

Agility 2017 Hands-on Lab Guide

F5 Identity and Access Management Solut

F5 Networks, Inc.



Contents:

1	Clas	s 1: SAML Federation with F5	5
	1.1	Getting Started	5
	1.2	Lab 1: SAML Service Provider (SP) Lab	7
	1.3	Lab 2: SAML Identity Provider (IdP) Lab	20
	1.4	Lab 3: Kerberos to SAML Lab	44
	1.5	Lab 4: [Optional] SaaS Federation iApp Lab	58
	1.6	Conclusion	66
2	Clas	s 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	29
	2.4	Lab 3: Reporting and Session Management	67
	2.5	Lab 4: Troubleshooting	171
	2.6	Conclusion	73
3	Clas	s 3: SWG - Securing Outbound Internet Access	75
	3.2	SWG: Securing Outbound Internet Access	177

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:

Lab AGILITY 2017 330 SAML Federation with F5 Lab											
app.partner.com 10.1.10.200/24 SAML SP Partner idp.partner.com 10.1.0.210/24											
Jump Host											
Lab Environment External Io1.10.2/24 10.1.10.245/24 10.1.20.245/24 Student Lapop 10.1.20.2/24 10.1.10.245/24 10.1.1.245/24 10.1.20.254/24											
Jı	ımp Host	(BIG-IP (ve)	0		ab Server		s A	ML Partners	Alloc	ated VLANs
OS	Windows 7 (64bit)	TMOS	12.1		OS	Windows 2012		SP	SAML SP Partner	TMOS	IP Subnet
Internal	10.1.20.2/24	Internal	10.1.20.245/24 (Self)		Internal	10.1.20.254/24		JF	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	External	10.1.10.0/24
	10 1 1 2/24	Mamt	10 1 1 245/24			IIS			10.1.10.210/24	Mamet	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 👻 SA	ML Identity Provider - SAML Resources OAuth Authorization Server -		OAuth Client / Resource Server - PingAccess		≩SS -				
	Local SP Services]								Create
	External IdP Connectors		SAML IdP Co	onnectors		Description		Partition		
	Connector Automation						_			
	Authentication Context Classes	3								

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	P Service	×
General Settings Control Settings Security Settings Authentication Context Advanced Settings	Name*: app.f5demo.com Entity ID*: https://f5demo.com Scheme : Host : Host : Description :	
	OK Cancel]

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

IdP Connector

- 1. 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

Acces	Access » Federation : SAML Service Provider : External MP Connectors											
* -	SAML Service Provider + SAML	Identity Provider 👻	SAML Resources				PingAccess					
Use th clicki	Local SP Services External IdP Connectors	connectors. When y	ou use this BIG-IP s	ystem as a SAML service provid	der, it sends authen	tication requests to	o the IdP and in turn r	eceives assertions fron	n the IdP. You can create, edit a	and delete	IdP connections by	
Connector Automation						Create	•					
	vallie		SAML SP Se	rvices		Description			Partition		Custom	
											From Metadata	
											From Template	.)

- 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

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	SAML IdP Connectors					
	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 Co	onnectors						
	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	Access » Profiles / Policies : Access Profiles (Per-Session Policies)											
☆ - A	ccess Pro	files Per-Request Policies		Customization -								
*	* Search Create_ Import.											
	Status -	Access Profile Name			Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	+ Partition / Path
]≢ a	cess				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.	.com-policy			
Parent Profile		access				
Profile Type		All	All			
Profile Scope		Profile				
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-tw) Korean (ko) Spanish (os) French (fr) Serman (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	th					
	💌 Status	 Access 	Profile Name				Application	Profile Type	Per-Session Policy
🗆 🏴 access					All	(none)			
	0.0	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	n Authentication Assignment	ent] (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) dient 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	
Can	cel Add Item	TAPAPP : A. M	Help

- 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				
AAA Server					

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

Logo	n Authentication Assignmen	nt [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
Can	cel 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:	session.saml.last.attr.name.emailaddress		

- 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

111111		
v	Properties* Branch Rules	
/ (Name: Variable Assign	
ack +		
	Add new entry Insert Before:	
	Assignment	
	1 empty change	
Cu	ustom Variable 🔍 Unsecure 🗨 🗧 Session Variable 💌	
ses	ssion.logon.last.username	
	session.sami.last.attr.name.emailadoress	
Ca	ancel 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 + - Successful +>- Variable Assign fallback +	+>-) <u>Deny</u>
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)

Local Traffic Virtual Ser	vers : Virtual Server	List						
🔅 🚽 Virtual Server List								
_								
	Sea	arch Reset Search						Create
Status - Name		Description	+ Application	• Destination	Service Port	Type	Resources	Partition / Path
No records to display.								
Enable Disable De	elete							

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

Resourc	es
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			
	Enabled	Available	_
iRules	/Common ^ application-irule <	_sys_auth_ssl_cc_ldap _sys_auth_ssl_crldp _sys_auth_ssl_ocsp _sys_auth_tacacs _sys_https_redirect	*
	Up Down		
Policies	Enabled	Available	
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/ × +	
(ih https://app.f5demo.com	
🚯 Big-IP 🗉 idp.f5demo.con 🗉 app.f5dem	10.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)

Acces	Access » Federation : SAML Identity Provider : Local IdP Services								
* -	SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources OAuth Authorization Server - OAuth Client / Resource Server - PingAccess -						
Local IdP Services									
	External SP Connectors						Create		
	Name 🔺 SAML SP Co	Artifact Resolution Services	s Portal Acc	ess 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

General Settings SAML Profiles Endpoint Settings Assertion Settings SAML Attributes Security Settings IdP Entity ID*: https://idp.f5demo.com/app IdP Name Settings Scheme : Host : https://idp.fsdemo.com/app Log Level :
Assertion Settings Assertion Settings Assertion Settings Assertion Settings IdP Entity ID*: https://idp.f5demo.com/app IdP Name Settings Scheme : Host : https Description : Log Level :
Scheme : Host : https Description : Log Level :
Log Level :
Notice
OK Cancel

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
Assertion Settings SAML Attributes Security Settings	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) :
	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 Endpoint Settings	SAML Attributes	Add
SAML Attributes	Name - Value(s)	Encrypt Type
	Edit	
		OK Cancel

Create Ne	w SAML Attribute
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	M		
	1		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 Mentity Provider : External SP Connectors									
🔅 🗸 SAML Service Provider 👻	SAML Identity Provider 👻	SAML Resources	OAuth Authorization Server 👻	OAuth Client / Re	source Server 👻	PingAccess -			
This application is used to manag	Local IdP Services	alG-IP (this de	evice), in its role as a SAML Iden	tity Provider, receiv	es an authenticatio	n request from a servic	e and in turn authentio	cates the user and sends an assertio	on back to the service.
	External SP Connector	s							
	Artifact Resolution Sen	rices							Create
Name 🔺		SAML IdP S	ervices		Description			Partition	Custom
saml_office365					Predefined SP co	nnector object for Offic	e 365	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

Acces	Access » Federation : SAML Identity Provider : Local IdP Services						
\$ -	SAML Service Provider 🔻	SAML Identity Provider 👻	SAML Resou	urces OAut	h Authorizatio	n Server 🔻	OAuth Client / Res
		Local IdP Services					
	-	External SP Connectors					
		Artifact Resolution Services					
	lame 🔺	SAML SP Connectors	Access	s Profiles		Portal Access	Resources
V io	☑ idp.f5demo.com-app						
_)		
	Edit Delete	Bind/Unbind IdP Connect	Expo	rt Metadata	J		

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 IdP	*
SP Connectors associated with this IdP Service	
	Create SP Connector 👻
SAML SP Connection Name	
/Common/app.partner.com	
Common/saml_office365	
	OK 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 \checkmark	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	nglish	
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	ss » Webtops:We	btop Lists					
⇔ -	Webtop Lists	Webtop Link List	Webtop Section List	Hosted Content	-		
					_		
							Create
•	Name				Тур	e 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)

Acce	ss » Prof	iles / Polic	cies : Access Profiles (P	Per-Session Policies	s)								
÷ -	Access F	Profiles											
*			Searc	h								C	create Import
	 Status 	+ Access	Profile Name			Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	Partition / Path
	0.	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

Acces	Access » Profiles / Policies : Access Profiles (Per-Session Policies)									
🔅 🚽 Access Profiles 🛛 Per-Reques		st Policies	Policy S	ync C	ustomization	~				
				Search						
	Statue	A Nama			Application	≜ Profile Type	Access Policy	Export	Conv	Loos
	Status	- Name		× /	Application	* Prome type	Accessioney	Export	Cob)	Logo
	0	access				All	(none)	(none)	(none)	
	1	idp.f5demo.	com-policy			All	Edit	Export	Сору	default-log-setting
Delete Apply Access Policy										

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
Logon A thentication Assig	nment Endpoint Security (Server-Side) Endpoint Security (Client-Side)	
O Otrix Logon Prompt	Configure logon options for Citrix clients	
 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)	
O Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials	
O VMware View Logon Page	Display logon screen on VMware View clients	
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

Logo	n Authentication Assignme	ent) [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	
Can	cel Add Item	TERER : 8.4	Help

- 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	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 + Logon Page fallback +	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

Logo	Authentication Assignment	ent 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	
Can	cel Add Item	******* *	Help

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			
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 💌
Nan : Successful	×
Expression: User's Primary Group ID is	100 change
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:	AD	Query	
Condition:	AD	Query	Passed

24. Click the **Add Expression** Button

Simple*	
Agent Se	AD Query
Condition	AD Query Passed
Active Dire	ectory 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	
Cancel Prinsned	Help
	Help
Properties Branch Rules*	Help
Properties Branch Rules* Add Branch Rule	Help
Properties Branch Rules* Add Branch Rule Name:	Help
Properties Branch Rules* Add Branch Rule Name: Successful Expression: Active Directory Query has Passed	Help
Properties Branch Rules* Add Branch Rule Name: Successful Expression: Active Directory Query has Passed Name: fallback	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.f50	demo.com-policy	Edit Endings	(Endings: Allow, Deny [de
Start fallback + Logon Page fallback + ->>-	AD Auth fallback +→>	AD Query falls	xeessful + - > <u>Deny</u> xack + ->> <u>Deny</u> <u>Deny</u>

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

Begin typing to search] in [Current Tab 💌
Static	<u>: ACLs 0/0</u> 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

Q 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

Start fallback + X Successful + X Successful + X fallback + X fallback X fallback </th <th>Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])</th>	Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])
AD Auth fallback + -+>	Start
falback +>	AD Auth
	falback +-=>

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

Select En	ding:	
Allow		
O Deny		
Cancel	Save	Help

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

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

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*

Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
🔅 🚽 Access Profiles 🛛 Per-Request		st Policies	Policy Sync Customization		-					
•				Search						
	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	e Ap	ply Access P	olicy							

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

Access Policy: /Common/idp.f5de	emo.com-policy Edit Endings (Endings: Allow, Deny [default])
Start failback + Logon Page	AD Auth fallback +
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 +-+> Denv Denv
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:	f5demo.com
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

Beg	in typing to search		٩
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	
۲	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	
С	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	
Car	Cel Add Item	TERER : 1. Markan Kan Kan A	Hab

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

Beg	in typing to search		Q
Logo	Authentication Assign	ment 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) 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	
0	**	TIPSPE : 1. 4 4 4 4 4	

- 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 🗸
CoordeEiltor	userPrincipalName=%{session.logon.last.username}
Fetch Primary Group	Disabled 🗸
Cross Domain Support	Disabled V
Fetch Nested Groups	Disabled V
Complexity check for Password Reset	Disabled 🗸
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 💌
Nar : Successful	×
Expression: User's Primary Group ID is 100	
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:	AD	Query	
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

) A ) A ) B ) C	ACL Assign AD Group Resource Assign Advanced Resource Assign BWC Policy Citrix Smart Access	Absign existing Access Control Lists (ACLs) Map ACLs and resources based on user Active Directory group membership Expression-based assignment of Connectivity Resources, Webtop, and ACLs Assign Bandwidth Controller policies	
) A ) A ) B ) C	AD Group Resource Assign Advanced Resource Assign BWC Policy Citrix Smart Access	Map ACLs and resources based on user Active Directory group membership Expression-based assignment of Connectivity Resources, Webtop, and ACLs Assign Bandwidth Controller policies	
) A ) B ) C	Advanced Resource Assign BWC Policy Citrix Smart Access	Expression-based assignment of Connectivity Resources, Webtop, and ACLs Assign Bandwidth Controller policies	
) B ) C ) D	BWC Policy Citrix Smart Access	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	
) u	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	
) P	Pool Assign	Assign a Local Traffic Pool	
R	RDG Policy Assign	Assign an access profile to use to authorize host/port on the Remote Desktop Gateway	
R	Resource Assign	Assign Connectivity Resources	
) R S	Route Domain and SNAT Selection	Dynamically select Route Domain and SNAT settings	
S	SSO Credential Mapping	Enables Single Sign-On (SSO) credentials caching and assigns SSO variables	
v	Variable Assign	Assign custom variables, configuration variables, or predefined session variables	
) v	VMware View Policy	Specify a policy that will apply to VMware View connections	

- 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 Add/Delete link

Properties* Branch Rules
Name: Advanced Resource Assign
Resource Assignment
Add new entry
Expression: Empty change 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	ch		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						
Ommon/full_webtop						

- 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

Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])
Start       fallback

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

5 Apply Access Policy	
Access Policy. / Common/hap.f5demo.com-policy Edit Endings (Endings: Allow, Dwry [defect])	
Start     felback     ************************************	
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://idp.f5demo.com	(+	
🗲 🕧 🚔 https://idp.f5demo.com		
🕼 Big-IP 🔲 idp.f5demo.com 🗏 app.f	5demo.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 v 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	Local IdP Services	alG-IP (this d	evice), in its role as a SAML Ident	tity Provider, receiv	es an authenticatio	n request from a servi	ce and in turn authentio	cates the user and sends	an assertion ba	ck to the service.
Users can create, euit and delete	Sets call cleare, eux ain cleare External SP Connectors Tespecive Dutoris.									
	Artifact Resolution Serv	vices								Create
										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 :	an dealder
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 mana authentication request from a se				
Application Services		×.	A	pplic	ations	$\odot$	
Templates					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						
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 Salesforce.con	5	salesforce	Display Name	SalesForce	SP Initiate ?	No -	x	)

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

IDP Encryption Certificate and k	ey
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
IMPORTANT	The certificate can be either self-signed 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	iApps								
<del>*</del> •	Properties	Reconfigure	Components	Security	Analytics				
Nam	e				Availability	Туре			
-	BIG-IP								
-	sass					Application Service			
	🖯 📑 🔲 sass_vs				Unknown	Virtual Server			
	10.1.10.120	1				Virtual Address			
	sass_http					Profile			
	🖃 📃 sass_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 🛛 Vi		Virtual Address List	Statistics	-		
* Search						
🗹 💌 Status	▲ Name		Description	n 🗢 Appli	cation	Destination
	app.f5dem	o.com				10.1.10.100
	idp.f5demo	).com				10.1.10.110
	saas_redir	_vs		saas		10.1.10.120
	saas_vs			saas		10.1.10.120
Enable Dis	sable De	elete				

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

Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
\$ -	Access	Profiles	Per-Request	Policies	Polic	y Sync	;	Cus	tomization	-
_				- (a						
<u> </u>				Searc	:n					
	<ul> <li>Status</li> </ul>	<ul> <li>Name</li> </ul>		Applic	ation	Pro	file Type	Aco	cess Policy	Expor
	1	access				All		(no	ne)	(none
	<b>P</b>	app.f5der	no.com-policy			All			Edit	Expor
	pr -	idp.f5dem	io.com-policy			All			Edit	Expor
	<b>P</b>	saas		saas		All		٥	Edit	Expor
Dele	Delete Apply Access Policy									

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

Ac	Access » Profiles / Policies : Access Profiles (Per-Session Policies)									
₿	- Access	s Profiles	Per-Request I	Policies	Policy S	ync C	Customization	-		
•	Search									
•	<ul> <li>Status</li> </ul>	<ul> <li>Name</li> </ul>		÷ Ap	plication	Profile Type	Access Policy	Export	Сору	Logs
	Din .	access				All	(none)	(none)	(none)	
	0.0	idp.f5demo.	com-policy			All	Edit	Export	Сору	default-log-setting
Delete Apply Access Policy										

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	Webton: /Common/full_webtop
	Add/Delete

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

Static ACLs 0/0 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

S Apply Access Policy	
Access Policy: /Common/idp.f5demo.com-policy Edit Endings (Endings: Allow, Deny [default])	
Start       falback       +	
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 Member Of Password Replication						
Dial-in (	Dial-in Object Security			Sessions		
Remote control	Remote Desktop S	ervices Prof	ile COM+	Attribute Editor		
General Add	ress Account	Profile	Telephones	Delegation		
User logon name	•:					
HTTP/kerberos	.acme.com	@acme.c	om	~		
User logon name	e (pre-Windows 2000	):				
ACME\		kerberos				
Logon Hours	Log On To					
Cullock account Account options:						
□ User must change password at next logon       ^         □ User cannot change password						
Account expires						
O End of: Tuesday , August 9, 2016 ■▼						
	ОК Са	ancel	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

Lab AGILITY 2017 331 OAuth Federation with F5 Lab								lb nment			
Big-IP 1 OAuth (C/RS) Internal Student Lapop Big-IP 1 OAuth (C/RS) Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Internal Inte											
Jump Host		t 🐠 31G-IP-1 (VE)				IG-IP-2 (VE)					VLANs
OS	Windows 7	TMOS	13.0.0	5	TMOS	13.0.0	2	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	1	External	10.1.20.11/24		Samiara	Web Service	External	10.1.20.0/24
3)-3/-3	1-3 -3 -3	Mgmt.	10.1.1.4/24	2	Mgmt.	10.1.1.5/24		Services	web services	Mgmt.	10.1.1.0/24
2. 20. 20									A CA		

# 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	Local Traffic » Virtual Servers : Virtual Server List									
÷ -	Virtual	Server List	r List Virtual Address List Statistics		-					
*			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
Enabl	e Disa	able Delete	e							

- 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.f5agility.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 V	
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 🗸
RTSP Profile	None
SSL Profile (Client)	Selected Available Clentssl-insecure-compatible Clientssl-secure Crypto-server-default-clientssl splitsesion-default-clientssl wom-default-clientssl
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 _stys_APM_ExchangeSupport_helper _stys_APM_ExchangeSupport_main _stys_APM_Office365_SAML_BasicAuth _stys_APM_activesync _stys_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 Pr	roperties					
Name		social-ap				
Parent Pr	ofile	access				
Profile T	уре	All				
Profile S	соре	Profile V				
Language Settings						
Additional Languages	Afar (aa)					
Languages	Accepted Languages	Factory Builtin Languages       Japanese (ia)       Chinese (Simplified) (2h-cn)       Chinese (Traditional) (2h-tw)       Korran (two)       Spanish (cs)       French (t)       German (co)				
Default Language	English (en) 🗸					
Cancel Finished						

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

zcess w Profiles / Policies : Access Profiles (Per Session Policies)									
O . Access Pholies Per-Request Policies Policy Sync Customization .									
* Search							0	reate Import	
🗹 💌 Status 🔺 Access Profile Name	· Application	Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	· Partition / Path	
🗅 🏴 eccess		All	(none)	(none)	(seer)			Common	
🗆 🏴 seciai-ap		All	Ø Edt.	Export	Copy	default-log-setting		Common	
Deteta. 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	n Authentication Assignm	ent   Endpoint Security (Server-Side)   Endpoint Security (Client-Side)   General Purpose	
0	Citrix Logon Prompt	Configure logon options for Citrix clients	
0	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	
0	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	
0	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials	
0	VMware View Logon Page	Display logon screen on VMware View clients	
Cano	Add Item		Help

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

-											
1	Properties*										
,	Name: OAuth Logon Page										
ľ	Logon Page Age	nt									
1	Split domain from	full Username	No	No V							
lł	CAPTCHA Configu	ration	None								
	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					
Language	en 🗸 Reset all defaults					
Form Header Text	cure Logon for FS 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	Impor	t					
Language	en V Reset all defaults						
Form Header Text	Secure Logon for F5 Networks						
Logon Page Input Field #1	oose a Social Logon Provider						
Input Field #1 Values	FS=>F5;Google=>Google;Facebook=>Facebook;Ping=>Ping Identity;Custom=>Custom;ROPC=>ROPC [cdit]						

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

Languge:	en 🗸
Add Option	Insert after last one
Value	Text (Optional)
2 Google	
3 Facebook 4 Ping	Facebook
5 Custom	Custom
6 ROPC Cancel Finished	ROPC I

9. Click Finished

Languge:	en $\sim$
Add Option	Insert after last one 🗸
Value	Text (Optional)
1 Google	Google 💌 🗙
2 Facebook	Facebook
Cancel Finished	Help
Properties* ) (Branch Rules) Name: [OAuth Logon Page	
Split domain from full Username No	
CAPTCHA Configuration None    None	
Type         Post Variable Name         Session Variable Name         Clean Variable           1         radio <ul></ul>	Values Read Only Facebook No

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

Add Branch Rule	Insert Before: 1: F5 V
Nama	
name: CT	× ×
Expression: OAuth provider is FS change	
Name: Google	
Expression: OAuth provider is Google change	
Name: Facebook	A V X
Expression: OAuth provider is Facebook change	
Name: Ping	
Expression: OAuth provider is Ping change	
Name: Custom	a z x
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		• • ×
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	stics	•					
*				Sea	arch			
	<ul> <li>Status</li> </ul>	🔺 Name				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 × +										-	
https://conscie.developers.google.com	C Q, Search	☆ 0	۵	+	• •	- 3+	11 1-	41   *	٠	ø	-
	Google										
	Sign in to continue to Google Cloud Pla	itform									
	Email or phone										
	More options			NEXT							
Englis	h (United States) 👻	Help		thacy	Terms						

**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	h-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 🔻	۹
API	API Manager	с	redentials
٩	Dashboard	Cr	edentials OAuth consent screen Domain verification
曲	Library	Er	nail address
0+	Credentials		<this account="" be="" google="" id="" will="" your=""></this>
		Pr	oduct name shown to users 🛞
		(	DAuth Lab
		н	omepage URL (Optional)
		1	https:// or http://
		Pr	oduct logo URL (Optional)
		1	ttp://www.example.com/logo.png
		Pr	This is how your logo will look to end users Max size: 120x120 px
		0;	ntional until you deploy your app
			ntps.// or http://
		Te	rms 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 Crodentials		
				oreactions		
				You need credentials to access APIs, Enable the APIs you plan to		
				APL you need an API key, a service account, or an CAuth 2.0 client ID. Refer to the API documentation for defails.		
				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				
Ш.	Library	Appli v	eation type Veb application		
64	Credentials		Market Laam more Start hap Learn more Start hap Learn more Start hap Learn more Start hap Learn more styleting a start hap the start hap	vildcard nust inclus 23 after the 24 a proto	de it in × volume v

 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>	۳
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 autou	ab =	٩			**	ø	0	8	I	
API	API Manager	🗲 Googi	e+ API ENABLE								
$\Phi$	Dashboard	About this	401		Demonstration				the Prest	_	^
12	Library	The Cooperation	i Per i 2N anablas dasalaman ba'n di na bin of iba Gaudas shaffare.		USC INVESTIGATION		.,	416.4	a capa	1.61	
2	Crederžiais	Using crede Accessing us You can acce 2.0 client ID. data Include	entities with this APP er departed to approximate and the second of the conservation program conservation in some other and the SM C on the Conservation program access come entered to inservation accesses for that your approximate access come to access the wome making your API cost to Brongen. Least mean that clear ID available accessing your API cost to Brongen. Least mean	C2		CE110	<b>1</b> •		- <b>1</b>	e dut	
		Server to serve You can use to a web application enables appli- used to author	ver internation It is API to partnern server-to-server interaction, for example between titon and a deague service. You'll need a service account, which evel authentication. You'll also need a service account key, which is true your API call to Googlia. Law move	• • • •		9			•	-	

≡	Google APIs Diversities	- q. II D D & I 🔮
API	API Manager	Coogle+ API Costant
$\Phi$	Dashboard	Onaview Quebas
0×	Library tredentials	About this API Decaretation - Try the API is API is API in SPA Copiers - Y
		Zu Alfreenerst +     Zu Alfreenerst +     Zu Alfreenerst +     <b>La Alfreenerst</b> +     <b>La Alfreenerst</b> +     <b>La Alfreenerst</b> +     <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreenerst</b> +   <b>La Alfreeners</b> +   <b>La Alfreeners</b> +   <b>La Alfreenerst</b> +   <b>L</b>
		Errors gymnates -

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

nr1	API Manager	÷	Client ID for Web	application	2 DOWNLOAD JSON	C RESET SEC
¢	Dashboard					
	Library	Clie	nt ID	< this will be	our specific client ID>	
		Clie	nt secret	<this be="" td="" will="" y<=""><td>our specific client secret&gt;</td><td></td></this>	our specific client secret>	
0+	Credentials	Cre	ntion date May 3	7, 2017, 12:07:25 PM		
		Restri	ctions levaScript origina, redirect URIs	, or both		
		Restri Enter J Fo (h) th	ctions issuScript origina, redirect UBs thorized JavaScript origina r use with requests from a bro rule with requests from a bro rule with requests from a bro rule origin UBS. thos: & social.fSagility.com	, or both naer. This is the origin UR http://esample.com/isub	of the cleant application. It can't conta bit). If you're using a nonatanderd port	ein e velidoard ; you must include it i
		Restri Enter - Fo (h) th	ctions lawaScript origins, redirect URIs shorized JawaScript origins row with requests from a born pt// waxreple.com) or a path origin URI. ttps://social.fSagility.com rttp://www.cxample.com	, or both nave. This is the origin UR http://eaample.com/isub	of the cherri application. It carri contr (b), if you're using a nonstandard port,	ain a wildcard ,you muat include it i ×
		Restrict Enter: A Po Po Po Po Po Po Po Po Po Po Po Po Po	ctions interfaced JawaScript origins use with request of form a time origin UB. https://baceface.org/line/ https://baceface.org/ https://baceface.org/ https://baceface.org/ https://baceface.UBIs ruse with requests form a wed heterisated with Googth and wedl formed content with, Floggments o	, or both new. This is the origin UR http://waample.com/aub acrover. This is the puth i relative paths. Corrot by	of the chart application. It carri creats (b), if you're using a nonextended port (b), if you're using a nonextended port your application that usors are robre the authorization code for access. Mi	ain a velicioard , you must include it b cool to after they have at have a protocol.
		Rectin Enter - Ar So () Th So So So So So So So So So So So So So	ctions interfaced JawaScript origina interview requests from a time interview requests from a time interview its interview its intervie	, or both new. This is the origin UR http://example.com/sub http://example.com/sub acrives. This is the puth in eth will be appended with relative paths. Carnot be subth/citient/redirect	of the chert application. It can't certain (b), if you're unleg anorenendent port (b), if you're unleg anorenendent port yner application that users are redre the authorization code for access. Me	ain a velidoard , you must include it i cool to office they have at have a protocol. X

#### 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



- 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 Commonsys_APM_ExchangeSupport_OA_BasicAuthsys_APM_ExchangeSupport_OA_NtlmAuthsys_APM_ExchangeSupport_helper
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

A County of County	
r > Statut + Access Profile Name - Application	Profile Type Per-Session Policy Export Copy Logs Virtual Servers © Partition /
	All (none) (none) (none) Common
🗆 🕨 social-ap	All D Edt Expert Copy default log-setting Common

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

Loso	n Authentication Assianme	nt Cindpoint Security (Server-Side) Cindpoint 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
	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	OAuth Client	OAuth Client
0	QAuth 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	APA Provide Los Scalos advantados de colos con destado

- 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 +-	X- OAuth Logon Page	Google + →→ Facebook + → fallback + →→	Google OAuth	Client Successful +



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
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	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
Canco	el Add Item	MAR Provide New Content and

- 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/GoogleValidationScop	zesRequest 🗸	
Add new entry			Insert Before: 1 🗸
Scope Name		Request	
1 [ps://www.googleapis.com/auth	/userinfo.profile]	/Common/GoogleScopeUserinfoProfileRequ	×
Cancel Save "Data in tab has been change	l, 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	
0	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 Before	1 ~
Assignment	
1 empty change	×
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 V Unsecure V	= Session Variable
session.logon.last.username	Session Variable [Lession.cauth.scope.last×]
Cancel Finished	Help

5. Review the Google Variable Assign object and click Save

	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>	×
0	ancel Save ( ^a Data in tab has been changed, please don't forget to save)	Help

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 (Endings: Alex, Deny (Endine))							
Start	Sceple +	Secole OAuth Client	Successful + -40-	Google QAuth Scope	and + -10- Google Veriable Assign	sack + -++++++++++++++++++++++++++++++++++	
OAuth I	Logon Page		fallback + -+0			Dany	
	Pacebook	0		Alaw		) Deny	
	fallback + -+>			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	DCial-ap Edit Endings (Endings: Allow, Deny (default))
Start )-	fsilback +	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/m	y.policy	☆ :
	G Sign in - Google Accounts × +		- u /
Secure Logon for F5 Networks Choose a Social Logon Prov © Google Facebook Logon Logon	The second	A D ▼ + 1	

**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
Dashboard	Let us help you find new ways to grow your app. Click here to talk to our support team. #
Settings	
Roles	Product Setup
Alerts	
App Roview	Facebook Login
PRODUCTS	The work's number area social login product. Read Documentation
+ Add Product	
	Audience Network: Mentite year makin year welste with sole ads fees 3 million Facebook advectores. Read Documentian
	Analytics Understand has people angage with your beamers across apps, denses, platferrs and modules. Band Discontention

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

	•	
he Facebook SDK Istalled, instead yo synchronously load lements of your pa	for JavaScript doesn't have any standalone files that nee u simply need to include a short piece of regular JavaScri d the SDK into your pages. The async load means that it ge.	to be downloaded or ipt in your HTML that will does not block loading other
he following snippe 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 of the state of</body>	e options are set to their most on each page you want to load
<pre>script&gt;</pre>		Copy Code
<pre>script&gt; window.fbAsys</pre>	ncInit = function() {	Copy Code ^
<pre><soript> window.fbAsy FB.init({</soript></pre>	<pre>ncInit = function() {</pre>	Copy Code ^
<pre><soript> window.fbAsys FB.init({     appId</soript></pre>	<pre>hcInit = function() {     : '178071772721497',</pre>	Copy Code
<pre>cscript&gt; window.fbAsyn FB.init{{     appId     cookie</pre>	<pre>ncInit = function() {     : '178071772721497',     : true,</pre>	Copy Code
<pre><script></script></pre>		

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

ofunction -	APP ID: K Your App ID > 🛹 View Analytics				
		Let us here	you find new ways to graw your ap	p. Click <u>here</u> to talk to our support leave. (	6
nga -					
		IOS	Android	Web	Other
~~~		1. Tell Us about Yo	ur Website		
		2. Set Up the Face	book SDK for Javascript		
98.					
		3. Check Login Sta	10.19		•
		4. Add the Facebo	ok Login Button		•
		5. Next Steps			-
		Congrats, you've ad documentation page Login Datog (3 Invoke the Login Dia	ded Facebook Login to yeer webs as for more advanced guides. alog using your own button instea	ifel Be sure to check out our other d of the Facebook Login bullon.	
		Access Tokens 🕑 Use the Access Tok	ens generated by Facebook Logi	n for your website.	
		Permissions 🗹 Manage what data y	our app has access to through Fe	icebook Login.	
		App Baview [2] Submit your app for audience.	review to ensure the best possibl	le Facebook experience for your app	
					Back

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

A	Client OAuth login is enabled but you haven't listed any valid OAuth redirect URIs. Click here for more information.							
Clien	t OAuth	h Settings						
Yes		Client OAuth Login Enables the standard OAuth client token flow. Secure your application and pre which token redirect URIs are allowed with the options below. Disable globally	vent abuse by locking down if not used. [?]					
Yes	•	Web OAuth Login Ho Force 1 Enables web based OAuth client login for building custom login flows. [7] When on Facebo- web. [7] Force 1	Web OAuth Reauthentication a, prompts people to enter their ik password in order to log in on the					
	No	Embedded Browser OAuth Login Enables browser control redirect un for OAuth client login. [7]						
Valio	d OAuth r ps://social	h redirect URIs						
	No	Login from Devices Enables the OAuth client login flow for devices like a smart TV (?)						
Deau	thorize	•						
Dea	uthorize	e Callback URL						
	hat shoul	uld we ping when a user deauthorizes your app?						
			Discard Save Changes					

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 [?]	ab o ment mode and can only be used by app admins, developers and testers 19 App ID
XOX	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

•	assa u Federation : Olumi Chent / Researce Server : Ditath Server										
						CAMP Cleft / Resource Server -	PingAccess -				
	_										
	- Saach										
ð	+ Name	•						* Mode	+ Provider	+ Application	Partition / Path
	Geogle							Client - Resource Server	Geogle		Common
Đ	érte										

- 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 + Profiles / Policies : Access Profiles (Per Session Policies)								
o . Access Proties Per-Request Policies Policy Sync Customization +								
P × Search							0	wale Import
v Status * Access Prolie Name	Application	· Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	· Partition / Path
🖸 🏓 acons		All	(seer)	(seet)	(none)			Common
🗆 🕨 social-ap		All	Ø Edt.	Export	Copy	default-log-setting		Common
Dekte_ Apply								

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

Access Policy: /Common/s	ocial-ap Edit Endings (Endinger	Allow, Deny [default])
Start)-failaidi +- OAuth Legen Page	Geogle + +0 Secole Chath Cleat Feedbox 1 + Geogle + +0 Secole Chath Cleat	teendul + -et- <u>Social Outh Scale</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Association</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Associ</u> <u>Social Vacialis Association</u> <u>Social Vacial Va</u>

Add New Macro

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

Log	an Authentication Assignme	ent [Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
	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
С	CRLDP Auth	Certificate Revocation List Distribution Point (CRLDP) client certificate authentication
0	HTTP Auth	HTTP authentication of end user credentials
С	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
С	NTLM Auth Result	NTLM authentication of end user credentials
0	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
۲	OAuth Client	OAuth Client
D	OAuth Scope	OAuth Scope
С	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
С	OTP Generate	Generate One Time Passcode (OTP)
C	OTP Verify	Verify One Time Pesscode (OTP)
С	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
С	RADIUS Auth	RADJUS authentication of end user credentials
Cano	el Add Item	RPE Franktig have be does and handland and and anon my deathch

- 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					
Iame: 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 Edit Endings (Endings Derry (default), Alow)						
Start hilask +- Oderhizeen Peer	Stands					

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

Logo	m Authentication Assignme	ent 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
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
	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	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
Canc	el Add Item	1996 Concertin have deviate and contraction of an diversion deviation

- 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	(Common/Facebook 😒				
Scopes Request	/Common/FacebookValidationScopesRequest 🗠				
Add new entry			Insert Before: $\underline{1 \lor}$		
Scope Name		Request			
public_profile /Common/FaceboolScopePublicProfile 😪 👔					
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

Log	on Authentication Assignme	nt Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose
	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
	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
	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
0	VMware View Policy	Specify a policy that will apply to VMware View connections
Can	cel Add Item	

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

Properties* Branch Rules	
Name: 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

Properties*	Branch Rules	
Name: Faceb	ook Variable Assign	
Variable As	ign	
Add new en	Insert Befo	re: 1 🗸
	Assignment	
1 session.lo change	ion.last.username = Session Variable session.oauth.scope.last.scope_data.public_profile.name	×
Cancel	*Data in tab has been changed, please don't forget to save)	Help

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	Asobr/	Access Policy					
Access	s Policy: ,	/Common/so	ocial-ap	idit Endings (Endinge: A	ilov, Dery (default	D	
Start	failback + _ [X-	Google +	Secole Olisth Client Facebook Olisth Client	Successful + -++- falback + -+) Successful + -++- falback + -+0	× Geode Okuth Score × Facebook Okuth Score	Second 4 +

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
	🗲 🛛 🗊 🖨 https://www.facebook.com/ 🛛 C 🔍 Search 🔄 🛱 🖾 🖉 🐇 🏦 🚳 🗸
	facebook 📟
Secure Logon for F5 Networks	
Choose a Social Logon Provi	Log into Facebook
 Google Facebook 	Email or Phone Number
Logon	Log In
	Create New Account
	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

Linked in • Developers	Home	Docs	Support	Partners	Blog	Logal	My Apps
My Applications					9	reate Ap	plication

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 I	Keys
------------------	------

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

Acce	Access in Federation : Oluth Chent (Resource, Sorier - Prender									
					GAuth Client / Resource Server +	PingAccess +				
		Search								Create
	Namo						· Type	OAuth Servers	⁰ Application	· Partition / Path
0	5						F5			Common
	acebook						Facebook	Facebook		Common
0.4	Joogle						Google	Google		Common
0.	fing .						Ping			Common
Delef										

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/~

And Construction 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				
General Properties Name LinkedIn Description					
Cancel Repeat Finished					

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

g + SAML Service Provider + SAML Identity Provider + SAML Descarces Okuth Authorization Server + Okuth Client / Resource Server + Proylecters	•			
	_			_
Easth				Create.
✓ + Name	Copy	· Type	* Application	+ Partition / Pat
C F5Aut/RedrectReport	Capy	auth-redirect-request		Common
C EStatesPresent	Cepy.	validation-scopes-request		Common
C FSTokerReheshRequest	Copy.	token-refresh-request		Common
FSTokenReguedByAuttzCode	Copy	token-request		Common
	6			

- 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	
1	
Parameter Type:	client-id ~
Parameter Name:	client_id
Add	
Parameter Type:	redirect-uri ~
Parameter Name:	redirect_uri
Add	
Parameter Type:	90003
r arameter 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	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 west
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 : GAuth Clerel / Researce Server : Request.									
	SAML Senice Provider + SAML detilly Provider + SAML Resources OAuth Autorization Server + OAuth Client / Resource Server + ProgAccess +									
					_					
1	- David				Create.					
4	* Name	Copy	+ Type	* Application	+ Partition / Pat					
	F5At/RedextReport	Capy .	auth-redirect-request		Common					
	FSBcookRequest	Cepy	validation-scopes-request		Common					
	FSTokerReheahRequest	Copy	token-refresh-request		Common					
	FSTokenRequestRyAuttzCode	Copy	token-request		Common					
	EST-classifier and and the second	1000	token encodet		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 C	Client / Resource Server : Request » New Request
General Properties	
Name	LinkedInValidationScopesRequest
Description	
Request Settings	
HTTP Method	GET V
Туре	validation-scopes-request \sim
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 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

econs + Federatios : Okath Clorel/Researce Server : Report										
10 • SAML Senice Provider • SAML Identity Provider • SAML Resources Oviuth Authorization Server • OAuth Client / Resource Server • P	Pegiccess +									
					_					
- Cearth					Create					
V Allana		Copy	+ Tipe	* Application	+ Partition / Path					
C FSAdtRodredReport		Copy	auth-redirect-request		Common					
C FS8condReamst		Cepy	validation-scopes-request		Common					
C FSTokenReheahRequest		Copy	token-refresh-request		Common					
E FSTokenRequedEpAdtr2Code		Capy	token-request		Common					
PL_EXTransformer#ultrenew#		Para	Initian particular		Poeneon					

- 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							
Conoral D	roportion						
Name	Topernes	LinkedInScopeBasicProfile					
Descripti	on						
Poquest 6	ottinge						
HTTP Me	ethod	GET V					
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	Headers	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-serverssi
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 + Profiles / Policies : Access Prodies (Per Session Policies)										
B • Access Prolies Per-Repet Polices Pelcy Sync Customization •										
F s faurt Crude inport.										
v Status * Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	· Patition / Path		
🗆 🏓 access		All	(none)	(seec)	(none)			Common		
🗆 🎽 sacial-ap		All	Ø Edit	Export	Сору	detault log setting		Common		
Deixte Apply										

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 🗸
2	none \checkmark	oauthprovidertyperopc	oauthprovidertyperopc	No 🗸		No $\!$
3	none \checkmark	username	username	No 🗸		No 🗸
4	none \checkmark	password	password	No 🗸		No 🗸
5	none \checkmark	field5	field5	No \vee		No 🗸

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 Option		Insert after la	st one 🗸 🗸
Valu	e	Text (Optional)	
1 Google		Google	V X
2 Facebook		Facebook	
3 LinkedIn		LinkedIn	
Cancel Finishe	d		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	plit domain from	full Username No	~			
c	APTCHA Configu	ration	e 🗸			
	Type	Post Variable Name	Session Variable Name	Clean Variable	Values	Read Only
1	radio 🗸	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 LinkedIn	××
Name: Google	a e X
Name: Facebook	× ×
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	<u>id</u>	
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 🗸 🗸
OAuth pro	vider is LinkedIn
Cancel	Add Expression

25. Click Finished on the Simple Expression tab

Simple* Advanced	
OAuth provider is LinkedIn	×
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: L	inked:	In	V
Name: LinkedIn	6	-	×
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 Tota in tab has been changed, please don't forget to save)		ł	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

 Scope: r_basicprofile 	*(Note	underscore)	*
---	--------	-------------	---

Properties* Branch Rules	
Name: LinkedIn OAuth Client	
OAuth	
Туре	Client V
Server	/Common/LinkedIn 💟
Grant Type	Authorization code \smallsetminus
Authentication Redirect Request	/Common/LinkedInAuthRedirectRequest \vee
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

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
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	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
\cap		nes e

- 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	/Common/LinkedInValidationScopesRequest	2			
Add new entry	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

Log	on 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	
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	
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	
Can	cel 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.firs
	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 Access Policy	
Access Policy: /Common/s	OCial-ap Edit Endings (Endings Allow, Deny (default))
Start) ^{(dised} + - Ofish icon. Peer	Linkelle + Liskelle Clark Clark Aller Liskelle Clark Clark Aller Songle + Gould Vanishe Assie Aller Songle + Gould Vanishe Assie Aller Songle + Gould Vanishe Assie Baller Songle + Gould Vanishe Assie Baller Songle + Gould Vanishe Assie Baller Songle + Songle Chark Songle + Gould Vanishe Assie Baller Songle + Songle Chark Baller Songle
	fallack + -12
	1-0 Deev

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

Acce	Access 1) Profiles / Policies : Per-Request Policies									
۰ تە	Access Profiles	Per-Request Policies								
					_					
٠	Creale Import									
	Per-Request Policy Name Per-Request Policy Export Copy Virbual Servers Parlion / Path						+ Partition / Path			
dynamic-prp				/P Edt	Export	Copy		Common		
Delet	e									

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

Access » Profiles / Policies : Pe	er-Request Policies
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 +	Allow
-------	------------	-------

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

Auth	entication Assignment End	point 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	
0	Empty	An Empty Action for constructing custom Branch Rules	
۲	HTTP Headers	Modify HTTP Headers	
0	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	
0	Protocol Lookup	Protocol Lookup	
0	Proxy Select	Proxy Select	
\bigcirc	Request Analytics	Request Analytics	
0	Response Analytics	Response Analytics	
0	SSL Bypass Set	SSL Bypass Set	
0	SSL Intercept Set	SSL Intercept Set	
0	SSO Configuration Select	Selection of configured SSO Config	
0	URL Branching	Simple branching rules based on the URL	
0	URL Filter Assign	Assign a Filter to lookup URLs	
Canc	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	roperties* Bran	ch Rules				
Na	me: HTTP Heade	rs]			
н	TTP Header Mod	lify				
4	Add new entry				Insert Befo	re: 1 🗸
	Header Operation	Header Name	Header V	'alue	Header Delimiter	
1	replace 🗸	X-Provider	%{session.logon.last	.oauthproviderty		X
2	replace 🗸	X-User	%{session.logon.last	username}		
н	ITP Cookie Modi	fy				
	Add new entry				Insert Bef	ore: 🗸
	Cool	kie Operation	Cookie Name	Cookie \	/alue	
(Cancel	(*Data in tab has been changed, ple	ase 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.

1. 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

Local	Traffic »	Virtual S	ervers : Virtual S	erver List							
÷	Virtual S	erver List		ist Statistics	-						
*				Search							Create
	 Status 	▲ Name			Description	Application	Destination	♦ Service Port	⇔ Type	Resources	
		dns_host_	resolver				10.1.20.99	53	Standard	Edit	Common
		social.agil	ity.com-vs				10.1.20.111	443 (HTTPS)	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.

Domo		Weber Testan Alberta	
Graha	m Alde	erson's Tasks	
Grana			
Home (5)	Profile 🗊 📕	-teaders 💼	
	-	soulTagliyaan	
connection			
upgrade-insec	ure-requests		
user-agent			
referer			
scoept-encodi			
scoept-langua	84		
x-provider			
		Grater Alderson	

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

Create the Virtual Server

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

Lo	Local Traffic » Virtual Servers : Virtual Server List											
\$	÷	Virtual S	erver List	Virtual Address List		-						
*				Se	arch							Create
	1	Status	▲ 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
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
SSL Profile (Server)	Selected Available (Common apm-default-serverssl crypto-client-default-serverssl serverssl serverssl
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 Set	nd 💙 Save 🗠	
Authorization Headers Body Pre-request Script Tests			Cookies Co	de
Type No Auth 🗸				
Note: Headers Tab View				
Authorization Headers Body Pre-request Script Tests			Cookies Co	de
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

Configure the Database Instance

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

Access - Federation : OAuth Authorization Server : Database Instance								
🚓 🗸 SAML Service Provider 👻			OAuth Authorization Server 👻			PingAccess +		
1	× Search							Create
🗹 🕴 Nano					OAuth P	'tolde	Partit	on / Path
 asuthdb 							Comr	non
Delete								

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

Access » Federation : OAuth Authorization Server : Scope								
⇔ -	SAML Service Provider +	SAML Identity Provider +		O/with /withorization Server +	O/uth Cik		Fing/access	-
*		Search						Create
	Name	Scope Name		Scope Value		Client Application		Partition / Path
No rea	cords to display.							
Delete								

- 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	shi	
Language	English	
Caption	HR API	
Detailed Description		
ecurity Settings		
Authentication Type	O None Secret Certificate	
	Selected	Availab
Scope +	oauth-scope-username	
	>>	
Grant Type		
	Resource Owner Password Credentials	
	Add https://www.getpostman.com/gauth2/callback	
Redirect URI(s)		
	~	
	Edit Delete	
oken Management Configuration	Edt[Delete	
oken Management Configuration Use Profile Token Management Settings	Edit Delete	

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 👻		PingAccess -				
Create									
						Partition / Path			
No records to display.									
Delete Download Resource Servers									

- 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	O None Secret C Certificate					
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	Pa	artition / Path
	auth							Co	mmon
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 » 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				
	Additional sections	is removed			
Cancel Repeat Finished					

Configure the APM Per Session Policy

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

Access in Profiles / Policies : Access Profiles (Per-Session Policies)								
a - Access Profiles Per-Request Policies Policy Sync Customization +								
Search							C	reate Import
👻 💌 Status 🔺 Access Profile Name	+ Application	· Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	· Partition / Path
D 🕨 access		AL	(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.

ŀ	lcces	s » Prol	files / Poli	cies : Access Profiles	(Per-Session Polici									
4	# -	Access F	Profiles											
						,								
ŀ				× Sear	rch								[Create Import
E		Status	Access	Profile Name			Application	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	+ Partition / Path
	0	p#	access					All	(none)	(none)	(none)			Common
		pe -	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

Logo	n Authentication Assignme	ent Endpoint Security (Server-Side) Endpoint Security (Client-Side) General Purpose	
0	Citrix Logon Prompt	Configure logon options for Citrix clients	
0	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)	
0	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication	
0 0	OAuth Logon Page Virtual Keyboard	OAuth Logon Page used for OAuth Client authentication Enables a virtual keyboard on the logon page for entering credentials	
0 0 0	OAuth Logon Page Virtual Keyboard VMware View Logon Page	OAuth Logon Page used for OAuth Client authentication Enables a virtual keyboard on the logon page for entering credentials Display logon screen on VMware View clients	

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

Properties Branch F	Rules					
Name: Logon Page]			
Logon Page Agent	licername	No				
CAPTCHA Configuratio	on	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	box Save Pass	word				
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	n Authentication Assignme	ent 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
$^{\circ}$	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
۲	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
0	OAuth Client	OAuth Client
0	OAuth Scope	OAuth Scope
Canc	el Add Item	

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 ∨ 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 fa	uccessful +→>-	Deny
				*>	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 f	allback + <u>Logon Page</u> fall	<u>back</u> + →>- OAuth A	X- Su Authorization fal	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 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	۲							
	Additional sections removed									
Cancel Repeat	Finished									

2.3.4 Task 3: Resource Server

Configure the OAuth Provider

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

Acc	Access » Federation : OAuth Client / Resource Server : Provider										
*					rver 🔻 C	DAuth Client / Resc	PingAccess				
*		Search						Create			
•	▲ Name				† Type	OAuth Servers	Application	Partition / Path			
	F5				F5			Common			
	Facebook				Facebool	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

Name	oauthas.f5agility.com-provider								
Description									
Туре	F5 T								
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

Ace	Access » Federation : 0Auth Client / Resource Server : 0Auth Server										
*		SAML Identity Provider 🝷	SAML Resources	rization Server 👻 OAuth Client / Re			ource Server 🝷	PingAccess			
*		Search							Create		
•	▲ Name				A Mode		+ Provider	Application	Partition / Path		
	Facebook				Client + Resource	Server	Facebook		Common		
	Google				Client + Resource	Server	Google		Common		
	LinkedIn				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	•
DNS Resolver +	oauth-dns 🔻	
	Selected	Availab
iRules	 < >> 	/ Common _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

Ac	Access » Profiles / Policies : Access Profiles (Per-Session Policies)										
₿	Access Profiles Per-Request Policie										
										_	
치				Search						C	reate Import
v	💌 Status	Access	s Profile Name	Application	on 💠 Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Servers	+ Partition / Path
	Dia 1	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 T

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

Acce	Access » Profiles / Policies : Access Profiles (Per-Session Policies)												
Access Profiles Per-Request Policies		Policies f											
*				Search	h								Create
	▼ Status	▲ Access	Profile Name	Applica	ation 🗢 F	Profile Type	Per-Session	n Policy	Export	Сору	Logs	Virtual Servers	≑ Partitic
	p#	access			All		(none)		(none)	(none)			Common
	p#	api-ap			OA	Auth-Resource Ser	ver 🗖 Edit		Export	Сору	default-log-setting		Common
	p#	social-ap			All		🗖 Edit		Export	Сору	default-log-setting	social.agility.com-vs	Common

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

6	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

Acces	Access » Profiles / Policies : Per-Request Policies									
⇔ -		Per-Request Policies			-					
*	Search Create Import									
•	Per-Request Policy Name				Per-Request Policy	Export	Сору	Virtual Servers		tion / Path
🔲 p	prp-x-user-insertion			🗖 Edit	Export	Сору	social.agility.com-vs	Commo	n	

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						
v	Per-Request Policy Name Per-Request Policy Export					Export	
🗖 api-prp 🗖 Edit Expor					Export		
	prp-x-user-insertion Expor					Export	

12. Click Add New Subroutine

Per-Request Policy: /Common/api-prp Edit				
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

Logo	n Authentication Assignme	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
Cance	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

Local	Local Traffic » Virtual Servers : Virtual Server List									
🛪 🚽 Virtual Server List Virtual Address List Statistics 🔫										
*			Se	arch						
	 Status 	▲ Name				Description	Application	Destination		
		api.f5agility.com-vs						10.1.20.112		
		dns_host_resolver								
		social.agility.com-vs						10.1.20.111		

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 T					
Per-Request Policy	api-prp 🔻					
VDI Profile	None T					
Application Tunnels (Java & Per- App VPN)	Enabled					
OAM Support	Enabled					
PingAccess Profile	None T					
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	 ✓ ⑤ ⋠
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	k 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	F	No Environment	· · • •
▶ Test API Call			
GET V https://a	api.f5agility.com/department	Params	Send 💙 Save 🗡
Authorization Headers	Body Pre-request Script	Tests	Cookies Code
Туре	No Auth		
Body Cookies Head	No Auth Basic Auth	Status: 401 Unauthoriz	ed Time: 250 ms Size: 93 B
Connection -> Close	Digest Auth OAuth 1.0		
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	a714c196289cb770a45 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	04a714c19628 903a5bf770dd	9cb770a45 3
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 🔻
 Authorization 		Bearer c89884a4df2e89f40)d14939497bab069385c5410ba

11. Click Send at the top of the Postman screen

GET \smallsetminus	https://ap	Params	Sei	nd 🗸	Sav	e 🗸				
Authorization	Headers (1)		Pre-request	Script	Tests				Cookie	s Code
Туре		OAuth 2.0	~							
Existing Tokens		Get Ne	w Access Toke	n	MyToken			Delete	Use	Foken
MyToken					Add token to	Header	\sim			
					access_toke n	e ec42165e10611860001db5bac66f8d6db6 339f242a9f7d5824ec0ab7a93408			626	
					expires_in	300				
					token_type	Bearer				

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	Preview	JSON 🗸	₽				ΓQ
1 • 2 • 3 4	("WATER "POLIC "GENER	ents": [MGMNT", E", AL SERVICES"	2					

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

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	Display Options								
Auto Refresh	Disabled	▼ Refr	resh						
Refresh Session Table									
Total Active Sessions									
Active Session Count	1								
*	* Search								
💌 💌 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.

			_		scone	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 "GENER	ents": [MGMNT", ", AL SERVICES"	,					

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.

Acces	ss » Overview : OAuth Reports : Tok	ens							
	Active Sessions Access Reports	OAuth Reports 👻	SWG Reports 👻 E	vent Logs 🛛 👻					
0	OAuth Tokens Revoke Refresh								
DI	DB Instance: Access Token Issued: *								
/Co	ommon/oauth-api-db 🔻 Last week	• U	ser or Client App	Search					
	User ~	Client App 🛛 🗸	Access Token Issued 😽	Access Token Expires ${}^{\prime}$	Access Token Status 🗸	Refresh Token Issued Y			
	/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	-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	cess » Overview : OAuth Reports : Takens									
\$ -	Active Sessions Access Reports	OAuth Reports 👻	SWG Reports 👻 E	ivent Logs 🛛 👻						
0	DAuth Tokens Revoke Refresh									
DE /Co	DB Instance: Access Token Issued: Image: Common/Oauth-api-db Image: Common/Oauth									
~	User ~	Client App ~	Access Token Issued 😽	Access Token Expires 🗸	Access Token Status 🗸	Refresh Token Issued ~ F				
~	/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				

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									
Total Active Sessions									
Active Session Count	1								
*	* Search								
💌 💌 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="invalid_token",error_description="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)

Acce	ss » Overview : Acc	ess Reports						
\$ -	Active Sessions	Access Reports	OAuth Reports 🛛 👻	SWG Report	s 🔻	Event Logs	-	
Repo	orts Browser	~	All Sessions 🛞					
Favo	rites	+	😣 Export to CSV File	🔣 Show in Pop	up Window	/ 🗾 View Repo	ort Constraints 🗼 S	et to default repor
Built	In Reports	-	Local Time	Session ID	Logon	Active	Session Variables	State
🙀 F	avorite	💽 Run	2017-05-30 23:45:27	975c3806	user	N	View Session Variak	oles
A A			2017-05-30 23:44:45	<u>12b6d17e</u>	user	N	View Session Variak	oles
ACL	Summary (Session ID)	•	2017-05-30 23:39:02	e0804cb9	user	N	View Session Variak	oles
ACL	Summary (All Sessions)	1	2017-05-30 23:29:31	<u>4e9abf2f</u>		N	View Session Variak	oles
Alloy	wed ACL Details (Sessi	n ID)	2017-05-30 23:25:34	<u>92218414</u>	user	N	View Session Variak	bles
Allov	wed ACLs (All Sessions	2)	2017-05-30 23:14:59	<u>c5c2800e</u>	user	N	View Session Variak	oles
Deni	ied ACL Details (Sessior	n ID)	2017-05-30 23:09:36	75eed6b0	user	N	View Session Variak	oles
Deni	ied ACLs (All Sessions)		2017-05-30 22:53:17	0c6b03d2	user	N	View Session Variak	oles
	······		2017-05-30 22:24:41	<u>c851f7ad</u>	user	N	View Session Variak	bles
B	'owser/App Reports		2017-05-30 22:19:38	5a3c7d6b		N	View Session Variak	oles
App	lication and OS Distribut	ion	2017-05-30 22:12:10	9008d848	user	N	View Session Variab	<u>oles</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.

Access » Overview : Active Sessions									
🔅 👻 Active Sessions	Active Sessions Access Reports				SWG Rep	orts 👻	Event Logs	s 🔻	
Display Options									
Auto Refresh	Auto Refresh Disabled V Refresh								
Refresh Session Table									
Total Active Sessions									
Active Session Count		1							
*	* Search								
Status +	♦ Se	ssion ID	Variables	▲ Use		Client IP		Start Ti	
	df4a5	200	View	Chas L	esley.	192.168.18	7.169	2017-05-3	
Kill Selected Sessions									

 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 : Active Sessions										
🔅 👻 Active Sessions	Acce	ss Reports	OAuth Rep	orts 👻	SWG Report		Event Log			
Display Options	Display Options									
Auto Refresh		Disabled	Refre	sh						
Refresh Session Table	Refresh Session Table									
	,									
Total Active Sessions										
Active Session Count		1								
*	* Search									
🖌 💌 Status 🛛 🛨	\$ Se	ession ID	Variables	▲ Use	r ¢	Client IP		Start Ti		
	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	ccess » 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						Λ	
	0.01							
	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	Ξ	😣 Export to CSV File	🔛 Show in Popup Window 🛐 View Report Constraints Current default report name: "All Sessions"
🙀 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 192.168.18
		2017-05-31 13:49:24	$eq:common/social-ap:Common/social-ap_act_oauth_client_1_ag: OAuth Client: authorization_code auth_client_1_ag: OAuth Client_1_ag: OAUth Cl$
		2017-05-31 13:49:24	/Common/social-ap:Common:df4a5200:/Common/social-ap_act_oauth_client_1_ag: OAuth Client: User redirected to a
		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 sen
		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 si
		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 CPI
		2017-05-31 13:50:15	/Common/social-ap:Common:df4a5200: Start (fallback) OAuth Logon Page (Facebook) Facebook OAuth Client (Si

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.

Access » Overview : Event Logs : Settings								
🚓 🗸 Active Sessions 🛛 Ac		Access Reports	OAuth F	Reports 👻	SWG Reports 🛛 🔫		Event Logs	•
	,,							
	Name 🔺	Description		Access Syste	em Logs	URL Requ	iest Logs	Access
	default-log-setting	Default log sett	ing for	Enabled		Enabled		<u>api-ap</u>
	Edit Dele	te						

Edit APM Log Setting		^
 General Information Access System Logs URL Request Logs Access Profiles SSO Objects 	Publisher*: /Common/sys-db-access-publis Access Policy : Notice ACL : Notice Secure Web Gateway : Notice OAuth : Notice VDI : Notice VDI : Notice VDI : Notice VDI :	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						
212 packets captured 2 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 SWG: Securing Outbound Internet Access

3.2.1 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

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

Access » Authentication » A	D_F5DEMO				
Properties Groups					
General Properties					
Name	AD_F5DEMO				
Partition / Path	Common				
Туре	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			
Update Delete	,				

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

1	Access » Profiles / Policies : Access Profiles (Per-Session Policies)											
1	0 -	Access I	Profiles	Per-Request	Policies	Polic	cy Sync	Customization -				
*	* Search											
6		Status	 Access 	Profile Name	Applic	ation	Profile Type	Per-Session Policy	Export	Сору	Logs	Virtual Se
0		p#	AP_Explic	cit_Auth			SWG-Explicit	Edit	Export	Copy	default-log-setting	
] #	access				All	(none)	(none)	(none)		

• 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					
Name: HTTP 407 Response					
407 Response Settings					
Basic Auth Realm					
HTTP Auth Level	basic 🔻				
Customization					
Language	en T				
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

Begin typing to search					
Logo	Authentication Assignme	nt Endpoint Security (S			
0	AD Auth	Active Directory authen			
0	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 🔻				
Server	/Common/AD_F5DEMO V				
Cross Domain Support	Disabled 🔻				
Complexity check for Password Reset	Disabled V				
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
| 6 Apply Access Policy | |
|--|----------------------------------|
| Access Policy: /Common/AP_Explicit_Auth Edit Endings | (Endings: Allow, Deny [default]) |
| Start $fallback$ + $gasic$ | |
| HTTP 407 Response Negotiate | |
| T - 27 | Select Ending |
| fallback + →> | |
| | 🔘 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 Add Macro button to add a purpose-built set of pr | |

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, 20	17 User: admin 1907) – Bole: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	Access » Secure Web Gatewa	y:URL Filters » LAB_URL_FILTER
Statistics	🔅 👻 Properties	
iApps	General Properties	
🔁 Wizards	Name	LAB_URL_FILTER
Col Orchastrator	Partition / Path	Common
SSE OFCIRESTICIO	Description	
Local Traffic	Update Delete	
C Traffic Intelligence		
	Associated Categories	
Acceleration	Category	Sub-Category
Access	Custom Categories	
Quantian	🔽 🗈 Abortion	
	🔽 🗈 Adult Material	
Profiles / Policies	Advocacy Groups	
Authentication	- Autocacy croups	
Single Sign-On	🗹 🖾 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)

	Religion	0
	Security	0
	Shopping	0
	Social Organizations	Θ
V 🗈	Social Web - Facebook	8
	Social Web - LinkedIn	Θ
	Social Web - Twitter	0
	Social Web - Various	Θ
	Social Web - YouTube	Θ
	Society and Lifestyles	Θ
	Special Events	0
	Sports	Θ
	Tasteless	Θ
	Travel	Θ
	Vehicles	Θ
	Violence	Θ
	Weapons	Θ
Allow	Confirm Block	

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

8	Access » Profiles / Policies : Per-Request Policies						
	🚓 🗸 Access Profiles	Per-Request Policies	Policy Sync	Customizat			
1				_	_		
	*	Searc	h 🖌			C	reate Import
	Per-Request Policy	Name	Per-Request Polic	y Export	Сору	Virtual Servers	Partition / Path
	Lab_Per_Request		🗗 Edit	Export	Сору		Common
ĺ	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	cy: /Common/Lab	Per Request Edit Endings (Endings: Allow, Reject [default])
Startfallback	Beg	in typing to search	
Add New Macro	Auth	entication Assignment End	point Security (Server-Side) General Purpose
	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	\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
	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 I	${fallback} + \rightarrow \rightarrow \frac{Allow}{Reject}$		
Add New Macro				
Add New Subroutine	Beg	in typing to search		
	Auth	entication Assignment End	point Security (Server-Side)	
An access policy consist action, click on the x 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 F	Rules
	0	HTTP Headers	Modify HTTP Headers	
		iRule Event	Raises an iRule ACCESS PER RECHEST 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

6	
*Per-Request Policy: /Common	n/Lab_Per_Request Edit Endings (Endings: Allow, Reject [default])
Start	$+ \rightarrow - \underbrace{Category \ Lookup}_{k} fallback}_{k} + \rightarrow - \underbrace{Allow}_{k} + and and a content of the second $
Add New Macro	Properties* Branch Rules Name: URL Filter Assign
Add New Subroutine Add New Subrouti An access policy consists of a start point, action	URL Filter /Common/LAB_URL_FILTER Note: To supply categories, a Category Lookup item must occur in the per-request policy before runs.

Important: Change the Ending of the Allow outcome on the "fallback" branch from "Reject" to Allow

<u>6</u>	
Per-Request Policy: /Comr	mon/Lab_Per_Request [Edit Endings] (Endings: Allow, Reject [default])
Start fallback +	X HTTPS +

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 inline help				
Do you want to enable advanced options?	No, do not enable advanced options			
Which type of SWG configuration do you	Explicit Proxy			
Do you want to use ICAP to forward requests	No. do not uso ICAP for DLP			
for inspection by DLP servers?				
What IP address and port do you want to use				
for the virtual server?	– IP Address: 10.1.20.200			
	– Port: 3128			
What is the FQDN of this proxy?	proxy.f5demo.com. The local hosts file on			
	your Jump Host has already been modified to			
	indicated above			
On which ports should the system accept	80			
HTTP traffic?	00			
On which ports should the system accept	443			
HTTPS traffic?				
Which SWG-Explicit Access Policy do you	AP Explicit Auth			
want to use?				
Which Per-Request Access Policy do you	Lab_Per_Request			
want to use?				
Do you want the system to forward all name	Yes, forward all name requests			
requests?				
Which DNS servers do you want to use for	– IP: 10.1.20.20			
forwarding?	– Port: 53			
Which SSL profile do you want to use for	Create a new Client SSL profile			
client-side connections?				
Which Subordinate CA certificate do you	f5agility.crt			
want to use?				
Which CA key do you want to use?	f5agility.key			
Does the key require a password? If so, type	F5labs			
	0			
which SSL profile do you want to use for	Create a new Server SSL profile			
server-side connections?				

2. Click Finished – you will see a large number of objects created for you on the Components tab.

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.

Internet Options		?	8		
General Secur	ty Privacy Content Connections	Programs Advance	d		
Certificates -					
Us	certificates for encrypted connection	ns and identification.			
Clear	SL state Certificates	Publishers			
AutoComplete	Certificates				×
on for	Intended purpose: <a>				•
Feeds and We	Intermediate Certification Author	rities Trusted Root Ce	ertification Aut	norities Trusted Pub	• •
	Issued To Iss	ued By	Expiratio	Friendly Name	
pro	Entrust Root Certifi Ent	trust Root Certifica	11/27/2026	Entrust	
	Entrust Root Certifi Ent	trust Root Certifica	12/7/2030	Entrust.net	
	Entrust.net Certific Ent	trust.net Certificati	7/24/2029	Entrust (2048)	=
	Equitax Secure Cer Equ	Arithe CA	8/22/2018	GeoTrust	
	GeoTrust Clobal CA	Agiirty CA oTrust Global CA	5/21/2022	GeoTrust Global CA	
	GeoTrust Primary Com Geo	oTrust Primary Cer	12/1/2022	GeoTrust Primar	
	GlobalSign Glo	balSign	3/18/2029	GlobalSign	
	GlobalSign Root CA Glo	balSign Root CA	1/28/2028	GlobalSign	-
	Import Export	Remove		Advar	nced
	Certificate intended purposes				
	<all></all>				
				View	
	Learn more about <u>certificates</u>			Clo	se

• Double-click on the certificate to view its properties, then close this window and the Certificates window.

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 -	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

https://www.wellsfarg	io.com/	Q - A d
	Website Identification	×
	F5 Agility CA has identified this site as: www.wellsfargo.com	
	This connection to the server is encrypt Should I trust this site?	ed.
	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.



3.2.2 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)

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

65				
Per-Request Policy: /Com	nmon/Lab_Per_Request_SSL	Bypass Edit Endings (Endings: Reject	[default], Allow)	
Start Fallback +	HTTPS +	$\begin{array}{c} \text{Banks} + \rightarrow & \underbrace{\text{SSL Bypass Set}}^{\text{K}} \text{fallback} + \rightarrow & \\ & \underbrace{\text{fallback}}^{\text{K}} + \rightarrow & \underbrace{\text{SSL Intercept Set}}^{\text{K}} \text{fallback} + \rightarrow & \\ & \underbrace{\text{fallback}}^{\text{K}} + \rightarrow & \underbrace{\text{SSL Intercept Set}}^{\text{K}} \text{fallback} + \rightarrow & \\ \end{array}$	Bypass URL Filter 	Allow + \rightarrow Allow Confirm + \rightarrow Reject fallback + \rightarrow Reject Allow + \rightarrow Allow Confirm + \rightarrow Allow Confirm + \rightarrow Reject fallback + \rightarrow Reject fallback + \rightarrow Reject
	fallback +			Allow

Add New Macro

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

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



3.2.3 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)

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!

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	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

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 NTLM Auth Result Fallback +->- Deny	

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

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 🗵	Activo Soco
Favorites	Ξ	😣 Export to CSV File	🔛 Show in Popup Window 📳 View Report Constraints Current default report name: "All Sessions"	Active Dest
🙀 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.	🛛 🔽 🔽 Sta
		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 roun: SWG-Explicit	
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c; Received client info - Hostname: Type: IE Version: 11 Platton, vin7 CPU: unknown UI Mode: Full Javascript Support: 1 Active	Kill Selecte
		2017-06-20 10:22:58	/Common/AP_Explicit_NTLM:Common:bfde395c: Start (fallbary) NTLM Auth Result (Successful) Allow Endine 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_Techr	

3.2.4 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)

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.

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: bigiqt.f5ogiity.com IP Address: 10.1.1.30 Time: Jul 07, 2017 20.59(PDT) Administrator admin 🛓
Monitoring Configuration	Deployment Devices System
< ALERTS & NOTIFICATIONS	Summary
▶ AUDIT LOGS	CSV Report Refresh
▼ DASHBOARDS	ALL So MOUNDENT ALL SO AND A
▼ Access	
Application Summary	U 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 Fri
▶ Federation	
▶ Sessions	REQUEST COUNTS PER ACTION OVER TIME
User Summary	AVG # requests / 11 days — Allowed — Blocked — Overall
▶ Logging Messages (All)	d d
Remote Logging Configuration	20,000
▶ Secure Web Gateway	15.000
▶ Device	
DNS	18.899
▶ Local Traffic	
▶ REPORTS	3.000
► EVENTS	
	Thu 15 Sat 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 CO
	www.google.ena/tics70 III S Set Uritigiues ature2020 State S
	agress contended by the second s

Click on SSL Bypass and view the breakdown between HTTPS Inspected and Bypassed Content

🚯 BIG-IQ	🔹 stanoalaore Hostinare bayat Isayaty sayaty
Monitoring Configuration	Deployment Devices System
ALERTS & NOTIFICATIONS	SSL Bypass
▶ AUDITLOGS	CSV Report Refresh
▼ DASHBOARDS	ACCSS GROUNDVICE TIMEFRAME: All Managed Devices (SW) V Last 30 days V Show Blocked
▼ 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 Fri7 U
▶ Federation	
▶ Sessions	TOP 5 55L BYPASS BY CONNECTION COUNT OVER TIME
User Summary	AVG # connections / 11 days
▶ Logging Messages (All)	
Remote Logging Configurat	20,000
▼ Secure Web Gateway	1.000
Applications	Lune
Application Families	10,000
Categories	
Client IP Addresses	3,000
Host Names	
SSL Bypass	Thu 15 Sat 17 Mon 19 Wel 21 Fri 23 jun 25 Tue 27 Thu 29 july Mon 03 Wed 05 Fri 07 jul 09
SWG Logs	
URL Filters	Top 1000 SSL Bypass by Connection Count

• Click on Host Name to look at the hosts your users are accessing

🚯 BIG-I	Q						Stan	dalone Hostname:	bigiq1.f5agility.com	IP Address: 10.1.1.30) Time: Jul 07, 201	17 21:01(PDT)	Administrator	admin <u>‡</u> √
Monitoring	Configuration	Deployment	Devices	System										٩
ALERTS & NOTIFI	ICATIONS	Host Names												
▶ AUDITLOGS													CSV Report	Refresh
▼ DASHBOARDS		All Managed De	vices (SWG)	Last 30 days	•	Show Blocked								
▼ Access					F	Requests		III						
Application S	Summary	II Fri 9	Sat Sun M	on 12 Tue Wed 1	Thu Fri16	Sat Sun Mo	m 19 Tue Wed 2	21 Thu Fri 23 9	at Sun Mor	26 Tue Wed 28 Th	u Fri 30 Sat 1	Sun Mon 3	Tue Wed 5	Thu Fri 7
▶ Federation														
▶ Sessions						тс	P 5 HOST NAME	S BY REQUEST CO	UNT OVER TIM	E				
User Summa	ry			-o- www.googl	.com —	 www.google-ar 	halytics.com	-o- ssl.gstatic.co	om – o–	pagead2.googlesyndic	ation.com -	-o- dlptest.com	m — 🔶	- Overall
▶ Logging Mes	sages (AII)	AVG # re	quests / 11 days											
Remote Logg	ging Configurat ≡	300 👡	<											
▼ Secure Web (Gateway	250												
Application	ns	200												
Application	n Families	150												
Categories														
Client IP Ac	ddresses	100				\sim								
Host Name	25	50 0												
SSL Bypass	;	0 8-	Sat 17	Mon 19	Wed 21	Fri 23	jun 25	Tue 27	Thu 29	july M	o Ion 03 Wea	105 F	Fr1 07	[ul 09

• Click on **URLs** to get detail on what URLs your users are accessing

🚯 BIG-IQ	🐠 Standalone Hostnamerbigigt,f5agilty.com 12-Address:10.1.1.30 Timer.Jul 07, 2017-21:02,PDT) Administrator admin 🛓	+ 1
Monitoring Configuration	Deployment Devices System	a)
ALERTS & NOTIFICATIONS	VRLs	
▶ AUDIT LOGS	CSV Report Refrest	ah
▼ DASHBOARDS	ACCESS GROUP/DEVICE: TIMEFRAME: All Managed Devices (SWG) V Last 30 days Show Blocked	
▼ Access	Nequests	_
Application Summary	u Fri9 Sat Sun Mon12 Tue Wed14 Thu Fri16 Sat Sun Mon19 Tue Wed121 Thu Fri23 Sat Sun Mon26 Tue Wed28 Thu Fri30 Sat1 Sun Mon3 Tue Wed5 Thu Fri7	U
▶ Federation		
▶ Sessions	TOP 5 URLS BY REQUEST COUNT OVER TIME	
User Summary		
▶ Logging Messages (All)		
Remote Logging Configurat		
▼ Secure Web Gateway	20,000	
Applications		
Application Families	15,000	
Categories	10,000	
Client IP Addresses		
Host Names	3,000	
SSL Bypass		
SWG Logs	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	-0
URL Filters		
LIRI s	✓ Fiter	T
UNCS		

3.2.5 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)

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

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

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.

3.2.6 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)

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 Branch	n Rules					
Vame: Logon Page						
Logon Page Agen	t					
Split domain from fu	II Username	No 🔻				
CAPTCHA Configura	ation	None 🔻				
Туре	Post Vari	iable 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 🔻
1 none T	field4		field4	No 🔻		No 🔻
5 none V	field5		field5	No 🔻		No 🔻
Customization						Import
Language en Reset all defaults						
Form Header Text Secure Logon for F5 Networks						
Logon Page Input Field #11 ^{lenter} email address						

- Click Save
- Click on the **Deny** ending and change it to **Allow**
- Click Apply Access Policy

<u>f5</u>	
Access Policy: /Common/AP_Transparent_Captive_Portal	Edit Endings
Start	

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

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.

3.2.7 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

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

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.









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.