ 🦳 user					session.user

### Session Variable Manipulation via TCL

Variables can be parsed, modified, manipulated, etc using TCL. Although the tables below are not an exhaustive reference for writing and using TCL expressions, it includes some common operators and syntax rules.

### **Standard Operators**

You can use TCL standard operators with most BIG-IP® Access Policy Manager® rules. You can find a full list of these operators in the TCL online manual, at http://www.tcl.tk/man/tcl8.5/TclCmd/expr.htm. Standard operators include:

Op-	Description
er-	
a-	
tor	
- +	Unary minus, unary plus, bit-wise NOT, logical NOT. None of these operators may be applied to
~ !	string operands, and bit-wise NOT may be applied only to integers.
**	Exponentiation. Valid for any numeric operands.
* /	Multiply, divide, remainder. None of these operators may be applied to string operands, and re-
%	mainder may be applied only to integers. The remainder will always have the same sign as the
	divisor and an absolute value smaller than the divisor.
+ -	Add and subtract. Valid for any numeric operands.
<<	Left and right shift. Valid for integer operands only. A right shift always propagates the sign bit.
>>	
< >	
<=	
>=	
	Boolean less than, greater than, less than or equal to, and greater than or equal to. Each operator
	produces 1 if the condition is true, 0 otherwise. These operators may be applied to strings as well
	as numeric operands, in which case string comparison is used.
==	Boolean equal to and not equal to. Each operator produces a zero/one result. Valid for all operand
!=	types.
eq	Boolean string equal to and string not equal to. Each operator produces a zero/one result. The
ne in	operand types are interpreted only as strings. List containment and negated list containment. Each operator produces a zero/one result and
ni	treats its first argument as a string and its second argument as a Tcl list. The in operator indicates
	whether the first argument is a member of the second argument list; the ni operator inverts the
	sense of the result.
&	Bit-wise AND. Valid for integer operands only.
<u>م</u>	Bit-wise exclusive OR. Valid for integer operands only.
1	Bit-wise OR. Valid for integer operands only.
* &&	Logical AND. Produces a 1 result if both operands are non-zero, 0 otherwise. Valid for boolean
	and numeric (integers or floating-point) operands only.
	Logical OR. Produces a 0 result if both operands are zero, 1 otherwise. Valid for boolean and
	numeric (integers or floating-point) operands only.
x?y:	z If-then-else, as in C. If x evaluates to non-zero, then the result is the value of y. Otherwise the
-	result is the value of z. The x operand must have a boolean or numeric value.

# **Standard Operators**

A rule operator compares two operands in an expression. In addition to using the TCL standard operators, you can use the operators listed below.

Operator	Description
contains	Tests if one string contains another string.
ends_with	Tests if one string ends with another string
equals	Tests if one string equals another string
matches	Tests if one string matches another string
matches_regex	Tests if one string matches a regular expression
starts_with	Tests if one string starts_with another string
switch	Evaluates one of several scripts, depending on a given value

# **Logical Operators**

Logical operators are used to compare two values.

Operator	Description
and	Performs a logical and comparison between two values
not	Performs a logical not action on a value
or	Performs a logical or comparison between two values

### **Getting/Setting Session Variables**

During the pre-logon sequence, using the Visual Policy Editor (VPE) you can get and set Session Variables. The following are some quick examples.

- To set/modify a variable: Variable Assign action
- To **get** a value the last username entered by a user, use expr or return: expr { [mcget {session.logon.last.username}]]

**expr** evaluates an expression, whereas **return** simply returns the result. For example, we have a two custom variables:

- session.custom.value1 = 3
- session.custom.value2 = 4

Using **expr** we can construct the following expression, this would return a value of 7 (i.e. the evaluation of 3+4):

expr { "[mcget session.custom.value1] + [mcget session.custom.value2]" }.

Using return we can construct the following expression, this would return simply "3+4" as shown.

return { "[mcget session.custom.value1] + [mcget session.custom.value2]" }

### **Using iRules**

In all the "Access" events

ACCESS::session data get/set "variable_name" ["value"]

#### **Set Secure Variables**

You can also set Secure Variables. The value of a secure session variable is stored as encrypted in the session db. The value is not displayed as part of session report in UI, nor is it logged as part of logging agent. Secure variables require the -secure flag, both for mcget and access::session data get/set.

Custom Variable	▼ Secure ▼	
	*	
4	▼ ↓	

Review these two examples below. The first is a Variable Assign action that is SETTING the Session Variable ID of "session.logon.last.upn" with the information extracted from an x509 Client Certificate that was presented by the user's computer/browser upon connection to the VIP.

Sets the information extracted from the Certificate to a custom variable named session.logon.last.upn	× •	<pre>set e_fields [split [mcget {session.ssl.cert.x509extension}] "n"]; foreach qq \$e_fields {     if {[string first "othername:UPN" \$qq] &gt;= 0} {         return [string range \$qq [expr { [string first "&lt;" \$qq] + 1 } ][expr { [string first "&gt;" \$qq] - 1 } ]; } return ""; Extracts the user principal name field from the x509 Client Certificate presented by the user</pre>
-------------------------------------------------------------------------------------------------------------	-----	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The second example show a message box displaying a Session Variable value by calling out the Session Variable ID in the Message Box for the user to see.

1		
Properties* Branch R	ules	
Name: Message Box		
Message Box		
Customization		
Language	en 🔻	Reset all defaults
Message	My SessionID is %(session.user.sessionid) Pulling a pre-set variable o	utside of
Link	Click here to continue a Variable Assign	

### Session Variable Exercise

The following are some exercises to demonstrate how session variables can be utilized.

STEP 1

Acce	ss Policy	» Access Profiles : Access Profiles List								
۰ -	Access F	Profile List Access Policy Sync CAPTCHA Configuration List								
1		Search								reate Import
4	<ul> <li>Status</li> </ul>	<ul> <li>Name</li> </ul>	<ul> <li>Application</li> </ul>	<ul> <li>Profile Type</li> </ul>	Access Policy	Export	Copy	Logs	Virtual Servers	<ul> <li>Parttion / Path</li> </ul>
	. (M	Agility-Lab-Access-Profile		All	🖉 Edit	Export	Copy	default-log-setting	Agility-LTM-VIP	Common
	1	access		All	(none)	(none)	(none)			Common

1. Open the APM VPE for the Agility-Lab-Access-Profile Access Policy we have been working with.

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: Alow, Deny [defaut])



2. Edit the Message Box in the VPE.

Name: Message Box	(	
Customization		
Language	en 💌	Reset all defaults
Message	My username is: %{session.logon.last.username}	
Link	Click here to continue	h.

3. In the Message text box enter: **My username is: %{session.logon.last.username}** Then click the **Save** button



TEST 1

Secure Logon	
for F5 Networks	
Username	
student	
Password	
•••••	
Logon	
1. Now logon with the "student" username to th	e test site.

← ⇒ C	ک https://10.128.10.100/my.policy
<b>(5</b> )	
My userna	me is: student

Click here to continue

2. When the message box appears, you should see a message stating, "**My username is: student**". Was it successful?

### STEP 2

Acc	Access Podey » Access Profiles : Access Profiles Ust									
	, Access	Profile List Access Policy Sync CAPTCHA Configuration L								
_										
1		Search							C	reate Import
•	· Status	A Name	Application	Profile Type	Access Policy	Export	Copy	Logs	Virtual Servers	Parttion / Path
8	(M)	Agility-Lab-Access-Profile		Al	🗖 Edt	Export	Copy	default-log-setting	Agility-LTM-VIP	Common
	- (M. 1	access		AI	(none)	(none)	(none)			Common

1. Go back into the VPE

Beg	in typing to search			
Logo	n Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose		
0	ACL Assign	Assign existing Access Control Lists (ACLs)		
0	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership		
0	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs		
$\bigcirc$	BWC Policy	Assign Bandwidth Controller policies		
0	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop		
$\bigcirc$	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP		
0	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership		
$\bigcirc$	Links Sections and Webtop Assign	Assign a Webtop, Webtop Links and Webtop Sections		
0	Pool Assign	Assign a Local Traffic Pool		
$\bigcirc$	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway		
0	Resource Assign	Assign Connectivity Resources		
$\bigcirc$	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings		
0	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables		
۲	Variable Assign	Assign custom variables, configuration variables, or predefined session variables		
0	VMware View Policy	Specify a policy that will apply to VMware View connections		
Canc	el Add Item	Help		
Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: Alow, Deny [defaut])				
Sta	art - Logon F	$\frac{1}{2} \int \frac{1}{2} \int \frac{1}$		

Add New Macro

2. Add a Variable Assign action from the Assignment action tab and place it before the Message Box action.

Properties Branch Rules				
Name: Variable Assign				
Variable Assign				
Add new entry	Insert Before:			
Assignment				

3. When the properties screen opens, click the Add New Entry button.

Properties* Branch Rules	
Name: Variable Assign	
Variable Assign	
Add new entry Insert Before:	1 💌
Assignment	
1 empty <u>change</u>	×

4. Then click the "Change" link.

Custom Variable	▼ Unsecure ▼	= Custom E	xpression 💌	
	^			^
	Ţ			
<	▶	4		•
Cancel Finished				Help

5. A window will pop up with *Custom Variable* on the left and *Custom Expression* on the right. You will notice both boxes are currently empty.

	v		
redefined Session Variable 💌 Unsecure 💌	=	AAA Attribute	
riable: Network Access client IPv4 💌		Agent Type: AD	
		Attribute Type: Use user's attribute	
		AD attribute name	
			0.00
Finished			19
ustom Variable 💌 Unsecure 💌	=	Custom Expression 💌	
	=	Custom Expression  mcget (session.ad.last.attr.)	^
			*
			^
	Â		
	Â	moget (session.ad.last.attr.)	
	Â	moget (session.ad.last.attr.)	, ,
	Â	moget (session.ad.last.attr.)	• •
	Â	moget (session.ad.last.attr.)	
ustom Variable 💽 Unsecure 💌	Â	moget (session.ad.last.attr.)	

6. Often you may forget how to start off with the variable name or the expression so a trick you can use to get you started is first select a pre-defined variable on the left side and a AAA attribute on the right side and then reselect custom variable and custom expression. This will populate each box with example data that you can now edit.

### *This is not a required step, just a tip!*

Custom Variable 🔹 Uns	ecure 💌	=	Custom Expression 💌	
session.custom. <u>mynewvar</u>	^		mcget {session.user.clientip}	<b>^</b>
4			4	
Cancel Finished				Help

- On the Custom Variable side type: session.custom.mynewvar (Be sure to make it lowercase). On the Custom Expression side type: mcget {session.user.clientip} (There is a space between mcget and the { bracket)
- 8. Click the Finished button.

Properties* Branch Rules	
Name: Variable Assign	
Variable Assign	
Add new entry	Insert Before: 1 💌
Assignment	
1 session.custom.mynewvar = Session Variable session.user.clientip change	×
Cancel Save (*Data in tab has been changed, please don't forget to save)	Help

#### 9. Click the Save button.

Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])

$\begin{array}{c} x \\ \text{Start} \end{array} \xrightarrow{falback} + - \underbrace{Logon Page}_{x} falback}_{x} + \rightarrow - \underbrace{Variable Assign}_{x} falback}_{x} + \rightarrow - \underbrace{Message Box}_{x} falback}_{x} + \rightarrow - \underbrace{Allow}_{x} falback}_{x} + \rightarrow - \underbrace{Variable Assign}_{x} + \rightarrow - Variable $	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Add New Macro

### 10. Click on the Message Box.

Properties Bra	nch Rules		
Name: Message E	Box		
Message Box			
Customization			
Language	en	Reset all defaults	
Message	My username is: %{session.logon.last.user My Client IP is: %{session.custom.mynewn	mame} var}	
Link Click here to continue			

11. After the closing } bracket in the first line of the message section add a space and then type <br>

12. Then on the next line type, My Client IP is: %{session.custom.mynewvar}

13. Then click the **Save** button.

6	Apply Access Policy		
Access	Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])

14. Then click Apply Access Policy.

TEST 2

6	
Secure Logon for F5 Networks	
Username	
student	
Password	
••••••	
Logon	

1. Now logon to the test site as a user again and review the message box text.

4	$\rightarrow$	G	Lttps://10.128.10.100/my.policy		
(	5				

My username is: student My Client IP is: 10.128.10.1

Click here to continue

2. Does it display your client IP address?

/ariable Name	Variable Value	Variable ID
	valiable value	session
session		
⊳ 🧰 access		session.access
⊳ 🧰 client		session.client
≡ createdfrom	ACCESS	session.createdfrom
a 🔄 custom		session.custom
⊇ mynewvar	10.128.10.1	session.custom.mynewv
E ha_unit	7e1185d64ff41bba33ba5dba81bde70b	session.ha_unit
inactivity_timeout	900	session.inactivity_timeou
▷ 🧰 logon		session.logon
⊒ partition_id	Common	session.partition_id
D policy		session.policy
⊳ 🧰 rest		session.rest
Server		session.server
<u>≡</u> snapshotid	465e3004b978_600000000000000000	session.snapshotid
⊳ 🧰 stats		session.stats
<u></u> timeout	eval_timed_out	session.timeout
Þ 🧰 ui		session.ui
⊳ 🧰 user		session.user

- 3. Now run the All Sessions Report and review the View Session Variables for the active SessionID. (Access ??Overview ?Access Reports)
- 4. Notice the folder icon named custom and the corresponding Variable ID of session.custom. This was generated automatically during the Variable Assign action that you added to the policy. When you set the Custom Variable to session.custom.mynewvar APM used the next word after the session as the new container (custom) for variable (mynewvar).

a 🔄 custom		session.custom
nynewvar	10.128.10.1	session.custom.mynewvar

5. If you expand custom folder you will notice a new Variable named mynewvar and in the next column you will see your client ip address and in the third column the variable id of session.custom.mynewvar

As you can see this could be expanded upon to be very useful. For example, maybe you are enabling two-factor authentication for both Active Directory and RSA Secure ID. Well the AAA server authentication Action objects expect to see a specific session variable name sent to them for so that they can correctly parse that data and verify against the AAA server. As an example both the AD Auth and the RSA Auth expect to see session.logon.last.password as the variable used to hold the password value. However, if you create a logon page with three input fields, one for username, a second for AD password and the third for the RSA Token/PIN then they must each have their own unique post and session variable name as they are configured in the Logon Page object.

This means that as the third variable for the RSA toke/pin is passed to APM no longer as session.logon.last.password because the AD Password field was already set to use that variable on the logon page. What do we do now?

Variable Assign to the rescue, take a look at this below example to fix this problem as it mimics what we just accomplished with the session.custom.mynewvar exercise. Consider the following screen shots.

	Logon Page Agent	
	Split domain from full Username No 🔽	
	CAPTCHA Configuration None 🗸	
	Type Post Variable Name	Session Variable Name Values Read Only
Adding the name of the	1 text 🔽 username	username No 💌
variable in <i>Logon Page</i> action	2 password V password	password No 🗸
detion	3 password V rsapin	rsapin × No V
	4 none 🔽 field4	field4 No 🗸
	5 none 🔽 field5	field5 No 💙
Setting the custom variable	Custom Variable V Unsecure V	
Access Policy: /Common/test-vpn Edt Endings (Endings: Deny (default), Alow) A full view of the policy Start falback +		

# 8.7 Lab 5: Command Line Tools

This lab will show you how to make use of some of the Command Line Utilities for troubleshooting Access Policy Manager when dealing with Authentication issues that you could experience.

# 8.7.1 Questions to ask yourself (LAB5)

- · What should I expect in the Logs with Default Settings?
- Can I review the APM configuration from TMSH?
- Can I review Session Data from the CLI?
- · How can I test if the AAA server responds to Authentication Tests using CLI Tools?
- · How can I test if the AAA server respond to Query Tests using CLI Tools?
- · How can I change the Logging Level for more Verbose details?
- · How can I use iRules for Troubleshooting Assistance?
- How can I use TCPDump for Troubleshooting Assistance?

# 8.7.2 What's Not Covered but we will discuss

- VDI Troubleshooting/Debug Logging
- SAML Troubleshooting Tools SAML Tracer (Not CLI based)

# 8.7.3 Checking APM Logs

APM Logs by default show the same information you can get from the Manage Sessions menu, as well as APM module-specific information.

Access Policy Manager uses syslog-ng to log events. The syslog-ng utility is an enhanced version of the standard logging utility syslog.

The type of event messages available on the APM are:

Event	File	Description
Mes-	Lo-	
sages	ca-	
	tion	
Access	/var/log	Appress Policy event messages include logs pertinent to access policy, SSO, network
Policy		access, and web applications. To view access policy events, on the navigation pane,
Events		expand System menu and click Logs.
Audit	/var/log	Audit event messages are those that the APM system logs as a result of changes
Logging		made to its configuration.

When setting up logging you can customize the logs by designating the minimum severity level or log level, that you want the system to report when a type of event occurs. The minimum log level indicates the minimum severity level at which the system logs that type of event.

**Note:** Files are rotated daily if their file size exceeds 10MB. Additionally, weekly rotations are enforced if the rotated log file is a week old, regardless whether or not the file exceeds the 10MB threshold.

The **default** log level for the BIG-IP APM access policy log is **Notice**, which does ***not*** log Session Variables. Setting the access policy log level to **Informational** or **Debug** will cause the BIG-IP APM system to log Session Variables, but it will also add additional system overhead. If you need to log Session Variables on a production system, F5 recommends setting the access policy log level to Informational temporarily while performing troubleshooting or debugging.

We need to add some more actions to the APM Profile in the VPE we have been working with to go along with the next few lab tests.

#### STEP 1

Access Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Allow, Deny [default])
Start $-\frac{x}{Logon Page}$ falback $+ \rightarrow -\frac{x}{Variable Assign}$ falback $+ \rightarrow -\frac{x}{Variable Assign}$	Message Box	lback + →> Allow

Add New Macro

1. Open the VPE and add a new AD Query action after the first Message Box action by selecting the + sign that follows.

_			
Beg	in typing to search		Q
Logo	n Authentication Assignm	ent Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
0	AD Auth	Active Directory authentication of end user credentials	
۲	AD Query	Active Directory query to pull user attributes for use with resource assignment or other functions, such as AD group mapping	
0	Client Cert Inspection	Check the result of client certificate authentication by the Local Traffic Client SSL profile	
$\bigcirc$	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
0	HTTP Auth	HTTP authentication of end user credentials	
$\bigcirc$	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
0	LDAP Auth	LDAP authentication of end user credentials	
$\bigcirc$	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping	
0	LocalDB Auth	Local Database Authentication	
$\bigcirc$	NTLM Auth Result	NTLM authentication of end user credentials	
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management	
$\bigcirc$	OAuth Client	OAuth Client	
0	OAuth Scope	OAuth Scope	
$\bigcirc$	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication	
0	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	
$\bigcirc$	OTP Generate	Generate One Time Passcode (OTP)	
0	OTP Verify	Verify One Time Passcode (OTP)	
$\bigcirc$	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off	
Canc	RADIUS Auth	RADIUS authentication of end user credentials	Help

2. Navigate to the Authentication tab and select the AD Query radial and click Add Item.

Properties* Branch Rules			
Name: AD Query			
Active Directory			
Туре	Query		
Server	/Common/LAB_AD_AAA 🔻		
SearchFilter		•	
Fetch Primary Group	Disabled V		
Cross Domain Support	Disabled		
Fetch Nested Groups	Disabled <b>V</b>		
Complexity check for Password Reset	Disabled <b>T</b>		
Max Password Reset Attempts 3			
Prompt user to change password before expiration	none 🔻 🛛		
Add new entry	Insert	Before: 1 🔻	
	Required Attributes (optional)		
1	cn	▼ X	
2	displayName		
3	distinguishedName		
4	dn		
5	employeeID		
6	givenName		
7	homeMDB		
Cancel Save (*Data in tab h	as been changed, please don't forget to save)	Hel	

3. In the AD Query, use the drop-down dialog box on Server to select the /Common/LAB_AD_AAA server. Click the Save button.

Access Policy: /Common/Agility-Lab-Access-Profile	(Endings: Allow, Deny [default])
Start falback + - Logon Page falback + -+>- Variable Assign falback + -+>- Message B	$\frac{1}{1000} \frac{1}{1000} + \frac{1}{1000} + \frac{1}{1000} + \frac{1}{10000} + \frac{1}{10000000000000000000000000000000000$

Add New Macro

4. On the top branch following the AD Query action, add another Message Box.

Hint: A Message Box can be added by clicking the + sign, navigating to the General Purpose tab and selecting Message Box

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: Deny [default], Alow)	
Start falback + Logon Page falback + -+> Variable Assign falback + -+> Message Box falback + -+> AD Query falback + -+>	10 s 100 + ++++- Message Box(1) faback ++++ Allow Denv

Add New Macro

5. After the second Message Box add the AD Auth action from the Authentication tab

Hint: An AD Auth action can be added by clicking the + sign, navigating to the Authentication tab and selecting AD Auth

Î	Properties Branch Rules					
	Name: AD Auth					
l	Active Directory					
	Туре	Authentication 💌				
Server /Common/LAB_AD_AAA 💌		/Common/LAB_AD_AAA				
l	Cross Domain Support	Disabled 💌				
l	Complexity check for Password Reset	Disabled				
Show Extended Error Disabled		Disabled 💌				
l	Max Logon Attempts Allowed	3 -				
1	Max Password Reset Attempts Allowed	3 -				
l						
	Cancel Save	Help				

- 6. In the AD Auth properties window use the server drop-down menu to select /Common/LAB_AD_AAA server.
- 7. Click the Save button.

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: D	p: Deny [default], Alow)	
Start)	AD.Query	Now Keny Keny

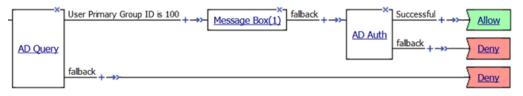
Add New Macro

8. Your policy should now look like this

Notice that one the top branch to the AD Query object the line reads User Primary Group ID is 100 (See graphic in Step 8 above, just after AD Query). Maybe you do not want to query for that information and would prefer to delete that branch. You must be ***careful*** in what you select or do when deleting that branch when you have other actions following it in the policy or they could be deleted when you do not want them to be deleted. Here is a trick you can use to preserve the actions that follow the ad query when you need to delete a branch.

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Indegs:	Deny (default), Alow)
Start	AD_Query         faback + -ap         AD_Auth         faback + -ap         AD_Auth         faback + -ap         Deny           faback + -ap         faback + -ap         Deny         faback + -ap         Deny
Add New Mazo	

9. Just before the second Message Box after the "User Primary Group ID is 100" and after the + symbol there is a double arrow symbol. This will allow us to swap portions of the policy that come after that ->>- double arrow to another location in the VPE policy.



#### 10. Click the ->>- double arrow.

Access Policy: /Comm	non/Agility-Lab-Access-Profile Edit Endings (Endings: Deny [default], Alow)	
Start faback Logon Page	faback Variable Assign faback Message Box faback AD Query faback AD Query faback faback Der	ny
	You are now in swap mode. To cancel swapping please press: Cancel Swap Mode	

11. You will now notice a **vertical arrow** pointing to other locations in the VPE where this section highlighted in green can be swapped.

#### 12. Click on the Vertical Arrow

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: Deny [default], Alow)	
Start) fabersk + - Logon Page fabersk + <u>Variable Assign</u> fabersk + <u>Message Box</u> fabersk + <u>Message Box</u> fabersk + <u>AD-Query</u> fabersk + <u>Message Box(1)</u> fabersk +	X Successful + →→→ Allow AD. Auth faback + →→→ Deny

Add New Macro

- 13. Now click the AD Query action in your policy and go to Branch Rules tab
- 14. Click the X to the right in the gray box for the Branch Rule
- 15. Click Save to save your settings



Add New Macro

16. Your policy should now look like this. Now you can see how the Swap function can help with moving action objects throughout the VPE



17. Click Apply Access Policy to save and implement or work

Now let's see what can be seen in the logs when set at the default logging level of Notice.

TEST 1

	Access			wing additional co ne system using th	nfiguration options to refir e Setup Utility.	
	Overview		Þ	Active Sessions	rtificate	
	Profiles / Po	licies	÷	Access Reports		
	Authenticati	on	Þ	OAuth Reports	⊢ n	
	Single Sign-	-On	Þ	SWG Reports	Þ	
	Federation		÷	Event Logs	> URL	Request Logs dev
	Connectivity	/VPN	Þ	Dashboard	🗷 Setti	ngs 🛵
	Secure Web	Gateway	Þ	Run Co	nfig Sync/HA Utility	
Access	» Overview : Event	Logs : Setting	S			
<b>\$</b> - A	ctive Sessions Ac	cess Reports	OAuth Reports	▼ SWG Reports	✓ Event Logs ✓	
Nat	me 🔺	Descriptio		Access System Logs	URL Request Logs	Access Profiles 5
	ault-log-setting		g setting for all	Enabled	Enabled	Agility-Lab-Access-Profile
	General Information Access System Logs	Publisher*: /Common/	sys-db-access-publ	isher 👻 🖸	Create	
4	URL Request L Access Profiles		Access Pol	icy :	Per-Request	Policy :
1	SSO Objects		Notice	*	Notice	×
		ACL :		SSO :		
			Notice	*	Notice	Y
			Secure We Notice	b Gateway :	ECA : Notice	¥
			OAuth :		PingAccess F	Profile :
			Notice	*	Notice	~
			VDI :			nagement System:
			Notice	Y	Notice	Y
11						
					0	Cancel

- 1. Review the current Access Policy Logging (Access ? Overview ? Event Logs -> Settings)
- 2. Select **default-log-setting**, then Click Edit to view settings.
- 3. Select Access System Logs

Section 2017 Putty Configuration		×		
Category:				
Session	Basic options for your PuTTY session			
Logging	Specify the destination you want to connect to			
Keyboard	Host Name (or IP address)	Port		
-Bell	10.128.1.245	22		
- Features Window - Appearance	Connection type: Raw <u>I</u> elnet Rlogin <u>S</u> SF	l 🔘 Se <u>r</u> ial		
- Behaviour - Translation - Selection - Colours	Load, save or delete a stored session Sav <u>e</u> d Sessions agilitylab			
<ul> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	Default Settings agilitylab	Load Save Delete		
	Close window on exit: Always Never Only on closed	ean exit		
About	<u>O</u> pen	<u>C</u> ancel		

4. Logon to the BIGIP APM console using an SSH client (PuTTY from your desktop). Select **agilitylab** > Load > Open

config	# tail	f	/var/log/apm
<ul> <li>Sec.</li> <li< th=""><th>a <b>SECOLLS</b> : A Speci config # tol2 -f /eat/big/age</th><th></th><th>ener lata 🖬</th></li<></ul>	a <b>SECOLLS</b> : A Speci config # tol2 -f /eat/big/age		ener lata 🖬
An DE DESERTE LE	1 CONSTRUCT DESIGNATION DESIGN TO THE DESIGN ADDRESS OF THE DES	<ol> <li>Common Chapter and points on Start, institutional points on Start (Common Coard Local Jacob (Common Coard), and the Start of Coard, managing (Coard), and address Common Coard), and Coard Address Coard, managing (COARD), Address Coard), Address Coard, managing (COARD), Address Coard), Address Coard, Address Coard, Ad</li></ol>	Handlah di Chu anoma partilar / Common Fugi Chu / C
ten 30 Oktikete Mage mettem nyd(23081)			dink has been applied. Hendy active generation count is: Mi

- 5. Maximize your SSH window to reduce line wrapping when reviewing the logs from the CLI.
- 6. From the CLI prompt, type tail -f /var/log/apm and hit Enter so you can start see the logs being displayed

6	
Secure Logon for F5 Networks	
Username	
student	
Password ••••••	
Logon	

With the SSH console logging, open a browser and access the APM as the user student.

Virtual Server	User-Agent header	Client IP			
Jun 30 11:04:19 bigip notice tmm1(24365): 01490506:9:30952afd: Received User-Agent header: Mozila%275.0%20(Windows%20NT%206.1%35%20W0W64)%20AppleWebKt%27537.36%20(KHTML%2C%20like%20Gecko)%20 C httpm=%2743.0.2357.130%20Safan%27337.36.					
Jun 30 11:04:15 bigip notice tmm1(24365): 01490344:5: 30932afd: Received client info - Type: Mozila Version: 5 Platform: Win7 CPU: unknown UI Mode: Rull Javascript Support: 1 ActiveX Support: 0 Plugin Support: 1 F Jun 30 11:04:15 bigip notige tmm1(24365): 01490500:5: 30952afd: New session from client IP 10:128:10:1 (ST=/CC=/C=) at					
VIP 10.128.10.100 Listener /Common/Agility-LTM-VIP (Reputation=Urknown) Jun 30 11:04:22 bigip notice apd(23881): 01490010:5: 30952aft; Username 'student' Jun 30 11:04:52 bigip err apd(23881):01490010:5: 30952aft; AD module: query with 'sAMAccountName=student' failed: failed to find primary group dn from cache (-1)					
Jun 30 11:05:29 big p notice apd[2388	13: 01490010:5: 30952afd: Rollowing rule 'Succe 11: 01490010:5: 30952afd: Access policy result:				
Username	Branch Rule	Policy Result			

7. Notice the logs being produced at the different stages of the users session as it first reaches the VIP, then when the user authenticates, receives message boxes or other policy actions, and then when the user reaches the policy result.

With the *default logging* level, there are no session variables being logged.

In the Next test we will turn up logging to Informational and restart the user session and then in the last test change logging level to Debug and notice the differences from Informational and Notice logging levels.

# 8.7.4 Turning up the heat on Logging

Now let's test more verbose logging. You can step up from Notice to Informational and then to Debug if you want to see the differences yourself. For the purpose of this test though I will jump straight to Debug. You can use the GUI to make the log level changes to Debug or you could use the Traffic Management Shell (TMSH) command from the CLI to adjust the logging.

### STEP 1

Edit APM Log Setting		×
<ul> <li>General Information</li> <li>Access System Logs</li> <li>URL Request Logs</li> <li>Access Profiles</li> <li>SSO Objects</li> </ul>	Publisher*: /Common/sys-db-access-publisher Access Policy : Debug   ACL : Notice  Secure Web Gateway : Notice  OAuth : Notice  VDI : Notice  VDI : Notice  VDI : Notice  VDI :	Create         Per-Request Policy :         Notice         SSO :         Notice         ECA :         Notice         PingAccess Profile :         Notice         Endpoint Management System :         Notice
		OK Cancel

1. Change Access Policy log setting to Debug (Access -> Overview ? Event Logs ? Settings, select default-log-setting, then click Edit)

TIP: Make sure you change setting back to Notice when not troubleshooting. High levels of logging not only consume more disk space, but also consume other resources, such as CPU, when enabled.



Jun 30 17 42 40 bigs ratios terre/243651_01490566_5_c0446566_5_c0446566_5_c0446566_5_c0446565_0520Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h306_1%30h20Windows/k2007h
aut 30 17:42 40 tags name two/243651 2040544.5: ck46(3):8: Reseved clean into - Yope: Month Version: 5 Pathon: We3 CPU; unknown UK Monte: Full Isoascript Support: 3 ActiveX Support: 3
Jun 30 17 42 40 bigg notice terre(24363) 4040500 5: d8465303: New session from client #10 128 30 1 (51+/CC+/C+) at V# 30 128 10 300 Uniterer //Common/Applity-ETM-VI# (Reputation-Unknown)
tun 30 17 A2 40 bagis debug apti(1884) 41460002 7. Acaso/Astroph cystum)* Inte, 663 Mig. //www.www.www.www.www.www.www.www.www.
Jun 30 17 A2 40 https://doi.org/aptic/18813_0198000_7_Autor/MotyO cpa funct_Innovative features received
Jun 10 17 42 40 Yorg stellug spol[1383] S1490000 7. ActemPrintyD gap func. "process request?" fine, 665 Mag. //www.ananonanananananananananananananananana
nor 30 17 42 40 bisits on base and EMBEL 62480000 7. HTTP://www.con.func. "read/com/sociatit" inter. 40 Most: Subst. received. 255, Nov. 255
sun 30 17 42 40 topic delag aut(23851) \$1450000 7 HTTPParter cals funct "resoff-central-bett" line: 87 Mag. Best header received: GET /mg.actics HTTP/1.1
p.m. 30 17 42 40 basis debug spd238831 02490000 7: HTTPReser cop func. "paratritrophroastitivader)" Inn. 330 Mag. HTTP Method received, GET
aut 30 17 42 40 topic datuse and [21883] 01490000 7: HTTPParter cap func: "same/triplecovers/insaler()" time: 339 Mog. HTTP URI received: /ins. datus
aux 30 17.42 40 logic delag aut(23883) 014500007. HTTPParter con funct "sanahtrofinauestrinader(1" line: 384 Mig; HTTP mator version received 1
aun 30 17 42 40 bagio debug epd(21881); 01490000 7: HTTPPaner cop func: "parai/http/ixquect/teader()" (mr. 185 Mig. HTTP minor vension received; 1
kin 35 17 42 40 bigs debig apd(20883) (2440000 2: HTTPParer op func: "read/romSocket()" ine: 14 Mig. generic header received: client-session-id: VV012/2020blch4663th
Ion 30 17 42 40 bips debug apd(23881) 01490000 7. HTTPParter cold fam: "parter/thp/Generic/Header/1" Intel 432 Mag. Header retritived, client.secjion-id: \$70712M2RebBiblics2070b3cB4655b3
au 30 17-42 40 base debug apd(23883) (249000) 7: HTTPParter cap func: "read/renforbett)" (inc. 94 Mile, generic header received anxion-two ad/05/30/MIDO46830)
ton 10 17:42-40 biglo-debug epd[23883] 01490000 7: HTTPParter op hunc: "parterHttpGeneric/Header()" Inve-432 Mig. Reader received, epoton-key, aditiv3399/94201a816/531504446315
Isin 30 17 42 40 biglo-delay apd(23881) \$14900007. HTTPParser cop func: "readFortSocket()" line: 54 Mig, generic header received; profile-dd: /Common/Ag81x-Lab-Acons-Profile
Jun 30 17 42 40 bags debug ept[21883] 01400000 7: HTTPParter cpp func: "parter/trpGeneric/reader)" Iner 453 Mag Header received, profile-sc. /Common/AgittyLab-Access-Profile
avr 30 17 42 40 topo detrug april 20001 2: HTTPParter cop funct: "read/hom/actent)" Intel 34 Mills generic header incohent classification 40 classification
Jun 30 17 4240 bipp debug apt(2883)-014000017. HTTPParter.cop Tunc: "parter/htpGeneric/Header()" Ine: 432 Mig: Header received, section-kt. 0448/85
pun 30 17,42-40 biglip debug apd(21881).01400000 7. HTTPParver cgp hunc: "readFrontDocket()" line. 14 Mag. generic header received: anaphot 4d. 6226631790-4e_15000000000000000000000000000000000000
Jun 30 17 A240 bips debug apt[23812]. 01450000 2: HTTM'arter cps funct: "partent/tipderent/Treader()" line: 432 Mig; Treader received, shaphet id: 622663125b4e, 1500000000000000
Jun 50 17.42.40 bipb debug apd(23881), 01450000 7. HTTPParter.cop Func. "readProviSochet)" line: 54 Mag; generic Reader received. cmp-du. 0
son 30 37.42.40 bigs debug ext(2)3883).03490000-2; HTTPParter cop funct: "parser/top/secenci/Header(1: fine, 412 Mig; Header received, crop-pu: 0
pun 30 17.42.40 bigs debug apd[23831]. 01400000 2: HTTPParser.op funct: "readfromSocket)" Inne: 82 Mag. Complete header recolved. 255
Jun 30 17:42:40 bipp debug apt[[3881]:014000017: AccmsPolicy0 cpp func: "process_imputiti)" line: 683 Mig: Received Sension Id: "GM466303"
pin 30 17 A2-40 bg/a delvag add(23883), 614500002; AccessRolicyD can func: "process_request()" line: 680 Mog. Received Profile 4: "/Common/Agitry-cat-Access Profile"
pun 30 17.42.40 bigip debug apd[23811] 6140000 7: AccessFolicyD upp func. "process, property" fine: 645 Mag: request/from: **
Jun 30 17:42:40 bigip debug apd(23843) 01490000 2: AccessRolicyD cpa func: "process_request()" line: 687 Mag: clientesa-mode: "
sun 30 17 A2 KD biggs debug aud(21883), 05400000 7: Accessibility/G.cop Aunic: "process_insupertition-host-mode."
pun 30 17 42-40 bige debug apt[73811] C1400000 7: AccessibilityD (zp func. "anotess, impuest)" Time 692 Mag. Received CMP Process Unit: "0, inc = 0xdoub3944"
twn 30 37 82 40 bigin debug apd(3883); 01460000 7: AccessPolicy0, cpp func: "process, impuest)" line: 603 Mig; start processing of the access policy
sun 30 17 42 40 bigle aeting aut(21883), 61400000.7: AccessProlicyProcessor (boresProlicyProcessor (boresProlicyProcessor), 6re- 447 Mag, access policy processor, 0
turn 30 17 A2 40 big/p debug apd[23881], 414600007. AccessPolicy/Processor(AccessPolicy cgp Amc: "rearcuter) ² (ine: 315 Mag: Lat's evaluate rules, total number of rules for this action+1
pun 30 17.42.40 bigip debug spd(23881) 61490000 7: AccessPolicy-rop func: "execute)/ line: 323 Mig: Rule to evaluate + ""
sun 30 17 42 40 bigs vide apd(23461) -01490006-6. 08464085. Feboving rule failback from lem "later" to item "Legen Page"
Sun 30 17 42-40 big/p debag apd(23883).01400011-7: c8H466385: Lopon agent: ENTER Punction executeientance
Inn 30 17.42.40 bij/p debug spd(2088)) 0148000027 modules/LogonRige/SimpleLogonRige/SimpleLogonRigeAgent, cap func. 'SimpleLogonRigeAgenteecuteInstance(?' Inn. 1134 Mag. SDM recoins name variables. Request Type - Request Domain , GroupHame : UserName : DeerCache 0
Sun 30 17 42-40 bigiti debug ab4(25882). 0140002.7. dH466363: Lapon agent: LEAVE function exercite/instance
Non 50 17:42:40 bigip into apd(13M13)=01400004.6:.cl446555.Executed agent: \Common/Agilty-Lab-Accese-Profile_set_logon_gage_gd', return value 3

1. Once you have the logging level increased restart you user session with the browser to the APM VIP and walk through the policy message boxes and other actions taking note of the additional verbosity in the logs you see in the SSH terminal window.

For sake of saving space in this document we will not include the screen shots showing the Informational and Debug logging messages and allow you to experience that yourself during your tests.

# 8.7.5 SessionDump Command

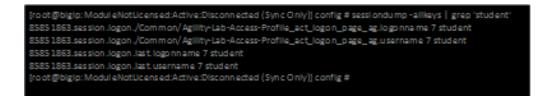
SessionDump is a command line utility that shows sessions and their associated session variables (like GUI Reports)

The sessiondump command has sever switches that can be used and you can further enhance your troubleshooting by additionally using other CLI utilities like grep to help filter the results to certain information. As you can see from the examples below, the first command simple provides all keys to be dumped for any/all user sessions while the second using grep allows you to filter the output to those associated with a given username. Refer to the screen shots below if you need additional detail.



This first example uses just the -allkeys switch.

sessiondump –allkeys



This second example also uses the –allkeys switch. However, it also adds the |grep command to search for the "username"

#### sessiondump -allkeys | grep 'student'

STEP 1



1. On the command line, if you still had the tail command showing logging then stop that now by typing CTRL-C

[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync (	Only]] config # sessiondum p -all k	eys
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync 0	Only]] config #	

Remember back in previous labs we learned that Session Variables cannot be displayed in the Reports screens if the User Session is not in an ***Active*** state. Well that is the same with the CLI sessiondump utility. There must be active sessions through APM in order to dump details.

2. Once you are at the command prompt again try using the **sessiondump –allkeys** command first. Did you receive any data after running the command? If not, then why?

Secure Logon
for F5 Networks
Username
student
Password
••••••
Logon

3. If all your previous sessions have expired then startup and new session as a user and logon to APM and click through the message boxes.



4. Now on the console type: sessiondump -allkeys. You should see a long list of information.



Compare that with running: sessiondump –allkeys | grep student You should then only see the lines that had the username you specified in the command to be returned

Now let us have some fun with using this utility to help with SSO troubleshooting/validation.

#### STEP 2

Access Policy Access Profiles : Access Profiles List										
۰.	Access F	Totlie List Access Policy Sync CAPTCHA Configuration List NT								
				_						
1		Search							C	reate Import
•	· Status	▲ Name	• Application	Profile Type	Access Policy	Export	Сору	Logs	Virtual Servers	Parttion / Path
8	14	Agility-Lab-Access-Profile		All	🕫 Edit	Export	Copy	default-log-setting	Agility-LTM-VIP	Common
	14 C	access		All	(none)	(none)	(none)			Common

1. Edit the VPE for the **Agility-Lab-Access-Profile** policy we have been working with.

Access Policy: /Common/Agility-Lab-Access-Profile Edit Endings (Endings: Demy [default], Alow)	
$\begin{tabular}{lllllllllllllllllllllllllllllllllll$	AD Auth faback + -=> Allow

Add New Macro

2. Add two new actions to the policy after the AD Auth on the successful branch.

x	n Authentication Assignme	rt [Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
	ACI, Assign	Assign existing Access Control Lists (ACLs)	
	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
	BWC Policy	Assign Bandwidth Controller policies	
	Citrix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	
	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership	
	Pool Assign	Assign a Local Traffic Pool	
	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
	Resource Assign	Assign Connectivity Resources	
	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
	SSO Credential Mapping	Enables Single Sign On (SSO) credentials caching and assigns SSO variables	
	SWG Scheme Assign	Assign a Secure Web Gateway (SWG) Scheme	
	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
	Webtop and Links Assign	Assign a Webtop and Webtop Links	

3. First after AD Auth add the SSO Credential Mapping action from the Assignment Tab. Click Add Item

Properties Branch Rules Name: SSO Credential Mapping					
Variable Assign: SSO Crede	ntial Mapping				
SSO Token Username	Username from Logon Page				
330 Towart Oschlame	mcget (session.logon.last.username)				
SSO Token Password	Password from Logon Page 💌				
3.50 TONET PUBLICITY	mcget (session.logon.last.password)				
Cancel Save	Cancel Save Help				

4. Keep the default settings and click Save.

200	Authentication Assignment	et [Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
	ACL Assign	Assign existing Access Control Lists (ACLs)	
	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership	
	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs	
	BWC Policy	Assign Bandwidth Controller policies	
	Obtix Smart Access	Enable Citrix SmartAccess filters when deploying with XenApp or XenDesktop	
	Dynamic ACL	Assign and map Access Control Lists (ACLs) retrieved from an external directory such as RADIUS or LDAP	
	LDAP Group Resource Assign	Map ACLs and resources based on user LDAP group membership	
	Pool Assign	Assign a Local Traffic Pool	
	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
	Resource Assign	Assign Connectivity Resources	
	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
	SWG Scheme Assign	Assign a Secure Web Gateway (SWG) Scheme	
	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
	Webtop and Links Assign	Assign a Webtop and Webtop Links	

### 5. Next add after the SSO Credential Mapping action add a Pool Assign action from the Assignment tab.

Properties (Branch Rales)			
Name: Pool Amign			
Pool Assignment			
Static Pool (0) Add/Dekte			
Canod See	Holp		

### 6. In the next window click the Add\Delete link.

Properties* Banch Roles					
Name: Pool Assign					
Pool Assignment					
Static Pool (1) Hide					
/Common/Agility-Lab-Pool					
None 😟 /Common/Agility-Lab-Pool					
Ganoal Sover ("Data in tab has been changed, please don't forget to save) Hele					

7. Then select the radio button for /Common/Agility-Lab-Pool. Now click the Save button.

6	Apply Access Policy		
Access I	Policy: /Common/Agility-Lab-Access-Profile	Edit Endings	(Endings: Deny [default], Allow)

8. Then click Apply Access Policy link on top left of page.

### **TEST 2**

Secure Logon for F5 Networks
Username
student
Password
Logon

1. Restart a new APM user session. Logon and follow through all the policy actions

C https://10.128.10.100/my.; ×		
← → 🗙 🕼 bttp5://10.128.10.100/my.policy#		☆ 🛽 🗉
Please click the link below to continue.	Authentication Required × The server https://10.128.10.100.443 requires a username and password. User Name: Password: Log In Cancel	
This product is licensed from FS Networks. © 1999-2014 FS Networks. All rig	hts reserved.	

2. This time instead of seeing a browser error you should be getting prompted for authentication for a website which is the site being hosted on the pool member that we assigned to the policy. Why are we getting prompted for authentication though? Did we not add the SSO Credential Mapping to the policy as well?

[root@bigip:ModuleNotLicensed:Active:Disconnected (SyncOnly)] config # sessiondump -alikeys   grep 'sso'
314212a0.session.sso.toke.nlast.pas.sword.10 ** **** ****
314212a0.session.sso.token.last.usernam e 7 student
[root@blg[p:ModuleNotLicensed:Active:Disconnected (Sync Only)] config #

 Let's use the following command at the console to check if we are getting credentials mapped to token variables properly: sessiondump –allkeys | grep 'sso' You should see two lines that show something like this following picture.

If you see the two lines with session.sso.token.last, then we know the credential mapping is happening and the username should be displayed accordingly. So what's missing?

#### STEP 3



1. Next go to the Access Policy menu, click on Access -> Profiles/Policies -> Access Profiles (Per-Session Policies) .

Acc	ess » Pro	files / Poli	cies : Access Profiles (	Per-Session Policie	s)								
₩ -	, Access	Profiles	Per-Request Policies		Customia	zation 👻							
*			Sear	ch								C	reate Import
	▼ Status	<ul> <li>Access</li> </ul>	Profile Name			Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
	p#	Agility-La	b-Access-Profile				All	Edit	Export	Сору	default-log-setting	Agility-LTM-VIP	Common
	)#	access					All	(none)	(none)	(none)			Common
Dele	ete App	ly											

2. In the list of access profiles, click the NAME of your access profile, Agility-LAB-Access-Profile

Acces	Access » Profiles / Policies : Access Profiles (Per-Session Policies) » Agility-Lab-Access-Profile							
⇔ -	Properties	SSO/	Auth Domains	Access Policy	Logs			
Genera	I Properties							
Name	e de la companya de l		Agility-Lab-Access-Profile					
Partiti	on / Path		Common					
Paren	Parent Profile		access					
Profile Type		All						
Profil	le Scope		Profile	¥				

3. When this page opens, look at the top, there are four tabs, click the SSO / Auth Domains tab

Access » Pr	Access » Profiles / Policies : Access Profiles (Per-Session Policies) » Agility-Lab-Access-Profile							
🚓 👻 Proper	rties	SSO/	Auth Domains	Access Policy	Logs			
SSO Across A	uthenticatio	n Dom	ains					
Domain Mode			Single Domain O Multiple Domains					
Domain Cook	Domain Cookie							
Cookie Options			<ul> <li>Secure</li> <li>Persistent</li> <li>HTTP Only</li> </ul>					
SSO Configuration			Agility_Lab_SSO_NTLM					
Update								

4. On this page, use the drop down menu on the SSO Configuration row to select **Agility_Lab_SSO_NTLM**. Then click Update

	Apply Acces	s Policy					
Main	Help	About	Acces	ss Policy » Acce	ss Profiles : Access Pro	ofiles List » Agility	-Lab-Access-Profile
Statisti	ics		<b>*</b> -	Properties	SSO / Auth Domains	Access Policy	Logs

5. Then click **Apply Access Policy** on the top left of the page and apply the policy on the next page.

### **TEST 3**

Secure Logon
for F5 Networks
Username
student
Password
••••••
Logon

1. Restart your user session again to the VIP and logon and click through the actions.

If necessary, you can kill your existing session by navigating to Access Policy ? Manage Sessions, then select the user/session and Click Kill Selected Sessions

← → C (k berg%//10.128.10.1 III Apps () 805-018	00	☆ ■
	Windows Server	
	Internet Information Services	
	Welcome Bienvenue Tervetuloa	
	Microsoft Veikommen Veikommen	

2. Now what do you see when the policy has completed? Are you seeing the web application without being prompted for an additional logon prompt from the application? If so, then you were successful.

# 8.7.6 ADTest Tool

In this section we will get familiar with anther CLI utility to assist in verifying proper authentication and query capabilities to an Active Directory domain. We need to prepare for this lab by making a quick change to the BIGIP's configuration.

STEP 1

Syste	m » Configuration : I	Device : DNS
☆ -	Device 👻	Local Traffic 👻 AWS 👻
Proper	ties	
_		Address:
		Add 10.128.20.100
DNS I	Lookup Server List	
		Edit Delete Up Down
		Address:
		Add
BIND	Forwarder Server List	^
		-
		Edit Delete Up Down
		Address: agilitylab.com
		Add
DNS	Search Domain List	localdomain  agilitylab.com
		Edit Delete Up Down
DNS	Cache	
IP Ver	sion	IPv4 💌
Upda	te	

- 1. Navigate to System > Configuration > Device ? DNS
- 2. Highlight 10.128.10.100 in the DNS Lookup Server List and click Delete.
- 3. Also highlight and **Delete** the DNS Search Domain List of **agilitylab.com**
- 4. Click the **Update** button.

The /usr/local/bin/adtest utility is a test tool for APM's Active Directory Module

tYPICAL USAGE	
Auth Test with Administrative username & pass- word (not necessary)	[root@bigip:ModuleNotLicensed:Active:Standalone] config # adtest -t auth -r "agilityi ab.com" -A.a.dministrator -W.adminpass -u.student -w.password Test done: total tests: 1, success=1, fallure=0 [root@bigip:ModuleNotLicensed:Active:Standalone] config #
Auth Test without just username and password	[root@bigip:ModuleNotLicensed:Active:Standalone] config # adtest -t auth -r "agilitylab.com" -u student -w password Test done: total tests: 1, success=1, failure=0 [root@bigip:ModuleNotLicensed:Active:Standalone] config #
Query Test With Administrative username and password	[rootg/bigip:ModuleNotUcensed:Active: Stand alone] config # adtest -t query -r "ag Iitylab.com" -A administrator -W adminipass -u student -w password Test done: total tests: 1, success=1, failure=0 [rootg/bigip:ModuleNotUcensed:Active: Stand alone]config #

The ADTest tool can help point out potential issues with a BIG-IP's configuration or interoperability issues on the server's side.

COMMON ERRORS	
ERROR: query with '(sAMAccountName=student)' failed in	The cause of this is
krb5_get_init_creds_password(): Preauthentication failed, principal name:	simply failed admin-
administrator@agilitylab.com (-1765328360)	istrative credentials
Test done: total tests: 1, success=0, failure=1	while attempting a
	query
ERROR: query with '(sAMAccountName=student)' failed in	The cause of this is
Idap_sasl_interactive_bind_s(): Local error, SASL(-1): generic failure: GSSAPI	typically failed DNS
Error: Unspecified GSS failure. Minor code may provide more information	resolution
(Cannot find KDC for requested realm) (-2)	
Test done: total tests: 1, success=0, failure=1	

Refer to the screen shots below if you need additional information regarding the options of ADTest.

	adtest [options]	
-t	<auth query chgp< th=""><th><pre>swdljoin chgmpswd&gt; test type [auth query chgpswd]join chgmpswd]</pre></th></auth query chgp<>	<pre>swdljoin chgmpswd&gt; test type [auth query chgpswd]join chgmpswd]</pre>
-T		timing
- r	<domain_name></domain_name>	realm
-h	<kdc_name></kdc_name>	hostname
-p	< <u>num&gt;</u>	port
-A	<admin_name></admin_name>	adminName
	<admin_pass></admin_pass>	
-f	<filter></filter>	filter [default: 'sAMAccountName= <username>']</username>
-C	<cache_root></cache_root>	credential cache file root [default: '/ <u>tmp</u> ']
	<user_name></user_name>	userName
	<machine_name></machine_name>	
		n_name> operatingSystemName
		n_version operatingSystemVersion
		tion> machineDescription
-D	<user_domain></user_domain>	
	<user_pass></user_pass>	userPassword
-N	<new_pass></new_pass>	newPassword
-5		check new password against domain password policies
-g		fetch primary group
-G		fetch nested groups
-P		fetch password expiration time
-U		cross-realm support (UPN enable)

6		
Secure l	ogon	
	etworks	
The userna Please try		d is not correct.
Username		
Password		
Logon		

1. Try logging on to the VIP as a user again after removing the DNS entries. You will notice that your logon will likely fail and you will receive the following screen.

<ul> <li>Export to CSV File   Show In Popup Window View Report Constraints Current def</li> <li>Local Time Log Message</li> <li>2014-05-30 13:58:57 Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%20)</li> <li>2014-05-30 13:58:57 Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unit</li> <li>2014-05-30 13:58:57 New session from client IP 10.10.50.27 (ST=/CC=/C=) at VIP 10.10.50</li> </ul>	
2014-05-30 13:58:57         Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%20)           2014-05-30 13:58:57         Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unit           2014-05-30 13:58:57         New session from client IP 10.10.50.27 (ST=/CC=/C=) at VIP 10.10.50.27	ault report name: "All S
2014-05-30 13:58:57         Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unit           2014-05-30 13:58:57         New session from client IP 10.10.50.27 (ST=/CC=/C=) at VIP 10.10.50.	
2014-05-30 13:58:57 New session from client IP 10.10.50.27 (ST=/CC=/C=) at VIP 10.10.50.	.1%3b%20WOW64)%
	nown UI Mode: Full Ja
2014 05 20 42 50 40 Ulastrana landanal	1 Listener /Common/.
2014-05-30 13:59:10 Username 'apmdemo'	
2014-05-30 13:59:12 AD module: query with '(sAMAccountName=apmdemo)' failed: (0)	
2014-05-30 13:59:16 AD module: authentication with 'apmdemo' failed: (1589641232)	

2. Review the session details for this logon session in reports or manage sessions. As we can see from the session details the AD Query is failing as well as AD Auth

[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # adtest -t auth -r "aglIltylab.com" -u student -w password.

3. Now we can test from the console. Open a console/ssh session. Using the following command let us first test authentication using the ADtest utility. **adtest -t auth -r "agilitylab.com" -u student -w password**. What result did you get with that test?

```
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # adtest-t
query -r "agliitylab.com" -A Administrator -W adminpass -u student -w password
```

4. Now let's try a query test. adtest -t query -r "agilitylab.com" -A Administrator -W adminpass -u student -w password. What result was returned?

System » Configuration : Device : DNS				
* -	Device -	Local Traffic 🔫 AWS 🔫		
Proper	ties			
DNSI	Lookup Server List	Address: 10.128.20.100		
BIND	Forwarder Server List	Edit Delete Up Down Address: Add Edit Delete Up Down Edit Delete Up Down		
DNS	Search Domain List	Address: agilitylab.com Add localdomain agilitylab.com		
DNS	Cache			
IP Ver	rsion	IPv4 💌		
Upda	te			

5. Go back to the DNS Settings section and re-add the DNS server IP and domain. Then re-test the Auth and Query using the ADtest utility.

### 8.7.7 iRules Logging Assistance

As many know one of the most useful features of F5 BIGIP TMOS is the flexibility provided by iRules.

With APM and iRules you can accomplish many things, in fact you can now use iRules to create APM sessions. We are not going to go over that here however for the purpose of how iRules can be used for troubleshooting we will provide some highlights.

Often you can run into problems wherein an application single sign-on is not being processed and completing as it should. What happens as a result of the initial setup not working im/_static/class4tely is that many people start second guessing what is happening as traffic passes from the clients browser, to the front client side of the BIGIP VIP, then what F5 VIP is actually able to SEE, next What does LTM see, APM see, what is being passed along the way at each stage of the transaction through the BIGIP, and of course what does the BIGIP APM then forward to the Backend Server Application and How does that Backend Server Application respond? Fortunately, iRules can be very beneficial in this process to collect and subsequently log specific data at each stage which greatly enhances the troubleshooting capabilities.

We all know that TCPDump can be your friend in capturing data to analyze however at times the application workflows between client f5 and server and encryption along the way can hamper what TCPDump could capture for analysis. Another issue with TCPDump is that is captures a lot of data that then needs to be analyzed. Granted TCPDump provides a filtering capability to weed through that extra data however when you compare it to using some targeted iRules to collect APM session variables and data to be output to logs it makes it easier to review the application flow more specific to the steps you are trying to validate.

By default, APM in the current code release automatically secures that variables that are entered into the logon page on APM. Furthermore, the password is hidden from the reports screen session variable view and hidden from the database. Yet there are times when the Admin of the APM may need to have access to the decrypted password to either verify that the correct information is being keyed by user, received by APM and sent from APM to servers. Fortunately, there is a way using an iRule to do just this for our troubleshooting purpose.

#### TEST 1

- 1. First open a console session to the BIGIP.
- 2. From the command prompt type: tail -f /var/log/ltm
- 3. Hit the enter key several times to move the text on the screen up to the top so you have a clear screen to start reviewing log data during this test.
- 4. Now open a browser and access the APM VIP and logon as a user.
- 5. When you reach the end of your APM policy take a look at the console session and note whether or not the logs provide any details about the username or password you just used to logon to APM.
- 6. Now in another browser open the APM Admin GUI.
- 7. Go to the reports screen and run the All Sessions Report.
- 8. Open the Session Variables link for the current session you have just started as the user.
- 9. Navigate down to the SSO folder and expand it.
- 10. Review the SSO Token Username and verify it displays the username you entered.
- 11. Review the SSO Token Password and verify it displays the password you entered. Or can you?
- 12. No, you cannot because it is obscured by default.

Next, we will implement an iRule to assist the Admin in verifying what password is being entered by the user.

An iRule has been created already and supplied for you so you won't need to create it yourself you only need to apply it to the Virtual Server under the Resources Tab.

#### STEP 2

1. Open the properties for the Virtual Server.

- 2. Click the resources Tab.
- 3. In the iRules section, click the Manage button.
- 4. In the right-side box scroll down to find the iRule named Agility-201-Troubleshooting
- 5. Highlight the iRule and click the arrow button to move it to the left box.
- 6. Click the finished button.

#### TEST 2

- 1. Navigate to Manage Sessions and Kill all existing sessions.
- In the console screen, hit the enter key several times to move any existing output up to the top of the window, then enter the following command tail –F /var/log/ltm
- 3. In the browser for user session testing, restart the session back to the APM VIP and logon with your username and password.
- 4. Click through to the end of the policy.
- 5. Now go back to the console session and review the log messages.
- 6. Do you see the username you entered in the logon page?
- 7. Do you see the password you entered in the logon page? If you answered yes then you were successful. Congratulations!

### 8.7.8 TCPDump Troubleshooting Assistance

Beginning in BIG-IP 11.2.0, you can use the "**p**" interface modifier with the "**p**" modifier to capture traffic with TMM information for a specific flow, and its related peer flow. The "**p**" modifier allows you to capture a specific traffic flow through the BIG-IP system from end to end, even when the configuration uses a Secure Network Address Translation (SNAT) or OneConnect. For example, the following command searches for traffic to or from client **10.128.10.100** on interface **0.0**:

#### tcpdump -ni 0.0:nnnp -s0 -c 100000 -w /var/tmp/capture.dmp host 10.128.10.100

Once **tcpdump** identifies a related flow, the flow is marked in TMM, and every subsequent packet in the flow (on both sides of the BIG-IP system) is written to the capture file.

## 8.8 Conclusion

In this lab, you learned how to use various tools including APM logs, ADTest, TCPDump to aid in troubleshooting common Access Policy Manager (APM) issues relating to Access Policy configuration, user authentication, and session variables.

#### 8.8.1 Learn More

#### Links & Information

Identity & Access Management Labs

http://clouddocs.f5.com/training/community/iam/html/

#### • BIG-IP APM 13.1.0 Knowledge Center

https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20APM&version= 13.1.0

#### Manual: F5 BIG-IP Access Policy Management Operations Guide

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/f5-apm-operations-guide.html

Manual: F5 BIG-IP Edge Client Operations Guide

https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/f5-edge-client-operations-guide. html

• K13595: Frequently used tools for troubleshooting BIG-IP APM and Edge Gateway issues (11.x)

https://support.f5.com/csp/article/K13595

- K14184: Troubleshooting BIG-IP APM portal applications
   https://support.f5.com/csp/article/K14184
- K12444: Overview of the Client Troubleshooting Utility for Windows https://support.f5.com/csp/article/K12444
- K11898: Information required when opening a support case for BIG-IP APM https://support.f5.com/csp/article/K11898

# **Class 9: Multi-Factor Auth for Cloud Applications**

This lab will teach you how to configure APM environment in order to configure multi factor authentication (MFA) using F5 Adaptive Authentication, google authenticator(GA) and DUO. Also, you will be able to configure Single Sign On (SSO) for cloud apps (AWS, Salesforce).

This class covers the following topics:

- Create a basic APM Policy
- Setup AWS Connector
- Setup Salesforce Connector
- · Set up Google Authenticator (GA) as Second Auth Factor
- Set up DUO as Second Auth Factor

Expected time to complete: 3 hours

## 9.1 Getting Started

All lab prep is already completed if you are working in the Ravello blueprint. The following information will be critical for operating your lab. Additional information can be found in the Learn More section of this guide for setting up your own lab.

Please follow the instructions provided by the instructor to start your lab and access your jump box.

**Note:** All work for this lab will be performed exclusively from the Windows **Jumpbox**. No installation or interaction with your local system is required.

### 9.1.1 Lab Topology

The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE_13 (10.1.1.245)
  - Provisioned with APM
- 1 x Windows 7 (10.1.1.199)

- Jumpbox machine
- Jumpbox user (external_user)
- 1 X Windows Server 2008 (10.1.1.245)
  - AAA server (Active Directory)
  - User (administrator)
- 1 X Windows 7 Internal (10.1.1.198)
  - Internal server used to demo SSO to RDP servers
- 1 X Linux LAMP Webserver
  - Internal Portal

#### Lab Components

The following credentials will be utilized throughout this Lab guide:

HOST/RESOURCE	USERNAME	PASSWORD
BIG-IP Configura-	admin	password
tion Utility (GUI)		
BIG-IP CLI Ac-	root	password
cess (SSH)		
Jumphost Access	external_user	password
Windows Server	administrator	password
2008 (AD) Access		
Sales User	sales_user	sales
Sales Manager	sales_manager	manager
User		
Partner User	partner_user	partner

## 9.2 Pre-Work Activities

In this module you will create or download all the requirements to configure the MFA for Cloud Apps Lab

#### 9.2.1 Lab - Pre-Work

Estimated completion time: 10 minutes

### 9.2.2 Task - Create AWS Account

1. Go to AWS page	https://console.aws.amazon.com/console/home
	aws
	Sign in o
	Email address of your AWS account
	To sign in as an IAM user, enter your <u>account ID</u> or <u>account alias</u> instead.
	Next
	New to AWS?
	Create a new AWS account
2. Click create new AWS account	
	Create an AWS account
	Email address
	Password
	Confirm password
	AWS account name
	Continue
	Sign in to an existing AWS account
	© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy   Terms of Use
<b>440</b> 3. Complete all of the required fields.	

Note: Payment information – Default Usage tier is free for 1 year with 750 hours a month compute (we will not be using any compute for this lab) and 5GB storage (we will not be using any storage for this lab).

### 9.2.3 Task - Create Salesforce Account

1. Go to Salesforce page	https://developer.salesforce.com/signup		
	Get your very own Developer Edition A full-featured copy of Lightning Platform, for FREE.		
	Name First Email		
	Your email address Role		
	Company Name		
	Country United States		
	Postal Code		
	Username Ex: name@yourcompany.com		
2. Click create new Salesforce account			
3. Complete all of the required fields.			

# https://my.freenom.com 1. You can use my.freenom to create a new public domain Services V Partners V About Freenom Register a New Domain Freenom World Free and Paid domains Domain Price Chart WHOIS 2. Go to Services, and then, Register a New Domain. mytestvlab.tk Yes mytestvlab.tk is available! 2 domains in cart Checkout 3. Introduce your new domain mytestvlab.tk (select your own), and check availability. 1 domain in cart Checkout 4. At the bottom, click Checkout Use your new domain 5. Click in "Use DNS", and then "Use your own DNS" and introduce the hostnames : "art.ns.cloudflare.com" and " ines.ns.cloudflare.com". Select also a Period of 12 Months (Free) 6. Finish the configuration signing in or 443 registering with a personal account

### 9.2.4 Task - Create (or use an existing) public domain

# 9.2.5 Task - Download Google Authenticator and DUO

<ol> <li>Download Google Authenticator client to your smartphone.</li> </ol>	<ol> <li>Android         <ul> <li>(a) https://support.google.com/accounts/ answer/1066447?co=GENIE. Platform%3DAndroid&amp;hl=en</li> </ul> </li> <li>iOS         <ul> <li>(a) https://itunes.apple.com/us/app/ google-authenticator/id388497605? mt=8</li> </ul> </li> </ol>
2. Download <b>DUO</b> client to your smartphone	<ol> <li>iOS         <ul> <li>(a) https://itunes.apple.com/us/app/ duo-mobile/id422663827?mt=8</li> </ul> </li> <li>Android         <ul> <li>(a) https://play.google.com/store/ apps/details?id=com.duosecurity. duomobile&amp;hl=en</li> </ul> </li> </ol>

## 9.2.6 Task - Create a DUO account

	Get Your Free Duo Account Current customers can upgrade now to try more features.		
	First Name Last Name		
	Email Address (201) 555-5555		
	Company / Account Name Select an Option ~		
	☐ I'm an MSP, Reseller, or Partner		
	By signing up I agree to the Terms and Privacy Policy		
	I'm not a robot		
	Create My Account		
1. Sign up for a <b>DUO account</b> .			
<ol> <li>Log in to the Duo Admin Panel and navigate to Applications, then click Protect an Application and locate F5 BIG-IP APM in the applications list.</li> </ol>	• 1. Starte for same group, applications, or down            • 1. Starte for same group, applications, or down            • Notestime to buc, Clear Banching:            • Notestime to buc, Clear Banching:            • Outcome		
	battoon 3 / Bridlow AM  F5 BIG-IP APM  Authentication Log    Renove Application  to they are 15 BIG-IP APM documentation of to Integrate Duo Into your 15 BIG-IP Genice.   Potails  Reset Secret Key  Reset Secret Key  Click to store.  APH bottman  gicl-RISGBBL-Assecurity.cm		
<ol> <li>Click Protect this Application to get your Integration Key, Secret Key, and API hostname. We will use this information later.</li> </ol>			

# 9.2.7 Task - Log in to Ravello

<ol> <li>Go to the URL provided by the instructor and login using the username and password assigned to you.</li> </ol>	<pre>http://tbctrainingportal-xxxxxsrv.ravcloud.com 1. Username = latam_studentXX 2. Password = f5DEMOs4u</pre>
2. Search LATAM_MFA_Cloud_Apps_Agility environment, then click on the link and verify that the VMs are running.	
<ol> <li>Connect to Windows 7 External VM. You can use either Console shortcut or a RDP client.</li> <li>Then verify time settings and modify if it is necessary.</li> </ol>	Date and Time       Addional Clocks       Internet Time         Date and Time       Date:       Thursday, April 05, 2018         Time       244:36 PM       Change date and time         Time zone       (UTC-06:00) Guadalajara, Mexico City, Monterrey       Change time zone         Daylight Saving Time ends on Sunday, October 28, 2018 at 2:00 AM. The clock is set to go back 1 hour at that time.       Notify me when the clock changes         Get more time zone information online       How do 1 set the clock and time zone?       Apply         Image: Time zone       OK       Cancel       Apply         Image: Time zone information online       How do 1 set the clock and time zone?       Image: Time zone       Image: Time zone         Image: Time zone time zone information online       How do 1 set the clock and time zone?       Image: Time zone       Image: Time zone         Image: Time zone time zone information online       How do 1 set the clock and time zone?       Image: Time zone       Image: Time zone         Image: Remote Desktop Connection       Image: Time zone       Image: Time zone       Image: Time zone       Image: Time zone         Image: Services       Image: PutTY       Image: Time zone       Image: Time zone       Image: Time zone       Image: Time zone         Image: Services       Image: Figure Time zone       Image: Time zone       Image: Time zo
	All Programs      Search programs and files      Log off

# 9.3 Lab 1: Create a basic APM Policy

In this module you will learn how to configure a basic APM Policy

### 9.3.1 Lab – Create an APM Policy

This lab will teach you how to create a basic APM Policy using the GUI. Estimated completion time: 20 minutes

## 9.3.2 Task - Setup Virtual Server

1. Go to Local Traffic -> Virtual Servers -> Create	tee de la sinda de constante de la solución de la s	Conne i Stavagnar i Agendara i Stavataka i Stavar Mati i Stavar Mati i Stavar Mati i Padra (Mat
	Local Traffic » Virtual Server	s : Virtual Server List » New Virtual Server
	General Properties	
	Name	webtop_demo_vs
	Description	
	Туре	Standard 🔶
	Source Address	
	Destination Address/Mask	10.1.10.47
	Service Port	443 (HTTPS \$)
	Notify Status to Virtual Address	
	State	Enabled \$
	Configuration: Basic \$	
	Protocol	TCP \$
	Protocol Profile (Client)	tcp 🗘
	Protocol Profile (Server)	(Use Client Profile)
	HTTP Profile	http 🔶
	HTTP Proxy Connect Profile	None 🗘
	FTP Profile	None \$
	RTSP Profile	None \$
	SSL Profile (Client)	Selected         Available           //Common         clientssl-insecure-compatible clientssl-secure           f5demo_client_ssl         <<           vplto-server-default-clientssl         >>           vom-default-clientssl         wom-default-clientssl
	SSL Profile (Server)	Selected Available Common apm-default-serverssl cypto-client-default-serverssl poicip-default-serverssl serverssl
	SMTPS Profile	None 🗘
2. Enter the following values (leave others default) Name: webtop_demo_vs Destination Address: 10.1.10. 47 Service Port: 443 HTTP Profile: http SSL Profile (Client): f5demo_client_ssl Source Address Translation: Àutomap		

# 9.3.3 Task - Create a Connectivity Profile

1. Go to Access -> Connectivity/VPN -> Profiles -> Add	Acces + Concepty (**) Concepty, Politik (*) Concepty * None - Deception (*) Concepty	y Tannis VII / R2P • Movied Evaluate Paret Public	Padal Access - Aqeinatan Vahad	Patkorika Como
<ol> <li>Enter the following values (leave others default)</li> <li>Name: webtop_demo_cp</li> <li>Parent Profile: /Common/</li> </ol>	Create New Connectivity General Setting Compassion Setting Chercolic Access General Setting Chercolic Seting Chercolic Setting Chercolic Se	y Profile Profile Name*: webtop_demo_cp Parent Profile*: //Common/connectivity // FEC Profile : Select a value // Partition : Common		X OK Cancel

## 9.3.4 Task - Create an AD Server as AAA

. Go to Access -> Authentication -> Active Di-	la s   A A Server M A Server M Server Server → Rama Research Server → Rama Research Server Dens	Acces Public Par	Nequest Policy   Partsion / Path   IP Ad
ectory -> Create	Access » Authentication »	New Server	
	General Properties		
	Name webtop_demo_aaa_srvr		
	Туре	Active Directory	
	Configuration		
	Domain Name	f5demo.com	
	Server Connection	Use Pool O Direct	
	Domain Controller	10.1.20.251	
	Admin Name	service_account	
	Admin Password	•••••	
	Verify Admin Password		
	Group Cache Lifetime	30	Days
	Password Security Object Cache Lifetime	30	Days
	Password Security Object Cache Lifetime	30	Days
	Kerberos Preauthentication Encryption Type	None \$	
	Timeout	15	seconds
	Cancel Repeat Finished		
2. Enter the following values (leave others de- fault)			
Name:			
webtop_demo_aaa_srvr			
Domain Name: f5demo.com			
Server Connection: Direct Domain Controller: 10.1.20.			
251			
Admin Name:			
service_account			
Admin Password: password			

# 9.3.5 Task - Create a container (webtop)

1. Go to Access -> Webtop -> Webtop Lists -> Create	Assesses = Nameses Laboration         ************************************	Cons. Too: Anna Malla I Pennar Pan	
	Access » Webtops : Webtop Lists » New Webtop		
	Name	webtop_demo_webtop	
	Туре	Full	
	Configuration		
	Minimize To Tray	C Enabled	
	Show a warning message when the webtop window close	C Enabled	
	Show URL Entry Field	C Enabled	
	Show Resource Search	Z Enabled	
	Fallback Section		
	Initial State	Expanded \$	
	Cancel Repeat Finished		
2. Enter the following values (leave others default) Name: webtop_demo_webtop Type: Full			

### 9.3.6 Task - Create a Portal Access

1. Go to Access -> Connectivity/VPN: Portal Ac- cess List -> Create	A case a carendy (19th (Pad Assoc New Acase Mat (g • CaseAs)) (19th (Pad Assoc New Acase Mat (g • CaseAs)) (19th (Pad Assoc New Acase Mat (g • CaseAssoc New Acase Mat (g • CaseAssoc New Acase New	1/02 • Novel College Pad Asse • Gene all Argentine College • Unit Stel • Unit Stel • Unit Stel • Designer Asses Paller • Parente Asses
	General Properties	
	Name	portal_intranet
	Description	
	ACL Order	First \$
	Configuration: Basic \$	)
	Match Case For Paths	Yes 🖨
	Patching	Type Full Patching ✓ HTML Patching ✓ JavaScript Patching ✓ CSS Patching ✓ Flash Patching Java Patching
	Publish on Webtop	✓ Enable
	Link Type	Application URI \$
	Application URI	http://10.1.20.32
	Customization Settings for E	English
	Language	English
	Caption	INTRANET
	Detailed Description	
	Image	Choose File No file chosen View/Hide
	Cancel Create	
<pre>2. Enter the following values (leave others de- fault)     Name: portal_intranet     Link Type: Application URI     Application URI: http://10.1.     20.32     Caption: INTRANET</pre>		

## 9.3.7 Task - Setup APM Profile

1. Go to Access -> Profiles / Policies -> Access Profiles (Per Session Policies) -> Create	Access - Indian (Ascess Access Parking PD Second Palance) <b>a</b> - Access Parking (Palance) (Palance) (Palance) (Palance) <b>b</b> - Access Parking (Palance) (P
2. Enter the following values (leave others default) then click Finished Name: webtop_demo Profile Type: All Profile Scope: Profile Languages: English	Access >> Profiles / Policies : Access Profiles (Per-Session Policies) >> New Profile         General Properties         Name       webtop_demo         Parent Profile       access         Profile Type       All         Profile Scope       Profile ‡         Language Settings       Add         Additional Languages       Add (amount)         English (en)
3. Click <b>Edit</b> for <b>webtop_demo</b> , a new browser tab will open	Sourch
4. Click the + between <b>Start</b> and <b>Deny</b> , select <b>Lo- gon Page</b> from the <b>Logon</b> tab, click <b>Add Item</b>	Access Policy: //common/webtop_demo       Edit Endings       (Endings: Allow, Deny (default))         Start_biller       Deny    Add New Macro             Image: Comparison of the start of the
	Troperties         Branch Rules           Name:         Logon Page Agent           Split domain from full Username         No *           CAPTCHAC Configuration         Non *           Type         Post Variable Name         Session Variable Name           Type         Post Variable Name         Clean Variable           Values         Read Only           1         text ÷         username           2         password         No *           3         none ÷         field3           4         none ÷         field4
	s     none ÷     ReddS     No ÷     No ²     No ²     455       Customization     Import       Language     en ÷     Reset all defaults       Form Header Text     Secure Logon Secure Logon Logon Seve Innet Field #1     Username

### 9.3.8 Task - Add the Access Policy to the Virtual Server

1. Go to Local Traffic -> Virtual Servers -> webtopdemo_vs	Los Totas - Non denno, Visal Antonez Li 6. Wall dennez V. Mar Antonez V. Maran V. Rasa - New V. Rasa - New Rasa - New Ras	come. - Osanyser i Ageloste i Detecter i Sena Ital i Sya Mercera i Aeles An - 4.1567 40 prima, Bacter E.e., Como			
	Content Rewrite				
	Rewrite Profile +	rewrite			
	HTML Profile	None			
	Access Policy				
	Access Profile	webtop_demo			
	Connectivity Profile +	webtop_demo_cp \$			
	Per-Request Policy	None			
	VDI Profile	None			
	Application Tunnels (Java & Per- App VPN)	Enabled			
	OAM Support	Enabled			
	ADFS Proxy	Enabled			
2. Modify the <b>Rewrite Profile</b> setting to rewrite,	PingAccess Profile	None 🖨			
Access Profile to webtop_demo and Connectiv-					
ity Profile to webtop_demo_cp, then click Up-					
date					
3. Test access to https://webtop.vlab.					
f5demo.com (you can use the bookmark in					
Chrome) from the jump host, you should see a lo-					
gon page. You can login with any user:					
• sales user					
sales_manager					
• partner user					

# 9.4 Lab 2: Setup an AWS Connector

In this module you will learn how to configure an AWS Connector

### 9.4.1 Lab – Setup AWS Connector

This lab will teach you how to create a SAML AWS connector. Estimated completion time: 30 minutes

## 9.4.2 Task - Download AWS metadata

1. From the jumpbox machine ( <b>Win7</b> ), open new window browser tab to https://signin.aws.amazon.com/static/saml-metadata. xml and <b>download</b> de xml file to the <b>Desktop</b> . This file will be used to create and AWS external SP Connector on the BIG-IP.	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

### 9.4.3 Task - Create an external SP connector to AWS

1. Logon onto BIG-IP, then go to Access -> Fed- eration: SAML Identity Provider -> External SP Connectors -> Create -> From Metadata	the classics will be able to be classical distribution of the
2. Enter the following values (leave others default) then click OK Select File: saml-metadata.xml Service Provider Name: AWS_EXT_SP	Create New SAML Service Provider         Select File*:         saml-metadata.xml         Browse         Service Provider Name*:         AWS_EXT_SP         Select Signing Certificate :         Select a value         OK

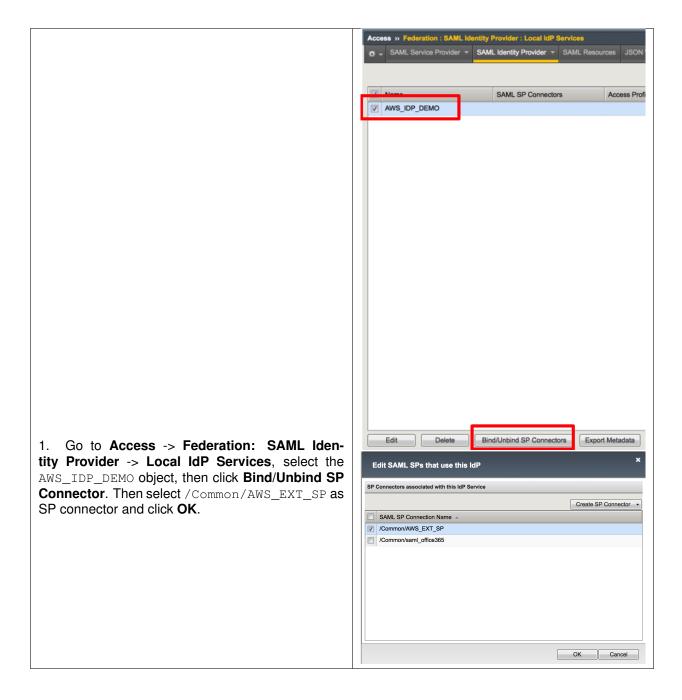
# 9.4.4 Task - Create a local IDP Service to AWS

1. Logon onto BIG-IP, then go to Access -> Feder- ation: SAML Identity Provider -> Local Idp Ser-	Aures - Scholards Huller & State Registrate : Solid Rescall         2001 Not Scholar - Solid Rescall         Implement         Implement
vices -> Create	Create New IdP Service X
	Concert Nature 2010/00       IdP Service Name*: AVX_[DP_DEMO         Security Settings       IdP Entity (DP: Inteps/webcie), viab 56demo.com/idp/f5/         Security Settings       IdP Name Couldfer:         IdP Name Couldfer:       IdP Name Couldf
2. Enter the following values (leave others default) on the General Settings Idp Service Name: AWS_IDP_DEMO IdP Entity ID: https://webtop.vlab. f5demo.com/idp/f5/	CK Carcel
	Create New IdP Service       *         General Settings       SAML Netrolies         Reservice Settings       *         SAML Attributes       *         Security Settings       *         Assertion Subject Value*       *         Mentioation Context Class Reference :       *         Automatication Context Class Reference :       *         Becurity Settings       *         Automatication Context Class Reference :       *         Become Sameters:       *         Become Sameters:       *         Become Sameters:       *         Become Sameters:       *         Becom Validay (in seconds) :       *         Becom Validay (in seconds) :       *         Become Sameters:       * <tr< th=""></tr<>
3. Enter the following values (leave others default)	СК Салсеі
on the Assertion Settings. Assertion Subject Type: Unspecified Assertion Subject Value: %{session.ad.last.attr. sAMAccountName} Authentication Context Class Refer- ence:	
<pre>urn:oasis:names:tc:SAML:2. 0:ac:classes:PasswordProtectedTranspor</pre>	t
	Create New IdP Service X Create New IdP Service Add. Concert Datings SMUL Profiles SMUL Profiles SMUL Profiles Add Add Add Add Add Create New IdP SetIngs Add
460	

## 9.4.5 Task - Download IdP metadata from BIG-IP for AWS

	Access » Federation : SAML Identity Provider : Local IdP Services
	SAML Service Provider - SAML Identity Provider - SAML Resources JSON
	Image: Name and SAML SP Connectors         Access Profile
	AWS_IDP_DEMO
	Edit Delete Bind/Unbind SP Connectors Export Metadata
1. Go to Access -> Federation: SAML Iden-	Edit Delete Bindronbind SF Connectors Export Metadata
tity Provider -> Local IdP Services, select the	× Export IdP Service
AWS_IDP_DEMO object, then click Export Meta-	Export IdP Service
data. Leave the Sign Metadata to No, and then	
click <b>Download</b> .	Sign Metadata: No 🗸
	No user configurable settings
	Use VMware View Format
	Download Cancel
	Download Cancel

### 9.4.6 Task - Bind IdP and SP Connector to AWS



## 9.4.7 Task - Create an IdP provider in AWS

<ol> <li>Sign in to the AWS Management Con- sole and open the IAM console at https:/</li> </ol>	Welcome to Identity and Access Management Muser sign-1 line: https://57254246970.signin.aws.amazon.com/console 2() IAM Resources Users: 0 Groups: 0 Groups: 0 Roles: 0 Security Status
/console.aws.amazon.com/iam/ then click Identity Provider	Create Provider Delete Providers Filter
2. Click Create Provider	Provider Name   No records found.  Configure Provider
3. Enter the following values (leave others default) on the <b>Configure Provider</b> tab, then click <b>Next</b> <b>Step</b> <b>Provider Type:</b> SAML <b>Provider Name:</b> f5demo <b>Metadata Document:</b> PATH\\AWS_IDP_DEMO_metadata. xml For the metadata document choose the file that you already downloaded.	Configure Provider type Provider Type* SAML • Provider Name* f5demo Maximum 128 characters. Use alphanumeric and '' characters. Metadata Document* C:\fakepath\AWS_IDP_DEMO_n Choose File
	Verify Provider Information         Verify the following provider information. Click Create to finish.         Provider Name         Type         SAML
4. Verify the information you have pro- vided, and then click <b>Create</b> .	

### 9.4.8 Task - Create a new Role in AWS

	Search IAM	Roles	
	Dashboard		
	Groups	What are IAM roles?	
	Users	IAM roles are a secure way to	grant permissions to entities that you trust. Examples of entities incl
	Roles	<ul> <li>IAM user in another account</li> </ul>	
	Policies		an EC2 instance that needs to perform actions on AWS resources
	Identity providers		to act on resources in your account to provide its features ctory who use identity federation with SAML
	Account settings		
	Credential report		alid for short durations, making them a more secure way to grant at
		Additional resources: IAM Roles FAQ	
	Encryption keys	IAM Roles Documentation	
		Tutorial: Setting Up Cross Ar	ccount Access
		Common Scenarios for Role	15
		Create role Delete role	
		Q Search	
		Role name 👻	Description
		Note name	Description
4. In the left neutration name, slick Dalas			
<ol> <li>In the left navigation pane, click Roles.</li> </ol>			
	_		
	Create ro	Delete rol	8
	Q Searcl	า	
	-		
	Role	name 🔻	
2. Click Create Role			
E. Onor Oreale Hole			
	Create role		1 2 3
	Select type of trust	ed entity	
			- Mah idantifu
	EC2, Lambda and othe	s Another AWS account Belonging to you or 3rd party	Coprito or any OpenID Your corporate directory
		s Another AWS account Belonging to you or 3rd party d with SAML 2.0 to assume this role to perfor	Cognito or any OpenID Tour corporate directory
	Allows users that are federate	Belonging to you or 3rd party d with SAML 2.0 to assume this role to perfor	Cognito or any OpenID Tour corporate directory
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	Belonging to you or 3rd party d with SAML 2.0 to assume this role to perfor	Cognito or any OpenID Tour corporate directory
	Allows users that are federate Choose a SAML 2.	Belonging to you or 3rd party d with SAML 2.0 to assume this role to perfor D provider access, choose an Attribute and then type a	Cognito or any OpenID     provider     mactions in your account. Learn more
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s Belonging to you or 3rd party d with SAML 2.0 to assume this role to perfor D provider access, choose an Attribute and then type a SAML provider (55demo	Create new provider C     Create new provider C     Refresh
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s AML provider [556mo] Altor provider [556mo] Altor provider [556mo] Altor provider [556mo]	Cognitio or any OpenID     Cognitio or any OpenID     Cognition or any OpenID     The comparison directory      matchans in your account. Learn more      value to include in the role. This nestricits access to users with the specified      Create new provider C     Refresh      tic access only
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3-departy     With SAML 2.0 to assume this role to perfor     D provider     SAML provider     SAML provider     SAML provider     SAML provider     Allow programma     Market programma	Control or any OpenID     Control or an
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s AML provider [556mo] Altor provider [556mo] Altor provider [556mo] Altor provider [556mo]	Cognitio or any OpenID     Cognitio or any OpenID     Cognition or any OpenID     The comparison directory      matchans in your account. Learn more      value to include in the role. This nestricits access to users with the specified      Create new provider C     Refresh      tic access only
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s Benging to you of and party with SAML 2.0 to assume this role to parfor D provider SAML provider [5:demo Allow programma & Allow pogramma Attribute SAMLaud	Cognitio or any OpenID     Cognitio or any
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s Benging to you of and party with SAML 2.0 to assume this role to parfor D provider SAML pro	Cognitio or any OpenID     Cognitio or any
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	s Benging to you of and party with SAML 2.0 to assume this role to parfor D provider SAML provider [5:demo Allow programma & Allow pogramma Attribute SAMLaud	Control or any Open(D     Control or an
<ol> <li>Enter the following values (leave others default)</li> </ol>	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Allows users that are federate Choose a SAML 2. If you're creating a role for AP	S     Compared to you or 3rd party     with SAML 2.2 to assume this role to perfor     O provider     SAML provider     SAML provider     SAML programma     Allow pogramma     Attribute SAMLaud     Valuer     https://signin.aws.am	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Atows users that are federate Choose a SAML 2. If you're creating a note for AP attributes.	s in the decision of the part	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are foderate Choose a SAML 2. If you're counting a role for AP attributes.	Encoding to you of all party     with SAML 2.2 to assume this role to perform     Or provider     SAML provider     SAML provider     SAML provider     SAML provider     SAML provider     SAML acud     Wave      New programma     Attribute     SAML acud     Valuer     Condition     C Add condition (or     Add condition (or     SAML c	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Atows users that are federate Choose a SAML 2. If you're creating a note for AP attributes.	Encoding to you of all party     with SAML 2.2 to assume this role to perform     Or provider     SAML provider     SAML provider     SAML provider     SAML provider     SAML provider     SAML acud     Wave      New programma     Attribute     SAML acud     Valuer     Condition     C Add condition (or     Add condition (or     SAML c	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are foderate Choose a SAML 2. If you're counting a role for AP attributes.	s i i i i i i i i i i i i i i i i i i i	Control or any Open(D     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altons users that are foderate Choose a SAML 2. If you're coating a role for AP attributes.	s in the deciding is you of a party with SAML 2.2 to assume this role to perform D provider SAML provider Moderna Altribute and then type a SAML provider Moderna Altribute Kentaud Value* Moderna Altribute Kentaud Value* Moderna Altribute Condition Altribute Condition Altribute policies attach to your new role. attach	Control or any Open()     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are foderate Choose a SAML 2. If you're creating a role for AP attributes.	s i i i i i i i i i i i i i i i i i i i	Conclusion and your and y
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are fodorate Choose a SAML 2. If you're counting a relef or AP attributes. Attach permissions Choose one or more policies to Create policy 2 Refre Filter: Policy type · Q Policy name · Q	s Menoping to you of all party is with SAML 2.0 to assume this role to perform O provider SAML provider SAML provider SAML provider SAML provider SAML and Allow programma Attrabute SAML and the programma Attrabute SAML and Allow programma Attrabute Attrabute Allow programma Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute Attrabute	Control or any Open()     Control or an
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are foderate Choose a SANL 2. If you're creating a note for AP attributes.	s Menoping is you of a party with SAML 2.2 to assume this role to perform D provider SAML provider Allow programma Attribute King Allow programma Attribute Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition Condition C	
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altons users that are fodorate Choose a SAML 2. If you're contains a note for AP attributes. Choose one or more policies in Create policy 2 Refer Filter: Policy type Policy name = Policy haraconfiltor + 10 Annoconfiltor + 10 Annoconfiltor + 10 Annoconfiltor + 10 Annoconfiltor	s i i i i i i i i i i i i i i i i i i i	Control or any Open (C)     Control or any Open (C)
on the Select type of trusted entity tab, then click Next: Permisions Type of trusted entity: SAML 2.0 SAML provider: f5demo Select: Allow programmatic and AWS Management Console Attribute: SAML:aud Value: https://signing.aws.	Altows users that are foderate Choose a SANL 2. If you're creating a note for AP attributes.	s Menoping to you of all party in the role to perform to you of all party in the role to perform to you of all party in the role to perform access, choose an Attribute and then type a SAML provider Eddemo Allow programma Attribute SAMLaud Allow programma Attribute SAMLaud Integration of Add condition (of Add conditio	

### 9.4.9 Task - Create a AWS SAML resource in BIG-IP

1. Go to Access -> Federation: SAML Re- sources -> Create.	Access or induction 1048 (Baseline)         Box (Baseline)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         Box (Baseline)         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Box (Baseline)         2001 Bix         2001 Bix           Image: Transmission (Constraints)         Execonstraints)         2001 Bix	or have " - Out indexinan have - 1 (Suit Hard Haven have - 1 (Frighteen		
	Access » Federation : SAML Resources » New SAML Resource			
	Name	AWS_SAML_DEMO		
	Description			
	Publish on Webtop	✓ Enable		
	Configuration			
	SSO Configuration	AWS_IDP_DEMO \$		
	Customization Settings for Eng	lish		
	Language	English		
	Caption	AWS (SAML)		
	Detailed Description			
	Image	Choose File No file chosen View/Hide		
2. Enter the following values (leave others default) on the New SAML Resource tab, then click Fin- ished. Name: AWS_SAML_DEMO SSO Configuration: AWS_IDP_DEMO Caption: AWS (SAML)	Cancel Repeat Finished			

# 9.4.10 Task - Assign the AWS SAML resource

	Status Access Profile Name     access		le Type Per-Session Policy
1. Go to Access -> Profiles/Policies -> Access	scoop     scoop_demo	AI AI	Edit
Profiles, then click Edit for webtop_demo, a new browser tab will open			
	Access Policy: /Comm	On/webtop_demo Edit Endings (Endings: Allow, Deny (default))	
	Start fallback + Logon Page		→>→ <u>Allow</u>
		AD_Auth fallback	Deny
2. Click the + between <b>AD Auth</b> and <b>Advanced</b>	Add New Macro		
Resource Assign, select AD Query from the Au-	. Begin typing to search		٩
thentication tab, click Add Item		Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
		Active Directory authentication of end user credentials Active Directory query to pull user attributes for use with resource assignment or other function	s, such as AD group
		mapping Check the result of client certificate authentication by the Local Traffic Client SSL profile	
	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication	
		F5 MFA Device Registration	
		F5 MFA User Verification HTTP authentication of end user credentials	
	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action	
		LDAP authentication of end user credentials	
	LDAP Query     LocalDB Auth	LDAP query to pull user attributes for use with resource assignment or other functions, such as Local Database Authentication	LDAP group mapping
	0	NTLM authentication of end user credentials	
	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management	
		OAuth Client	
		OAuth Scope Online Certificate Status Protocol (OCSP) client certificate authentication	
	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate	
		Generate One Time Passcode (OTP)	
	OTP Verify	Verify One Time Passcode (OTP)	
	Cancel Add Item		Help
	Properties* Branch Rules		
	Name: AD Query		
	Active Directory		
	Туре	Query +	
	Server	/Common/webtop_demo_aaa_srvr \$	
	SearchFilter		
	Fetch Primary Group Cross Domain Support	Disabled \$	
	Fetch Nested Groups	Disabled \$	igl
	Complexity check for Password Reset	Disabled \$	S
	Max Password Reset Attempts Allowed	3\$	
	Prompt user to change passwo before expiration	rd none \$0	
	Add new entry	Insert	Before: 1 ¢
		Required Attributes (optional)	
	1	[cn	××
	2	displayName	
	3	distinguishedName	
	4	dn	
	5	givenName	
	7	lomeMDB	
	8	mail	
		ab has been changed, please don't forget to save)	Help
3. Enter the following values (leave others default)			
then click Save			
Server: /Common/			
webtop_demo_aaa_srvr			
	Access Deline 10	the Jame (	
468		vtop_demo Edit Endings (Endings: Allow, Deny (default))	Talback
	Start falback + Logon Page falback	AD Auth	
4. Click on the AD Query object, a new window		fallook +-+0	Deny
will open. Click on the <b>Branch Rules</b> tab	[		

# 9.5 Lab 3: Setup a Salesforce Connector

In this module you will learn how to configure a Salesforce Connector.

## 9.5.1 Lab – Setup Salesforce Connector

This lab will teach you how to create a SAML Salesforce connector. Estimated completion time: 30 minutes

## 9.5.2 Task - Create a local IDP Service to Salesforce

1. Logon onto BIG-IP, then go to Access -> Feder- ation: SAML Identity Provider -> Local Idp Ser- vices -> Create	Attack         State School Mark School (Self Marcanic)         State School (Self Mark Schol (Self Mark School (Self Mark School (Self Mark Sch	Losse Antes Corren
	Create New IdP Service	×
2. Enter the following values (leave others default) on the General Settings Idp Service Name: SALESFORCE_IDP_DEMO IdP Entity ID: https://webtop. vlab.f5demo.com/idp/f5/		OK Cancel
	Create New IdP Service Create New IdP Service Create Setting Creat	×
<pre>3. Enter the following values (leave others default) on the Assertion Settings.     Assertion Subject Type: Email     Address     Assertion Subject Value:     %{session.ad.last.attr.mail}     Authentication Context Class Reference:     urn:oasis:names:tc:SAML:2. 0:ac:classes:PasswordProtectedTranspor</pre>		OK Cancel
	Edit IdP Service	*
		471

## 9.5.3 Task - Download IdP metadata from BIG-IP for Salesforce

1. Go to Access -> Federation: SAML Iden- tity Provider - Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download.		Access » Federation : SAML Identity Provider : Local IdP Services
1. Go to Access -> Federation: SAML Identity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Export IdP Service         Export IdP Service         Substrate         No user configurable settings         Image: Substrate         Image: Substrate		🚓 🗣 SAML Service Provider 👻 SAML Identity Provider 👻 SAML Resources JSON We
1. Go to Access -> Federation: SAML Identity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Export IdP Service         Export IdP Service         Substrate         No user configurable settings         Image: Substrate         Image: Substrate		
1. Go to Access -> Federation: SAML Identity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Export IdP Service         Export IdP Service         Substrate         No user configurable settings         Image: Substrate         Image: Substrate		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download.		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download.		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
1. Go to Access -> Federation: SAML Iden- tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Ex- port Metadata. Leave the Sign Metadata to No, and then click Download. Sign Metadata: No No user configurable settings		
tity Provider -> Local IdP Services, select the SALESFORCE_IDP_DEMO object, then click Export Metadata. Leave the Sign Metadata to No, and then click Download.	1 Go to Access -> Federation: SAMI Iden-	Edit Delete Bind/Unbind SP Connectors Export Metadata
SALESFORCE_IDP_DEMO object, then click Export Metadata. Leave the Sign Metadata to No, and then click Download.		v
port Metadata. Leave the Sign Metadata to No, and then click Download.		🔧 Export IdP Service
and then click <b>Download</b> .	SALESFORCE_IDF_DEMO Object, then click Ex-	4
No user configurable settings Use VMware View Format		Sign Metadata: No v
Use VMware View Format	and then click <b>Download</b> .	
		No user configurable settings
		Use VMware View Format
Download Cancel		
		Doubland
		L Download Cancer

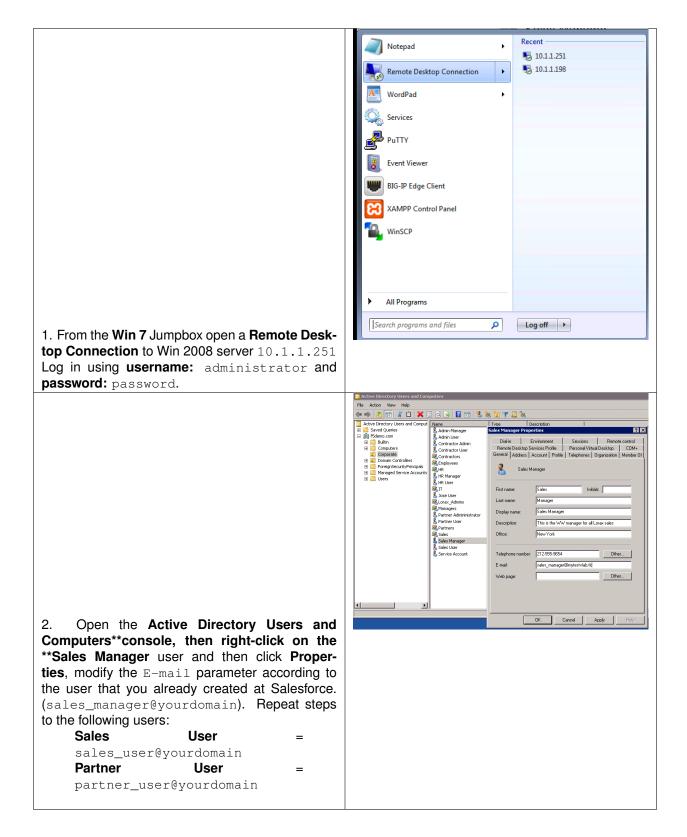
# 9.5.4 Task - Create an IdP provider in Salesforce

	Username Username Password Ug In Remember me Forgot Your Password? Use Custom Domain
<ol> <li>Log in to Salesforce https://login. salesforce.com</li> </ol>	
2. In Quick Find search box, type <b>single</b> , and then click <b>Single Sign-On Settings.</b> After that click the <b>Edit</b> button and check the <b>SAML Enabled</b> box, and then click <b>Save</b> .	Coper Manager  Coper
3. Click New from Metadata file.Then click Choose File, select SALESFORCE_IDP_DEMO_metadata.xml export file you downloaded from BIG-IP, and then click Create.	SAML Single Sign-On Settings         New Trom Metadata File         New from Metadata URL           No SAML Single Sign-On Settings         SAML Single Sign-On Settings           Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)           Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)           Create Context         Create Context           Metadata File         Choose File           SALESFORCEdata_xml         Create Context
474	

## 9.5.5 Task - Create a new user in Salesforce

	salesforce
	Username
	Password
	Log In
	Remember me
	Forgot Your Password? Use Custom Domain
	Not a customer? Try for Free
1. Log in to Salesforce https://login.	
salesforce.com	
	All Users On this page you can create, view, and manage users.
	In addition, download SalesforceA to view and edit user details, reset passwords, and perform other administrative t. View: All Users  View Edit I Create New View
	A   B
	New User         Reset Password(s)         Add Multiple Users           Action         Full Name +         Alias         Username
	Edit Chatter Expert Chatter shatty.0006a000002iranuam.0jos6h257mvo@chatter.salesforce.com     Edit Sanchez.Oscar OSanc jose@oscasme2380.com
	IEdit User.Integration integration@00d6a000002iranuam.com     IEdit User.Security, sec. insipitissecurity@00d6a000002iranuam.com
2. Under Administration, click <b>Users</b> -> <b>Users</b> -> <b>New User.</b>	New User Reset Password(s) Add Multiple Users
	New User
	User Edit Texa Texa Texa Texa Texa Texa Texa Texa
	Lark None <u>blanagar</u> Uner Lanse Force com - Free • • • • • • • • • • • • • • • • • •
	Uniterim         Earlies_managed@modelab         Reveales the           Name         Issue_managed@modelab         Other the           Tail         Reveales the         Issue_managed@modelab           Tail         Reveales the         Issue_managed@modelab
	Company File Star
	Werk was there Decement of the section of the secti
3. Enter the following values (leave others default) on the <b>New User</b> .	Accessibility Rode (Discos Gradu (Series)) (5)
First Name: Sales	
Last Name: Manager	
<b>E mail:</b> sales_manager@yourdomain <b>Username:</b>	
sales_manager@yourdomain	
Nickname: sales_manager	
Role: VP, North American Sales	
<b>476</b> User License: Free Repeat steps to the following users and change the	
<b>Role</b> as you want:	
Sales User = sales_user@yourdomain	
Partner liser - partner user Avourdomain	

## 9.5.6 Task - Modify the users in Active Directory



### Access = 1 SAML IOP BO Create • Custom From Metadata From Template | 1. Logon onto BIG-IP, then go to Access -> Federation: SAML Identity Provider -> External SP Connectors -> Create -> From Metadata × Create New SAML Service Provider Select File*: SAMLSP-00D6A000002iRAn.xml Browse Service Provider Name*: SALESFORCE_EXT_SP Select Signing Certificate : Select a value. Y OK Cancel 2. Enter the following values (leave others default) then click **OK** Select File: SAMLSP-XXXX.xml Service Provider Name: SALESFORCE EXT SP Use the ${\tt XML}$ file that you downloaded from TASK 3.

## 9.5.7 Task - Create an external SP connector to Salesforce

## 9.5.8 Task - Bind IdP and SP Connector to Salesforce

	Name 🔺	SAML SP Connectors	Access Profiles
	AWS_IDP_DEMO	AWS_EXT_SP	
	SALESFORCE_IDP_DEMO		
1. Go to Access -> Federation: SAML	Edit Delete B	ind/Unbind SP Connectors	Export Metadata
			×
Identity Provider -> Local IdP Services, se-	Edit SAML SPs that use this IdF		
lect the SALESFORCE_IDP_DEMO object, then click	SP Connectors associated with this IdP Serv	ce	
Bind/Unbind SP Connector. Then select Common/			Create SP Connector
SALESFORCE_EXT_SP as SP connector, and click	SAML SP Connection Name		
OK.	Common/AWS_EXT_SP		
	VCommon/SALESFORCE_EXT_SP		
	Common/saml_office365		
	L		
		C	OK Cancel

## 9.5.9 Task - Create a Salesforce SAML resource in BIG-IP

1. Go to Access -> Federation: SAML Re- sources -> Create.	Nome + Tableton Statis Research Product - Statis Research Product - Statis Research Nome + Statis Configuration No work Studies Nome -	201 No Yuu ' Yuu Adonado Bow * Out Dari Naxon Bow * Paylona '
	Access » Federation : SAM General Properties Name	IL Resources >> New SAML Resource
	Description	
	Publish on Webtop	✓ Enable
	Configuration	
	SSO Configuration	SALESFORCE_IDP_DEMO \$
	Customization Settings for Er	English
	Caption	SALESFORCE (SAML)
	Detailed Description	
	Image	Choose File No file chosen View/Hide
2. Enter the following values (leave others default) on the New SAML Resource tab, then click Fin- ished. Name: SALESFORCE_SAML_DEMO SSO Configuration: SALESFORCE_IDP_DEMO Caption: SALESFORCE (SAML)	Cancel Repeat Finished	

## 9.5.10 Task - Assign the SALESFORCE SAML resource

1. Go to Access -> Profiles/Policies -> Access Profiles, then click Edit for webtop_demo, a new browser tab will open	Secon         5 Application         1 Application         1 Politik Type         Period Secon         Politik Type         Period Secon         Politik Type         Period Secon         Politik Type         Period Secon         Politik Type
2. Click on the Advanced Resource Assign object, a new window will open. Click Add/Delete, then choose /Common/AWS_SAML_DEMO and /Common/SALESFORCE_SAML_DEMO from the SAML tab and click Update, then Save.	Access Policy: /Common/Webtop_demo test training: (todays Akes, day (shut))  Access Policy: /Common/Webtop_demo test training: (todays Akes, day (shut))  ("myerke (todays) the test of test o
3. Click <b>Apply Access Policy</b> in the top left and then close the browser tab	Surt         States
<ul> <li>4. Go to https://webtop.vlab.f5demo. com from the jump host, You can login with any user:</li> <li>sales_user</li> <li>sales_manager</li> <li>partner_user</li> <li>You should see two SAML resources AWS and SALESFORCE</li> <li>5. Click on the AWS and SALESFORCE links. You should be able to access both because of SSO (SAML).</li> </ul>	Enter an internal resource

## 9.6 Lab 4: Set up Google Authenticator (GA)

In this module you will learn how to configure Google Authenticator as Second Auth Factor

## 9.6.1 Lab – Set up Google Authenticator (GA)

This lab will teach you how to configure Google Authenticator as Second Auth Factor. Estimated completion time: **30 minutes** 

# 9.6.2 Task - Create the VS used to generate GA tokens

1. Log in to the BIG IP then go to Local Traffic -> Virtual Servers -> Virtual Server List. Click on Create.	Las Fulta e Nuna desarro Vale denos de a - Vale de Marcía Nan Las Formas	Com. i Dangtor   Aquitate   Dannas   Savasht   Tyra   Percent (M 11162/ 40)4779; Bender K. Com
Create.	Local Traffic >> Virtual Server         General Properties         Name         Description         Type         Source Address         Destination Address/Mask         Service Port         Notify Status to Virtual Address         State         Configuration:       Basic \$         Protocol         Protocol Profile (Client)	s : Virtual Server List » New Virtual Server VS_GENERATE_TOKEN Standard • 10.1.10.80 443 HTTPS • Enabled • TCP • (cp •
	Protocol Profile (Server) HTTP Profile HTTP Proxy Connect Profile FTP Profile RTSP Profile SSL Profile (Client)	(Use Client Profile)       http       None       None ‡       None ‡       Selected       /Common       f5demo_client_ssl       <       >>>       splitsesion-default-clientssl       wom-default-clientssl
2. Enter the following values (leave others default) and then finished. Name: VS_GENERATE_TOKEN Destination Address: 10.1.10.80	SSL Profile (Server) Resources	Selected     Available       /Common     apm-default-serverssi       c     pcolp-default-serverssi       pcolp-default-serverssi     serverssi   Enabled       Common     sys_auth_ssl_ordsp       sys_auth_ssl_ordsp     sys_auth_sacas       sys_auth_sacas     sys_acde_verify
Service Port: 443 HTTP Profile: http SSL Profile (Client): f5demo_client_ssl iRules: generate_ga_code		Up Down

## 9.6.3 Task - Generate a token

	https://generategacode.x
	← → C ■ Secure   https://generategacode.vlab.f5demo.com
	III Apps 🗅 generategacode 🚯 BIG-IP® - apm.f5derr 🗉 webtop
	<b><u>Google Authenticator</u></b> key (shared secret) generator
	account:
	secret: *optional 10 character key (additional chars truncated), random secret used if blank
	generate QR code?  submit *a request will be made to Google to generate QR code
1. Open a <b>Chrome</b> browser and click on <b>generate</b> -	Submit
gacode bookmark. You should see the GA gen-	
erator App.	
	https://generategacode x
	← → C ■ Secure https://generategacode.vlab.f5demo.com
	H Apps D generategacode 👔 BIG-IP® - apm.fSdem E webtop
	Google Authenticator key (shared secret) generator
	account: sales_manager @ f5demo.com secret: *optional 10 character key (additional chars truncated), random secret used if blank
	generate QR code?
2. Enter the account: sales_manager and do-	Submit
-	
main: f5demo.com. Also check the generate	
<b>QR code</b> , and then click <b>Submit</b>	
	NEXTRACTORY
	<u> </u>
	7824697666
3. Open up your <b>Google Authenticator</b> app and	account: sales_manager@f5demo.comkey (secret): G4ZEIWDJLBJE4ZCM
touch the "plus sign", select scan barcode and	
scan the QR code. Save the secret, we will need	
it soon.	
11 30011.	
	Local Traffic » IRules : Data Group List
	🗱 👻 iRule List Data Group List iFile List Statistics I
	Sauch
	• Search
	Type Name
	Type     Ame       Address     aol
	Type Name
	Type     Ame       Address     aol
	Type     Name       Address aol       String     google_auth_keys
	Type     Name       Address     aol       String     google_auth_keys       String     images
4. Conto Local Traffia y iBulas y Data Crown	Type     Name       Address     aol       String     google_auth_keys       String     images       Address     private_net
4. Go to Local Traffic -> iRules -> Data Group	Type     Name       Address     aol       String     google_auth_keys       String     images       Address     private_net       String     sys_APM_MS_Office_OFBA_DG
<ol> <li>Go to Local Traffic -&gt; iRules -&gt; Data Group List .Click on google_auth_keys.</li> </ol>	Type     Name       Address     aol       String     google_auth_keys       String     images       Address     private_net       String     sys_APM_MS_Office_OFBA_DG
	Type     Name       Address     aol       String     google_auth_keys       String     images       Address     private_net       String     sys_APM_MS_Office_OFBA_DG
	✓     Type     ▲ Name       Address aol       String google_auth_keys       String images       Address private_net       String sys_APM_MS_Office_OFBA_DG
	V       Type       • Name         Address aol
	V       Type <ul> <li>Name</li> <li>Address aol</li> <li>String google_auth_keys</li> <li>String images</li> <li>Address private_net</li> <li>String sys_APM_MS_Office_OFBA_DG</li> <li>Delete</li> </ul> Local Traffic >> IRules : Data Group List >> google_auth_keys <ul> <li>Properties</li> </ul>
	V       Type       Name         Address aol       Address aol         String google_auth_keys       String images         Address private_net       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> IRules : Data Group List >> google_auth_keys         Image: Comparison of the system         Image: Comparison of the system         General Properties
	✓ Type       ▲ Name         △ Address aol         String google_auth_keys         String images         △ Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Local Traffic >> IRules : Data Group List >> google_auth_keys
	V       Type       Name         Address aol       Address aol         String google_auth_keys       String images         Address private_net       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> IRules : Data Group List >> google_auth_keys         Image: Comparison of the system         Image: Comparison of the system         General Properties
	V       Type       Name         Address aol       Address aol         String google_auth_keys       String images         Address private_net       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Vocal Traffic >> Rules : Data Group List >> google_auth_keys         Properties       Properties         General Properties       Properties         Name       google_auth_keys         Partition / Path       Common         Type       String
	✓ Type       ▲ Name         △ Address aol         String google_auth_keys         String images         △ Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ♦ ●         Properties         General Properties         Name       google_auth_keys         Partition / Path       Common
	✓       Type       Name         △ Address aol
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ✓       Properties         String       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM
	✓       Type       Name         △ Address aol
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ✓       Properties         String       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ✓       Properties         String       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Cocal Traffic >> iRules : Data Group List >> google_auth_keys         ◆       > Properties         General Properties         Name       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G42EIWDJLBJE42CM         Acd
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ◆       Properties         General Properties         Name       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM         Atd
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Local Traffic >> iRules : Data Group List >> google_auth_keys         ◆       Properties         General Properties         Name       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM         Atd
List .Click on google_auth_keys.	✓ Type       ▲ Name         △ Address aol         String google_auth_keys         String images         △ Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Local Traffic >> IRules : Data Group List >> google_auth_keys         ♂ Properties         General Properties         Name       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G4ZEIWDJLBJE4ZCM         Add
	✓       Type       ▲ Name         △       Address aol         ○       String google_auth_keys         ○       String images         △       Address private_net         ○       String sys_APM_MS_Office_OFBA_DG         Delete       Delete         Cocal Traffic >> iRules : Data Group List >> google_auth_keys         ◆       > Properties         General Properties         Name       google_auth_keys         Partition / Path       Common         Type       String         Records       String: sales_manager         Value:       G42EIWDJLBJE42CM         Acd
List .Click on google_auth_keys.	▼ Type       ▲ Name         Address aol         String google_auth_keys         String images         Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Local Traffic >> IRules : Data Group List >> google_auth_keys         ♂ ● Properties         Records         String Records         String Records
List .Click on google_auth_keys.         484         5. Create a new record, using the info saved in	Yppe       Name         Address aol         String google_auth_keys         String images         Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Concert Properties         Records         String:       sales_manager         Value:       G4ZEIWDJLBJE4ZCM         Add         Edit       Delete Record
List .Click on google_auth_keys.	Yppe       Name         Address aol         String google_auth_keys         String images         Address private_net         String sys_APM_MS_Office_OFBA_DG         Delete         Concert Properties         Records         String:       sales_manager         Value:       G4ZEIWDJLBJE4ZCM         Add         Edit       Delete Record

# 9.6.4 Task - Update the VS with the verification iRule

	Local Traffic » Virtual Server List Address List Statistics Search
<ol> <li>Go to Local Traffic -&gt; Virtual Servers -&gt; Virtual Server List, then find the Virtual Server webtop_demo_vs and click on it.</li> </ol>	V     Status     A Name       VS_GENERATE_TOKEN       webtop_demo_vs       Enable     Disable   Delete
<ol> <li>In the following page, choose <b>Resources</b> and click on manage in the iRules section</li> </ol>	Conception of the conception o
	Resource Management Enabled Available
	Rule Up Down
3. Find the <b>ga_code_verify</b> irule in the right list and <b>click on the arrows</b> pointing left. The irule should now moved to the left side. Then Click <b>finished</b> .	Cancel Finished

# 9.6.5 Task - Update the Access Policy

<ol> <li>Go to Access -&gt; Profiles/Policies -&gt; Access Profiles. Find the webtop_demo policy and click on Edit.</li> </ol>	Access o Profiles (Publics: Access Politics (Publics)
2. In the <b>VPE</b> (Visual Policy Editor), click the + between <b>AD Auth</b> and <b>AD Query.</b>	Access Policy: /Common/webtop_demo Edit Endings (Endrops Alow, Demy (and web)
3. In the <b>Logon tab</b> , choose <b>Logon Page</b> and	Begin tryining to search         Exclosine:           Usign Regine:         Exclosine:         Exclosine: <td< th=""></td<>
then <b>Add Item</b>	Properties     Branch Rules       Name:     Set Ga Code       Logon Page Agent       Split domain from full Username     No 0       CAPTCHA Configuration     Non 0       Type     Post Variable Name       Session Variable Name     Gean Variable Values       Type     Post Variable Name       Lext 0     ge_code_attempt       No 0     No 0       No 0     No 0
<ol> <li>Modify the values according to the picture (leave others default) and then Save.</li> </ol>	3       none 0       Fled3       Fled3       No 0       No 0         4       none 0       Fled4       Fled4       No 0       No 0         5       none 0       Fled4       Fled4       No 0       No 0         5       none 0       Fled4       Fled4       No 0       No 0         5       none 0       Fled4       Fled4       No 0       No 0         Customization       Import       Import       Import         Language       en 0       Reset all defaults         Form Header Text
Name: Get Ga Code         Post Variabl:e ga_code_attempt         Session       Variable:         ga_code_attempt         Form Header Text: Empty         Logon       Page Input Field: Google	487

# 9.7 Lab 5: Set up DUO

In this module you will learn how to configure DUO as Second Auth Factor.

## 9.7.1 Lab – Set up DUO as Second Auth Factor

This lab will teach you how to configure DUO as Second Auth Factor. Estimated completion time: 30 minutes

## 9.7.2 Task - Get the values from DUO Admin Panel

1. Log in to the <b>Duo Admin Panel</b> and navigate to <b>Applications</b> . Then click on F5 BIG-IP APM.	A Start for user, group, applications, or device     If here and     Occur Starther u       Databoard     Weatows to Due, Guar Starther     If here and     Occur Starther u       Packade     Databoard     If here and     Databoard       Packade     Databoard     If here and     Databoard       Protect and Applications     If here and     Databoard       Protect and Applications     If here and     Databoard       Protect and Applications     If here and     If here and       Addisely hores     If here and     If here and       Recycts     Type     Application Nature
	F5 BIG-IP APM documentation 12 to integrate Duo into your F5 BIG-IP device.         Details         Integration key       DIATIYEWND2T7USIE8K7         Secret key       Click to view
2. Copy the values for: Integration key Secret key API hostname	Don't write down your secret key or share it with anyone. API hostname api-fd136d88.duosecurity.com

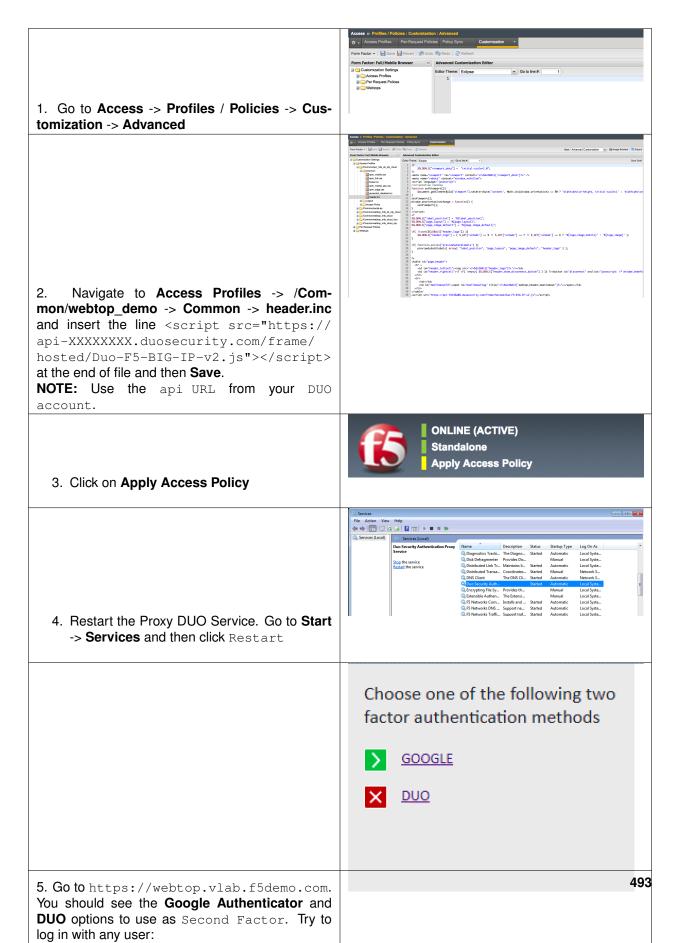
# 9.7.3 Task - Configure the Proxy for APM

	🚱 🕡 📲 🔸 Computer + Local Disk (C) + Program Files + Duo Security Authentication Proxy + conf 🔹 4- 4- 5earch conf 🔎
	Organize 🕶 🕘 Open 💌 New folder
	Favorites Name Date modified Type Size
	Dektop     jutproxy     9/12/2017 10:56 PM     CFG File     5 KB
	Downleads     Downleads     Car-bundle     B/16/2017 10:15 AM     Security Certificate     7 KB     Recent Places
	an Actorix Places
	C Libraries
	Documents
	M Computer
1. In the Win 7 External open (as	Network
administrator) the file C:Program Files-	
Duo Security Authentication Proxyconfauth-	
proxy.cfg	
6	
	adhproy - Notepad
	File Edit Format View Help ;client=ad_client
	: Port on which to listen for incoming RADIUS ACCESS Requests :port=1812
	r adfuc_server_ffrem shows users a web-based authentication prompt. This mode is only available on supported divices. confrig options: https://duo.com/docs/authproxy_reference#radius-fframe [radius_arger_efframe]
	: Config options: https://duo.com/docs/authproxy_reference#radius-iframe [radius_server_iframe]
	cype=15_Drg1p
	14
	radius_secret_l=password falimode=safe
	client=duo.only_client port=1812
	; radius_server_challenge presents users with a textual challenge after entering ; their existing passwords ; comfig options; https://duo.com/docs/authproxy_reference@radius-challenge
	: [radius_server_challenge] : radius_server_concat has users append a Duo passcode to their existing passwords
	; Config Options: https://duo.com/docs/authproxy_reference#radius-concat ' ;[radius_server_concat]
	: Include radiu_server.duo.only when primary auto is handled elsenbere and you want I to submit the passode or factor.choice as the RADUS passured field : Corfig options: https://duo.com/docs/authproxy_reference/radius-duo-only : [radius_server.duo.only]
	; Include ldap_server_auto to use with an LDAP integration. The passcode or factor ; will be appended to the passenord or a default factor can be selected ; configurines; https://dou.com/docs/authorps/yreference/ldap-auto
	: config options: https://duo.com/docs/authproxy_reference#ldap-auto [Idap_server_auto]
1. Controls the contion <b>Inadius</b> convex if remained	
1. Search the section [radius_server_iframe] and	1. ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (
modify the following values according to your <b>DUO</b>	
account	
account	
• ikey	
TV01	
• skev	
2	
• api	

# 9.7.4 Task - Modify the Access Policy to include DUO

	Access in Authenticetion (RADINS) g - All AMA Server Dat (AMA Servers Dy Type -	
1. Go to Access -> Authentication -> RADIUS -> Create.	V a constraint de la co	cours Annas Thofas : Portingal May   f Jostan (Jhai   P Admenthal
	Access » Authentication »	DUO_RADIUS
	Name	DUO_RADIUS
	Partition / Path	Common
	Туре	RADIUS
	Configuration	
	Mode	Authentication
	Server Connection	
	Server Address	10.1.10.199
	Authentication Service Port	1812
	Secret	•••••
	Confirm Secret	
	NAS IP Address	
	NAS IPV6 Address	
	NAS Identifier	
	Timeout	60 seconds
	Retries	3
	Character Set	Windows-1252 \$
	Service Type	Default
2. Create a new record, using the following info and then Finished. Name: DUO_RADIUS Mode: Authentication Server Connection: Direct Server Address: 10.1.10.199 Authentication Service Port: 1812 Secret: password Confirm Secret: password Timeout: 60	Update Delete	
3. Go to Access -> Profile / Policies -> Access Profile then locate the webtop_demo profile and click Edit.	Access on Profiles (Patiente Access Profiles (Profiles Profiles Profiles) Coress on Profiles (Patiente Access Profiles (Patiente Statutes) Coress Profiles (Patiente Statutes) Coress Profiles (Patiente Statutes) Coress Profiles (Patiente Statutes) Coress Profiles (Patiente Access Profiles (Patiente Statutes) Coress Profiles (Patiente Statu	) Costonization -   # Application   # Portie Type   Per-Session Polic Al (none) Al C Edit
4. Click on Add New Macro	금 🗄 Macro: Verify Google	e Token (Terminals: Successful, Failure [default])
	Select Macro template: Empty Name: DUO Teminals: Out [de Empty macro with one teminal	

## 9.7.5 Task - Configure the APM to use the DUO Service



# 10

## **Class 10: Privileged User Access**

Welcome to the Self Guided Priviledged User Access Hands-on Lab Guide. The following labs and exercises will instruct you on how to configure the IrulesLX Priviledged User Access Solution.

## 10.1 Lab Network Setup

In the interest of focusing as much time as possible configuring and performing lab tasks, we have provided some resources and basic setup ahead of time. These are:

- · Cloud-based lab environment complete with Virtual BIG-IP.
- The Virtual BIG-IP has been pre-licensed and provisioned with Access Policy Manager (APM).
- Pre-staged configurations to speed up lab time, reducing repetitive tasks to focus on key learning elements.

If you wish to replicate these labs in your environment you will need to perform these steps accordingly.

**Note:** All work for this lab will be performed within the BIG-IP GUI and CLI. No installation or interaction with your local system is required.

## **10.1.1 Authentication – Credentials**

The following credentials will be utilized throughout this Lab guide. All other credentials will be indicated at the time of use.

Credential Use	User ID	Password
BIG-IP Configuration Utility (GUI)	admin	4g1L17Y2018
BIG-IP CLI Access (SSH)	root	4g1L17Y2018

### **10.1.2 Utilized Browsers**

The preferred browser for this lab is Firefox. Shortcut links have been provided to speed access to targeted resources and assist you in your tasks. Except where noted, either browser can be used for all lab tasks.

## **10.1.3 General Notes**

As noted previously, environment staging has been done to speed up lab time, reducing repetitive tasks to focus on key learning elements. Where possible steps that have been optimized have been called out with links and references provided in the *Additional Information* section for additional clarification. The intention being that the lab guide truly serves as a resource guide for all your future federation deployments.

### **10.1.4 Acknowledgements**

This lab is built upon the work of prior F5 Agility's and the work of many individuals behind the scenes in addition the 2018 Agility Lab Team. Many thanks to Michael Coleman and Bill Church.

## 10.1.5 Presented by

No Presenter, but written by Michael Coleman & stolen mostly from Bill Church.

## 10.2 Lab 1: WebSSH and APM

The Privileged User Authentication (PUA) solution is made up of three parts.

- 1. WebSSH2 Client Plugin
- 2. Ephemeral Authentication Plugin
- 3. Access Policy Manager (APM) policy configuration

### **10.2.1 Requirements**

- BIG-IP with TMOS v13.1.0.2 or greater.
- 1-5 IP addresses for virtual servers (see Resource Table)

### **10.2.2 Prerequisites**

BIG-IP with at least APM and iRules LX licensed and provisioned

The *build_pua.zip* or *build_pua_offline.zip* installation script found here:

https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua.zip

https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua_offline.zip

Note: These requirements, and prerequisites have all been provisioned ahead of time for you.

### **10.2.3 Installation Overview**

The installation will consist of installing and testing (in order)

- 1. BIG-IP Preparation
- 2. Script download and execution

#### 3. Customization of APM policy

## 10.2.4 Resource Table

Resource	Description	Value
WebSSH_proxy_vs_IP	Virtual server IP Address of WebSSH2 service.	10.1.10.240
APM_Portal_vs_IP	Virtual server IP Address of APM portal for authentication	10.1.10.240
RADIUS_proxy_vs_IP	Virtual server IP address of RADIUS proxy service	10.1.10.240
LDAP_proxy_vs_IP	Virtual server IP address of LDAP proxy service	10.1.10.240
LDAPS_proxy_vs_IP	Virtual server IP address of LDAPS proxy service	10.1.10.240
LDAP_server_IP	IP Address of site LDAP or AD server (required for LDAP use)	10.1.10.240
RADIUS_server_IP	IP Address of site RADIUS server (if RADIUS bypass is used)	10.1.10.240

## 10.2.5 Installation

This script will configure a reference implementation of the F5 Privileged User Authentication solution. The only requirements are a running and licensed system ("Active"), initial configuration complete (licensed, VLANs, self IPs), and preferably already provisioned for LTM+APM+ILX. The script will check for and can enable it for you if you wish.

You will be prompted for IP addresses for 5 services:

- WebSSH Proxy This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/2222) do not conflict. This proxy is ultimately called by the APM web top. It's also important to note that SNAT may not be used on this virtual server. (webssh_proxy)
- RADIUS Proxy This runs the RADIUS Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (udp/1812) do not conflict. (radius_proxy)
- LDAP Proxy This runs the LDAP Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/389) do not conflict. (ldap_proxy)
- LDAPS Proxy This runs the LDAPS (ssl) Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/636) do not conflict. (ldaps_proxy)
- Web top This runs the LDAP Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/443) do not conflict. By default SNAT is disabled for this vs as the WebSSH proxy may not interoperate with SNAT. If you change this option be sure to institute some sort of selective disable option (iRule) when connecting to the webssh_proxy as a portal resource.

WebSSH, LDAPS, and web top will all be initially configured with a default client-ssl profile, after testing this should be changed to use a legitimate certificate.

A blank APM policy is created and attached to the web top vs "pua_webtop", this policy will need to be built out for the pua_webtop service to operate correctly.

**Note:** For this lab, the scripts have been preloaded to /tmp, and we will be using build_pua_offline.sh and using Offline Installation Method. The online instructions, in the event you wish to deploy in your own environment, can be located here: https://raw.githubusercontent.com/billchurch/f5-pua/master/docs/PUA% 20Solution%20Install%20Guide.docx If the scripts do not appear in /tmp, they have also been copied to /root.

## 10.2.6 Offline Installation Method

This method utilizes the *build_pua_offline.sh/zip* method to install the PUA solutions from a closed network or a BIG-IP with limited or no Internet connectivity.

## 10.2.7 Run Installation Script

**Note:** This lab utilizes the Non-Interactive Install mode. A file called pua_config.sh may be placed in the same directory as build_pua.sh or build_pua_offline.sh to fully automate the install, or provide defaults for a "semi-automatic" deployment. See pua_config.sh as an example.

When started, build_pua.sh or build_pua_offline.sh both check for the existence of this file.

Additionally, most of the variables set in the top of pua_config.sh and pua_config_offline.sh may be overridden by this file.

- 1. Run /tmp/build_pua_offline.sh or /root/build_pua_offline.sh
- 2. Win.

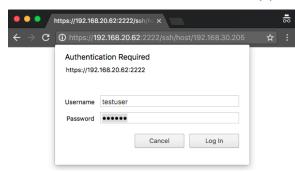
## **10.3 Validation**

### 10.3.1 WebSSH2 Client

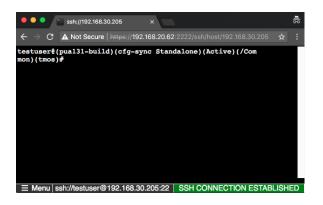
1. Open a web browser and DO NOT navigate to the first URL given by the script. The IP show in the script is internal and will not be accessible externally. Instead, you will have to use the IP from the Student Portal "Webtop" link.

example: https://{[]VS_IP{]}:2222/ssh/host/10.1.0.240

2. Enter the username testuser with any password and click login.



3. You should be greeted with a tmsh prompt to the BIG-IP the script was installed on, logged in as the user ***testuser***.

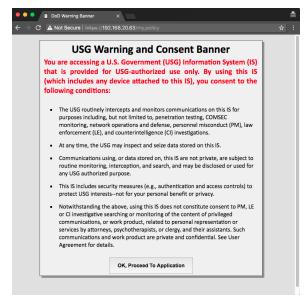


## 10.3.2 APM Policy and Portal Mode

1. Open a web browser and navigate to the second URL given by the script.

example: https://[Public IP of Virtual Server]

2. The sample USG Warning and Consent Banner should appear, click OK.



3. Enter a random username other than testuser and any password. Click Logon.

•••	192.168.20.63		×
$\boldsymbol{\leftarrow}  \Rightarrow  \mathbf{G}$	A Not Secure	https://192	2.168.20.63/my.policy
<b>f5</b>			
Secure Log for F5 Netv	·		
Username			
otheruser			
Password			
•••••			
Logon			

4. You should be directed to the webtop, click the WebSSH Portal icon.

• • • F5 Dynamic Webtop X	
← → C ▲ Not Secure   https://192.168.20.63/vdesk/we	btop.eui?w
<b>(5</b> )	
Enter an internal resource	
Applications and Links     WebSSH Portal	
Webssit Folda	

5. You should be presented with another WebSSH2 screen, logged into the BIG-IP the script was installed on as the user you provided in step 3.

