Agility 2018 Hands-on Lab Guide

Contents:

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:

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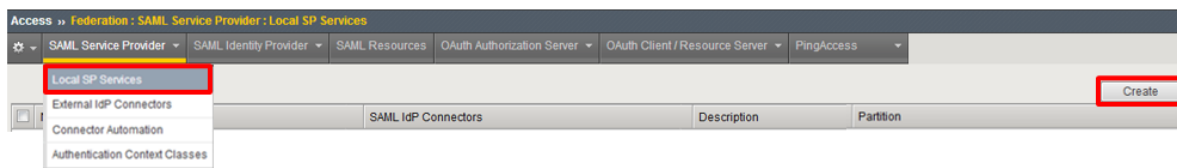
3. In the **Create New SAML SP Service** dialog box click **General Settings** in the left navigation pane and key in the following as shown:

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

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

Create New SAML SP Service

General Settings
Endpoint Settings
Security Settings
Authentication Context
Advanced Settings

Name*:
app.f5demo.com

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

SP Name Settings
Scheme :   Host :
https

Description :

Relay State :

OK   Cancel

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

IdP Connector

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
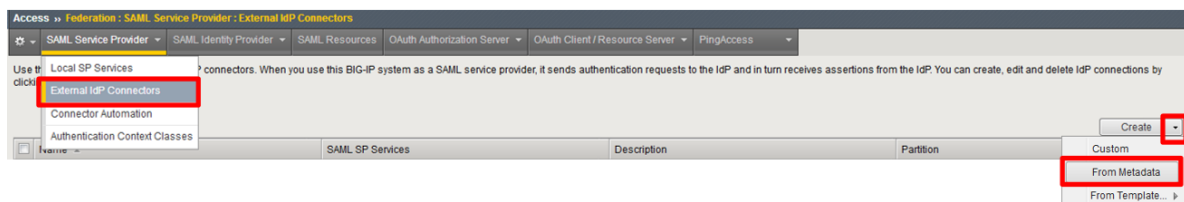
4. In the **Create New SAML IdP Connector** dialogue box, click **Browse** and select the **idp.partner.com?app_metadata.xml** file from the Desktop of your jump host.

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 Connectors** at the bottom of the GUI

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

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

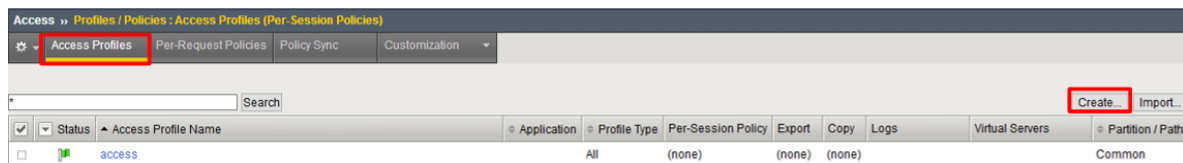| Name:	`app.f5demo.com`
SAML IdP Connectors:	`idp.partner.com`

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)

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.
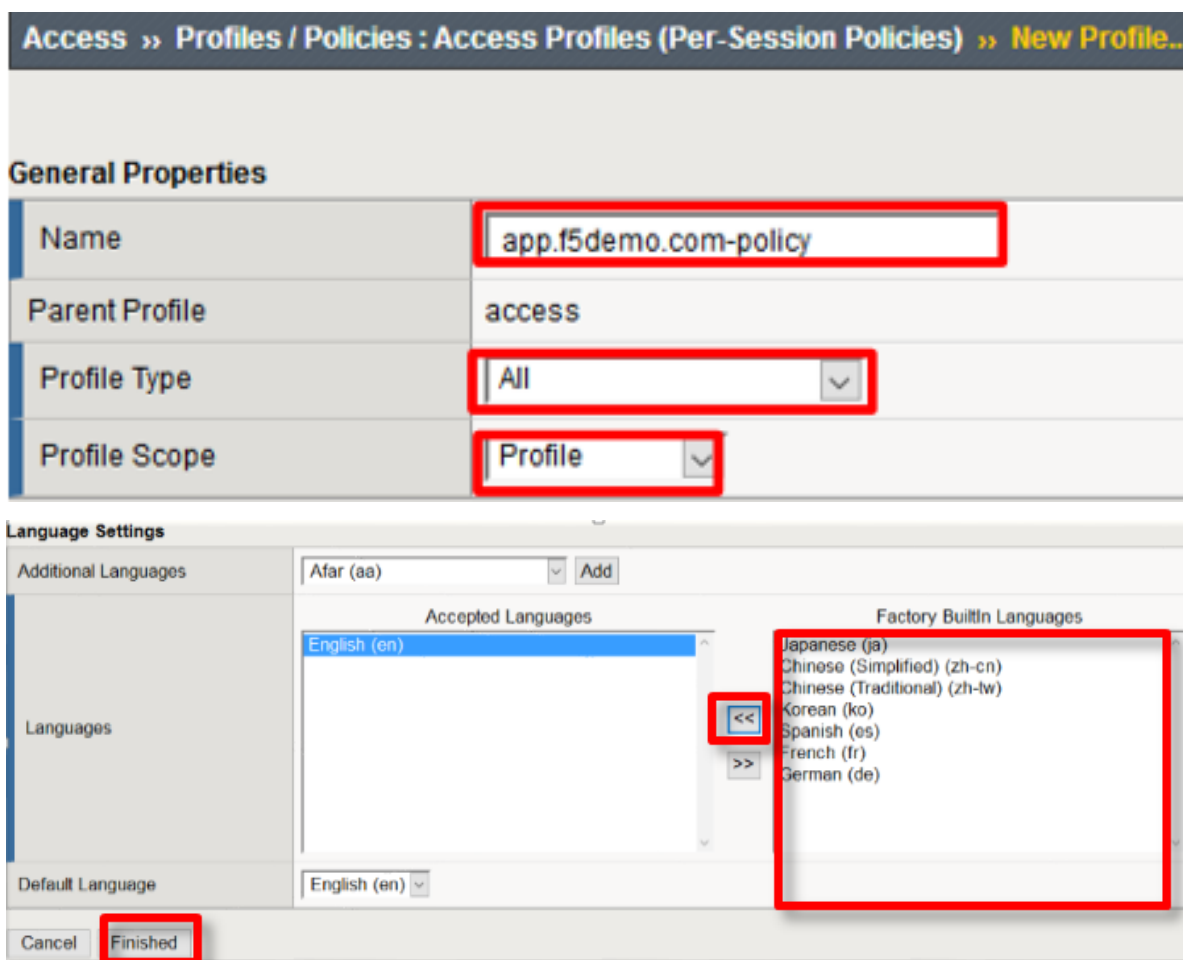
6. From the **Access ?> Profiles/Policies ?> Access Profiles (Per?Session Policies)** screen, click the **Edit** link on the previously created `app.f5demo.com?policy` line
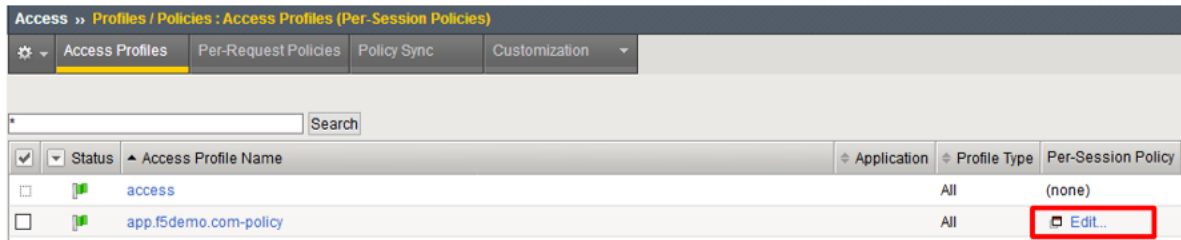
7. In the Visual Policy Editor window for `/Common/app.f5demo.com?policy`, click the **Plus (+) Sign** between **Start** and **Deny**
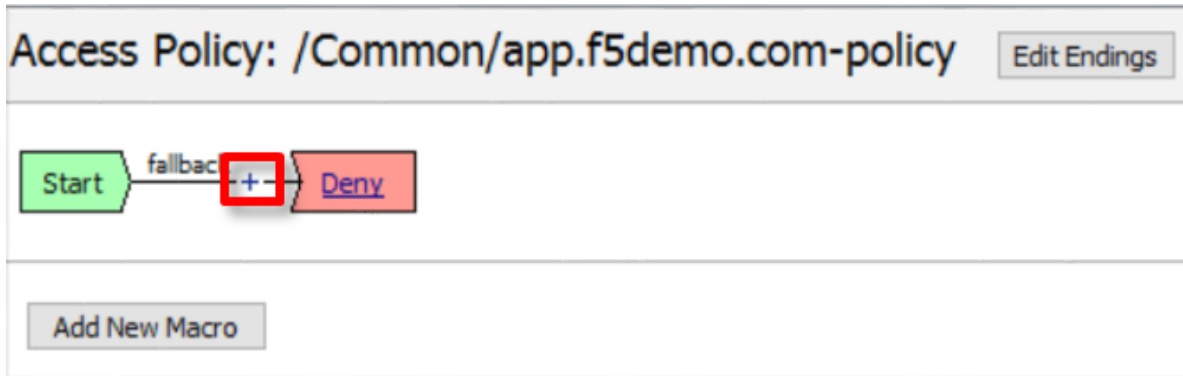
8. In the pop?up dialog box, select the **Authentication** tab and then click the **Radio Button** next to **SAML Auth**

9. Once selected, click the **Add Item** button
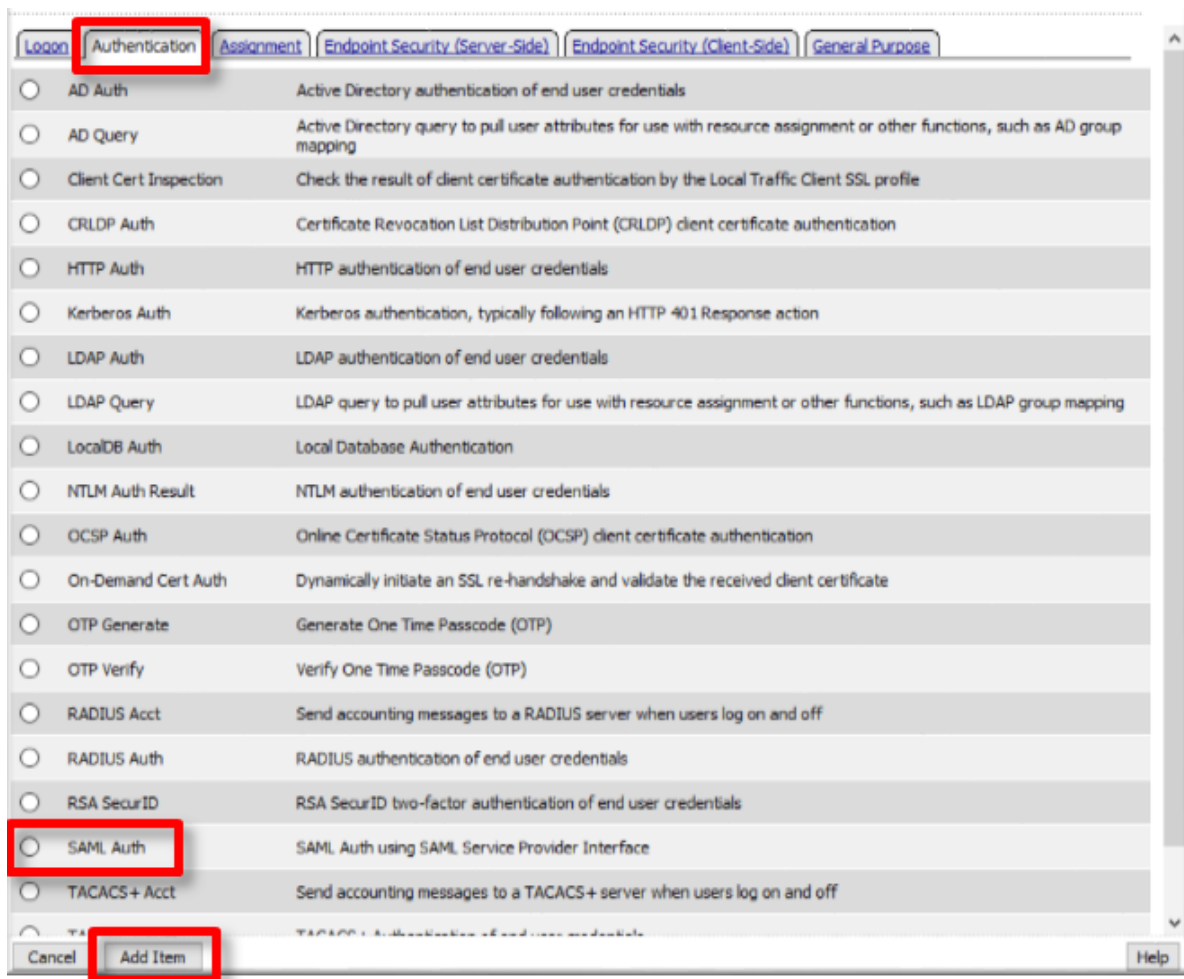
10. In the **SAML Auth** configuration window, select `/Common/app.f5demo.com` from the **AAA Server** drop down menu

11. Click the **Save** button at the bottom of the window
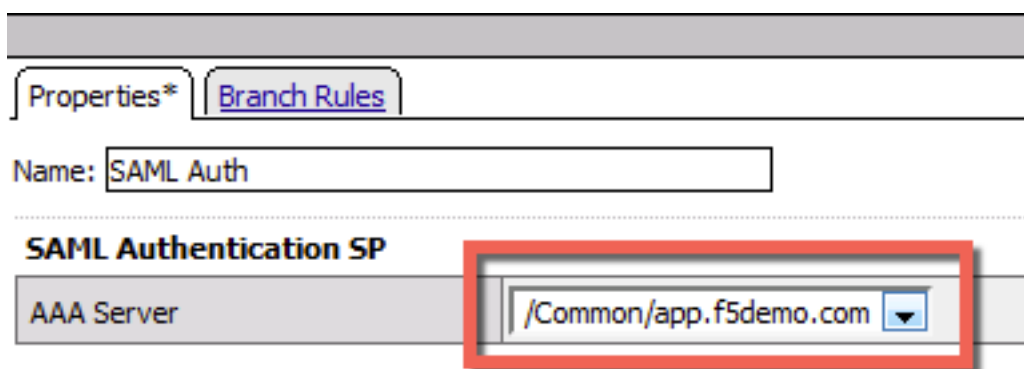
12. In the **Visual Policy Editor** window for `/Common/app.f5demo.com?policy`, click the **Plus (+) Sign** on the **Successful** branch following **SAML Auth**

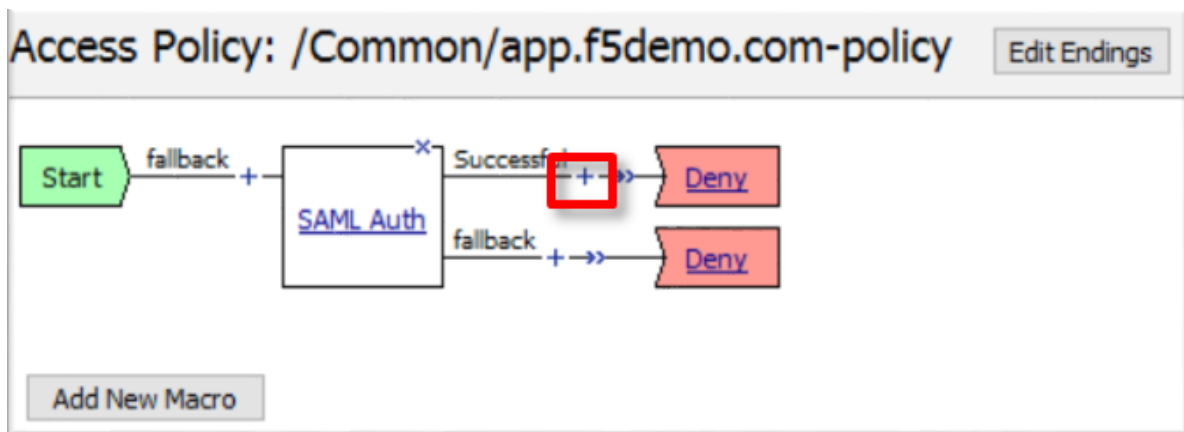Access Policy: /Common/app.f5demo.com-policy [Edit Endings]

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

| Logon | Authentication | Assignment | Endpoint Security (Server-Side) | Endpoint Security (Client-Side) | General Purpose |

○	ACL Assign	Assign existing Access Control Lists (ACLs)
○	AD Group Resource Assign	Map ACLs and resources based on user Active Directory group membership
○	Advanced Resource Assign	Expression-based assignment of Connectivity Resources, Webtop, and ACLs
○	BWC Policy	Assign Bandwidth Controller policies
○	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

Cancel   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
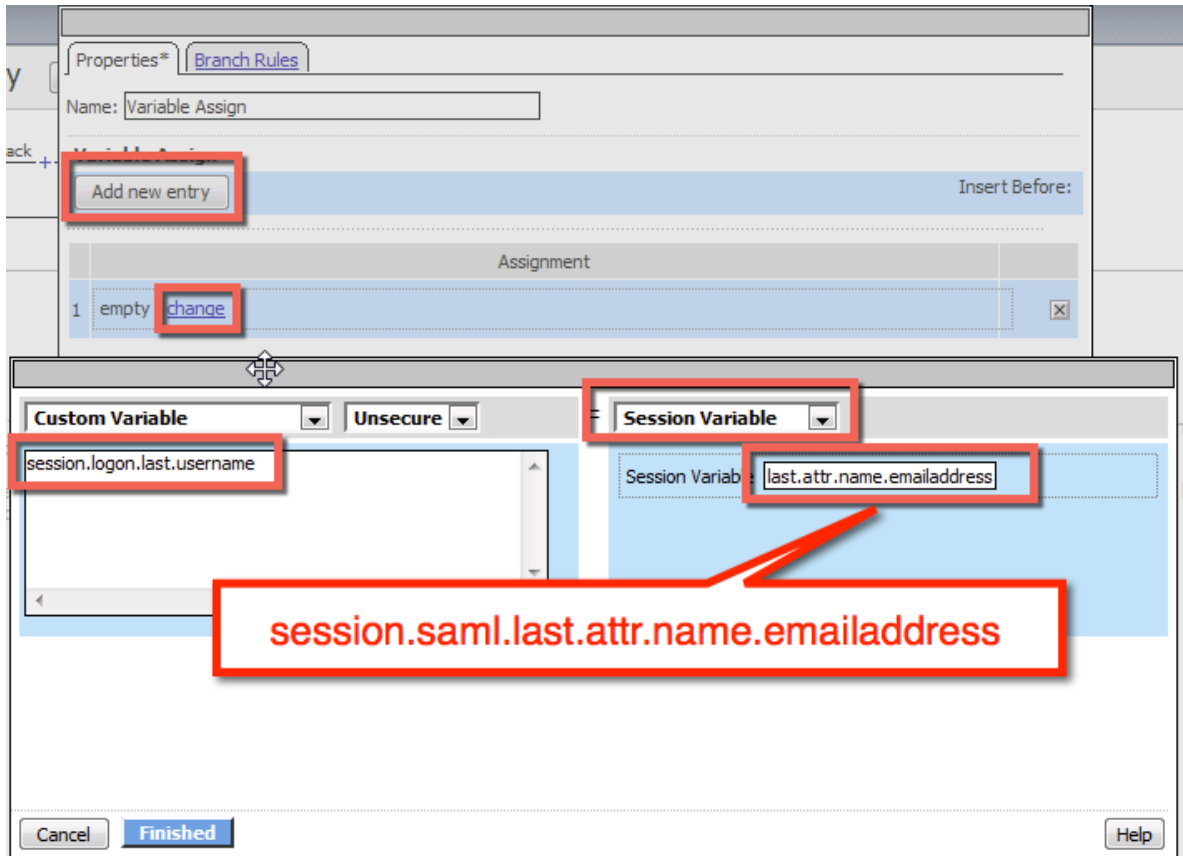
20. In the **Visual Policy Editor** select the **Deny** ending along the **fallback** branch following the **Variable Assign**
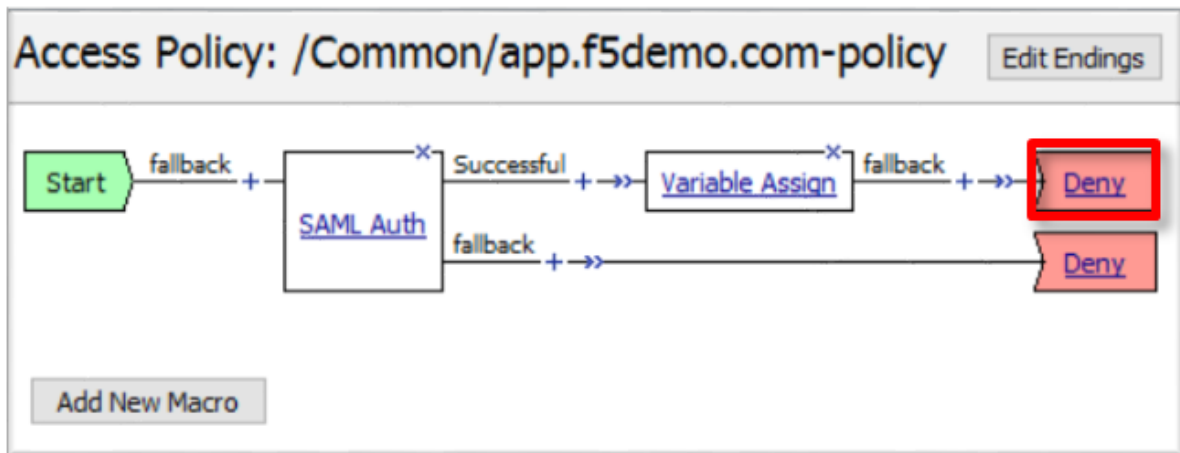
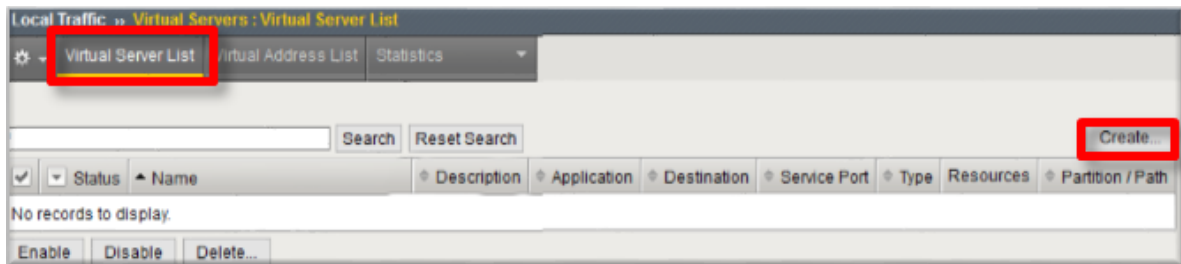21. From the **Select Ending** dialog box, select the **Allow** button and then click **Save**

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

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)

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

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

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

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

Resources	
iRules:	`application?irule`

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

Local Traffic ›› Virtual Servers : Virtual Server List ›› New Virtual Server...

General Properties

Name	app.f5demo.com
Description	
Type	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
SSL Profile (Client)	Selected / Available /Common app.f5demo.com-clientss clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl wom-default-clientssl

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)
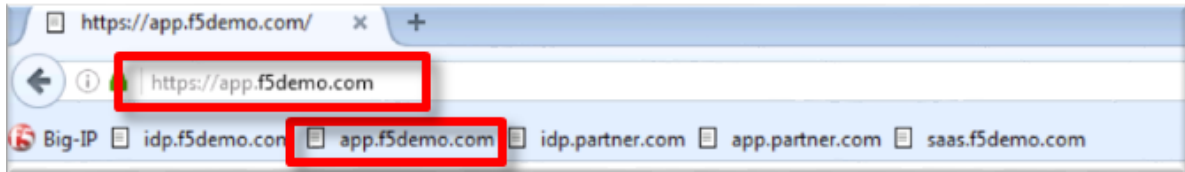
2. Did you successfuly redirect to the IdP?

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
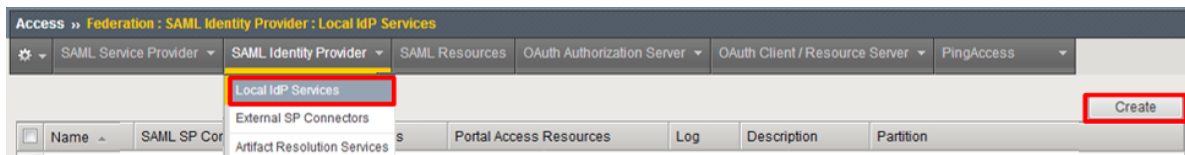
Lab Requirements:

- 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)

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`

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:	`%{session.logon.last.username}` (drop down)

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 Service

- General Settings
- SAML Profiles
- Endpoint Settings
- Assertion Settings
- **SAML Attributes**
- Security Settings

SAML Attributes

Add...

|	Name ▲	Value(s)	Encrypt	Type
☐				

Edit...   Delete...

OK   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
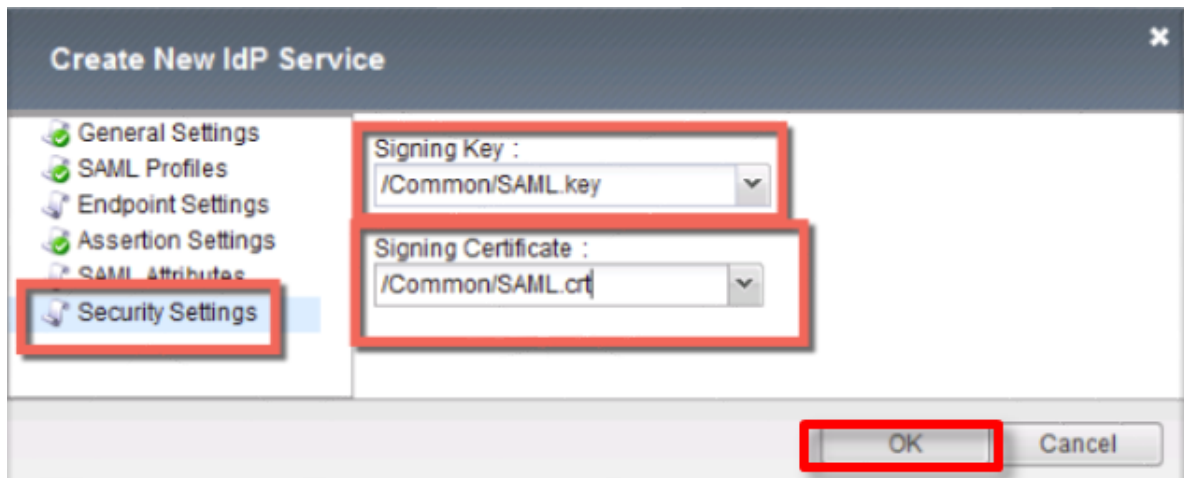
SP Connector

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
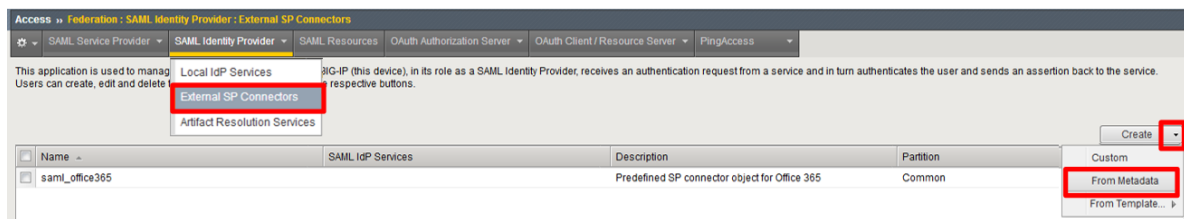
4. In the **Create New SAML Service Provider** dialogue box, click **Browse** and select the *app.partner.com_metadata.xml* file from the Desktop of your jump host

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
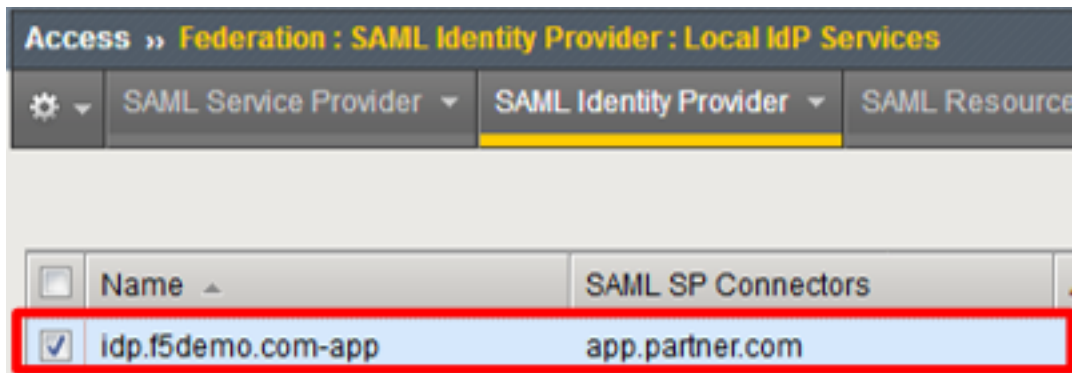

9. In the **Edit SAML SP's that use this IdP** dialog, select the `/Common/app.partner.com` SAML SP Connection Name created previously

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

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

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

Webtop

1. Select **Access ?> Webtops ?> Webtop List**
2. Click the **Create** button (far right)
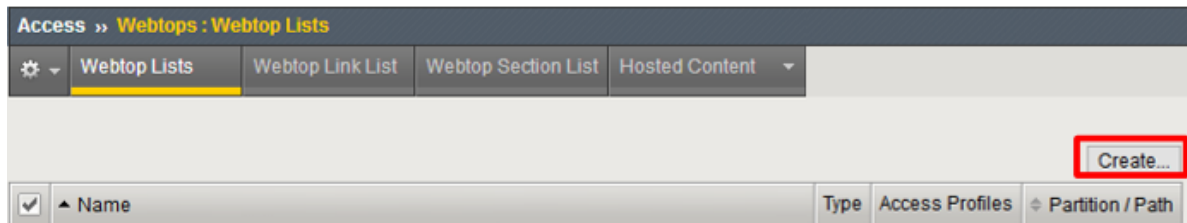
3. In the resulting window, enter the following values:

Name:	`full_webtop`
Type:	`Full` (drop down)

4. Click **Finished** at the bottom of the GUI

SAML IdP Access Policy

1. Select **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)**
2. Click the **Create** button (far right)
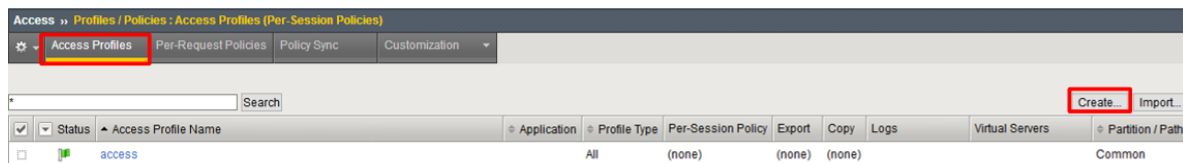
3. In the **New Profile** window, enter the following information:

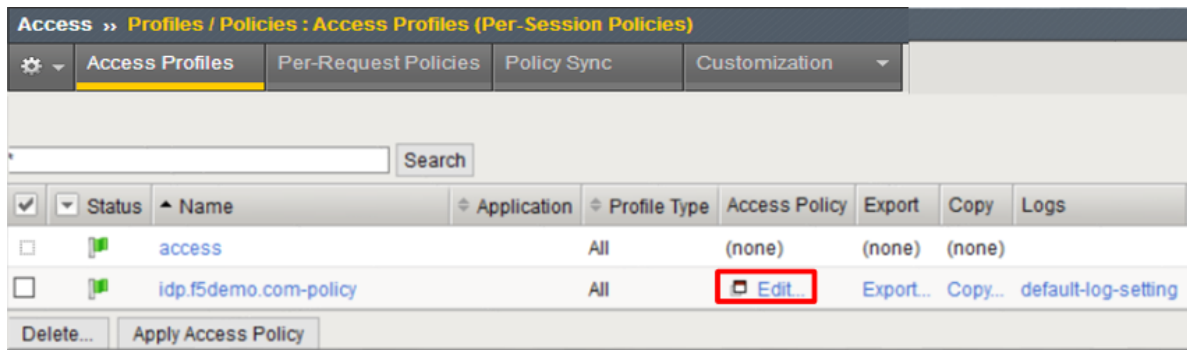| Name:	`idp.f5demo.com?policy`
Profile Type:	`All` (drop down)
Profile Scope:	`Profile` (default)

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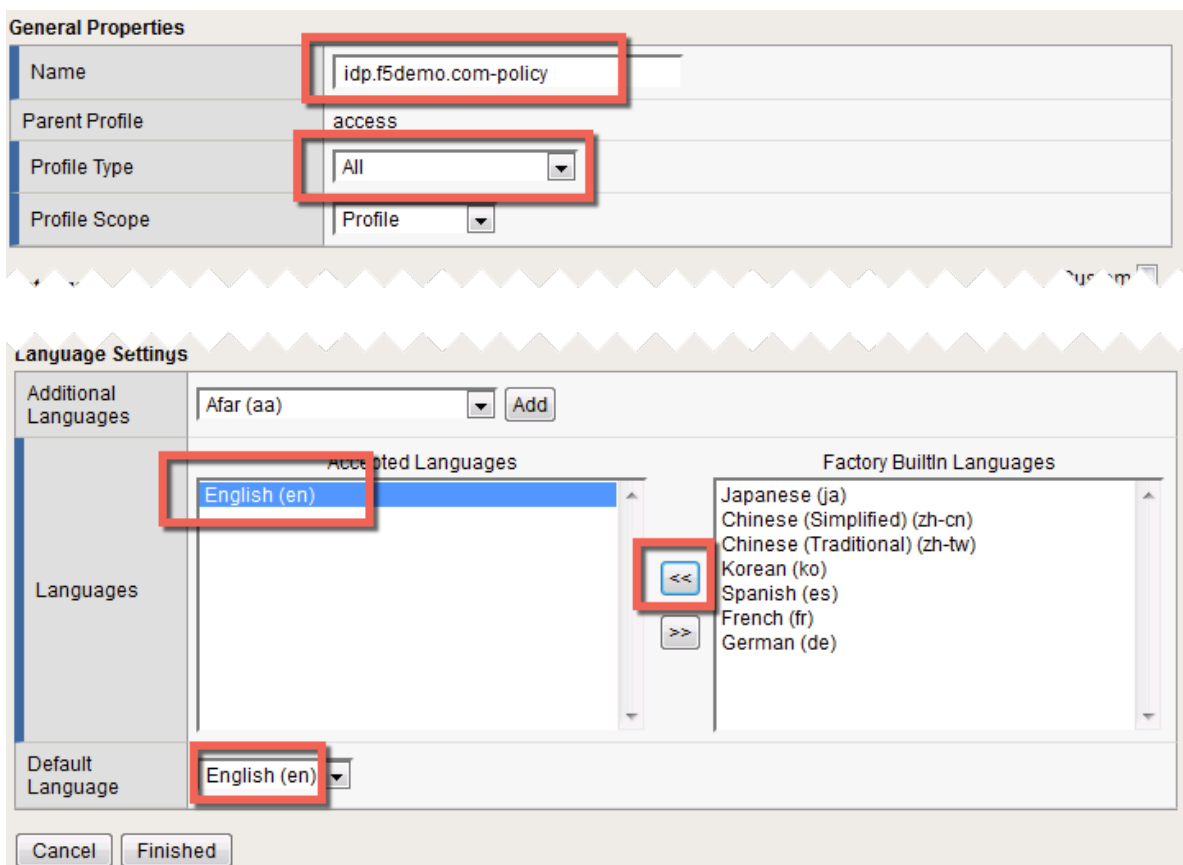
7. From the **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies) screen**, click the **Edit** link on the previously created `idp.f5demo.com?policy` line

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


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
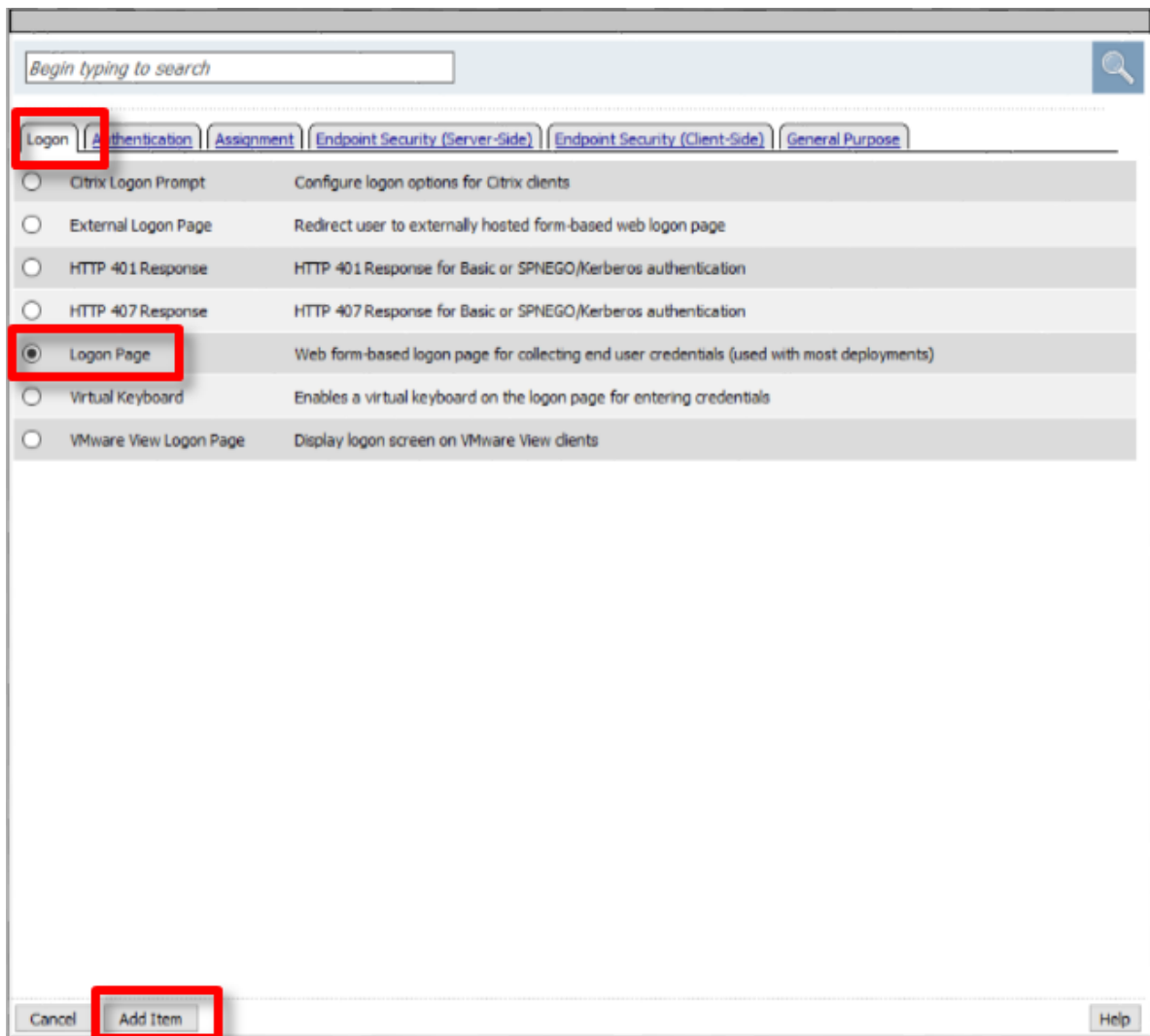
11. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** between **Logon Page** and **Deny**
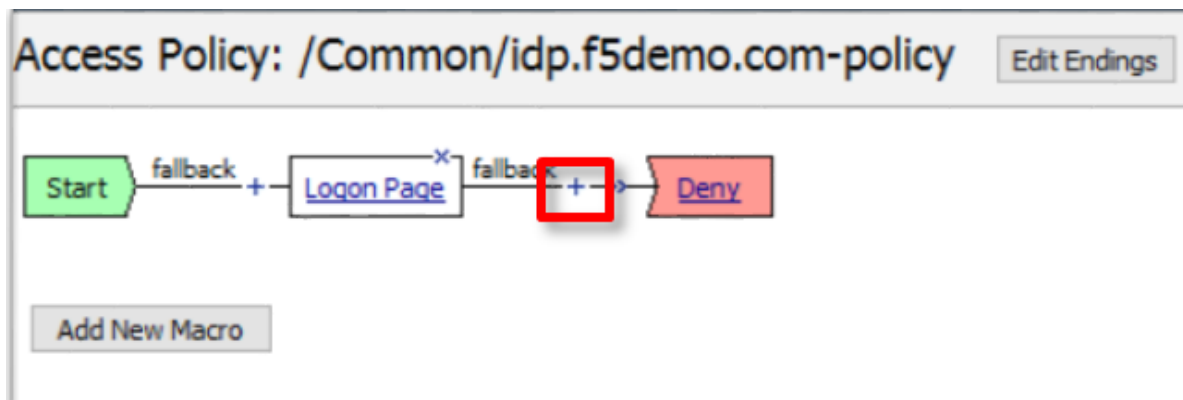
12. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Auth**, and click the **Add Item** button
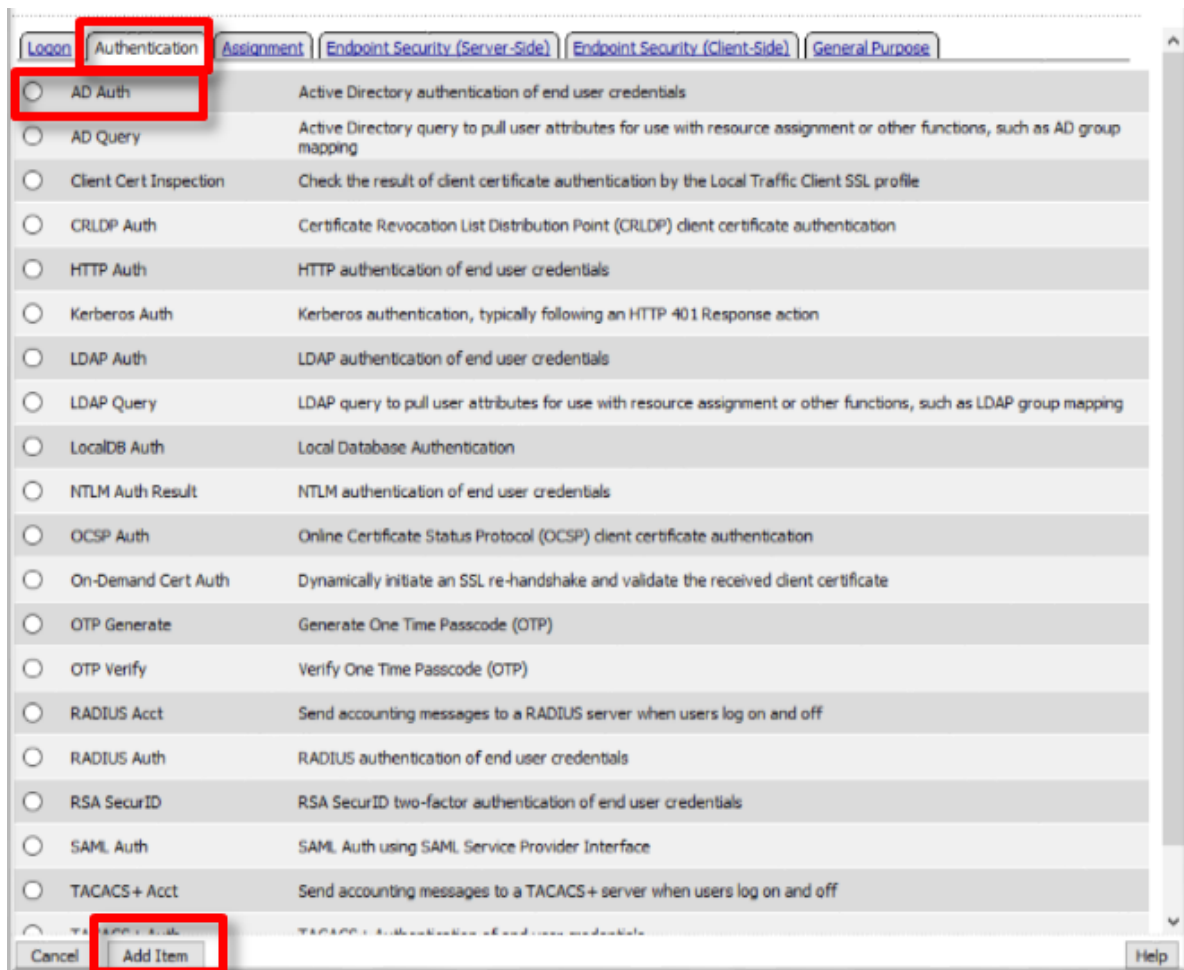
13. In the resulting **AD Auth** pop-up window, select `/Common/f5demo_ad` from the **Server** drop down menu

14. Click **Save** at the bottom of the window
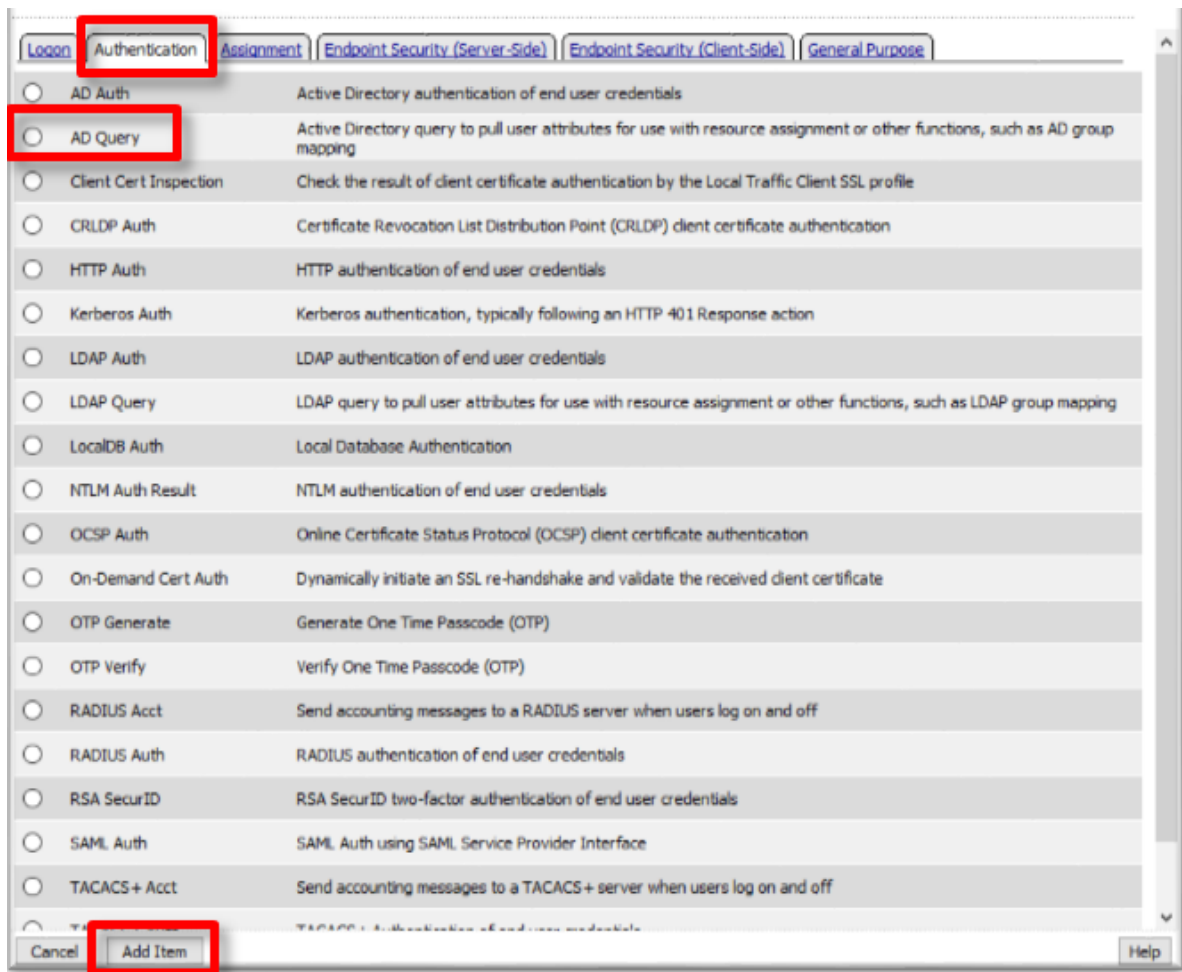
Properties | Branch Rules

Name: AD Auth

Active Directory

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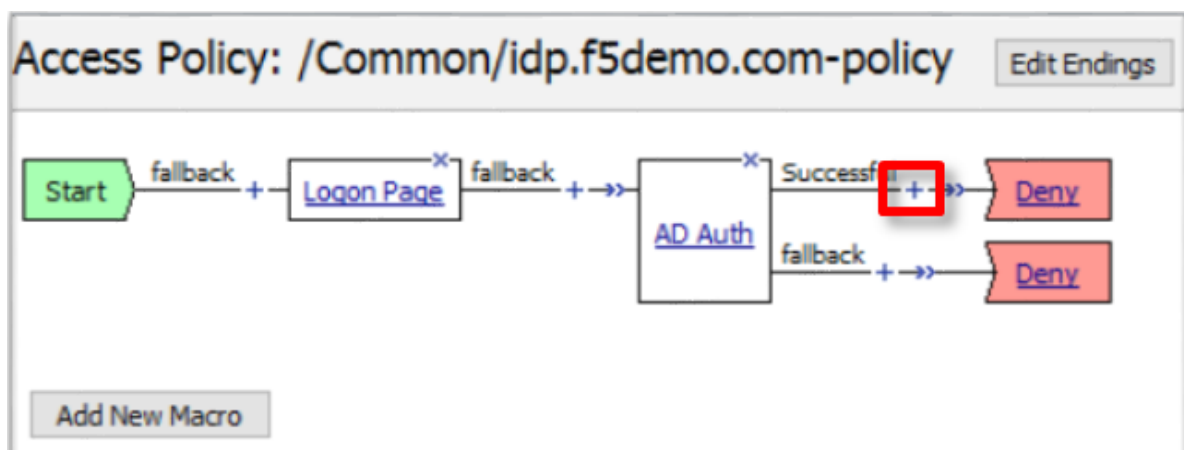
16. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button

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

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**

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

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

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

25. Click the **Finished** button to complete the expression
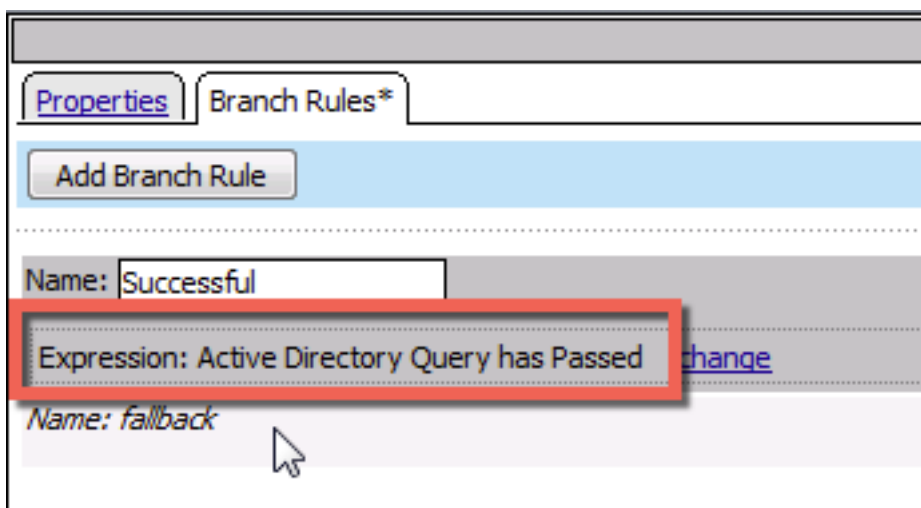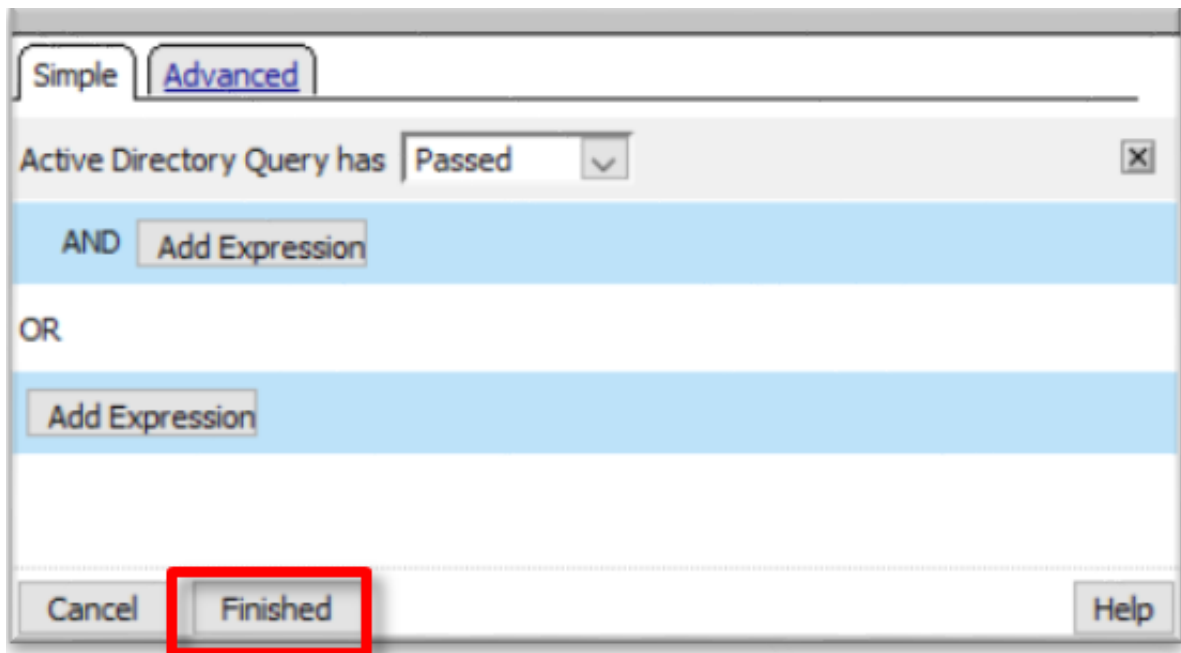
26. Click the **Save** button to complete the **AD Query**

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

Access Policy: /Common/idp.f5demo.com-policy   Edit Endings   (Endings: Allow, Deny [de
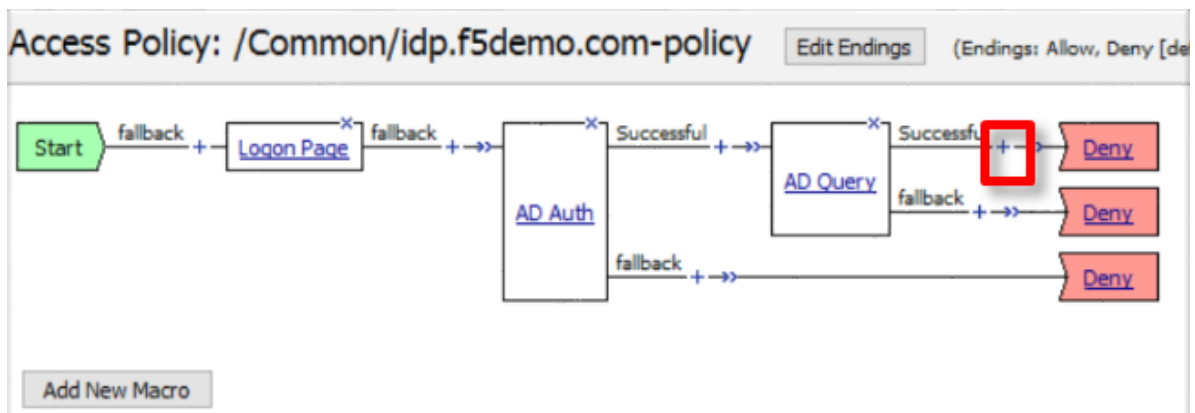
28. In the pop-up dialog box, select the **Assignment** tab and then select the **Radio** next to **Advanced Resource Assign**, and click the **Add Item** button
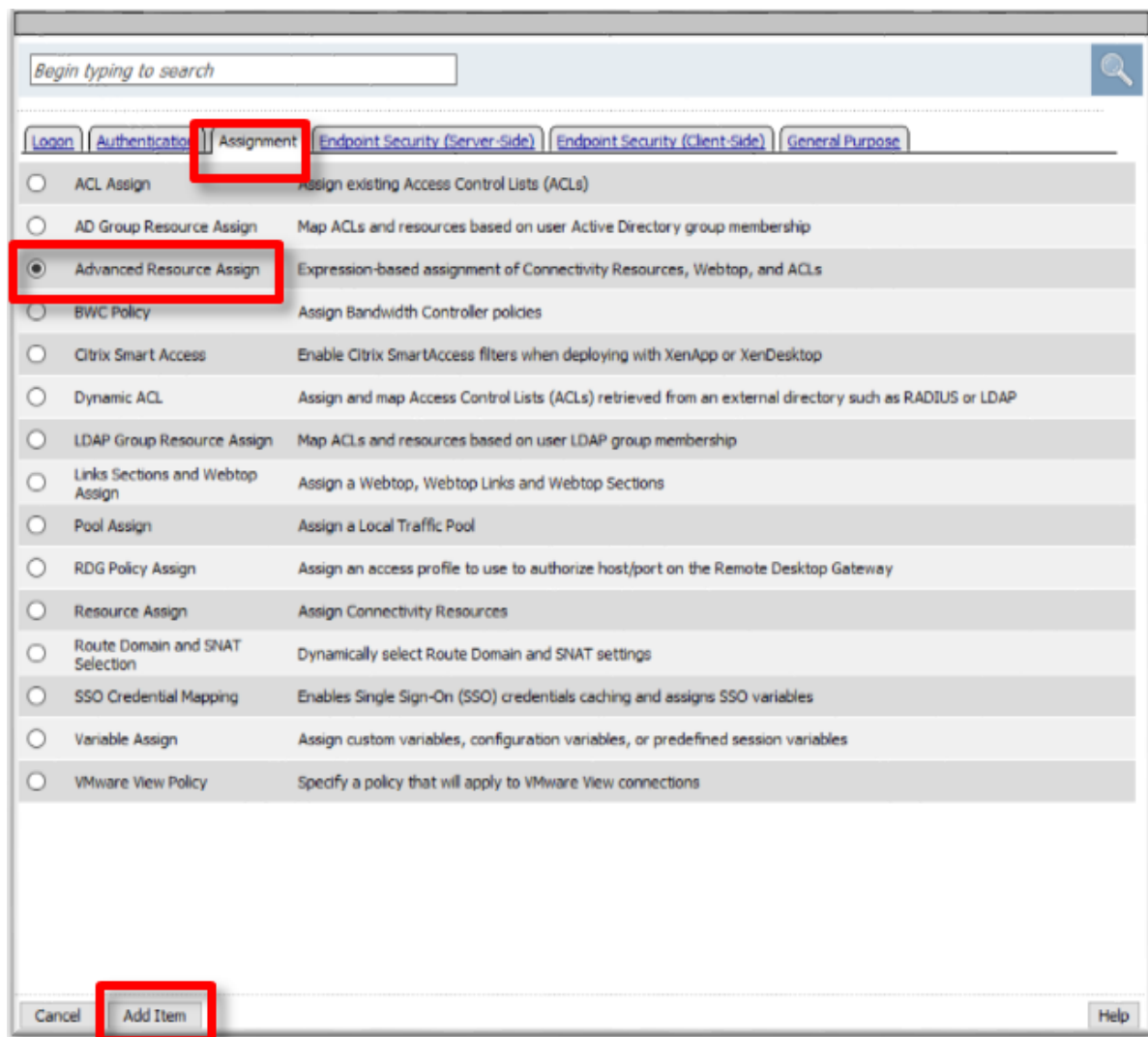
29. In the resulting **Advanced Resource Assign** pop-up window, click the **Add New Entry** button

30. In the new Resource Assignment entry, click the **Add/Delete** link

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

32. Click the **Webtop** tab, and select the **Checkbox** next to `/Common/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 Re-source Assign**
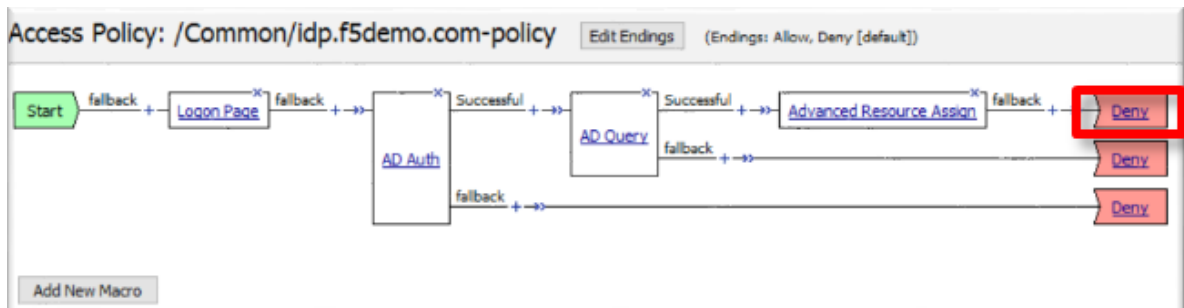
36. In the **Select Ending** dialog box, selet the **Allow** radio button and then click **Save**
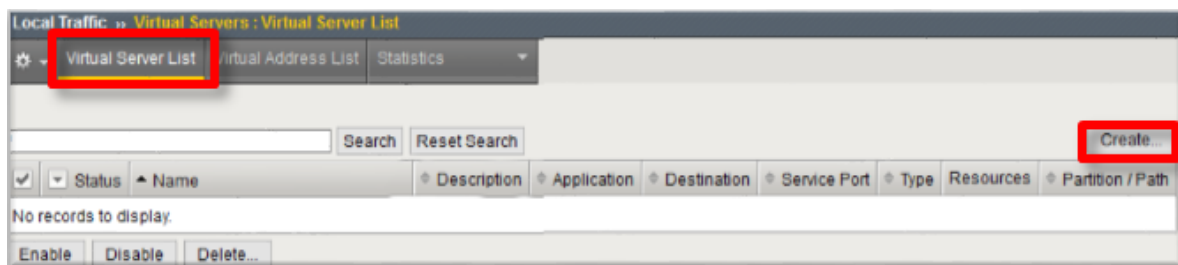

37. In the **Visual Policy Editor**, click **Apply Access Policy** (top left), and close the **Visual Policy Editor**
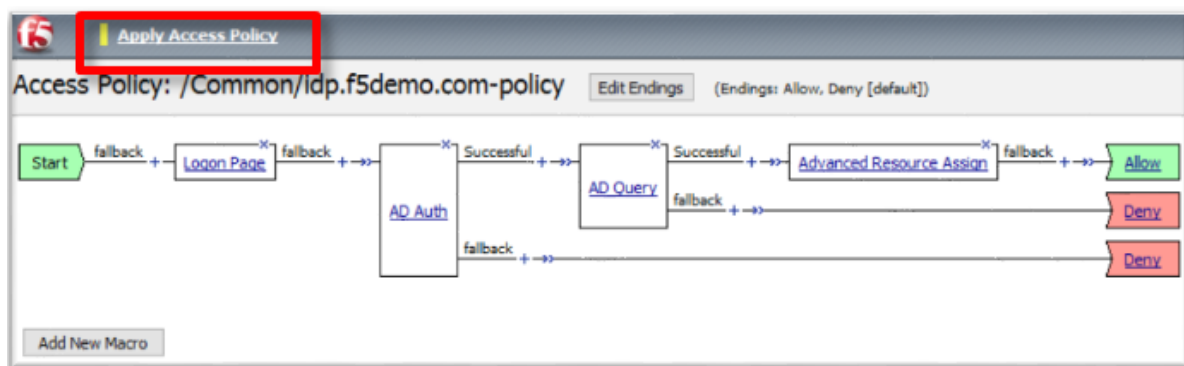
1.3.3 TASK 3 - Create the IdP Virtual Server and Apply the IdP Access Policy

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

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	
Type	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 pool member(s) either don't have service che
Syncookie Status	Off
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
SSL Profile (Client)	Selected / Available

SSL Profile (Client)

Selected
/Common
idp.f5demo.com-clientssl

<< >>

Available
/Common
app.f5demo.com-clientssl
clientssl
clientssl-insecure-compatible
clientssl-secure

Selected   Available

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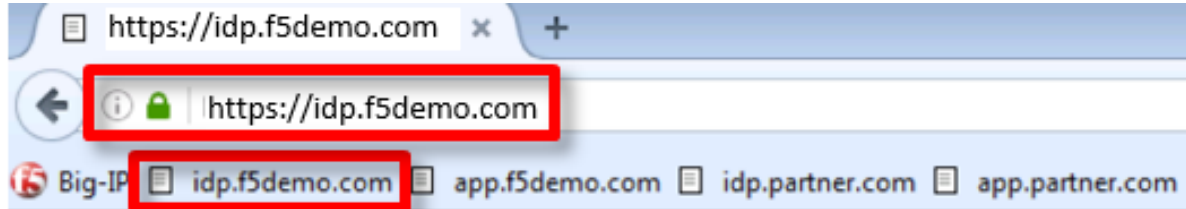
2. Log in to the IdP. Were you successfully authenticated? Did you see the webtop with the SP application?

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

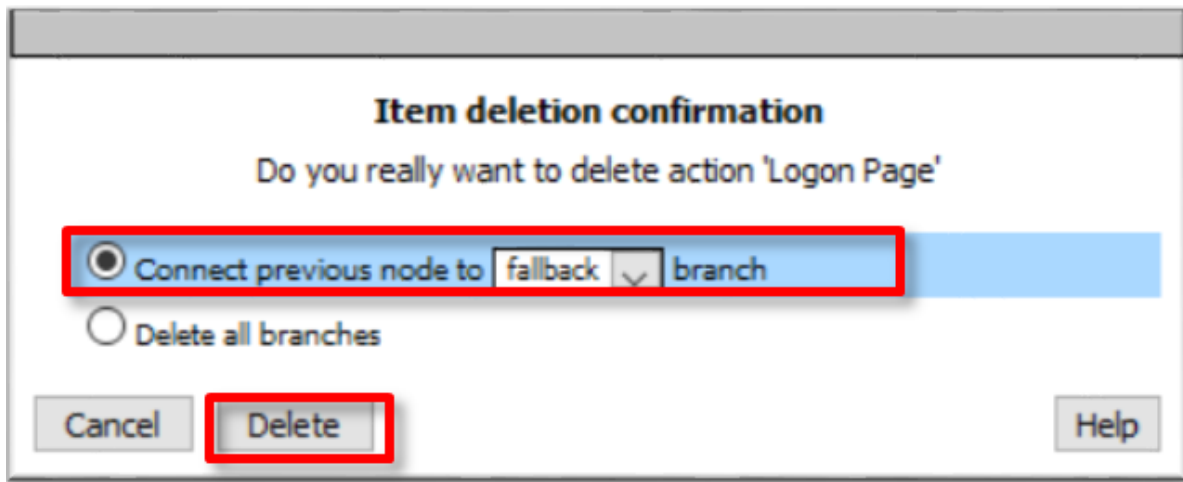## 1.4.1 TASK 1 – Modify the SAML Identity Provider (IdP) Access Policy

1. 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*
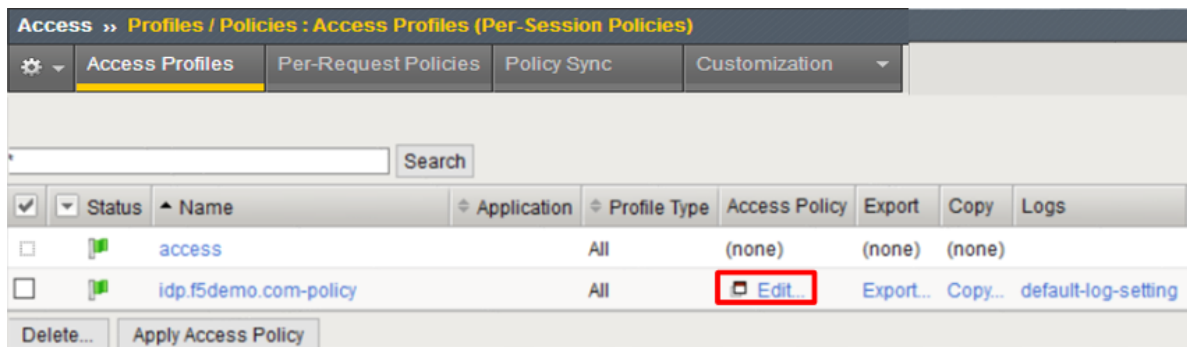

2. Delete the **Logon Page** object by clicking on the **X** as shown
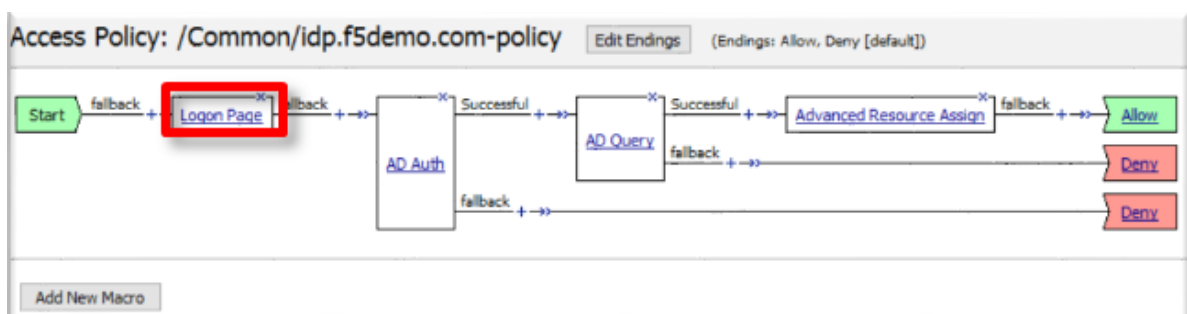
3. In the resulting **Item Deletion Confirmation** dialog, ensure that the previous node is connect to the **fallback** branch, and click the **Delete** button

Item deletion confirmation

Do you really want to delete action 'Logon Page'

- ⦿ Connect previous node to [fallback ⌄] branch
- ○ 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])
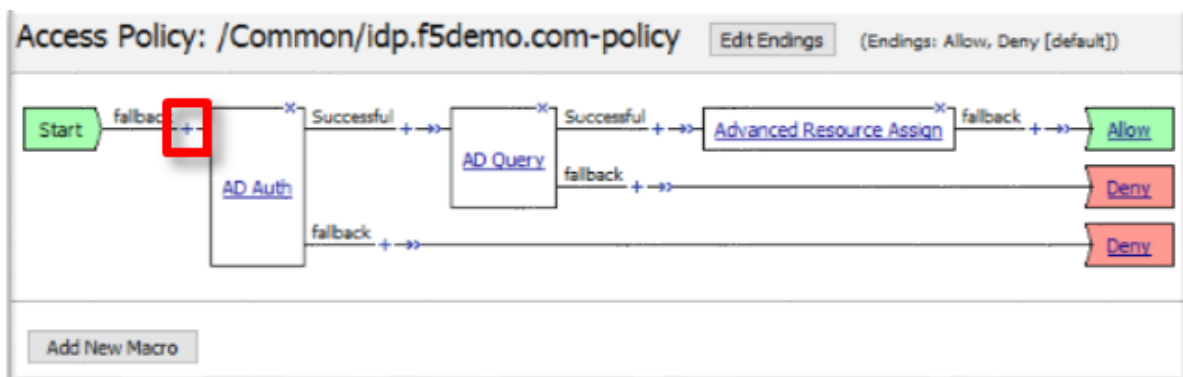
5. In the pop-up dialog box, select the **Logon** tab and then select the **Radio** next to **HTTP 401 Response**, and click the **Add Item** button
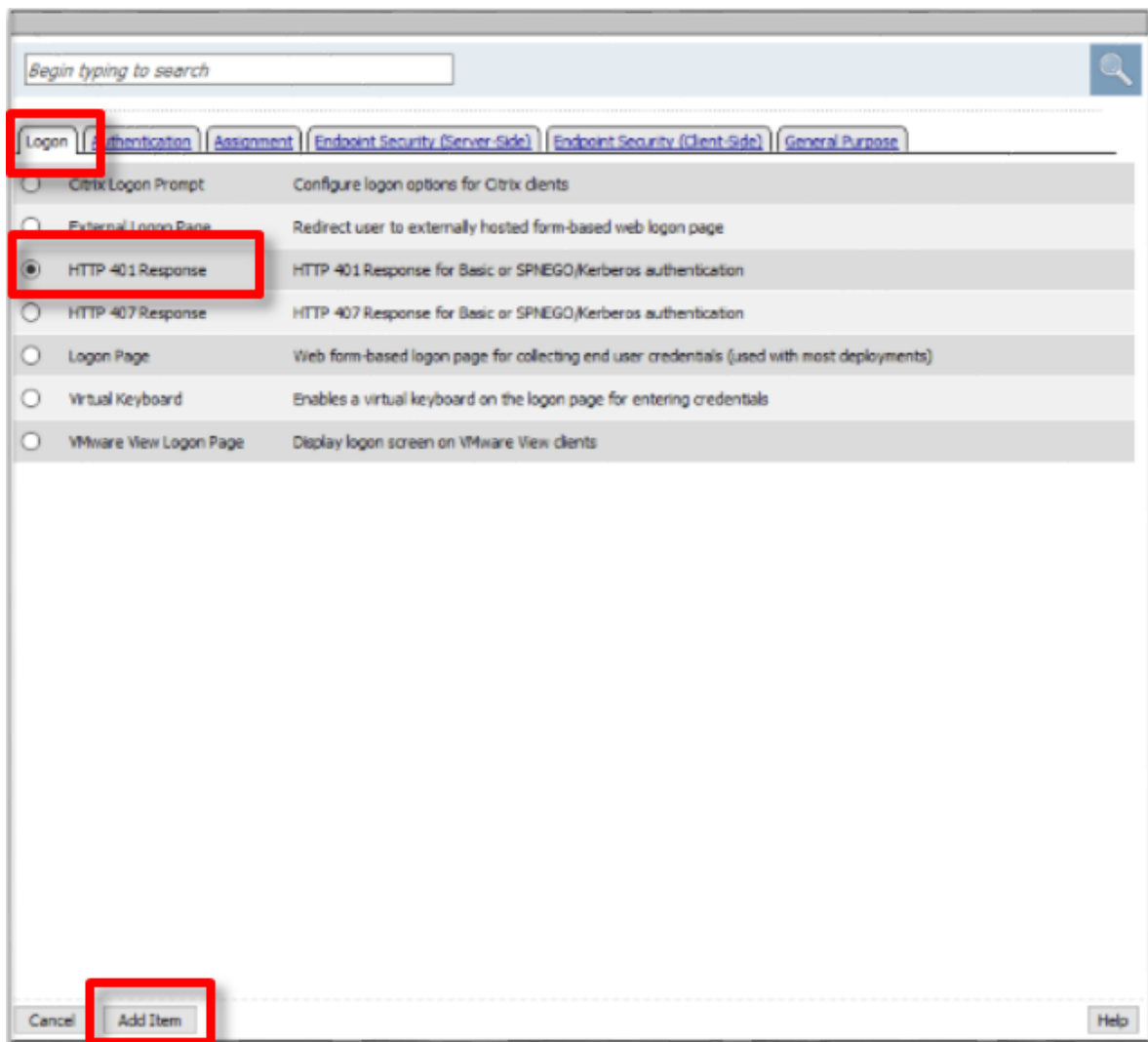
6. In the **HTTP 401 Response** dialog box, enter the following information:

| Basic Auth Realm: | f5demo.com |
| HTTP Auth Level: | basic+negotiate (drop down) |

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

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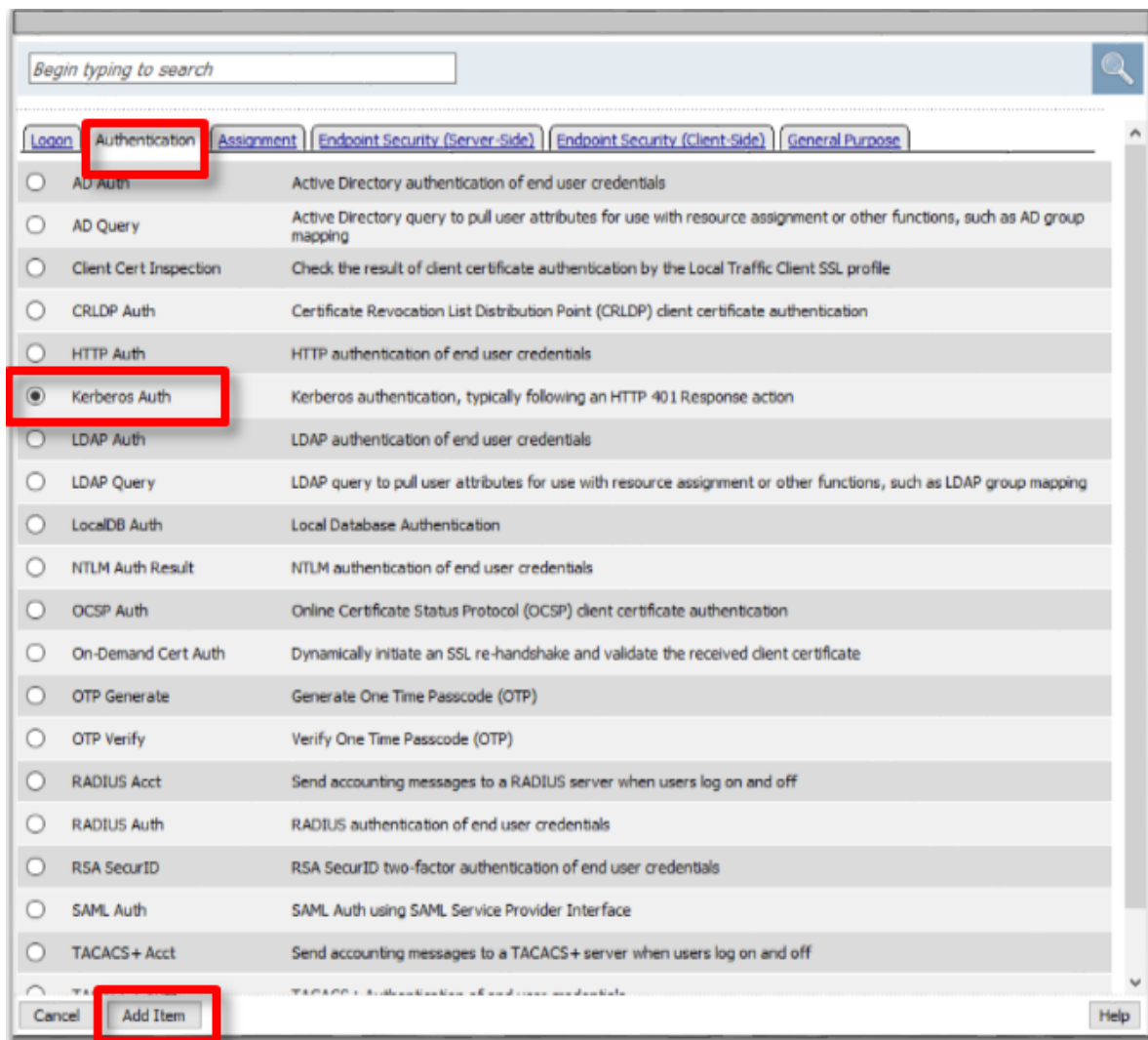
10. In the **Kerberos Auth** dialog box, enter the following information:

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

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**
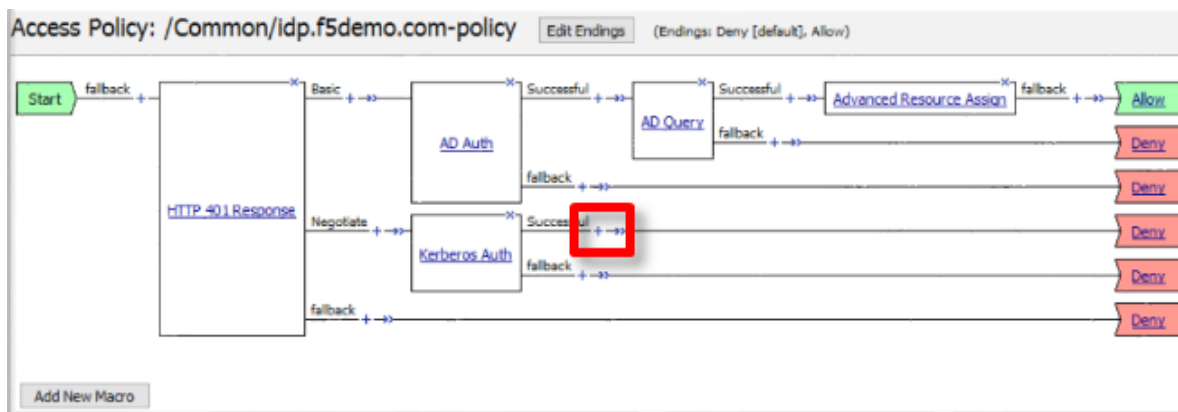
13. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button
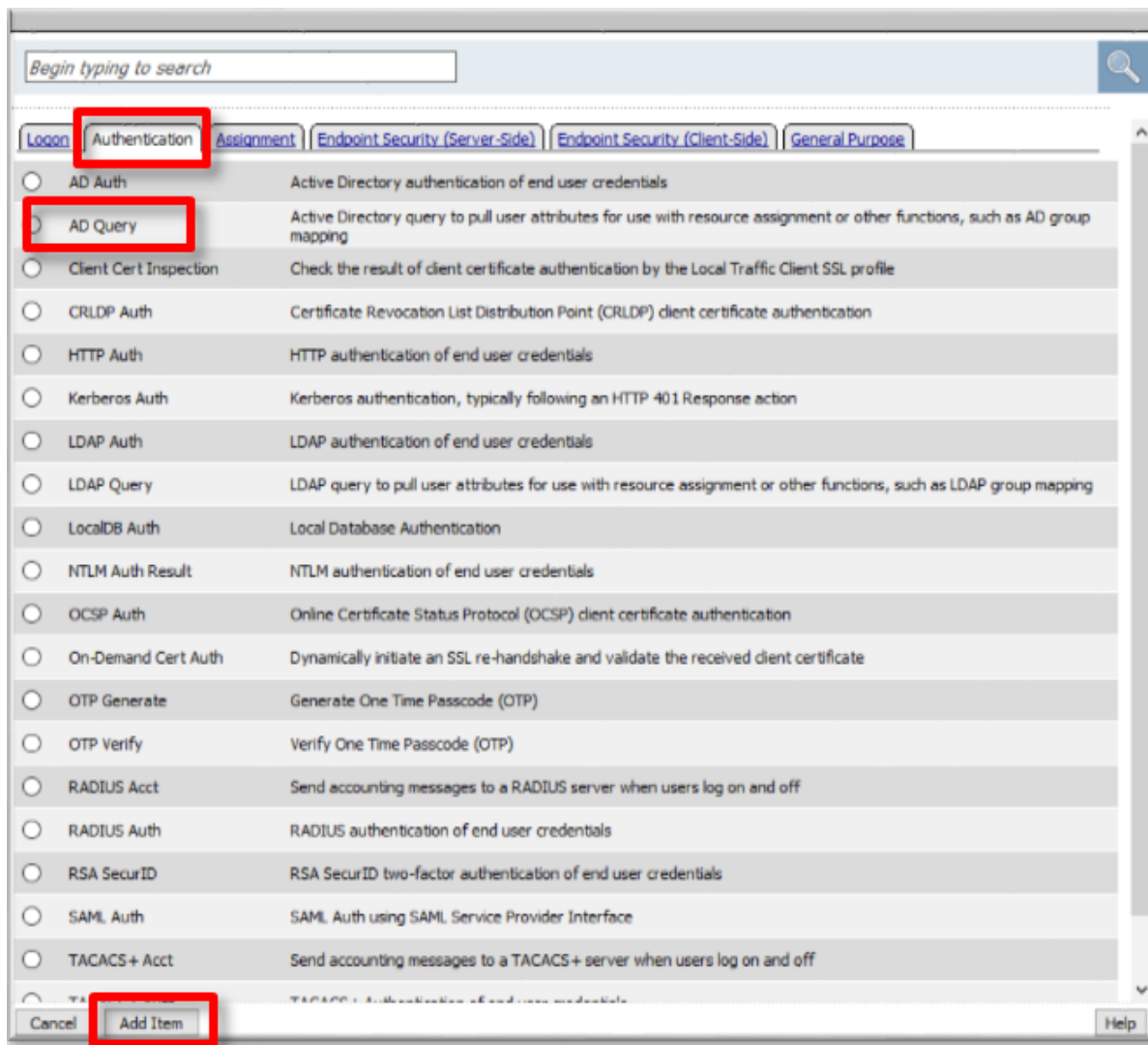
14. In the resulting **AD Query(1)** pop-up window, select `/Commmon/f5demo_ad` from the **Server** drop down menu

15. In the **SearchFilter** field, enter the following value: `userPrincipalName=%{session.logon.last.username}`

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**

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

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

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
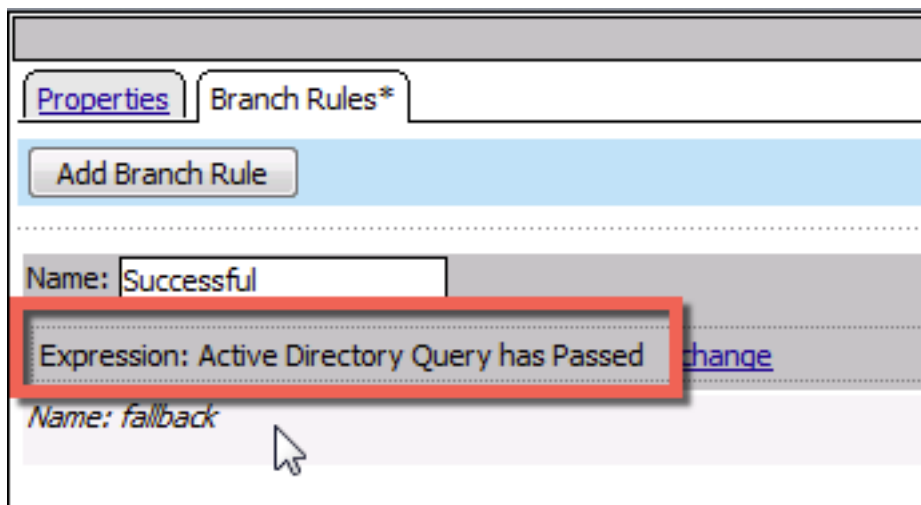

23. Click the **Finished** button to complete the expression
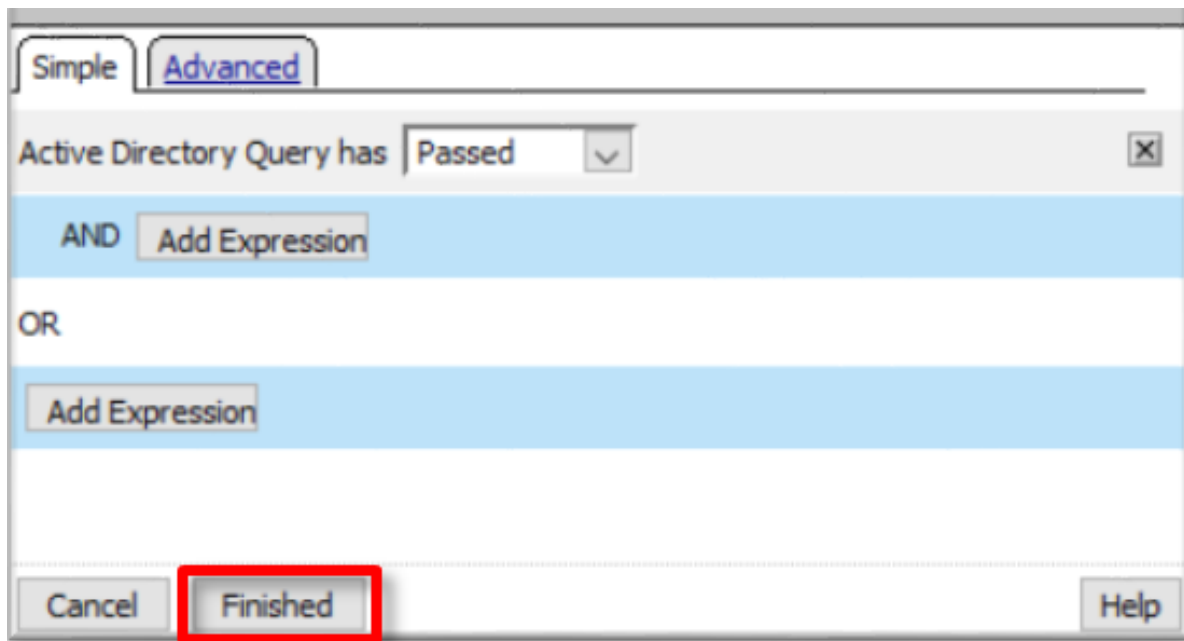
24. Click the **Save** button to complete the **AD Query**

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
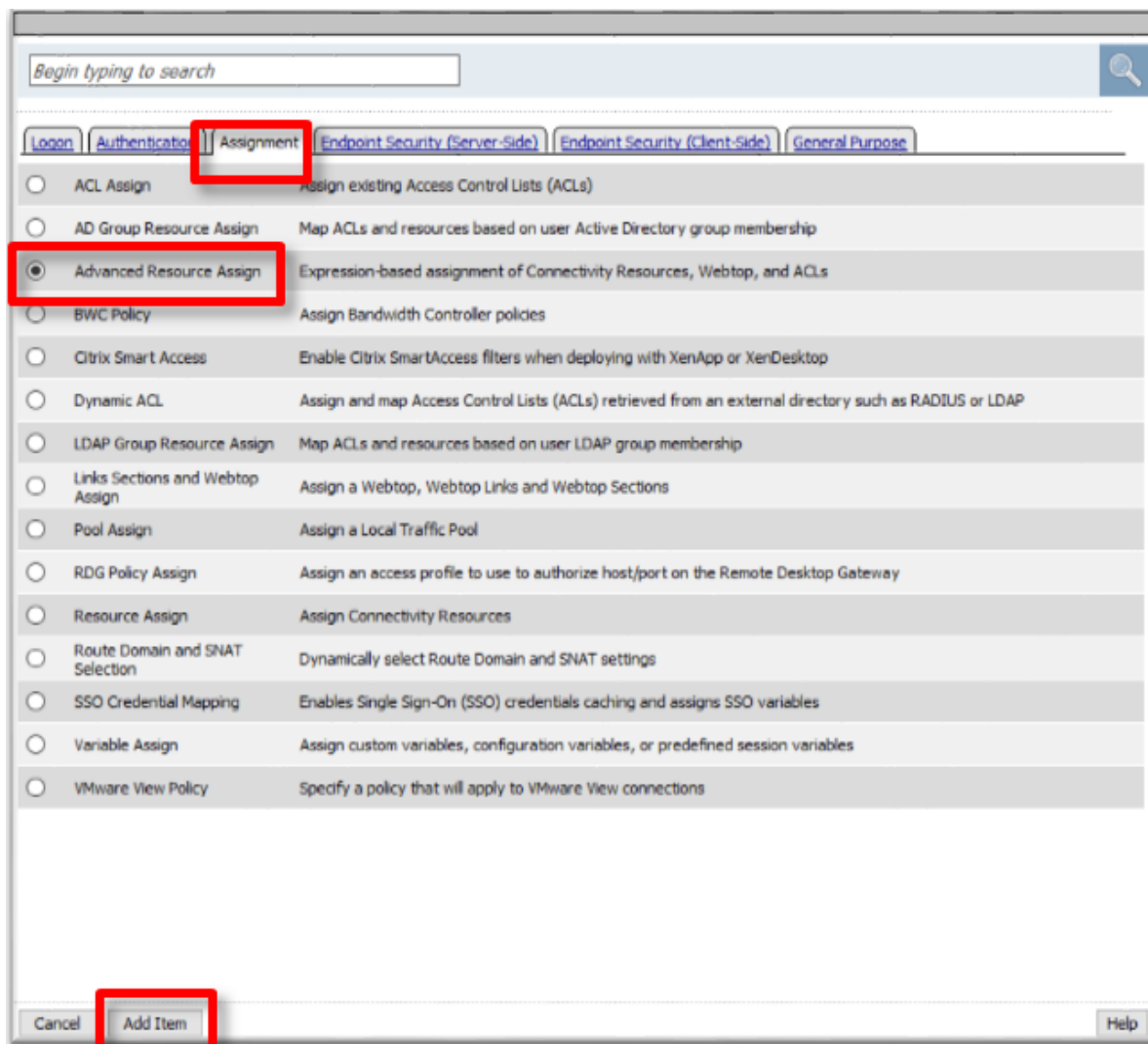
27. In the resulting **Advanced Resource Assign(1)** pop-up window, click the **Add New Entry** button

28. In the new Resource Assignment entry, click the **Add/Delete** link

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

30. Click the **Webtop** tab, and select the **Checkbox** next to `/Common/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 Re-source Assign**
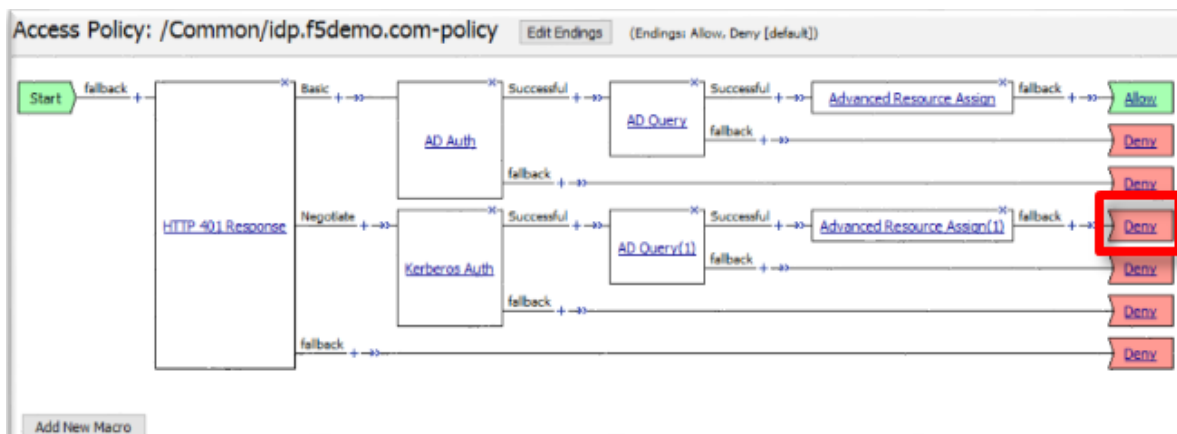
34. In the **Select Ending** dialog box, selet the **Allow** radio button and then click **Save**


35. In the **Visual Policy Editor**, click **Apply Access Policy** (top left), and close the **Visual Policy Editor**
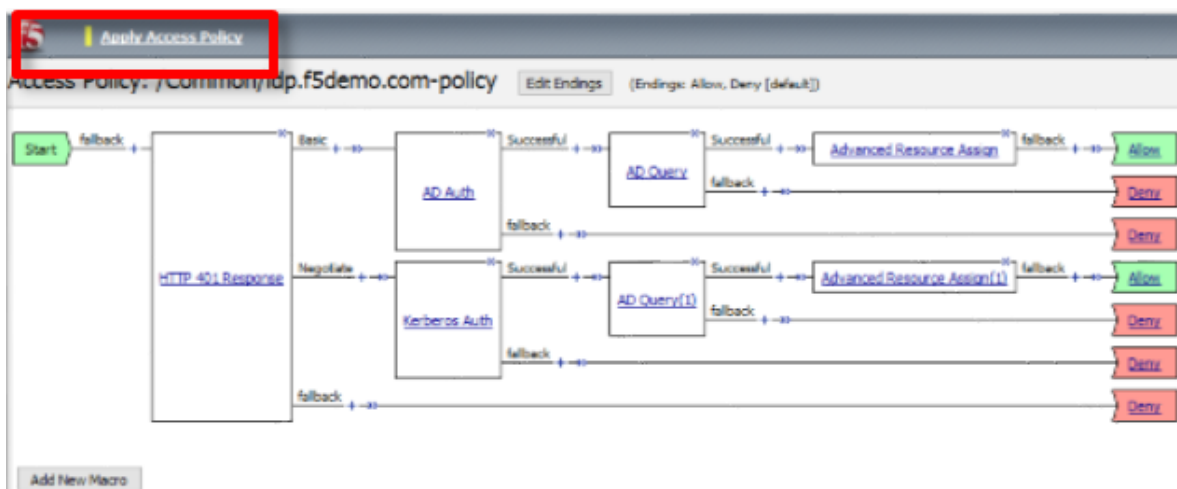
1.4.2 TASK 2 - Test the Kerberos to SAML Configuration

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)
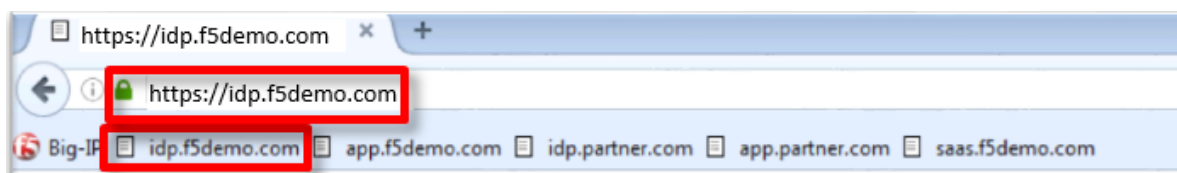
2. Were you prompted for credentials? Were you successfully authenticated? Did you see the webtop with the SP application?

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
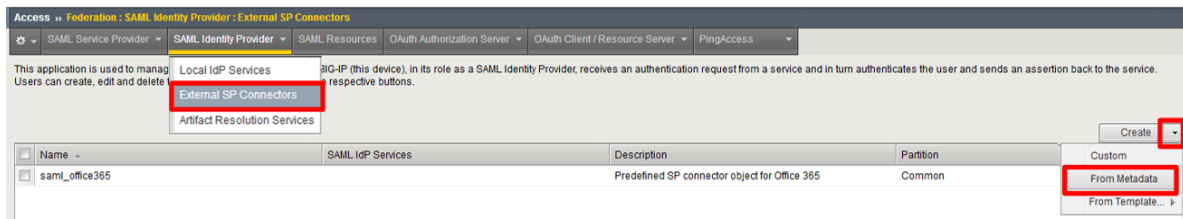
4. In the **Create New SAML Service Provider** dialogue box, click **Browse** and select the `SAMLSP-00D36000000jjkp.xml` file from the Desktop of your jump host

5. In the **Service Provider Name** field, enter: `salesforce`

6. Click **OK** on the dialog box
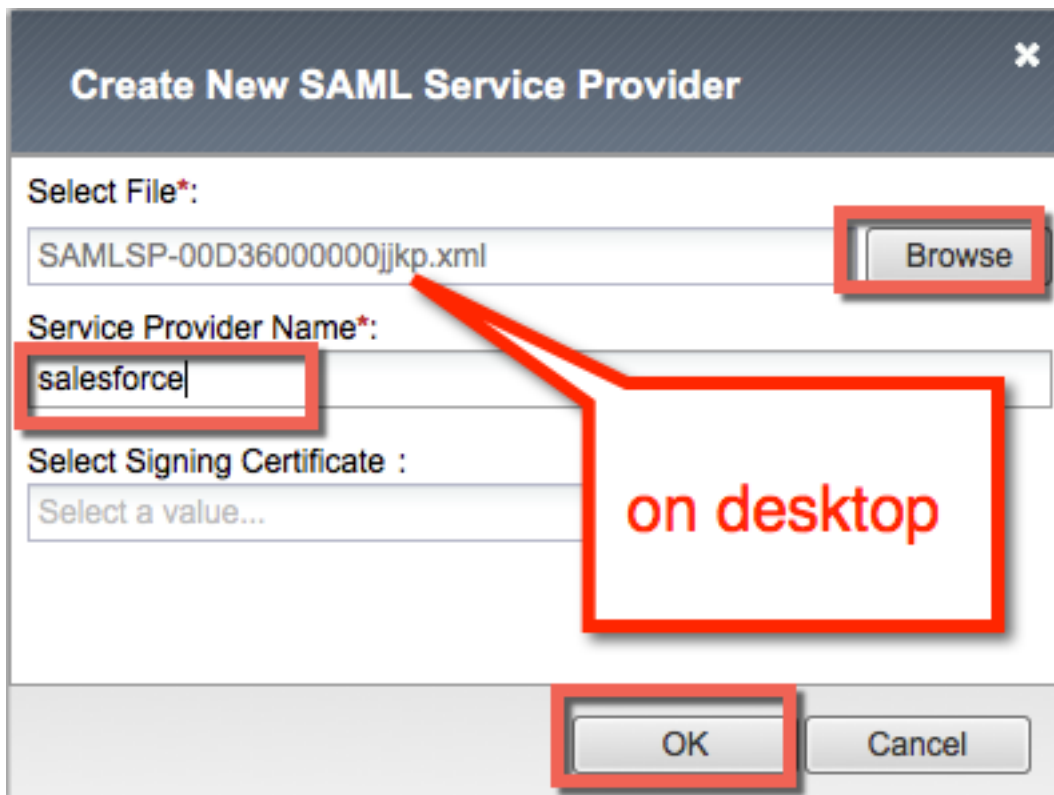
1.5.2 TASK 2 - Deploy the SaaS Federation iApp

1. Navigate to **iApps ?> Application Services -> Applications** and click on the **Plus (+) Sign** as shown
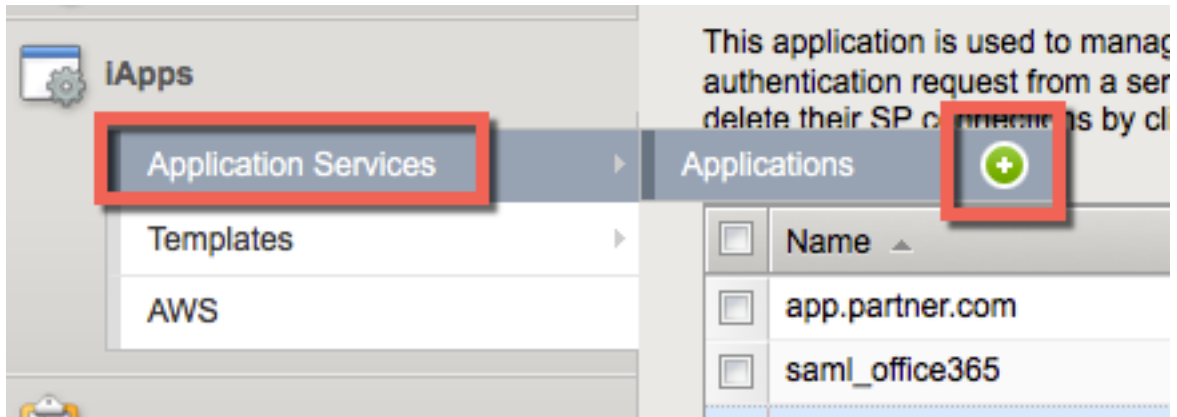
2. In the resulting **New Application Service** window, enter *saas* as the *Name*

3. Select `f5.saas_idp.v1.0.rc1` from the **Template** drop down menu

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`

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

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 authentication?	`idp.f5demo.com.crt`
What is the associated private key?	`idp.f5demo.com.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 key

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

5. Scroll to the bottom of the configuration template and click **Finished**

6. Once deployed, you can review the built out SaaS Federation iApp at **iApps ?> Application Services ?> Applications ?> saas**

iApps ›› Application Services : Applications ›› sass					
⚙ ▾ Properties	Reconfigure	Components	Security	Analytics	⤢

Name		Availability	Type
⊟ 🖥 BIG-IP			
⊟ ☐ sass			Application Service
⊟ 🖥☐ sass_vs		🔵 Unknown	Virtual Server
🖥 10.1.10.120			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**
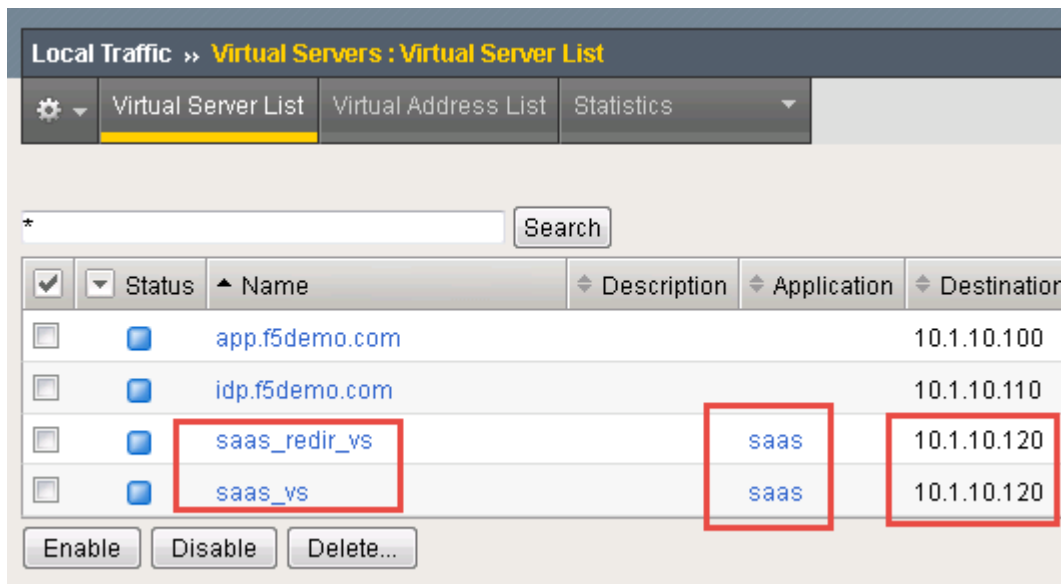
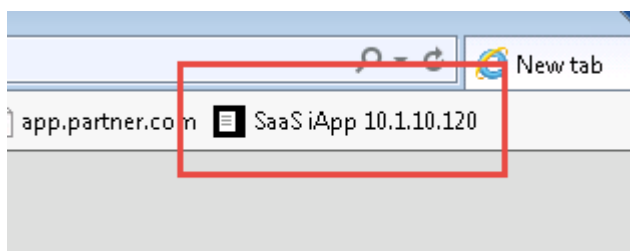8. Review the new Access Policy built by the iApp at **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)** and select the **Edit** link next to the *saas* Access Policy
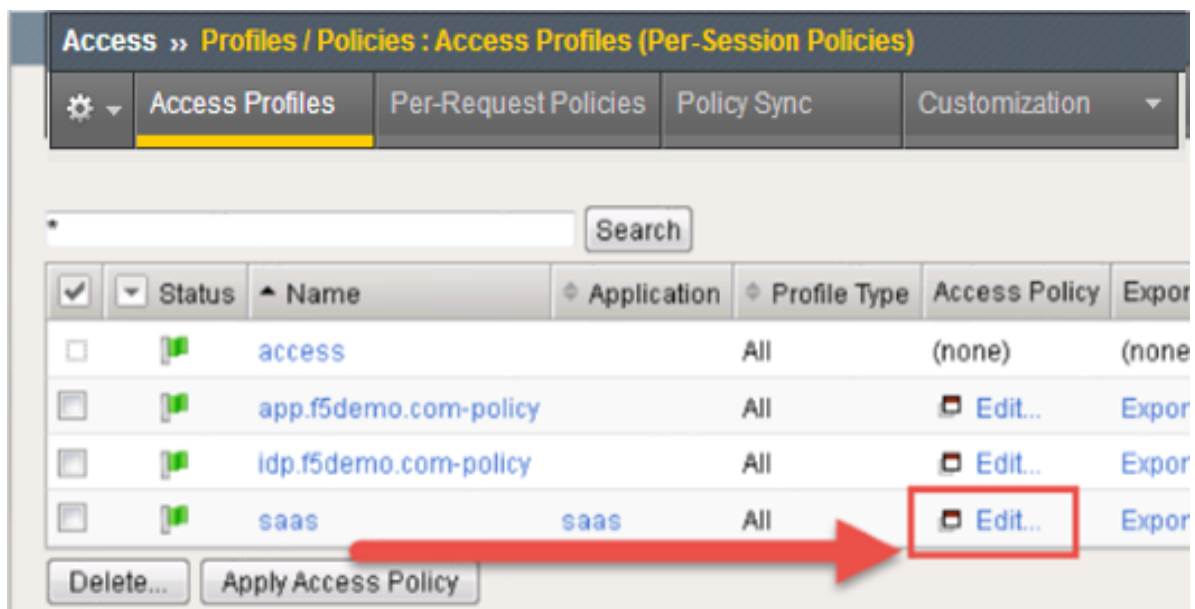
9. Test the SaaS iApp by clicking on the bookmark in your browser.

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

through the warning to see the resulting page.

### 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.

1. 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`
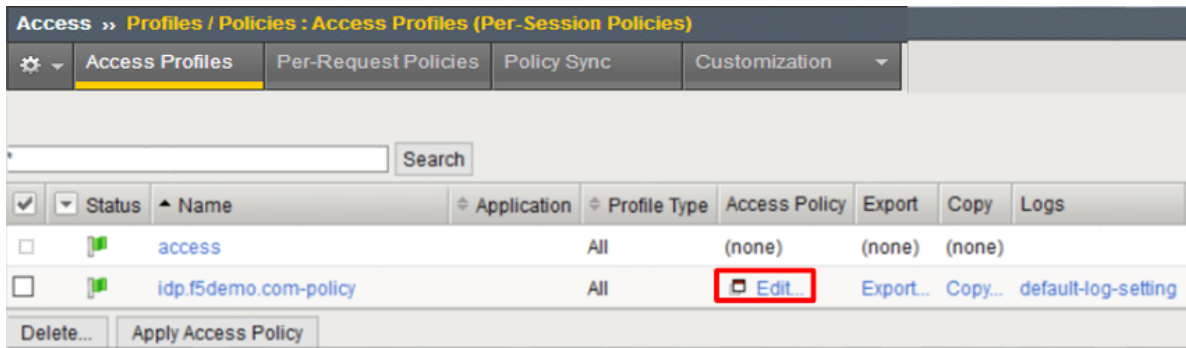
2. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Advanced Resource Assign** object.
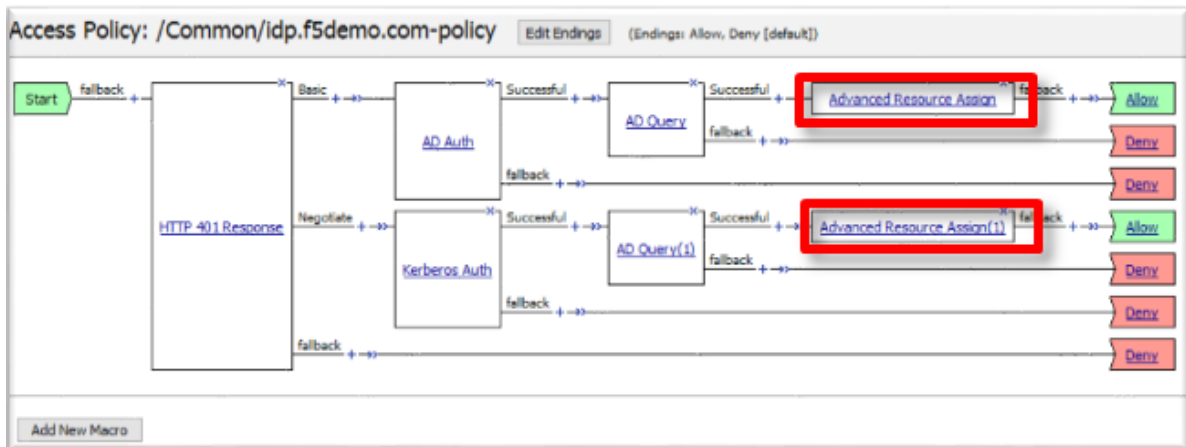
3. Click the **Add/Delete** link on the Resource Assignment item

4. Click the **SAML** tab, and select the checkbox next to `/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**
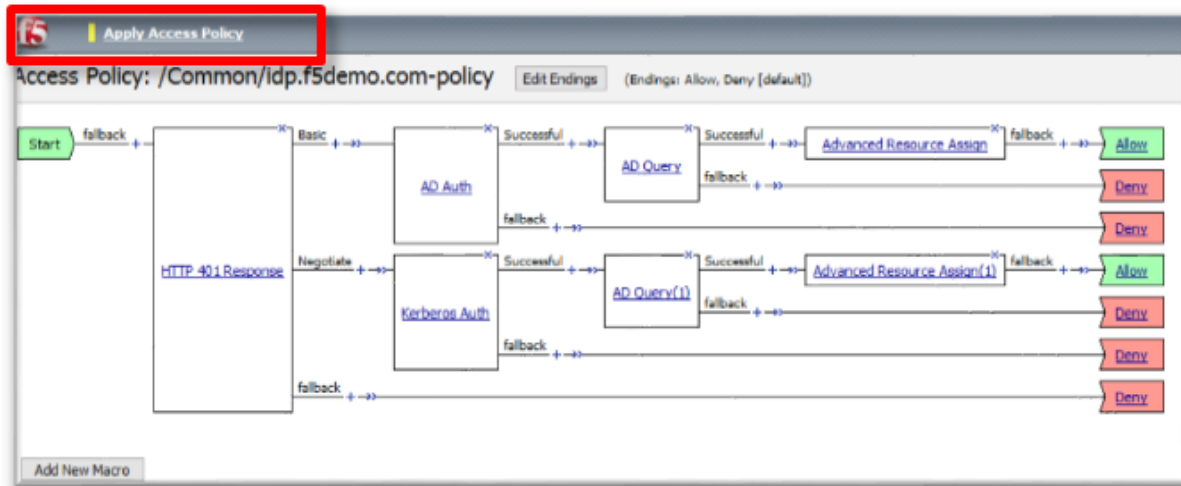
1.5.4 TASK 4 - Test the SaaS Federation Application

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)
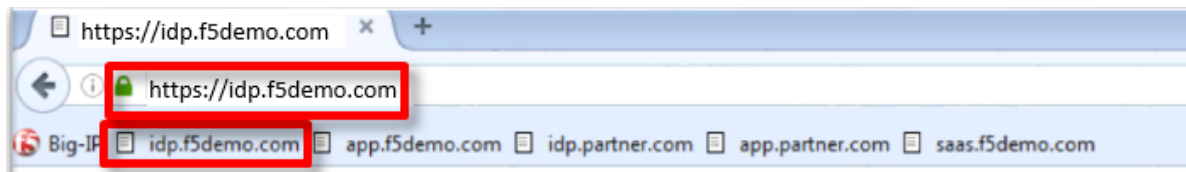
2. Were you prompted for credentials? Were you successfully authenticated? Did you see the webtop with the new SaaS SP application?

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-an

- **Access Policy Manager (APM) Deployment Guides:**

  - **F5 Deployment Guide for Microsoft Exchange 2010/2013:** https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2010-and-2013-big-ip-v11

  - **F5 Deployment Guide for Microsoft Exchange 2016:** https://f5.com/solutions/ deployment-guides/microsoft-exchange-server-2016-big-ip-v11-v12-ltm-apm-afm

- **F5 Deployment Guide for Microsoft SharePoint 2010/2013:** https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2010-and-2013-new-supported-iapp-big-ip-v114-ltm-apm-asm-aam

- **F5 Deployment Guide for Microsoft SharePoint 2016:** https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2016-big-ip-v114-v12-ltm-apm-asm-afm-aam

- **F5 Deployment Guide for Citrix XenApp/XenDesktop:** https://f5.com/solutions/deployment-guides/citrix-xenapp-or-xendesktop-release-candidate-big

- **F5 Deployment Guide for VMWare Horizon View:** https://f5.com/solutions/deployment-guides/vmware-horizon-view-52-53-60-62-70-release-candidate-iapp-big-ip-v11-v12-ltm-apm-afm?tag=VMware

- **F5 Deployment Guide for Microsoft Remote Desktop Gateway Services:** https://f5.com/solutions/deployment-guides/microsoft-remote-desktop-gateway-services-big-ip-v114-ltm-afm-apm

- **F5 Deployment Guide for Active Directory Federated Services:** https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm

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

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

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
Type	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**

_2_

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
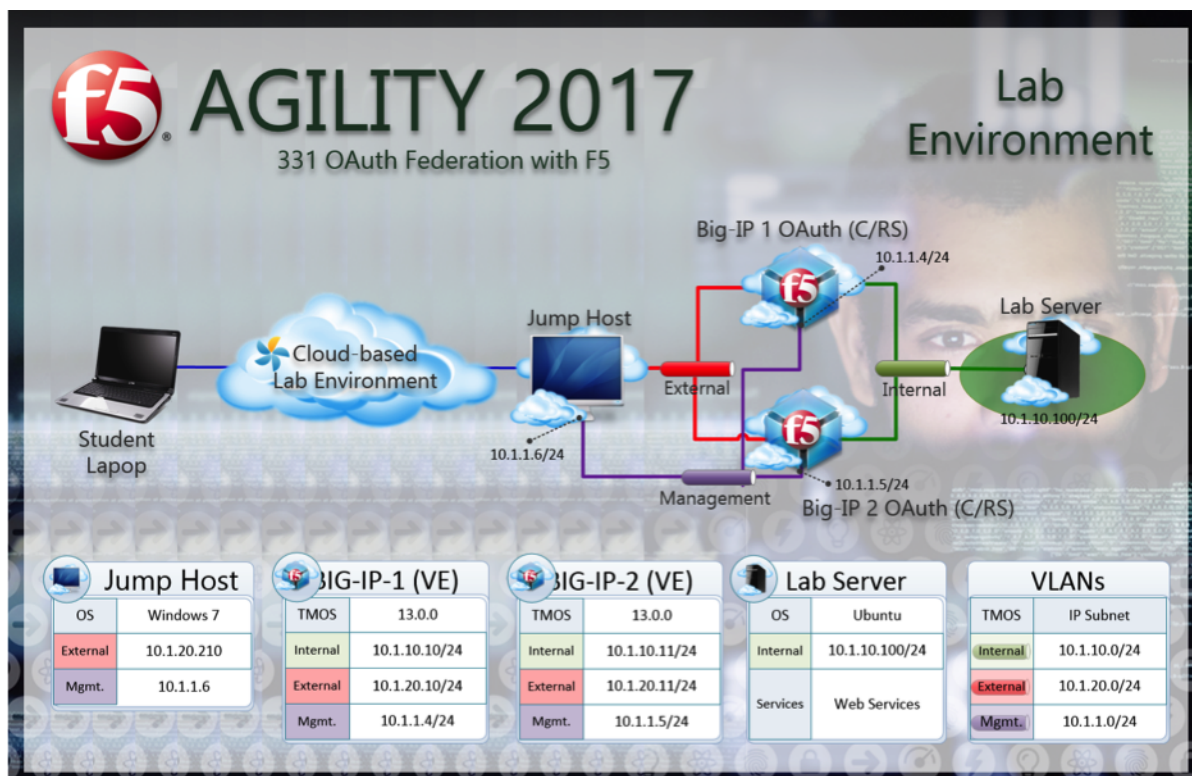
2.2 Lab 1: Social Login Lab

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**
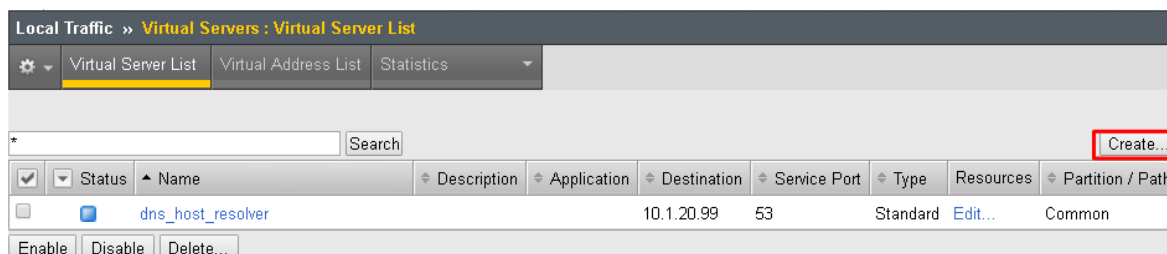
2. Enter the following values *(leave others default)*

- **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	
Type	Standard
Source Address	
Destination Address/Mask	10.1.20.111
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	**Selected** /Common f5agility-wilcard-self-clientssl **Available** clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl wom-default-clientssl
SSL Profile (Server)	**Selected** **Available** /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

3. Select webapp-pool from the Default Pool drop down and then click **Finished**
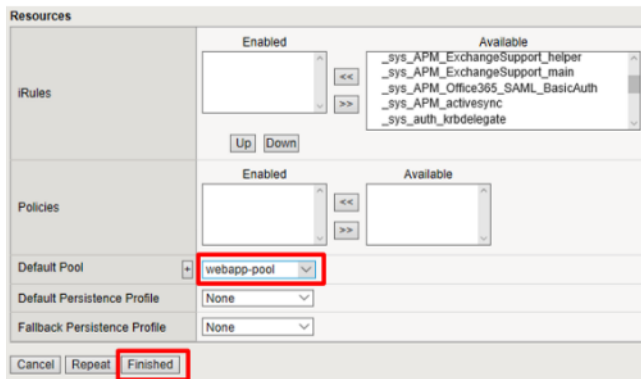
4. Test access to `https://social.f5agility.com` from the jump host's browser.

   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.
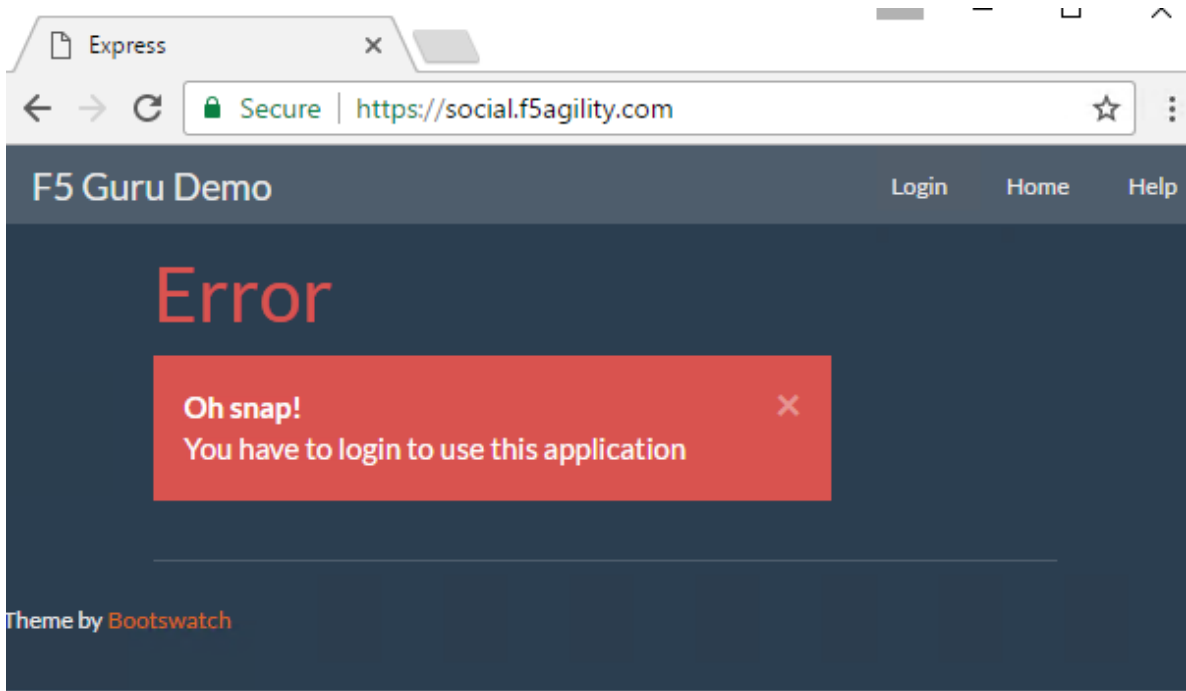
2.2.3 Task 2: Setup APM Profile

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

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

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

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

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

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

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

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

9. Click **Finished**

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**

11. Click **Save**

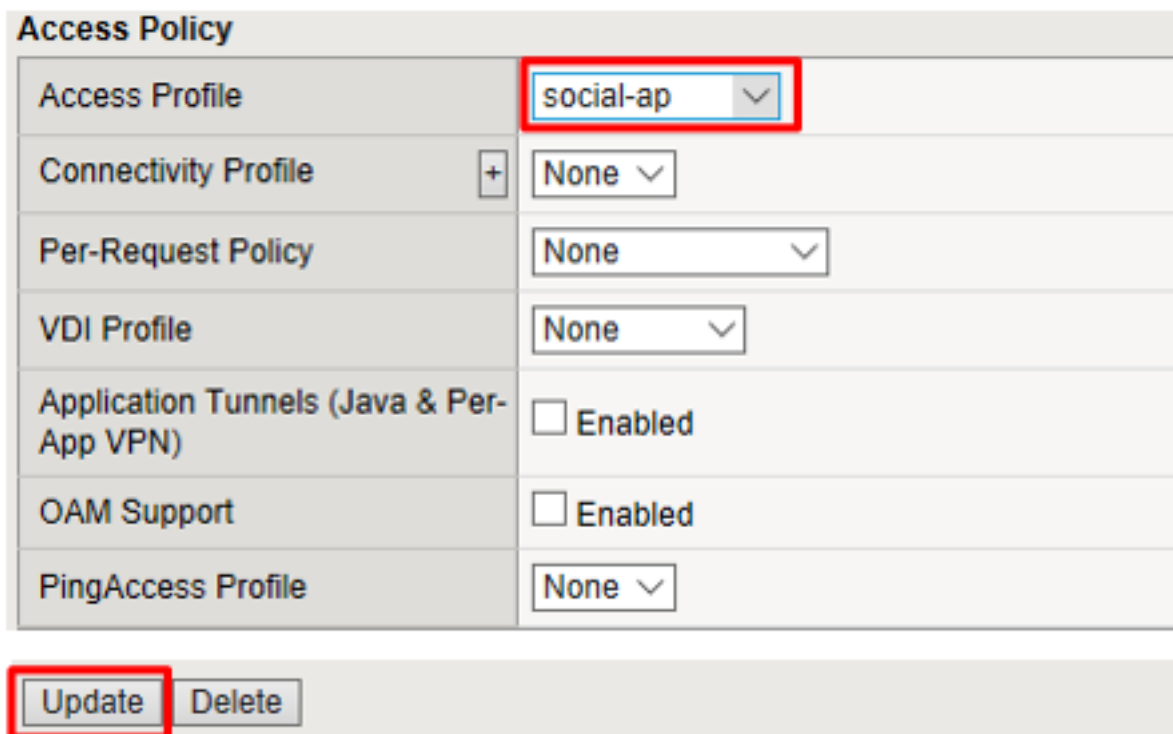12. Click **Apply Access Policy** in the top left and then close the browser tab

2.2.4 Task 3: Add the Access Policy to the Virtual Server
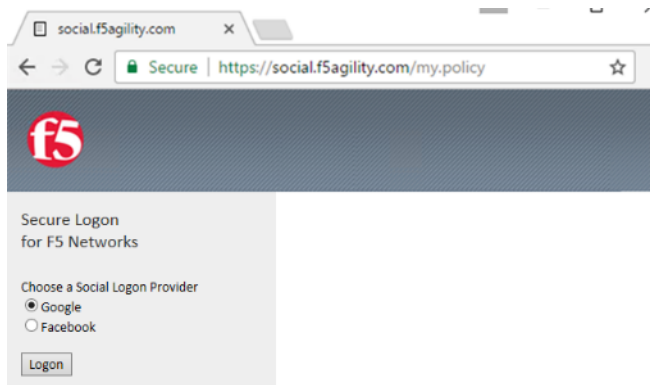
1. Go to **Local Traffic -> Virtual Servers -> social.f5agility.com-vs**

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

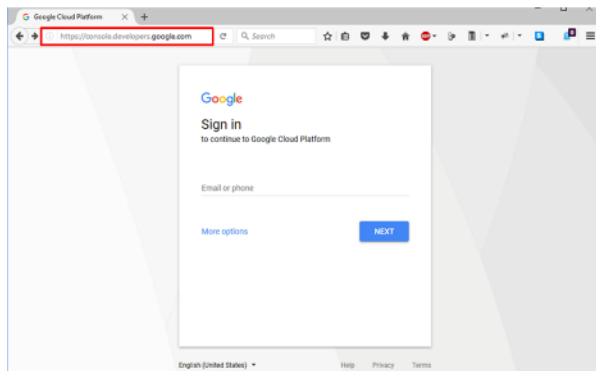3. Test access to https://social.f5agility.com from the jump host again, you should now see a logon page requiring you to select your authentication provider. Any attempt to authenticate will fail since we have only deny endings.
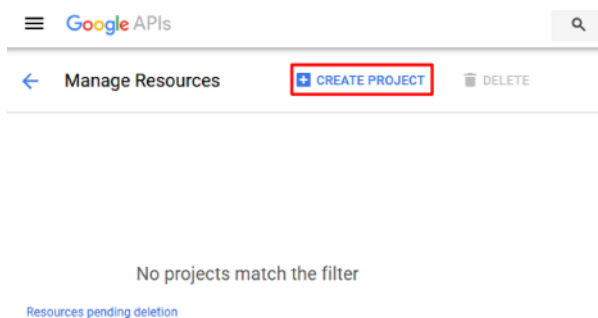
2.2.5 Task 4: Google (Built-In Provider)

Setup a Google Project

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

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**

No projects match the filter
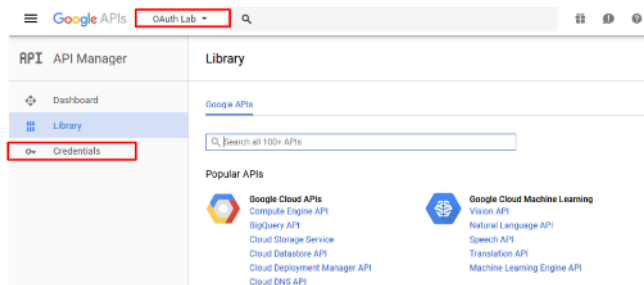
Resources pending deletion

Note: You may have existing projects 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
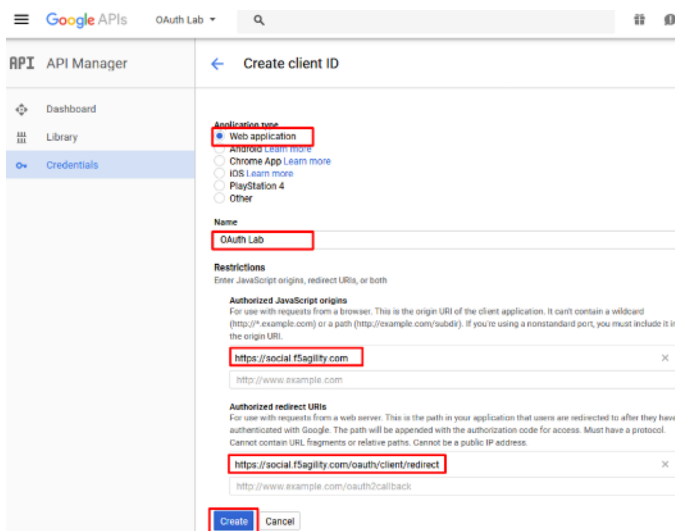
5. Go to the **Credentials** tab (if you are not taken there), click **Create Credentials** and select **OAuth Client ID**
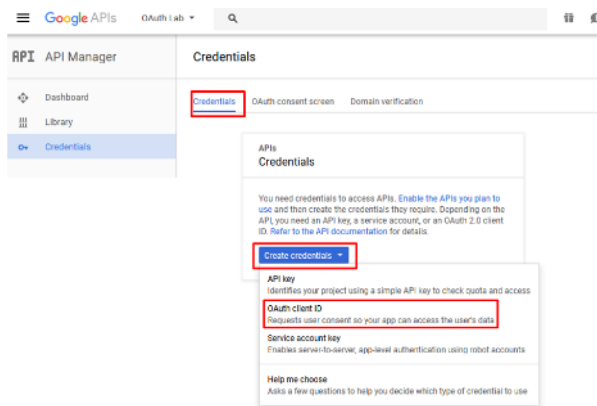
6. Under the **Create Client ID** screen, select and enter the following values and click **Create**

   • **Application Type:** `Web Application`

   • **Name:** `OAuth Lab`

   • **Authorized Javascript Origins:** `https://social.f5agility.com`

   • **Authorized Redirect URIs:** `https://social.f5agility.com/oauth/client/redirect`

7. 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 will be your specific client ID>

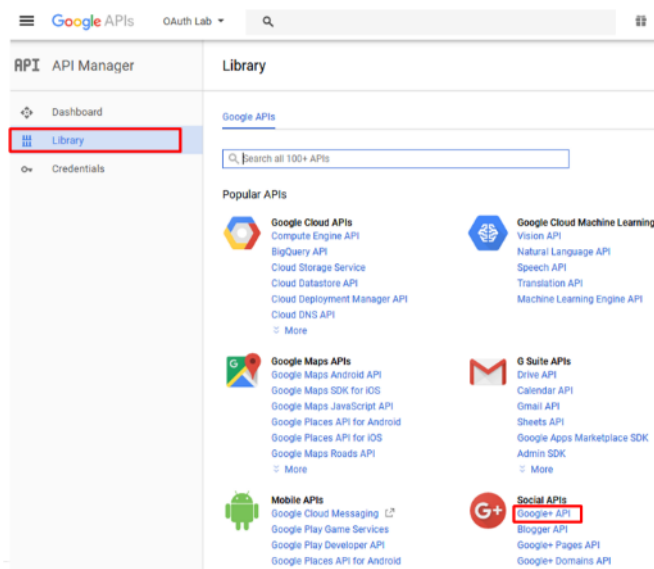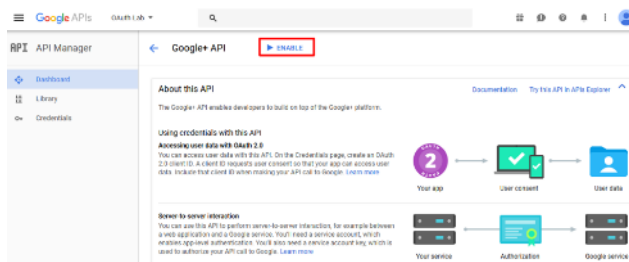Here is your client secret
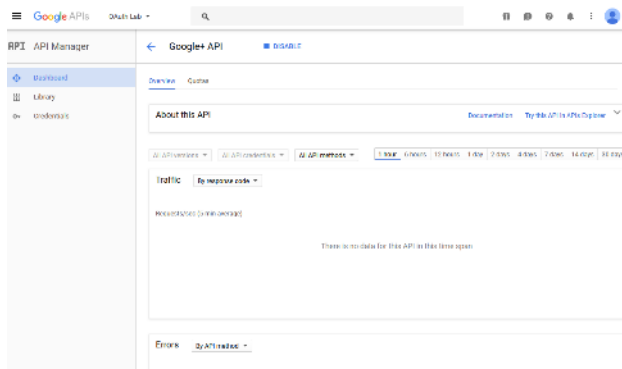
<This will be your specific client secret>

OK

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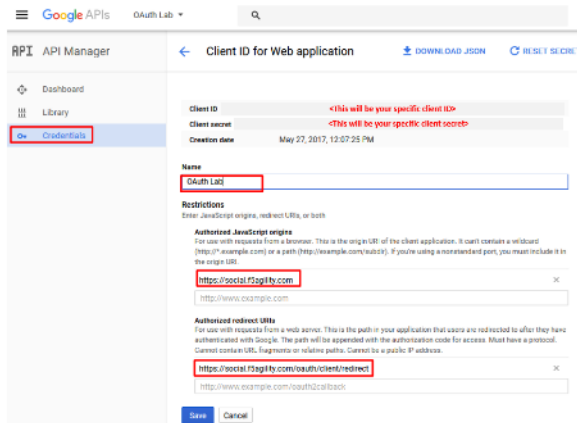

9. Click **Enable** and wait for it to complete, you will now be able to view reporting on usage here
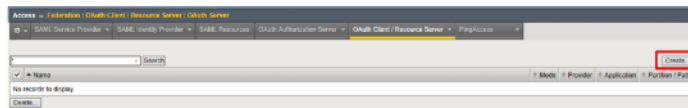
10. For Reference: This is a screenshot of the completed Google project:

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>`

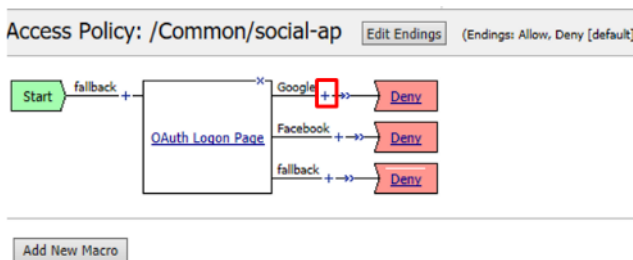- **Resource Server's ServerSSL Profile Name:** `apm-default-serverssl`

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

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

5. Select **OAuth Client** from the **Authentication** tab and click **Add Item**
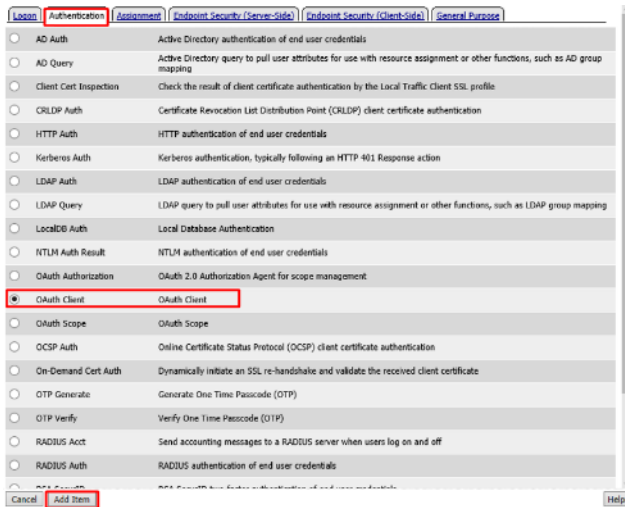
6. Enter the following in the **OAuth Client** input screen and click **Save**

- **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`

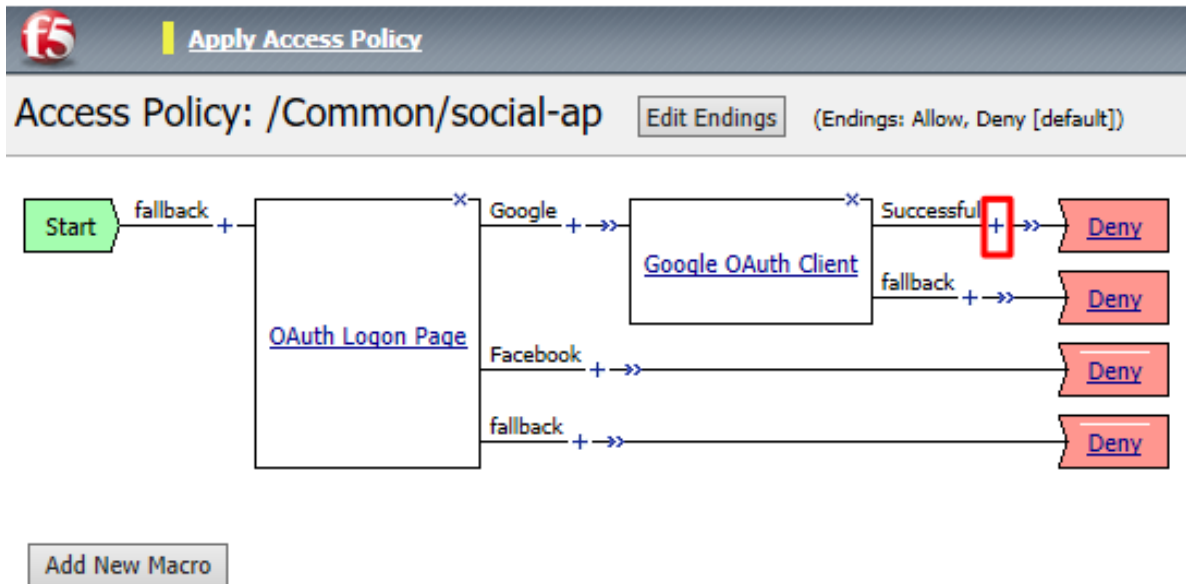7. Click **+** on the **Successful** branch after the **Google OAuth Client**

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

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`

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

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

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

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`

5. Review the **Google Variable Assign** object and click **Save**
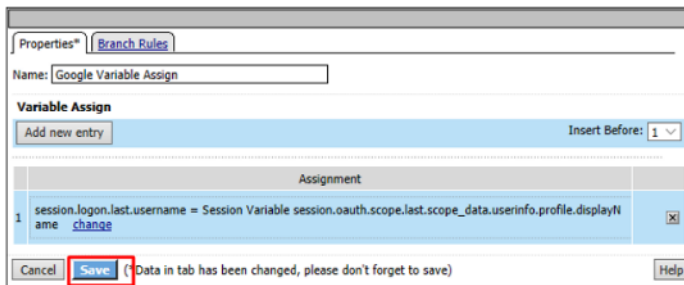
6. Click **Deny** on the **Fallback** branch after the **Google Variable Assign** object, select **Allow** in the pop up window and click **Save**
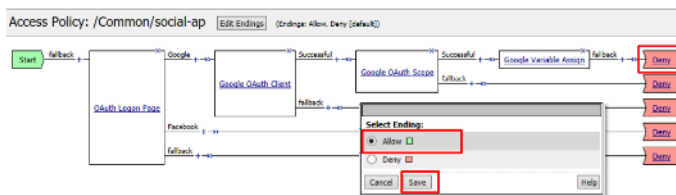
7. Click **Apply Access Policy** in the top left and then close the tab
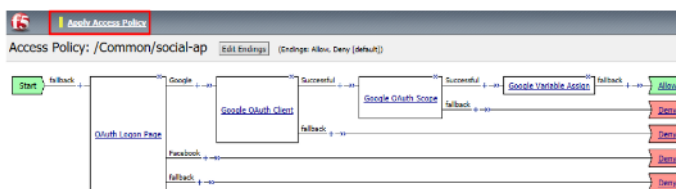
Test Configuration

1. Test by opening Chrome in the jump host and browsing to `https://social.f5agility.com`, select the provider and attempt logon.
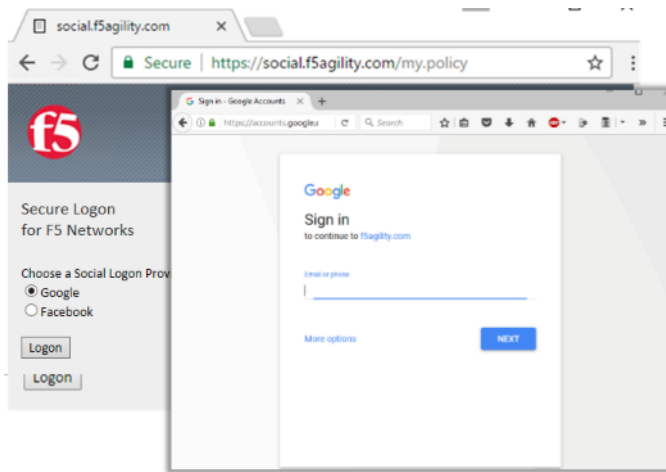
Note: You are able to login and reach the app now, but SSO to the app has not been setup so you get an application error.

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

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
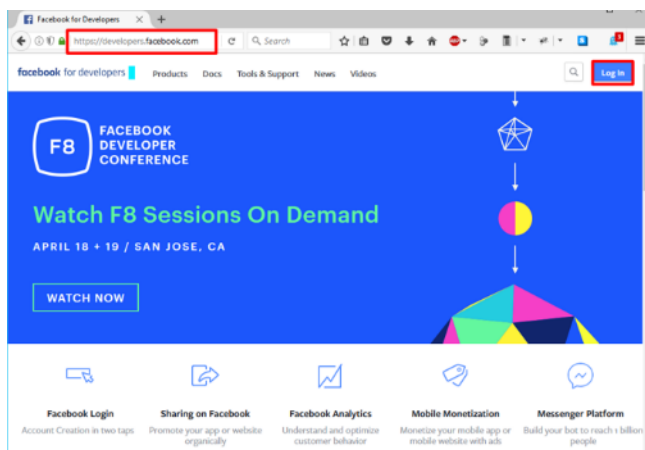
2. If prompted click, **Get Started** and accept the **Developer Policy.** Otherwise, click **Create App**
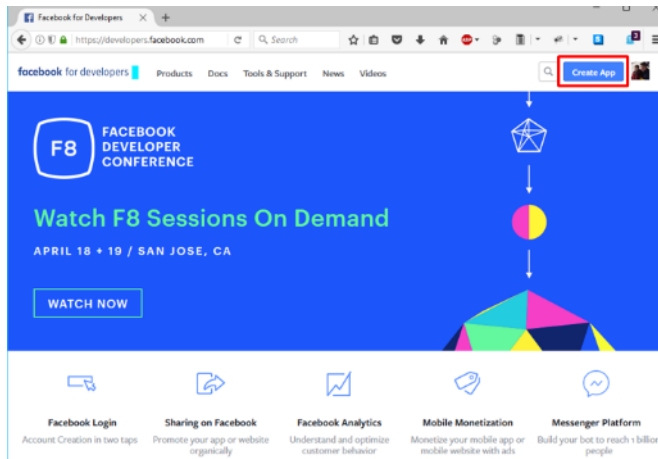
3. Click **Create App** and name (**Display Name**) your app (Or click the top left project drop down and create a new app, then name it). Then click **Create App ID**.

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

---
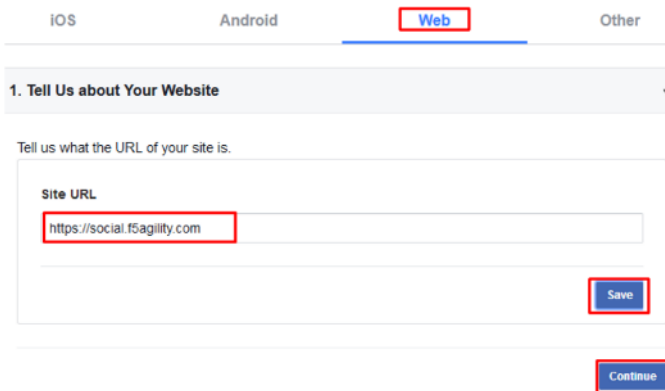
4. Click **Get Started** in the **Facebook Login** section (*Or click + Add Product and then Get Started for Facebook*)
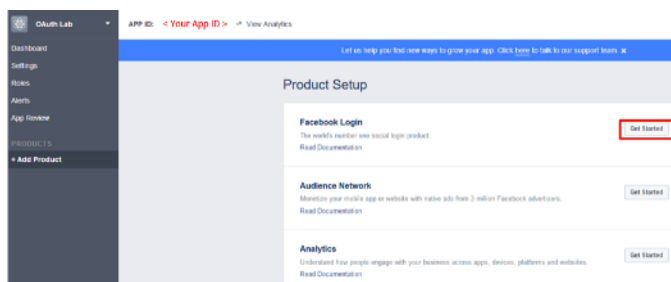
5. From the *"Choose a Platform"* screen click on **WWW (Web)**
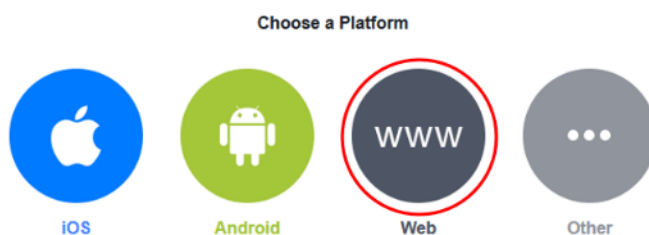
6. In the *"Tell Us about Your Website"* prompt, enter `https://social.f5agility.com` for the **Site URL** and click **Save** then click **Continue**

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

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.

Additional code & text removed

Back | **Next**

10. Click **Facebook Login** on the left side bar and then click **Settings**
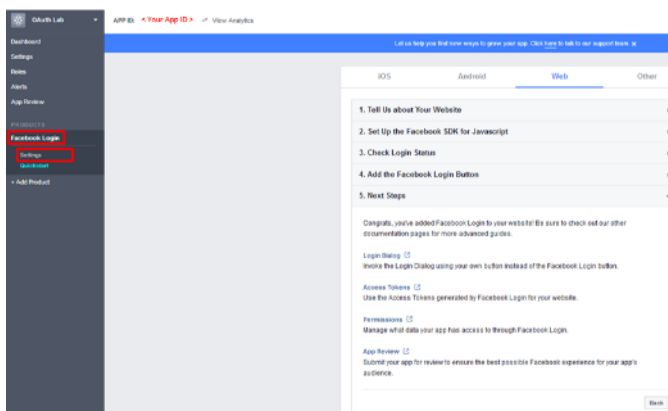
11. For the **Client OAuth Settings** screen in the **Valid OAuth redirect URIs** enter `https://social.f5agility.com/oauth/client/redirect` and then click enter to create it, then **Save Changes**

12. Click **Dashboard** in the left navigation bar
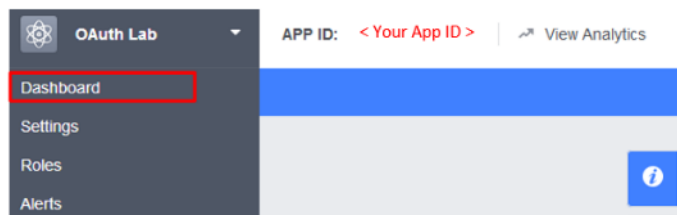
13. Here you can retrieve your **App ID** and **App Secret** for use in Access Policy Manager (APM).

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**
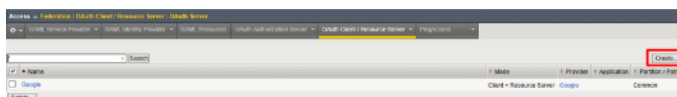
2. Enter the values as shown below for the **OAuth Server** and click **Finished**

- **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`

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
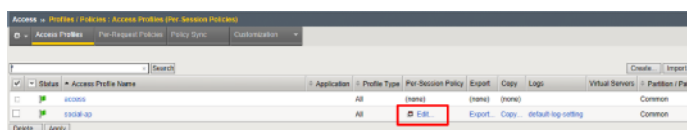
4. Click the + on the **Facebook** provider's branch after the **OAuth Logon Page**
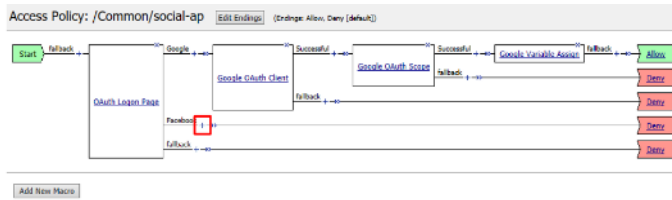
5. Select **OAuth Client** from the **Authentication** tab and click **Add Item**
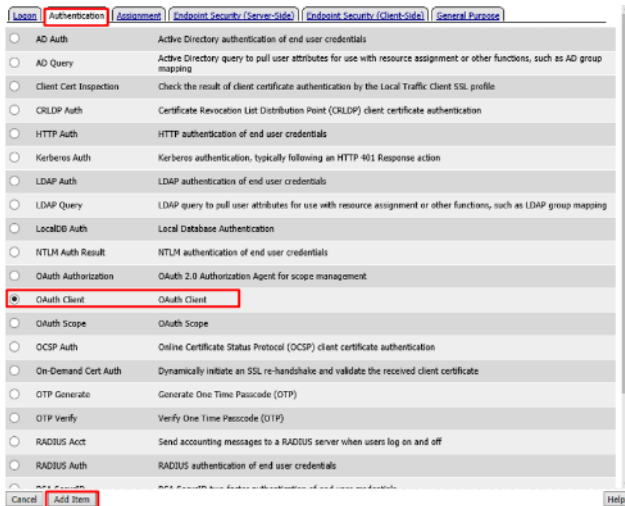
6. Enter the following in the **OAuth Client** input screen and click **Save**

   - **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)*

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

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

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

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

Access Policy: /Common/social-ap   Edit Endings   (Endings: Deny [default], Allow)
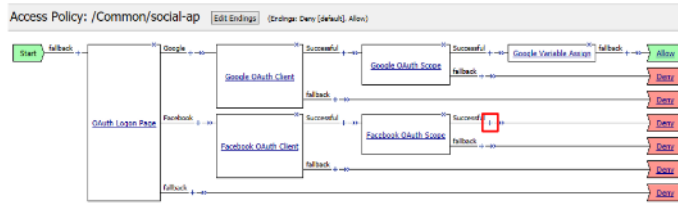
11. Select **Variable Assign** from the **Assignment** tab, and click **Add Item**

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

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`

14. Review the **Facebook Variable Assign** object and click **Save**

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

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.

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 should be prompted to authorize your request. Click **Continue as <Account>** (Where <Account> is your Facebook Profile name)
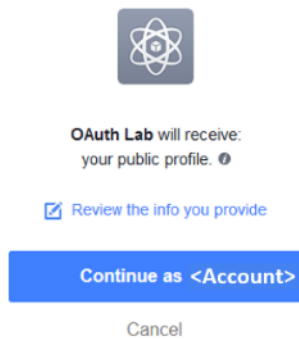
2.2.8 Task 6: LinkedIn (Custom Provider)

1. Login at `https://www.linkedin.com/secure/developer`
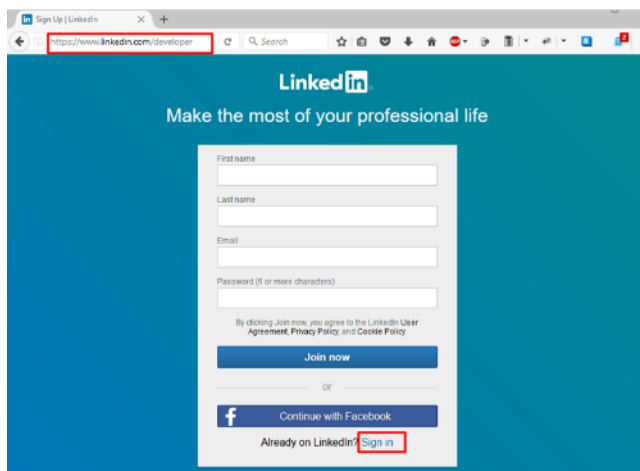
Note: This portion of the exercise requires a LinkedIn Account. You may use an existing one or create one for the purposes of this lab*

---

2. Click **Create Application**
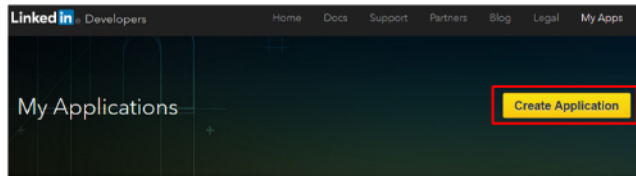
Manage your desktop and mobile applications that leverage LinkedIn APIs.

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

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.

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**
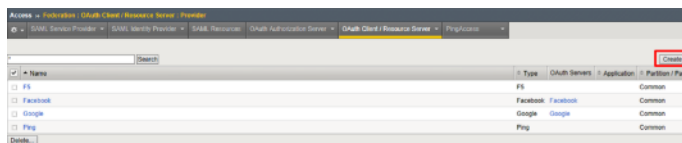
Note: You are creating a "Provider"

---

2. Enter the values as shown below for the **OAuth Provider** and click **Finished**

   - **Name:** `LinkedIn`

   - **Type:** `Custom`

   - **Authentication URI:** `https://www.linkedin.com/oauth/v2/authorization`

   - **Token URI:** `https://www.linkedin.com/oauth/v2/accessToken`

   - **Token Validation Scope URI:** `https://www.linkedin.com/v1/people/~`

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

General Properties

Name	LinkedIn
Description	
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/~

Cancel | Repeat | Finished

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

4. Enter the values as shown for the **OAuth Request** and click **Finished**

- **Name:** `LinkedInAuthRedirectRequest`
- **HTTP Method:** `GET`
- **Type:** `auth-redirect-request`

5. Add the following request parameters and click **Add** after entering the values for each:

- **Parameter Type:** `custom`
- **Parameter Name:** `response_type`
- **Parameter Value:** `code`

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

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

Parameter Type:	custom
Parameter Name:	response_type
Parameter Value:	code

Add

Parameter Type:	client-id
Parameter Name:	client_id

Add

Parameter Type:	redirect-uri
Parameter Name:	redirect_uri

Add

Parameter Type:	scope
Parameter Name:	scope

Add

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

Resource Server -> Request and click **Create**
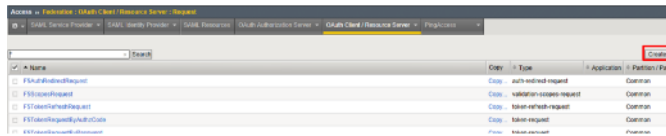
7. Enter the values as shown for the **OAuth Request** and click **Finished**

- **Name:** `LinkedInTokenRequest`
- **HTTP Method:** `POST`
- **Type:** `token-request`

General Properties

Name	LinkedInTokenRequest
Description	

Request Settings

HTTP Method	POST ∨
Type	token-request ∨
	Add values here. → Parameter Type: client-secret ∨
	Parameter Name:
	Add
Request Parameters	grant-type | grant_type redirect-uri | redirect_uri client-id | client_id client-secret | client_secret
	Edit Delete
	Header Name:
	Header Value:
	Add
Request Headers	
	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`

111

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

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

10. Enter the values as shown for the **OAuth Request** and click **Finished**

- **Name:** `LinkedInValidationScopesRequest`
- **HTTP Method:** `GET`
- **Type:** `validation-scopes-request`

General Properties

| Name | LinkedInValidationScopesRequest |
| Description | |

Request Settings

| HTTP Method | GET ∨ |
| Type | validation-scopes-request ∨ |

Add values here. →

Parameter Type: custom ∨
Parameter Name:
Parameter Value:

Add

custom | oauth2_access_token | %{session.oauth.client.last.access_toke
custom | format | json

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`

12. Configure the **OAuth Scope Data Request** Profile Object: Go to **Access -> Federation -> OAuth Client / Resource Server -> Request** and click **Create**
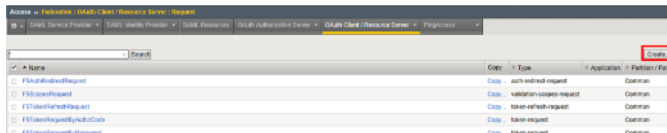
13. Enter the values as shown for the **OAuth Request** and click **Finished**

- **Name:** `LinkedInScopeBasicProfile`

- **HTTP Method:** `GET`

- **URI:** `https://api.linkedin.com/v1/people/~`

- **Type:** `scope-data-request`

General Properties

Name	LinkedInScopeBasicProfile
Description	

Request Settings

HTTP Method	GET ∨
Type	scope-data-request ∨
URI	https://api.linkedin.com/v1/people/~

Add values here.

Parameter Type: custom ∨
Parameter Name:
Parameter Value:

Add

custom | oauth2_access_token | %{session.oauth.client.last.access_toke
custom | format | json

Request Parameters

Edit Delete

Header Name:
Header Value:

Add

Request Headers

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`

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`

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

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

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

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

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

23. Click **Add Expression** on the **Simple** tab

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**

25. Click **Finished** on the **Simple** Expression tab

26. Click **Save** on the completed **Branch Rules** tab

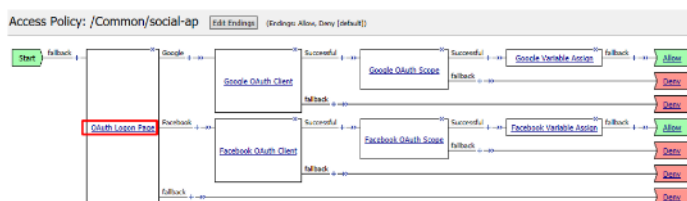27. Click the + on the **LinkedIn** provider's branch after the **OAuth Logon Page**

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)*`

30. Click **+** on the **Successful** branch after the **LinkedIn OAuth Client**
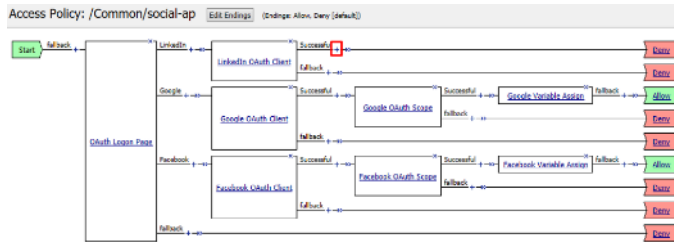
31. Select **OAuth Scope** from the **Authentication** tab, and click **Add Item**

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`
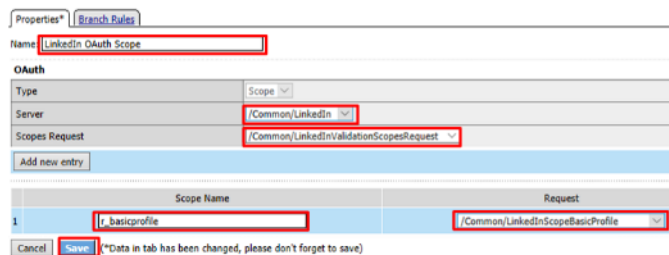
33. Click the **+** on the **Successful** branch after the **LinkedIn OAuth Scope** object
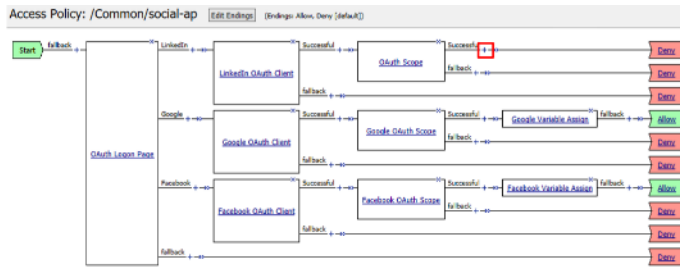
34. Select **Variable Assign** from the **Assignment** tab, and click **Add Item**

35. Name it LinkedIn Variable Assign and click **Add New Entry** then **change**
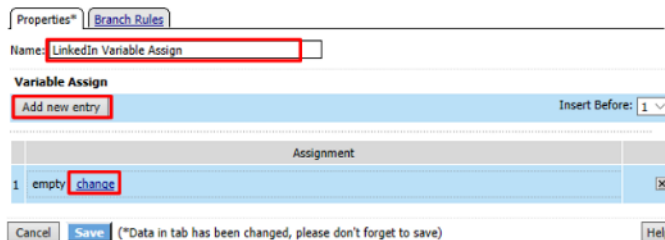
36. Enter the following values and click **Finished**

Left Side:

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

Right Side:

- **Type:** Session Variable
- **Session Variable:** session.oauth.scope.last.firstName
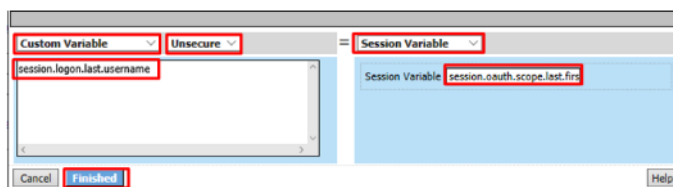
37. Review the **LinkedIn Variable Assign** object and click **Save**
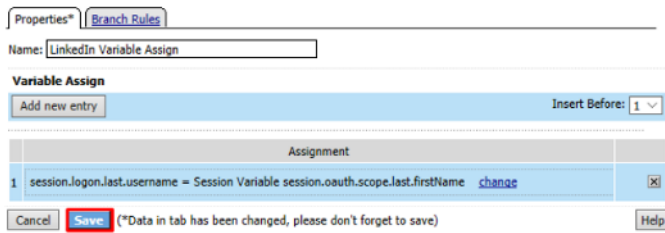
38. Click **Deny** on the **Fallback** branch after the **LinkedIn Variable Assign** object, select **Allow** in the pop up window and click **Save**
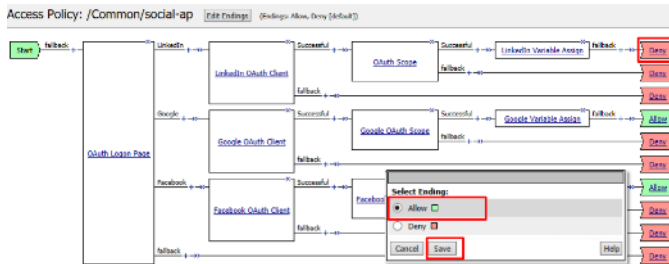
39. Click **Apply Access Policy** in the top left and then close the tab
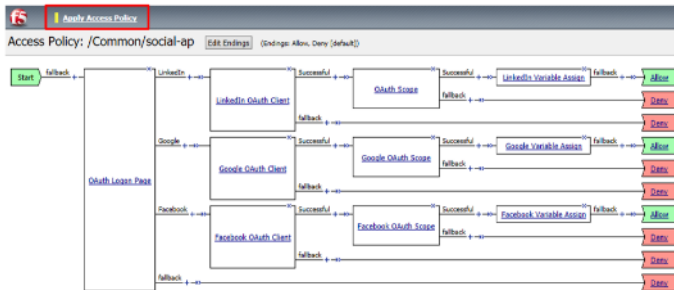
Test Configuration

1. Test by opening Chrome in the jump host and browsing to `https://social.f5agility.com`, select the provider and attempt logon.
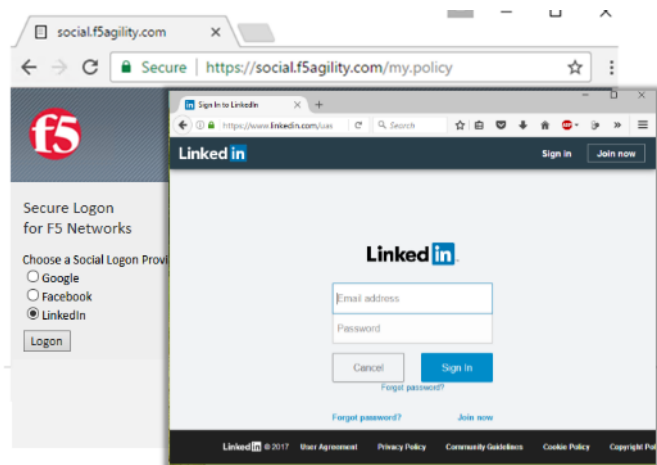
Note: You are able to login and reach the app now, but SSO to the app has not been setup so you get an application error.

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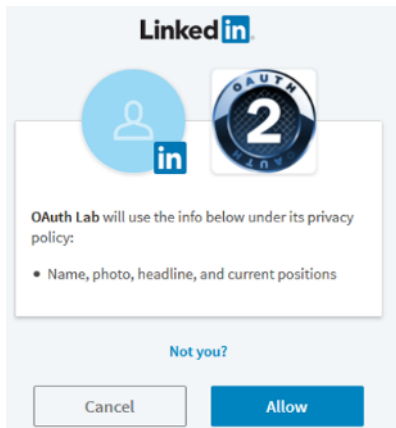
2.2.9 Task 7: Add Header Insertion for SSO to the App

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**

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

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

4. Click the **+** symbol between **Start** and **Allow**

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

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}`

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

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

Add the Per Request Policy to the Virtual Server

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

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**

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.
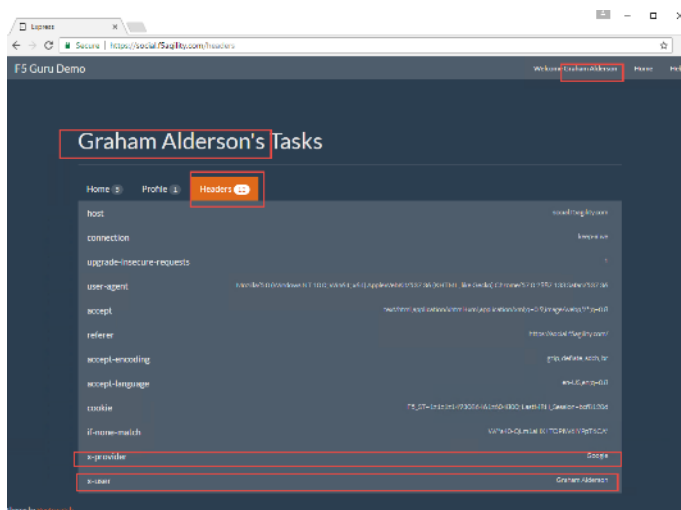
2.3 Lab 2: API Protection

2.3.1 Purpose

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

2.3.2 Task 1: Setup Virtual Server for the API

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

Create the Virtual Server

1. Go to **Local Traffic -> Virtual Servers** and click on **Create**
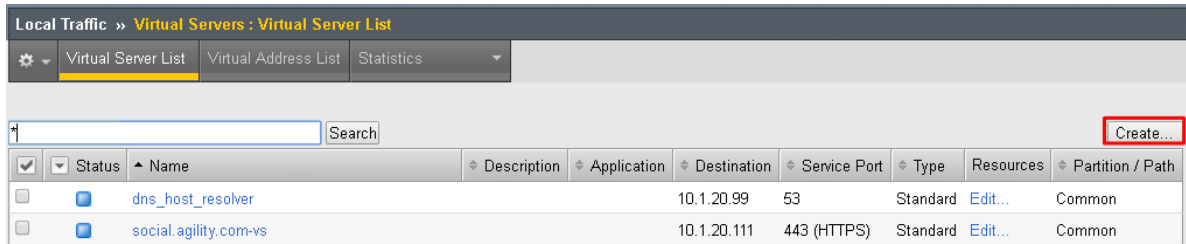
2. Enter the following values *(leave others default)* then scroll down to **Resources**

   - **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`

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

   Default Pool: `api-pool`

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)
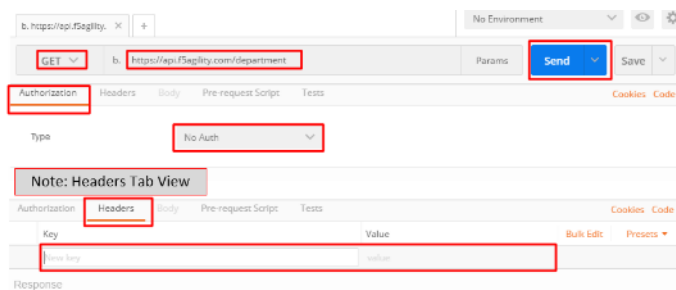
3. You should receive a 200 OK, 4 headers and the body should contain a list of departments.
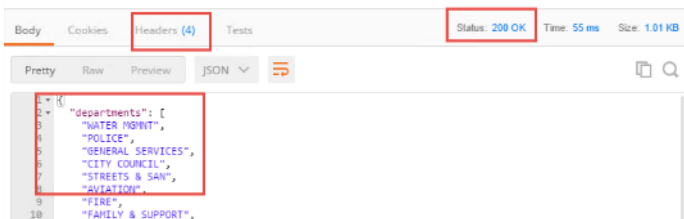
   Note: This request is working because we have not yet provided any protection for the API.*

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

2.3.3 Task 2: Authorization Server

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

Configure the Database Instance

1. Go to **Access -> Federation -> OAuth Authorization Server -> Database Instance** and click **Create**
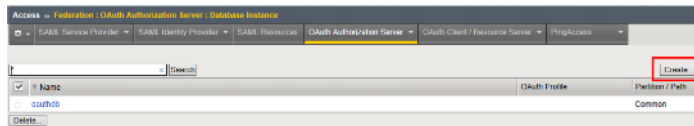
2. Enter oauth-api-db for the **Name** field and click **Finished**.

Configure the Scope

1. Go to **Access** -> Federation -> **OAuth Authorization Server -> Scope** and click **Create**
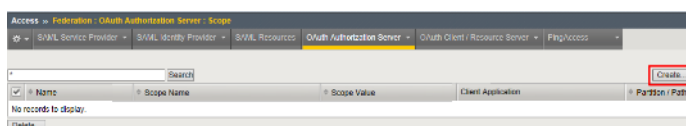
2. Enter the following values and and click **Finished**.

   - **Name:** `oauth-scope-username`
   - **Scope Name:** `username`
   - **Scope Value:** `%{session.logon.last.username}`
   - **Caption:** `username`

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

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**

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

- **Name:** `oauth-api-rs`
- **Application Type:** `Secret`

Configure the OAuth Profile

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

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`

Configure the APM Per Session Policy

1. Go to **Access -> Profiles/Policies -> Access Profiles (Per Session Policies)** and click **Create**
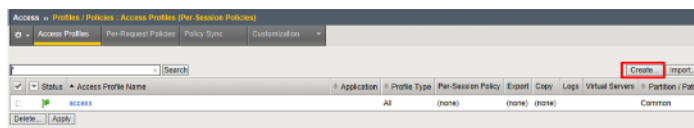
2. In the **General Properties** section enter the following values

   - **Name:** `oauthas-ap`
   - **Profile Type:** `All`
   - **Profile Scope:** `Profile`

General Properties

Name	oauthas-ap
Parent Profile	access
Profile Type	All
Profile Scope	Profile

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
OAuth Profile	+ oauth-api-profile

4. In the **Language Settings** section enter the following value and then click **Finished**.

   • **Languages:** `English`
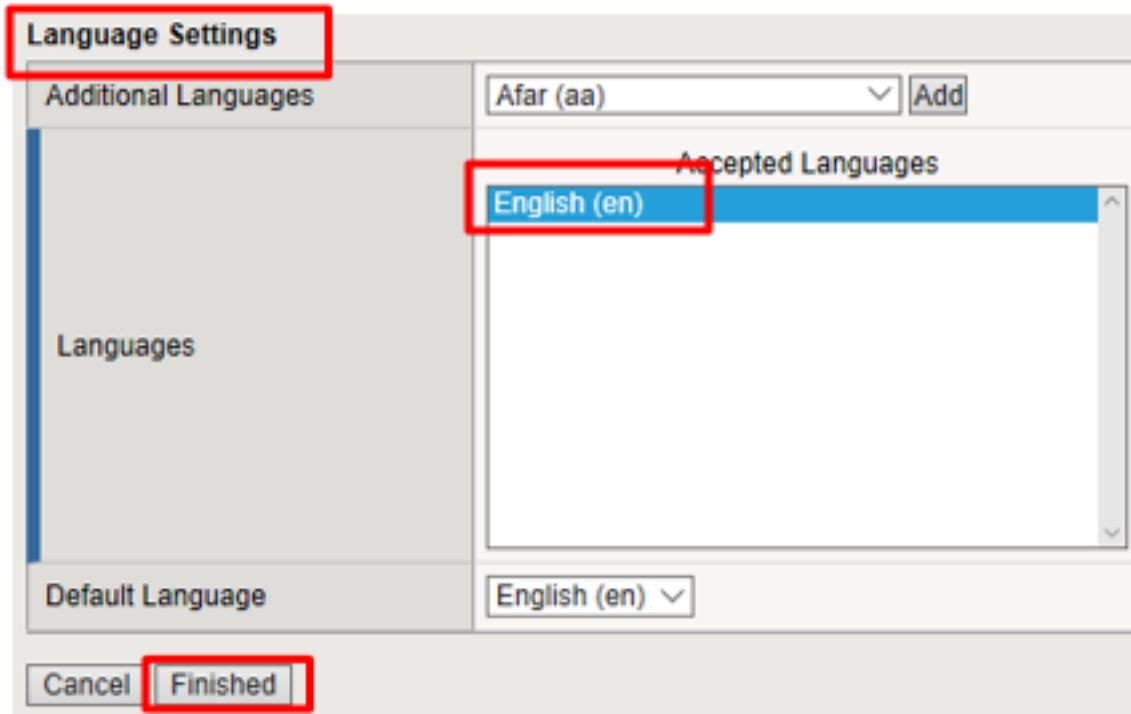
5. Click **Edit** on the **oauthas-ap** policy, a new browser tab will open.

6. Click the **+** between **Start** and **Deny**

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

○	Citrix Logon Prompt	Configure logon options for Citrix clients	
○	External Logon Page	Redirect user to externally hosted form-based web logon page	
○	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication	
○	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)	
○	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication	
○	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials	
○	VMware View Logon Page	Display logon screen on VMware View clients	

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

9. Click the **+** between **Logon Page** and **Deny**
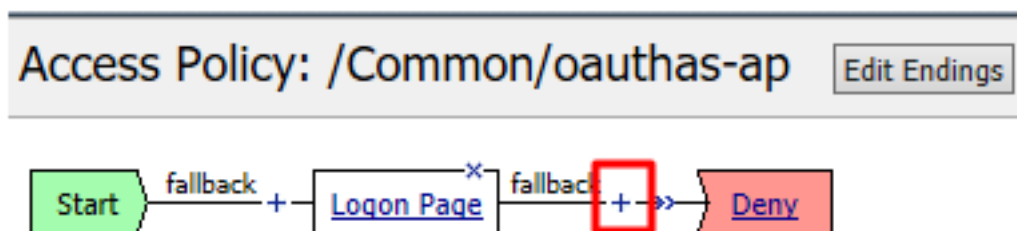
10. Select **OAuth Authorization** from the **Authentication** tab and click **Add Item**

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

12. Click **Deny** on the **Successful** branch after the **OAuth Authorization** object, select **Allow**, click **Save**
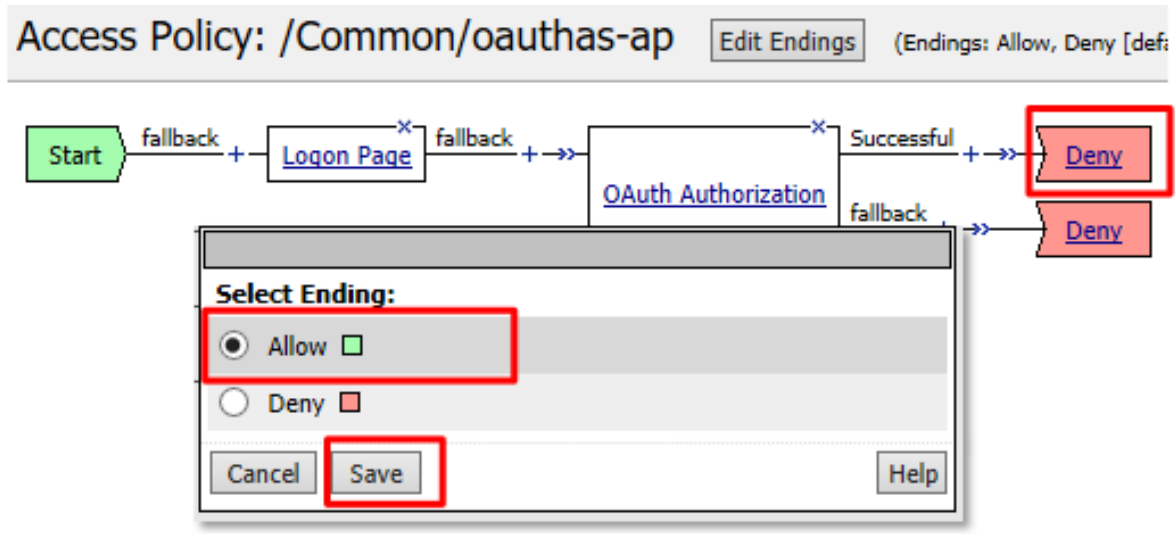
13. Click **Apply Access Policy** in the top left and then close the tab

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**
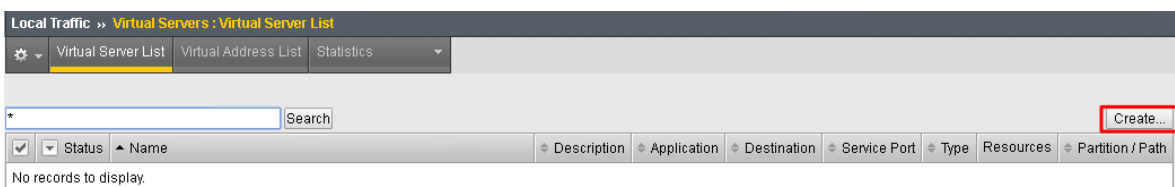
2. Enter the following values for the Authorization Server Virtual Server

- **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	
Type	Standard
Source Address	
Destination Address/Mask	10.1.20.110
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
Traffic Acceleration Profile	None
FTP Profile	None
RTSP Profile	None

SSL Profile (Client)

Selected

/Common
f5agility-wilcard-self-clientssl

Available

clientssl
clientssl-insecure-compatible
clientssl-secure
crypto-server-default-clientssl
splitsession-default-clientssl

SSL Profile (Server)

Selected

Available

/Common
apm-default-serverssl
crypto-client-default-serverssl
pcoip-default-serverssl
serverssl

SMTPS Profile	None
Client LDAP Profile	None
Server LDAP Profile	None
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

144

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.

2.3.4 Task 3: Resource Server

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

Configure the OAuth Provider

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

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`

Configure the OAuth Server

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

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

General Properties

Name	api-resource-server
Description	
Mode	Resource Server ▼
Type	F5 ▼
OAuth Provider	+ oauthas.f5agility.com-provider ▼
DNS Resolver	+ oauth-dns ▼
iRules	Selected Available `<<` `>>` /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-default-serverssl 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

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**

5. Enter the following values and then click **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

	Status	Access Profile Name	Application	Profile Type	Per-Session Policy	Export	Copy	Logs	Virtual Servers	Partiti
☐		access		All	(none)	(none)	(none)			Common
☐		api-ap		OAuth-Resource Server	☐ Edit...	Export...	Copy...	default-log-setting		Common
☐		social-ap		All	☐ Edit...	Export...	Copy...	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

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

Apply Access Policy

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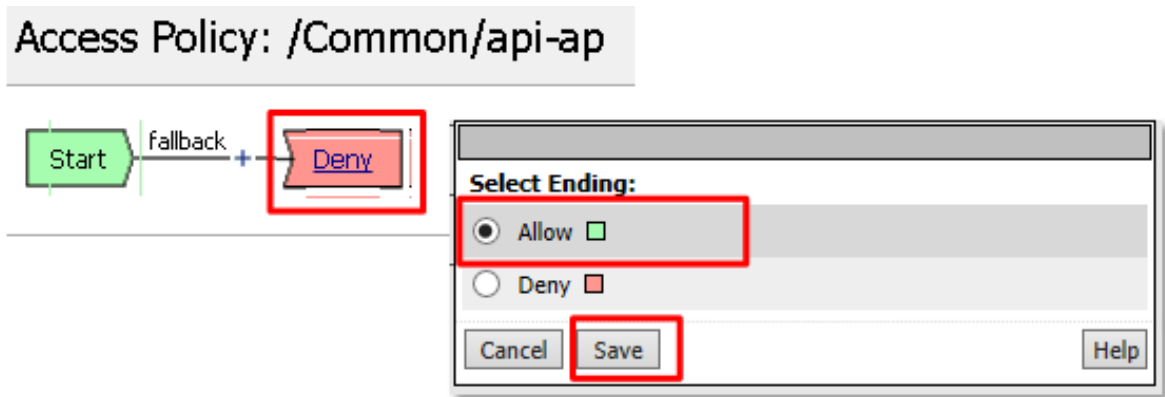
9. To configure the **APM Per Request Policy** go to **Access -> Profiles / Policies -> Per Request Policies** and then click **Create**

	Per-Request Policy Name	Per-Request Policy	Export	Copy	Virtual Servers	Partition / Path
☐	prp-x-user-insertion	☐ Edit...	Export...	Copy...	social.agility.com-vs	Common

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

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

12. Click **Add New Subroutine**

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

14. Click the **+** next to the **RS Scope Check**

15. Click Edit Terminals on the RS Scope Check Subroutine

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

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

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

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

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

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

22. Enter the following values and then click **Save**

    - **Server:** `/Common/api-resource-server`
    - **Scopes Request:** /Common/F5ScopesRequest

23. Verify that the **Successful** branch terminates in **Success** and the **Fallback** branch terminates in **Failure**
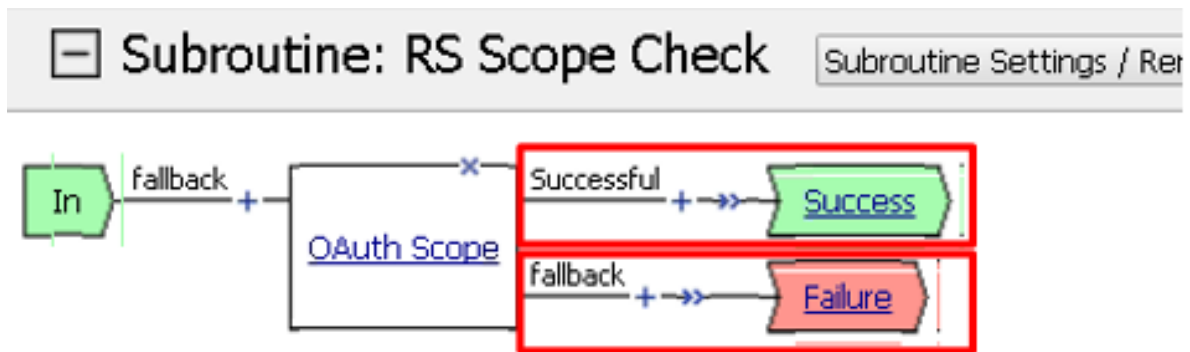
24. In the main policy, click **+** between the **Start** and **Allow**
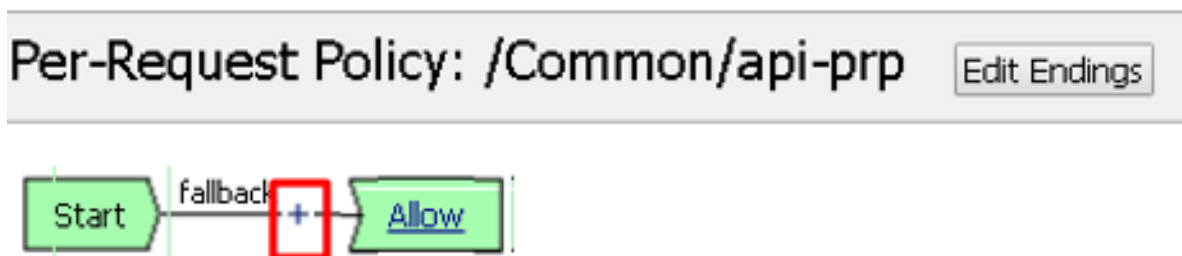
25. Select **RS Scope Check** from the **Subroutines** tab and click **Add Item**
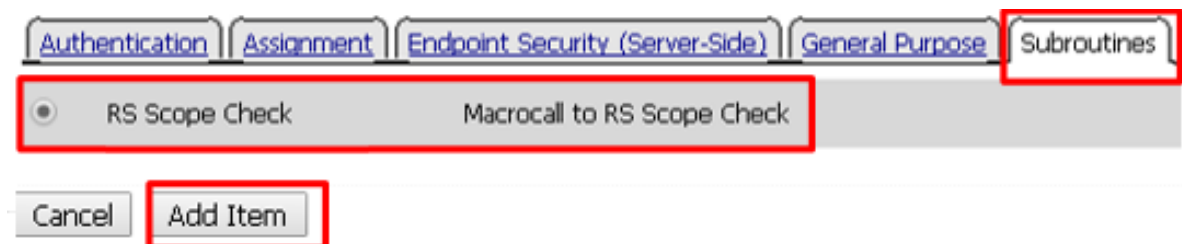
26. Verify that the Success branch terminates in Allow and the Fallback branch terminates in Reject
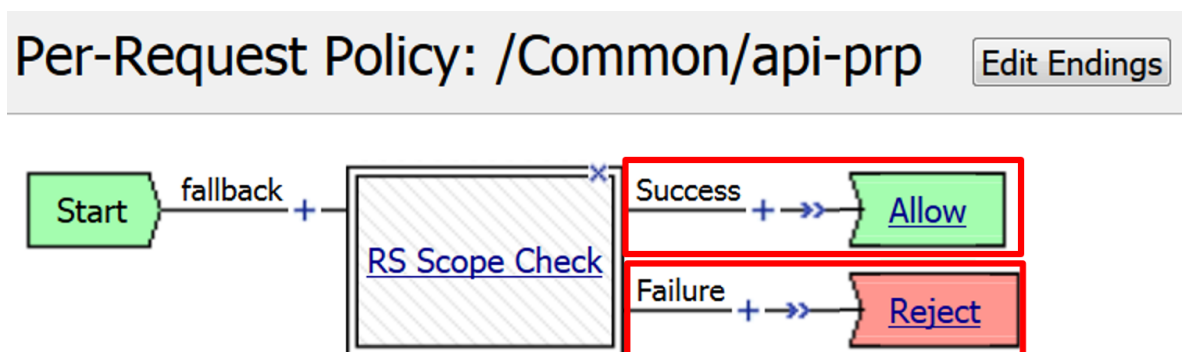
Note: You do not need to "Apply Policy " on Per Request Policies*

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

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

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**
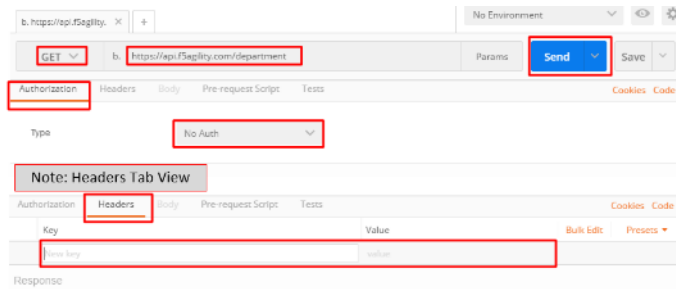
- **Method:** `GET`
- **Target:** `https://api.f5agility.com/department`
- **Authorization:** `No Auth`
- **Headers:** `(none should be set)`

3. You should receive a `401 Unauthorized` and **3 headers**, including `WWW-Authenticate: Bearer`. The body will be empty.
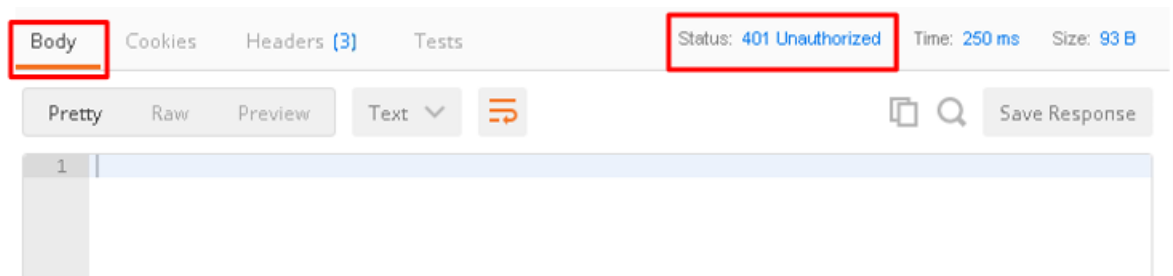
Note: Your API call failed because you are not providing an OAuth token. Both tabs shown
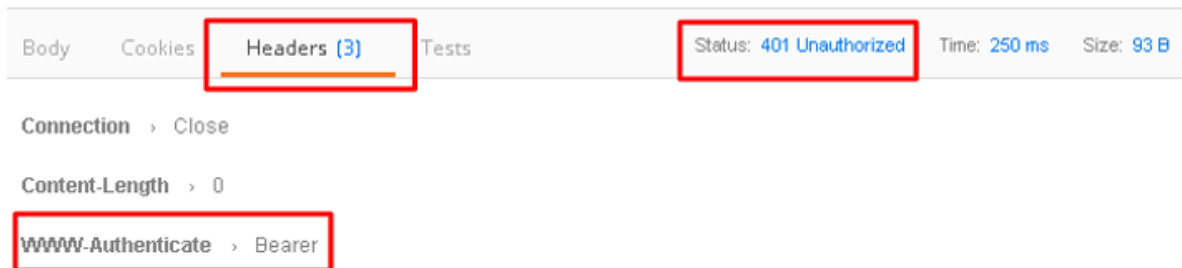
4. Click the **Authorization** tab and change the **Type** from **No Auth** to OAuth 2.0
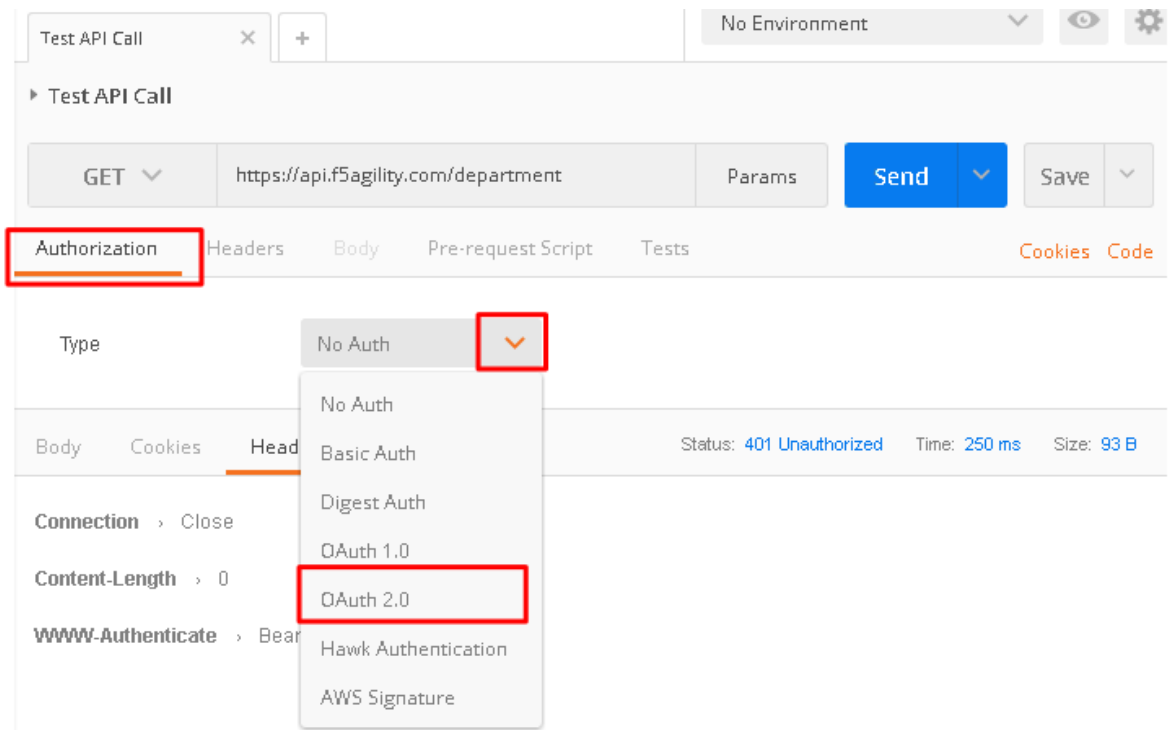
5. If present, select any existing tokens on the left side and delete them on the right side. Click **Get New Access Token**
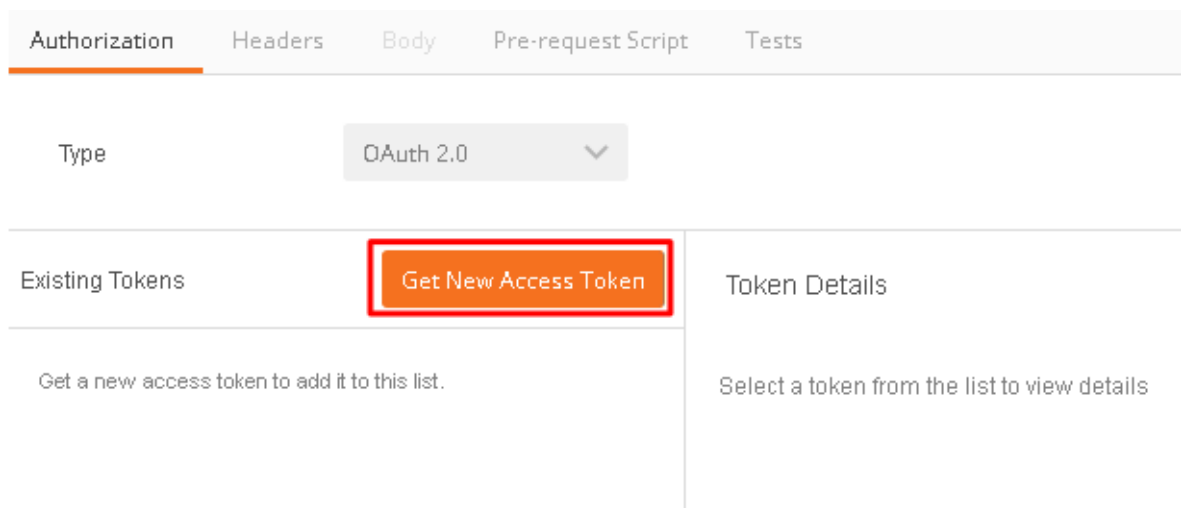
6. In the **Get New Access Token** window, if the values do not match then adjust as needed, and click **Request Token**

   - **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

Callback URL   https://www.getpostman.com/oauth2/callback
                  Set this as the callback URL in your app settings page.

Token Name   MyToken

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

Access Token URL https://oauthas.f5agility.com/f5-oauth2/v1/toke

Client ID   **Your oauth-api-client ID from Big-IP 2**

Client Secret   **Your oauth-api-client secret from Big-IP 2**

Scope (Optional)

Grant Type   Authorization Code   ⌄

              ✓   Request access token locally

                              Cancel   Request Token

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

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

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_token   3c9f4d3bdd9381104a714c196289cb770a45
9507c693a23c862903a5bf770dd3

expires_in   300

token_type   Bearer

The Header tab data is shown in the screenshot

Authorization   Headers (1)   Body   Pre-request Script   Tests   Cookies   Code

Key	Value	Bulk Edit	Presets ▼
☑ Authorization	Bearer c89884a4df2e89f40d14939497bab069385c5410ba...		

11. Click **Send** at the top of the Postman screen
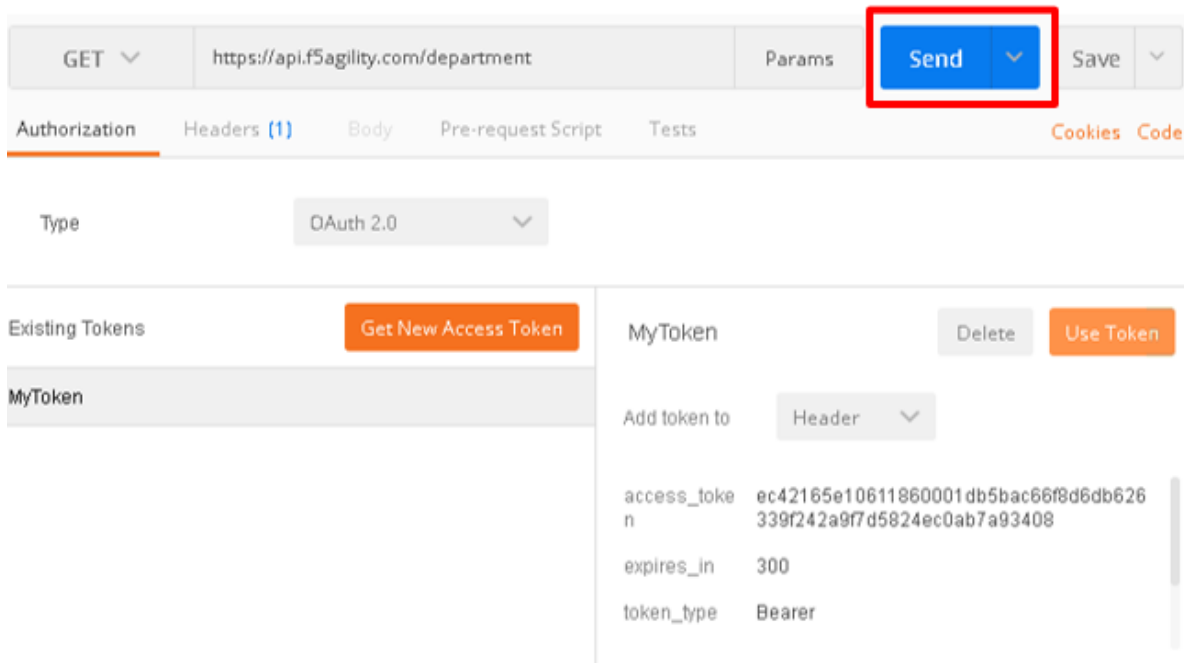
12. You should receive a **200 OK**, **5 headers** and the **body** should contain a list of departments
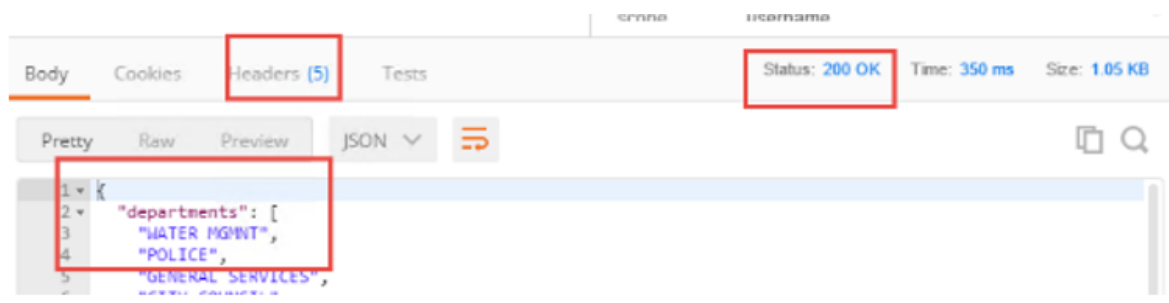
Note: This time the request was successful because you presented a valid OAuth token to the resource server (the Big-IP), so it allowed the traffic to the API server on the backend.

2.3.6 Task 4: Testing Session and Token States

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

Invalidate the Session

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

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.

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.

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

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**

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.

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**

2. 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)*

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*.

2. 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.

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

df4a5200.session.oauth.scope.last.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**

4. 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)*

2.5 Lab 4: Troubleshooting

2.5.1 Task 1: Logging Levels

1. 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.

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
```


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.

3

Class 3: SWG - Securing Outbound Internet Access

Welcome to the APM 231: SWG - Securing Outbound Internet Access lab. These lab exercises will instruct you on configuring F5 Secure Web Gateway (SWG) for typical use cases. This guide is intended to complement lecture material provided during the course and to serve as a reference guide when configuring SWG in your own environment. Expected time to complete: **3 hours**

3.1 Lab Environment

In the interest of time, the following components have been set up with basic configurations for you in a cloud-based virtual lab environment with:

- **Windows Jump Host – Provides remote access the virtual lab** environment via RDP (note: you will need to connect to it using your Remote Desktop Client for Windows/Mac). This will also be your test client.

- **BIG-IP Virtual Edition (VE) – Pre-licensed and provisioned for Access** Policy Manager (APM) and Secure Web Gateway (SWG)

- BIG-IQ Centralized Management (CM) VE – BIG-IQ console

- BIG-IQ Data Collection Device (DCD) VE – BIG-IQ logging node

- Windows Server – Active Directory and DNS services

- DLP Server – ICAP mode

Each student's lab environment is independent.

3.1.1 Lab Environment Diagram

The following diagram illustrates the lab environment's network configuration and will be useful if you wish to replicate these exercises in your personal lab environment:
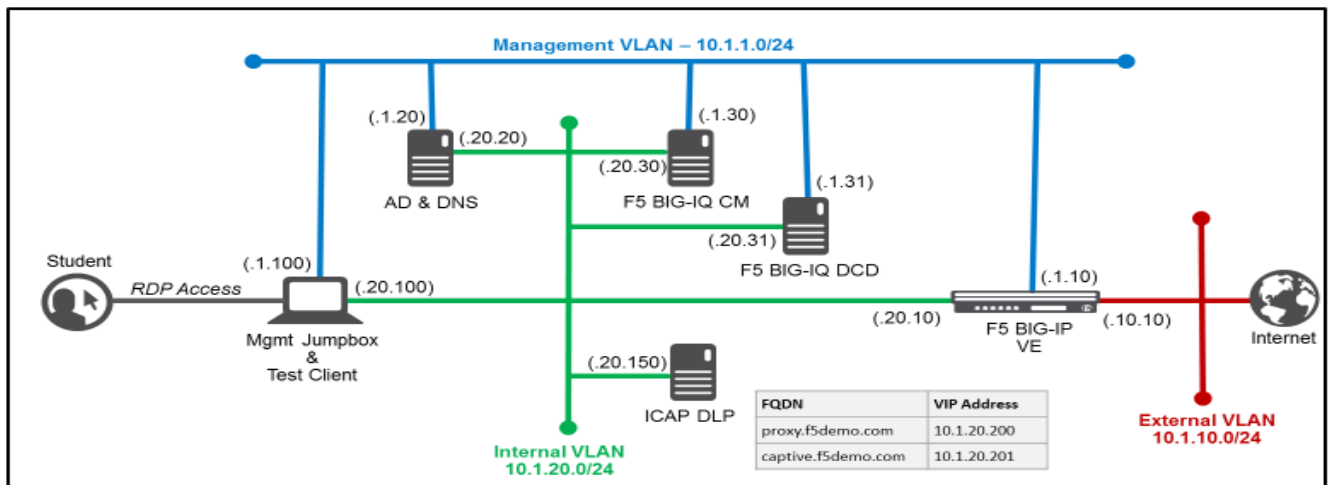
3.1.2 Timing for Labs

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. Below is an estimate of how long it will take for each lab:

Lab Timing

Lab name (Description)	Time Allocated
Use Case: Enterprise Web Filtering	
Lab 1: SWG iApp - Explicit Proxy for HTTP and HTTPS	30 minutes
Lab 2: URL Category-based Decryption Bypass	25 minutes
Lab 3: Explicit Proxy Authentication - NTLM	25 minutes
Use Case: Access Reporting	
Lab 4: SWG Reporting with BIG-IQ	15 minutes
Use Case: Guest Access Web Filtering	
Lab 5: SWG iApp – Transparent Proxy for HTTP and HTTPS	15 minutes
Lab 6: Captive Portal Authentication	25 minutes
Use Case: SSL Visibility	
Lab 7: SSL Visibility for DLP (ICAP)	15 minutes

3.1.3 General Notes

Provisioning Secure Web Gateway (SWG) requires Access Policy Manager (APM to also be provisioned.

When working with iApp templates for the first time, you should change the BIG-IP Configuration Utility's default "**Idle Time Before Automatic Logout**" setting to a larger value. This has already been done for you in the lab environment to save time.

3.1.4 Accessing the Lab Environment

To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces using HTTPS and SSH. You will also be using the Jump Host as a test client.

You class instructor will provide additional lab access details.

1. **Establish an RDP connection to your Jump Host and login with the** following credentials:

   • User: JUMPBOX\external_user

   • Password: password

1. Use Firefox to access the BIG-IP GUI (https://10.1.1.10).

2. **Login into the BIG-IP Configuration Utility with the following** credentials:

   • User: admin

   • Password: admin

3.2 Lab 1: SWG iApp – Explicit Proxy for HTTP and HTTPS

In this lab exercise, you will learn how to automate and simplify a deployment of SWG using an iApp template.

Estimated completion time: 30 minutes

Objectives:

   • Create an Explicit Proxy configuration by deploying the SWG iApp template

   • Test web browsing behavior

Lab Requirements:

   • BIG-IP with SWG licensed

   • BIG-IP must have access to the public Internet

   • BIG-IP must have access to a DNS server that can resolve queries for public Internet web site names

   • The latest iApp for SWG can be downloaded from **https://downloads.f5.com/** (browse to BIG-IP **iApp Templates**) Note: The iApp has already been downloaded and imported for you.

Before you can deploy the SWG iApp template, you must have the following objects configured:

   • AD AAA server

   • SWG-Explicit Access Policy

   • Custom URL Filter

   • Per-Request Access Policy

3.2.1 Task 1 – Create an "SWG-Explicit" Access Policy for Authentication

Create an AD AAA Server

- Create an AD AAA server by selecting **Access >> Authentication >> Active Directory** and clicking on **Create. . .**
- Change the Name to **AD_F5DEMO**
- Change the Domain Name to **f5demo.com**
- Change Server Connection to **Direct**
- Change the Domain Controller to **10.1.20.20**
- Click **Finished**

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
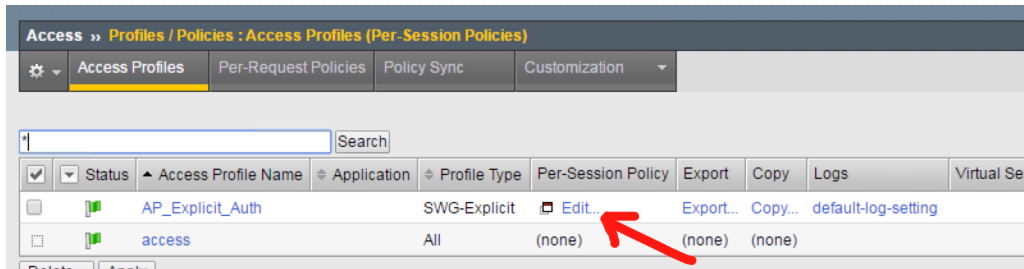
- Select the **+** between Start and Deny and **Add** an **HTTP 407 Response** object
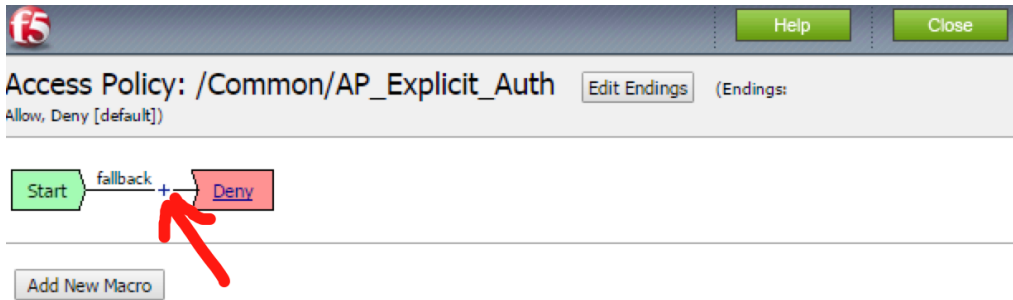
- Change the **HTTP Auth Level** to **basic**

- Click **Save**
- On the **Basic** branch of the **HTTP 407** Object, **Add** an **AD Auth** Object

- Change the **Server** to **/Common**/**AD_F5DEMO** and change **Show Extended Error** to **Enabled**

- 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
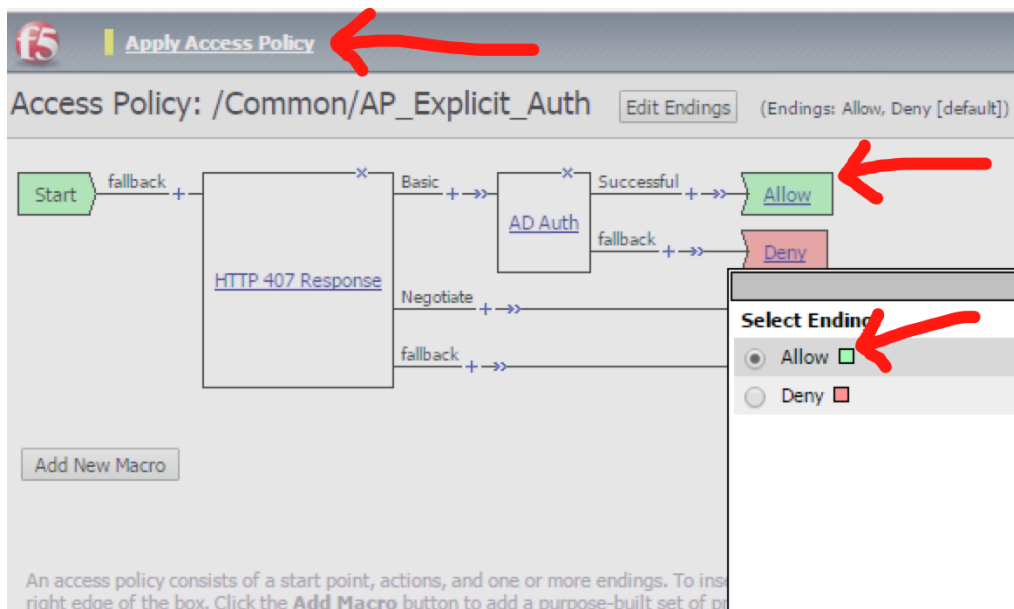
3.2.2 Task 2 – Create a custom URL Filter

- Browse to **Access >> Secure Web Gateway >> URL Filters** and click **Create. . .**
- Name your filter **LAB_URL_FILTER** and click **Finished**
- Click on the first check box to select all categories
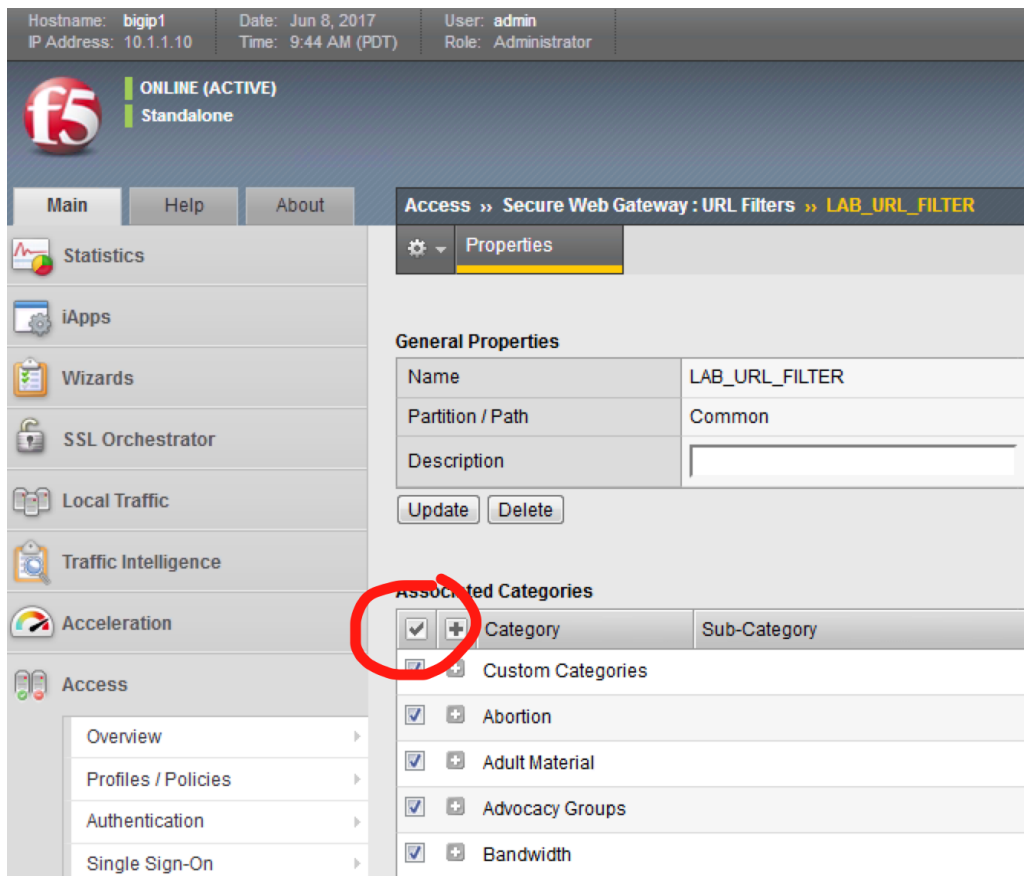
• Click **Allow** at the bottom of the page
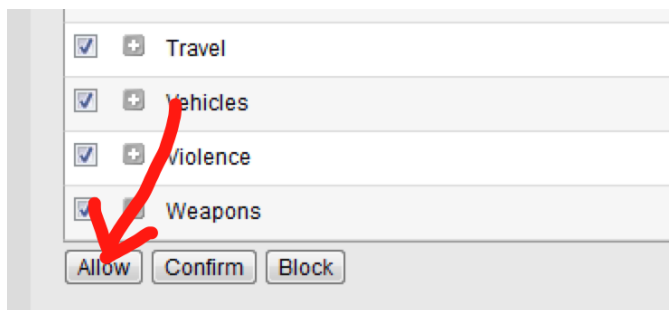
• Click the check box to select **Social Web – Facebook** and then click **Block** (for this lab, our URL filter will only block Facebook)
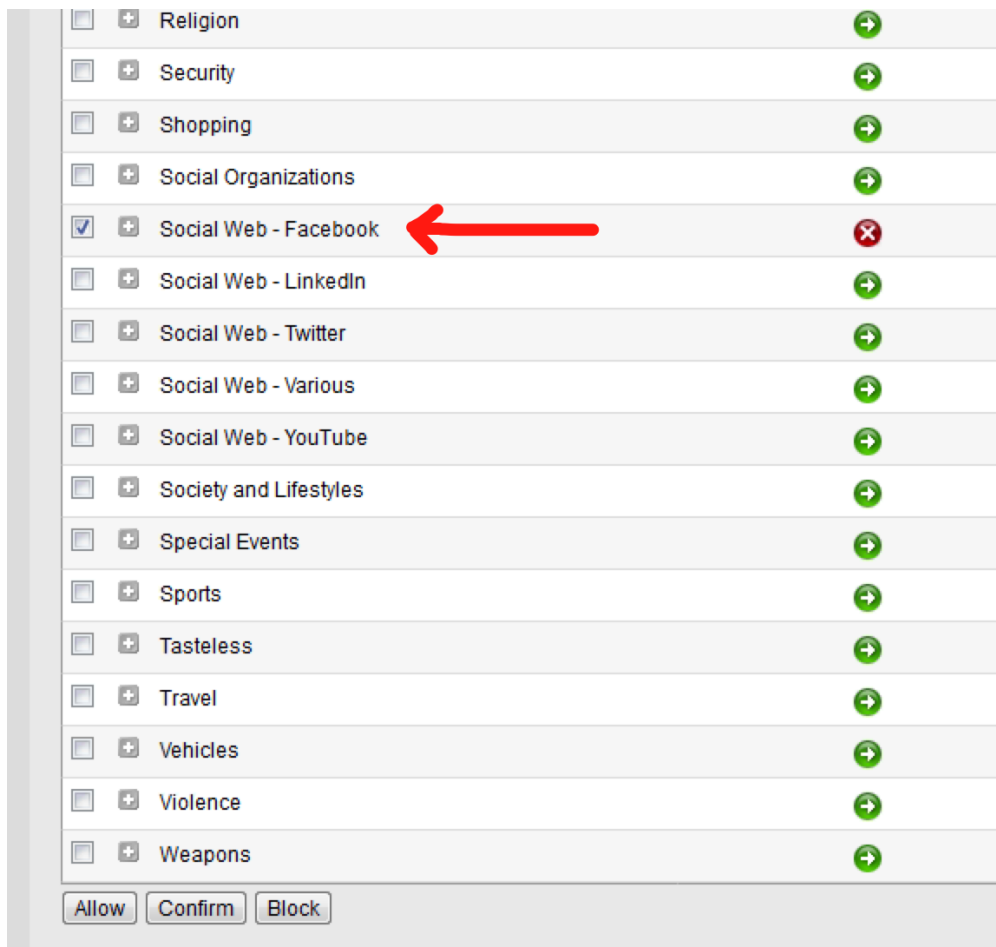
3.2.3 Task 3 – Create a "Per-Request" Access Policy

- Browse to **Access >> Profiles / Policies >> Per-Request Policies** and click **Create...**
- Name your policy **Lab_Per_Request**
- Click **Finished**
- Click on the **Edit...** link for the appropriate Per-Request Policy created above, then go back to the VPE tab in your browser
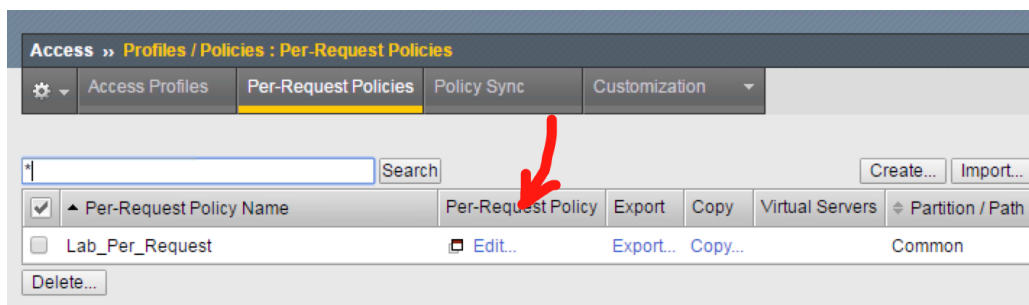
- Click on the **+** symbol between **Start** and **Allow**
- Go to the **General Purpose** tab and add a **Protocol Lookup** object
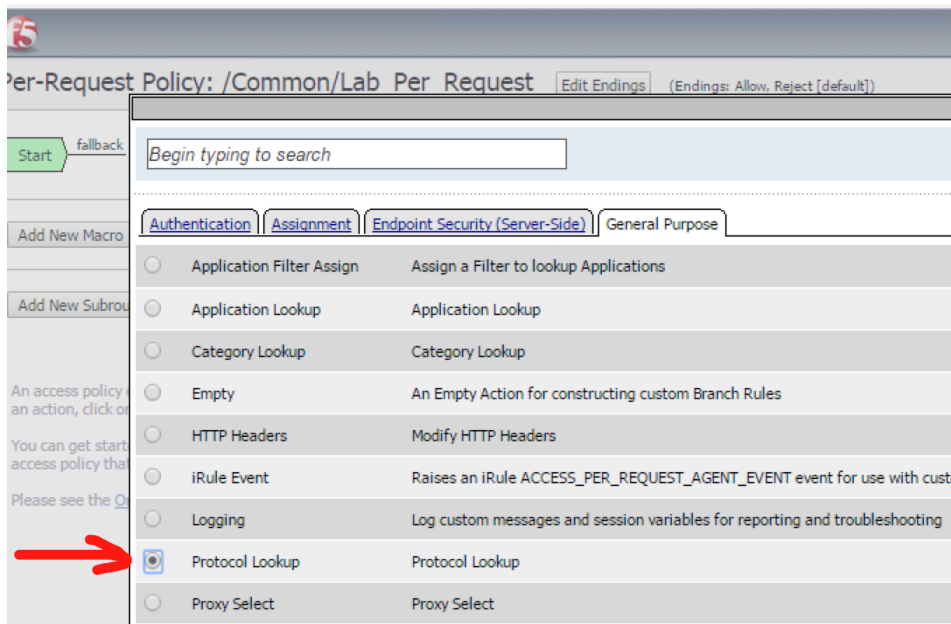
- Click **Add Item**

- Click **Save**

- On the HTTPS branch, click the **+** and **Add** a **Category Lookup** object (**General Purpose** tab)
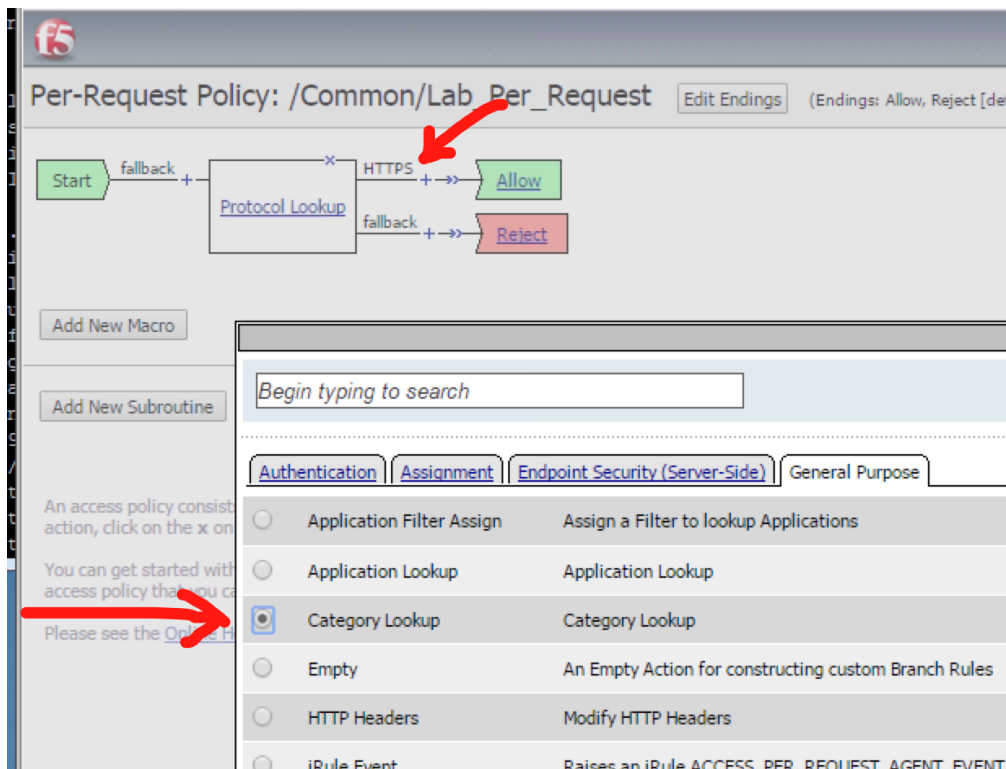
- Select **Use SNI in Client Hello** for **Categorization Input**

- 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**
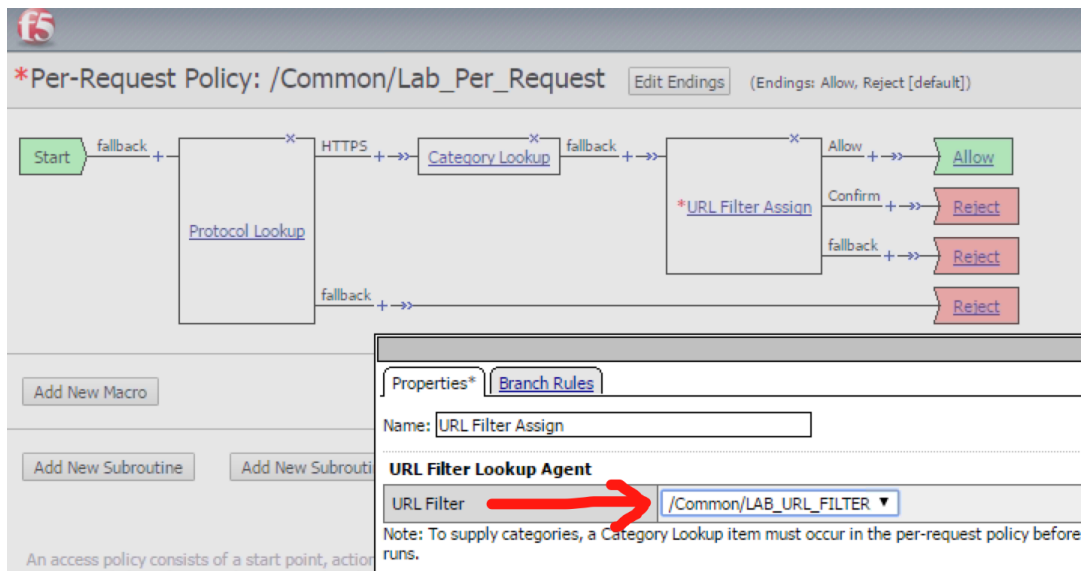
Important: Change the Ending of the **Allow** outcome on the "fallback" branch from "Reject" to **Allow**
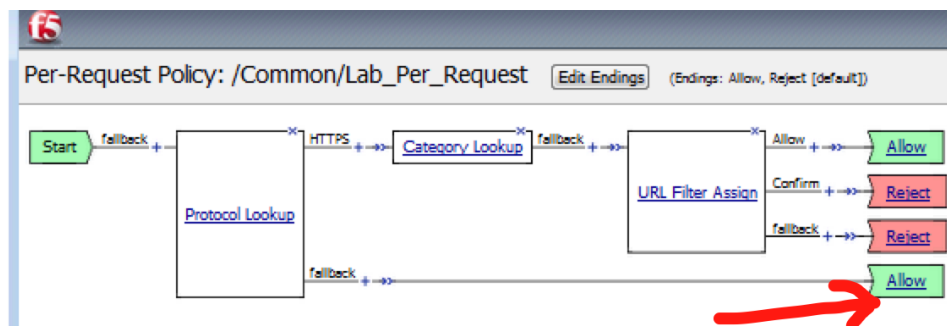
3.2.4 Task 4 – Create Explicit Proxy Configuration using the SWG iApp

Import the SWG iApp template into the BIG-IP – Note: This has been done for you.

• In the BIG-IP Management UI, browse to **iApps >> Templates** and click **Import. . .**

• Click **Choose File** or **Browse. . .** and select the iApp file (at the time of writing the current version is 1.1.0rc4 (f5.secure_web_gateway.v1.1.0rc4.tmpl).

• Click **Open** and **Upload**

Create a SWG proxy configuration

• Browse to **iApps >> Application Services**

• Click **Create. . .**

• Change the name to **SWG**

• Change the Template to **f5.secure_web_gateway.v1.1.0rc4** (your version may be newer)

1. Answer the questions as follows:

Question	Answer
Do you want to see inline help? | Yes, show inline help	
Do you want to enable advanced options?	No, do not enable advanced options
Which type of SWG configuration do you want to deploy	Explicit Proxy
Do you want to use ICAP to forward requests for inspection by DLP servers?	No, do not use ICAP for DLP
What IP address and port do you want to use for the virtual server?	– 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 resolve this FQDN to the correct IP address indicated above.
On which ports should the system accept HTTP traffic?	80
On which ports should the system accept HTTPS traffic?	443
Which SWG-Explicit Access Policy do you want to use?	AP_Explicit_Auth
Which Per-Request Access Policy do you want to use?	Lab_Per_Request
Do you want the system to forward all name requests?	Yes, forward all name requests
Which DNS servers do you want to use for forwarding?	– IP: 10.1.20.20 – Port: 53
Which SSL profile do you want to use for client-side connections?	Create a new Client SSL profile
Which Subordinate CA certificate do you want to use?	f5agility.crt
Which CA key do you want to use?	f5agility.key
Does the key require a password? If so, type it here	F5labs
Which SSL profile do you want to use for server-side connections?	Create a new Server SSL profile

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

3.2.5 Task 5 – Verify that the "F5 Agility CA" certificate is trusted

A Windows Domain Group Policy was configured to deploy the CA certificate that SWG uses to forge new certificates (on behalf of the origin server) to domain-joined machines.

- Open Internet Explorer on your Jump Host client machine
- Click the gear icon or hit `Alt-X` and select **Internet options**
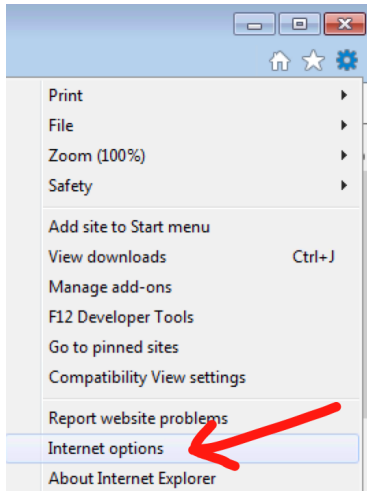
- Go to the **Content** tab and click **Certificates**

- Click on the **Trusted Root Certification Authorities** tab and scroll down. You should see the **F5 Agility CA** certificate in the list.
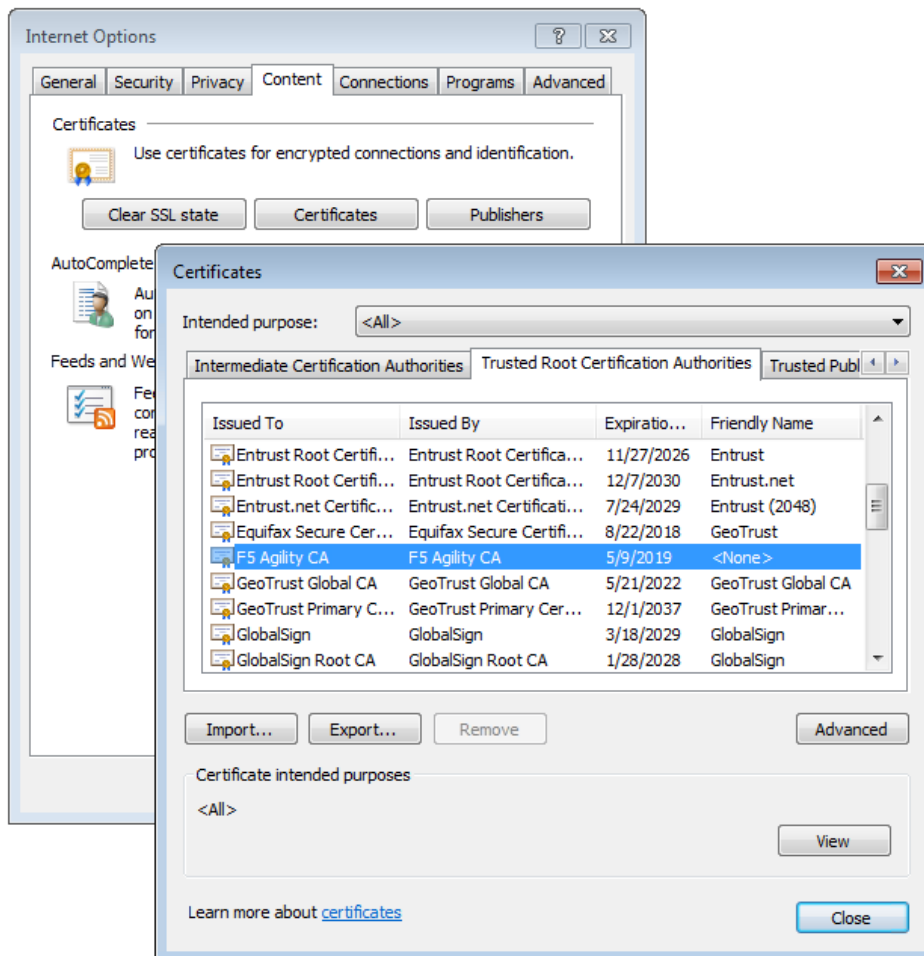
- Double-click on the certificate to view its properties, then close this window and the Certificates window.

3.2.6 Task 6 – Testing

Configure your browser with a "Proxy Server"

- Go to the **Connections** tab and click **LAN settings**
- Enable the checkbox for **Use a proxy server for your LAN** and enter:
    - Address: **10.1.20.200**
    - Port: **3128**
- Click **OK** twice.
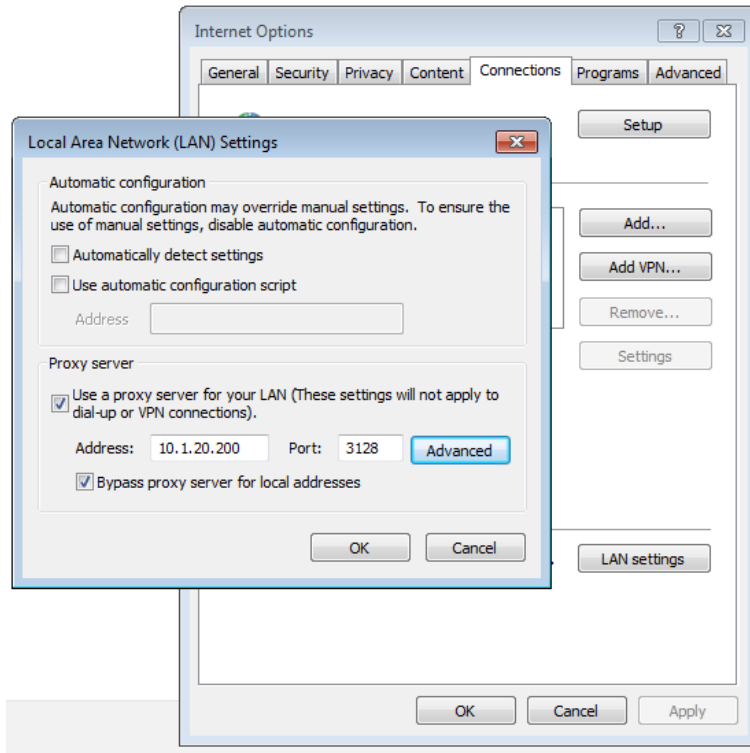
Test 1:

- Open a new Internet Explorer "InPrivate" browser window on your Jump Host client machine
- Browse to **https://www.google.com**
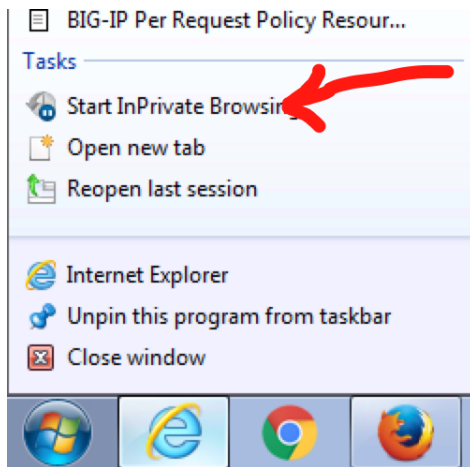
- The browser should prompt you for authentication. Submit your credentials:

  – User: `user1`

  – Password: `AgilityRocks!`

- Verify defined user has an Access Session ID

- Browse to **Access > Overview > Active Sessions**
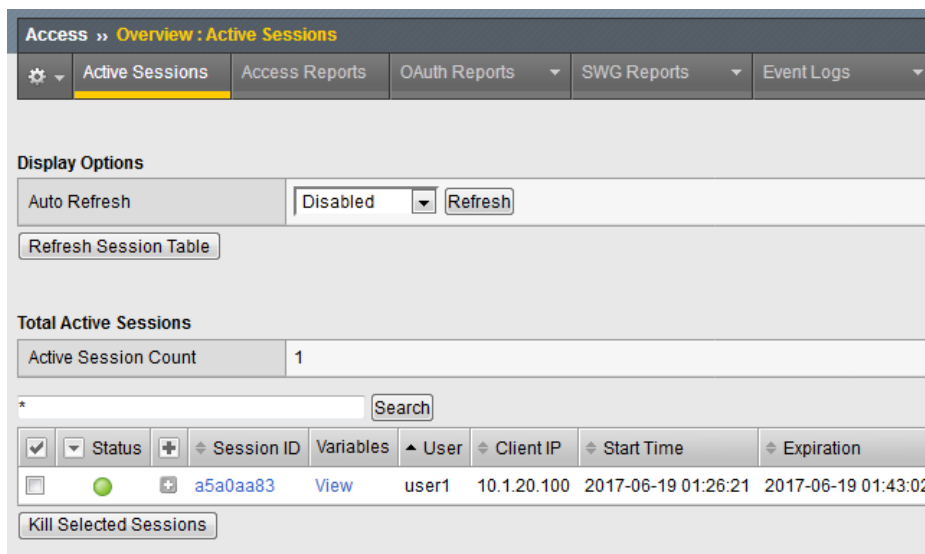
Test 2:

- 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
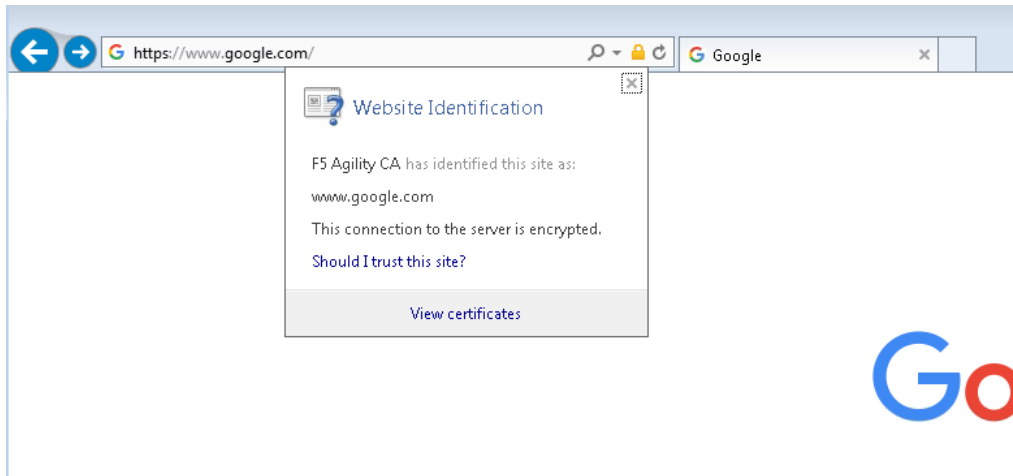
- Using an InPrivate browser window from the client test machine, go to https://www.wellsfargo.com and examine the certificate to verify that it is signed by the same **F5 Agility CA** you configured in Lab 1
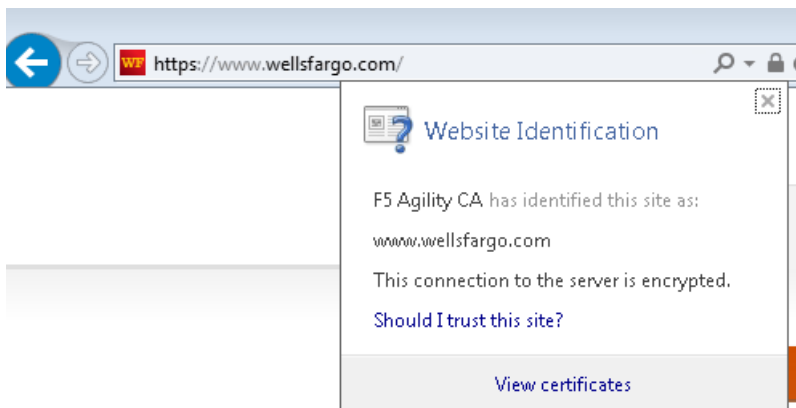
Test 3:

- Using an InPrivate browser window from the client test machine, go to https://www.facebook.com and verify that you are instead delivered a SWG Block Page, in accordance to the URL Filter you configured above.
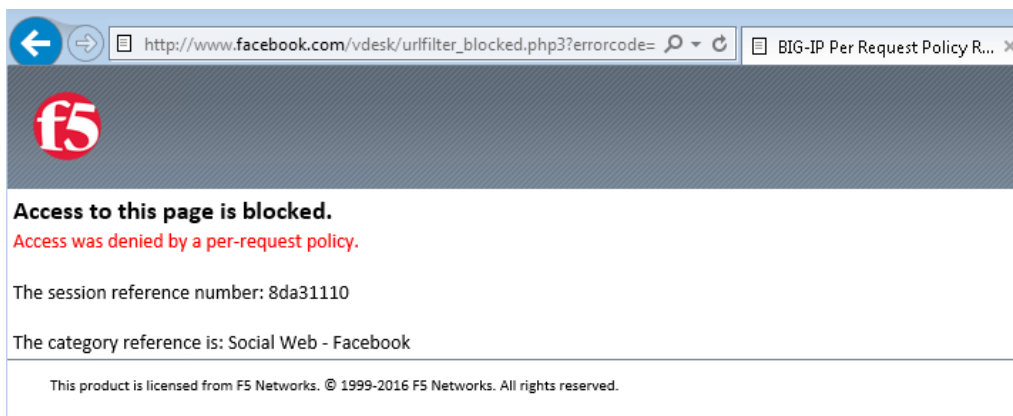
3.3 Lab 2: URL Category-based Decryption Bypass

In this lab exercise, you will bypass SSL decryption based on requests to URLs categorized as financial services web sites.

Estimated completion time: 25 minutes

Objectives:

- Apply a new Per-Request Policy to bypass SSL decryption for specific URL categories
- Test web browsing behavior

Lab Requirements:

- Lab 1 previously completed successfully (working SWG iApp deployment)

3.3.1 Task 1 – Copy and configure new Per-Request Policy

- Copy the **Lab_Per_Request** Per Request Policy by browsing to **Access Policy > Per-Request Policies** and click **Copy**
- Name the copy **Lab_Per_Request_SSL_Bypass**
- Edit the new Per-Request Policy by clicking **Edit**, then go to the VPE tab in your browser
- Modify the Encrypted Category Lookup object to include a branch for SSL Bypass:
- Click on the existing **Category Lookup** object
- On the **Properties** tab, change the name to **Encrypted Category Lookup**
- Click to access the **Branch Rules** tab
- Click **Add Branch Rule** and name it **Banks**
- Click **Change** to modify the Expression of this new Branch Rule
- Click **Add Expression**
- Change **Agent Sel**: to **Category Lookup**
- Change **Category is**: to **Financial Data and Services**
- Click **Add Expression**
- Click **Finished**
- Click **Save**
- Add an **SSL Bypass Set** object (from the General Purpose tab) on the **Banks** branch of the **Encrypted Category Lookup**
- Click **Save**
- Add an **SSL Intercept Set** object (from the General Purpose tab) on the "fallback" branch of the **Encrypted Category Lookup**
- Click **Save**
- Add a **URL Filter** object on the **SSL Bypass** Branch; select the **LAB_URL_FILTER URL** filter previously created in Lab1
- Click **Save**

- Change the **Allow** branch to an ending of **Allow**
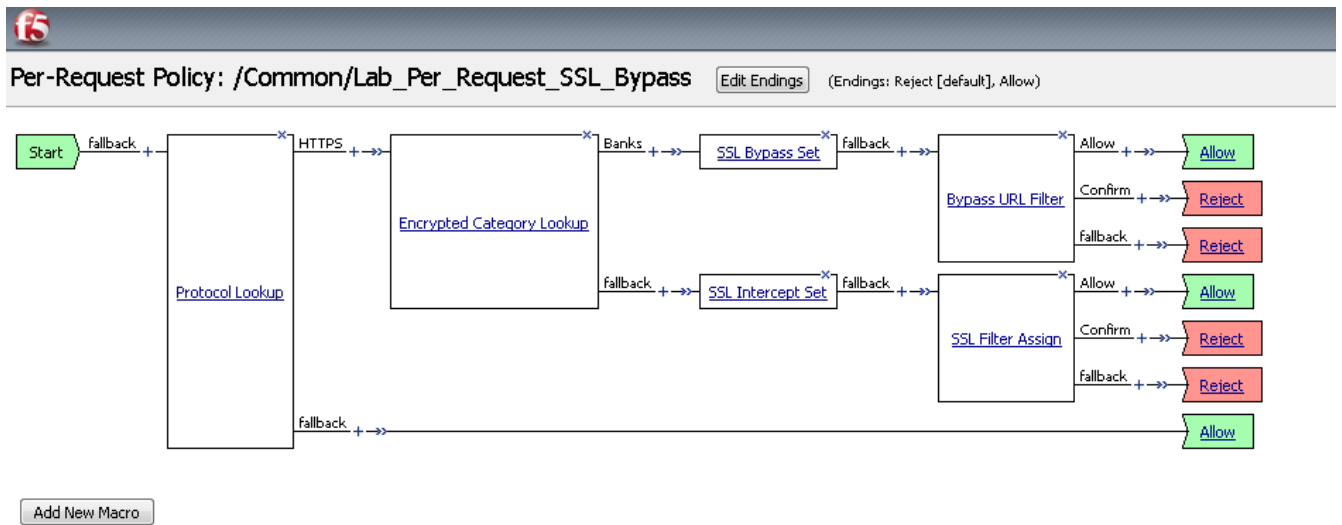
3.3.2 Task 2 – Reconfigure SWG iApp to assign New Per-Request Policy

- Browse to **iApps >> Application Services > Applications"**
- Click on **SWG**
- Click **Reconfigure**
- Find the section **Which Per-Request Access Policy do you want to use?**
- Change the per-request policy to **Lab_Per_Request_SSL_Bypass**
- Scroll to the bottom and click **finished**

3.3.3 Task 3 – Testing

Test 1:

- Open **Internet Explorer** on your Jump Host client machine
- Browse to **http://www.wellsfargo.com**
- The browser should prompt you for authentication. Submit your credentials.
- User: `user1`
- Password: `AgilityRocks!`
- Verify the site loads correctly and inspect the SSL certificate to confirm that it is originated from Wells Fargo and SSL Bypass was enabled
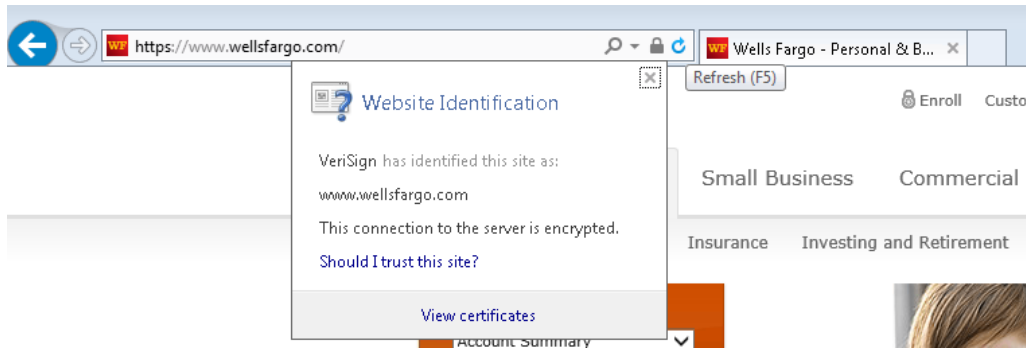
3.4 Lab 3: Explicit Proxy Authentication – NTLM

In this lab exercise, you will reconfigure authentication for seamless login of AD domain-joined client using NTLM.

Estimated completion time: 25 minutes

Objectives:

- Enable APM client-side NTLM authentication for the SWG explicit proxy
- Test web browsing behavior

Lab Requirements:

- Lab 1 previously completed successfully (working SWG iApp deployment)

3.4.1 Task 1 – Logout and log back in as domain user

- Logout of the windows remote desktop.
- Login as a domain user with the following credentials (**Switch User/Other User**):
  - **Username** : `F5DEMO\\user1`
  - **Password:** `AgilityRocks!`

3.4.2 Task 2 – Join BIG-IP to Domain

- Use Firefox to access the **BIG-IP** GUI (https://10.1.1.10, admin/admin)
- Browse to Access ›› Authentication : NTLM : Machine Account
- Click **Create**
- Fill out the fields as follows:
  - **Name:** `agility-ntlm`
  - **Machine account:** `bigip1`
  - **Domain FQDN:** `f5demo.com`
  - **Domain controller FQDN:** `f5demo-dc.f5demo.com`
  - **Admin user:** `admin`
  - **Admin password:** `AgilityRocks!`

- 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**

- Click Finished

3.4.3 Task 3 – Create a new Access Policy

- Browse to **Access >> Profiles / Policies >> Access Profiles (Per-Session Policies)** and click **Create...**
- Name the profile **AP_Explicit_NTLM**
- Change the Profile Type to **SWG-Explicit**

Under Configurations:

Modify **User Identification Method** to **Credentials**

Modify **NTLM Auth Configuration** to **agility-ntlm**

- Add **English** to **Accepted Languages**
- Accept all other default settings and click **Finished**
- Click on the **Edit...** link for the appropriate Access Policy created above
- On the VPE browser tab, select the **+** between Start and Deny and **Add** a **NTLM Auth Result** object (from the Authentication tab)
- Click **Save**
- On the **Successful** branch of the **NTLM Auth Result** Object, click on the **Deny** Ending and change it to **Allow**
- Click **Save**
- Click **Apply Access Policy**
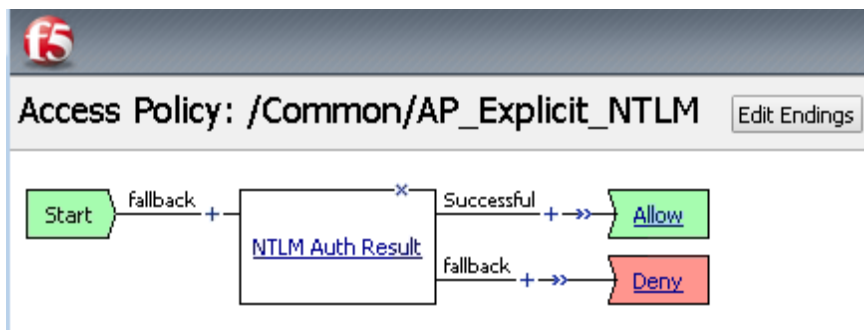
3.4.4 Task 4 – Reconfigure SWG iApp to apply NTLM Access Policy

- Browse to "iApps >> Application Services > Applications
- Click on **SWG**
- Click **Reconfigure**
- Find the section **Which SWG-Explicit Access Policy do you want to use?**
- Change the per-request policy to **AP_Explicit_NTLM**
- Browse to the bottom and click **Finished**

3.4.5 Task 5 – Testing

Before testing, close all browser sessions and kill all session in the GUI under **Access > Overview > Active Sessions**

- Open **Internet Explorer** on your Jump Host client machine

- Browse to https://www.f5.com. The browser should not prompt you for authentication since NTLM authentication is happening in the background (transparent to the user).

- Examine the user session details under **Access > Overview > Active Sessions**. Click on the session ID for details. You can see that NTLM authentication was performed.

3.5 Lab 4: SWG Reporting with BIG-IQ

In this lab exercise, you will explore SWG Reporting with Big-IQ Access.

Estimated completion time: 15 minutes

Objectives:

- View SWG activity reports using BIG-IQ Access

- Test web browsing behavior

Lab Requirements:

- Lab 3 previously completed successfully (working SWG iApp deployment)

3.5.1 Task 1 – Generate New Web Browsing Traffic

- Open Internet Explorer on your Jump Host machine and browse to several web sites, including facebook.com and banking sites to generate reporting data for traffic that is allowed, decrypted, SSL bypassed, and blocked by SWG.

3.5.2 Task 2 – View SWG Reporting Data

- Using Firefox, browse to the BIG-IQ Management GUI **https://10.1.1.30**

- Login with the following credentials:

    Username: **admin**

    Password: **admin**

- Browse to **Monitoring > Dashboards > Access > Secure Web Gateway > Users** to see the activity by users

- Click on **Categories** to view category information,

- Adjust the time period to **30 days or less**
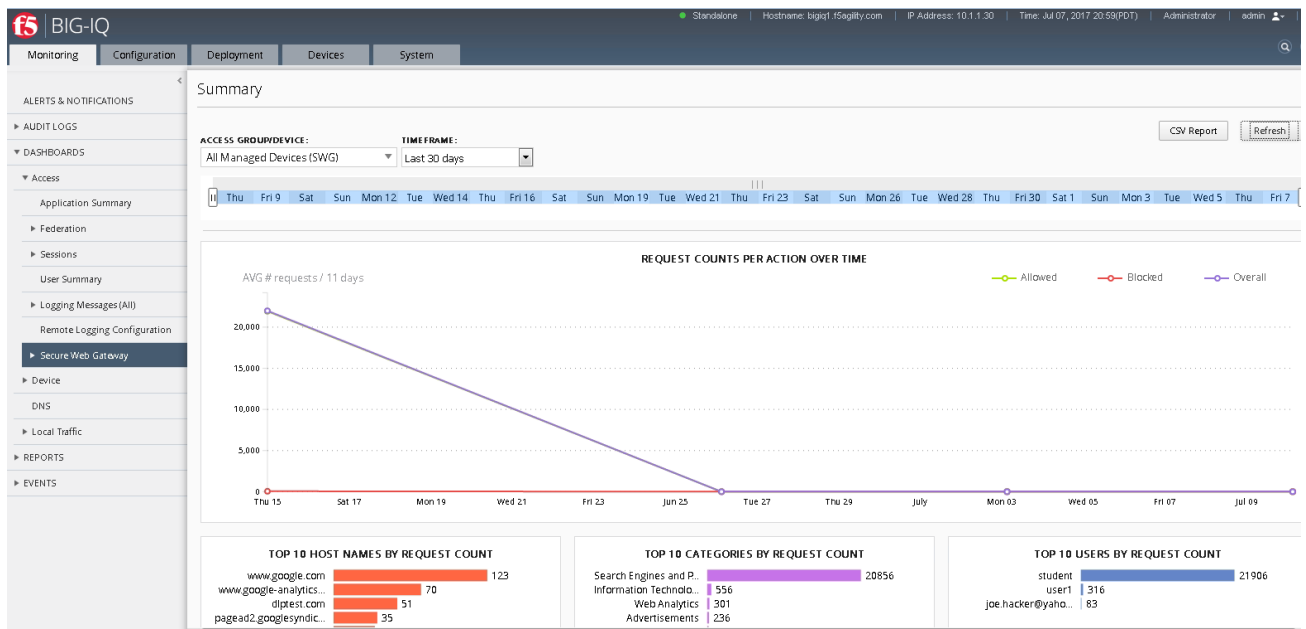
- Click on **SSL Bypass** and view the breakdown between **HTTPS Inspected** and **Bypassed** Content
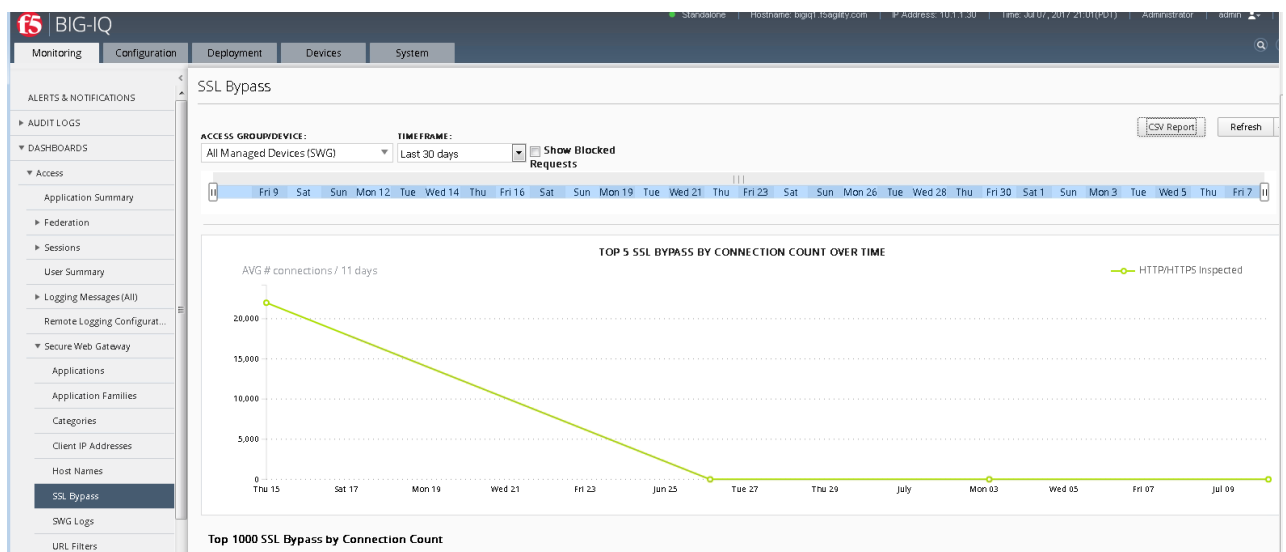
- Click on **Host Name** to look at the hosts your users are accessing
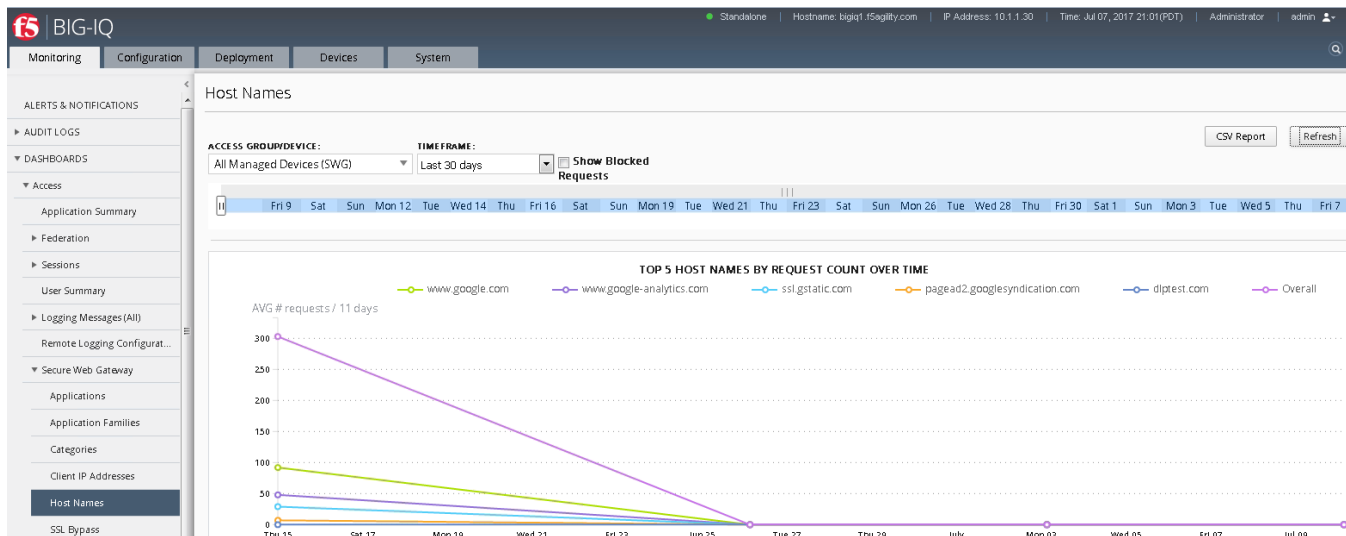
• Click on **URLs** to get detail on what URLs your users are accessing
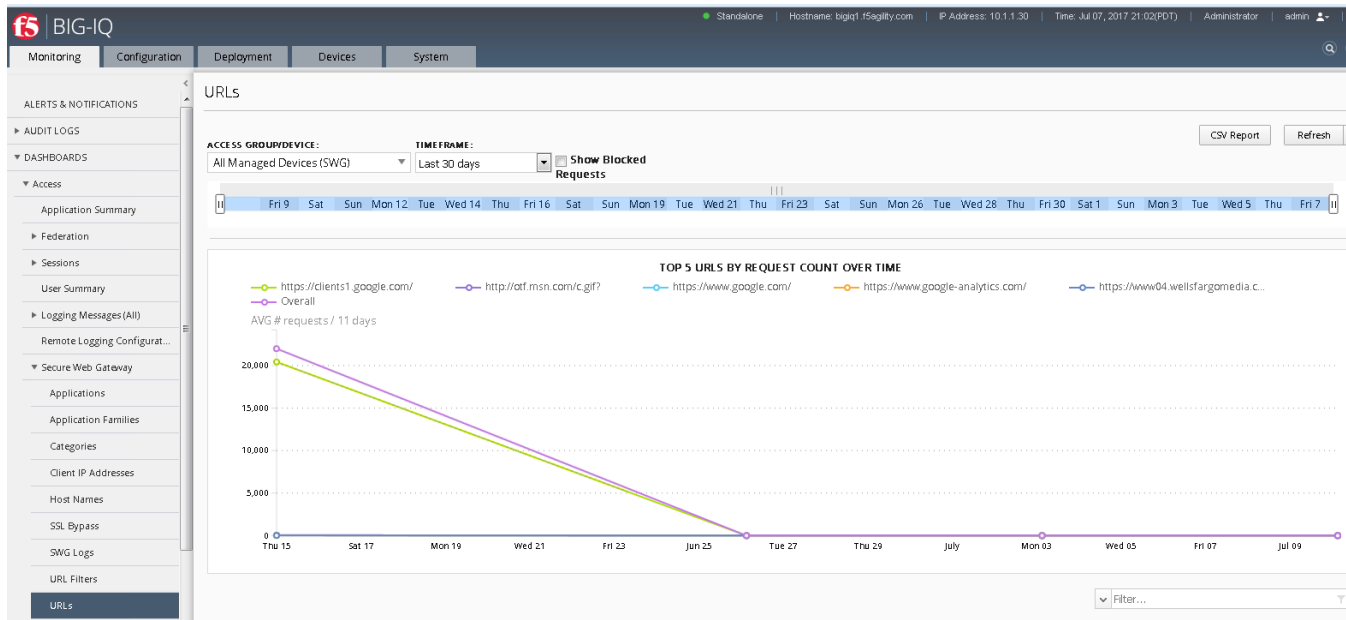
3.6 Lab 5: SWG iApp - Transparent Proxy for HTTP and HTTPS

In this lab exercise, you will configure SWG in transparent proxy mode to support environments where clients do not leverage an explicit proxy. BIG-IP is deployed inline on the client's outbound path to the Internet to intercept the traffic.

Estimated completion time: 15 minutes

Objectives:

• Deploy SWG in transparent proxy mode

• Test web browsing behavior

Lab Requirements:

- Lab 1 previously completed successfully (working SWG iApp deployment)
- BIG-IP must be in path between the client workstation and the Internet (this has already been done for you in this lab)

3.6.1 Task 1 – Create a new Access Policy

- Use Firefox to access the BIG-IP GUI (https://10.1.1.10, admin/admin)
- Browse to **Access >> Profiles / Policies >> Access Profiles (Per-Session Policies)** and click **Create. . .**
- Name the profile **AP_Transparent**
- Change the Profile Type to **SWG-Transparent**
- Add **English** to **Accepted Languages**
- Accept all other default settings and click **Finished**
- Click on the **Edit. . .** link for the appropriate Access Policy created above
- Go to the VPE tab in your browser and on the **fallback** branch, click on the **Deny** Ending and change it to **Allow**
- Click **Save**
- Click **Apply Access Policy**

3.6.2 Task 2 – Reconfigure SWG iApp to apply Transparent Access Policy

- Browse to **iApps >> Application Services > Applications**
- Click on **SWG**
- Click **Reconfigure**
- Change **Configuration Type** to **Transparent Proxy**
- Find the section **Which SWG-Transparent Access Policy do you want to use?**
- Change **Access Policy** to **AP_Transparent**
- Find the section **Which Per-Request Access Policy do you want to use?**
- Change the **per-request policy** to **Lab_Per_Request**
- Set **Should the system translate client addresses** to **Yes. . .**
- Set **Which SNAT mode do you want to use** to **use SNAT Auto Map**
- Browse to the bottom and click **Finished**

3.6.3 Task 3 – Testing

- Open Internet Explorer on your Jump Host client machine
- Ensure Internet Explorer options are configured to ***not*** use an explicit proxy
- Browse to https://www.nhl.com. You should not be prompted for authentication.

3.7 Lab 6: Captive Portal Authentication

In this lab exercise, you will a captive portal to authenticate client connecting to the Internet through the SWG transparent proxy.

Estimated completion time: 25 minutes

Objectives:

- Configure SWG with a Captive Portal to facilitate client authentication
- Test web browsing behavior

Lab Requirements:

- Lab 5 previously completed successfully (working SWG transparent proxy deployment)

3.7.1 Task 1 – Create a new Access Policy

- Use Firefox to access the BIG-IP GUI (https://10.1.1.10, admin/admin)
- Browse to **Access >> Profiles** / **Policies >> Access Profiles (Per-Session Policies)** and click **Create...**
- Name the profile **AP_Transparent_Captive_Portal**
- Change the Profile Type to **SWG-Transparent**
- Change Captive Portals to **Enabled**
- Set Primary Authentication URI to **https://captive.f5demo.com**
- Add **English** to **Accepted Languages**
- Accept all other default settings and click **Finished**
- Click on the **Edit...** link for the appropriate Access Policy created above
- On the VPE browser tab, select the **+** and **Add** a **Message Box** object (from the General Purpose tab)
- For the Message, enter: **Welcome to F5 Agility Guest Wifi Access. Please click the link to accept our terms and access the internet.**
- For the Link enter **Go**
- Click **Save**
- Select the **+** after the message box and **Add** a **Logon Page** object.
- Configure the **Logon Page** as shown below:

- Click **Save**
- Click on the **Deny** ending and change it to **Allow**
- Click **Apply Access Policy**
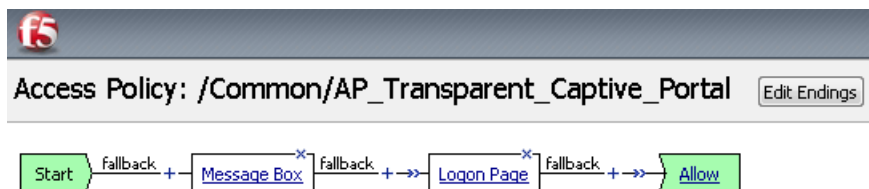
3.7.2 Task 2 – Reconfigure SWG iApp to enable Transparent Capture Portal

- Browse to **iApps >> Application Services** > **Applications**
- Click on **SWG**
- Click **Reconfigure**
- Find the section **Which SWG-Transparent Access Policy do you want to use?**
- Select **AP_Transparent_Captive_Portal**
- Change **Configure the transparent proxy to relay to a Captive Portal** to **Yes, relay to a captive portal**
- Set the **Captive Portal Configuration** as follows:
    - IP Address: **10.1.20.201**

- Port: **443**
  - SSL Certificate: **captive.f5demo.com**
  - SSL Key: **captive.f5demo.com**
- Browse to the bottom and click **Finished**

3.7.3 Task 3 – Testing

- Open Internet Explorer on your Jump Host client machine
- Ensure Internet Explorer options are configured to *NOT* use an explicit proxy
- Browse to **https://www.nhl.com**
- You should be redirected to the capture portal page, prompted to accept the policy by clicking **Go**, then prompted to provide your email address before being allowed through.

3.8 Lab 7: SSL Visibility for DLP (ICAP)

In this lab exercise, you will send decrypted traffic to an ICAP-based Data Loss Prevention (DLP) service for inspection. The DLP will block HTTP POSTs (uploads) of certain content such as credit cards numbers and documents with Top Secret data classification labels.

Estimated completion time: 15 minutes

Objectives:

- Re-configure the SWG iApp to send unencrypted HTTP and decrypted HTTPS traffic to an ICAP (DLP) server
- Verify that the DLP service is able to see SWG proxy traffic and block if a policy violation occurs

Lab Requirements:

- Working SWG iApp deployment

3.8.1 Task 1 – Re-configure SWG iApp to enable ICAP inspection

- Browse to **iApps >> Application Services > Applications**
- Click on **SWG**
- Click **Reconfigure**
- Scroll down to the **ICAP Configuration** section
- Change the ICAP option to **Yes, create a new ICAP DLP deployment**
- Enter **10.1.20.150** as the IP address of the DLP server (the default port of **1344** is correct).

- Browse to the bottom and click **Finished**

3.8.2 Task 2 – Testing

- Open Internet Explorer on your Jump Host client machine
- Browse to **http://dlptest.com**
- If you are prompted for authentication, login as `user1` with password `AgilityRocks!`
- Click on the **HTTP Post** link at the top of the page.
- Fill in the **Subject** and **Message** fields with some random text and then add a credit card numbers such as **4111 1111 1111 1111**.
- Click on the **Submit** button to see if the DLP service detects this. ***Hint:** You should receive a blocking page message.*
- Go back to the previous page try submitting again but with the words **top secret**. Again, you should receive a blocking page from the DLP service.
- Now, go back to the previous page and click on the **HTTPS Post** link at the top of the page.
- Perform the credit card number and **top secret** submissions again. You should again see the blocking pages since SWG is decrypting the HTTPS connection and sending the decrypted POST data to the DLP service for inspection.
- If you want to see the DLP policy violations, browse to **https://10.1.20.150/logs**. Log in as `mydlp` with password `mydlp`.

3.9 Conclusion

3.9.1 Learn More

Links & Information

- **Secure Web Gateway Services Product Info:**

  https://f5.com/products/big-ip/secure-web-gateway-services-swgs

- **SWG Reference Architecture:**

  https://f5.com/solutions/enterprise/reference-architectures/secure-web-gateway

Class 4: SAML Identity Provider (IdP) Lab

This lab covers the following topics:

- Configuring a SAML Identity Provider (IdP)
- Configuring Group-based Access Control

Expected time to complete: **2 hours**

To continue please review the information about the Lab Environment. Additionally, if you are new to the F5 BIG-IP Platform we've created an overview in the BIG-IP Basics section.

4.1 Lab Topology & Environments

All pre-built environments implement the Lab Topology shown below. Please review the topology first, then find the section matching the lab environment you are using for connection instructions.

Using Your Lab Environment

You will be using Ravello for this lab. We will be working with a Linux jumpbox, a BIG-IP Virtual Edition version 13.1, and a simulated SaaS application. We will be using the Linux desktop as our desktop for accessing the applications on the BIG-IP.

This diagram shows the topology of the network as it is currently configured:

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	Management IP	VLAN/IP Address(es)	Credentials
Linux Jumphost	10.1.1.10	**External:** 10.1.10.10	`f5student/f5DEMOs4u`
BIG-IP VE v13.1	10.1.1.245	**External:** 10.1.10.245 **Internal:** 10.1.20.245	`admin/admin` `root/default`
SaaS Application	10.1.1.55	**Internal:** 10.1.20.55	

How to Access the Labs

You will receive instructions from your proctor on how to access the workstation in the lab. On this workstation, you will have the following applications:
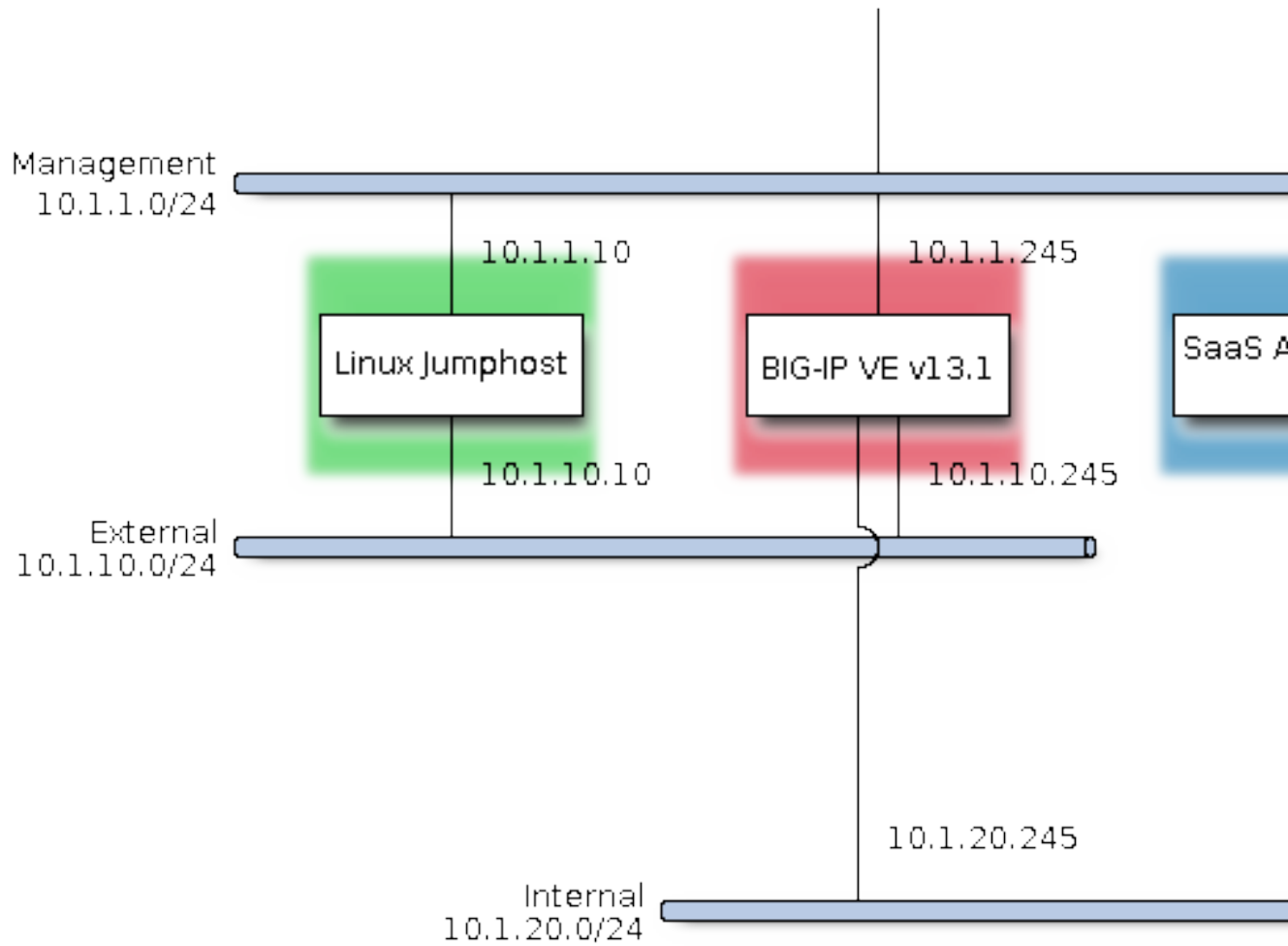
Fig. 4.1: Lab Topology

- Firefox Web Browser – For testing the applications we create and BIG-IP management access. Links are bookmarked just below the address bar.

- Putty SSH Client – For accessing the BASH and TMSH command line of the BIG-IP. The BIG-IP properties have been saved to the session labeled *BIG-IP*.

4.2 BIG-IP Basics (optional)

Just in case you're new to the F5 BIG-IP platform (or need a refresher) we've included some links and videos below that will help get you started.

4.2.1 What is BIG-IP

Source: https://devcentral.f5.com/articles/lightboard-lessons-what-is-big-ip-26793

4.2.2 BIG-IP Basic Nomenclature

Source: https://devcentral.f5.com/articles/lightboard-lessons-big-ip-basic-nomenclature-26144

4.2.3 F5 DevCentral BIG-IP Basics Articles

BIG-IP Basics Articles: https://devcentral.f5.com/articles?tag=devcentral+basics

4.2.4 Using F5 in Various Environments

- Public Cloud:
    - **AWS/Azure/GCP/etc.:** http://clouddocs.f5.com/cloud/public/v1/
- Private Cloud:
    - **OpenStack:** http://clouddocs.f5.com/cloud/openstack/
    - **VMware:** https://f5.com/solutions/technology-alliances/vmware
- Container Ecosystems:
    - **Cloud Foundry:** http://clouddocs.f5.com/containers/latest/cloudfoundry/
    - **Kubernetes:** http://clouddocs.f5.com/containers/latest/kubernetes
    - **Mesos Marathon:** http://clouddocs.f5.com/containers/latest/marathon
    - **RedHat OpenShift:** http://clouddocs.f5.com/containers/latest/openshift/

4.2.5 HA Proxy to BIG-IP Quick Start

If you're already familiar with HA Proxy, learning F5 BIG-IP is straightforward once you learn the associated F5 terminology.

Here is a list of common HA Proxy configuration terminology and its F5 equivalent:

HA Proxy	F5 BIG-IP
Frontend	Virtual Server (VIP)
Backend	Pool
Server	Member
mode http	HTTP Profile
default_backend	Default pool
use_backend	LTM policy
check port	Health monitor

4.2.6 NGINX to BIG-IP Quick Start

If you are already familiar with NGINX, learning F5 BIG-IP will be straightforward once you learn the F5 terminology.

NGINX administrators usually use multiple files and leverage the include command in their config to break down the config and make it easier to manage. F5 leverages *Profiles* which can be applied to a *Virtual Server*.

NGINX uses in-band (passive) health monitors which can be enabled on F5 through the creation of an *inband monitor*. BIG-IP also supports the use of active health monitors, which will poll the pool member periodically. Both can be used together for better monitoring of your services.

F5 BIG-IP supports control-plane and data-plane programmability with:

- Node.js through the use of iRulesLX, iControlLX and iAppsLX
- TCL through the use of iRules and iApp Templates

A lot of the manual configuration and scripting steps that are required with NGINX are supported more easily through various config parameters and profiles in BIG-IP. By leveraging the control-plane programmability features this class covers you can achieve full automation of your services with the BIG-IP platform.

F5 BIG-IP is designed to be a full proxy by default. In most cases there is no need to tune TCP & HTTP buffering like you would on NGINX (i.e. using `proxy_buffering`). This is because the default settings have been optimized and can adapt to most situations.

Here is a list of common NGINX configuration terminology and its F5 equivalent:

NGINX	F5 BIG-IP
listen	Virtual Server Port (VIP)
upstream	Pool
proxy_pass	Default Pool
server	Member
ssl_certificate	SSL Profile Option
return	LTM HTTP Policy Option
proxy_set_header X Forwarded For	HTTP Profile Option Insert X-Forwarded-For
proxy_set_header	LTM HTTP Policy Option
add_header	LTM HTTP Policy Option
location & proxy_pass	LTM HTTP Policy Option
Proxy Cache	Web Acceleration Policy

4.3 Module 1: SAML Identity Provider

In this lab we will learn the basics concepts required to use F5 Access Policy Manager as a SAML Identity Provider (IdP).

4.3.1 Lab 1.1: Create a SAML Identity Provider
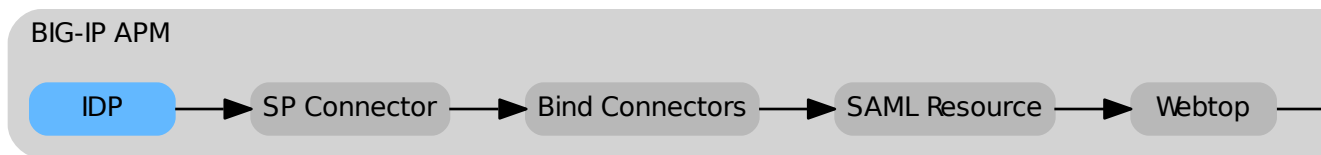
Task 1 - Create a Local IdP Service

In this lab we will create the local Identity Provider service. This service is responsbile for handling the authentication for the SaaS application.

Note: This guide may require you to Copy/Paste information from the guide to your jumphost. To make this easier you can open a copy of the guide by using the **Lab Guide** bookmark in Chrome.

---

1. Navigate to *Access → Federation → SAML Identity Provider → Local IdP Services*
2. Click the *+* sign
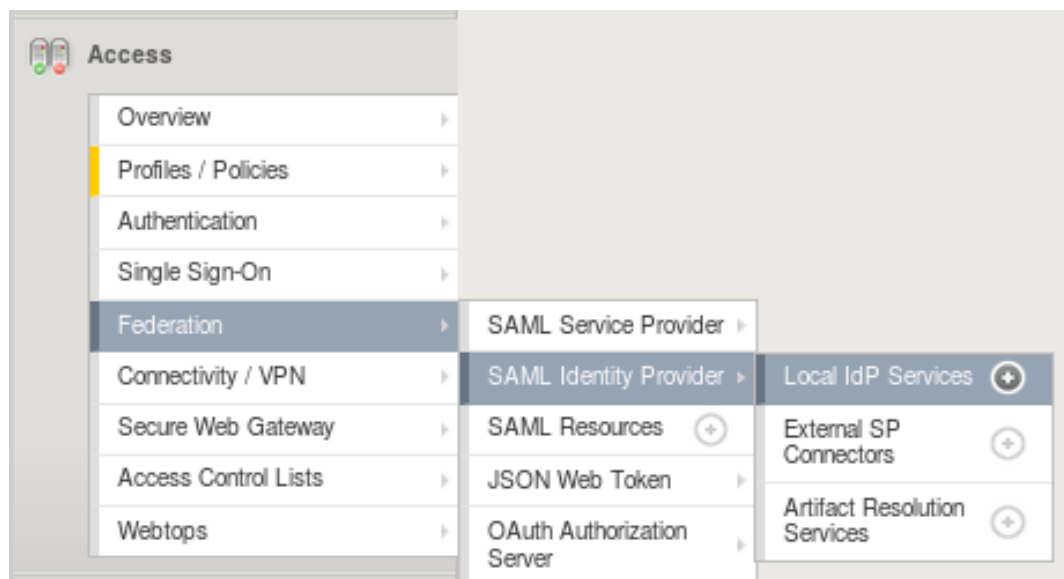
3. Configure the *General Settings*:

Property	Value
IdP Service Name	idp.f5demo.com
IdP Entity Id	https://idp.f5demo.com

4. Configure the *Assertiion Settings*:

Property	Value
Assertion Subject Value	%{session.logon.last.username}

5. Configure the *Security Settings*:

Property	Value
Signing Key	idp.f5demo.com.key
Signing Certificate	idp.f5demo.com.crt

6. Click the *OK* button.

4.3.2 Lab 1.2: Create an External SP Connector
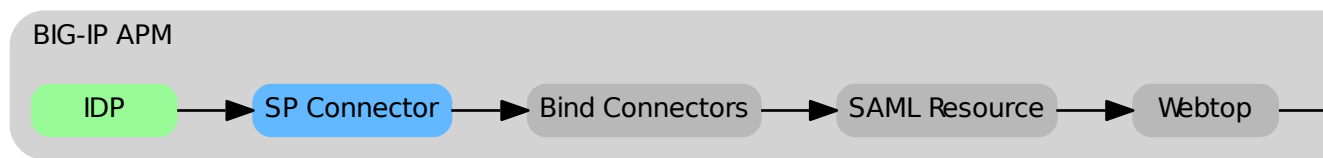
Now that we have the Identity Provider configured, we need to configure the BIG-IP so it is aware of the Service Provider (the SaaS application). We do this by defining an External SP Connector using the metadata provided by the SaaS application, importing it into the BIG-IP, and setting the appropriate cryptographic controls.

Task 1 - Obtain the SAML Service Provider Metadata

In a common deployment the metadata is provided by the application. This lab is no different, but the access method will vary. Follow the listed steps below to obtain the necessary XML file.

1. Open a browser and nagivate to https://app.f5demo.com/metadata.xml

2. Save the file as `app.f5demo.com.xml`

Task 2 - Create an External SP Connector

In this task we will create the External SP Connector object.

1. Navigate to *Access → Federation → SAML Identity Provider → External SP Connector*

2. Click on the triangle on the right side of the *Create* button and select *From Metadata*
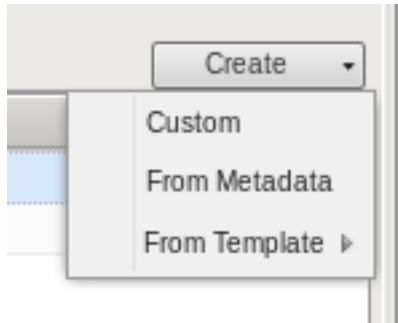
3. Enter the following information:

Property	Value
Select File	app.f5demo.com.xml
Service Provider Name	app.f5demo.com

4. Click the *OK* button

Task 3 - Modify the SP Connector Settings

Finally, for security purposes, we'll configure the External SP Connector object to require that resposes are cryptographically signed. This prevents an attacker from manipulating the response and potentially gaining unauthorized access.

1. Click the checkbox next to *app.f5demo.com* and click the *Edit* button

2. Modify the following *Security Settings*:

Property	Value
Response must be signed	checked

3. Click the *OK* button.

4.3.3 Lab 1.3: Bind SP Connectors
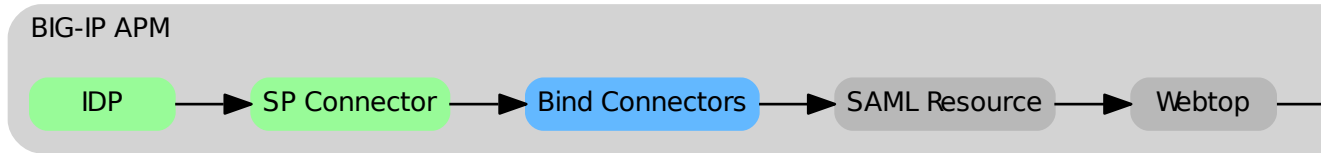
Once we have the Identity Provider and Service Provider objects configured, we need to link them together.

Task 1 - Bind the IdP and SP Connector

1. Navigate to *Access → Federation → SAML Identity Provider → Local IdP Services*
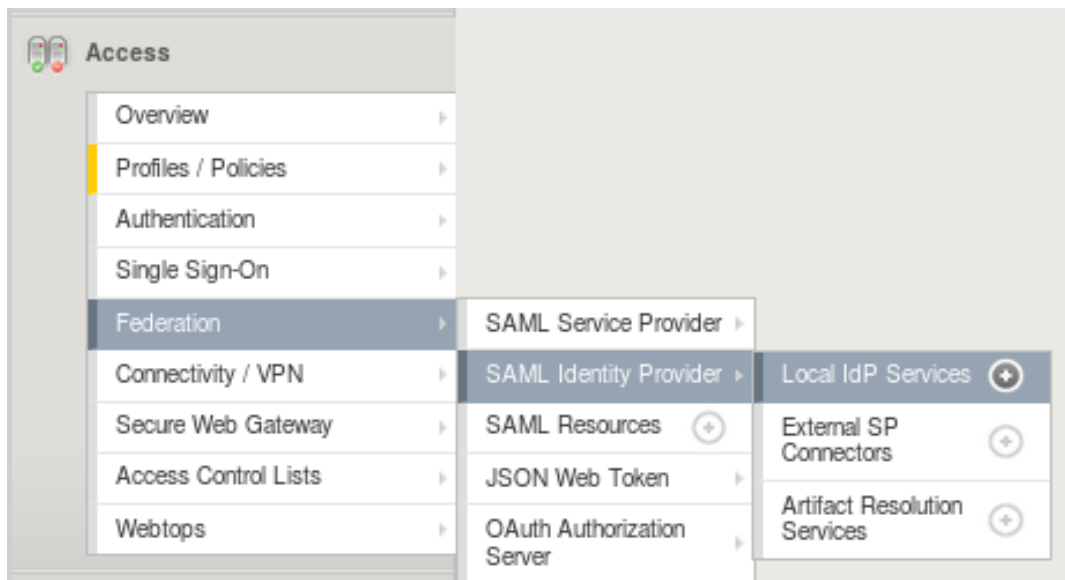
2. Check the radio button next to *idp.f5.demo.com*
3. Click on the *Bind/Unbind SP Connectors* button
4. Check the box next to */Common/app.f5demo.com*
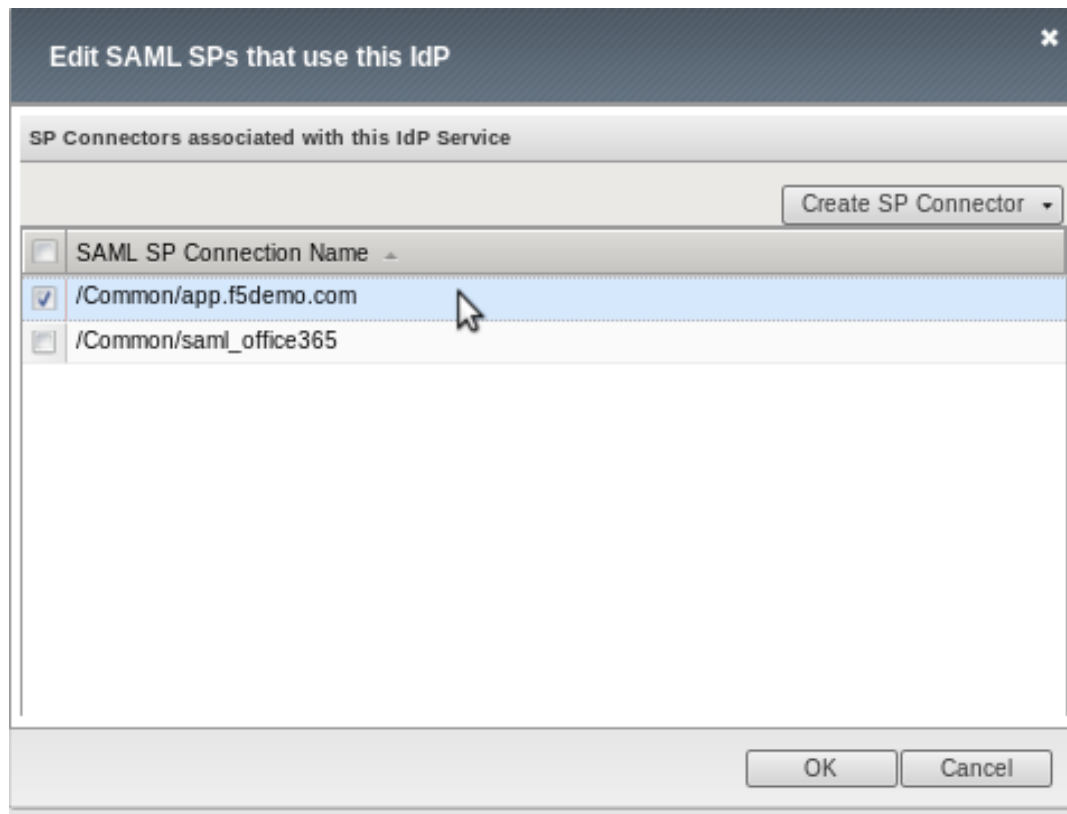
5. Click the *OK* button.

4.3.4 Lab 1.4: Create SAML Resource
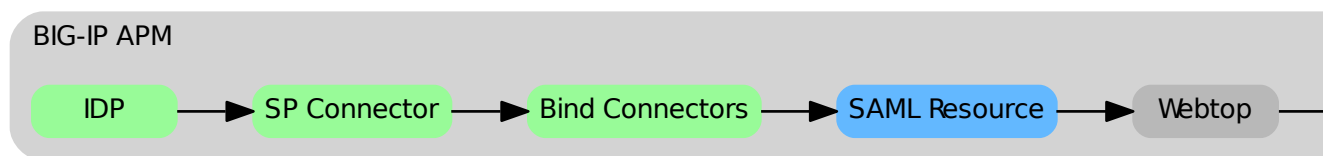
Task 1 - Create SAML Resource

1. Navigate to *Access* → *Federation* → *SAML Resource* and click the *+* sign
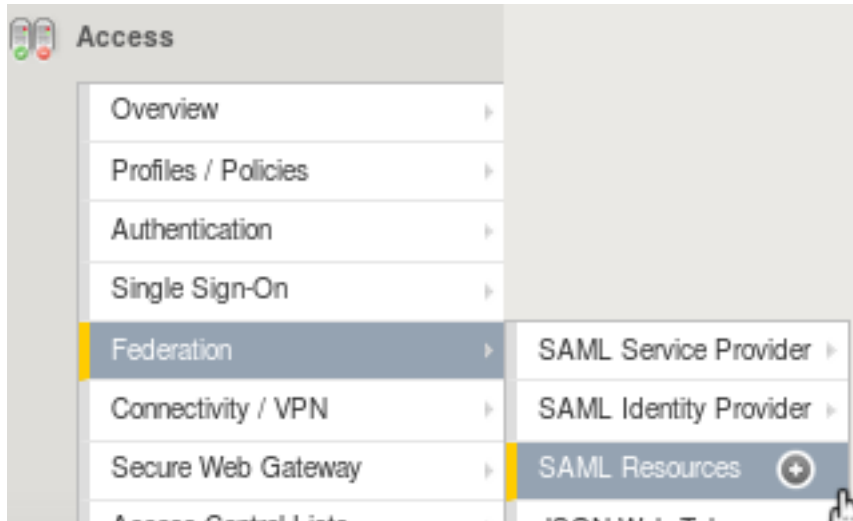
2. Configure the following settings:

Property	Value
Name	app.f5demo.com
SSO Configuration	idp.f5demo.com
Caption	app

3. Click the *Finished* button.

4.3.5 Lab 1.5: Create a Webtop
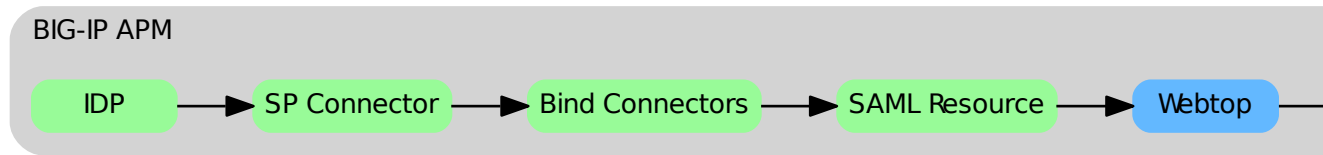
Task 1 - Create the SAML Webtop

1. Navigate to *Access → Webtops → Webtop Lists*
2. Click the *+* sign
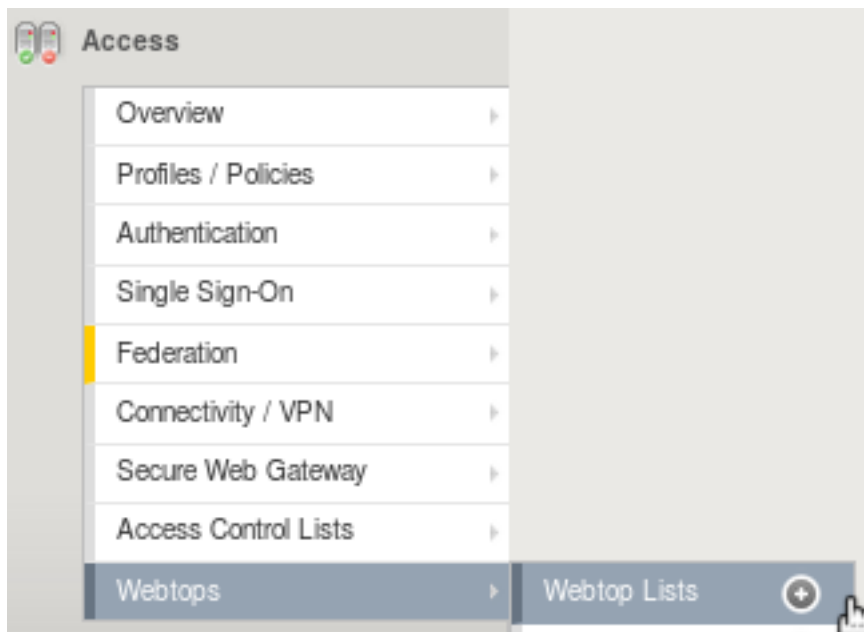
3. Configure the following settings:

Property	Value
Name	saml_webtop
Type	full

3. Click the *Finished* button.

4.3.6 Lab 1.6: Configure the Access Profile
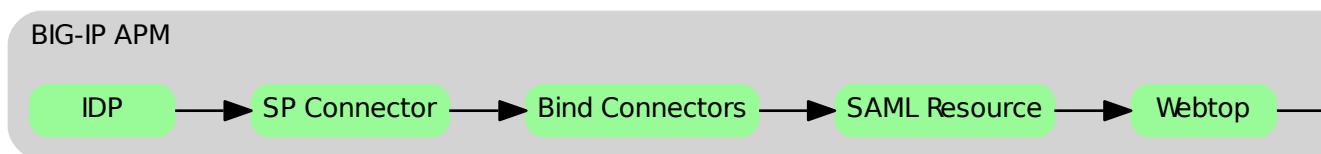
The Access Profile defines the characteristics of how we authenticate and authorize a user using the BIG-IP platform. It controls things like what type logon page is presented to the user (if any at all), what language any dialog messages should be presented in, and – most importantly – the flow through which we limit access and assign resources.

F5 BIG-IP Access Policy Manager supports two types of Access Policies:

1. Per-Session access policies

2. Per-Request access policies

The difference centers around how frequently a policy is evaluated, either once at time of initial logon or after every single HTTP request.

Task 1 - Create the Access Profile Object

1. Navigate to *Access → Profiles/Policies → Access Profiles (Per-Session Policies)*

2. Click the *+* sign

3. Configure the following settings:

Property	Value
Name	idp.f5demo.com-policy
Profile Type	All
Languages	English (en)

4. Click the *Finished* button.

Task 2 - Configure the Access Policy Using the Visual Policy Editor

The Visual Policy Editor (VPE) is where the administrator configures the heart of the Access Policy. Using a flow chart methodology, it is easy to create robust policies without adding burdensome management overhead. Even significant policies can be easily read and understood.

1. **Open the Visual Policy Editor**

   (a) Navigate to *Access → Profiles/Policies → Access Profiles (Per-Session Policies)*

   (b) Click the *Edit...* link and the VPE will open in a new window
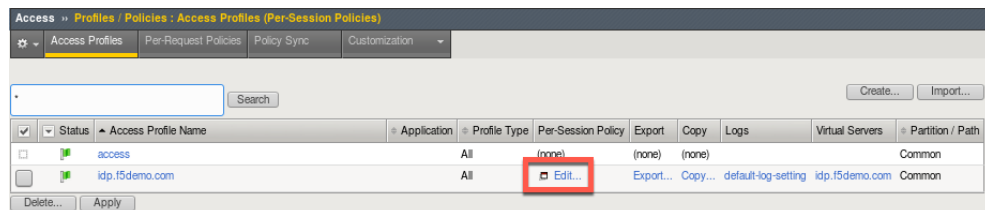
   We'll build a policy like the one below:
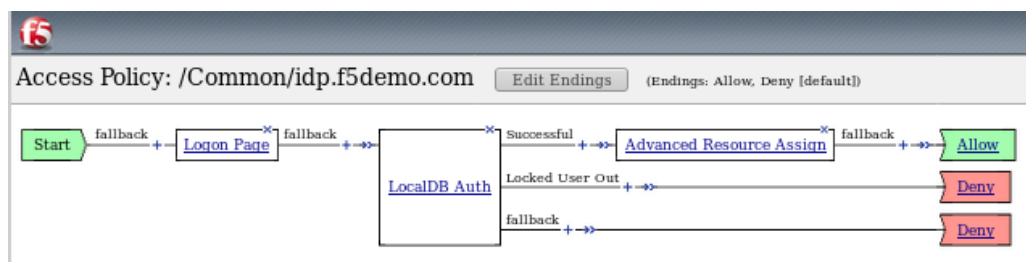
2. **Add a Logon Page**

   (a) Click on the *+* link after the *Start* node

   (b) Select the *Logon Page* tab and click the *Add Item* button

   (c) Use the default settings and click the *Save* button

3. **Add an Authentication Mechanism**

   (a) Click on the *+* link after the *Logon Page* node

   (b) Select the *Authentication* tab and select *LocalDB Auth* then click the *Add Item* button

(c) Configure the following settings:

Property	Value
LocalDB Instance	/Common/agility

Note: The administrator can select from a variety of Authentication Mechanisms, in-cluding Active Directory and LDAP, among others. In this lab, the *LocalDB Auth* has been pre-configured.

(a) Click the *Save* button.

4. **Add Advanced Resource Assign**

   (a) Click on the *+* link on the successful branch after the *LocalDB Auth* node

   (b) Select the *Assignment* tab and select *Advanced Resource Assign* then click the *Add Item* button

   (c) Click the *Add New Entry* button

   (d) Click the *Add/Delete* link

   (e) Select the *Webtop* tab and select the */Common/saml_webtop*

   (f) Select the *SAML* tab and select the */Common/app.f5demo.com*

   (g) Click the *Update* button, then click the *Save* button

5. **Change the ending to Allow**

    (a) Click on the *Deny* ending after the *Advanced Resource Assign*

    (b) Select *Allow*

    (c) Click *Save*

6. **Apply Policy Changes**

    (a) Click the *Apply Access Policy* in top left next to the F5 red ball

    (b) Close browser tab

4.3.7 Lab 1.7: Create the Virtual Server
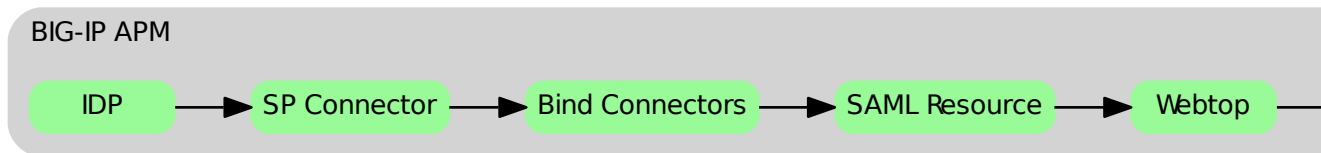
In order to access almost anything through an F5 BIG-IP, you must define a Virtual Server. The Virtual Server listens on the specified address and handles the requests either by making a load balancing decision or prompting for a logon (or both!).

Task 1 - Create the Virtual Server

1. Navigate to *Local Traffic → Virtual Server List*

2. Click the *+* sign
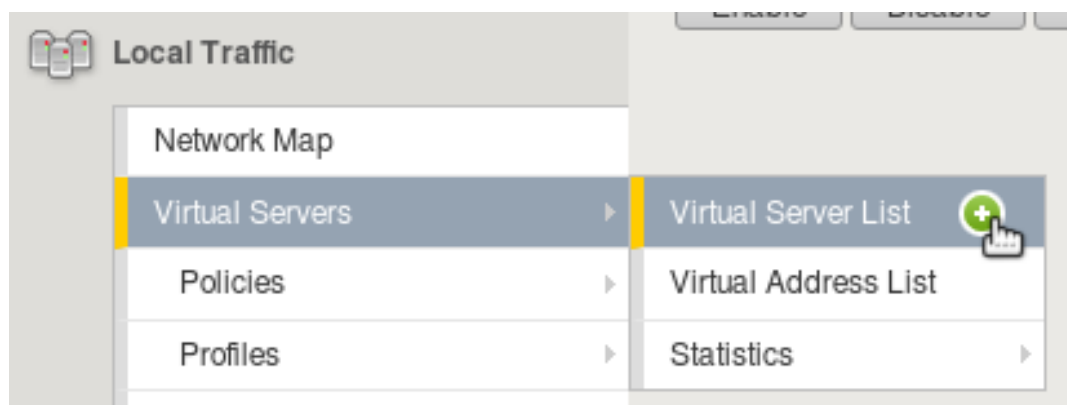
2. Configure the *General Properties* settings:

General Properties	
Property	Value
Name	idp.f5demo.com
Destination Address/Mask	10.1.10.101
Service Port	443

General Properties

Name	idp.f5demo.com
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.1.10.101
Service Port	443 Select...
Notify Status to Virtual Address	✔
State	Enabled

3. Configure the *Configuration* settings:

Configuration	
Property	Value
HTTP Profile	http
SSL Profile (Client)	idp.f5demo.com-clientssl
SSL Profile (Server)	serverssl

Configuration:	Basic
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	Selected /Common idp.f5demo.com-clientssl
SSL Profile (Server)	Selected /Common serverssl
SMTPS Profile	None

4. Configure the *Access Policy* settings:

Access Policy	
Property	Value
Access Profile	idp.f5demo.com

5. Click the *Finished* button.

4.3.8 Lab 1.8: Test the SAML Configuration
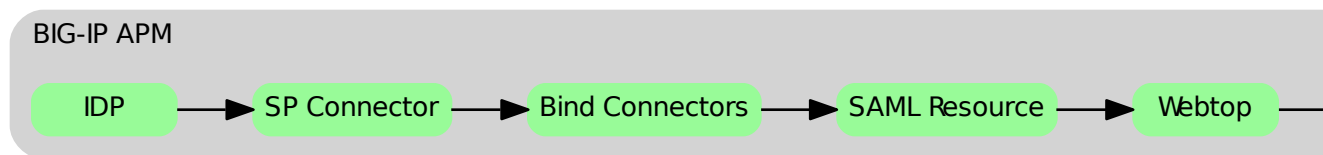
Now that we have all the pieces configured, the only thing left is to test and validate our setup to make sure it's working as expected.

Task 1 - Test SAML IdP

1. Open Chromium and navigate to https://app.f5demo.com

2. Notice how we've been redirected to the authentication page at https://...

3. Login with the test credentials below:

Username	Password
alice	agility

4. You should now see a demo application. If not, please step back through the configuration and make sure you did not mistype one of the settings
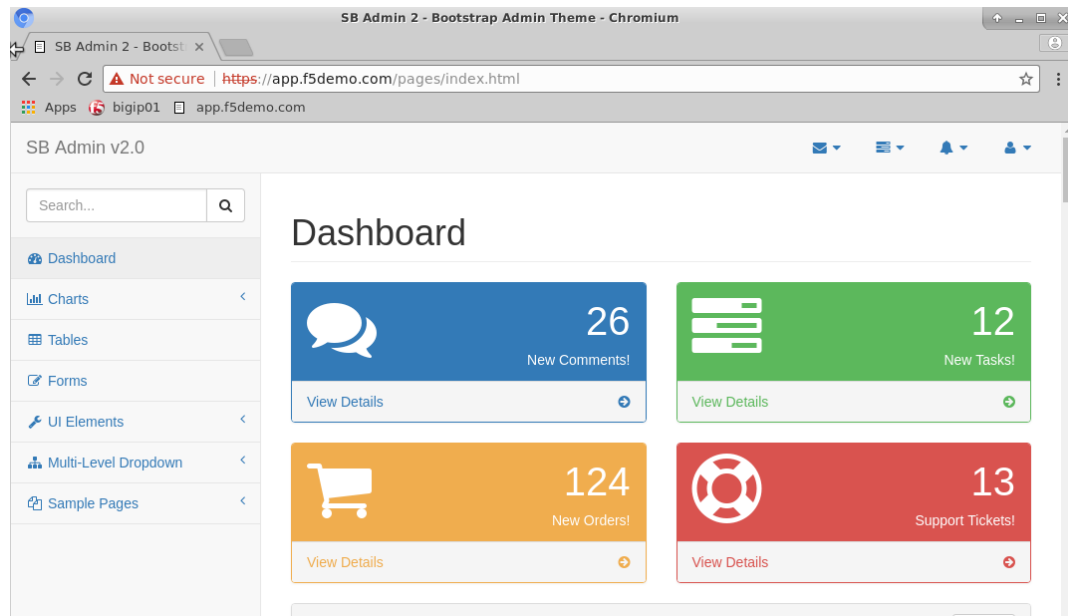
5. Close the Chromium browser

4.4 Module 2: Access Control

In this lab we will limit access to SaaS resources based on group membership.

4.4.1 Lab 2.1: Modify the Access Profile

Task 1 - Launching the Visual Policy Editor

1. Navigate to *Access → Profiles/Policies → Access Profiles (Per-Session Policies)*
2. Click the *Edit. . .* link
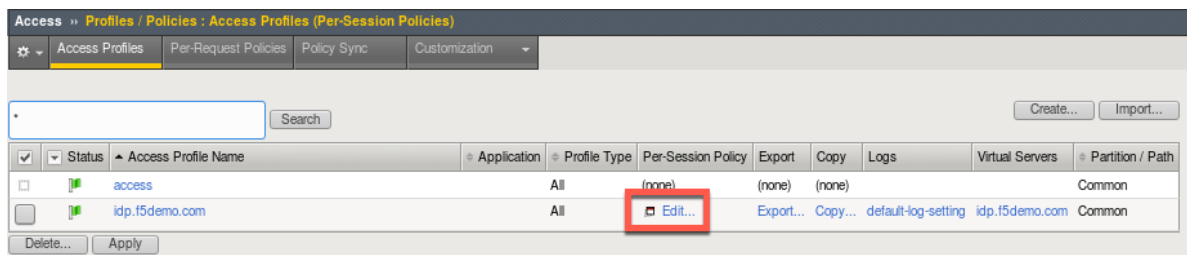
Task 2 - Add a LocalDB Query

1. Click on the *+* sign after *LocalDB Auth* on the *Successful* branch
2. In the search field type *local*
3. Select *Local Database* and click the *Add Item* button

4. Configure the following settings:

Property	Value
LocalDB Instance	/Common/Agility

5. Click the *Add new entry button*

6. Configure the following settings:

Property	Value
Action	read
Destination	session.localdb.groups
Source	groups

7. Click the *Save* button

Task 3 - Modify the Advance Resource Assignment

1. Click on *Advance Resource Assign*

2. Click on the *change* link

3. Click the *Add Expression* button

4. Configure the following settings:

Property	Value
Agent Sel	LocalDB Group Check
Condition	LocalDB Query
User is a member of	Sales

5. Click the *Add Expression* button

6. Click the *Finished* button

7. Click the *Save* button

8. Click the *Apply Access Policy* link in top left next to the F5 red ball

4.4.2 Lab 2.2: Test Access Control

Now that you have your IdP configured we need to test it to make sure it is working as expected.

Task 1 - Test with an Authorized User

1. Open Chromium and navigate to https://app.f5demo.com

2. Login with the test credentials

Username	Password
alice	agility

3. You should now see a demo application.
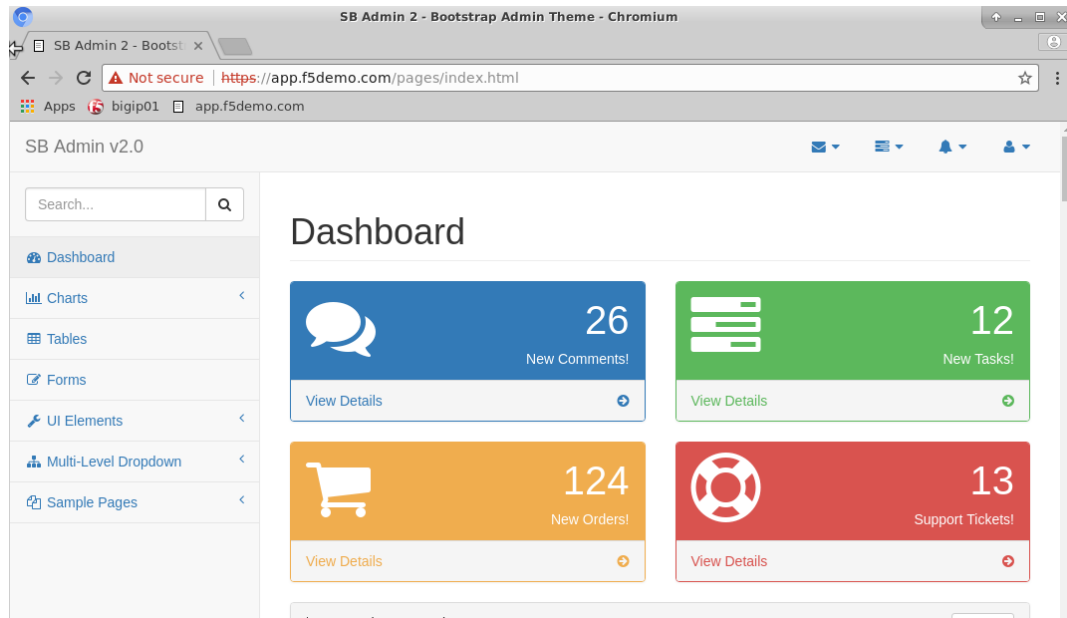
4. Click the user icon in the top right of the app and logout

Task 2 - Test with an Unauthorized User

1. Navigate to https://app.f5demo.com (you can click the bookmark)

2. Login with the test credentials

Username	Password
john	agility

3. You should now see an error page since John is not a member of the sales group
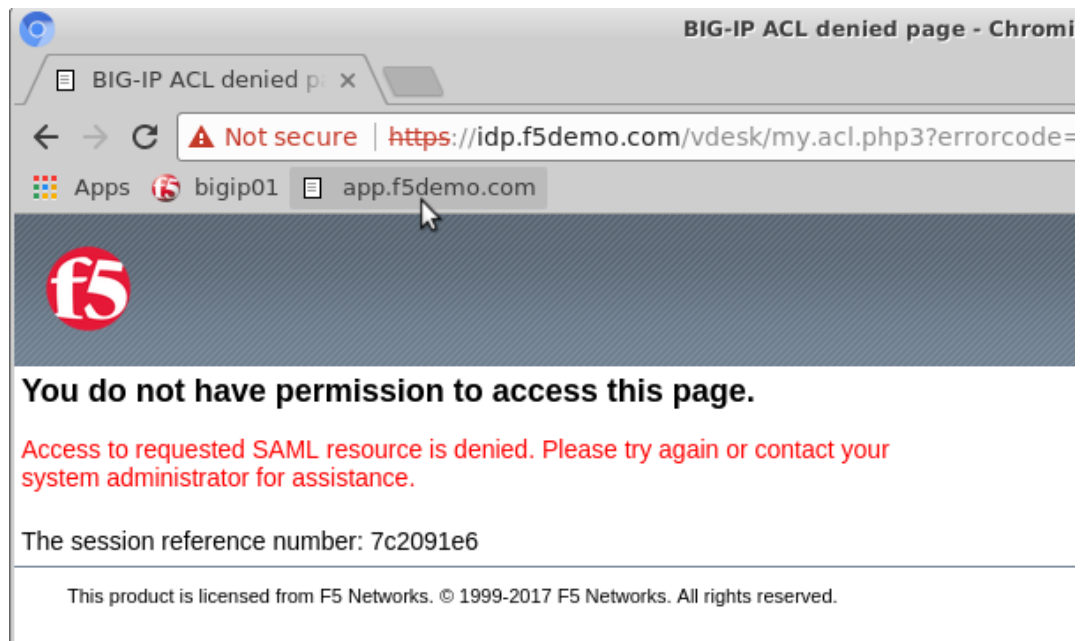
8. Close the Chromium browser

Class 5: AD FS Proxy Lab

This lab covers the following topics:

- Configuring AD FS Proxy Services on F5 BIG-IP

Expected time to complete: **2 hours**

To continue please review the information about the Lab Environment.

5.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

Note: All work for this lab can be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

5.1.1 Lab Topology

The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE (v13.1)
- 5 x Windows Server 2016

Lab Components

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials	Notes
BIGIP	• **Management:** 10.1.1.4 • **Internal:** 10.1.20.4 • **External:** 10.1.10.4 • **ADFS Proxy Virtual Server IP:** 10.1.10.100 • **ADFS Load Balancing Virtual Server IP:** 10.1.20.100	• `admin/admin` • `root/default`	Licensed with Best bundle, provisioned with LTM and APM. BIG-IP Version 13.1.
Client	• **Internal** 10.1.20.8	`user/user`	This is the client/jumphost used in the lab, it is domain joined. Windows Server 2016.
DC	• **Internal** 10.1.20.5	`admin/admin`	This is the domain controller and certificate authority. Windows Server 2016.
App	• **Internal** 10.1.20.10	`admin/admin`	Runs IIS with a claims app that is federated to ADFS. Windows Server 2016.
ADFS-1	• **Internal** 10.1.20.6	`admin/admin`	Primary ADFS farm node. Windows Server 2016.
ADFS-2	• **Internal** 10.1.20.7	`admin/admin`	Secondary ADFS farm node. Windows Server 2016.

5.2 Module: Connect and Validate Environment

In this module you will validate that ADFS and the application that requests ADFS authentication are functioning without the BIG-IP in the traffic flow.

5.2.1 Open an RDP session to the client machine

1. Open an RDP session to the client jumphost

2. Login with username: user and password: user

5.2.2 Change Client to Point at ADFS-1 Direct (BIG-IP not in traffic flow)

1. Double click the "ADFS-1 Direct" desktop shortcut
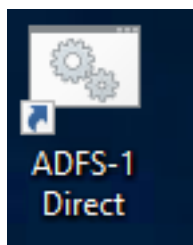
2. You should receive a notification that the HOSTS file now points adfs.vlab.f5demo.com directly at the ADFS-1 server.

Message from user 5/25/2018 5:42 PM   ✕

HOSTS file now points adfs.vlab.f5demo.com directly at ADFS-1, BIG-IP is out of
the traffic flow.

OK

5.2.3 Open the BIG-IP Management Interface

1. Open Chrome

2. Click the BIG-IP shortcut

3. Login with username: admin and password: admin

4. Nothing needs to be done here now, you are only validating you can access the BIG-IP.

5.2.4 Verify ADFS and App are Functional

1. Close any open Chrome incognito windows

2. Open Chrome if not already open

3. Right click the "ADFS Demo App" shortcut and click "open in incognito window"

VERY IMPORTANT: For all testing in this lab, close all incognito windows first, then open a new one for your test. This will ensure you do not have issues related to cache or cookies.

4. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

If the request failed and you do not see claims then the ADFS-1 Windows server may not have started correctly or

Option 1: You can restart services on the ADFS servers from your client with the shortcut on the desktop. This is the fastest option.
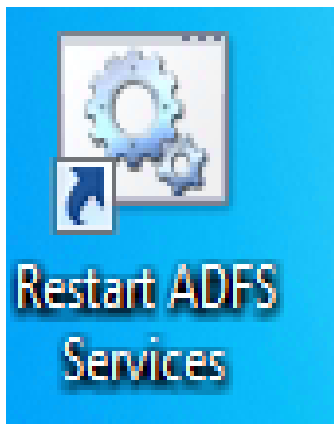
Option 2: You can restart the ADFS-1 and then ADFS-2 servers. This is much slower.

You should now see the following:

Welcome!

These are your claims:

Type	
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	true
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5dem
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.20.8
http://schemas.microsoft.com/claims/authnmethodsproviders	WindowsAu
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schem

5. Note that ADFS identified the user as inside the corporate network because they did not go through an MS-ADFSPIP compliant proxy.

6. What happened:

    (a) You made a request to App

    (b) App redirected you to ADFS for authentication

    (c) ADFS authenticated you automatically with Windows Integrated Authentication with your domain joined computer

    (d) ADFS redirected you back to App with a WS-Fed assertion

    (e) App validated the assertion and displayed the claims it received from ADFS

You should close all browser windows in the client and repeat these steps to validate ADFS-2 using the desktop shortcut labeled "ADFS-2 Direct". If it fails, use the desktop shortcut to restart ADFS services as noted above.

5.3 Module: Deploy ADFS Load Balancing Services

In this module you will deploy simple load balancing of ADFS for internal users. No proxy services are needed for internal users.

5.3.1 Change Client to Point at BIG-IP Load Balancing Virtual Server

1. Double click the BIG-IP ADFS Load Balancer desktop shortcut
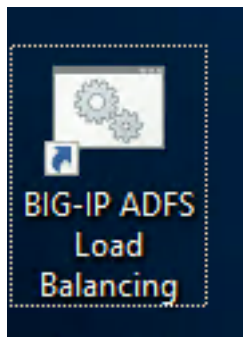
2. You should see that the HOSTS file now points ADFS at the load balancing virtual server (which is not yet created)

Message from user 5/25/2018 5:47 PM   ✕

HOSTS file now points adfs.vlab.f5demo.com at the ADFS load balancing Virtual
Server, like an internal client.

OK

3. Close any open Chrome incognito windows

4. Open a new Chrome window if not already open.

5. Right click the "ADFS Demo App shortcut" and open a new incognito window

   (a) It should fail because you cannot access ADFS through the BIG-IP until you deploy the configuration.

   (b) If it is still working, you may need to close Chrome and/or retry the HOSTS file shortcut.

5.3.2 Deploy ADFS iApp for ADFS Load Balancing

1. Open the BIG-IP configuration interface

2. Open Local Traffic -> Virtual Servers and notice nothing is deployed

3. Open iApps -> Application Services -> Applications

4. Click Create

Accept all default values except for those listed below.

5. **Name**: **adfs-lb**

6. **Template**: **f5.microsoft_adfs.v1.2.0rc7**

7. **SSL Encryption**

   (a) **How should the BIG-IP system handle SSL traffic?**

       i. **Encrypted traffic is forwarded without decryption (SSL pass-through)**

SSL Pass-Through is chosen because Microsoft requires it for supported load balancing of ADFS. SSL Bridging breaks the connectivity between WAP servers and ADFS servers because client certificate authentication is required. You can use SSL Bridging if you will not point WAP servers at your deployment but following Microsoft's guidelines and using SSL Pass-Through is recommended.

8. **High Availability**

   (a) **What IP address do you want to use for the virtual server?**

       i. **10.1.20.100**

10.1.20.x is the internal network in this environment.

1. **Which FQDN will clients use to access AD FS?**

   (a) **adfs.vlab.f5demo.com**

2. **Which servers should be included in this pool?**

   (a) **10.1.20.6**

   (b) Click Add

   (c) **10.1.20.7**

High Availability

What IP address do you want to use for the virtual server?	10.1.20.100
What service port do you want to use for the virtual server?	443
Which FQDN will clients use to access AD FS?	adfs.vlab.f5demo.com
Do you want to create a new pool or use an existing one?	Create a new pool
Which servers should be included in this pool?	IP Address 10.1.20.6 Port 443 Connection limit IP Address 10.1.20.7 Port 443 Connection limit Add
Do you want to configure support for client certificate authentication?	Yes, configure support for certificate authentication

9. Click Finished

5.3.3 Test the ADFS Load Balancing Functionality

1. Close any open Chrome incognito windows

2. Open a new Chrome window if not already open

3. Right click the "ADFS Demo App" shortcut and open in an incognito window

ClaimsXRay   ADFS Demo App

4. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

Welcome!

These are your claims:

Type	
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	true
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.20.4
http://schemas.microsoft.com/claims/authnmethodsproviders	WindowsAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/v
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-05-25T20:03:21.959Z

Server time: 5/25/2018 8:03:22 PM

1. Note that ADFS is still identifying the user as inside the corporate network because the user did not go through an MS-ADFSPIP compliant proxy solution.

2. What happened:

   (a) You made a request to App

   (b) App redirected you to ADFS for authentication

   (c) **The BIG-IP received the request and load balanced it to one of the ADFS servers (this is the only change from last time)**

(d) ADFS authenticated you automatically with Windows Integrated Authentication with your domain joined computer

(e) ADFS redirected you back to App with a WS-Fed assertion

(f) App validated the assertion and displayed the claims it received from ADFS

### 5.3.4 Review the ADFS Load Balancing Configuration

1. Go to Local Traffic -> Virtual Servers

2. Notice there are two deployed, one on port 443 and one on port 49443

   (a) 443 is for ADFS traffic

       i. Pool members use port 443

   (b) 49443 is for client certificate auth support

       i. Pool members use port 49443

5.4 Module: Deploy ADFS Proxy Services

In this module you will deploy ADFS Proxy functionality. The BIG-IP will perform the same role in front of ADFS as a Web Application Proxy (WAP) server does, supporting the protocol MS-ADFSPIP.

5.4.1 Change Client to Point at BIG-IP ADFS Proxy Virtual Server

1. Double click the BIG-IP ADFS Load Balancer desktop shortcut
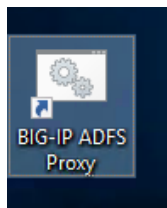
2. You should see that the HOSTS file now points ADFS at the load balancing virtual server (which is not yet created)
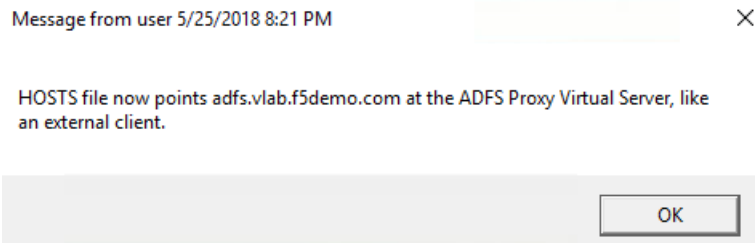
3. Close any open Chrome incognito windows

4. Open a new Chrome window if not already open

5. Right click the "ADFS Demo App" shortcut and open a new incognito window

   (a) It should fail because you cannot access ADFS through the BIG-IP until you deploy the configuration.

(b) If it is still working, you may need to close Chrome and/or retry the HOSTS file shortcut.

5.4.2 Deploy ADFS iApp for ADFS Proxy (with MS-ADFSPIP support)

1. Open the BIG-IP configuration interface

2. Open iApps -> Application Services -> Applications

3. Click Create

Accept all default values except for those listed below.

4. **Name**: **adfs-proxy**

5. **Template**: **f5.microsoft_adfs.v1.2.0rc7**

6. **Access Policy Manager (BIG-IP APM)**

   (a) **Would you like to configure BIG-IP as an ADFS Proxy?**

   i. **Yes, configure BIG-IP as an ADFS Proxy**

   (b) **What is the account to be used for establishing proxy trust with ADFS?**

   i. **admin@f5demo.com**

   (c) **What is the password associated with that account?**

   i. **admin**

Establishing trust with ADFS requires username in UPN or domain\username format. This is true whether in the iApp or establishing trust manually.

7. **SSL Encryption**

   (a) **Which SSL certificate do you want to use?**

   i. **internal-vlab.f5demo.com.crt**

   (b) **Which SSL private key do you want to use?**

   i. **internal-vlab.f5demo.com.key**

Note that this time we are doing SSL Bridging. This is required for the ADFS Proxy. Client certificate authentication can still be performed because BIG-IP supports MS-ADFSPIP.

8. **High Availability**

   (a) **What IP address do you want to use for the virtual server?**

   i. **10.1.10.100**

   10.1.10.x is the external/DMZ network in this environment. Notice this is .10 not .20 this time.

1. **Which FQDN will clients use to access AD FS?**

   (a) **adfs.vlab.f5demo.com**

2. **Which servers should be included in this pool?**

   (a) **10.1.20.6**

   (b) Click Add

   (c) **10.1.20.7**

3. **What Trusted CA would you like to use to validate the client certificate chain presented during certificate authentication?**

  (a) **F5demo-DC-CA.crt**

This is the AD Certificates Services CA certificate for this environment that was used to issue the client certificates so that the client certificate auth can be verified. It was pre-imported for you.

  9. Click Finished

5.4.3 Test the ADFS Proxy Forms Authentication Functionality

  1. Close any open Chrome incognito windows

  2. Open a new Chrome window if not already open

  3. Right click the "ADFS Demo App" shortcut and open a new incognito window
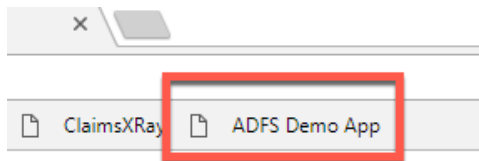
If you do not get the ADFS logon page noted below wait 60-120 seconds for the ADFS servers to sync and try again. If you are still getting the error you may have cache problems. Double check that you have closed all other incognito windows before trying this, and you can clear cache and cookies by performing ctrl+shift+del and selecting "all time".

  1. This time instead of automatically authenticating with Windows Integrated Authentication you are presented with a forms login page. This is because ADFS is configured to require Forms auth for external users.

    (a) Username: **user@f5demo.com**

    (b) Password: **user**

    (c) Click Sign In

  1. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

Welcome!

These are your claims:

| Type	Value
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy	APM
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	false
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.20.4
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip	10.1.1.8
http://schemas.microsoft.com/claims/authnmethodsproviders	FormsAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-05-25T21:15:05.387Z

Server time: 5/25/2018 9:15:05 PM

1. Note that ADFS now identifies the user as outside the corporate network, knows that APM acted as an ADFS Proxy, knows the user's true IP address, and that the user is now logging in with FormsAuthentication instead of WindowsAuthentication.

2. What happened:

    (a) You made a request to App

    (b) App redirected you to ADFS for authentication

    (c) **The BIG-IP received the request and load balanced it to one of the ADFS servers, as well as communicated data about the traffic using MS-ADFSPIP.**

    (d) **The ADFS server determined that you should be authenticated using the extranet policy and sent back a logon page which the BIG-IP forwarded on to you.**

    (e) **You submitted the forms and ADFS authenticated with your credentials**

    (f) ADFS redirected you back to App with a WS-Fed assertion

    (g) App validated the assertion and displayed the claims it received from ADFS

5.4.4 Test the ADFS Proxy Certificate Authentication Functionality

1. Close any open Chrome incognito windows

2. Open a new Chrome window if not already open

3. Right click the "ADFS Demo App" shortcut and open a new incognito window
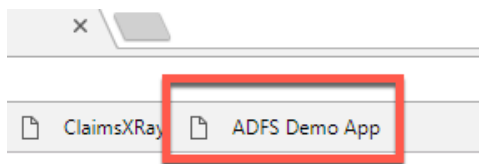
1. Click **Sign in using an X.509 certificate**

Sign in with your organizational account

user@f5demo.com

••••

Sign in

Sign in using an X.509 certificate

1. Note that you can configure ADFS extranet authentication settings to perform certificate authentication automatically. The ADFS server in this lab is setup to allow both forms and certificate authentication.

1. The certificate is already selected, click OK.

Select a certificate   ×

Select a certificate to authenticate yourself to adfs.vlab.f5demo.com:49443

Subject	Issuer	Serial
Users	f5demo-DC-CA	4A0000000CFA27D41...

Certificate information   OK   Cancel

1. You should see a set of claims displayed in the claims app at app.vlab.f5demo.com

Welcome!

These are your claims:

Type	Value
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-proxy	APM
http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork	false
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	user@f5demo.com
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-client-ip	10.1.20.4
http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-forwarded-client-ip	10.1.1.8
http://schemas.microsoft.com/claims/authnmethodsproviders	CertificateAuthentication
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/x509
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2018-05-25T22:14:40.914Z

Server time: 5/25/2018 10:14:41 PM

1. Note that ADFS now ADFS has identified the authentication type as CertificateAuthentication

2. What happened:

    (a) You made a request to App

    (b) App redirected you to ADFS for authentication

    (c) **The BIG-IP received the request and load balanced it to one of the ADFS servers, as well as communicated data about the traffic using MS-ADFSPIP.**

(d) **The ADFS server determined that you should be authenticated using the extranet policy and sent back a logon page which the BIG-IP forwarded on to you.**

(e) **You selected the Certificate Authentication, which caused you to be redirected to port 49443 where the BIG-IP performed certificate authentication**

(f) **BIG-IP forwarded on details about your authentication using MS-ADFSPIP to the ADFS server**

(g) ADFS redirected you back to App with a WS-Fed assertion

(h) App validated the assertion and displayed the claims it received from ADFS

5.4.5 Review the ADFS Proxy Configuration

1. Go to Local Traffic -> Virtual Servers

2. Notice there are two adfs-proxy virtual servers deployed, one on port 443 and one on port 49443

   (a) 443 is for ADFS traffic

      i. Pool members use port 443

   (b) 49443 is for client certificate auth support

      i. Pool members use **port 443**

         A. **This is different from the load balancing only, which pointed to port 49443. This is because the certificate auth is not passing through, BIG-IP is performing the certificate auth, then sending the data along to ADFS using MS-ADFSPIP.**

   (a) Click on the virtual server **adfs-proxy_adfs_vs_443**

      i. Scroll down and examine the Access Policy -> ADFS Proxy configuration item

         A. Note that ADFS Proxy functionality is enabled and a trust is established. The BIG-IP will auto-renew this prior to expiration.

         B. Note that no Access Profile is deployed. You can add one if desired for additional security. The iApp is capable of deploying it, along with the required bypass iRule for some URLs like the metadata sharing URL.

   (b) Go to Local Traffic -> Profiles -> SSL -> Server and click **adfs-proxy_server-ssl**

      i. Note that a certificate and key are used on the server side. These are created as part of establishing the trust with the ADFS server as noted in the previous step and then automatically input here.

      ii. This is shared by both the 443 and the 49443 virtual servers because they need the same settings to communicate with ADFS.

   (c) Change configuration mode to advanced

      i. Note that the server name field contains adfs.vlab.f5demo.com. ADFS requires SNI and this is how you configure it on the serverssl profile.

   (d) Go to Local Traffic -> Profiles -> SSL -> Client and click **adfs-proxy_client-ssl-cert-auth**

      i. This is the SSL profile that provides certificate auth on the port 49443 virtual server.

      ii. Note that Client Certificate is set to required and the Trusted Certificate Authorities is set to f5demo-DC-CA.

iii. You could use Advertised Certified Authority here if you wanted the client to only display certificates generated by a specific CA. This could be your primary CA, or even a specific subordinate CA if you wanted to issue client certificate auth user certificates from a specific CA to reduce the number shown to the user.

5.5 Module: Additional Information and Troubleshooting Tips

It is possible to implement an APM profile in front of the ADFS server. The deployment guide covers requirements, or you can select to deploy an APM profile in the iApp and it will handle everything including the required selective APM bypass iRule and SSO into ADFS.

When logging in to the default APM logon page, you do not need to specify the domain like you do on the ADFS logon page, just typing "user" (the samAccountName) will be sufficient. You can customize the APM logon page to accept samAccountName, UPN, or domain\username if desired.

The service that handles the MS-ADFSPIP trust relationship is adfs_proxy. You can restart this service if needed with the following CLI command: bigstart restart adfs_proxy.

If you cannot establish trust, it could be because the primary ADFS server is offline. The primary ADFS server in the farm must be functioning or new WAPs/Proxies cannot establish trust.

Microsoft provides a service called ClaimsXRay at https://adfshelp.microsoft.com that is very useful for troubleshooting ADFS related issues. There is a shortcut to it on your Chrome browser. The shortcut is configured to populate the values for ClaimsXRay for this lab environment so that you do not need to enter them into the webpage manually. It will redirect to your ADFS environment, where you can authenticate, then send you to ClaimsXRay where you can examine the claims.

For more information on this solution, go here: https://devcentral.f5.com/articles/ad-fs-proxy-replacement-on-f5-big-ip-30191

For the deployment guide, go here: https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm

5.6 Conclusion

5.6.1 Learn More

Links & Information

- **Microsoft Active Directory Federation Services Deployment Guide:**

  https://f5.com/solutions/deployment-guides/microsoft-active-directory-federation-services-big-ip-v11-ltm-apm
- **DevCentral: ADFS Proxy Replacement on F5 BIG-IP:**

  https://devcentral.f5.com/articles/ad-fs-proxy-replacement-on-f5-big-ip-30191

6

Class 6: Federating Common Services

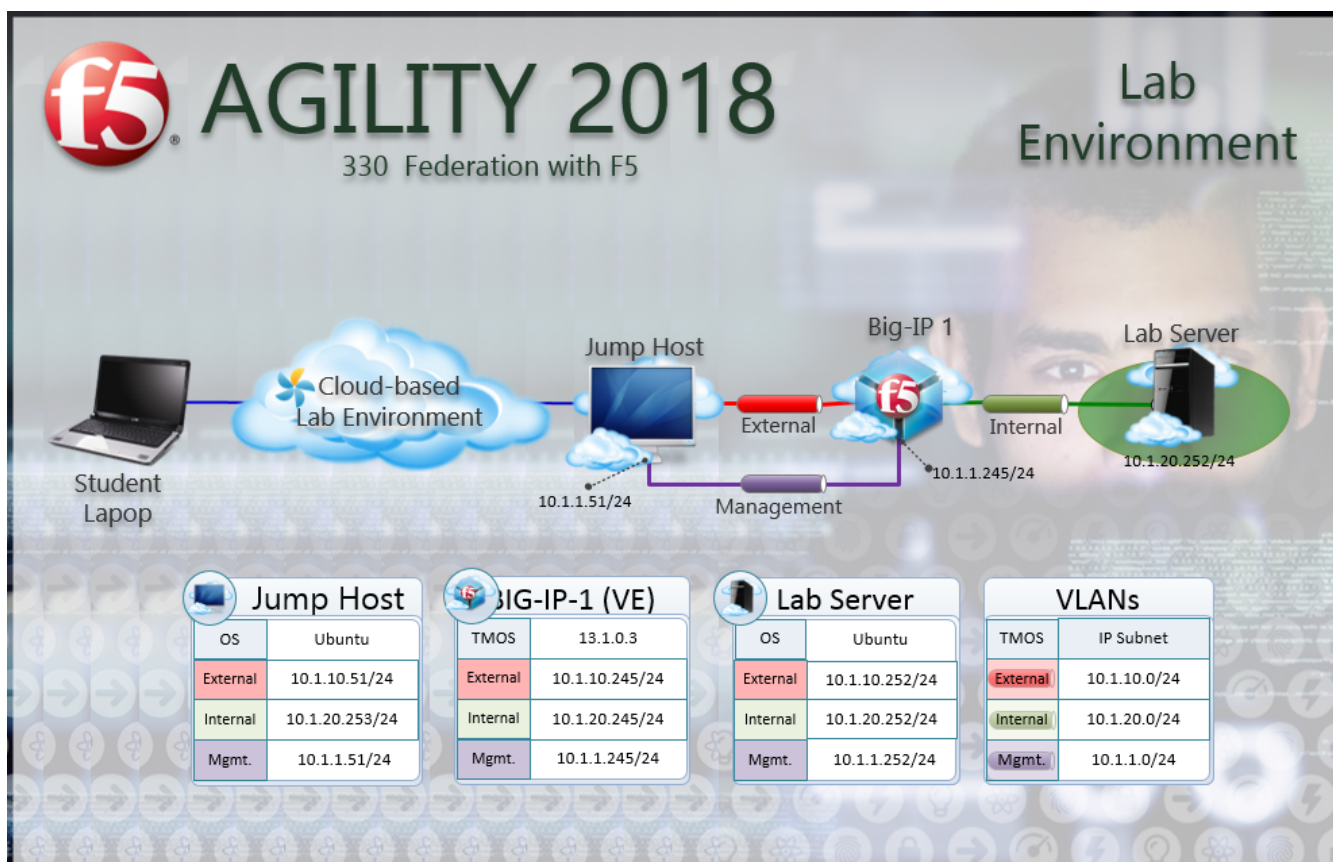Welcome to the Common Federation lab at F5 Agility 2018

6.1 Welcome

Welcome to the 330 Access Policy Manager (APM) Federation Hands-on Lab Guide. The following labs and exercises will instruct you on how to configure and troubleshoot federation use cases based on the experience of field engineers, support engineers and clients. This guide is intended to complement lecture material provided during the 330 course as well as a reference guide that can be referred to after the class as a basis for configuring federation relationships in your own environment.

6.1.1 Lab Network Setup

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

- Cloud-based lab environment complete with Jump Host, Virtual BIG-IP and Lab Server

- Duplicate Lab environments for each student for improved collaboration

- The Virtual BIG-IP has been pre-licensed and provisioned with Access Policy Manager (APM)

- Pre-staged configurations to speed up lab time, reducing repetitive tasks to focus on key learning elements.

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

6.1.2 Timing for labs

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

Lab Description	Time Allocated
LAB 1 - SAML Service Provider (SP)	25 minutes
LAB 2 - SaaS SAML Identity Provider (IDP) (OKTA)	25 minutes
LAB 3 - oAuth & OpenID Connect (Google)	25 minutes
LAB 4 - oAuth and Azure AD Lab	25 minutes

6.1.3 Authentication – Credentials

The following credentials will be utilized throughout this Lab guide. All other credentials will be indicated at the time of use.

Credential Use	User ID	Password
BIG-IP Configuration Utility (GUI)	admin	admin
BIG-IP CLI Access (SSH)	root	default
Jump Host Access	f5student	f5DEMOs4u

6.1.4 Utilized Browsers

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

6.1.5 General Notes

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

6.1.6 Acknowledgements

This lab is built upon the work of prior F5 Agility's and the work of many individuals behind the scenes in addition the 2018 Agility Lab Team. Many thanks to the 2017 Agility Lab Team for the SAML & OAuth Federation Labs, Lucas Thompson for his OAuth/OIDC Lab and our lab testers Matt Harmon, Dave Lipowsky & Stu McMath.

6.1.7 Presented by

APM 330 Presented by: Steve Lyons, Chris Miller & Chas Lesley

6.2 Lab 1: SAML Service Provider (SP) Lab

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

6.2.1 Objective:

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

6.2.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- Estimated completion time: 25 minutes

6.2.3 Lab 1 Tasks:

TASK 1: Configure the SAML Service Provider (SP)

Refer to the instructions and screen shots below:

1. Login to your lab provided **Virtual Edition BIG-IP**
2. Begin by selecting: **Access -> Federation -> SAML Service Provider** ->
   Local SP Services
3. Click the **Create** button (far right)
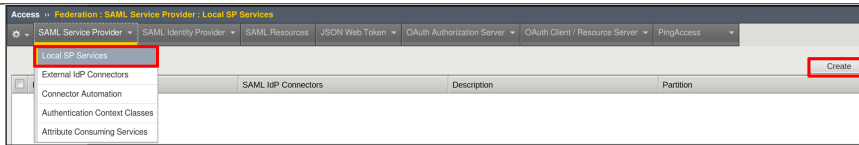
4. In the **Create New SAML SP Service** dialogue box click **General Settings** in
   the left navigation pane and key in the following as shown:
   - **Name**: **app.f5demo.com**
   - **Entity ID**: **https://app.f5demo.com**
   Note: The yellow box on Host will disappear when the Entity ID is entered.

5. Click on the **Security Settings** in the left navigation menu.
6. Check the **Sign Authentication Request** checkbox
7. Select /**Common/SAML.key** from drop down menu for the **Message Signing Private Key**
8. Select /**Common/SAML.crt** from drop down menu for the **Message Signing Certificate**
9. Click **OK** on the dialogue box

Create New SAML SP Service

General Settings
Endpoint Settings
Security Settings
Authentication Context
Requested Attributes
Advanced Settings

Authentication and Encryption Settings

☑ Sign Authentication Request

Message Signing Private Key*:
/Common/SAML.key

Message Signing Certificate*:
/Common/SAML.crt

☑ Want Signed Assertion

☐ Want Encrypted Assertion

Assertion Decryption Private Key :
Select a value...

Assertion Decryption Certificate :
Select a value...

OK   Cancel

TASK 2: Configure the External SAML IdP Connector

Refer to the instructions and screen shots below:

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

Access ›› Federation : SAML Service Provider : Local SP Services

| SAML Service Provider | SAML Identity Provider | SAML Resources | JSON Web Token | OAuth Authorization Server | OAuth Client / Resource Server | PingAccess |

Local SP Services
External IdP Connectors
Connector Automation
Authentication Context Classes
Attribute Consuming Services

Create

	SAML IdP Connectors	Description	Partition
			Common

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 the following: **idp.partner.com**
6. Click **OK** on the dialogue box.

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

TASK: 3: Bind the External SAML IdP Connector to the SAML SP

Refer to the instructions and screen shots below:

1. Click on the **Local SP Services** from the **SAML Service Provider** tab in the horizontal navigation menu.
2. Click the **Checkbox** next to the previously created **app.f5demo.com** and select **Bind/Unbind IdP Connectors** button at the bottom of the GUI.

3. In the **Edit SAML IdP's that use this SP** dialogue box click the **Add New Row** button
4. In the added row click the **Down Arrow** under **SAML IdP Connectors** and select the
   /**Common**/**idp.partner.com** SAML IdP Connector previously created.
5. Click the **Update** button and the **OK** button at the bottom of the dialogue box.
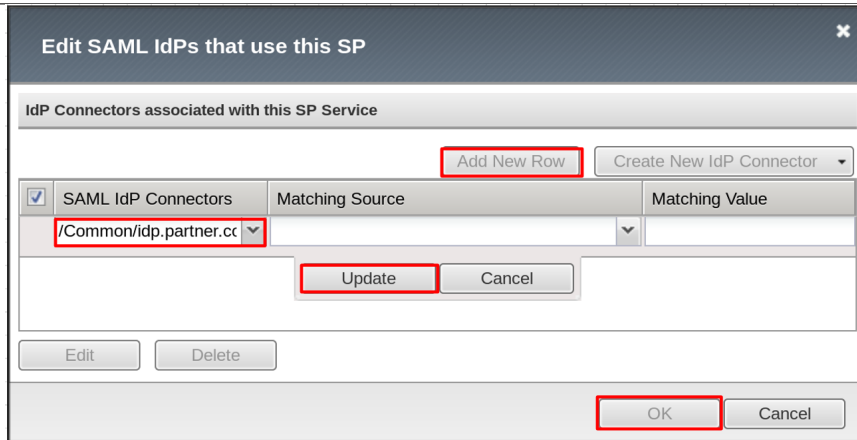
6. Under the **Access** -> **Federation** -> **SAML Service Provider** ->
   Local SP Services menu you should now see the following (as shown):
   - **Name**: **app.f5demo.com**
   - **SAML IdP Connectors**: **idp.partner.com**

TASK 4: Configure the SAML SP Access Policy

Refer to the instructions and screen shots below:

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

3. In the **New Profile** window, key in the following as shown:
    - **Name**: **app.f5demo.com-policy**
    - **Profile Type**: **All** (from drop down)
    - **Profile Scope**: **Profile** (default)
4. Scroll to the bottom of the **New Profile** window to the **Language Settings**
5. Select **English** from the **Factory Built-in Languages** menu on the right and click the **Double Arrow (<<)**, then click the **Finished** button.

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

7. In the **Visual Policy Editor** window for the **/Common/app.f5demo.com-policy**, click the **Plus (+) Sign** between **Start** and **Deny**.
8. In the pop-up dialogue box select the **Authentication** tab and then click the **Radio Button** next to **SAML Auth**. Once selected click the **Add Item** button.

Access Policy: /Common/app.f5demo.com-policy   Edit Endings

| Start | fallback | + | Deny |

Add New Macro

Begin typing to search

Logon | Authentication | Assignment | Endpoint Security (Server-Side) | Endpoint Security (Client-Side) | General Purpose

○	HTTP Auth	HTTP authentication of end user credentials
○	Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
○	LDAP Auth	LDAP authentication of end user credentials
○	LDAP Query	LDAP query to pull user attributes for use with resource assignment or other functions, such as LDAP group mapping
○	LocalDB Auth	Local Database Authentication
○	NTLM Auth Result	NTLM authentication of end user credentials
○	OAuth Authorization	OAuth 2.0 Authorization Agent for scope management
○	OAuth Client	OAuth Client
○	OAuth Scope	OAuth Scope
○	OCSP Auth	Online Certificate Status Protocol (OCSP) client certificate authentication
○	On-Demand Cert Auth	Dynamically initiate an SSL re-handshake and validate the received client certificate
○	OTP Generate	Generate One Time Passcode (OTP)
○	OTP Verify	Verify One Time Passcode (OTP)
○	RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
○	RADIUS Auth	RADIUS authentication of end user credentials
○	RSA SecurID	RSA SecurID two-factor authentication of end user credentials
○	SAML Auth	SAML Auth using SAML Service Provider Interface
○	TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off
○	TACACS+ Auth	TACACS+ Authentication of end user credentials
○	Transparent Identity Import	Import Identity (user) information from IF-MAP server

Cancel | Add Item | Help

---

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

Properties* | Branch Rules

Name: SAML Auth

SAML Authentication SP

AAA Server	/Common/app.f5demo.com ▾
Attribute Consuming Service	None ▾

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

11. In the **Visual Policy Editor** select the **Deny** along the **Successful** branch following the **SAML Auth**
12. From the **Select Ending** dialogue box select the **Allow Radio Button** and then click **Save**.
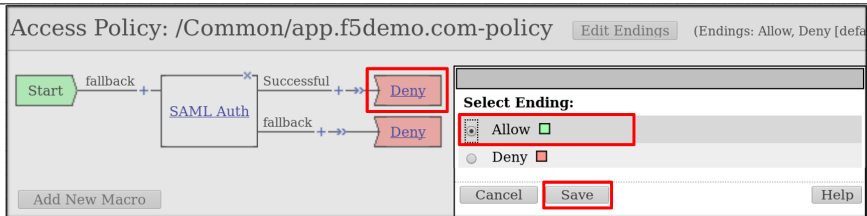
13. In the **Visual Policy Editor** click the **Apply Access Policy** (top left) and close the **Visual Policy Editor**.

Note: Additional actions can be taken in the Per Session policy (Access Policy). The lab is simply completing authentication. Other access controls can be implemented based on the use case
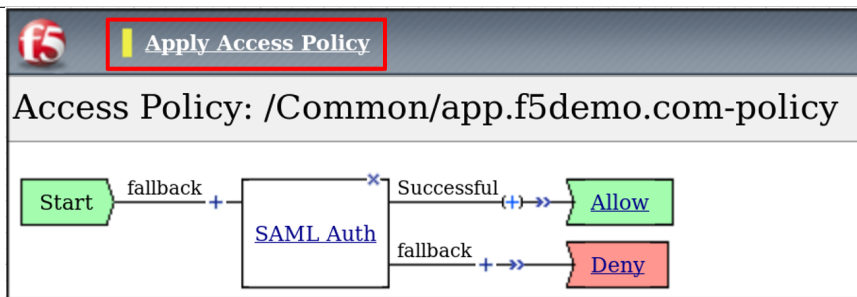
TASK 5: Create the SP Virtual Server & Apply the SP Access Policy

Refer to the instructions and screen shots below:

1. Begin by selecting: **Local Traffic** -> **Virtual Servers**
2. Click the **Create** button (far right)
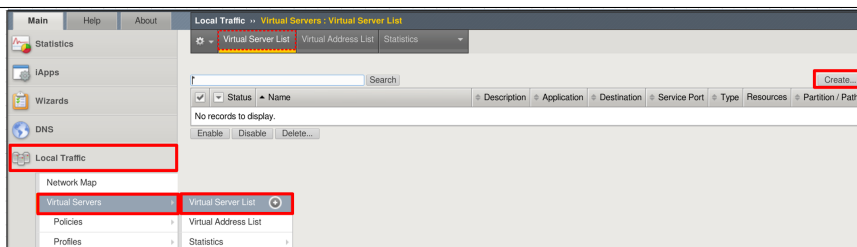
3. In the **New Virtual Server** window, key in the following as shown:
   - **Name**: **app.f5demo.com**
   - **Destination Address/Mask**: **10.1.10.100**
   - **Service Port**: **443**
   - **HTTP Profile: http** (drop down)
   - **SSL Profile (client): app.f5demo.com-clientssl**
   - **Source Address Translation: Auto Map**
4. Scroll to the **Access Policy** section
   - **Access Profile**: **app.f5demo.com-policy**
   - **Per-Request Policy: saml_policy**
5. Scroll to the Resource section
   - **Default Pool**: **app.f5demo.com_pool**
6. Scroll to the bottom of the configuration window and click **Finished**

Note: The use of the Per-Request Policy is to provide header injection and other controls.
These will be more utilized later in the lab.

Local Traffic ›› Virtual Servers : Virtual Server List ›› New Virtual Server...

General Properties

Name	app.f5demo.com
Description	
Type	Standard
Source Address	
Destination Address/Mask	10.1.10.100
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
State	Enabled

Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None

	Selected	Available
SSL Profile (Client)	/Common app.f5demo.com-clientssl << >>	/Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl

Scroll to Source Address Translation

VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Scroll to Access Policy Section

Access Policy

Access Profile	app.f5demo.com-policy
Connectivity Profile	+ None
Per-Request Policy	saml_policy

Scroll to Default Pool

Default Pool	+ app.f5demo.com_pool
Default Persistence Profile	None
Fallback Persistence Profile	None

TASK 6: Test the SAML SP

Refer to the instructions and screen shots below:

1. Using your browser from the Jump Host click on the provided bookmark or navigate to
   https://app.f5demo.com . The SAML SP that you have just configured.
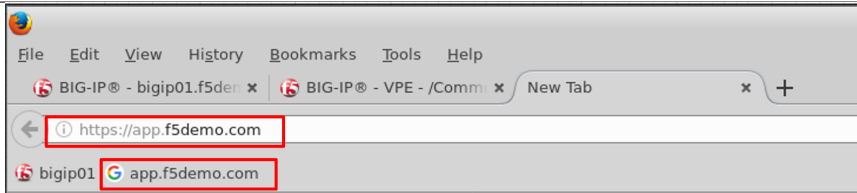
2. Did you successfully redirect to the IdP?
3. Login to the iDP, were you successfully authenticated? (use credentials provided in the
   Authentication Information section at the beginning of this guide)
   - **Username**: **user**
   - **Password**: **Agility1**
4. After successful authentication, were you returned to the SAML SP?
5. Were you successfully authenticated (SAML)?
6. Review your **Active Sessions** (**Access Overview** -> **Active Sessions**)
7. Review your Access Report Logs (**Access** -> **Overview Access Reports**)

6.3 Lab 2: IDaaS SAML Identity Provider (iDP) Lab (OKTA)

The purpose of this lab is to configure and test a IDaaS SAML Identity Provider. Students will configure a
IDaaS based SAML Identity Provider (in this case OKTA) and import and bind to a SAML Service Provider
and test IdP-Initiated and SP-Initiated SAML Federation.

6.3.1 Objective:

- Gain an understanding of integrating a IDaaS SAML Identity Provider(IdP)

- Gain an understanding of the access flow for IdP-Initiated SAML

6.3.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- Estimated completion time: 25 minutes
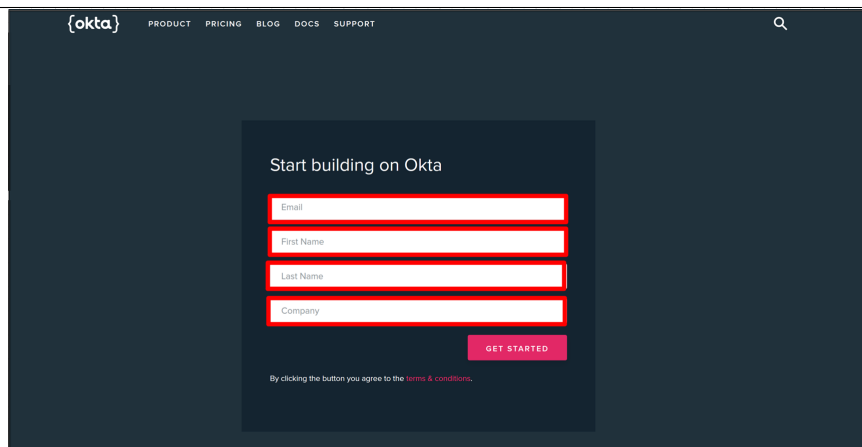
6.3.3 Lab 2 Tasks:

TASK 1: Sign Up for OKTA Developer Account
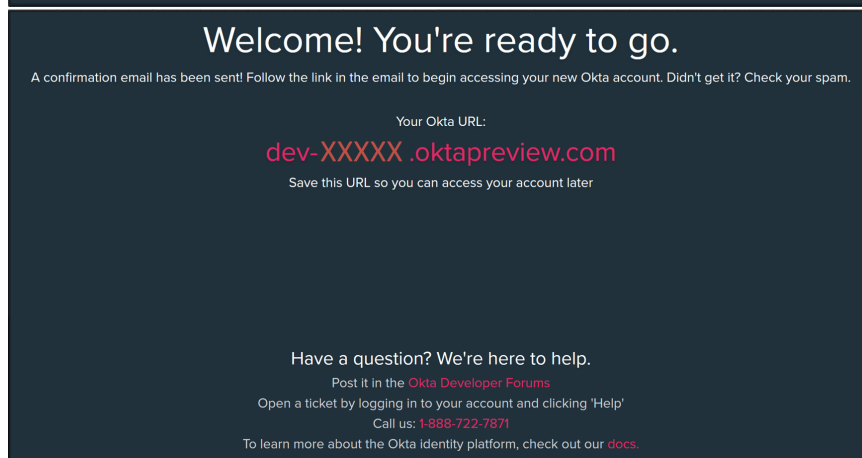
Refer to the instructions and screen shots below:

Note: The following steps provide instruction for setting up an OKTA developer account.
If you already have one, you may elect to use that account. Understand, however, that the
instructions below may need to be modified to match your environment.

1. Sign Up for an OKTA developer account by navigating to:
   https://developer.okta.com/signup/ and using a VALID email and click **Get Started**
2. Upon registration, you will be directed to a hyperlink (hostname) for your developer
   account. This link should be saved for future use.
3. Additional instructions will be sent to the email address provided during account setup.

4. Following the instructions received from the generated email, sign into the OKTA development environment with your provided, temporary password.

okta

Sign In

👤 |Username   ❓

🔒 Password   ❓

☐ Remember me

Sign In

Need help signing in?

5. Enter a **New Password** and the **Repeat New Password**
6. Use the drop down to select a **Forgot Password Question** and provide the Answer
7. Click a **Security Image**
8. Click **Create My Account**

TASK 2: OKTA Classic UI

Refer to the instructions and screen shots below:

1. For the purposes of the lab and SAML development, we will be using the OKTA Classic UI which provides access to SAML configurations. *(Note: At lab publication, the Developer Console did not have SAML resources.)*
2. In the top, left hand corner click the **<>** & select **Classic UI** from the drop down.
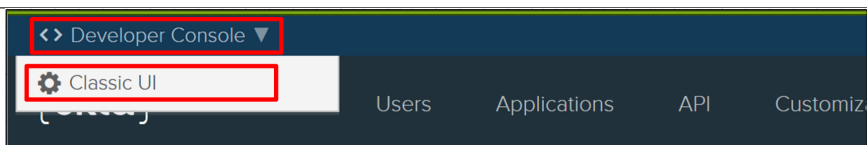
TASK 3: Enable OKTA Multi-Factor Authentication [OPTIONAL]

Refer to the instructions and screen shots below. This task will require a mobile app to enable a second factor.

[OPTIONAL]
Note: Enabling MFA will require a Smart Device with the appropriate OKTA client for your OS
The step can be skipped if you prefer to just use UserID/Password
1. Click **Security** from the top navigation, then click **Multifactor**
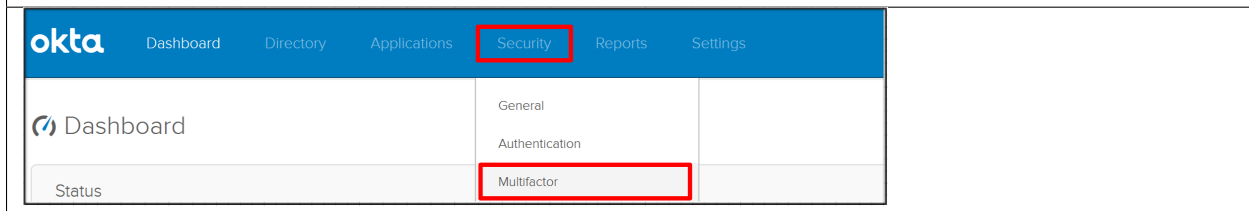
[OPTIONAL]
2. Under **OKTA Verify**, change the dropdown from **Inactive** to **Active**
3. Click the **Edit** button next to ***OKTA Verify Settings**
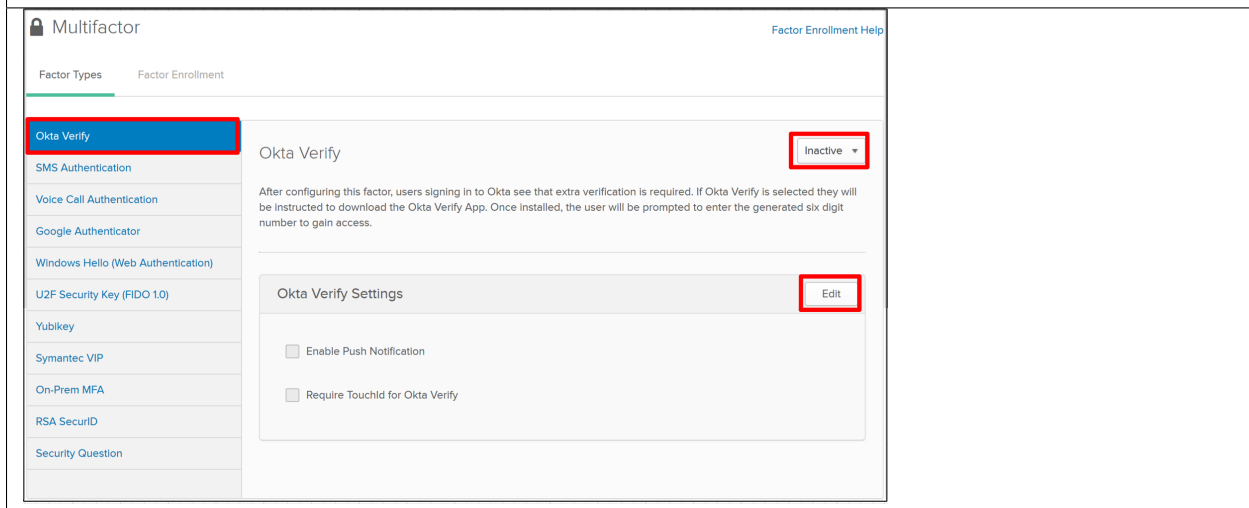
[OPTIONAL]
    4. Check **Enable Push Verification**
    5. Check **Require TouchID for OKTA Verify** (optional)
    6. Click **Save**

TASK 4: Build SAML Application - OKTA

Refer to the instructions and screen shots below:

1. In the main menu, click **Applications**, and **Applications** from the dropdown in the
    top navigation.
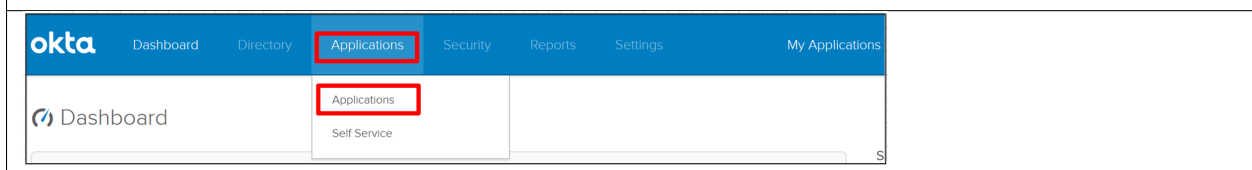
2. Click **Add Application** in the **Applications** dialogue window.
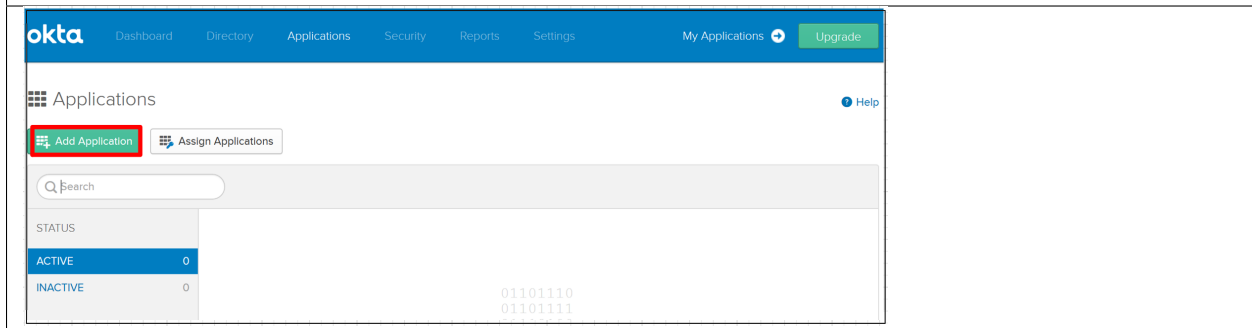
3. Click **Create New App** in the **Add Application Menu**
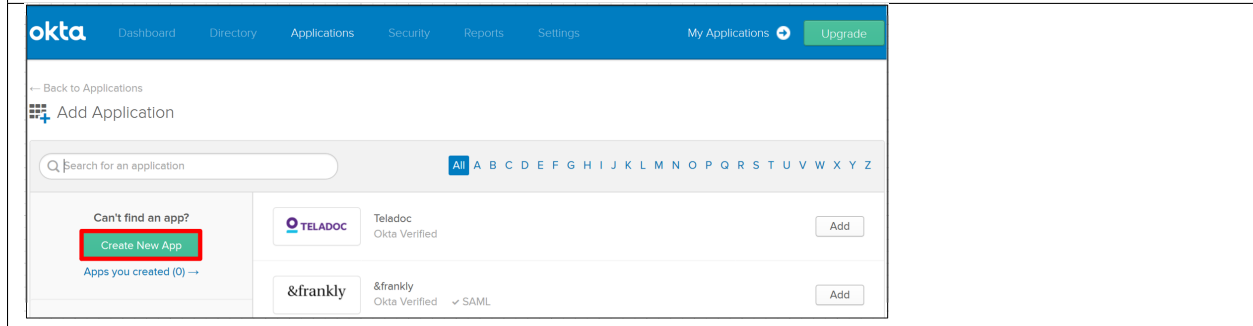
3. In the **Create a New Application Integration** dialogue box, select **Web** from the drop down for **Platform**.
4. Select the **SAML 2.0** radio button for **Sign on Method** and click **Create**.
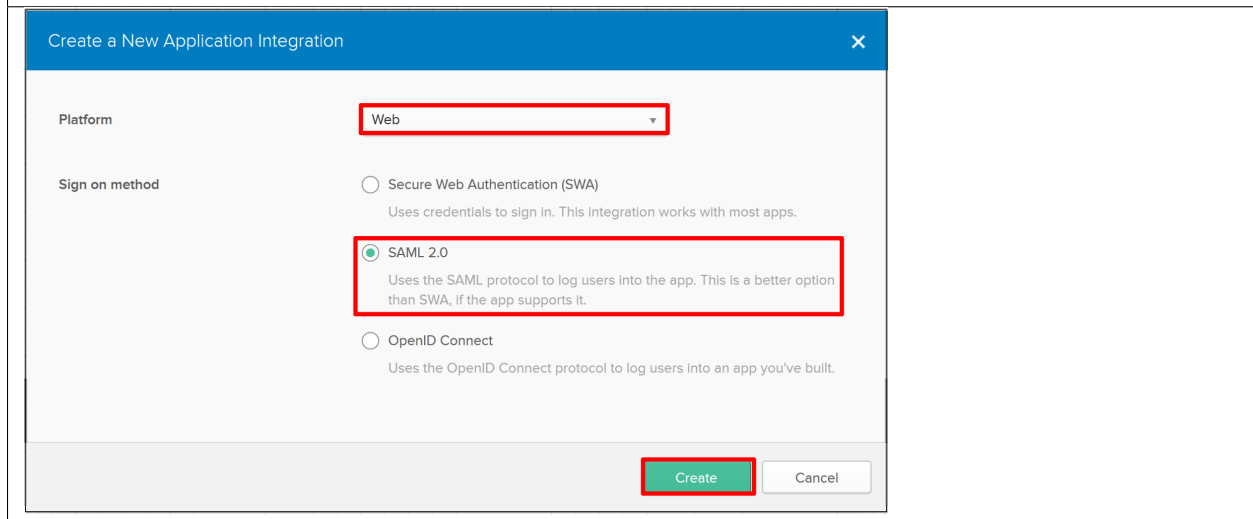
5. In the **Create SAML Integration** screen, enter **app.f5demo.com** for the **App Name**.
6. Leave all other values as default and click **Next**.

7. In the **Create SAML Integration** screen, enter the following values
8. In the **SAML Setting** section
    • **Single Sign on URL: https://app.f5demo.com/saml/sp/profile/post/acs**
    • **Audience URI (SP Entity ID): https://app.f5demo.com**
9. Leave all other values as default and click **Next**.

10. In the **Create SAML Integration** screen, select the:
    "I'm an OKTA customer adding an internal app" radio button for
    Are you a customer or partner?
11. In the resulting expanded window, select:
    "This is an internal app that we have created" for **App Type**
    and click **Finish**.

12. In the resulting application screen for **app.f5demo.com**, navigate to the
    SAML 2.0 section.
13. Right Click the **Identity Provider Metadata** hyperlink and click **Save Link As . . .**
14. Save the **metadata.xml** to your jumphost desktop. We will be using it in a later step
    in the Lab.

TASK 5: Add User to SAML Application

Refer to the instructions and screen shots below:

1. Within the **app.f5demo.com** application screen, Click **Assignments** then **Assign** and then **Assign to People** from the dropdown.

app.f5demo.com

Active ▾   View Logs

General   Sign On   Import   Assignments

Assign ▾   🔧 Convert Assignments   🔍 Search...   People ▾

Assign to People   Type

Assign to Groups
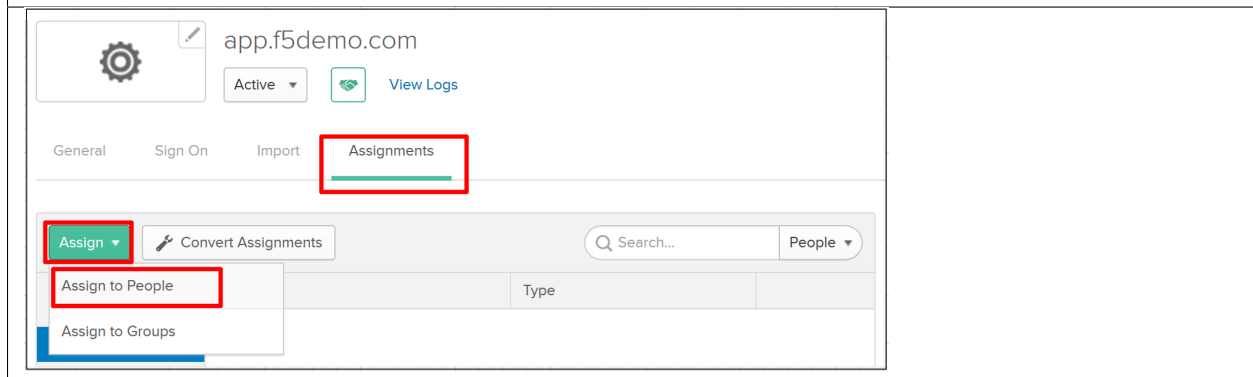
2. In the **Assign app.f5demo.com to People** dialogue box, select your **User ID**, click **Assign**, then **Done**.

Assign app.f5demo.com to People   ✕

🔍 Search...

Your selected user account   Assign
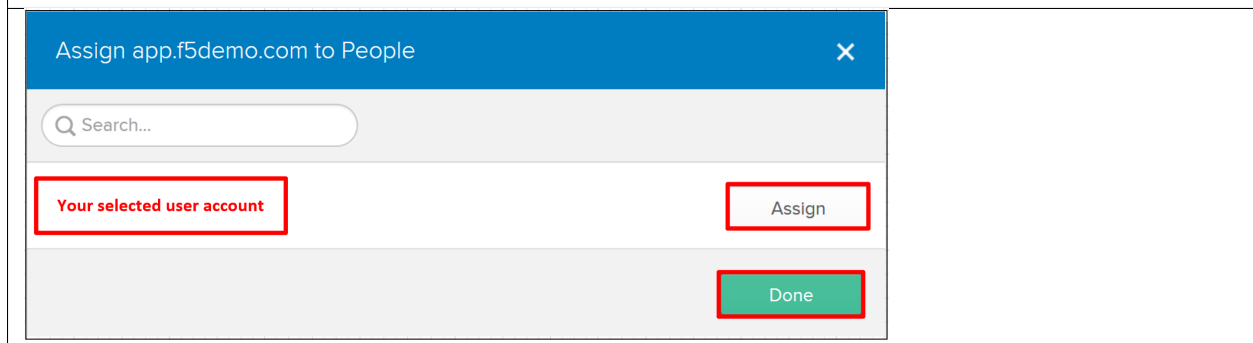
Done

3. Click **Save and Go Back**.

Assign app.f5demo.com to People   ✕

User Name   **Your selected user account**

Save and Go Back   Cancel

4. Click **Done**.

TASK 6: Add Multi-Factor Authentication Sign-On Policy [OPTIONAL]

Refer to the instructions and screen shots below. This section requires that **Task 3** be completed.

[OPTIONAL]
    1. Within the **app.f5demo.com** application screen, Click **Sign On**

[OPTIONAL]
    2. Scroll down to the **Sign On Policy** section and click **Add Rule**

[OPTIONAL]

3. In the **Add Sign On Rule** dialogue box, enter **MFA** for the **Rule Name**.
4. Scroll down to the **Actions** section.
5. In the **Actions** section, under **Access**, check the box for **Prompt for factor**.
6. Ensure **Every Sign On** radio button is selected.
7. Click **Save**.

TASK 7: Create the External IDP Connector

Refer to the instructions and screen shots below:

1. Login to your lab provided **Virtual Edition BIG-IP**
2. Begin by selecting: **Access** -> **Federation** -> **SAML Service Provider** -> **External IdP Connectors**.
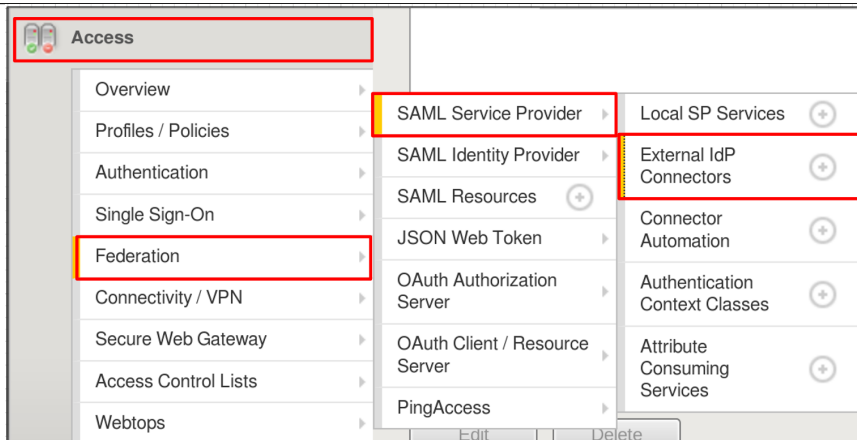
3. In the **External IdP Connectors** screen, click the **downward arrow** next to the word **Create** on the **Create** button (right side)
4. Select **From Metadata** from the drop down menu
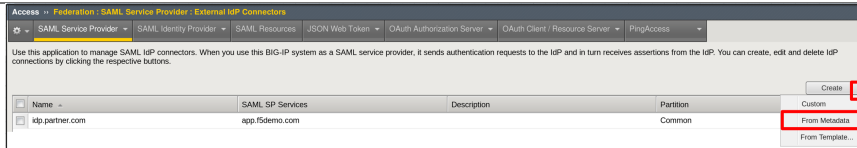
5. In the **Create New SAML IdP Connector** dialogue box, use the **Browse** button to select the **metadata.xml** from the desktop (created in Task 4).
6. Name the **Identity Provider Name**: **OKTA_SaaS-iDP**.
7. Click **OK**.
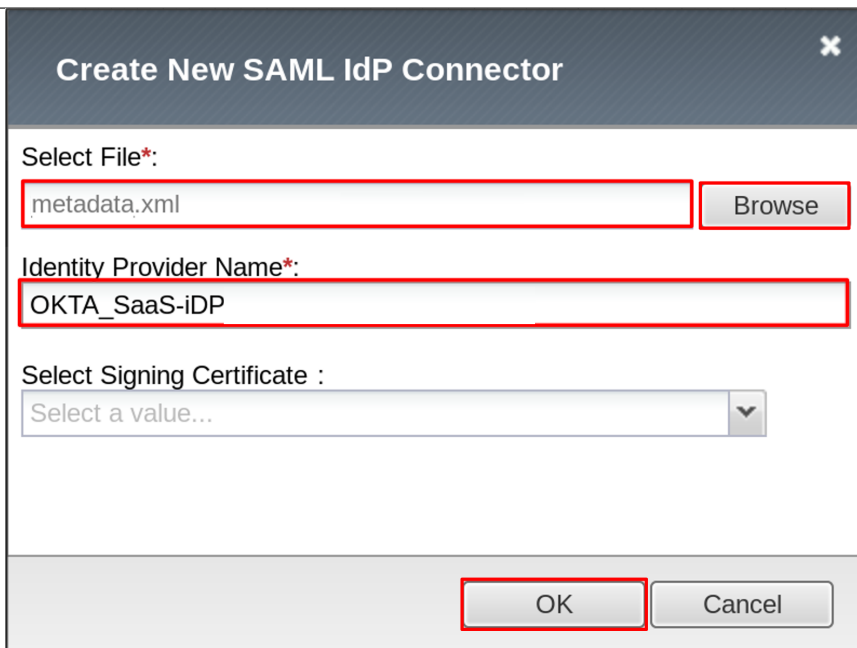
TASK 8: Change the SAML SP Binding

Refer to the instructions and screen shots below:

1. Begin by selecting: **Access** -> **Federation** -> **SAML Service Provider** ->
   Local SP Services
2. Select the checkbox next to **app.f5demo.com** and click **Bind\UnBind IdP Connectors**
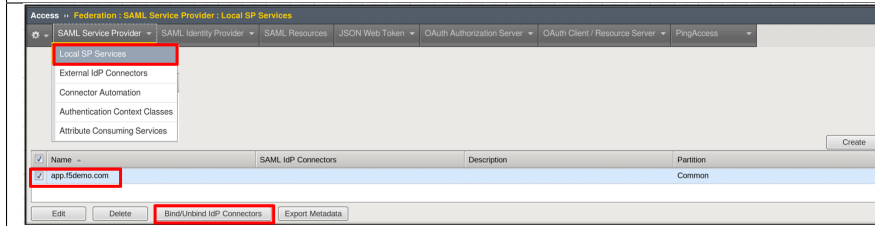
3. Check the existing binding and click **Delete**.
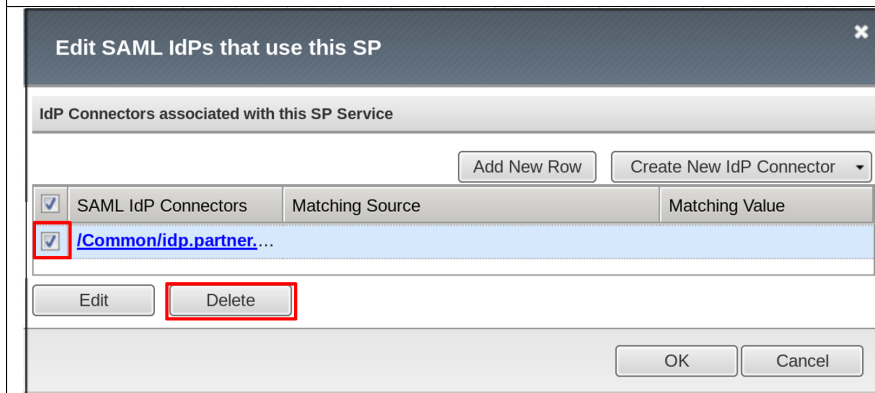
4. Click **Add New Row** and use the following values
   • **SAML IdP Connectors: /Common/OKTA_SaaS-iDP**
   • **Matching Source: %{session.server.landinguri}**
   • **Matching Value: /***
5. Click **Update** then **OK**.
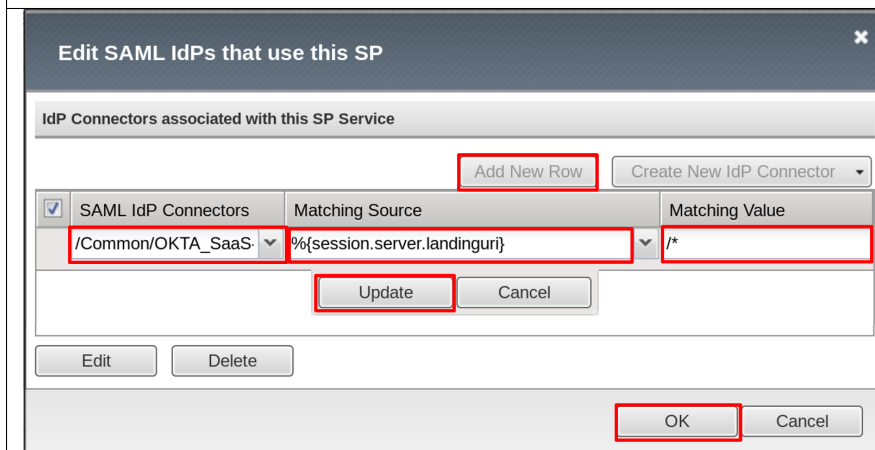
TASK 9: Apply Access Policy Changes

Refer to the instructions and screen shots below:

1. Click the **Apply Access Policy** link in the top left corner of the Admin GUI

| Hostname: | bigip01.f5demo.com | Date: | Jul 10, 2018 | User: | admin |
| IP Address: | 10.1.1.245 | Time: | 12:49 AM (PDT) | Role: | Administrator |

ONLINE (ACTIVE)
Standalone
Apply Access Policy
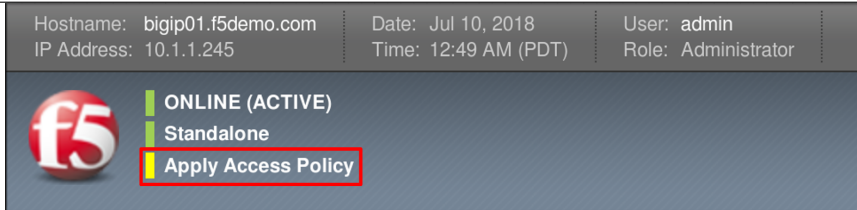
2. Ensure **app.f5demo.com-policy** is checked and click **Apply**

Access ›› Profiles / Policies : Access Profiles (Per-Session Policies)

| Access Profiles | Per-Request Policies | Policy Sync | Customization |

Search

Status ▲ Access Profile Name

☑ app.f5demo.com-policy

Apply
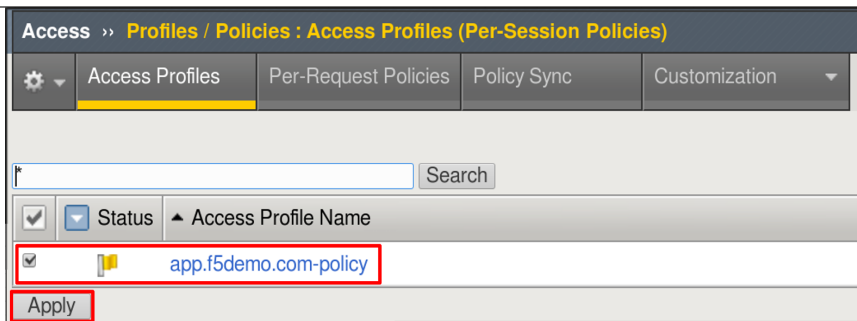
TASK 10 – Test Access to the app.f5demo.com application

Refer to the instructions and screen shots below:

1. Using your browser from the Jump Host click on the provided bookmark or navigate to:
   https://app.f5demo.com

File   Edit   View   History   Bookmarks   Tools   Help

BIG-IP® - bigip01.f5den ✕ | BIG-IP® - VPE - /Comm ✕ | New Tab ✕ +

https://app.f5demo.com

bigip01 G app.f5demo.com
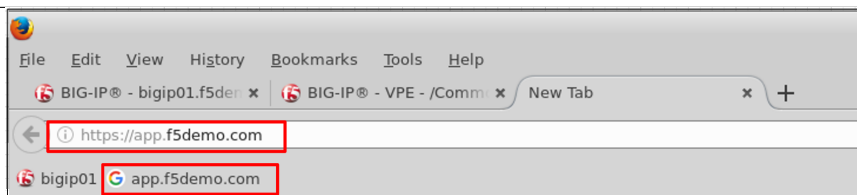
10. Destroy your Active Session by nagivating to **Access Overview** -> **Active Sessions**
    Select the checkbox next to your session and click the **Kill Selected Session** button.
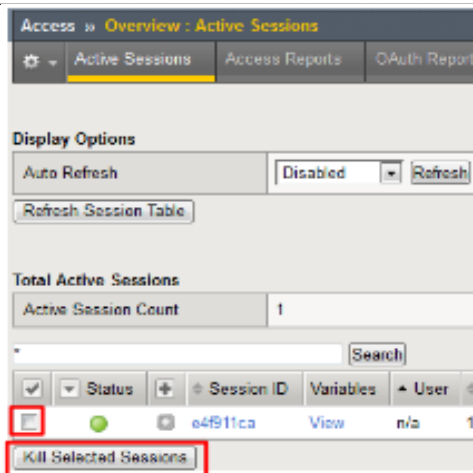
11. Close your browser and logon to your **https://dev-<Dev-ID>.oktapreview.com** account.
    Click on your **app.f5demo.com** application for IDP initiated Access.
12. After successful authentication, were you returned to the SAML SP?
13. Were you successfully authenticated (SAML)?
14. Review your **Active Sessions** (**Access Overview** -> **Active Sessions**).
15. Review your Access Report Logs (**Access Overview** -> **Access Reports**).

6.4 Lab 3: oAuth and OpenID Connect Lab (Google)

The purpose of this lab is to better understand the F5 use cases OAuth2 and OpenID Connect by deploying a lab based on a popular 3rd party login: Google. Google supports OpenID Connect with OAuth2 and JSON Web Tokens. This allows a user to securely log in, or to provide a secondary authentication factor to log in. Archive files are available for the completed Lab 2.

6.4.1 Objective:

- Gain a better understanding of the F5 use cases OAuth2 and OpenID Connect.

- Develop an awareness of the different deployment models that OAuth2, OpenID Connect and JSON Web Tokens (JWT) open up

6.4.2 Lab Requirements:

- All Lab requirements will be noted in the tasks that follow
- Estimated completion time: 25 minutes

6.4.3 Lab 3 Tasks:

TASK 1: Setup Google's API Credentials

Refer to the instructions and screen shots below:

Note: If you do not have Google/gMail account, you will need to set one up. Navigate to:
  - https://console.developers.google.com/apis/credentials & follow the directions for setup.*
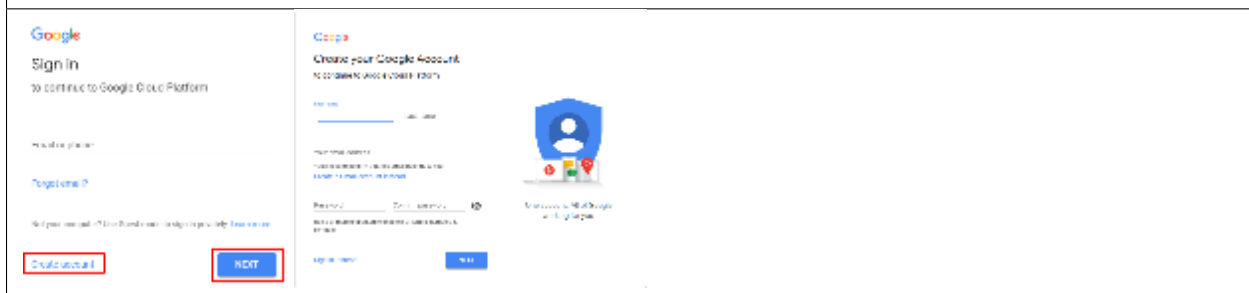
1. Navigate to https://console.developers.google.com/apis/credentials and log in with your developer account.
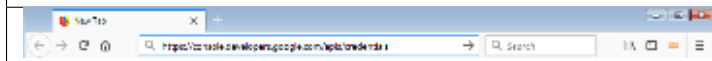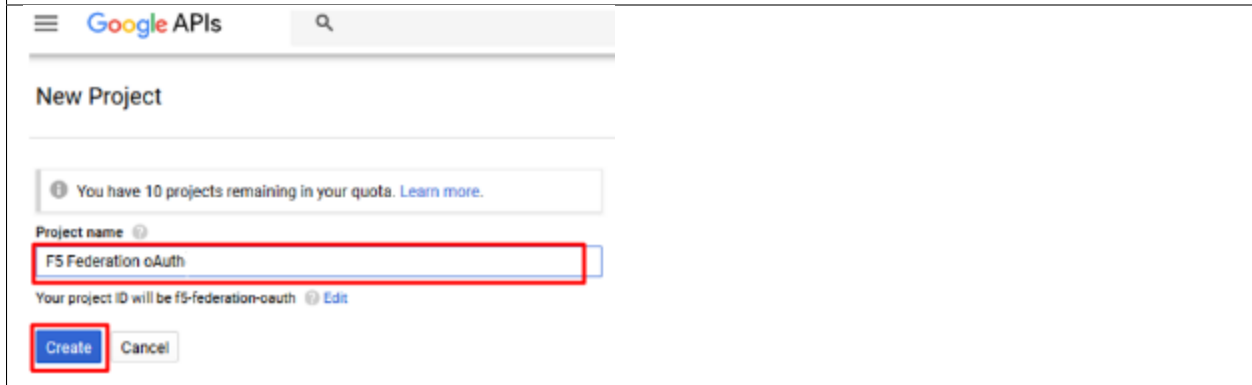
2. You will be redirected to the Google API's screen. If you are previously familiar with Google API's you can create a new Project.
3. If you have not been you will be prompted to create a New Project.
4. Click **Create** in the dialogue box provided.

274
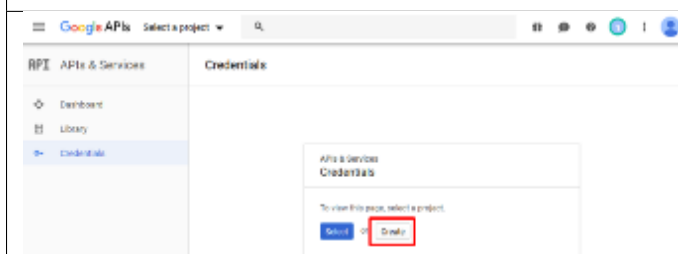
5. In the **New Project** window, provide a **Project Name**. The suggested value is:
   F5 Federation oAuth

Note: If you have exceeded your project quota you may have to delete a project or create a new account

6. In the next screen, select **OAuth Client ID** for the **Credentials** type and click **Create Credentials**
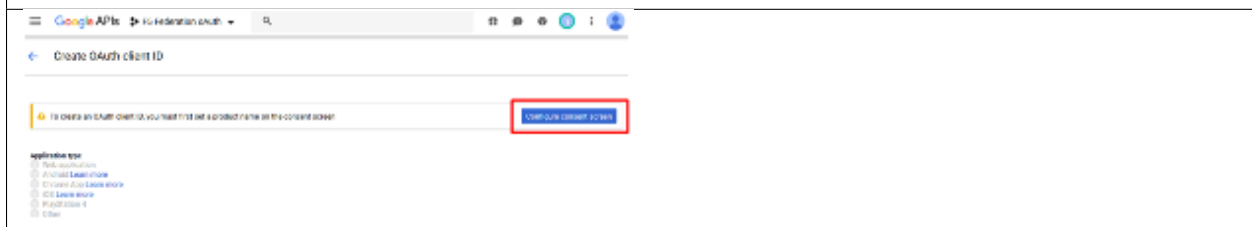
7. If you have not previously accepted a Consent Screen you may be prompted to do so. Click **Configure Consent Screen**.

8. On the **OAuth Consent Screen** tab, enter the **email address** of your developer
   account (pre-populated) for the **Email Address**.
9. For the **Product Name Shown to Users** enter **app.f5demo.com**.
10. Click **Save**.

11. In the **Create OAuth Client ID*** screen select or enter the following values:
    - **Application Type: Web Application**
    - **Name**: **app.f5demo.com**
    - **Authorized JavaScript Engine: https://app.f5demo.com**
    - **Authorized Redirect URIs: https://app.f5demo.com/oauth/client/redirect**
12. Click **Create**.

13. In the **OAuth Client** pop-up window copy and paste your **Client ID** and **Client Secret** in Gedit text editor provided on your desktop.

TASK 2: Setup F5 OAuth Provider

Refer to the instructions and screen shots below:

1. Create the **OAuth Provider** by navigating to **Access** -> **Federation** -> **OAuth Client/Resource Server** -> **Provider** and clicking **Create**.
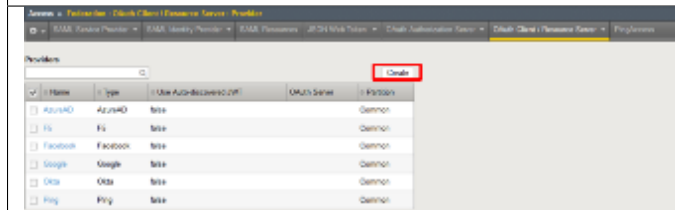
2. Using the following values to complete the OAuth Provider
   - **Name: Google_Provider**
   - **Type: Google**
   - **Trusted Certificate Authorities: ca-bundle.crt**
   - **Allow Self-Signed JWK Config: checked**
   - **Use Auto-discovered JWT: checked**
3. Click **Discover**.
4. Accept all other defaults.
5. Click **Save**.

TASK 3: Setup F5 OAuth Server (Client)

Refer to the instructions and screen shots below:

1. Create the **OAuth Server (Client)** by navigating to **Access** -> **Federation** -> **OAuth Client**/**Resource Server** -> **OAuth Server** and clicking **Create**.

2. Using the following values to complete the OAuth Provider
 • **Name: Google_Server**
 • **Mode: Client**
 • **Type: Google**
 • **OAuth Provider: Google_Provider**
 • **DNS Resolver: proxy_dns_resolver**
 • **Client ID: <your client id>**
 • **Client Secret: <your client secret>**
 • **Client's Server SSL Profile Name: serverssl**
3. Click **Finished**.

TASK 4: Setup F5 Per Session Policy (Access Policy)

Refer to the instructions and screen shots below:

1. Create the **Per Session Policy** by navigating to **Access -> Profile/Policies** ->
   Access Profiles (Per Session Policies) and clicking **Create**.

2. In the **New Profile** dialogue window enter the following values
   - **Name: Google_OAuth**
   - **Profile Type: All**
   - **Profile Scope: Profile**
   - **Language: English**
3. Click **Finished**.
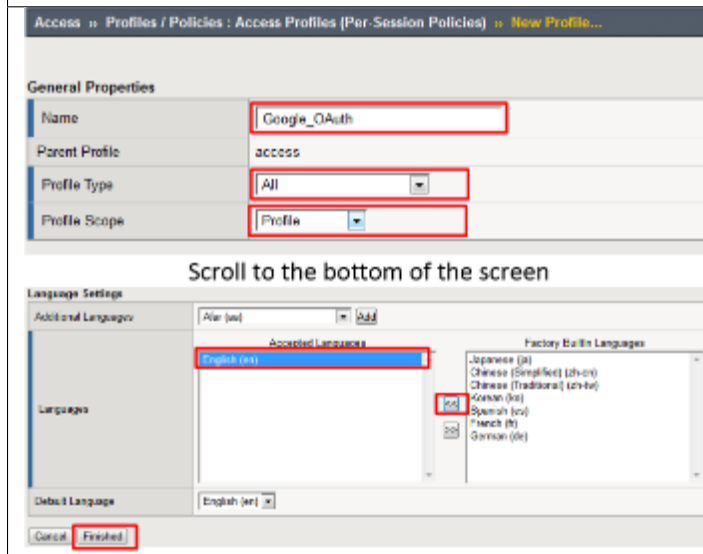
4. Click **Edit** link on for the **Google_OAuth** Access Policy.
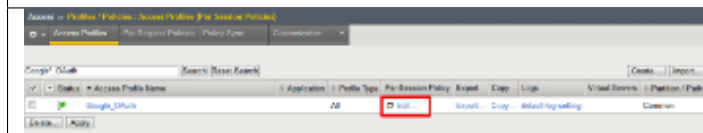
5. In the **Google_OAuth** Access Policy, click the "**+**" between **Start** & **Deny**
6. Click the **Authentication** tab in the events window.
7. Scroll down and click the radio button for **OAuth Client**.
8. Click **Add Item**.
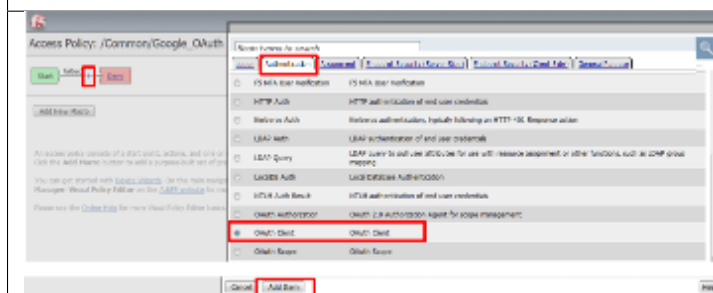
9. In the ***OAuth_Client*** window enter the following values as shown:
   - **Server: /Common/Google_Server**
   - **Grant Type: Authorization code**
   - **OpenID Connect: Enabled**
   - **OpenID Connect Flow Type: Authorization code**
   - **Authentication Redirect Request: /Common/GoogleAuthRedirectRequest**
   - **Token Request: /Common/GoogleTokenRequest**
   - **Refresh Token Request: /Common/GoogleTokenRefreshRequest**
   - **OpenID Connect UserInfo Request: /Common/GoogleUserinfoRequest**
   - **Redirection URI: https://%{session.server.network.name}/oauth/client/redirect**
   - **Scope: openid profile email**
10. Click **Save**.

11. Click on the **Deny** link, in the **Select Binding**, select the **Allow** radio button and click **Save**.

12. Click on the ***Apply Access Policy*** link in the top left-hand corner.
Note: Additional actions can be taken in the Per Session policy (Access Policy).
The lab is simply completing authorization. Other access controls can be implemented based on the use case.

TASK 5: Associate Access Policy to Virtual Server

Refer to the instructions and screen shots below:

1. Navigate to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List** and click on the **app.f5demo.com** Virtual Server link.
2. Scroll to the **Access Policy** section.

3. Use the **Access Profile** drop down to change the **Access Profile** to **Google_OAuth**
4. Use the **Per-Request Policy** drop down to change the **Per-Request Policy** to **Google_oauth_policy**
5. Scroll to the bottom of the **Virtual Server** configuration and click **Update**

TASK 6: Test app.f5demo.com

Refer to the instructions and screen shots below:

1. Navigate in your provided browser to **https://app.f5demo.com**
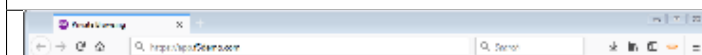
2. Authenticate with the account you established your Google Developer account with.
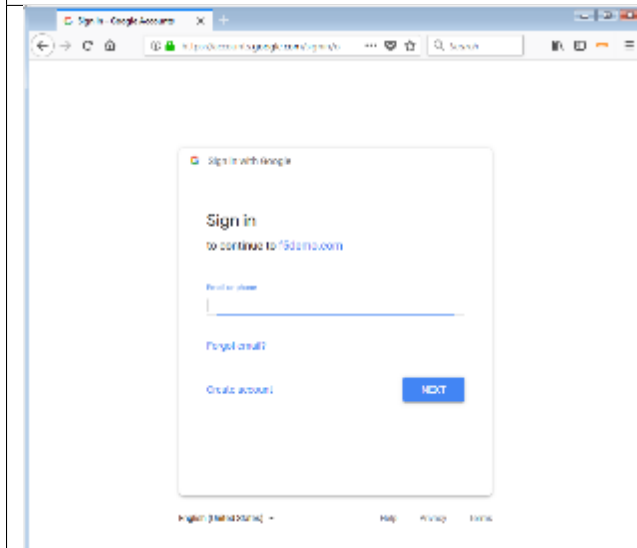
3. Did you successfully redirect to the Google?
4. After successful authentication, were you returned to the app.f5demo.com?
5. Did you successfully pass your OAuth Token?
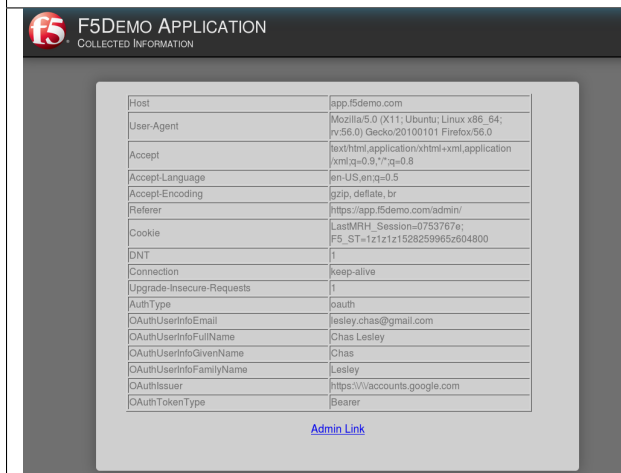
TASK 7: Per Request Policy Controls

Refer to the instructions and screen shots below:

1. In the application page for **https://app.f5demo.com** click the **Admin Link** shown
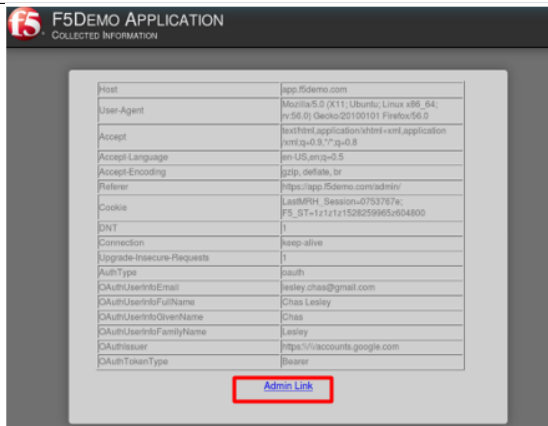
2. You will receive an **Access to this page is blocked** (customizable) message with a reference. You have been blocked because you do not have access on a per request basis.
3. Press the **Back** button in your browser to return to **https://app.f5demo.com**.

Access to this page is blocked.

Access was denied by a per-request policy.

The session reference number: 0753767e

The category reference is: Uncategorized

This product is licensed from F5 Networks. © 1999-2017 F5 Networks. All rights reserved.

4. Navigate to **Local Traffic** -> **iRules** -> **Datagroup List** and click on the
Allowed_Users datagroup.
5. Enter your **Google Account** used for this lab as the **String** value.
6. Click **Add** then Click **Update**.

*Note: We are using a DataGroup control to minimize lab resources and steps. AD or LDAP
Group memberships, Session variables, other user attributes and various other access
control mechanisms can be used to achieve similar results.*
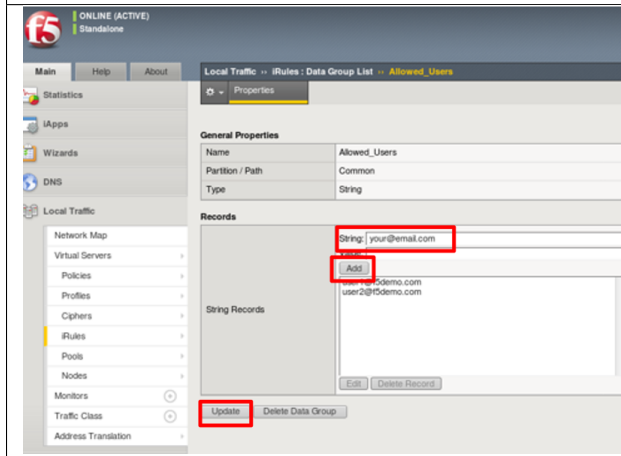
7. You should now be able to successfully to access the Admin Functions by clicking on the
Admin Link.

*Note: Per Request Policies are dynamic and do not require the same "Apply Policy" action as
Per Session Policies.*

8. To review the Per Request Policy, navigate to **Access Profiles/Policies** ->
Per Request Policies and click on the **Edit** link for the **Google_oauth_policy**.
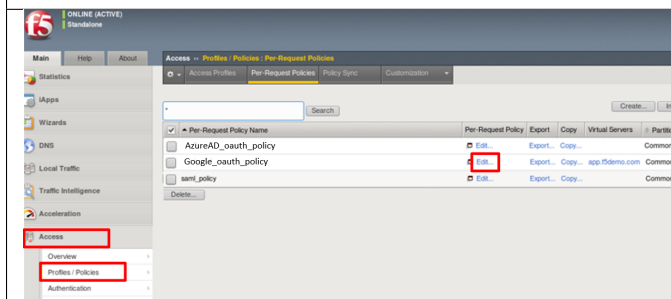
9. The various Per-Request-Policy actions can be reviewed
Note: Other actions like Step-Up Auth controls can be performed in a Per-Request Policy.

TASK 8: Review OAuth Results

Refer to the instructions and screen shots below:

1. Review your Active Sessions (**Access** -> **Overview** -> **Active Sessions**).
2. You can review Session activity or session variable from this window or kill the selected Session.

3. Review your Access Report Logs (**Access** -> **Overview** -> **Access Reports**).

4. In the **Report Parameters window** click **Run Report**.

5. Look at the **SessionID** report by clicking the **Session ID** Link.

6. Look at the **Session Variables** report by clicking the **View Session Variables** link.
    Pay attention to the OAuth Variables.
Note: Any of these session variables can be used to perform further actions to improve security or constrain access with logic in the Per-Session or Per Request VPE policies or iRules/iRulesLX.

7. Review your Access Report Logs (**Access** -> **Overview** -> **OAuth Reports** ->
   Client/Resource Server).

6.5 Lab 4: oAuth and AzureAD Lab

The purpose of this lab is to familiarize the Student with the using APM in conjunction with Microsoft Azure
AD. Microsoft Active Directory Domain Services is offered by Microsoft Azure as a cloud service. This can
be used together with OpenID to log in to APM.

6.5.1 Objective:

- Gain an understanding of additional F5 OAuth features
- Deploy a working configuration using F5 APM and Microsoft Azure AD

6.5.2 Lab Requirements:

- All lab requirements will be noted in the tasks that follow
- Estimated completion time: 25 minutes

6.5.3 Lab 4 Tasks:

TASK 1: Create/Review New Application Registration

Refer to the instructions and screen shots below:

*Note: The following steps in this task can just be "REVIEWED". As setting up a free Azure
account requires the entry of billing information, setting up an account and performing the
steps below is a [REVIEW] task. For those desiring to set up an account refer to the
"APPENDIX: Setting up an Azure Development Account". For those with existing accounts
these steps may be followed if desired. For all others, simply review the steps in
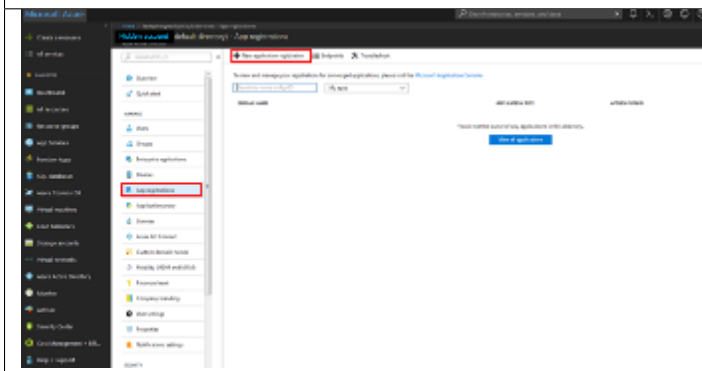Task1 and proceed to Task 2.*

[REVIEW]

1. Log into the Microsoft Azure Dashboard and click **Azure Active Directory** in the left
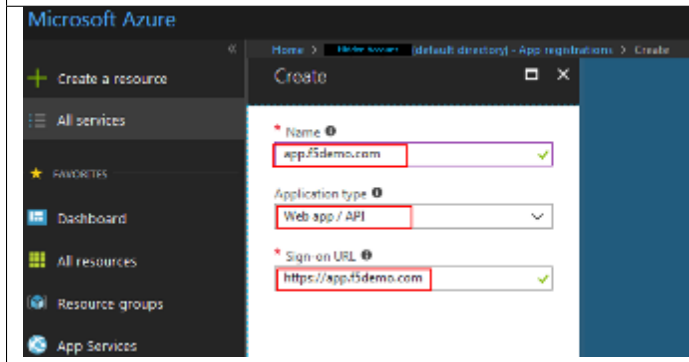   navigation menu.
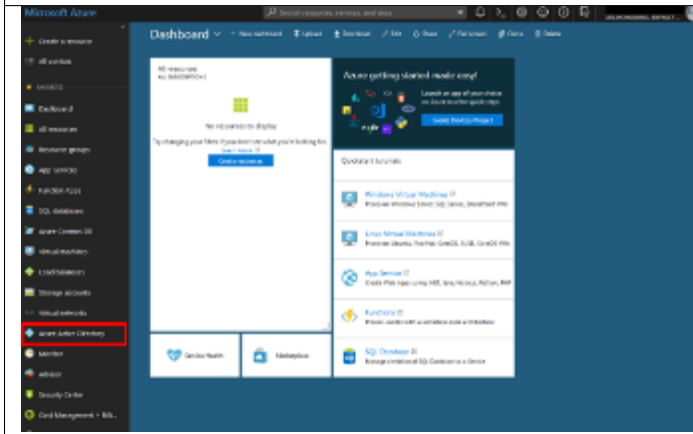
[REVIEW]

2. Click on **App Registration** on the resulting menu and then
   **New Application Registration** on the flyout menu.

[REVIEW]

3. In the pop menu for **Create App Registration**, enter the following values
   - **Name: app.f5demo.com**
   - **Application Type: Web App /API**
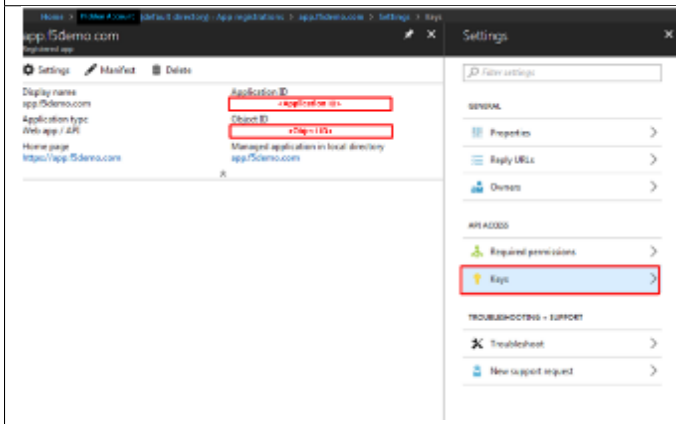   - **Sign On URL: https://app.f5demo.com**
4. Click **Create**.

[REVIEW]

5. In the resulting **app.f5demo.com Registered App** window, note & copy the **Application ID**. This will be used in a later setup step
6. Click **Settings**.
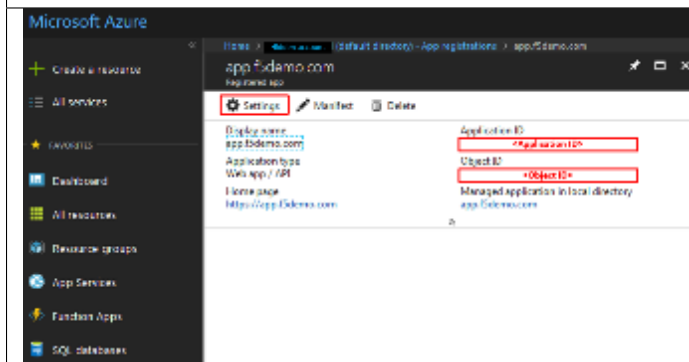
[REVIEW]

7. In the **Settings** flyout panel, click **Keys**

[REVIEW]

8. In the **Keys** flyout panel, enter the following values
   - **Description: app.f5demo.com**
   - **Expires: In 2 Years**
9. Click **Save**.
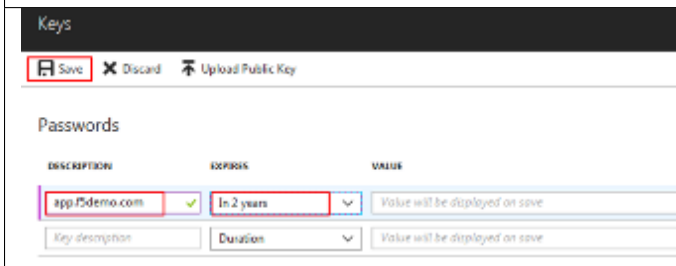
[REVIEW]

10. Note the message provided by Azure in the **Keys** panel.
11. Copy the ***Key Value*** for use in a later setup step.
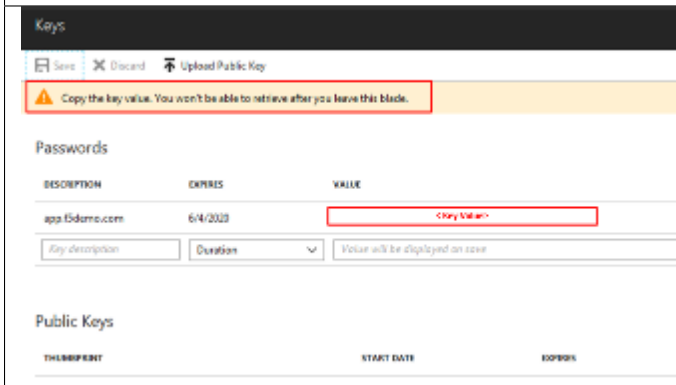
[REVIEW]

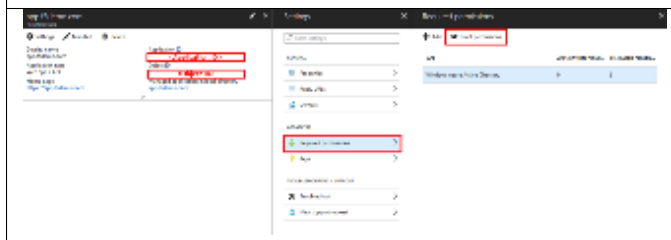   12. In the **Settings** flyout panel, click **Reply URL**.
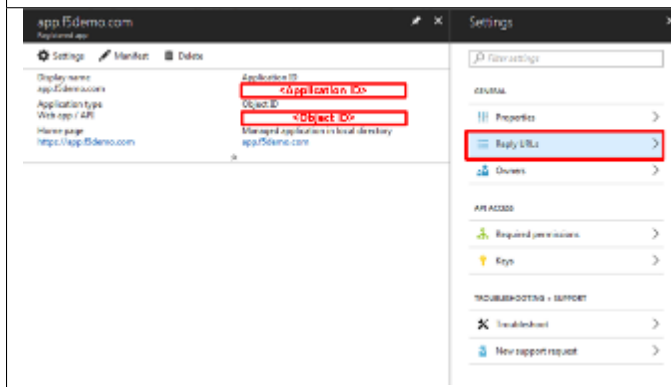
[REVIEW]

    13. In the **Reply URL** flyout panel, enter
        https://app.f5demo.com/oauth/client/redirect
    14. Click **Save**.
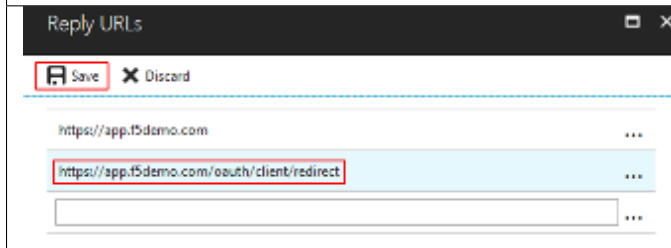
[REVIEW]

    15. In the **Settings** flyout panel, click **Required Permissions**
   16. In the **Required Permissions** flyout panel, click **Grant Permissions**

[REVIEW]

17. The following **Required Permissions** dialogue box may appear.
18. Click **Yes** to proceed.
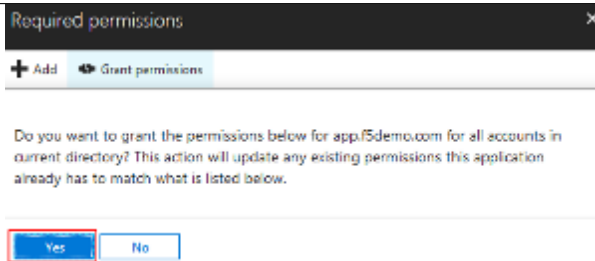
[REVIEW]

19. In the **Required Permissions** flyout panel, click **Windows Azure Active Directory**.
20. In the **Enable Access** flyout panel, ensure the **Sign In and Read User Profile**. permission is checked.
21. Click **Save**.
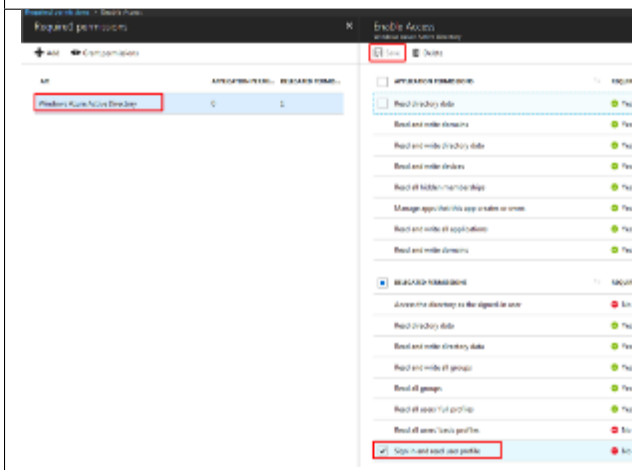
[REVIEW]

22. In the **Registered Application** panel, click **Manifest**.
23. In the **Edit Manifest** flyout panel, edit the **groupMembershipClaims** line (line 7) from **null** to **"All"** (note quotes are required).
24. Click **Save**.

Note: You can also update groupMembershipClaims to be "SecurityGroup".
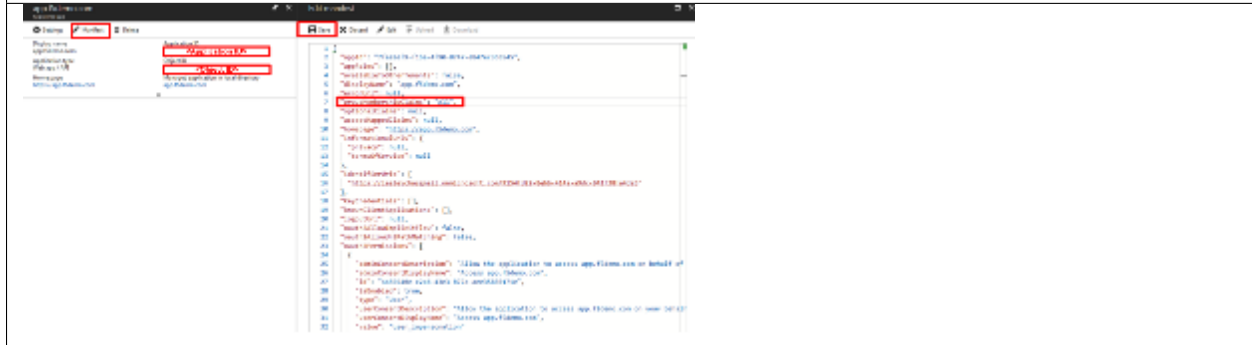
TASK 2: Create OAuth Request

Refer to the instructions and screen shots below:

1. Create the **OAuth Request** by navigating to **Access** -> **Federation** -> **OAuth Client/Resource Server** -> **Request** and clicking **Create**
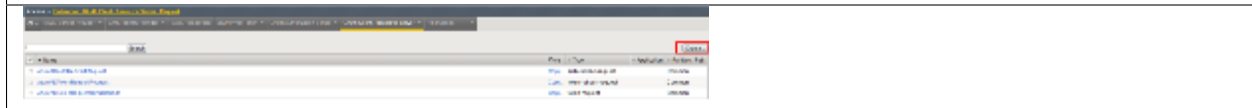
2. Use the following values to create the Request
   - **Name: Azure_AD_Token**
   - **HTTP Method: POST**
   - **Type: token-request**
3. Create the following Request Parameters using the Parameter Type drop down:
   - **Parameter Type: client-id**
   - **Parameter Name: client_id** (notice _)
   - **Parameter Type: client-secret**
   - **Parameter Name: client_secret** (notice _)
   - **Parameter Type: grant-type**
   - **Parameter Name: grant_type** (notice _)
   - **Parameter Type: redirect-uri**
   - **Parameter Name: redirect_uri** (notice _)
   - **Parameter Type: custom**
   - **Parameter Name: resource**
   - **Parameter Value: dd4bc4c7-2e90-41c9-9c41-b7eab5ab68b7**
4. Click **Finished**.

TASK 3: Create OAuth Provider

Refer to the instructions and screen shots below:

1. Create the **OAuth Provider** by navigating to **Access** -> **Federation** -> **OAuth Client/Resource Server** -> **Provider** and clicking **Create**.

2. Use the following values to create the Request
   - **Name**: **f5demo_AzureAD_Provider**
   - **Type**: **AzureAD**
   - **OpenID URI:** (replace **_tennantID_** with the following tenantID
     f5agilitydemogmail.onmicrosoft.com)

Resulting URI should be as follows:

https://login.windows.net/f5agilitydemogmail.onmicrosoft.com/.well-known/openid-configuration

3. Click **Discover**.
4. Click **Save**.

Note: if using another account you can find you TenantID by navigating to the "Azure Portal" and clicking "Azure Active Directory". The tenant ID is the "default directory" as shown. The full name of the TenantID will be your "TenantID.onmicrosoft.com"

TASK 4: Create OAuth Server

Refer to the instructions and screen shots below:

1. Create the **OAuth Server (Client)** by navigating to **Access** -> **Federation** -> **OAuth Client/Resource Server** -> **OAuth Server*** and clicking **Create**.
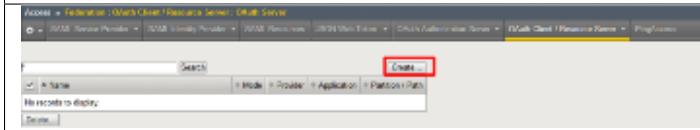
2. Using the following values to complete the OAuth Provider
   - **Name: f5demo_AzureAD_Server**
   - **Mode: Client**
   - **Type: AzureAD**
   - **OAuth Provider: f5demo_AzureAD_Provider**
   - **DNS Resolver: proxy_dns_resolver**
   - **Client ID: dd4bc4c7-2e90-41c9-9c41-b7eab5ab68b7**
   - **Client Secret: YqHbzTosdBxdaGl9A/hXCs1ex1HWi+BTUSkgcfhbTwA=**
   - **Client's Server SSL Profile Name: serverssl-insecure-compatible**
3. Click **Finished**.
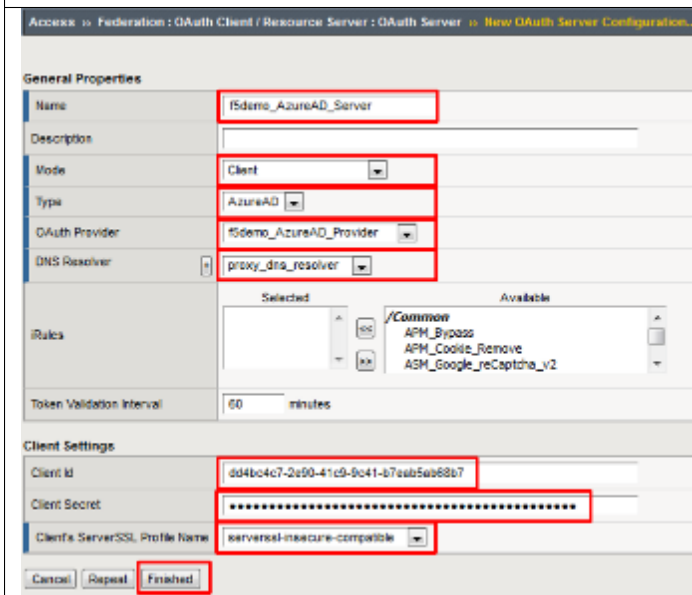
TASK 5: Setup F5 Per Session Policy (Access Policy)

Refer to the instructions and screen shots below:

1. Create the **Per Session Policy** by navigating to **Access** -> **Profile/Policies** -> **Access Profiles (Per Session Policies)** and clicking **Create**.

2. In the **New Profile** dialogue window enter the following values
   • **Name: AzureAD_OAuth**
   • **Profile Type: All**
   • **Profile Scope: Profile**
   • **Language: English**
3. Click **Finished**.
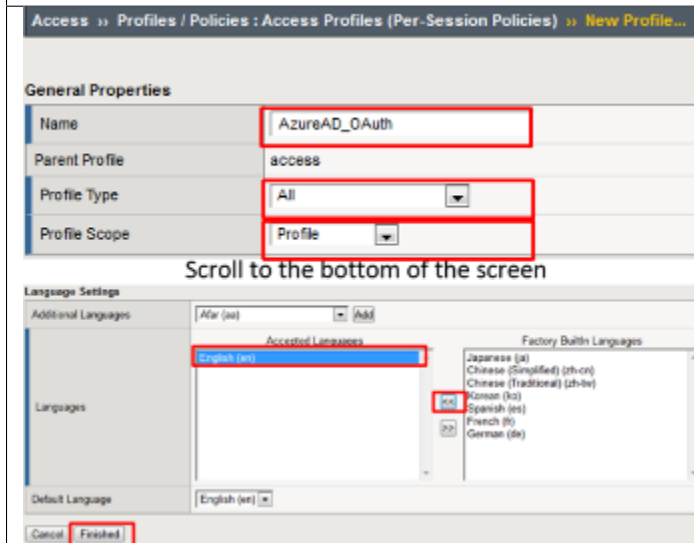
4. Click **Edit** link on for the **AzureAD_OAuth** Access Policy
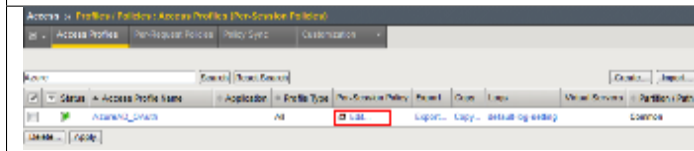
5. In the **AzureAD_OAuth** Access Policy, click the "**+**" between **Start** & **Deny**
6. Click the **Authentication** tab in the events window.
7. Scroll down and click the radio button for **OAuth Client**.
8. Click **Add Item**.
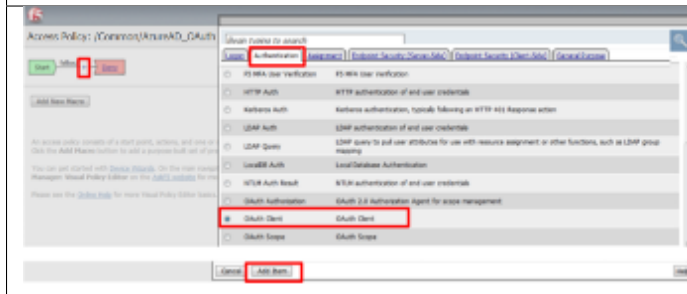
9. In the ***OAuth_Client*** window enter the following values as shown:
   - **Server: /Common/f5demo_AzureAD_Server**
   - **Grant Type: Authorization code**
   - **OpenID Connect: Enabled**
   - **OpenID Connect Flow Type: Authorization code**
   - **Authentication Redirect Request: /Common/AzureADAuthRedirectRequest**
   - **Token Request: /Common/Azure_AD_Token**
   - **Refresh Token Request: /Common/AzureADTokenRefreshRequest**
   - **OpenID Connect UserInfo Request: None**
   - **Redirection URI: https://%{session.server.network.name}/oauth/client/redirect**
10. Click **Save**.
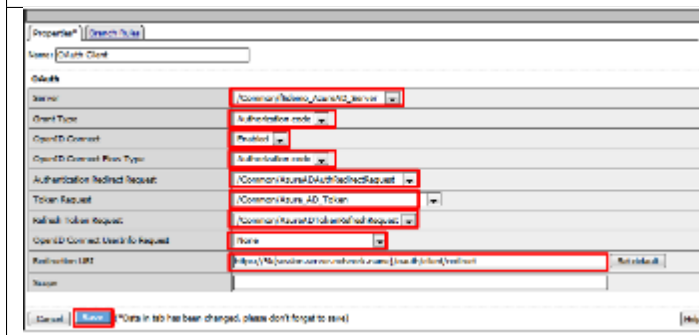
11. Click on the **Deny** link, in the **Select Binding**, select the **Allow** radio button
    and click **Save**.
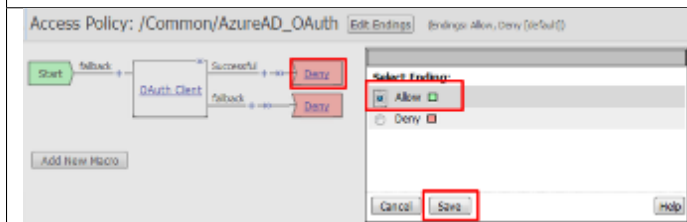
12. Click on the **Apply Access Policy** link in the top left-hand corner.
Note: Additional actions can be taken in the Per Session policy (Access Policy). The lab is simply completing authorization. Other access controls can be implemented based on the use case.

TASK 6: Associate Access Policy to Virtual Server

Refer to the instructions and screen shots below:

1. Navigate to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List** and click on the **app.f5demo.com** Virtual Server link
2. Scroll to the **Access Policy** section.

3. Use the **Access Profile** drop down to change the **Access Profile** to
   AzureAD_OAuth.
4. Use the **Per-Request Policy** drop down to change the **Per-Request Policy** to
   AzureAD_oauth_policy.
5. Scroll to the bottom of the **Virtual Server** configuration and click **Update**.

Access Policy

Access Profile	AzureAD_OAuth
Connectivity Profile	None
Per-Request Policy	AzureAD_oauth_policy

TASK 7: Test app.f5demo.com

Refer to the instructions and screen shots below:

1. Navigate in your provided browser to **https://app.f5demo.com**
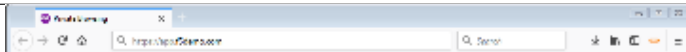
2. Authenticate with the following AzureAD account:
   • **Username: demouser@f5agilitydemogmail.onmicrosoft.com**
   • **Password: f5d3m0u$3r**
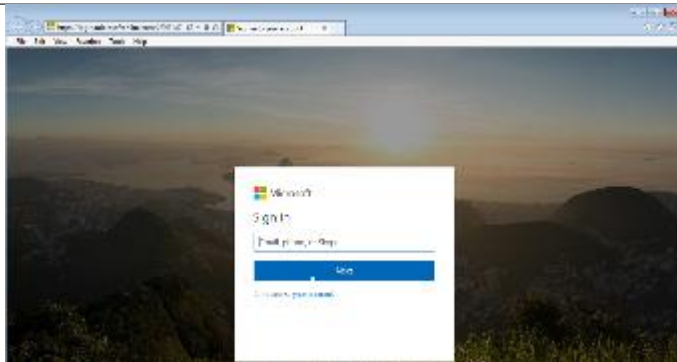
3. Did you successfully redirect to the AzureAD?
4. After successful authentication, were you returned to the app.f5demo.com?
5. Did you successfully pass your OAuth Token?

TASK 8: Per Request Policy Controls

Refer to the instructions and screen shots below:

1. As in the prior lab, you can experiment with Per Request Policy controls. In the
application page for **https://app.f5demo.com** click the **Admin Link** shown.

2. You will receive an **Access to this page is blocked** (customizable) message with a reference. You have been blocked because you do not have access on a per request basis.
3. Press the **Back** button in your browser to return to **https://app.f5demo.com**.
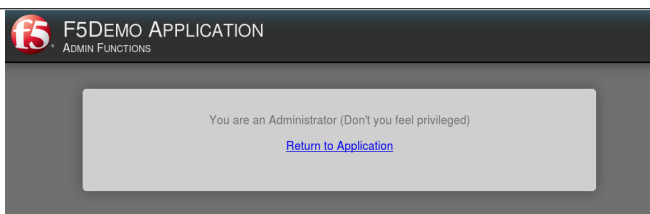

4. Navigate to **Local Traffic** -> **iRules** -> **Datagroup List** and click on the **Allowed_Users** datagroup.
5. Enter your **demouser@f5agilitydemogmail.onmicrosoft.com** used for this lab as the **String** value.
6. Click **Add** then Click **Update**.
Note: We are using a DataGroup control to minimize lab resources and steps. AD or LDAP Group memberships, Session variables, other user attributes and various other access control mechanisms can be used to achieve similar results.
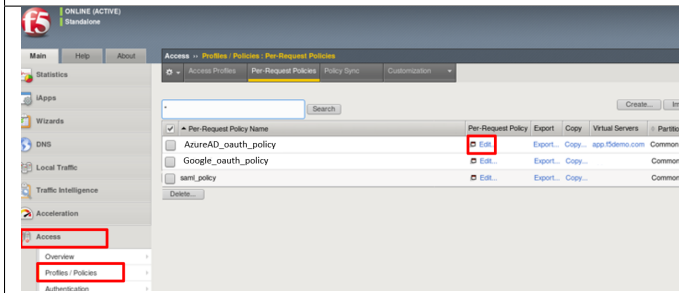

7. You should now be able to successfully to access the Admin Functions by clicking on the Admin Link.
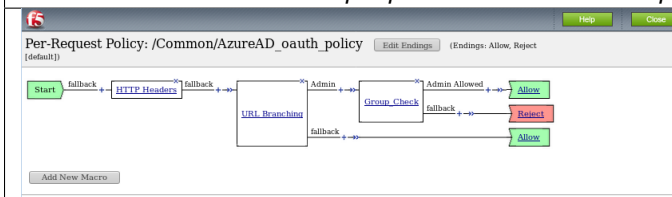*Note: Per Request Policies are dynamic and do not require the same "Apply Policy" action as Per Session Policies.*

8. To review the Per Request Policy, navigate to ***Access** -> **Profiles**/**Policies** ->
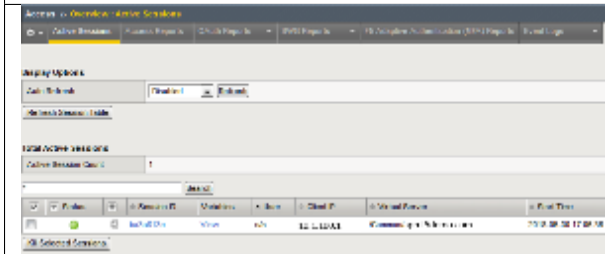   **Per Request Policies** and click on the Edit link for the **AzureAD_oauth_policy**.

9. The various Per-Request-Policy actions can be reviewed.
Note: Other actions like Step-Up Auth controls can be performed in a Per-Request Policy
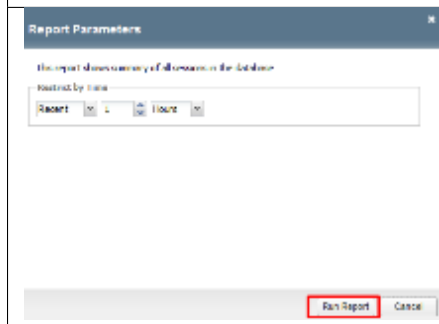

TASK 9: Review OAuth Results

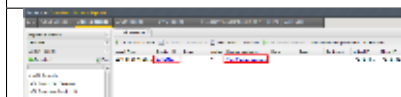Refer to the instructions and screen shots below:

1. Review your Active Sessions (**Access** -> **Overview** -> **Active Sessions**).
2. You can review Session activity or session variable from this window or kill the
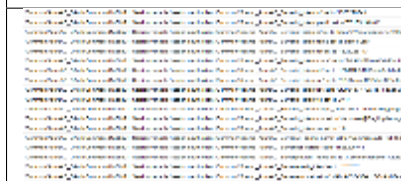   selected Session.

3. Review your Access Report Logs (**Access** -> **Overview** -> **Access Reports**).

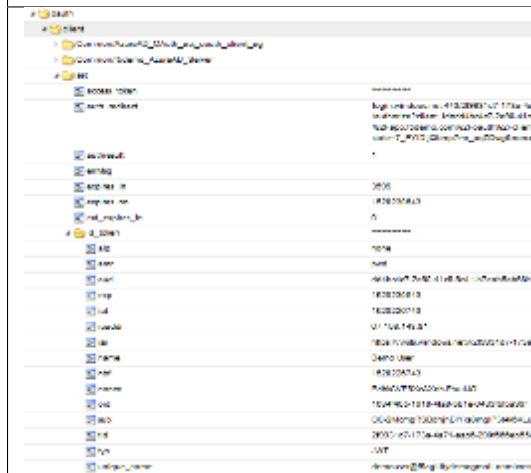4. In the **Report Parameters window** click **Run Report**.

5. Look at the **SessionID** report by clicking the **Session ID** Link.
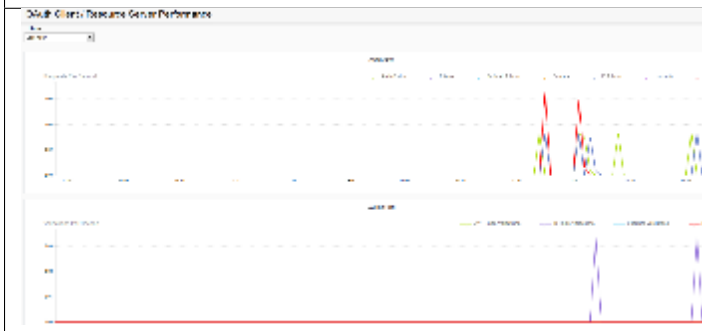

6. Look at the **Session Variables** report by clicking the **View Session Variables** link.
   Pay attention to the OAuth Variables.
Note: Any of these session variables can be used to perform further actions to improve
security or constrain access with logic in the Per-Session or Per Request VPE policies
or iRules/iRulesLX.

7. Review your Access Report Logs (**Access** -> **Overview** -> **OAuth Reports** -> **Client/Resource Server**).
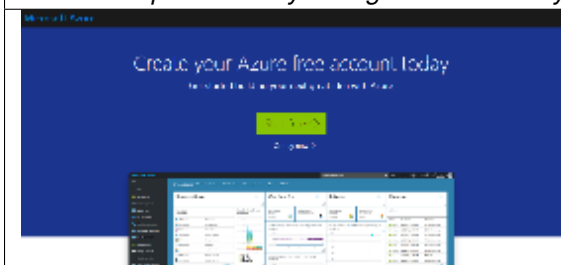

6.6 Conclusion

Thank you for your participation in the 330 Access Policy Manager (APM) Federation Lab. This Lab Guide has highlighted several notable features of SAML Federation. It does not attempt to review all F5 APM Federation features and configurations but serves as an introduction to allow the student to further explore the BIG-IP platform and Access Policy Manager (APM), its functions & features.

6.7 Appendix

6.7.1 Setting up an AzureAD Developer Account

The following steps are for informational purposes only and maybe subject to change based on Microsoft.

1. Navigate to the following URL to begin the process then follow the prompts as shown https://azure.microsoft.com/en-us/free/
2. The following images show the general flow to setup a free developer account
Note: This process may change as dictated by Microsoft

3. Initial Setup

4. About You

5. Identity Verification by Phone

2 Identity verification by phone

Country code

United States (+1)

Phone number

This field is required

[Text me] [Call me]

6. Identity Verification by Card

3 Identity verification by card

We keep prices low by verifying that account holders are real people, not bots or anonymous troublemakers. Don't worry, your card will not be charged unless you explicitly convert to a paid offer, though you may see a temporary authorization hold.

VISA [cards]

Card number

Expiration date   CVV

Month Year

Name on card

Address line 1

Address line 2
– Optional –

City

State   ZIP code

7. Agreement

4 Agreement

☐ I agree to the subscription agreement, offer details, privacy statement, and communications policy

I will receive information, tips, and offers about Azure, including Azure Newsletter and pricing updates, and other Microsoft products and services. privacy statement

[Sign up]

6.7.2 Links & Guides

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

- **Access Policy Manager (APM) Operations Guide:** https://support.f5.com/content/kb/en-us/products/big-ip_apm/manuals/product/f5-apm-operations-guide/_jcr_content/pdfAttach/download/file.res/f5-apm-operations-guide.pdf

- **Access Policy Manager (APM) Authentication & Single Sign on Concepts:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0.html

- **SAML:**

  - **Introduction:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/28.html#guid-28f26377-6e10-42c9-883a-3ac65eab9092

  - **F5 SAML IdP (Identity Provider with Portal):** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/29.html#guid-42e93e4b-e4fc-4c3d-ae53-910641d5755c

  - **F5 SAML IdP (Identity Provider without Portal):** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/30.html#guid-39ffed07-65f2-40b8-85ae-c80073cc4e82

  - **F5 SAML SP (Service Provider):** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/31.html#guid-be2cf224-727e-4a0f-aa68-676fdedba37b

  - **F5 Federation iApp (Includes o365):** https://www.f5.com/pdf/deployment-guides/saml-idp-saas-dg.pdf

  - **F5 o365 Deployment Guide:** https://www.f5.com/pdf/deployment-guides/microsoft-office-365-idp-dg.pdf

- **OAuth**

  - **OAuth Overview:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/35.html#guid-c1b617a7-07b5-4ad6-9b84-29d6ecd789b4

  - **OAuth Client & Resource Server:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/36.html#guid-c6db081e-e8ac-454b-84c8-02a1a282a888

  - **OAuth Authorization Server:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/37.html#guid-be8761c9-5e2f-4ad8-b829-871c7feb2a20

  - **Troubleshooting Tips**

    * **OAuth Client & Resource Server:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/36.html#guid-774384bc-cf63-469d-a589-1595d0ddfba2

    * **OAuth Authorization Server:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-sso-13-0-0/37.html#guid-8b97b512-ec2b-4bfb-a6aa-1af24842ee7a

- **Kerberos**

  - **Kerberos AAA Object**: (*See Reference section below*)

  - **Kerberos Constrained Delegation:** http://www.f5.com/pdf/deployment-guides/kerberos-constrained-delegation-dg.pdf

- **Two-factor Integrations/Guides** (**Not a complete list**)

  - **RSA Integration:** https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-12-1-0/6.html#conceptid

- **DUO Security:**
  - * https://duo.com/docs/f5bigip
  - * https://duo.com/docs/f5bigip-alt
- **SafeNet MobilePass:** http://www.safenet-inc.com/resources/integration-guide/data-protection/ SafeNet_Authentication_Service/SafeNet_Authentication_Service__RADIUS_Authentication_ on_F5_BIG-IP_APM_Integration_Guide
- **Google Authenticator:** https://devcentral.f5.com/articles/two-factor-authentication-with-google-authenticator-an

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

F5 Networks, Inc. | f5.com

Class 7: Introduction to Universal Access

Welcome to the **F5 Identity and Access Management Solutions** lab at F5 Agility 2018

The content contained here leverages a full DevOps CI/CD pipeline and is sourced from the GitHub repository at https://github.com/f5devcentral/f5-agility-labs-iam. Bugs and Requests for enhancements can be made by opening an Issue within the repository.

This class will cover APM concepts and will guide students through configuration steps for the following common use cases:

- Remote access VPN services
- Web portals (Webtops) for publishing internal applications
- Using different authentication protocols
- Single-Sign-On (SSO) functionality

7.1 Lab Information

7.1.1 Login instructions

Please follow the instructions provided by the instructor to start your lab and access your jump host.

To access your dedicated student lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces (HTTPS, SSH).

1. Establish an RDP connection to your Jump Host and login with the following credentials:

    - User: **user**
    - Password: **Agility1**

2. Access the **BIG-IP** GUI **https://10.128.1.245** (you can double-click on the red "f5 Big-IP" shortcut icon on the Windows desktop).

3. Login into the BIG-IP Configuration Utility with the following credentials:

    - User: **admin**
    - Password: **admin**

Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

7.1.2 Lab Topology
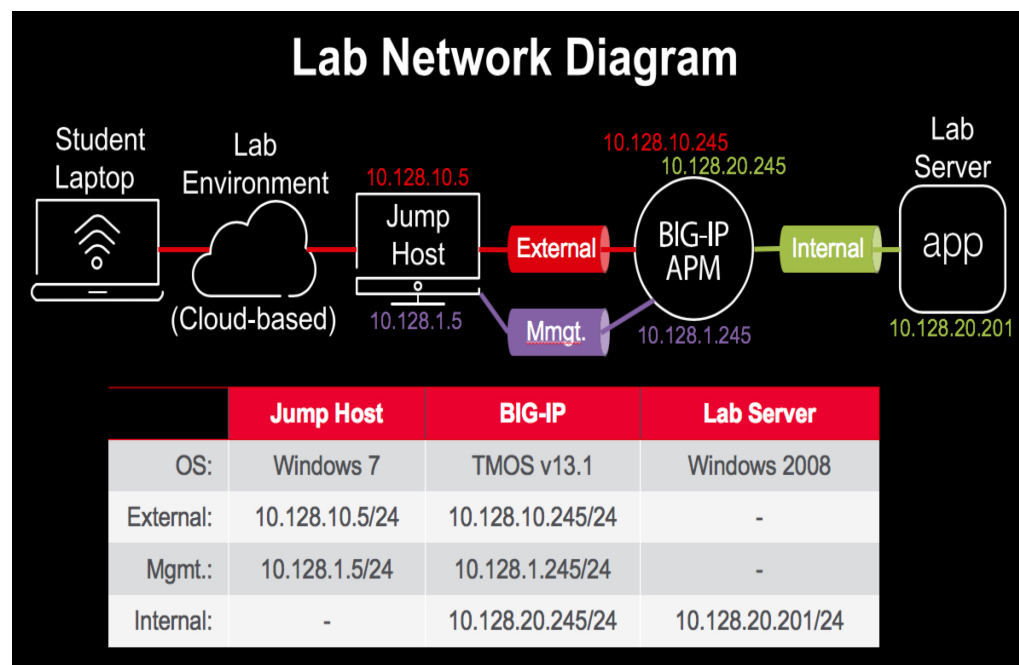
The following components have been included in your lab environment:

- 1 x F5 BIG-IP VE v13.1 (provisioned for Local Traffic Manager and Access Policy Manager)
- 1 x Windows Server running Active Directory and Web services
- 1 x Windows Jumphost

Note: The following entries have been added in the local hosts file of your Jumphost:

- 10.128.10.10 www.f5demo.com
- 10.128.10.11 myvpn.f5demo.com
- 10.128.20.200 www2.f5demo.com
- 10.128.10.11 webtop.f5demo.com
- 10.128.10.12 forms.f5demo.com
- 10.128.10.12 forms.f5demo.com
- 10.128.10.13 basic.f5demo.com
- 10.128.10.13 app1.f5demo.com
- 10.128.10.13 app2.f5demo.com
- 10.128.10.13 app3.f5demo.com
- 10.128.1.245 bigip1.f5demo.com

7.1.3 Lab Components

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
BIG-IP	• **Management:** 10.128.1.245 • **Internal:** 10.128.20.245 • **External:** 10.128.10.245	`admin/admin`
Jumphost	• **Management:** 10.128.1.5 • **External:** 10.128.10.5	`user/Agility1`
Lab Server	• **Internal:** 10.128.20.201	`administrator/Agility2018`

7.1.4 Labs Timing/Duration

The time it takes to perform each lab varies and is mostly dependent on accurately completing steps. Below is an estimate of how long it will take for each lab:

Lab name (Description)	Time Allocated
Lab 1 - Deploy a simple reverse proxy service	10 minutes
Lab 2 – Create My First Policy	15 minutes
Lab 3 – Configuring a VPN Policy	20 minutes
Lab 4 – Configuring an APM Webtop	10 minutes
Lab 5 – FORMS Based Authentication	15 minutes
Lab 6 – BASIC Authentication	15 minutes
Lab 7 – Single-Sign-On Across Authentication Domains	20 minutes

7.2 Lab 1 – Deploy a simple reverse proxy service

This lab will teach you how to configure resources including Virtual Servers, Pools, and monitors that we will use as the foundation for subsequent labs.

Note: Lab Requirements:

- BIG-IP with APM licensed and activated
- Web site up and running at 10.128.20.200:80, 10.128.20.201:80 and 10.128.20.202:80

7.2.1 Task – Create a pool

Follow these steps to complete this task:

1. Browse to **Local Traffic > Pools** and click the '**+**' next to **Pools List** to create a new pool.

2. Name the pool in "**http_pool**"

3. Assign the monitor "**http**" by selecting it and sliding it to the left.

4. **Add** the following "new node" members to the pool, then click **Finished**:

   - Node Name: **server1**, Address: **10.128.20.200**, Service Port **80**

   - Node Name: **server2**, Address: **10.128.20.201**, Service Port **80**

   - Node Name: **server3**, Address: **10.128.20.202**, Service Port **80**

7.2.2 Task - Create HTTP Virtual Server to redirect to HTTPS

1. Create a new Virtual Server by browsing to **Local Traffic** > **Virtual Servers** > **Virtual Server List** and click the '**+**' to create a new one.

2. Name the Virtual Server in the following format **http_vs_redir**. For "Destination Address/Mask", use **10.128.10.10**". For "Service Port", use **80**.

3. For "HTTP Profile" choose the default http profile called **http**

4. Under iRules at the bottom of the screen, select the **sys_https_redirect** irule from the "Available" list and slide it over to the "Enabled" list and click **Finished**.

7.2.3 Task - Create HTTPS Virtual Server

1. Create a new Virtual Server by browsing to **Local Traffic** > **Virtual Servers** > **Virtual Server List** and click the '**+**' to create a new one.

2. Name the Virtual Server in the following format **https_vs** .

3. For "Destination Address/Mask", use **10.128.10.10**. For "Service Port", use **443**.

4. For "HTTP Profile", choose the default **http** profile

5. For "SSL Profile (Client)", choose the **f5demo**, slide it over to the "Selected" column

6. For "Source Address Translation", choose **Auto Map**

7. For "Default Pool", select the pool created earlier (**http_pool**) and click **Finished**.

7.2.4 Task - Testing

You should now be able to browse to either Virtual Server (HTTP or HTTPs) and you should get the same page. Try: **http://www.f5demo.com** and **https://www.f5demo.com**
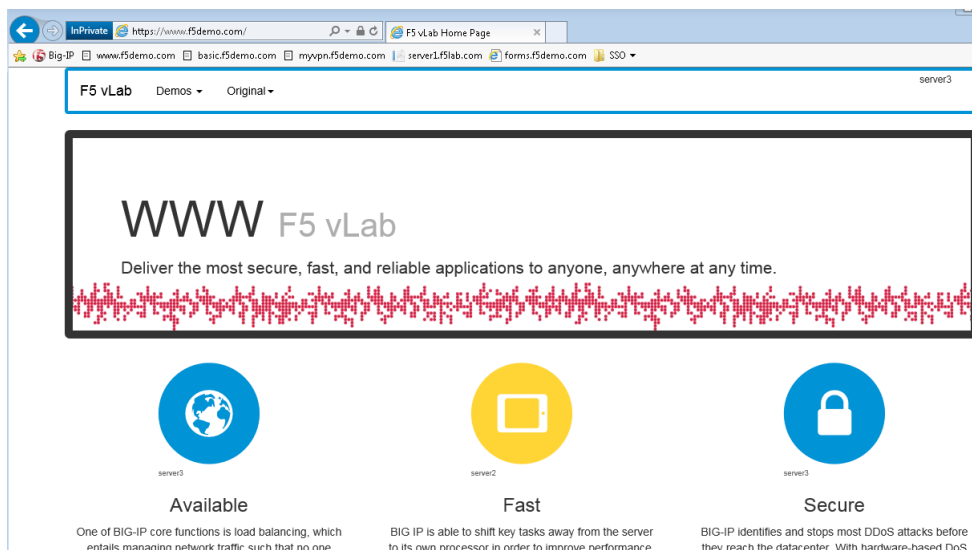
7.3 Lab 2 – Create My First Policy

In this lab, we will use the resources configured in the previous lab and configure a simple Access Profile using the Visual Policy Editor (VPE) to perform user authentication.

Note: Lab Requirements:

- Working HTTP and HTTPS Virtual Servers (from previous lab)

7.3.1 Task – Define an Authentication Server

Before we can create an access profile, we must create the necessary AAA server profile for our Active Directory.

Follow these steps to complete this task:

1. From the main screen, browse to **Access > Authentication > Active Directory**

2. Click **Create...** in the upper right-hand corner

3. Configure the new server profile as follows, then click **Finished**:

    - Name: **Lab_SSO_AD_Server**
    - Domain Name: **f5demo.com**
    - Server Connection: **Direct**
    - Domain Controller: **10.128.20.200**

7.3.2 Task – Create a Simple Access Profile

1. Navigate to **Access > Profiles / Policies > Access Profiles (Per-Session Policies)**

2. From the Access Profiles screen, click **Create. . .** in the upper right-hand corner

3. In the Name field, enter "**MyAccessPolicy**", and for "Profile Type", select the dropdown and choose **All**

4. Under "Language Settings", choose **English** and click the "<<" button to slide over to the "Accepted Languages" column.

5. Click **Finished**, which will bring you back to the Access Profiles screen.

6. On the Access Profiles screen, click the **Edit** link under the Per-Session Policy column. The Visual Policy Editor (VPE) will open in a new tab.

7. On the VPE page, click the '**+**' icon on the "fallback" path, to the right of the **Start** object.

8. On the popup menu, choose the **Logon Page** radio button under the Logon tab.

9. Click **Add Item**.

10. Accept the defaults and click **Save**.

Now let's authenticate the client using the credentials to be provided via the "Logon Page" object.

11. Between the "Logon Page" and "Deny" objects, click the '**+**' icon.

Access Policy: /Common/MyAccessPolicy

12. Select **AD Auth** found under the **Authentication** tab, and click the **Add Item** button.

13. Accept the default for the **Name** and in the **Server** drop-down menu select the AD server created above: /**Common/LAB_SSO_AD_Server**, then click **Save**.

Properties*	Branch Rules

Name: AD Auth

Active Directory

Type	Authentication ▼
Server	/Common/Lab_SSO_AD_Server ▼
Cross Domain Support	Disabled ▼
Complexity check for Password Reset	Disabled ▼
Show Extended Error	Disabled ▼
Max Logon Attempts Allowed	3 ▼
Max Password Reset Attempts Allowed	3 ▼

14. On the "Successful" branch between the **AD Auth** and **Deny** objects, click on the word **Deny** to change the ending.
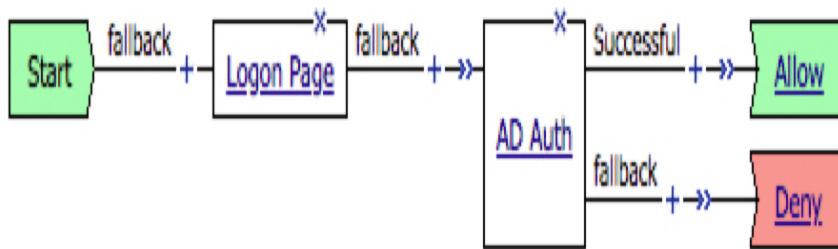

Add New Macro
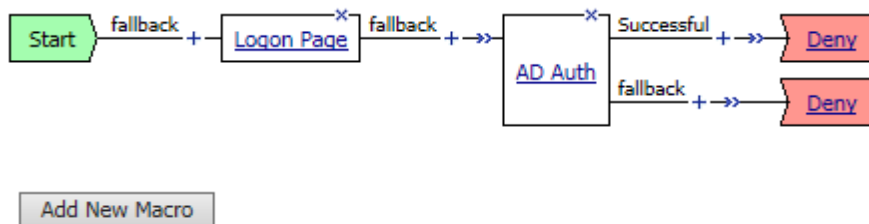
15. Change the "Successful" branch ending to **Allow**, then click **Save**.

Select Ending:

- ⦿ Allow ☐
- ○ Deny ▢

Cancel   Save   Help

16. In the upper left-hand corner of the screen, click on the **Apply Access Policy** link, then close the window using the **Close** button in the upper right-hand. Click **Yes** when asked "Do you want to close this tab?".

7.3.3 Task – Associate Access Policy to Virtual Servers

Now that we have created an access policy, we must apply it to the appropriate virtual server to be able to use it.

1. From the **Local Traffic** menu, navigate to the **Virtual Servers List** and click the name of the virtual server created previously: **https_vs**.

2. Scroll down to the "Access Policy" section, then for the "Access Profile" dropdown, select **MyAccessPolicy**.

3. Click **Update** at the bottom of the screen.

7.3.4 Task – Testing

Now you are ready to test.

1. Open a new browser window and open the URL for the virtual server that has the access policy applied: **https://www.f5demo.com**. You will be presented with a login window.
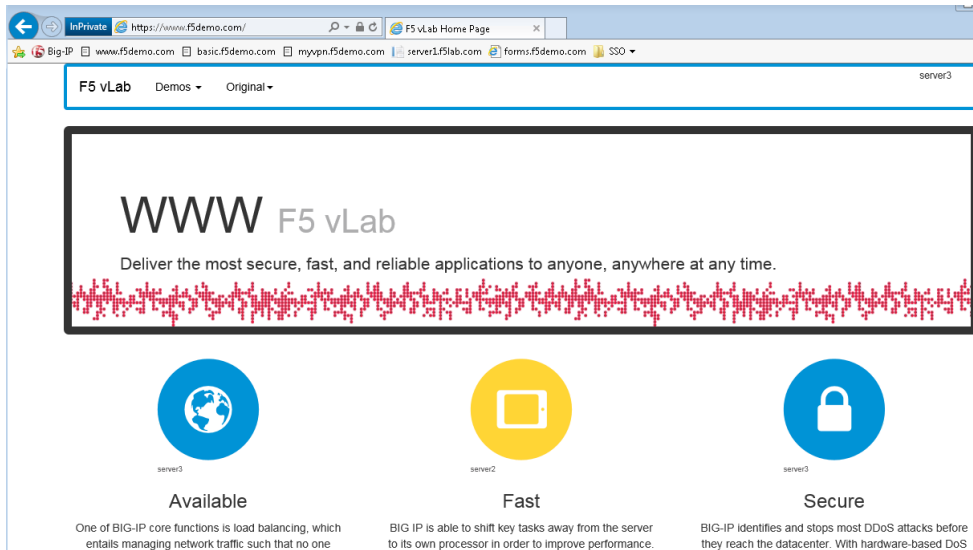

2. Enter the following credentials and click **Logon**:

    • Username: **user**

    • Password: **Agility1**

    You will see a screen similar to the following:

7.4 Lab 3 – Configuring a VPN Policy

In this lab, we will use the Device Wizard to configure a new SSL VPN service with the necessary Network Access Resources on APM.


Note: Lab Requirements:

- BIG-IP with APM licensed and activated
- Server running AD and Web services
- Local Host file entries on the Jump Host

7.4.1 Task – Use the Wizard to create a new Remote Access service

The Wizard simplifies configuration tasks for specific use cases.

1. From the main menu on the left side of the screen, browse to the **Wizards > Device Wizards** and select the radio button for "**Network Access Setup Wizard for Remote Access**".
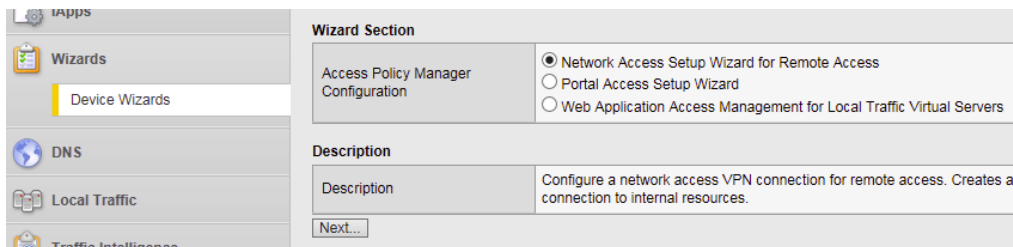
2. Click **Next**.

3. For the Policy Name field, enter **MyVPNPolicy**. This should auto populate the caption field. **Uncheck** the "**Enable Antivirus Check in Access Policy**" checkbox and click **Next**.

4. From the Select Authentication screen, choose the "**Use Existing**" radio button, select the AAA server "**Lab_SSO_AD_Server::Active Directory**" configured previously in Lab 2 and click **Next**.

5. Assign an IP Address Range to be used for the VPN connection on the "Configure Lease Pool" page. Click the radio button for "**IP Address range**" and enter the range "**10.1.1.1-10.1.1.2**", click **Add** and click **Next**.

6. On the "Configure Network Access" page, select "**Use split tunneling for traffic**" and for "IPV4 Lan Space", enter the network "**10.128.20.0**", mask "**255.255.255.0**", click **Add**, leave everything else default and click **Next**.

7. Accept the default on the "Configure DNS Hosts for Network Access" page and click **Next**.

Configure DNS Hosts for Network Access

Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers are used by the client when performing name resolution for internal network resources.

These settings may be different than the BIG-IP system settings configured under **System :** the navigation pane.

| IPV4 Primary Name Server | 10.128.20.200 ✕ |
| IPV4 Secondary Name Server | |

8. On the "Virtual Server (HTTPS connection)" page, enter "**10.128.10.11**" for the IP address of the Virtual Server that users will connect to for access to the VPN. **Uncheck** the "**Create Redirect Virtual Server**" option and click **Next**.

9. Verify your settings on the Review page and click **Next** when satisfied.

10. The Setup Summary page will display a list of the configuration objects that the Wizard created for you. Click **Finished**.

7.4.2 Task – Testing

1. Open a web browser to the virtual server created in the above step by navigating to **https://myvpn.f5demo.com**. You will be presented with a Logon page similar to the one from the last lab. |

2. Enter the following credentials:

Username: **user**

Password: **Agility1**

This will initialize, authenticate and establish a new VPN connection to the Network Resource that was configured. You will be presented with a new page that shows the connection details.

3. Open a new browser tab and confirm that you are now connected to the internal network by browsing directly to the HTTP server used in the pool for the previous labs: **http://server1.f5demo.com**. You should see a page similar to the following:
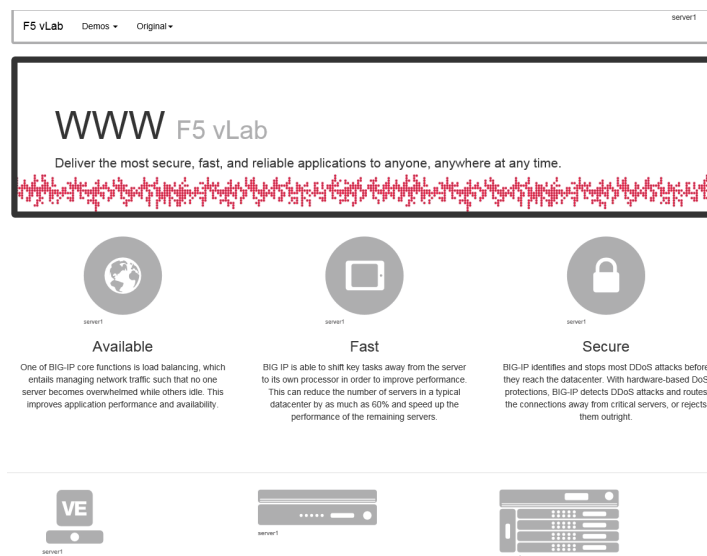
4. Close the page then click **Logout** on the F5 VPN page to terminate your VPN connection and close the browser window.

7.5 Lab 4 – Configuring an APM Webtop

In this lab, we will add a Webtop resource to the Access Policy created in the previous lab.

Note: Lab Requirements:

- Working HTTPS Virtual Server created in Lab 1 with Access Policy created in Lab 2 (Lab 2 successfully completed).

7.5.1 Task – Create a Webtop resource

1. Expand the **Access** tab from the main menu on the left and navigate to **Webtops** > **Webtop Lists**.

2. Click **Create** to create a new Webtop called **MyFullWebtop**, select Type "**Full**", uncheck "**Minmize To Tray**" and click **Finished**.

7.5.2 Task – Enable "Content Rewrite" on the Virtual Server

1. Browse to **Local Traffic** > **Virtual Servers > Virtual Server List** and click on the name of your VPN Virtual Server called **MyVPNPolicy_vs**.

2. Scroll down to the "Content Rewrite" section, select "**rewrite**" for the "Rewrite Profile" field and click **Update**.


7.5.3 Task – Add Webtop resource to existing Access Policy

1. Browse to **Access** > **Profiles** / **Policies > Access Profiles (Per-Session Policies)**, click on **Edit** for **MyVPNPolicy**. A new tab should open to the Visual Policy Editor for **MyVPNPolicy**.
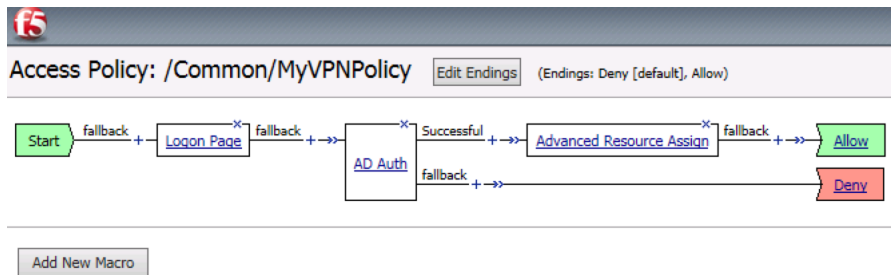
2. Select the **Advanced Resource Assign** object.

3. Click **Add/Delete**.

4. Click on the **Webtop** tab, select the radio button for **MyFullWebtop**, then click the **Update** button at the bottom of the screen.
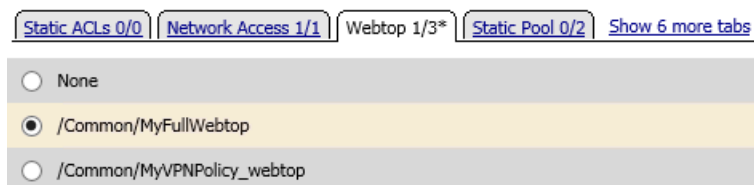

5. Click **Save**.

6. At the top left of the browser window, click on "**Apply Access Policy**", then close the tab.

7.5.4 Task – Testing

1. Open a web browser to the virtual server created in the previous lab by navigating to **https://myvpn.f5demo.com**. You will be presented with a Logon page similar to the one from the last lab.

2. Enter the following credentials:

   Username: **user**

   Password: **Agility1**

3. Click **Logon**.

   This will open the APM Webtop landing page that shows the resources you are allowed to access. In this lab, we've only configured one resource: **Network Access**, but you can add as many as you want and they will appear on this Webtop page.
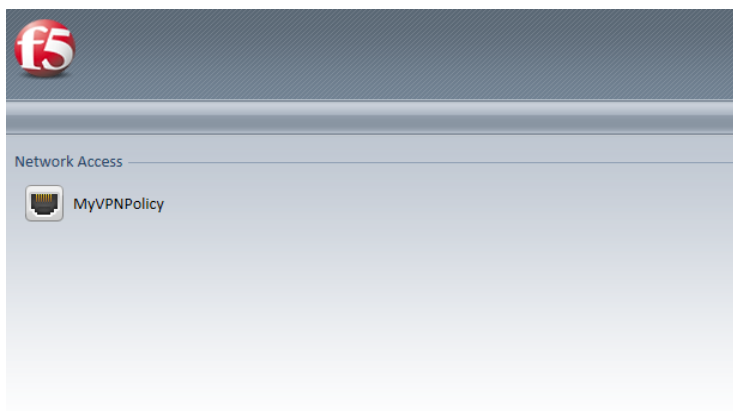
7.6 Lab 5 – FORMS Based Authentication

In this lab, we will show you how to configure APM to leverage SSO functionality with an application server that uses forms based authentication.

Note: Lab Requirements:

- BIG-IP with APM licensed and activated
- Server running AD and Web services
- Local Host file entries on the Jump Host

7.6.1 Task – Create a Pool

1. Browse to **Local Traffic > Pools** and click the '**+**' next to **Pools List** to create a new pool.

2. Name the pool "**forms_pool**"

3. Assign the monitor "**http**" by selecting the monitor and moving it to the left.

4. **Add** the following new member/node to the pool and click **Finished**:

    - Node Name: **forms**, Address: **10.128.20.204**, Service Port: **80**

7.6.2 Task – Create a Virtual Server

1. Browse to **Local Traffic > Virtual Servers** and click the '**+**' next to **Virtual Server List** to create a new one.

2. Use the following information to create the virtual server and leave the other settings at their default values, then click **Finished**:

   - Name the pool "**forms_vs**"

   - Destination Address/Mask: **10.128.10.12**

   - Service Port: **443**

   - HTTP Profile: **http**

   - SSL Profile (Client): **f5demo**

   - Source Address Translation: **Auto Map**

   - Default Pool: **forms_pool**

7.6.3 Task – Testing without APM

Observe the current behavior of the login page without authentication enforced by APM.

1. Open your web browser and go to **https://forms.f5demo.com**. You should see a page that looks as follows:

2. Log in with the following credentials:

   Username: **user**

   Password: **Agility1**

   Once successfully logged in you should see a web page similar to the following:

F5 Agility 2018

Hello, user! Logout
Home

Home Page. Welcome to F5 Agility. You ARE authenticated!!!

To learn more about Access Policy Manager visit https://f5.com/products/modules/access-policy-manager .

**Centralized, Secure Application Access Anytime, Anywhere**

BIG-IP Access Policy Manager (APM) secures and differentiates access to your applications, data, network, and the cloud based on user identity and context. That means it gives you centralized control over who's able to access your network or cloud, which applications they can access, and the devices and locations from which they can access those apps. In short, BIG-IP APM unifies and enforces identity-based, context-aware, dynamic policy-driven application access control—regardless of the location of the user or the application.
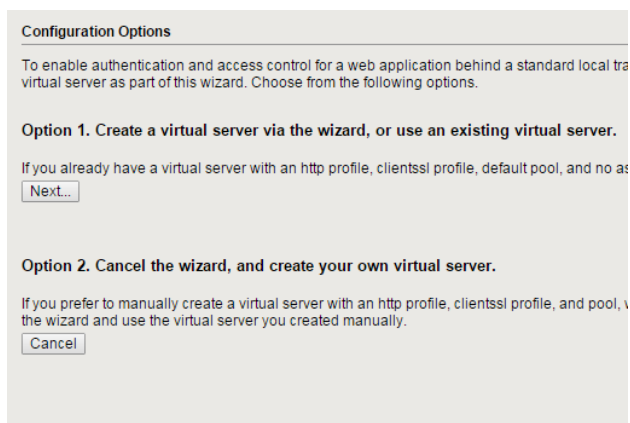
© 2018 - Agility

3. **Logout** using the link at the top right-hand corner of the page.

7.6.4 Task – Create Access Policy to use with Forms Based Authentication

1. Open the **Wizards > Device Wizards** page.

2. Select **Web Application Access Management for Local Traffic Virtual Servers**
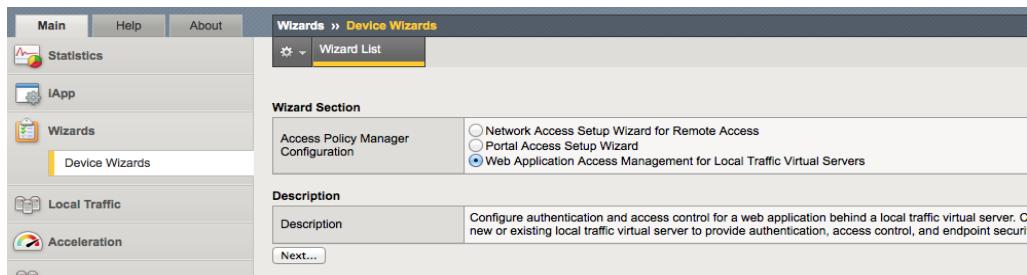
3. Click **Next**

4. Click **Next** for Option 1 on the Configuration Options page

5. Configure Basic Properties for the policy

   (a) For Policy Name enter **Forms_Access_Policy**

   (b) Uncheck **Enable Antivirus Check in Access Policy**

(c) Click **Next**

6. Configure the Authentication type used for this new policy

    (a) Select **Use Existing** for the Authentication Options

    (b) Select **Lab_SSO_AD_Server::Active Directory**

(c) Click **Next**

7. Configure Single Sign On

    (a) Select "**Create New**" for "SSO Options"

    (b) Choose **Form Based** for the SSO Method

    (c) **Uncheck** the option for "Use SSO Template"

    (d) Enter /**Account**/**Login*** in the "Start URI" field

    (e) Enter /**Account**/**Login** in the "Form Action" field

    (f) Enter **UserName** in the "Form Parameter For User Name" field

    (g) Enter **Password** in the "Form Parameter For Password" field

(h) Click **Next**

8. Configure Virtual Server

   (a) Select Use **Existing HTTPS Server**

   (b) Choose /**Common**/**forms_vs** for the Virtual Server

   (c) Click **Next**

9. Review configuration and click **Next**

10. Review the "Setup Summary", which shows all (existing and new) objects associated with this new policy and click **Finished**.

11. Add a logout URI Include to the new access policy

   (a) Open the **Access > Profiles** / **Policies > Access Profiles (Per-Session Policies)** page

   (b) Click on the name of the new policy **Forms_Access_Policy**

   (c) **Add** "/**Account**/**Logout**" to the "Logout URI Include" field

   (d) Change **Logout URI Timeout** to **1** second

(e) Click **Update**

12. Enable SSO

    (a) Click on the "SSO / Auth Domains" tab

    (b) For "SSO Configuration", select **Forms_Access_Policy_sso**

    (c) Click **Update**

7.6.5 Task – Applying Access Policy Changes

After you create or change an access policy, the link Apply Access Policy appears in yellow at the top left of the BIG-IP Configuration utility screen. You must click this link to activate the access policy for use in your configuration.
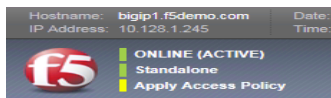
1. Click the **Apply Access Policy** link, which will bring you to the Apply Access Policy screen, with a list of access policies that have been changed.

2. Select the new Access Policy and click the **Apply** button (by default, all access policies that are new or changed are selected).
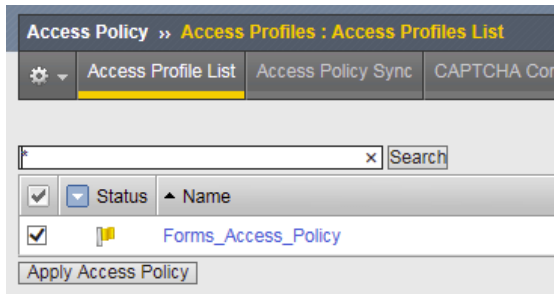
After you apply the access policy, the Access Profiles list screen is displayed.

7.6.6 Task – Testing with APM Authentication

Observe the behavior of the login page now that authentication is enforced by APM.

1. Open your web browser and go back to **https://forms.f5demo.com**. You should see a page that looks like the following:
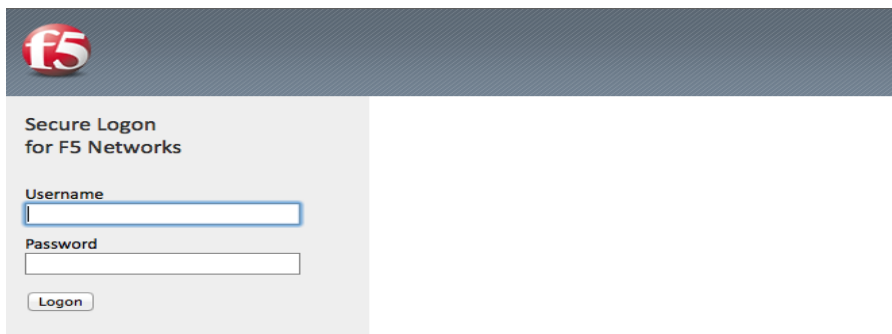
2. Logon with the following credentials:

   Username: **user**

   Password: **Agility1**

   Once successfully logged in you will see the same web page observed in task 2:

7.6.7 Task – Testing Logout

Earlier in Task 3, Step 9, we defined a **Logout URI Include** for this Access Policy. This is a list of logoff URIs that the access profile searches for in order to terminate the Access Policy Manager session. The URI we used was /Account/Logout, and the default logout delay is 5 seconds, which was modified to 1 second.

1. Logout using the **Logout** link at the top right-hand corner of the page.

2. Wait 1 second

3. Click the Home link in the banner at the top of the page

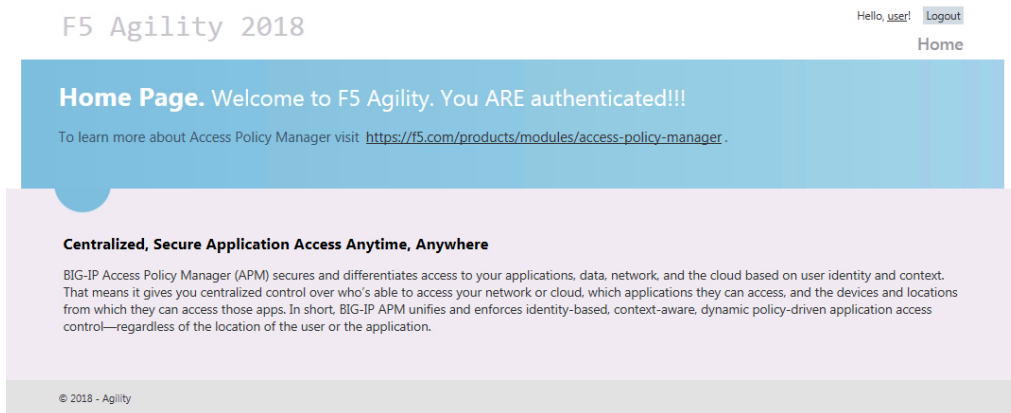4. You should be redirected back to the F5 logon page

7.7 Lab 6 – BASIC Authentication

In this lab, we will show you how to configure basic authentication leveraging the SSO functionality of APM.

Note: Lab Requirements:

- BIG-IP with APM licensed and activated

- Server running AD and Web services

- Local Host file entries on the Jump Host

7.7.1 Task – Create a Pool

1. Browse to **Local Traffic > Pools** and click the '**+**' next to **Pools List** to create a new pool.

2. Name the pool "**basic_pool**"

3. Assign the monitor "**http**" by selecting the monitor and moving it to the left.

4. **Add** the following "New Member/Node" to the pool and click **Finished**:

     - Node Name: **basic**, Address: **10.128.20.203**, Service Port: **80**

7.7.2 Task 2: Create a Virtual Server

1. Browse to **Local Traffic > Virtual Servers** and click the '**+**' next to **Virtual Server List** to create a new one.

2. Use the following information to create the virtual server and leave other settings as default, then click **Finished**:

   - Name the pool "**basic_vs**"
   - Destination Address: **10.128.10.13**
   - Service Port: **443**
   - HTTP Profile: **http**
   - SSL Profile (Client): **f5demo**
   - Source Address Translation: **Auto Map**
   - Default Pool: **basic_pool**

7.7.3 Task 3: Testing without APM

Observe the current behavior of the login page without APM authentication.

1. Open a private browsing window and go to **https://basic.f5demo.com**. You should receive a prompt that looks similar to the following screen shot:
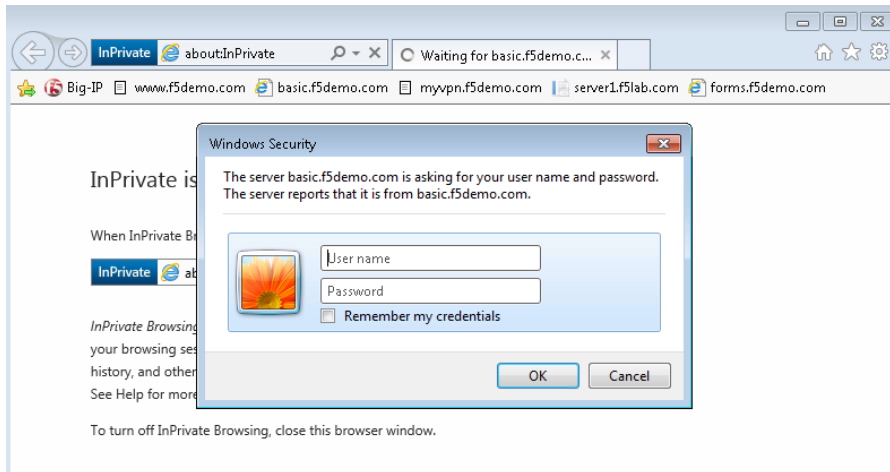
2. Enter the following credentials:

  • Username: **user**

  • Password: **Agility1**

3. Once successfully logged in you will see a webpage similar to this one:
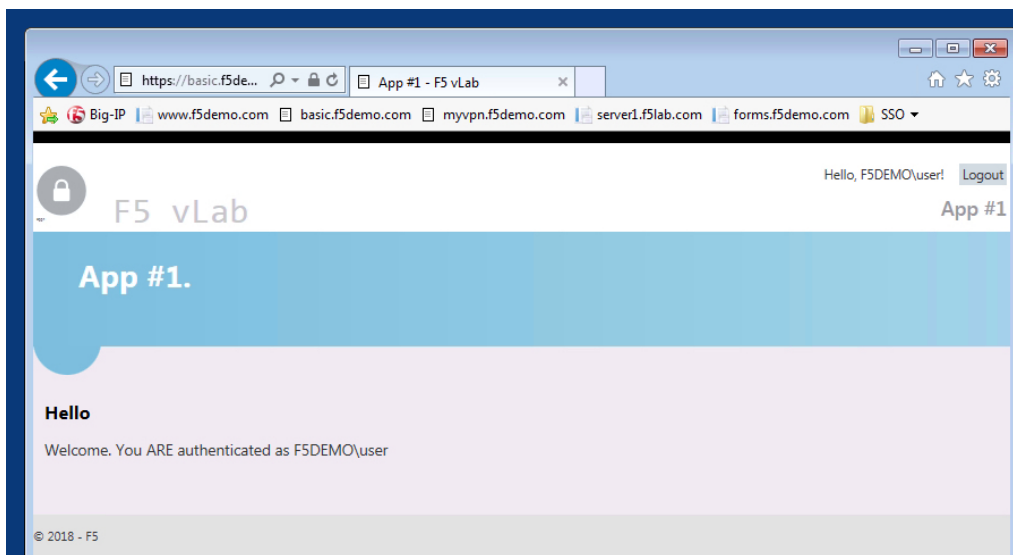
4. Close the private browsing window.

7.7.4 Task 4: Create Access Policy to use with Basic Authentication

1. Open the **Wizards > Device Wizards** page.

  (a) Select **Web Application Access Management for Local Traffic Virtual Servers**
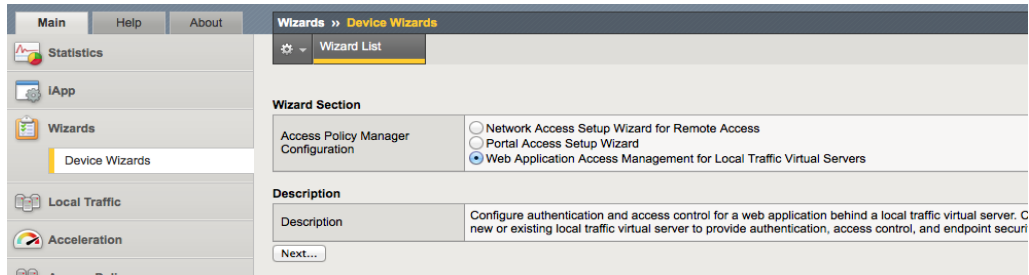
   (b) Click **Next**

2. Click **Next** for Option 1 on the Configuration Options page
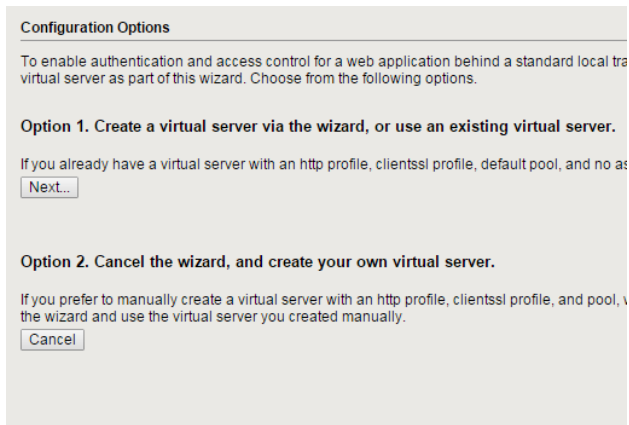
3. Configure Basic Properties for the policy

   (a) For Policy Name enter **Basic_Access_Policy**

   (b) **Uncheck** "Enable Antivirus Check in Access Policy"

   (c) Click **Next**

4. Configure Authentication type used for policy

   (a) Select **Use Existing** for the "Authentication Options"

   (b) Select **Lab_SSO_AD_Server::Active Directory**

(c) Click **Next**

5. Configure SSO

   (a) Select **Create New** for the "SSO Options"

   (b) Choose **HTTP Basic**

   (c) Click **Next**

6. Configure Virtual Server

   (a) Select Use **Existing HTTPS Server**

   (b) Choose /**Common**/**basic_vs** for the Virtual Server**

   (c) Click **Next**

7. Review configuration and click **Next**

8. Review the "Setup Summary", which shows all (existing and new) objects associated with this new policy.

9. Click **Finished**

10. Add a logout URI Include to the new access policy

    (a) Open the **Access > Profiles** / **Policies > Access Profiles (Per-Session Policies)** page

    (b) Click on the name of the new policy **Basic_Access_Policy**

    (c) **Add** "/**Home**/**Logout**" to "Logout URI Include"

    (d) Change **Logout URI Timeout** to **1** second

(e) Click **Update**

11. Enable the SSO Configuration

    (a) Click on the **SSO / Auth Domains** tab

    (b) For **SSO Configuration**, select **Basic_Access_Policy_sso**

    (c) Click **Update**

7.7.5 Task 5: Applying Access Policy

After you create or change an access policy, the link Apply Access Policy appears in yellow at the top left of the BIG-IP Configuration utility screen. You must click this link to activate the access policy for use in your configuration.
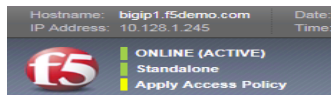
1. Click the **Apply Access Policy** link, which will bring you to the Apply Access Policy screen, with a list of access policies that have been changed.

2. Select the Access Policy and click the **Apply** button (by default, all access policies that are new or changed are selected).
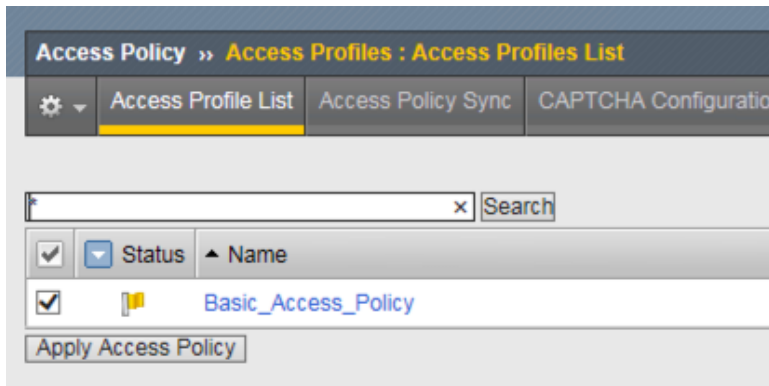
After you apply the access policy, the Access Profiles list screen is displayed.

7.7.6 Task 6: Testing with APM Authentication

Observe the behavior of the login page with authentication enforced by APM.

1. Open a private browsing window and go to **https://basic.f5demo.com**. You should see a page that looks like the following:
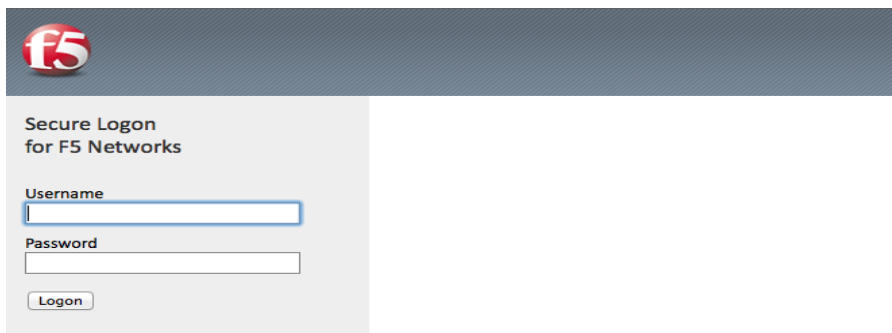
2. Logon with the following credentials:

   Username: **user**

   Password: **Agility1**

   Once successfully logged in you will see the same web page observed in task 3:
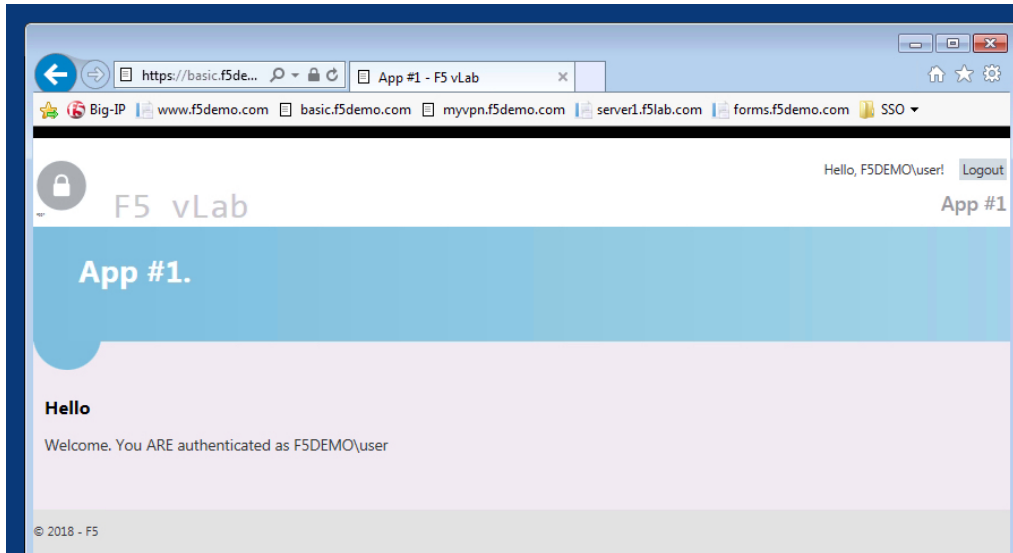
7.7.7 Task 7: Testing Logout

Earlier in Task 3, Step 9, we defined a **Logout URI Include** for this Access Policy. This is a list of logoff URIs that the access profile searches for in order to terminate the Access Policy Manager session. The URI we used was /Home/Logout, and the default logout delay is 5 seconds which was modified to 1 second.

1. Click the **Logout** link located at the top right of the web pagee

2. Wait 1 second

3. Click the "**App #1**" link in the banner at the top of the page

4. You should be redirected back to the F5 logon page

7.8 Lab 7 – Single-Sign-On Across Authentication Domains

In this lab, we will show you how to provide SSO across multiple applications. Normally APM will require authentication each time an application is accessed. By using a Domain Cookie it is possible to re-use an existing APM session to access multiple applications.

Note: Lab Requirements:

• Previous Labs 5 and 6 successfully completed

7.8.1 Task – Verify Authentication Required for different applications

1. Open a Private web browser or clear your browser cache and go to the Virtual Server used earlier **https://basic.f5demo.com**

2. You should be able to logon with the following credentials:

• Username: **user**

• Password: **Agility1**

3. Once successfully logged in, you will be presented with the same information page you observed earlier from basic.f5demo.com "App #1".

4. Now go to **https://app2.f5demo.com** you should be prompted to logon again.

5. You should be able to logon with the following credentials:

   • Username: **user**

   • Password: **Agility1**

6. Once successfully logged in, you will be presented with information about "App #2".

7. Logout and close the browser window.

7.8.2 Task - Specify Domain Cookie

1. Open the **Access > Profiles** / **Policies > Access Profiles (Per-Session Policies)** page

2. Click on the name of the policy **Basic_Access_Policy**

3. Click on the **SSO / Auth Domains** tab

4. Enter **f5demo.com** to **Domain Cookie**

5. Click **Update**

6. Don't forget to click on **Apply Access Policy** to put your changes in effect!

7.8.3 Task - Testing Authentication across domains

1. Open a Private web browser or clear your browser cache and go to the Virtual Server used earlier **https://basic.f5demo.com**

2. You should be able to logon with - Username: **user** - Password: **Agility1**

3. Once successfully logged in, you will be presented with the same information page you observed earlier.

4. Now go to **https://app2.f5demo.com**. You should not be prompted to logon again!

7.8.4 Task 4 (Bonus) - Authentication across domains & virtual servers

Repeat the previous steps, but for Forms_Access_Policy instead of Basic_Access_Policy.

Are you prompted for authentication when going from **https://forms.f5demo.com** to **https://basic.f5demo.com**?

Try changing the value for "Profile Scope" for **Basic_Access_Policy** and **Forms_Access_Policy** from Profile to **Global**

> ***Troubleshooting tips:**
>
> Did you forget to **Apply Access Policy** ?
>
> Verify the Domain Cookie configured on the SSO page... for both policies?

_8_

Class 8: Troubleshooting Universal Access

Welcome to the Troubleshooting Universal Access Lab. These lab exercises will instruct you on how to configure and troubleshoot common Access Policy Manager (APM) issues as experienced by field engineers, support engineers and customers. This guide is intended to complement lecture material provided during the course as well as a reference guide that can be referred to after the class as a basis for troubleshooting APM in your own environment.

Expected time to complete: **4 hours**

8.1 Getting Started

8.1.1 Timing for Labs

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

LAB Timing

LAB Name (Description)	Time Allocated
LAB 1: APM Troubleshooting Lab Object Prep (GUI) _Do EITHER Lab 1 OR Lab 2 (not both)_	20 minutes
LAB 2: APM Troubleshooting Lab Object Prep (TMSH) _Do EITHER Lab 1 OR Lab 2 (not both)_	20 minutes
LAB 3: General Troubleshooting	5 minutes
LAB 4: Visual Policy Editor (VPE) and Session Variables	20 minutes
LAB 5: Command Line Tools	25 minutes

8.1.2 General Notes

Provisioning Access Policy Manager (APM) is not required for basic Access Policy uses cases although this has been provisioned for you ahead of time. This was done to save time as provisioning often requires services to restart which takes away valuable lecture/lab time.

8.1.3 How to use this Guide

For each section, follow the instruction of the class moderator on when to begin. Carefully read and implement each item step by step.

Archives have been provided for each completed section and can be loaded if necessary at the beginning of each section for prior labs. You can install the UCS archive by using the **tmsh no-license** option. For the command syntax, refer to the following example:

```
tmsh load sys ucs [ucs file name] no-license
```

8.2 Lab Environment

8.2.1 Accessing the Lab Environment

To access the lab environment, you will require a web browser and Remote Desktop Protocol (RDP) client software. The web browser will be used to access the Lab Training Portal. The RDP client will be used to connect to the Jump Host, where you will be able to access the BIG-IP management interfaces (HTTPS, SSH).

Your class instructor will provide additional lab access details.

8.2.2 Lab Network Setup

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

- Cloud-based lab environment complete with Jump Host, Virtual BIG-IP (VE) and Lab Server
- Duplicate Lab environments for each student for improved collaboration
- Virtual BIG-IP has been pre-licensed and provisioned for Access Policy Manager (APM)

Note: All work for this lab will be performed exclusively from the Windows jump host. No installation or interaction with your local system is required.

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

8.2.3 LAB Environment Diagram

Lab Environment

VLAN	Subnet	Jump Host	BIG-IP VE (APM)	Lab Server
Management	10.128.1.0/24	10.128.1.1	10.128.1.245	N/A
External	10.128.10.0/24	10.128.10.1	10.128.10.245	N/A
Internal	10.128.20.0/24	10.128.20.1	10.128.20.245	10.128.20.100
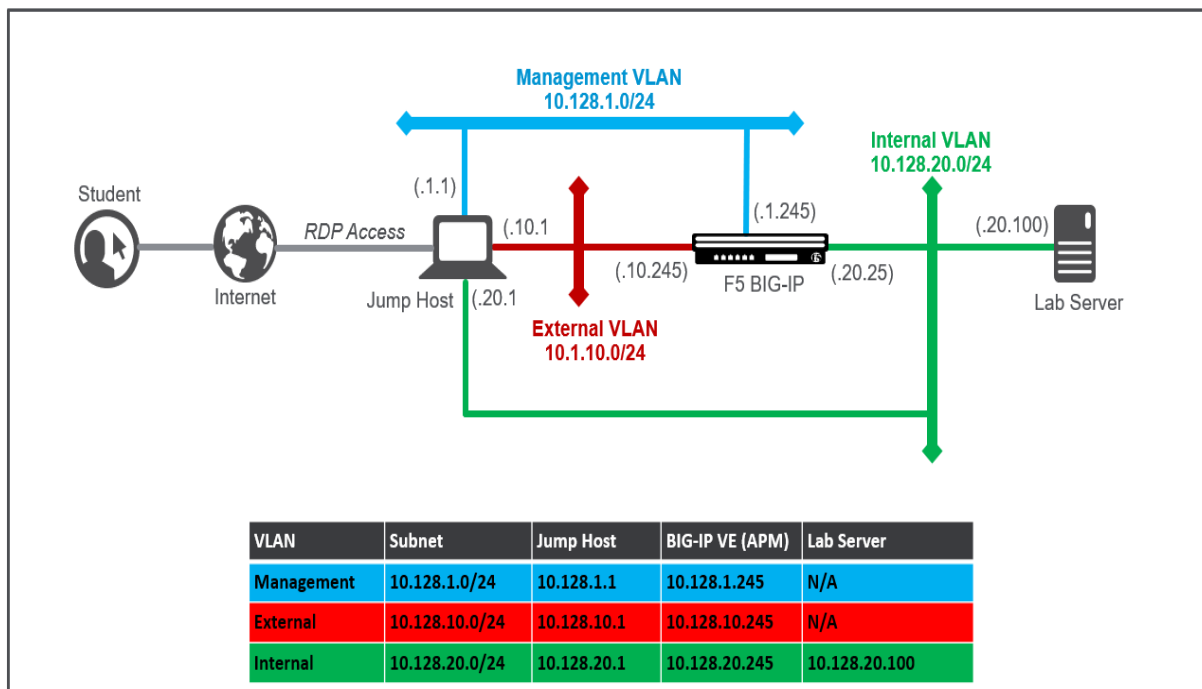
8.2.4 Lab Components

The following components have been included in your lab environment:

- 1 x Windows Jump Host
- 1 x F5 BIG-IP VE (v13.1)
- 1 x Windows Lab Server (AD/DNS/App)

The following table lists VLANS, IP Addresses and Credentials for all components:

Component	VLAN/IP Address(es)	Credentials
Jump Host	• **Management:** 10.128.1.1 • **Internal:** 10.128.20.1 • **External:** 10.128.10.1	`agility/Agility1`
BIG-IP VE	• **Management:** 10.128.1.245 • **Internal:** 10.118.20.245 • **External:** 10.118.10.245	`admin/admin`
Lab Server	• **Internal:** 10.128.20.100	`none`

8.3 Lab 1: APM Troubleshooting Lab Object Preparation (GUI)

Note: You only need to perform EITHER Lab 1 OR Lab 2. They accomplish the same goal, but using different methods. Lab 2 gets the Lab Preparation using TMSH

The purpose of this lab is to preconfigure some objects that will be used throughout the other labs. These objects are as follows:

- Domain Name Services (DNS) Resolver
- Network Time Protocol (NTP) Server
- Access Policy (APM) AAA Server – Active Directory
- Access Policy (APM) SSO Configuration – NTLMv1
- Access Policy (APM) Access Profile
- Local Traffic (LTM) Pool and Member
- Local Traffic (LTM) Virtual Server

8.3.1 Connect to the Lab

1. Establish an RDP connection to your Jump Host and double-click on the **BIG-IP** Chrome shortcut on the Windows desktop.

   - User: agility
   - Password: Agility1

2. Ignore the certificate warning.

3. Login into the BIG-IP Configuration Utility with the desktop icon (or Favorite link in Chrome) with the following credentials:

- User: **admin**
- Password: **admin**

8.3.2 DNS Resolver for System Configuration
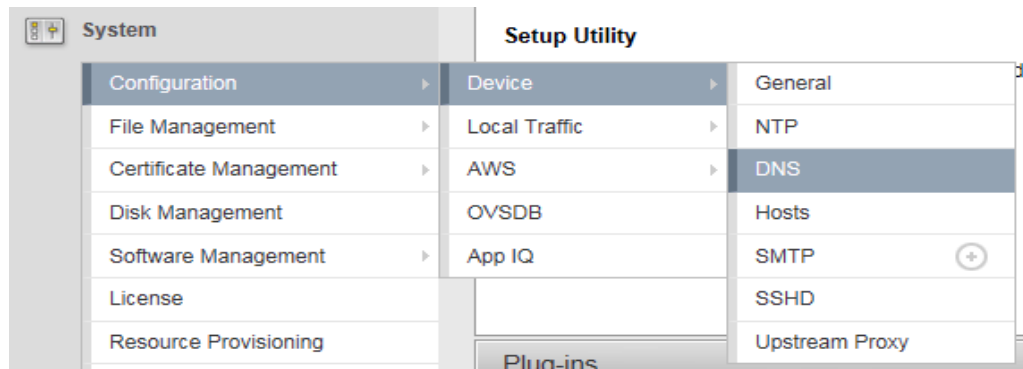
1. Create a DNS entry by selecting: System->Configuration->Device->DNS

System » Configuration : Device : DNS

| ⚙ ▾ | Device ▾ | Local Traffic ▾ | AWS ▾ | OVSDB |

Properties

|	
DNS Lookup Server List	Address: 10.128.20.100 Add 10.128.20.100 Edit Delete Up Down
BIND Forwarder Server List	Address: Add Edit Delete Up Down
DNS Search Domain List	Address: agilitylab.com Add localhost agilitylab.com Edit Delete Up Down
DNS Cache	☐
IP Version	IPv4 ▾

Update

2. In the Properties Section for DNS Lookup Server List, enter **10.128.20.100** in the Address field and click the **ADD** button.

3. Scroll down to the DNS Search Domain List section and enter **agilitylab.com** in the Address field and click the **ADD** button.

4. Click the **UPDATE** button at the bottom of the page to save the changes you just made.

8.3.3 NTP Server for System Configuration
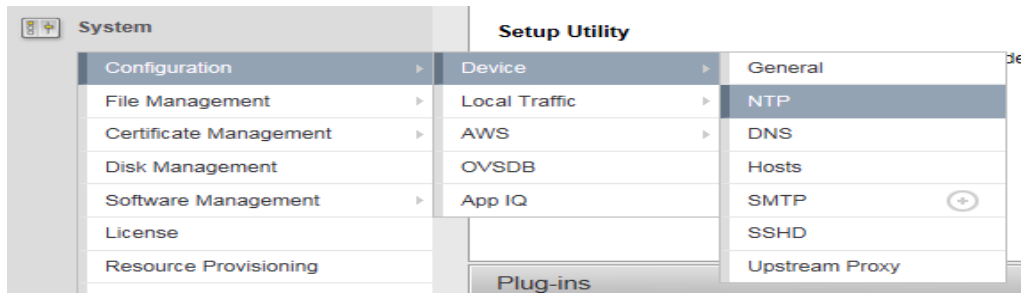
1. Create a NTP entry by selecting: System ? Configuration ? Device ? NTP
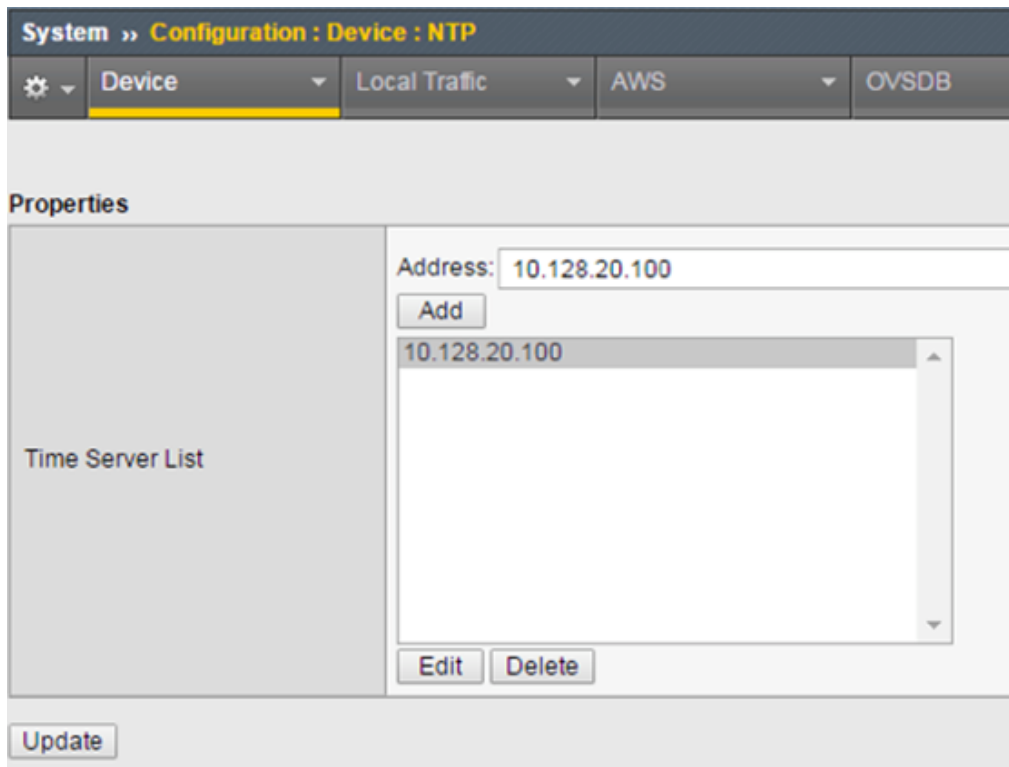

2. In the Properties Section for Time Server List, enter **10.128.20.100** in the Address field and click the **ADD** button.

3. Click the **UPDATE** button at the bottom of the page to save the changes you just made.

8.3.4 Access Policy (APM) AAA Server – Active Directory Object Creation

1. Create a new AAA Server Object of type Active Directory by selecting: Access ? Authentication ? Active Directory
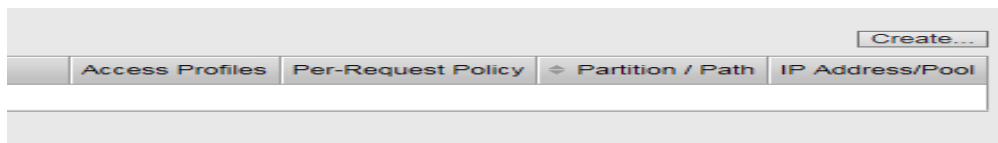
2. Click the **CREATE** button on right side of page.

General Properties

Name	LAB_AD_AAA
Type	Active Directory

Configuration

Domain Name	agilitylab.com ×
Server Connection	○ Use Pool ● Direct
Domain Controller	
Admin Name	
Admin Password	
Verify Admin Password	
Group Cache Lifetime	30 Days
Password Security Object Cache Lifetime	30 Days
Password Security Object Cache Lifetime	30 Days
Kerberos Preauthentication Encryption Type	None ▾
Timeout	15 seconds

Cancel   Repeat   Finished

3. Under General Properties type **LAB_AD_AAA** in the name field.

4. In the Configuration Section, Click the radio button option next to **Direct** in the Server Connection row.

5. In the Domain Name field enter **agilitylab.com**

6. Leave the Domain Controller, Admin Name and Admin Password fields blank for now.

7. Click the **FINISHED** button at the bottom of the page to save your changes.

8.3.5 Access Policy (APM) SSO Configuration – NTLMv1
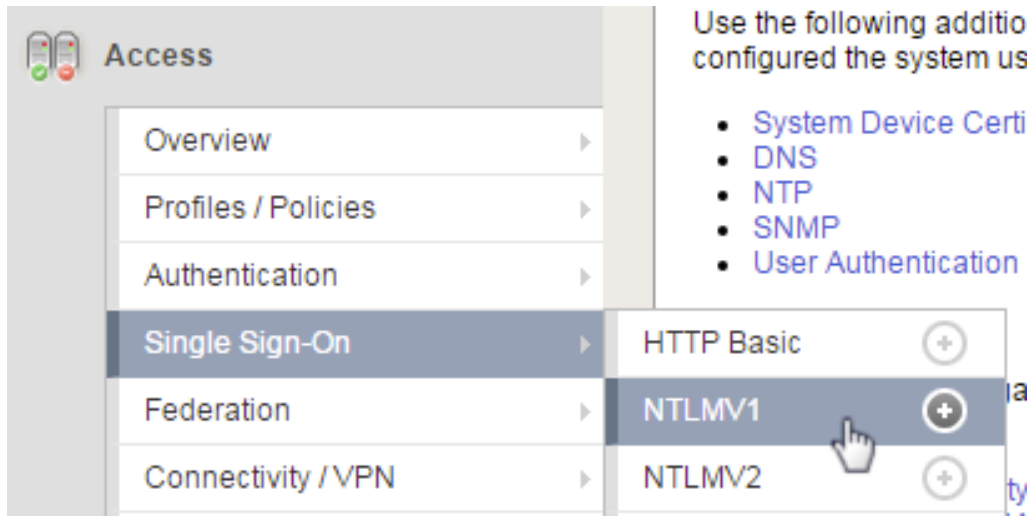
1. Create a new SSO Configuration Object of type NTLM by selecting: Access ? Single Sign-On ? NTLMV1
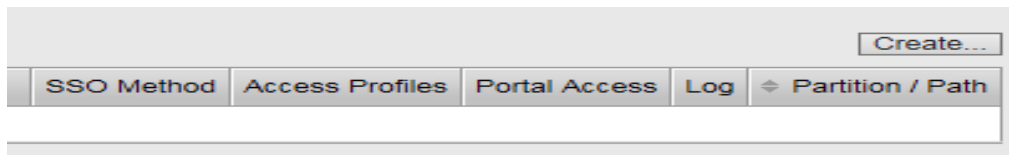
2. Click the **CREATE** button on the right side of the page.

General Properties: Basic ▾

Name	Agility_Lab_SSO_NTLM	×
SSO Method	NTLMV1	
Log Settings	+	From Access Profile ▾

Credentials Source

Username Source	session.sso.token.last.username
Password Source	session.sso.token.last.password
Domain Source	session.logon.last.domain

SSO Method Configuration

| Username Conversion | ☐ Enable |
| NTLM Domain | |

Cancel Finished

3. In the Name field enter **Agility_Lab_SSO_NTLM**

4. Click the **FINISHED** button at the bottom.

8.3.6 Access Policy (APM) Access Profile Creation
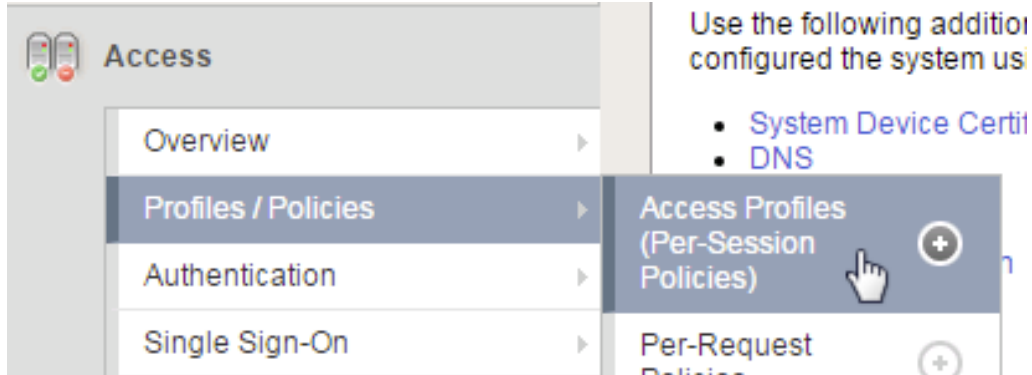
1. Create a new APM Profile Object of type ALL by selecting: Access ? Profiles/Policies ? Access Profiles (Per-Session Policies)
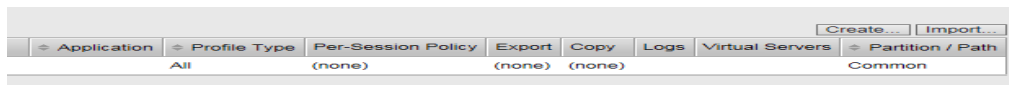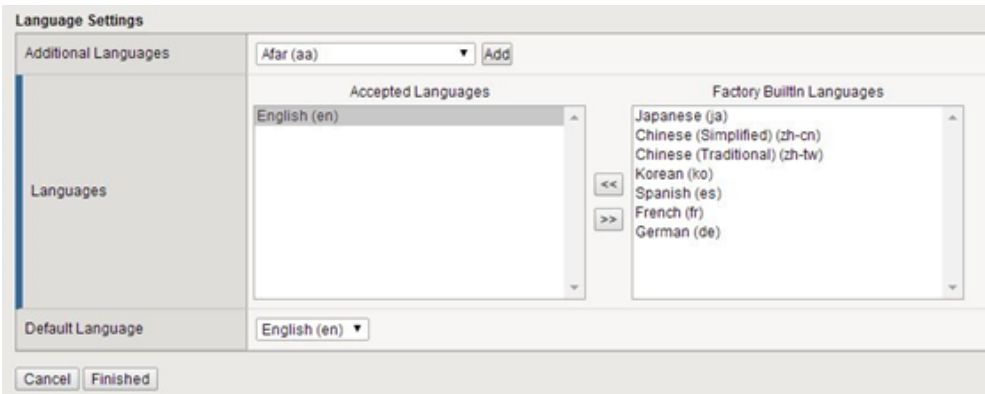
2. Click the **CREATE** button on the right side of the page.

3. In the Name field enter, **Agility-Lab-Access-Profile**

4. In the Profile Type drop down list select **All**
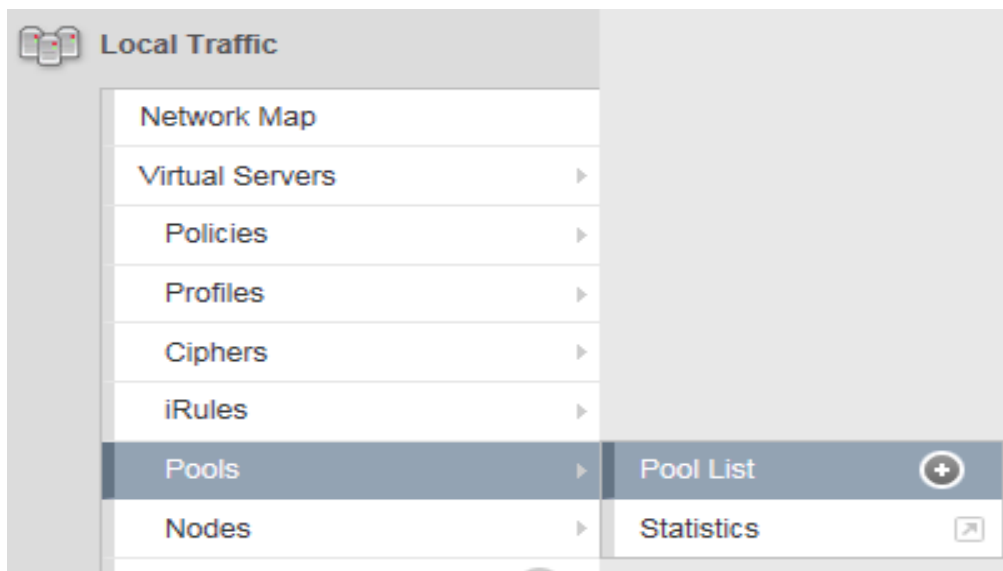
5. **In the Profile Scope drop down list select Profile**

6. In the Settings section click the checkbox to the right of Access Policy Timeout and change the value from 300, to **30**, seconds.
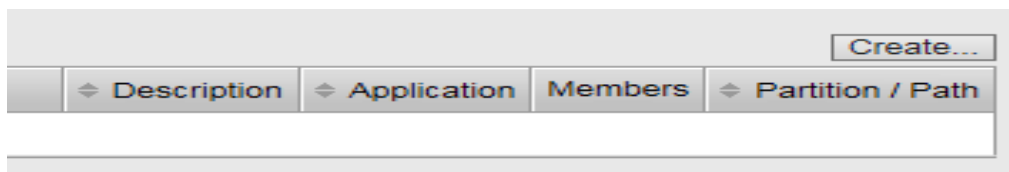

7. Scroll the bottom of the page and in the Language Settings section, click to highlight **English** in the Factory Builtin Languages box, then click the left **<<** arrows to move it to the left box labeled Accepted Languages.

8. Click the **FINISHED** button at the bottom of the page to save your changes.

8.3.7 Local Traffic (LTM) Pool and Member Creation

1. Create a new LTM Pool and Member by selecting Local Traffic ? Pools? Pools List

2. Click the **CREATE** button on the right side of the page.

Configuration: Basic

| Name | Agility-Lab-Pool |
| Description | |

Health Monitors

Active | Available
/Common
gateway_icmp
http
http_head_f5
https

`<<` `>>`

Resources

| Load Balancing Method | Round Robin |
| Priority Group Activation | Disabled |

New Members

● New Node ○ New FQDN Node

Node Name: (Optional)

Address: 10.128.20.100 ×

Service Port: 80 HTTP

Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.128.20.100	10.128.20.100	80		0

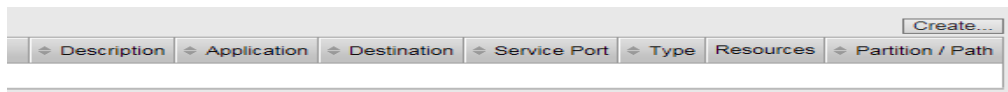Edit Delete

Cancel Repeat Finished

3. In the Name field enter **Agility-Lab-Pool**

4. In the Resources section, in the New Members area, enter **10.128.20.100** in the Address field.

5. In the Service Port field, enter **80**, or select **HTTP** from the drop-down menu.

6. Click the **ADD** button

7. Click the **FINISHED** button at the bottom to save your changes.

8.3.8 Local Traffic (LTM) Virtual Server Creation

This lab will walk you through creating the Virtual Server we will use during the course of the lab. This Virtual Server will be used to associate Access Policies which will be evaluated when authenticating users.

366
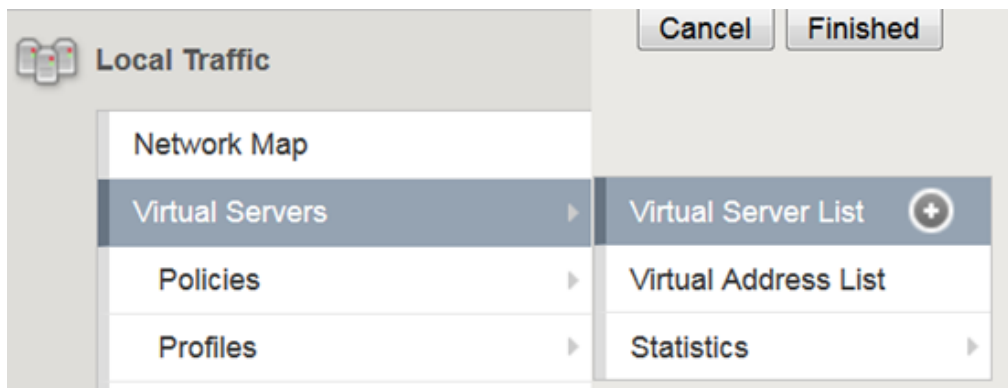
1. Create an new Virtual Server by selecting Local Traffic ? Virtual Servers ? Virtual Server List

2. Click the **CREATE** button on the right side of the page.

3. Under the General Properties section, in the Name field enter **Agility-LTM-VIP**

4. In the Destination Address field enter **10.128.10.100**

5. In the Service Port fields enter **443**, or select **HTTPS** from the drop-down menu

6. Under the Configuration section, in the HTTP Profile field use the drop-down menu to select **http**

7. In the SSL Profile (Client) field select **clientssl** from the Available profiles then use the **<<** left arrows to move it to the Selected box.

8. Ensure VLAN and Tunnel Traffic is set to **All VLANs and Tunnels**

9. In the Source Address Translation field select **Auto Map** from the drop-down menu.

10. Scroll down to the Access Profile section, select **Agility-Lab-Access-Profile** from the drop-down menu.

11. Click the **FINISHED** button to save your changes.
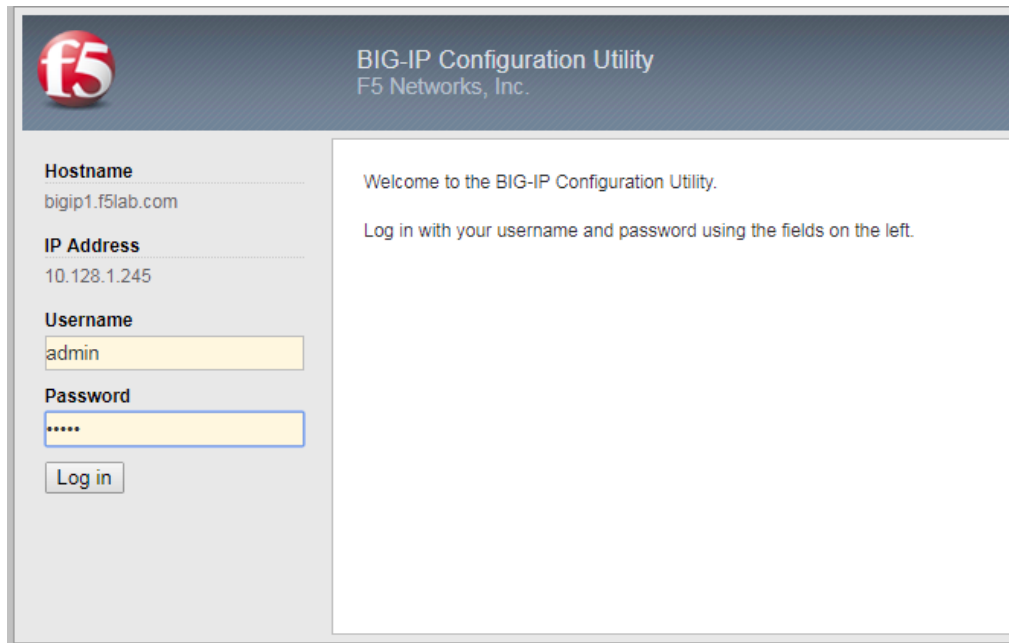
8.4 Lab 2: APM Troubleshooting Lab Object Preparation (TMSH)

Note: You only need to perform one of Lab 1, 2, or 3. They accomplish the same thing only in different ways. Lab 2 gets the Lab Preparation using TMSH

The purpose of this lab is to preconfigure some objects that will be used throughout the other labs. These objects are as follows:

  • Domain Name Services (DNS) Resolver

  • Network Time Protocol (NTP) Server

  • Access Policy (APM) AAA Server – Active Directory

  • Access Policy (APM) SSO Configuration – NTLMv1

  • Access Policy (APM) Access Profile

  • Local Traffic (LTM) Pool and Member

  • Local Traffic (LTM) Virtual Server

8.4.1 Connect to the Lab via SSH

1. Establish an RDP connection to your Jump Host and double-click on the **BIG-IP** Chrome shortcut on the Windows desktop. - User: agility - Password: Agility1

2. Ignore the certificate warning.

3. Login into the BIG-IP via SSH using putty and the following credentials: - User: root - Password: default

4. Log in to tmsh by typing the following command: **tmsh**

8.4.2 DNS Resolver for System Configuration (TMSH)

1. To add a name server to your /etc/resolv.conf file, use the following command syntax, replacing <IP addresses> with your IP addresses:

   modify sys dns name-servers add { <IP addresses> }

2. To add domains to your search list use the following command replacing <domains> with the domain you wish to add:

   modify sys dns search add { <domains> }

3. Configure as follows:

   modify sys dns name-servers add { 10.128.20.100 }

   modify sys dns search add { agilitylab.com }

   save sys config

4. To verify, use the following command: **list sys dns**

You should see the following reply:

```
root@(bigipa)(cfg-sync Standalone)(Active)(/Common)(tmos)# l:
sys dns {
    name-servers { 10.128.20.100 }
    search { localhost agilitylab.com }
}
```

8.4.3 NTP Server for System Configuration (TMSH)

1. To configure one or more NTP servers for the BIG-IP system, use the following command syntax:

   modify sys ntp servers add {hostname hostname. . . .}

2. Configure as follows:

   modify sys ntp servers add { 10.128.20.100 }

   save sys config

3. To verify, use the following command:

   list sys ntp

```
root@(bigipa)(cfg-sync Standalone)(Active)(/Common)(tmos)# l:
sys ntp {
    servers { 10.128.20.100 }
}
```

You snould see the following reply:

8.4.4 Access Policy (APM) AAA Server – Active Directory Object Creation (TMSH)

1. To configure an Active Directory AAA Server object, use the following command syntax:

   create apm aaa active-directory <name> domain <domain-name> use-pool <disabled>

2. Configure as follows:

   create apm aaa active-directory LAB_AD_AAA domain agilitylab.com use-pool disabled

   save sys config

3. To verify, use the following command:

   list apm aaa

```
root@(bigipa)(cfg-sync Standalone)(Active)(/Common)(tmos)# l:
apm aaa active-directory LAB_AD_AAA {
    domain agilitylab.com
    use-pool disabled
}
```

You should see the following reply:

8.4.5 Access Policy (APM) SSO Configuration – NTLMv1 (TMSH)

1. To configure an NTLMv1 SSO profile, use the following command syntax:

   create apm sso ntlmv1 <profile_name>

2. Configure as follows:

   create apm sso ntlmv1 Agility_Lab_SSO_NTLM

save sys config

3. To verify, use the command:

   list apm sso

8.4.6 Access Policy (APM) Access Profile Creation (see GUI steps)

Note: In order to gain familiarity with the Visual Policy Editor, please follow the GUI method of Access Policy creation: https://ua230-troubleshooting-2018-dev.readthedocs.io/en/latest/class4/module1/module1. html#access-policy-apm-access-profile-creation

---

8.4.7 Local Traffic (LTM) Pool and Member Creation (TMSH)

1. To configure a LTM Pool and Pool members, use the following command syntax:

   create ltm pool <pool-name> members add { <IP-addr>:<service-port> }

2. Configure as follows:

   create ltm pool Agility-Lab-Pool members add { 10.128.20.100:80 }

   save sys config

3. To verify, use the following command:

   list ltm pool

8.4.8 Local Traffic (LTM) Virtual Server Creation (TMSH)

1. To configure a virtual server, use the following command syntax:

   create ltm virtual Agility-LTM-VIP { destination 10.128.10.100:443 profiles add { clientssl http Agility-Lab-Access-Profile } vlans default source-address-translation { type automap } }

2. Configure as follows:

   create ltm virtual Agility-LTM-VIP { destination 10.128.10.100:443 profiles add { clientssl http Agility-Lab-Access-Profile } vlans default source-address-translation { type automap } }

   save sys config

3. To verify, use the following command:

   list ltm virtual

8.5 Lab 3: General Troubleshooting

In this lab exercise, you will learn where to look and what to look at when an Access Policy is not successfully allowing access or not performing as intended.

### 8.5.1 Questions to ask yourself (LAB3)

1. Do we have proper Network Connectivity?

2. Are there any Upstream/Downstream Firewall Rules preventing APM to be reachable or to reach destination targets it requires to access?

3. Do we have DNS setup properly?

4. Do we have NTP setup properly?

5. Are we receiving any Warnings or Error messages when we logon?

6. Are there any missing dependencies?

7. Time to check on our Sessions under Manage Session Menu

    (a) What can we see from the Manage Session Menu?

    (b) If we click the Session ID link what more information is available?

    (c) Is Authentication Successful or is it Failing?

    (d) Is the user receiving the proper ENDING ALLOW from the Policy?

8. Time to Review the Reports information for the Session in question

    (a) What information is available from the ALL SESSIONS REPORT?

    (b) Can we review the Session Variables for the user's session from the ALL SESSION REPORT? If YES then Why however If NO then WHY?

9. Can the BIG-IP TMOS Resolve the AAA server by Hostname and by Hostname.Domain?

    (a) Is the AAA reachable over the network, no Firewalls blocking communication from BIGIP Self-IP?

8.5.2 Verify DNS is setup from the CLI of the BIG-IP

Perform the following steps to verify DNS is correctly configured:
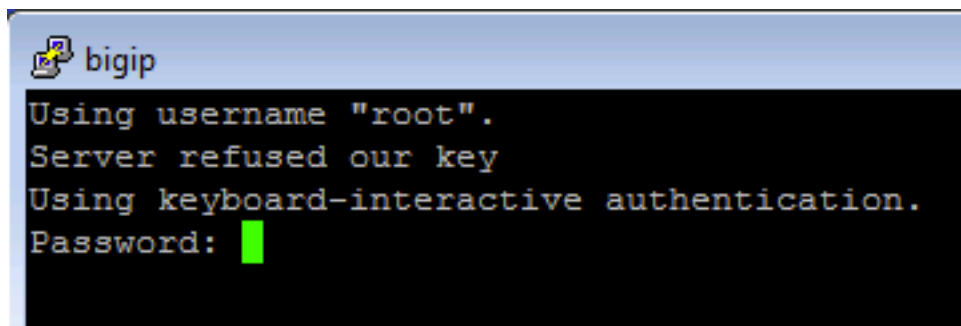

1. Click on the PuTTY (SSH client) to access the BIG-IP CLI
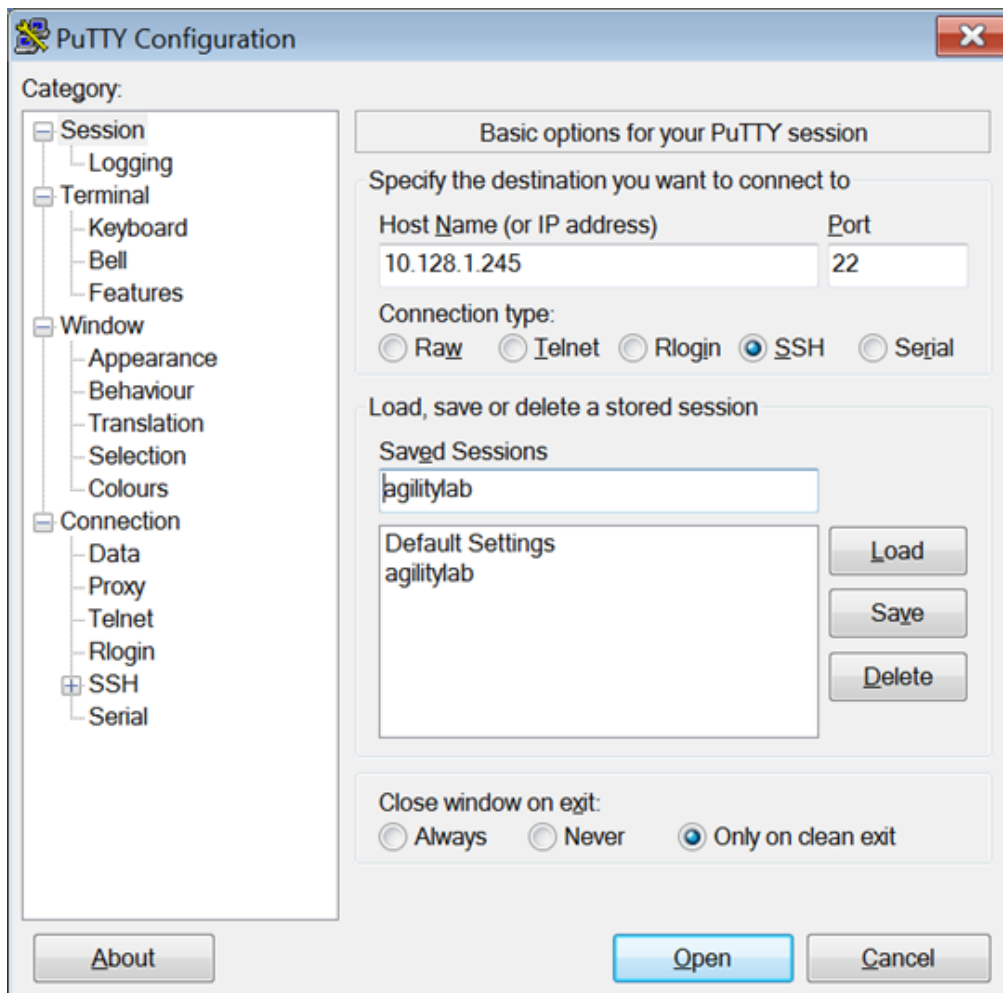
2. Click on the **agilitylab** Saved Session and click Load

3. The click on **OPEN**

Alternatively, you can simply double-click on the **agilitylab** Saved Session to open the session

4. Logon as **root** with password **default** if necessary (you should logon automatically)

```
[root@bigip1:Active:Standalone] config # dig agilitylab.com

; <<>> DiG 9.9.11-P1 <<>> agilitylab.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61961
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;agilitylab.com.                        IN      A

;; ANSWER SECTION:
agilitylab.com.         600     IN      A       10.128.20.100

;; Query time: 7 msec
;; SERVER: 10.128.20.100#53(10.128.20.100)
;; WHEN: Thu Jun 28 18:01:55 PDT 2018
;; MSG SIZE  rcvd: 59

[root@bigip1:Active:Standalone] config #
```

5. From the CLI type **dig agilitylab.com** and then press enter

6. The following results should be reviewed and verified.

7. If DNS is properly configured you should receive the returned IP address of **10.128.20.100**

```
[root@bigip1:Active:Standalone] config # nslookup
> agilitylab.com
Server:         10.128.20.100
Address:        10.128.20.100#53

Name:   agilitylab.com
Address: 10.128.20.100
>
```

8. From the CLI type **nslookup** and then press enter.

9. Type **agilitylab.com** and then press enter

10. The following results should be reviewed and verified.

11. If DNS is properly configured you should receive the returned IP address of **10.128.20.100**

12. Exit nslookup by typing **exit**

8.5.3 Verify NTP is setup from the CLI of the BIGIP

Perform the following steps to verify NTP is correctly configured:

```
[root@bigip:Active:Standalone] config # ntpq -pn
    remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.128.20.100    .LOCL.           1 u  113   64  377   13.933  -8921.0   3.918
```

1. From the CLI (via PuTTy –SSH Client) …. type **ntpq –pn** and then press enter.

2. The following results should be reviewed.

```
[root@bigip1:Active:Standalone] config # date
Wed May 24 11:49:20 PDT 2017
[root@bigip1:Active:Standalone] config #
```

3. If time is out of sync by too much of an offset you can update the local time using the following command:
   **date MMDDhhmmYYYY**

8.5.4 Manage Sessions within the Access Policy Manager menu

We use the Manage Sessions menu to view general status of currently logged in sessions, view their progress through a policy, and to kill sessions when needed.

STEP 1

New Tab   ✕

← → C 🗋 https://10.128.10.100
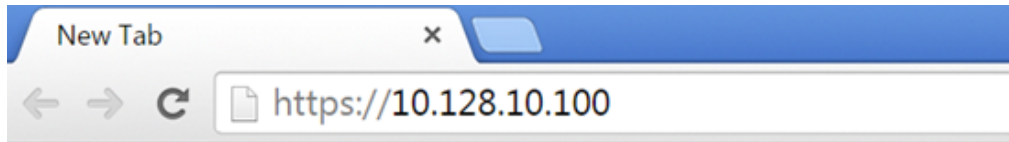
1. Open a USER session to APM through a new browser window by navigating to your first Virtual Server IP Address created in LAB I (**10.128.10.100**)

📄 BIG-IP logout page   ✕

← → C 🗋 https://10.128.10.100/vdesk/hangup.php3

f5
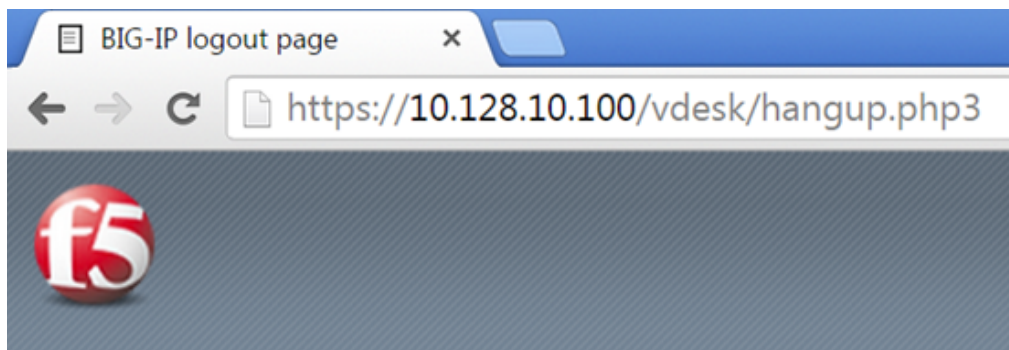
Your session could not be established.

The session reference number: ea45812d

Access was denied by the access policy. This may be due to a failure to meet access policy requirements.

If you are an administrator, please go to Access Policy >> Reports : All Sessions page and look up the session reference number displayed above.

To open a new session, please click here.

2. Did you receive an error message? If so, take note of the Session Reference Number

TEST 1
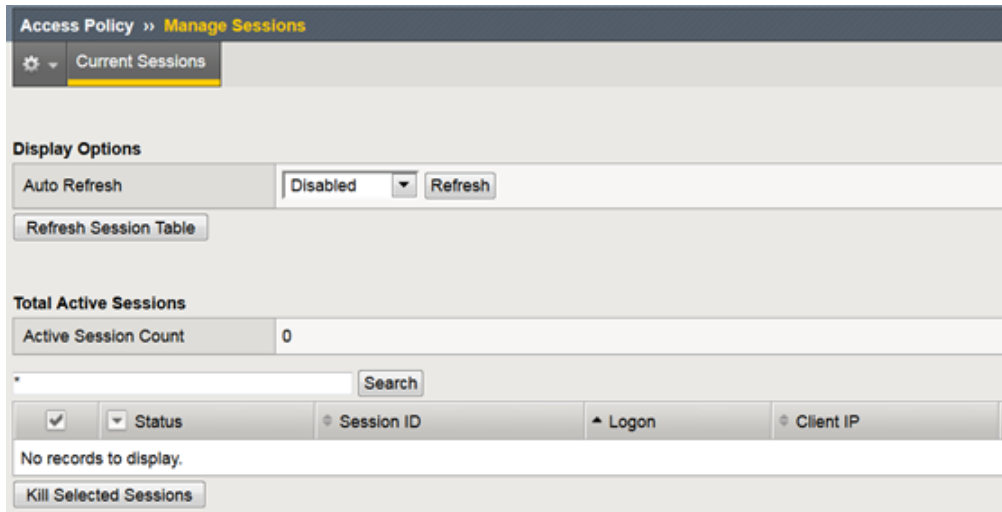
1. In the browser window, you are using to manage the BIG-IP, navigate to Access ? Overview > Active Sessions menu.

2. Review the Manage Sessions screen, is there an Active Session? If not then why?

STEP 2
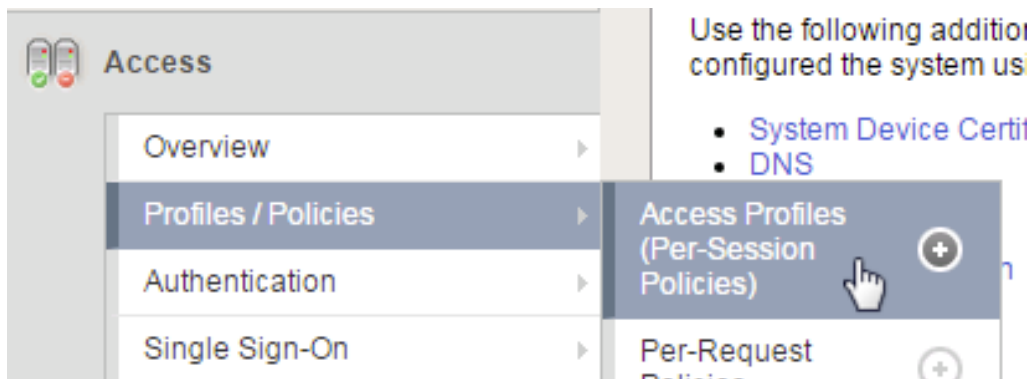
1. Now open the APM Visual Policy Editor (VPE) for the policy created/loaded in LAB I by navigating to Access ? Profiles/Policies -> Access Profiles (Per-Session Policies) menu.
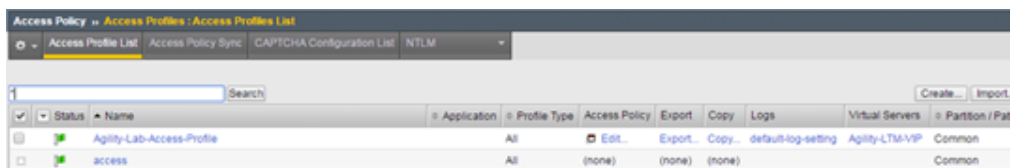
2. Then click the Edit link in the row that has the name of your Access Profile you are working with currently. (**Agility-Lab-Access-Profile**)

3. This will either launch a new browser or new tab depending on your browsers settings to display the APM Visual Policy Editor (VPE). The first policy we created was never edited to add any additional tasks that would instruct APM on what Actions it would need to take/enforce throughout a Policy Execution for the user's Session. So we will now adjust the policy and retest to see if we receive some new results.

4. Click on the **+** symbol between the Start and ending Deny objects.

Begin typing to search

| Logon | Authentication | Assignment | Endpoint Security (Server-Side) | Endpoint Security (Client-Side) | General Purpose |

○	Citrix Logon Prompt	Configure logon options for Citrix clients
○	External Logon Page	Redirect user to externally hosted form-based web logon page
○	HTTP 401 Response	HTTP 401 Response for Basic or SPNEGO/Kerberos authentication
○	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)
○	OAuth Logon Page	OAuth Logon Page used for OAuth Client authentication
○	Virtual Keyboard	Enables a virtual keyboard on the logon page for entering credentials
○	VMware View Logon Page	Display logon screen on VMware View clients

Cancel   Add Item   Help

5. This will pop up the Actions window where we can select from several Actions we wish to associate with our policy. On the Logon tab select the **Logon Page** radio button and then click the **ADD ITEM** button at the bottom of the page.

6. Click the **SAVE** button on the Logon Page properties window.
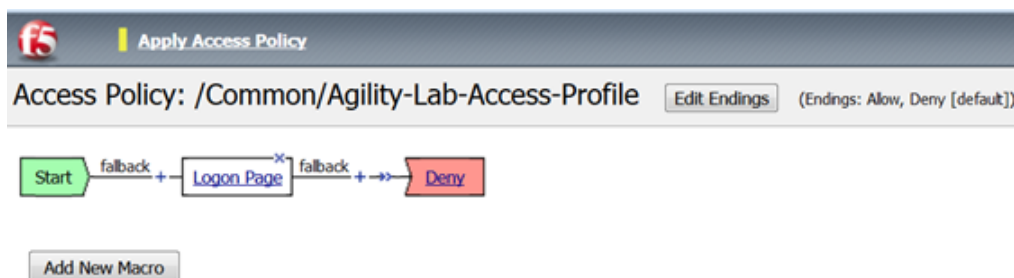
7. Then click the **Apply Access Policy** link on the top left of the page.

TEST 2
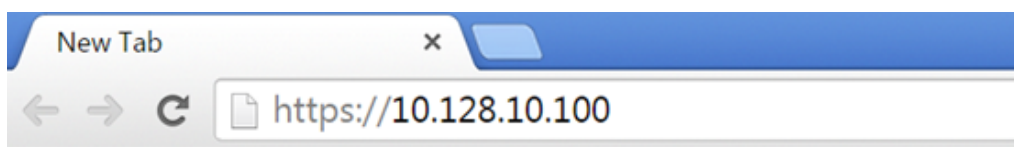
1. Restart your session to APM. (**https://10.128.10.100**)

Secure Logon
for F5 Networks

Username

Password

Logon

2. Did you receive and error this time? Or did you receive a Logon Page?

3. Open your browser or tab for managing APM and open the Active Sessions menu again.

4. Is there now an Active Session displayed on the page? If you were already on this page you may need to click the Refresh Session Table button.

5. What does the Status Icon look like? Is it a Green Circle or a Blue Square?

6. Is your username displayed in the Logon column?

7. Click on the Session ID for your session, this will open up a Session Details window.

Local Time	Log Message
2017-05-24 12:58:46	/Common/Agility-Lab-Access-Profile:Common:f49bfabb: Received User-Agent header: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KH...
2017-05-24 12:58:46	/Common/Agility-Lab-Access-Profile:Common:f49bfabb: New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener /Common/Ag...
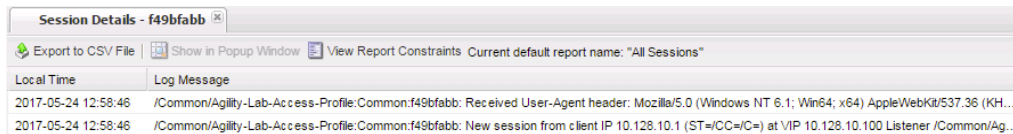
8. In the Session Details window, we can see some information about the session up to the point that the policy has executed so far.

9. Further down there is a reports section titled **Built-In Reports**, click that to open the list of built in reports.
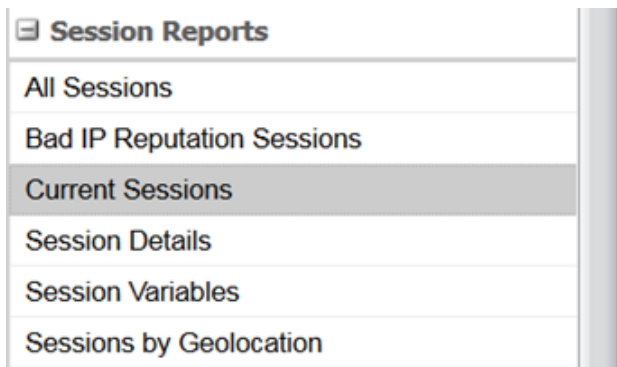
10. Scroll down to see the list of **Session Reports** and click the **Current Sessions** line and select **Run Report** from the pop up window.
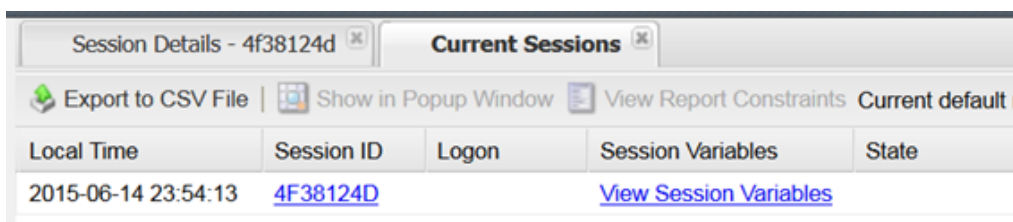
11. Do you see your Session ID displayed in the list of current sessions? If not then why?

TEST 3

Secure Logon
for F5 Networks

Username
student

Password
••••••••

Logon

1. Return to the browser or tab you are using for access to **https://10.128.10.100**. Restart a new session if necessary.

2. Next logon to the APM Logon page with:

   • Username: **student**

   • Password: **password**

Your session could not be established.

The session reference number: 323ab12d

Access was denied by the access policy. This may be due to a failure to meet access policy requirements.

If you are an administrator, please go to Access Policy >> Reports : All Sessions page and look up the session reference number displayed above.

To open a new session, please click here.

3. Did you receive and error after logging on? If so note the Session Reference Number.

4. Review the Manage Sessions menu, is your session listed?

5. Navigate to Access -> Overview ? Access Reports. When prompted Click Run Report.

Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent
2015-06-15 06:17:55	323AB12D	student	N	View Session Variables			

6. Do you see your Session ID listed in the list of All Sessions? Is the username listed in the Logon column?

Local Time	Log Message
2015-06-15 06:17:55	Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%206.1%3b%20WOW6
2015-06-15 06:17:55	Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode: Fu
2015-06-15 06:17:55	New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener
2015-06-15 06:22:48	\N: Session deleted due to user logout request.
2015-06-15 06:22:48	Username 'student'
2015-06-15 06:22:48	Following rule 'fallback' from item 'Logon Page' to ending 'Deny'
2015-06-15 06:22:48	Access policy result: Logon_Deny
2015-06-15 06:23:26	Session statistics - bytes in: 8530, bytes out: 12420

7. Click the Session ID to open the Session Details window.

8. Do you now see more information in this Sessions Details compared to the previous one we reviewed?

9. Is the username listed in the details?

10. In the Session Details screen we can see some important troubleshooting information, for example just below the username row we see a line that states that the Policy followed a path or branch called Fallback out of the Logon Page object to an Ending "Deny" thus the Access Policy Result was Logon_Deny.

Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent
2015-06-15 06:17:55	323AB12D	student	N	View Session Variables			

11. Now click back on the All Sessions tab at the top.

12. In the row for this session look to the right of the Logon column. You will see the next column states that the session is not Active. Now click the View Session Variables link in the next column.

Local Time	Session Variable Name	Session Variable Value

13. Do you see a lot of information recorded for Session Variables for this session? If not, then why?

8.6 Lab 4: Visual Policy Editor (VPE) & Session Variables

This lab will go a little deeper into understanding the Visual Policy Editor and Session Variables.

8.6.1 Questions to ask yourself (LAB4)

- Does the VPE Flow look correct?

- Does the VPE have the proper ENDING assigned to the appropriate BRANCH?

- Are your connection attempts following the intended VPE BRANCH/PATH during your test?

  – How could you alter the VPE to allow for better trouble shooting or pausing of a policy execution and termination?

- How can I pause the Policy Execution or Termination to review the session variable in Reports?

- What are VPE Actions?

- Are the Correct Session Variables being sent to the AAA Object?

- How can we GET or SET Session Variables in the VPE?

- How could I preserve the originally requested URI from the Client to pass to the internal server after APM authentication has complete?

8.6.2 Visual Policy Editor (VPE) Workflow, Actions, Branches, Endings

The Visual Policy Editor (VPE) is a screen on which to configure an access policy using visual elements. We have used it a few times already throughout our previous labs. This is meant to both review and explain in a bit more detail what the available Visual Policy Editor conventions are.

This table provides a visual dictionary for the Visual Policy Editor (VPE).

Visual Policy Editor (VPE) Visual Dictionary

Element type	Description	Visual element
Initial Access Policy	When an access profile is created, usually an initial access policy is also created.	Start —fallback— + — Deny Add New Macro
Start	Every access profile contains a start.	Start
Branch	A branch connects an action to another action or to an ending.	fallback
Add an action	Clicking this icon causes a screen to open with available actions for selection.	-+-
Action	Clicking the name of an action, such as Logon Page, opens a screen with properties and rules for the action. Clicking the x deletes the action from the access policy.	—×— Logon Page
Action that requires some configuration	The red asterisk indicates that some properties must be configured. Clicking the name opens a screen with properties for the action.	—×— *AD Auth
Ending	Each branch has an ending: Allow or Deny.	Allow
Configure ending	Clicking the name of an ending opens a popup screen.	**Select Ending:** ○ Allow ☐ ◉ Deny ☐
Add a macro for use in the access policy	Opens a screen for macro template selection. After addition, the macro is available for configuration and for use as an action item.	Add New Macro
Macro added for use	Added macros display under the access policy. Clicking the plus (+) sign expands the macro for configuration of the actions in it.	Add New Macro ⊞ Macro: AD_Auth (Terminals
Macro-call in an Access Policy	Clicking the *Macrocall* name expands the *Macro* in the area below the *Access Policy.*	Access Policy: /Common/plain Edit Endings (Endings: Allow, Start —fallback— + — AD_Auth —×— Out + → Deny Add New Macro ⊟ Macro: AD_Auth Rename / Settings Edit Terminals In fallback + —×— Successful + → Out *AD Auth **387** ack + → Out

8.6.3 Pausing the APM Policy Execution for Troubleshooting – The Message Box

Now that we have reviewed/refreshed our memory on VPE conventions lets edit our policy we were previously working on to add some more actions. This section we show a great tool for troubleshooting a policy that may have been reaching an ENDING DENY and closing the APM session too rapidly for proper inspection during the troubleshooting phase.

STEP 1
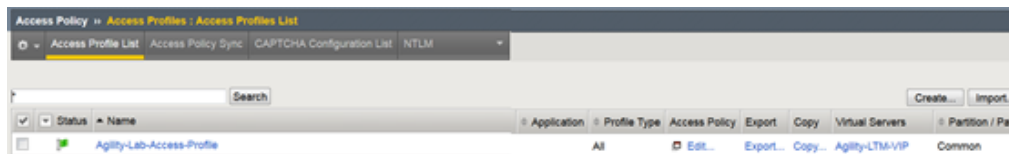
1. Navigate to Access ? Access Profiles ? Profiles/Policies -> Access Profiles (Per-Sessions Policies). Click Edit next to **Agility-Lab-Access-Profile** to open the Visual Policy Editor (VPE).
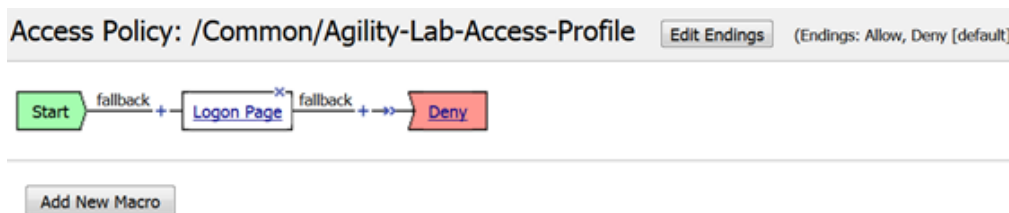
2. After the Logon Page object, on the fallback branch, click the **+** symbol to open the Actions window.

3. Click on the **General Purpose** tab and then click the radio button next to **Message Box** and click the **ADD ITEM** button at the bottom of the page.

4. Click the **SAVE** button on the next window

5. Now client the ending Deny.

6. In the pop-up window change it to Allow and click the **SAVE** button.
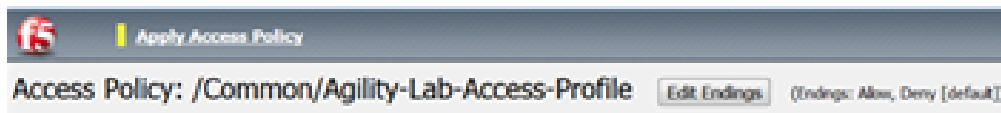
7. Then click the Apply Access Policy link at the top left.

TEST 1

Secure Logon
for F5 Networks

Username

student

Password

••••••••

Logon

1. Return to the browser or tab you are using for access to **https://10.128.10.100**. Restart a new session if necessary.

   • Username: **student**

   • Password: **password**

Please click the link below to continue.

Click here to continue

2. Did we receive an error this time after the logon page?

3. Did the Message Box display?
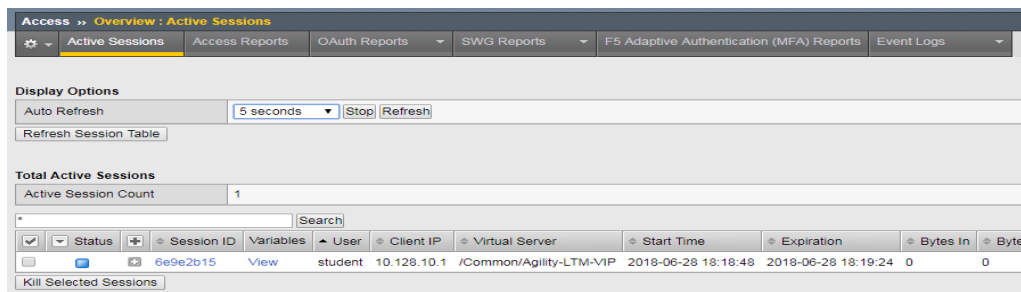
4. Keep the message box display there and move to the other browser to review the Manage Sessions menu.

5. Does the Manage Sessions menu show the Username this time?

6. Is the Status showing a Blue Square or Green Circle? Why?

7. Click the session ID to review the details for any new messages.

8. If things worked correctly you should see a message in the details stating, "Session deleted due to user inactivity or errors"
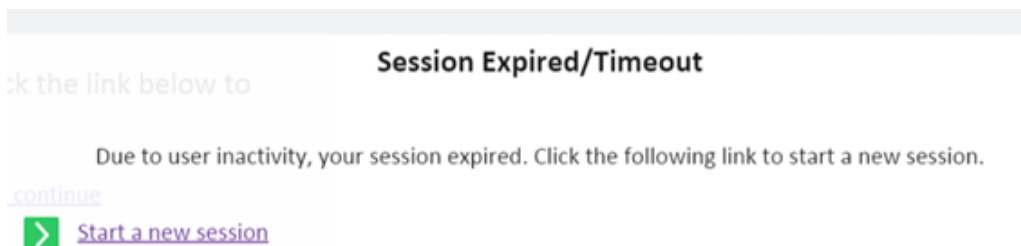
9. If you look back at the other browser window you should notice a Session Expired/Timeout message is being displayed.

STEP 2
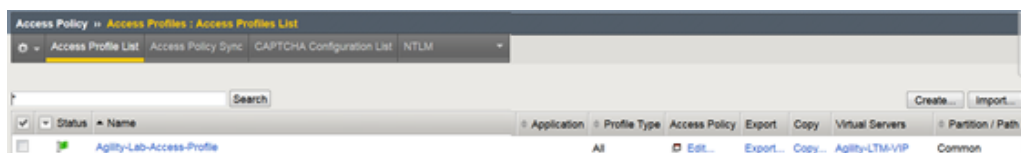
1. Navigate back to Access ? Profiles/Policies ? Access Profiles (Per-Session Policies). Click on **Agility-Lab-Access-Profile**

2. Access Policy Timeout from 30 seconds back to **300** seconds by removing the check from the custom column.

3. Click the **UPDATE** button at the bottom of the page.

4. Click Apply Access Policy link at the top left of the page.

5. Finalize the update by confirming the box is checked next to the profile and clicking **APPLY ACESS POLICY**

TEST 2

Secure Logon
for F5 Networks

Username

student

Password

••••••••

Logon

1. Now go back and restart the user session and logon.

Please click the link below to continue.

Click here to continue
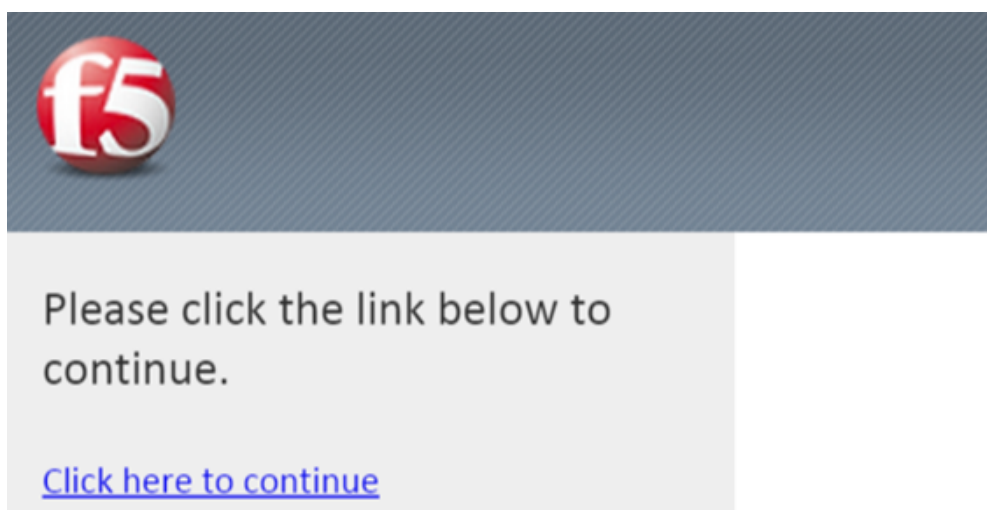
2. **Do NOT** click the message box link "Click here to continue"

3. Leave the message box message displayed for the time.

Total Active Sessions				
Active Session Count	1			

✔	▼ Status	⬍ Session ID	▲ Logon	⬍ Client IP
☐	☐	4121b0a9	student	10.128.10.1

Kill Selected Sessions

4. Go to the other browser/tab and open the Manage Sessions menu.

5. Your session should be there but the Status icon should still be a Blue Square.

6. Click on your Session ID
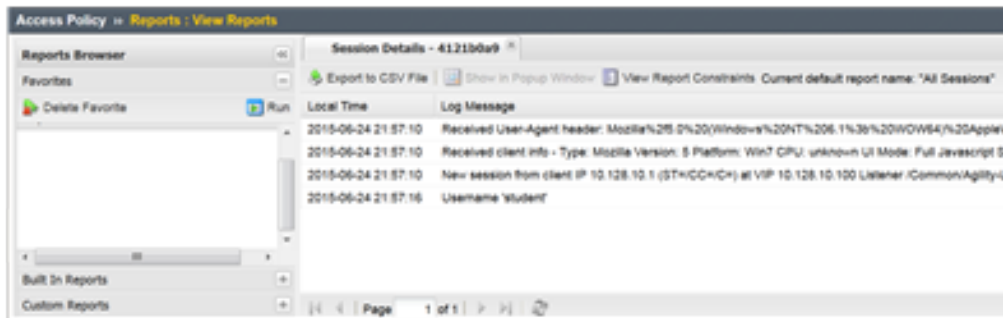
7. Click Built-in Reports
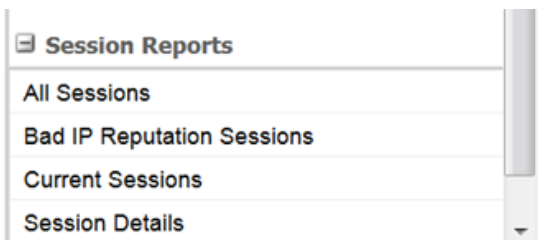
8. Click on All Sessions report, then choose Run Report on the pop-up menu.

9. Click the Session Variables for your current session.

10. Do you now have Session Variables being displayed for this session? If so why?

All Sessions ⊠	Session Variables - 10f1257e ⊠									

🔻 Export to CSV File | 🖼 Show in Popup Window 📄 View Report Constraints | 📄 Set to default report | Current default report name: "All Sessions"

Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent	Virtual IP	Client IP
2017-05-24 13:38:35	10f1257e	student	Y	View Session Variables				10.128.10.100	10.128.10.1

11. Click the All Sessions tab and look at the column labeled Active. Does it show a Y or N in the column?

Note that session variables will only be displayed for Active sessions. Since you placed a message box in the VPE to pause policy execution the session is seen as active. This provides you the ability to now review Session Variables that APM has collected up to this point in the policies execution.

Please click the link below to continue.

Click here to continue
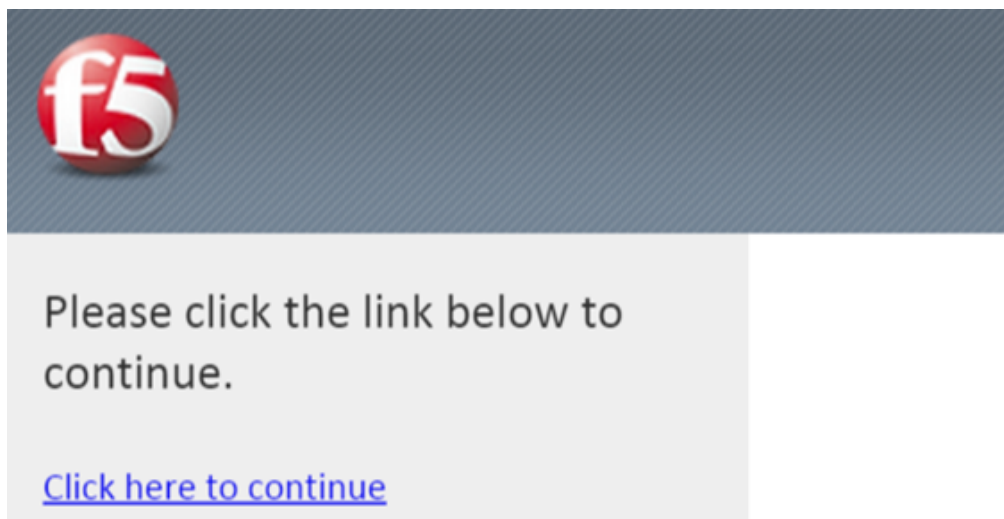
12. Now in the user browser click the link in the Message Box.

If it timed out then restart and this time click through the message box link.

Total Active Sessions

Active Session Count	1

		Search

✔	🔻 Status	➕	⬍ Session ID	Variables	▲ User	⬍ Client IP	⬍ Start Time	⬍ Expiration	⬍ Bytes In	⬍ Bytes Out	⬍ Session Type	⬍ Profile Name	⬍
☐	🟢	⊞	10f1257e	View	student	10.128.10.1	2017-05-24 13:38:34	2017-05-24 13:56:13	2342	790	ltm_apm	/Common/Agility-Lab-Access-Profile	

Kill Selected Sessions

13. Now review the Active Sessions menu and note what icon is shown in the status column. Green Circle finally? Success!!

Session Details - 10f1257e ⊠	

🔻 Export to CSV File | 🖼 Show in Popup Window 📄 View Report Constraints | Current default report name: "All Sessions"

Local Time	Log Message
2017-05-24 13:38:35	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Received User-Agent header: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KH...
2017-05-24 13:38:35	/Common/Agility-Lab-Access-Profile:Common:10f1257e: New session from client IP 10.128.10.1 (ST=/CC=/C=) at VIP 10.128.10.100 Listener /Common/A...
2017-05-24 13:38:58	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Username 'student'
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Following rule 'fallback' from item 'Message Box' to ending 'Allow'
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Access policy result: LTM APM_Mode
2017-05-24 13:41:09	/Common/Agility-Lab-Access-Profile:Common:10f1257e: Received client info - Hostname: Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode:...

14. If you now click the Session ID you will see that the Policy has reached an ending Allow thus the Access Policy Result is now showing we have been granted LTM+APM_Mode access.

15. Now open the All Sessions report once more to review the Session Variables collected.

16. Click the logon folder in the Session Variables page that opens for your session.

17. Click the folder icon named *last* to expand its contents.

Notice on the left column labeled Variable Name above and to the right the next column is Variable Value and the third column is Variable ID. If you look at the Variable Name of username you will see to the right its value is recorded as student as you entered it in the logon page. The next column displays APM's matching session Variable ID for this information. You will see that the naming convention follows the session hierarchy starting with session. then the first folder logon. then the next folder last. then finally the Variable Name of Username.

We will use some session variables in the next lab to GET and SET information for the users session.

8.6.4 Session Variables – Setting and Retrieving (Some Quick Information)

This section will provide some guidance on how to both retrieve and set session variables within a policy for a user's session. Session Variables are very useful in many areas of policy execution. They can be used to assist in areas like authentication or single sign-on or assigning resource items for users based on information APM can collect from the backend AAA server and its associated directory.

Currently cached session Variables are available in APM Reports for review by an administrator. Additional available variables can always be found in the APM Configuration Guides. What is really nice is that APM is not limited to only having awareness of Session Variable it collects from the user session establishment or from the AAA server, administrators can actually create or set their own custom session variables for

use within a policy. This means that an administrator could create new session variables via the VPE's Variable Assign action or session variables could even be set from an iRule attached to a virtual server. This means that information that the LTM VIP can see or be gathered via an iRule could then be set as a session variable that could then be retrieved and used within the VPE.

About Session Variable Names

The name of a session variable consists of multiple hierarchical nodes that are separated by periods (.):
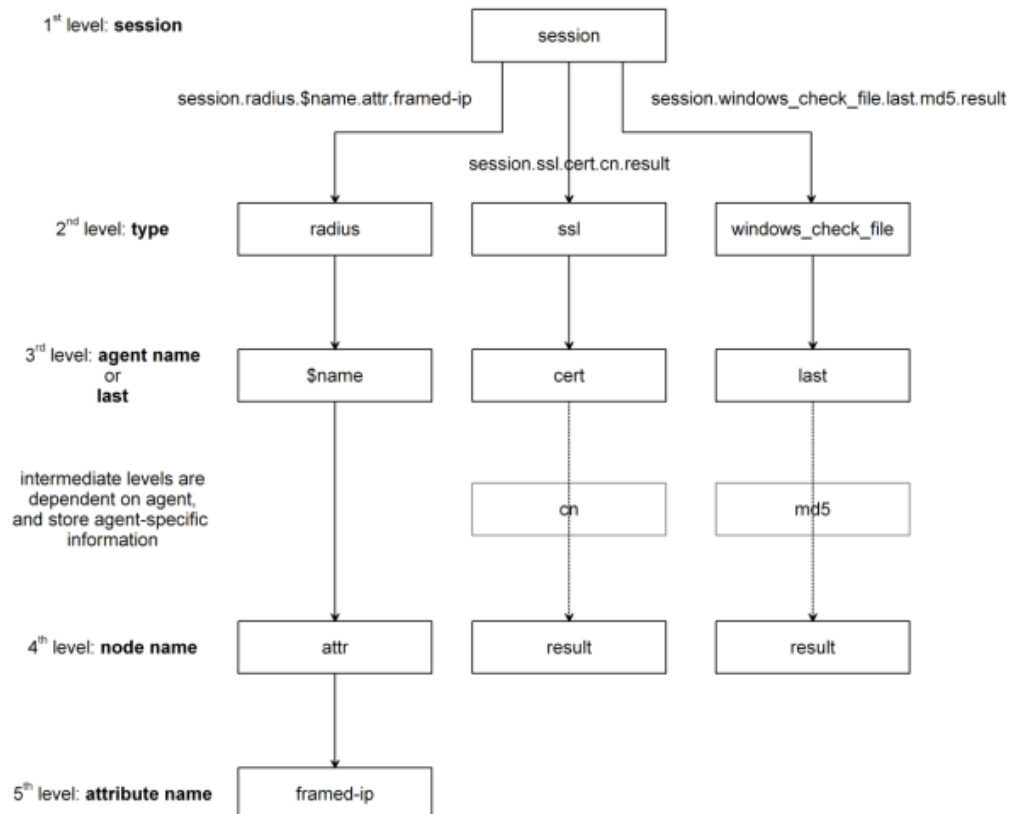
Session Variable Reference

APM Session Variable references are provided in APM documentation. Current release information can be found at the following link: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-visual-policy-editor-13-0-0/5.html

Partial Session Variable list

ACTION ITEM	SESSION VARIABLE	TYPE	DESCRIPTION
Denied Ending	session.policy.result	string	Access policy result: the access policy ended at Deny. The value is **access_denied**.
Redirect Ending	session.policy.result	string	Access policy result: the access policy ended at Redirect. The value is **redirect**.
	session.policy.result.redirect.url	string	URL specified in the redirect, for example, **http://www.siterequest.com**.
Allowed Ending	session.policy.result	string	Access policy result: the access policy ended at Allow. The value is **allowed**.
	session.policy.result.webtop.network_access.autolaunch	string	Name of the resource that is automatically started for a network access webtop.
	session.policy.result.webtop.type	string	Type of webtop resource: **network_access** or **web_application**.
Session management	session.ui.mode	enum	UI mode, as determined by HTTP headers.
	session.ui.lang	string	Language in use in the session, for example **"en"** (English).
	session.ui.charset	string	Character set used in the session.
	session.client.type	enum	Client type as determined by HTTP headers: portalclient or "Standalone".
	session.client.version	string	
	session.client.jailbreak	bool	Mobile device is jailbroken/rooted: • **0** - No • **1** - Yes
	session.client.js	bool	Client is capable of executing JavaScript: • **0** - No • **1** - Yes
	session.client.activex	bool	Client is capable of running ActiveX Controls: • **0** - No • **1** - Yes
	session.client.plugin	bool	
	session.client.platform	string	Client platform as determined by HTTP headers: • **"Android""** • **"ChromeOS"** • **"iOS""** • **"Linux""** • **"MacOS""** • **"Win10"** • **"Win2k"** • **"Win2k""** • **"Win7"** • **"Win8.1"** • **"Win8"** • **"WindowsPhone"** • **"WinLH"** • **"WinNT""** • **"WinVI""** • **"WinXP""**

Session Variable Categorization

While these are not formal categories, Session Variables fall under three general categories:

Category	Examples
Variables returned by Access Policy actions	• Active Directory query results • Antivirus Check results • Windows Info and Registry check results
Special purpose user variables	• Lease Pools • Client IP assigned to a client session • Username and Password
Network access resource variables and attributes	• Split tunneling • DNS Settings • Compression, etc.

Active Session Variables

Below is a short breakdown of information gathered and cached during an Active session. Additional information can be gathered from the results of End Point checks when they are put into a policy. These would display as folders like check_av or check_fw if the actions were added to the policy

Session Variable Manipulation via TCL

Variables can be parsed, modified, manipulated, etc using TCL. Although the tables below are not an exhaustive reference for writing and using TCL expressions, it includes some common operators and syntax rules.

Standard Operators

You can use TCL standard operators with most BIG-IP® Access Policy Manager® rules. You can find a full list of these operators in the TCL online manual, at http://www.tcl.tk/man/tcl8.5/TclCmd/expr.htm. Standard operators include:

Operator	Description
- + **~ !**	Unary minus, unary plus, bit-wise NOT, logical NOT. None of these operators may be applied to string operands, and bit-wise NOT may be applied only to integers.
**	Exponentiation. Valid for any numeric operands.
* / **%**	Multiply, divide, remainder. None of these operators may be applied to string operands, and remainder may be applied only to integers. The remainder will always have the same sign as the divisor and an absolute value smaller than the divisor.
+ -	Add and subtract. Valid for any numeric operands.
<< **>>**	Left and right shift. Valid for integer operands only. A right shift always propagates the sign bit.
< > **<=** **>=**	
	Boolean less than, greater than, less than or equal to, and greater than or equal to. Each operator produces 1 if the condition is true, 0 otherwise. These operators may be applied to strings as well as numeric operands, in which case string comparison is used.
== **!=**	Boolean equal to and not equal to. Each operator produces a zero/one result. Valid for all operand types.
eq **ne**	Boolean string equal to and string not equal to. Each operator produces a zero/one result. The operand types are interpreted only as strings.
in **ni**	List containment and negated list containment. Each operator produces a zero/one result and treats its first argument as a string and its second argument as a Tcl list. The in operator indicates whether the first argument is a member of the second argument list; the ni operator inverts the sense of the result.
&	Bit-wise AND. Valid for integer operands only.
^	Bit-wise exclusive OR. Valid for integer operands only.
|	Bit-wise OR. Valid for integer operands only.
&&	Logical AND. Produces a 1 result if both operands are non-zero, 0 otherwise. Valid for boolean and numeric (integers or floating-point) operands only.
||	Logical OR. Produces a 0 result if both operands are zero, 1 otherwise. Valid for boolean and numeric (integers or floating-point) operands only.
x?y:z	If-then-else, as in C. If x evaluates to non-zero, then the result is the value of y. Otherwise the result is the value of z. The x operand must have a boolean or numeric value.

Standard Operators

A rule operator compares two operands in an expression. In addition to using the TCL standard operators, you can use the operators listed below.

Operator	Description
contains	Tests if one string contains another string.
ends_with	Tests if one string ends with another string
equals	Tests if one string equals another string
matches	Tests if one string matches another string
matches_regex	Tests if one string matches a regular expression
starts_with	Tests if one string starts_with another string
switch	Evaluates one of several scripts, depending on a given value

Logical Operators

Logical operators are used to compare two values.

Operator	Description
and	Performs a logical and comparison between two values
not	Performs a logical not action on a value
or	Performs a logical or comparison between two values

Getting/Setting Session Variables

During the pre-logon sequence, using the Visual Policy Editor (VPE) you can get and set Session Variables. The following are some quick examples.

- To **set/modify** a variable: Variable Assign action

- To **get** a value the last username entered by a user, use expr or return:
  expr { [mcget {session.logon.last.username}]}

expr evaluates an expression, whereas **return** simply returns the result. For example, we have a two custom variables:

- session.custom.value1 = 3

- session.custom.value2 = 4

Using **expr** we can construct the following expression, this would return a value of 7 (i.e. the evaluation of 3+4):

    expr { "[mcget session.custom.value1] + [mcget session.custom.value2]" }.

Using **return** we can construct the following expression, this would return simply "3+4" as shown.

    return { "[mcget session.custom.value1] + [mcget session.custom.value2]" }

Using iRules

In all the "Access" events

```
ACCESS::session data get/set "variable\_name" ["value"]
```

Set Secure Variables

You can also set Secure Variables. The value of a secure session variable is stored as encrypted in the session db. The value is not displayed as part of session report in UI, nor is it logged as part of logging agent. Secure variables require the -secure flag, both for mcget and access::session data get/set.
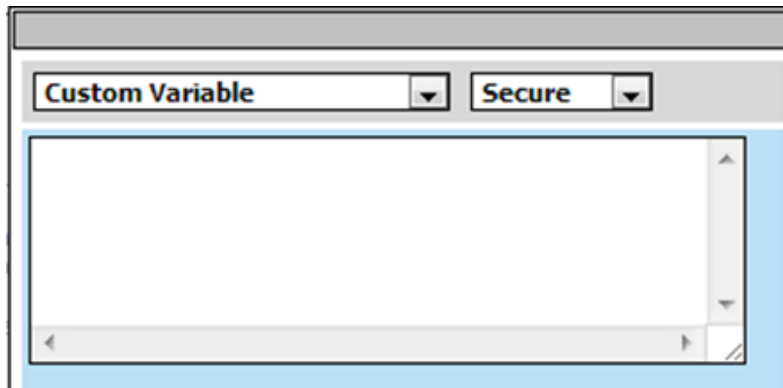
Review these two examples below. The first is a Variable Assign action that is SETTING the Session Variable ID of "session.logon.last.upn" with the information extracted from an x509 Client Certificate that was presented by the user's computer/browser upon connection to the VIP.
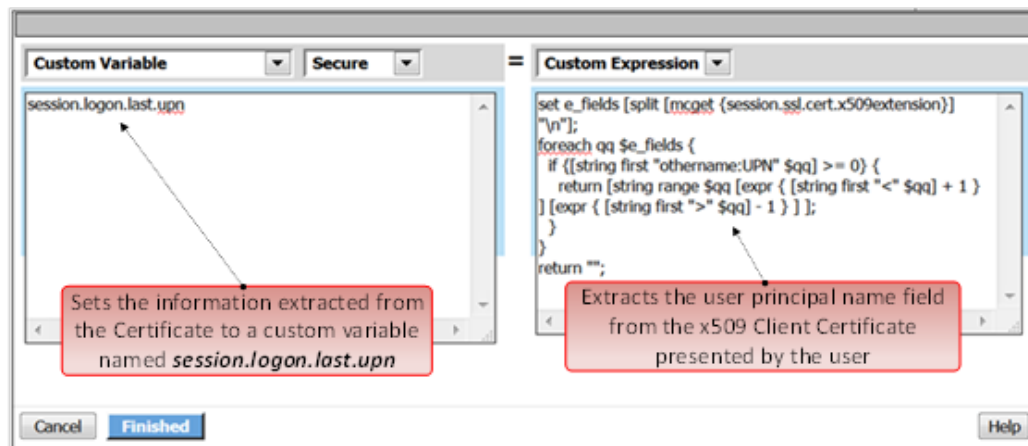
The second example show a message box displaying a Session Variable value by calling out the Session Variable ID in the Message Box for the user to see.
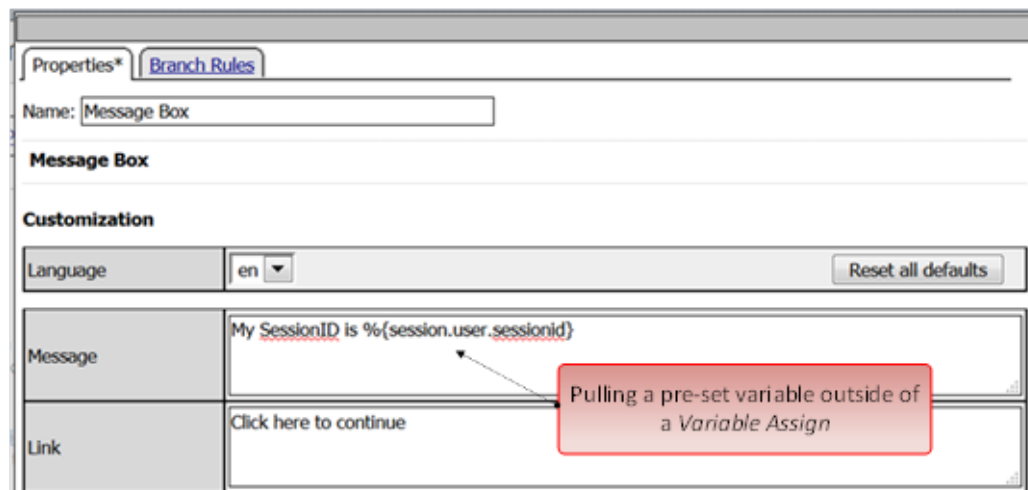
Session Variable Exercise

The following are some exercises to demonstrate how session variables can be utilized.

STEP 1
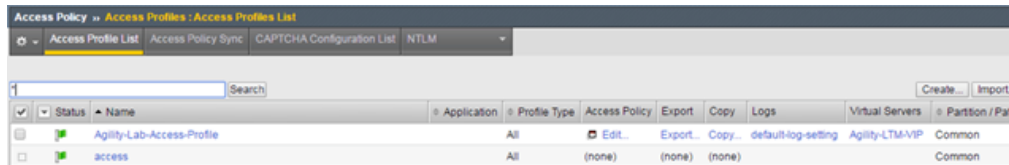
1. Open the APM VPE for the **Agility-Lab-Access-Profile** Access Policy we have been working with.

2. Edit the Message Box in the VPE.

3. In the Message text box enter: **My username is: %{session.logon.last.username}** Then click the **Save** button
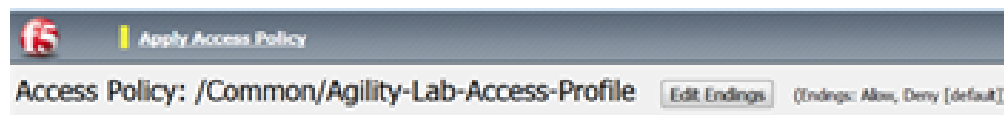
4. Then click Apply Access Policy

TEST 1

Secure Logon
for F5 Networks

Username
student

Password
••••••••

Logon

1. Now logon with the "student" username to the test site.

https://10.128.10.100/my.policy

My username is: student

Click here to continue

2. When the message box appears, you should see a message stating, "**My username is: student**". Was it successful?

STEP 2

1. Go back into the VPE

Access Policy: /Common/Agility-Lab-Access-Profile [Edit Endings] (Endings: Allow, Deny [default])

2. Add a Variable Assign action from the Assignment action tab and place it before the Message Box action.

3. When the properties screen opens, click the **Add New Entry** button.

4. Then click the "Change" link.

5. A window will pop up with *Custom Variable* on the left and *Custom Expression* on the right.

You will notice both boxes are currently empty.
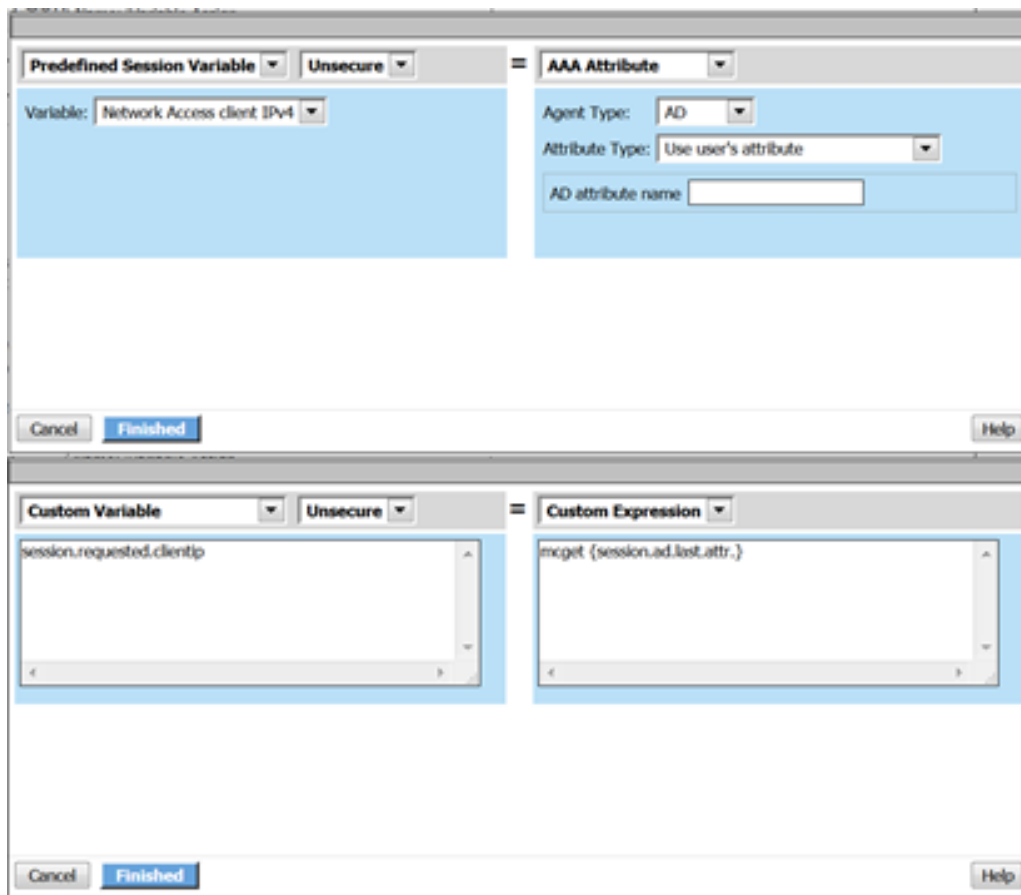
6. Often you may forget how to start off with the variable name or the expression so a trick you can use to get you started is first select a pre-defined variable on the left side and a AAA attribute on the right side and then reselect custom variable and custom expression. This will populate each box with example data that you can now edit.

This is not a required step, just a tip!
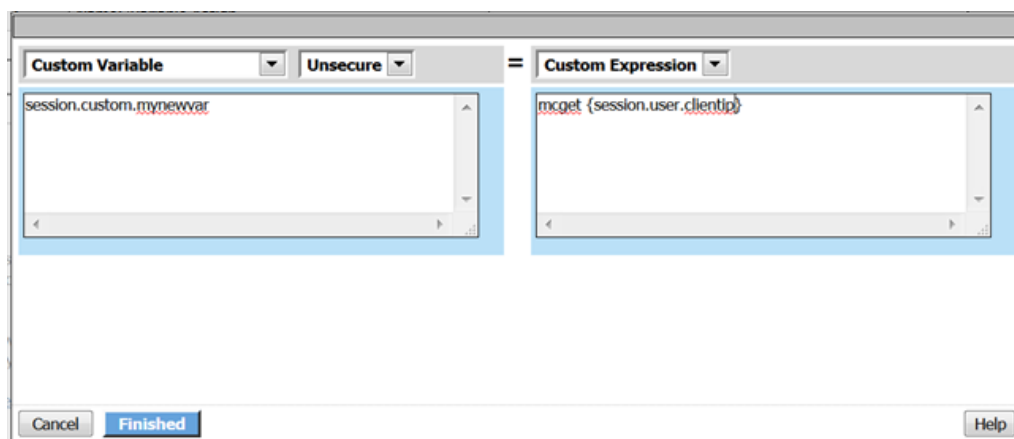
7. On the Custom Variable side type: **session.custom.mynewvar** (Be sure to make it lowercase). On the Custom Expression side type: **mcget {session.user.clientip}** (There is a space between mcget and the { bracket)

8. Click the **Finished** button.

9. Click the **Save** button.
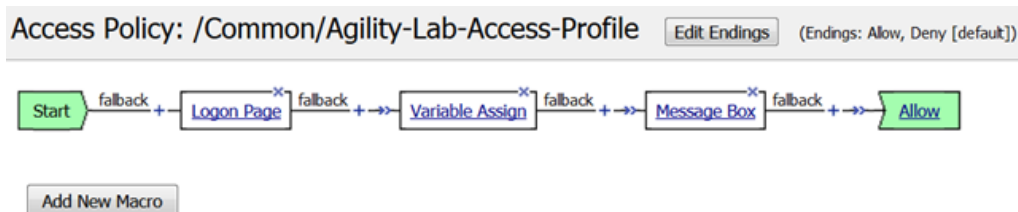
10. Click on the Message Box.

11. After the closing **}** bracket in the first line of the message section add a space and then type **
**

12. Then on the next line type, **My Client IP is: %{session.custom.mynewvar}**

13. Then click the **Save** button.

14. Then click Apply Access Policy.

TEST 2

Secure Logon
for F5 Networks

Username

student

Password

••••••••|

Logon

1. Now logon to the test site as a user again and review the message box text.

← → C   ✗ ~~https~~://10.128.10.100/my.policy

My username is: student
My Client IP is: 10.128.10.1

Click here to continue

2. Does it display your client IP address?

3. Now run the All Sessions Report and review the View Session Variables for the active SessionID. (Access ??Overview ?Access Reports)

4. Notice the folder icon named custom and the corresponding Variable ID of session.custom. This was generated automatically during the Variable Assign action that you added to the policy. When you set the Custom Variable to session.custom.mynewvar APM used the next word after the session as the new container (custom) for variable (mynewvar).

5. If you expand custom folder you will notice a new Variable named mynewvar and in the next column you will see your client ip address and in the third column the variable id of session.custom.mynewvar

As you can see this could be expanded upon to be very useful. For example, maybe you are enabling two-factor authentication for both Active Directory and RSA Secure ID. Well the AAA server authentication Action objects expect to see a specific session variable name sent to them for so that they can correctly parse that data and verify against the AAA server. As an example both the AD Auth and the RSA Auth expect to see session.logon.last.password as the variable used to hold the password value. However, if you create a logon page with three input fields, one for username, a second for AD password and the third for the RSA Token/PIN then they must each have their own unique post and session variable name as they are configured in the Logon Page object.

This means that as the third variable for the RSA toke/pin is passed to APM no longer as session.logon.last.password because the AD Password field was already set to use that variable on the logon page. What do we do now?

Variable Assign to the rescue, take a look at this below example to fix this problem as it mimics what we just accomplished with the session.custom.mynewvar exercise. Consider the following screen shots.

Logon Page Agent

Split domain from full Username	No	
CAPTCHA Configuration	None	

	Type	Post Variable Name	Session Variable Name	Values	Read Only
1	text	username	username		No
2	password	password	password		No
3	password	rsapin	rsapin		No
4	none	field4	field4		No
5	none	field5	field5		No

Adding the name of the variable in *Logon Page* action

Custom Variable — Unsecure = Custom Expression

session.logon.last.password = mcget {session.logon.last.rsapin}

Setting the custom variable

Access Policy: /Common/test-vpn Edit Endings (Endings: Deny [default], Allow)

Start → fallback → Logon Page → fallback → AD Auth → Successful → Variable Assign → fallback → *RSA SecurID → Successful → Resource Assign → fallback → Allow; fallback → Deny; fallback → Deny

A full view of the policy

8.7 Lab 5: Command Line Tools

This lab will show you how to make use of some of the Command Line Utilities for troubleshooting Access Policy Manager when dealing with Authentication issues that you could experience.

8.7.1 Questions to ask yourself (LAB5)

- What should I expect in the Logs with Default Settings?
- Can I review the APM configuration from TMSH?
- Can I review Session Data from the CLI?
- How can I test if the AAA server responds to Authentication Tests using CLI Tools?
- How can I test if the AAA server respond to Query Tests using CLI Tools?
- How can I change the Logging Level for more Verbose details?
- How can I use iRules for Troubleshooting Assistance?
- How can I use TCPDump for Troubleshooting Assistance?

8.7.2 What's Not Covered but we will discuss

- VDI Troubleshooting/Debug Logging
- SAML Troubleshooting Tools – SAML Tracer (Not CLI based)

8.7.3 Checking APM Logs

APM Logs by default show the same information you can get from the Manage Sessions menu, as well as APM module-specific information.

Access Policy Manager uses syslog-ng to log events. The syslog-ng utility is an enhanced version of the standard logging utility syslog.

The type of event messages available on the APM are:

Event Messages	File Location	Description
Access Policy Events	/var/log/apm	Access Policy event messages include logs pertinent to access policy, SSO, network access, and web applications. To view access policy events, on the navigation pane, expand System menu and click Logs.
Audit Logging	/var/log/audit	Audit event messages are those that the APM system logs as a result of changes made to its configuration.

When setting up logging you can customize the logs by designating the minimum severity level or log level, that you want the system to report when a type of event occurs. The minimum log level indicates the minimum severity level at which the system logs that type of event.

Note: Files are rotated daily if their file size exceeds 10MB. Additionally, weekly rotations are enforced if the rotated log file is a week old, regardless whether or not the file exceeds the 10MB threshold.

The **default** log level for the BIG-IP APM access policy log is **Notice**, which does ***not*** log Session Variables. Setting the access policy log level to **Informational** or **Debug** will cause the BIG-IP APM system to log Session Variables, but it will also add additional system overhead. If you need to log Session Variables on a production system, F5 recommends setting the access policy log level to Informational temporarily while performing troubleshooting or debugging.

We need to add some more actions to the APM Profile in the VPE we have been working with to go along with the next few lab tests.

STEP 1
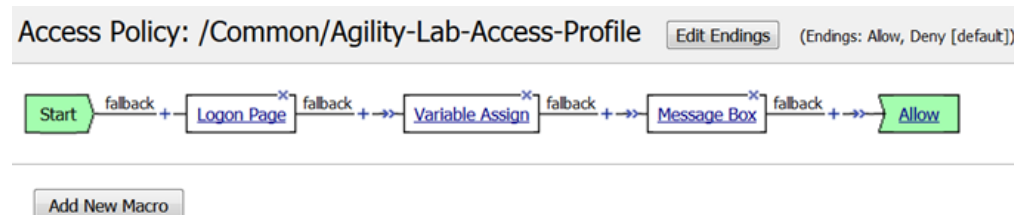
1. Open the VPE and add a new AD Query action after the first Message Box action by selecting the **+** sign that follows.

	Begin typing to search	🔍

Logon | **Authentication** | **Assignment** | **Endpoint Security (Server-Side)** | **Endpoint Security (Client-Side)** | **General Purpose**

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

Cancel | Add Item | Help

2. Navigate to the Authentication tab and select the AD Query radial and click **Add Item**.

3. In the AD Query, use the drop-down dialog box on Server to select the /**Common/LAB_AD_AAA**
   server. Click the **Save** button.
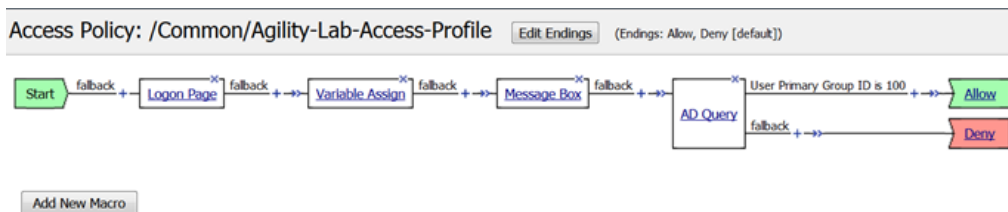
4. On the top branch following the AD Query action, add another Message Box.

Hint: A Message Box can be added by clicking the **+** sign, navigating to the General Purpose tab and
selecting Message Box

Add New Macro
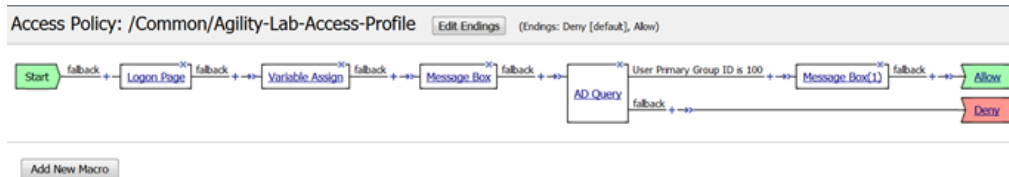
5. After the second Message Box add the AD Auth action from the Authentication tab

Hint: An AD Auth action can be added by clicking the **+** sign, navigating to the Authentication tab and selecting AD Auth

6. In the AD Auth properties window use the server drop-down menu to select /**Common**/**LAB_AD_AAA** server.

7. Click the **Save** button.

Add New Macro
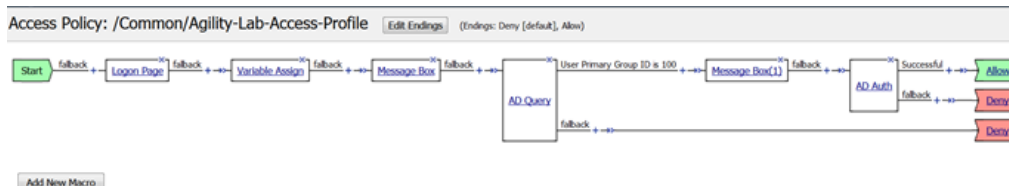
8. Your policy should now look like this

Notice that one the top branch to the AD Query object the line reads User Primary Group ID is 100 (See graphic in Step 8 above, just after AD Query). Maybe you do not want to query for that information and would prefer to delete that branch. You must be ***careful*** in what you select or do when deleting that branch when you have other actions following it in the policy or they could be deleted when you do not want them to be deleted. Here is a trick you can use to preserve the actions that follow the ad query when you need to delete a branch.

Add New Macro

415
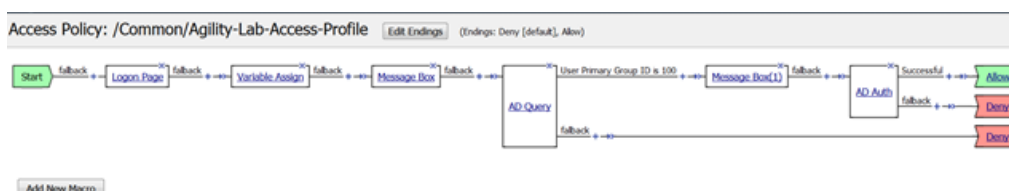
9. Just before the second Message Box after the "User Primary Group ID is 100" and after the **+** symbol there is a double arrow symbol. This will allow us to swap portions of the policy that come after that **->>-** double arrow to another location in the VPE policy.
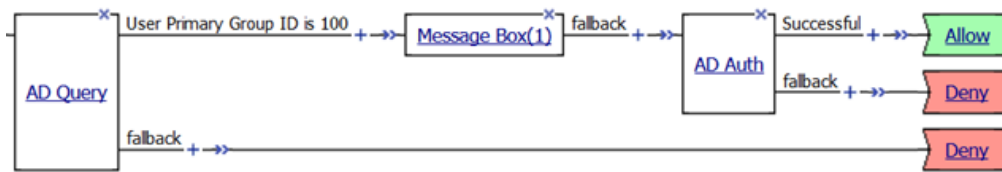
10. Click the **->>-** double arrow.
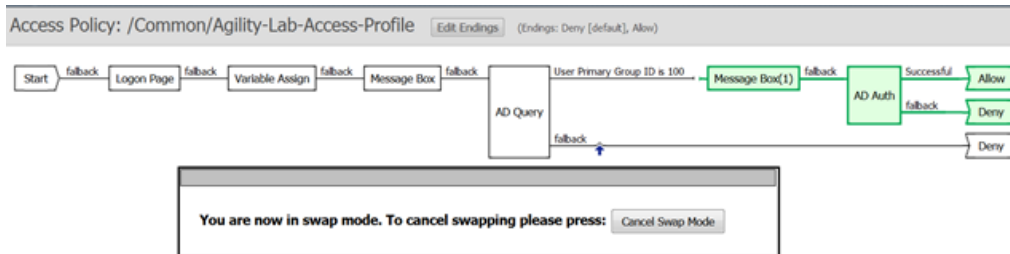
11. You will now notice a **vertical arrow** pointing to other locations in the VPE where this section high-lighted in green can be swapped.

12. Click on the **Vertical Arrow**
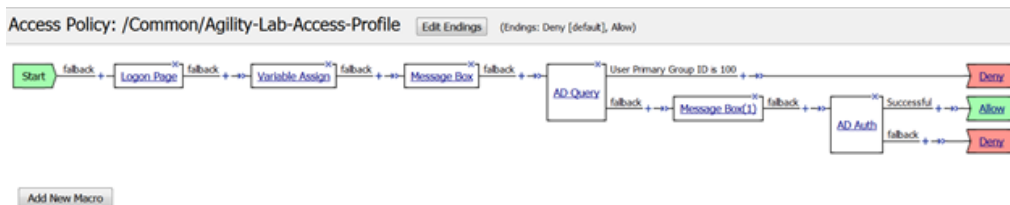
13. Now click the **AD Query** action in your policy and go to **Branch Rules** tab

14. Click the **X** to the right in the gray box for the Branch Rule

15. Click **Save** to save your settings
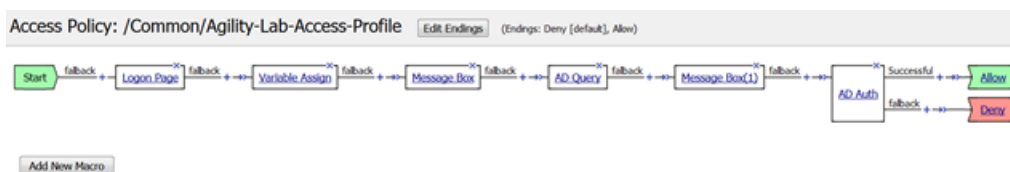
16. Your policy should now look like this. Now you can see how the Swap function can help with moving action objects throughout the VPE
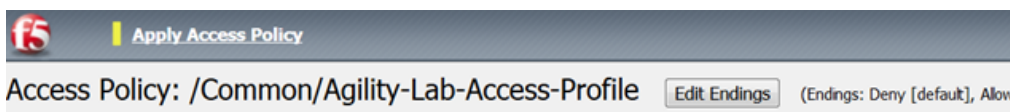
17. Click **Apply Access Policy** to save and implement or work

Now let's see what can be seen in the logs when set at the default logging level of Notice.

TEST 1
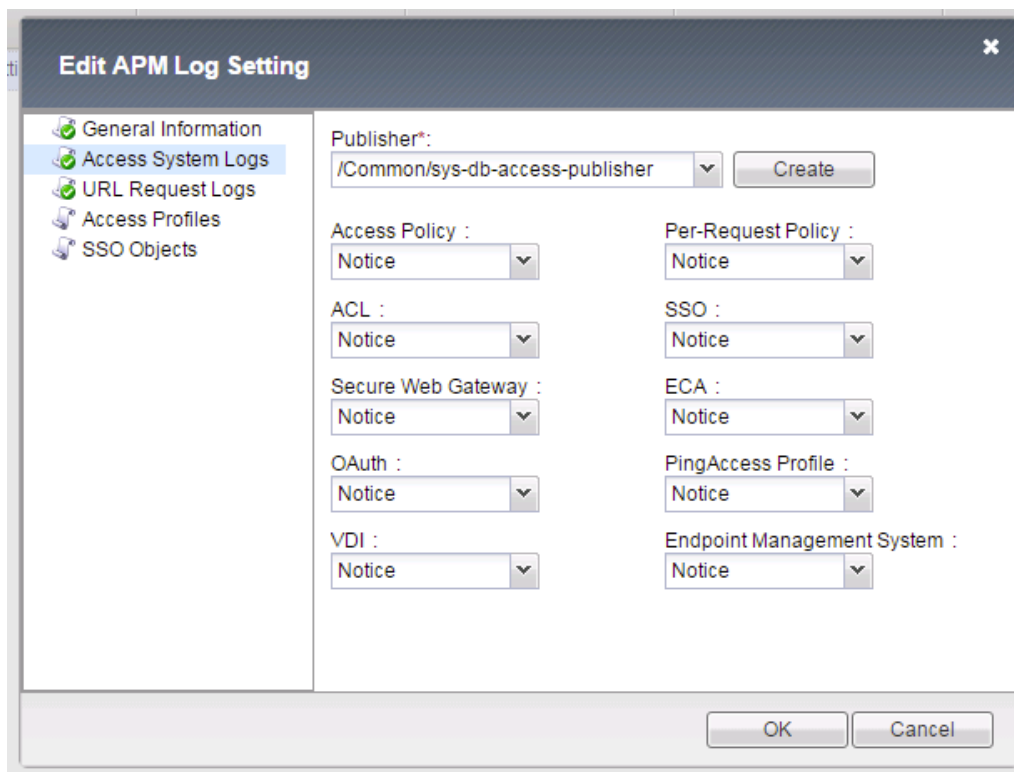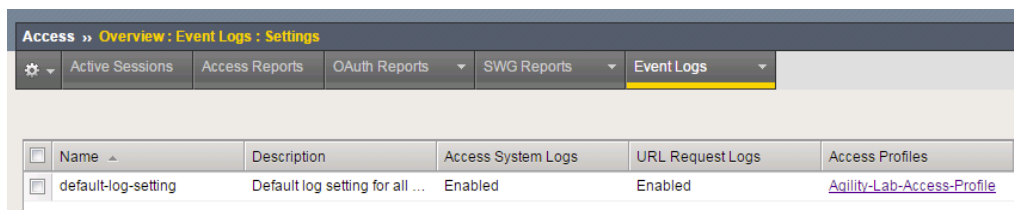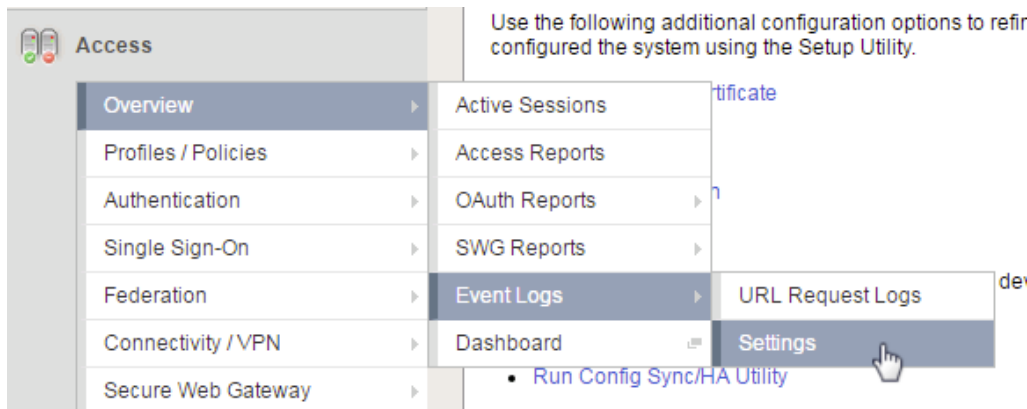
1. Review the current Access Policy Logging (Access ? Overview ? Event Logs -> Settings)

2. Select **default-log-setting**, then Click Edit to view settings.

3. Select **Access System Logs**
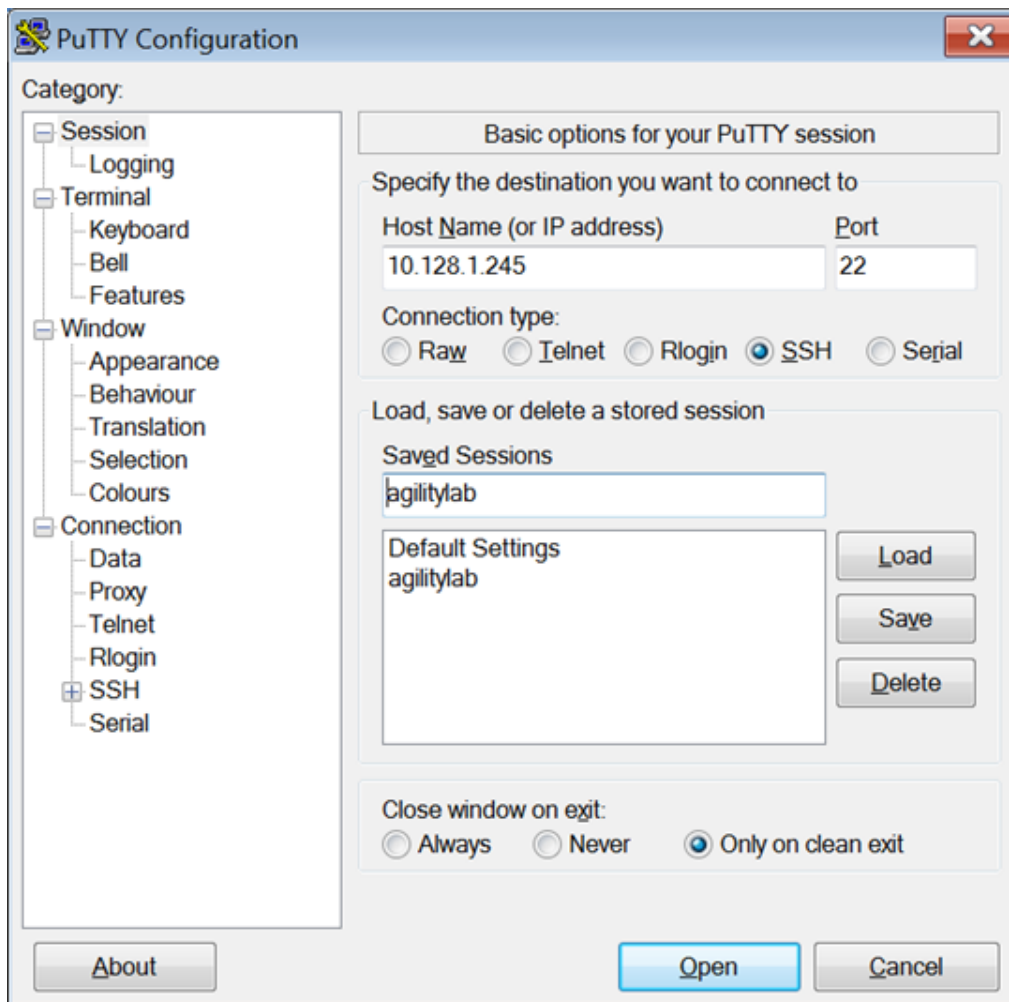
4. Logon to the BIGIP APM console using an SSH client (PuTTY from your desktop). Select **agilitylab** > **Load** > **Open**
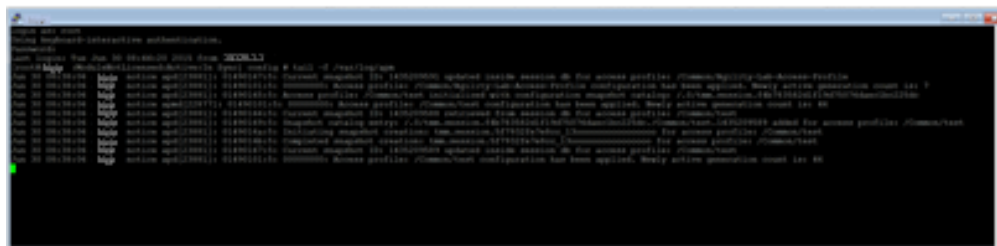
5. Maximize your SSH window to reduce line wrapping when reviewing the logs from the CLI.

6. From the CLI prompt, type **tail –f /var/log/apm** and hit **Enter** so you can start see the logs being displayed

Secure Logon
for F5 Networks

Username

student

Password

••••••••

Logon

With the SSH console logging, open a browser and access the APM as the user **student**.
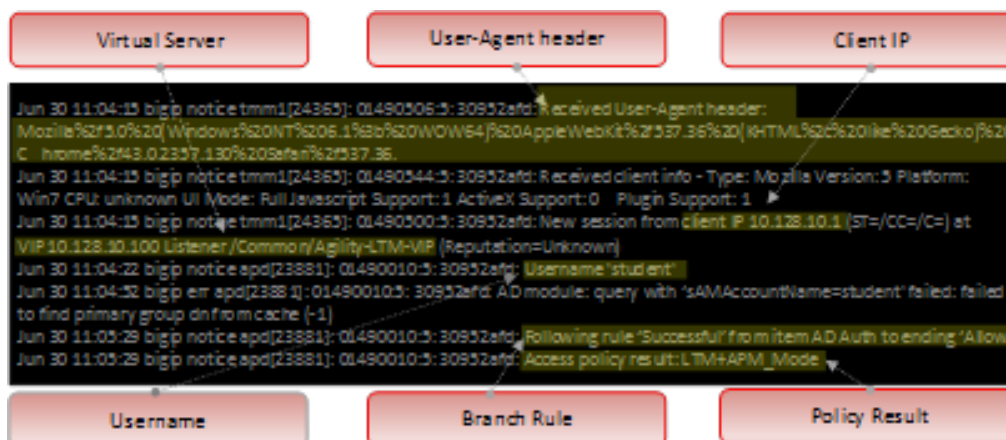
7. Notice the logs being produced at the different stages of the users session as it first reaches the VIP, then when the user authenticates, receives message boxes or other policy actions, and then when the user reaches the policy result.

With the *default logging* level, there are no session variables being logged.

In the Next test we will turn up logging to Informational and restart the user session and then in the last test change logging level to Debug and notice the differences from Informational and Notice logging levels.

8.7.4 Turning up the heat on Logging

Now let's test more verbose logging. You can step up from Notice to Informational and then to Debug if you want to see the differences yourself. For the purpose of this test though I will jump straight to Debug. You can use the GUI to make the log level changes to Debug or you could use the Traffic Management Shell (TMSH) command from the CLI to adjust the logging.

STEP 1

---

1. Change Access Policy log setting to Debug (Access -> Overview ? Event Logs ? Settings, select default-log-setting, then click Edit)

TIP: Make sure you change setting back to Notice when not troubleshooting. High levels of logging not only consume more disk space, but also consume other resources, such as CPU, when enabled.

TEST 2

1. Once you have the logging level increased restart you user session with the browser to the APM VIP and walk through the policy message boxes and other actions taking note of the additional verbosity in the logs you see in the SSH terminal window.

For sake of saving space in this document we will not include the screen shots showing the Informational and Debug logging messages and allow you to experience that yourself during your tests.

8.7.5 SessionDump Command

SessionDump is a command line utility that shows sessions and their associated session variables (like GUI Reports)

The sessiondump command has sever switches that can be used and you can further enhance your troubleshooting by additionally using other CLI utilities like grep to help filter the results to certain information. As you can see from the examples below, the first command simple provides all keys to be dumped for any/all user sessions while the second using grep allows you to filter the output to those associated with a given username. Refer to the screen shots below if you need additional detail.

This first example uses just the –allkeys switch.

sessiondump –allkeys

```
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # sessiondump -allkeys | grep 'student'
8585 1863.session.logon ./Common/Agility-Lab-Access-Profile_act_logon_page_ag.logonname 7 student
8585 1863.session.logon ./Common/Agility-Lab-Access-Profile_act_logon_page_ag.username 7 student
8585 1863.session.logon.last.logonname 7 student
8585 1863.session.logon.last.username 7 student
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config #
```

This second example also uses the –allkeys switch. However, it also adds the |grep command to search for the "username"

sessiondump -allkeys | grep 'student'

STEP 1
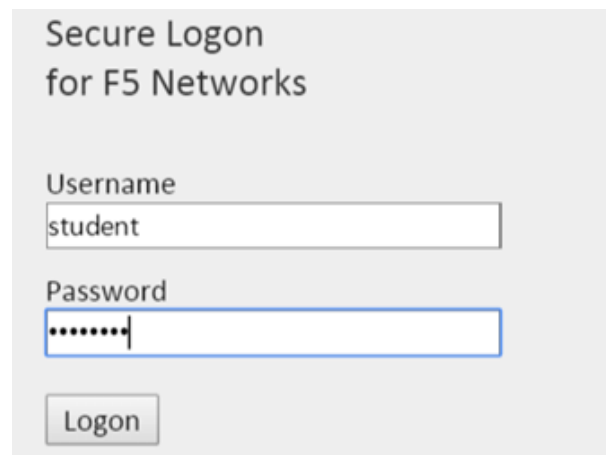
```
Jun 30 18:08:22 bigip notice tmm[24365]: 01490521:5: 8585 1863: Session statistics - bytes in: 3775, bytes out: 2696
^C
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config #
```

1. On the command line, if you still had the tail command showing logging then stop that now by typing **CTRL-C**

```
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # sessiondump –allkeys
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config #
```

Remember back in previous labs we learned that Session Variables cannot be displayed in the Reports screens if the User Session is not in an ***Active*** state. Well that is the same with the CLI sessiondump utility. There must be active sessions through APM in order to dump details.

2. Once you are at the command prompt again try using the **sessiondump –allkeys** command first. Did you receive any data after running the command? If not, then why?

Secure Logon
for F5 Networks

Username

student

Password

••••••••

Logon

3. If all your previous sessions have expired then startup and new session as a user and logon to APM and click through the message boxes.

4. Now on the console type: **sessiondump –allkeys.** You should see a long list of information.

Compare that with running: sessiondump –allkeys | grep student You should then only see the lines that had the username you specified in the command to be returned

Now let us have some fun with using this utility to help with SSO troubleshooting/validation.
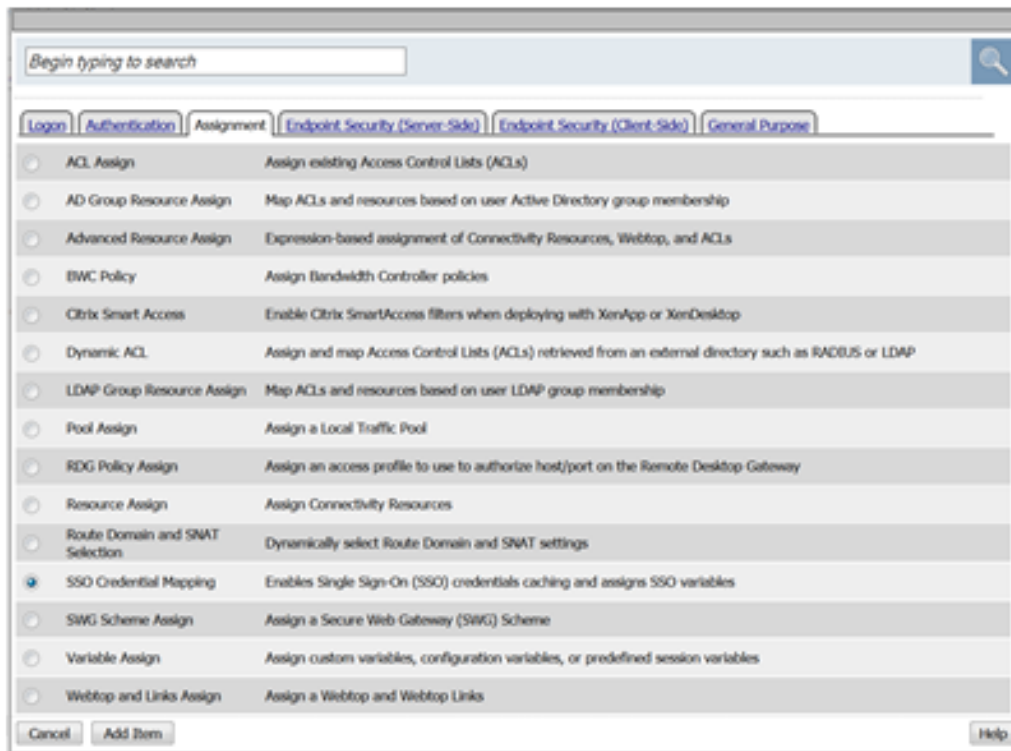
STEP 2

1. Edit the VPE for the **Agility-Lab-Access-Profile** policy we have been working with.

2. Add two new actions to the policy after the AD Auth on the successful branch.

3. First after AD Auth add the SSO Credential Mapping action from the Assignment Tab. Click **Add Item**
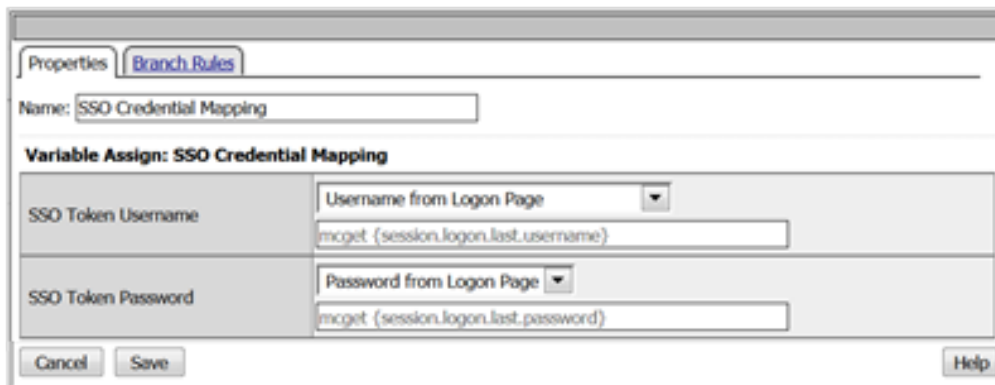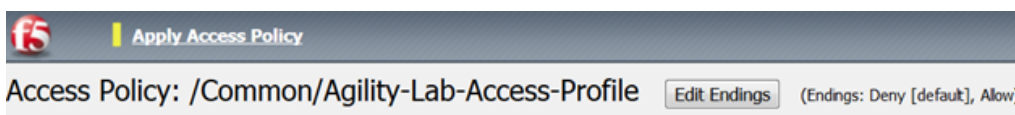

4. Keep the default settings and click **Save**.
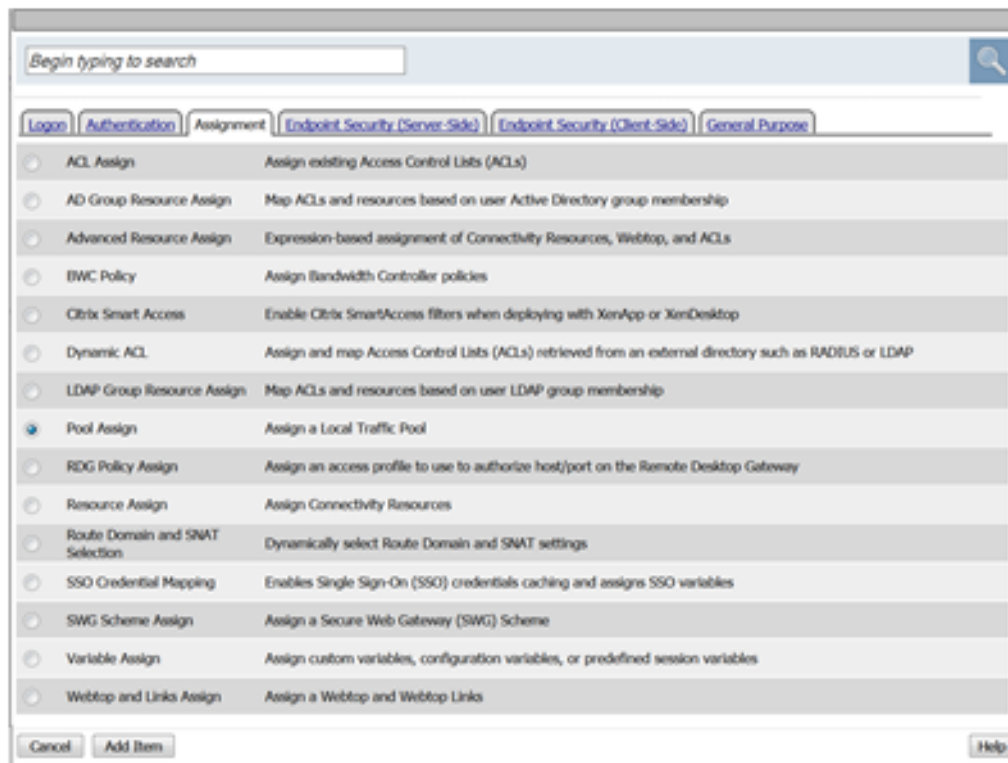
5. Next add after the SSO Credential Mapping action add a Pool Assign action from the Assignment tab.

6. In the next window click the **Add\Delete** link.

7. Then select the radio button for /**Common**/**Agility-Lab-Pool**. Now click the **Save** button.

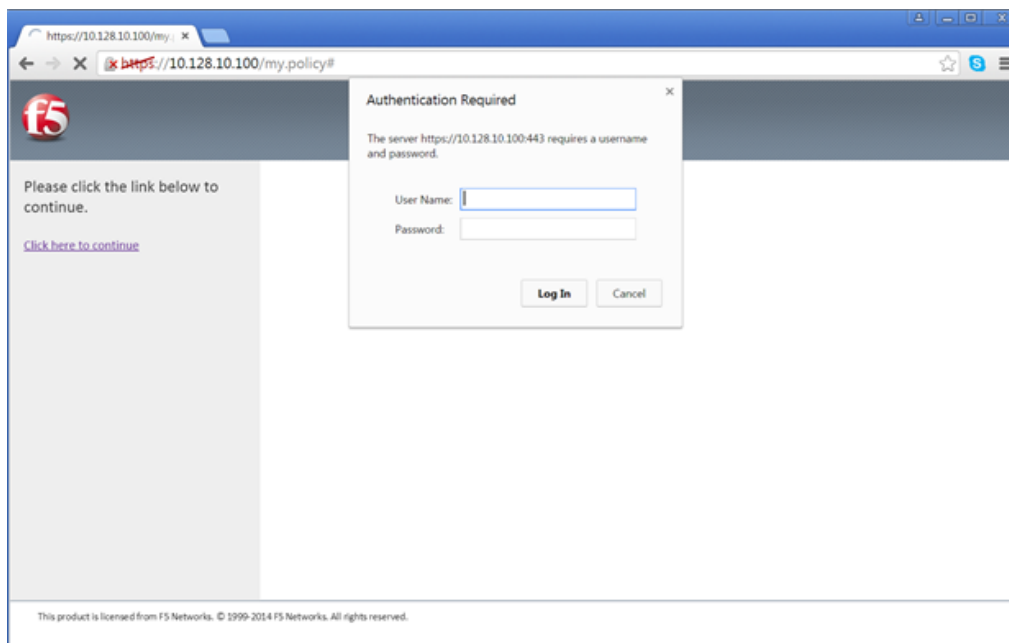8. Then click Apply Access Policy link on top left of page.

TEST 2

Secure Logon
for F5 Networks

Username
student

Password
••••••••

Logon

1. Restart a new APM user session. Logon and follow through all the policy actions

2. This time instead of seeing a browser error you should be getting prompted for authentication for a website which is the site being hosted on the pool member that we assigned to the policy. Why are we getting prompted for authentication though? Did we not add the SSO Credential Mapping to the policy as well?


3. Let's use the following command at the console to check if we are getting credentials mapped to token variables properly: **sessiondump –allkeys | grep 'sso'** You should see two lines that show something like this following picture.

If you see the two lines with session.sso.token.last, then we know the credential mapping is happening and the username should be displayed accordingly. So what's missing?
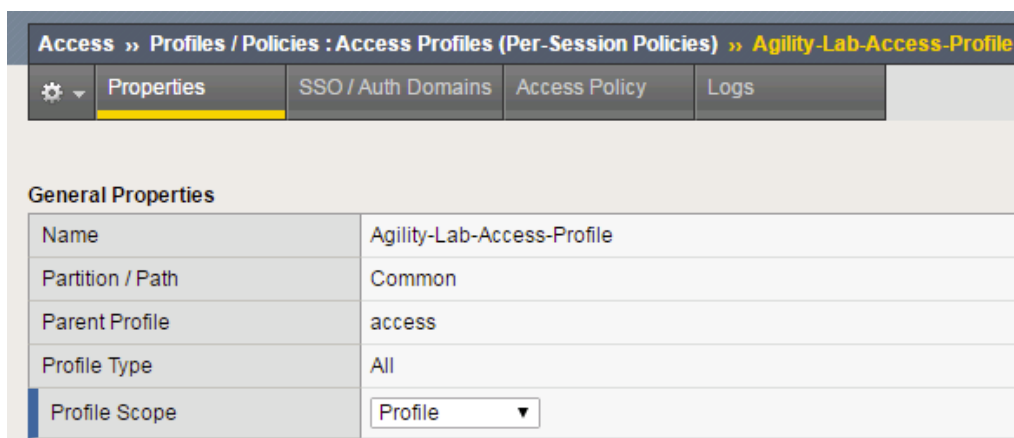
STEP 3
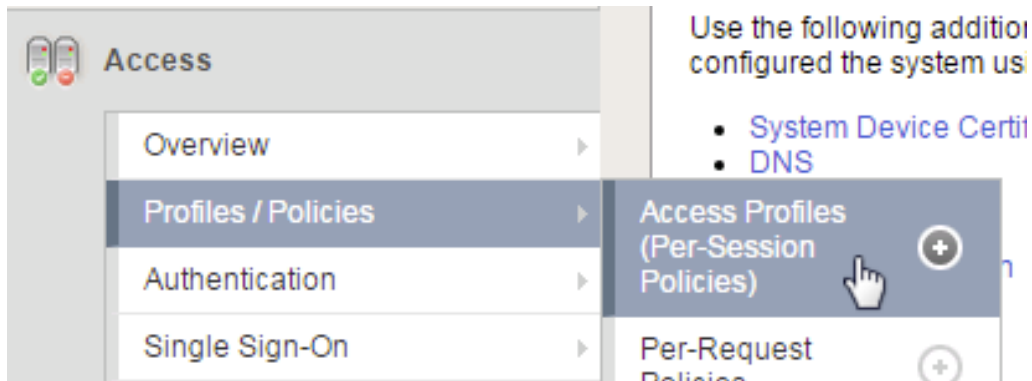
1. Next go to the Access Policy menu, click on Access -> Profiles/Policies -> Access Profiles (Per-Session Policies) .
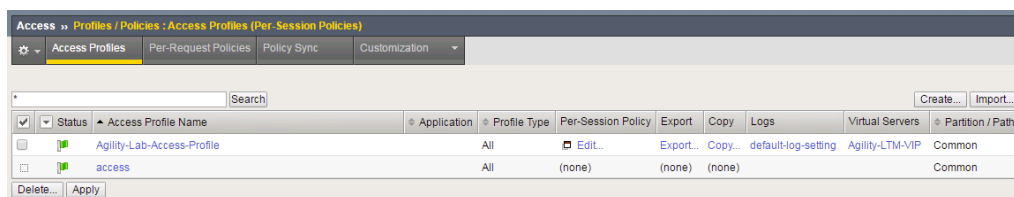
2. In the list of access profiles, click the NAME of your access profile, **Agility-LAB-Access-Profile**

3. When this page opens, look at the top, there are four tabs, click the **SSO** / **Auth Domains** tab

4. On this page, use the drop down menu on the SSO Configuration row to select **Agility_Lab_SSO_NTLM**. Then click Update

5. Then click **Apply Access Policy** on the top left of the page and apply the policy on the next page.

TEST 3

1. Restart your user session again to the VIP and logon and click through the actions.

If necessary, you can kill your existing session by navigating to Access Policy ? Manage Sessions, then select the user/session and Click Kill Selected Sessions
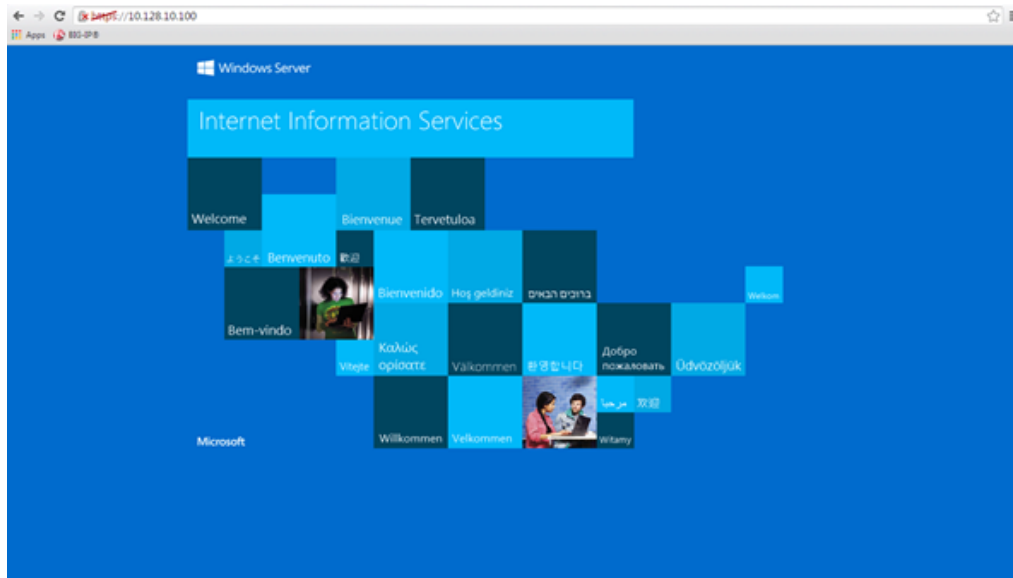
2. Now what do you see when the policy has completed? Are you seeing the web application without being prompted for an additional logon prompt from the application? If so, then you were successful.

8.7.6 ADTest Tool

In this section we will get familiar with anther CLI utility to assist in verifying proper authentication and query capabilities to an Active Directory domain. We need to prepare for this lab by making a quick change to the BIGIP's configuration.

STEP 1

1. Navigate to System > Configuration > Device ? DNS

2. Highlight **10.128.10.100** in the DNS Lookup Server List and click **Delete**.

3. Also highlight and **Delete** the DNS Search Domain List of **agilitylab.com**

4. Click the **Update** button.

The **/usr/local/bin/adtest** utility is a test tool for APM's Active Directory Module

tYPICAL USAGE	

Auth Test with Administrative username & password (not necessary)	`[root@bigip:ModuleNotLicensed:Active:Standalone] config # adtest -t auth -r "agilitylab.com" -A administrator -W adminpass -u student -w password`
	`Test done: total tests: 1, success=1, failure=0`
	`[root@bigip:ModuleNotLicensed:Active:Standalone] config #`

Auth Test without just username and password	`[root@bigip:ModuleNotLicensed:Active:Standalone] config # adtest -t auth -r "agilitylab.com" -u student -w password`
	`Test done: total tests: 1, success=1, failure=0`
	`[root@bigip:ModuleNotLicensed:Active:Standalone] config #`

Query Test With Administrative username and password	`[root@bigip:ModuleNotLicensed:Active:Standalone] config # adtest -t query -r "agilitylab.com" -A administrator -W adminpass -u student -w password`
	`Test done: total tests: 1, success=1, failure=0`
	`[root@bigip:ModuleNotLicensed:Active:Standalone] config #`

The ADTest tool can help point out potential issues with a BIG-IP's configuration or interoperability issues on the server's side.

COMMON ERRORS	
ERROR: query with '(sAMAccountName=student)' failed in krb5_get_init_creds_password(): Preauthentication failed, principal name: administrator@agilitylab.com (-1765328360) **Test done: total tests: 1, success=0, failure=1**	The cause of this is simply failed administrative credentials while attempting a query
ERROR: query with '(sAMAccountName=student)' failed in ldap_sasl_interactive_bind_s(): Local error, SASL(-1): generic failure: GSSAPI Error: Unspecified GSS failure. Minor code may provide more information (Cannot find KDC for requested realm) (-2) **Test done: total tests: 1, success=0, failure=1**	The cause of this is typically failed DNS resolution

Refer to the screen shots below if you need additional information regarding the options of ADTest.

```
usage: adtest [options]
   -t <auth|query|chgpswd|join|chgmpswd>      test type [auth|query|chgpswd|join|chgmpswd]
   -T                       timing
   -r <domain_name>      realm
   -h <kdc_name>         hostname
   -p <num>              port
   -A <admin_name>       adminName
   -W <admin_pass>       adminPassword
   -f <filter>           filter [default: 'sAMAccountName=<userName>']
   -C <cache_root>       credential cache file root [default: '/tmp']
   -u <user_name>        userName
   -M <machine_name>     machineName
   -O <operating_system_name>   operatingSystemName
   -V <operating_system_version>        operatingSystemVersion
   -E <machine_description>      machineDescription
   -D <user_domain>      userDomain
   -w <user_pass>        userPassword
   -N <new_pass>         newPassword
   -s                    check new password against domain password policies
   -g                    fetch primary group
   -G                    fetch nested groups
   -P                    fetch password expiration time
   -U                    cross-realm support (UPN enable)
```

TEST 1

f5

Secure Logon
for F5 Networks

The username or password is not correct.
Please try again.

Username

Password

Logon

1. Try logging on to the VIP as a user again after removing the DNS entries. You will notice that your logon will likely fail and you will receive the following screen.

Local Time	Log Message
2014-05-30 13:58:57	Received User-Agent header: Mozilla%2f5.0%20(Windows%20NT%206.1%3b%20WOW64)%
2014-05-30 13:58:57	Received client info - Type: Mozilla Version: 5 Platform: Win7 CPU: unknown UI Mode: Full Ja
2014-05-30 13:58:57	New session from client IP 10.10.50.27 (ST=/CC=/C=) at VIP 10.10.50.71 Listener /Common/.
2014-05-30 13:59:10	Username 'apmdemo'
2014-05-30 13:59:12	AD module: query with '(sAMAccountName=apmdemo)' failed: (0)
2014-05-30 13:59:16	AD module: authentication with 'apmdemo' failed: (1589641232)

2. Review the session details for this logon session in reports or manage sessions. As we can see from the session details the AD Query is failing as well as AD Auth

```
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # adtest -t
auth -r "agilitylab.com" -u student -w password.
```

3. Now we can test from the console. Open a console/ssh session. Using the following command let us first test authentication using the ADtest utility. **adtest -t auth -r "agilitylab.com" -u student -w password**. What result did you get with that test?

```
[root@bigip:ModuleNotLicensed:Active:Disconnected (Sync Only)] config # adtest -t
query -r "agilitylab.com" -A Administrator -W adminpass -u student -w password
```

4. Now let's try a query test. **adtest -t query -r "agilitylab.com" -A Administrator -W adminpass -u student -w password**. What result was returned?

System » Configuration : Device : DNS

Device | Local Traffic | AWS

Properties

DNS Lookup Server List	Address: 10.128.20.100 [Add] 10.128.20.100 [Edit] [Delete] [Up] [Down]
BIND Forwarder Server List	Address: [Add] [Edit] [Delete] [Up] [Down]
DNS Search Domain List	Address: agilitylab.com [Add] localdomain agilitylab.com [Edit] [Delete] [Up] [Down]
DNS Cache	☐
IP Version	IPv4 ▾

[Update]

5. Go back to the DNS Settings section and re-add the DNS server IP and domain. Then re-test the Auth and Query using the ADtest utility.

8.7.7 iRules Logging Assistance

As many know one of the most useful features of F5 BIGIP TMOS is the flexibility provided by iRules.

With APM and iRules you can accomplish many things, in fact you can now use iRules to create APM sessions. We are not going to go over that here however for the purpose of how iRules can be used for troubleshooting we will provide some highlights.

Often you can run into problems wherein an application single sign-on is not being processed and completing as it should. What happens as a result of the initial setup not working im/_static/class4tely is that many people start second guessing what is happening as traffic passes from the clients browser, to the front client side of the BIGIP VIP, then what F5 VIP is actually able to SEE, next What does LTM see, APM see, what is being passed along the way at each stage of the transaction through the BIGIP, and of course what does the BIGIP APM then forward to the Backend Server Application and How does that Backend Server Application respond? Fortunately, iRules can be very beneficial in this process to collect and subsequently log specific data at each stage which greatly enhances the troubleshooting capabilities.

We all know that TCPDump can be your friend in capturing data to analyze however at times the application workflows between client f5 and server and encryption along the way can hamper what TCPDump could capture for analysis. Another issue with TCPDump is that is captures a lot of data that then needs to be analyzed. Granted TCPDump provides a filtering capability to weed through that extra data however when you compare it to using some targeted iRules to collect APM session variables and data to be output to logs it makes it easier to review the application flow more specific to the steps you are trying to validate.

By default, APM in the current code release automatically secures that variables that are entered into the logon page on APM. Furthermore, the password is hidden from the reports screen session variable view and hidden from the database. Yet there are times when the Admin of the APM may need to have access to the decrypted password to either verify that the correct information is being keyed by user, received by APM and sent from APM to servers. Fortunately, there is a way using an iRule to do just this for our troubleshooting purpose.

TEST 1

1. First open a console session to the BIGIP.

2. From the command prompt type: **tail –f /var/log/ltm**

3. Hit the enter key several times to move the text on the screen up to the top so you have a clear screen to start reviewing log data during this test.

4. Now open a browser and access the APM VIP and logon as a user.

5. When you reach the end of your APM policy take a look at the console session and note whether or not the logs provide any details about the username or password you just used to logon to APM.

6. Now in another browser open the APM Admin GUI.

7. Go to the reports screen and run the All Sessions Report.

8. Open the Session Variables link for the current session you have just started as the user.

9. Navigate down to the SSO folder and expand it.

10. Review the SSO Token Username and verify it displays the username you entered.

11. Review the SSO Token Password and verify it displays the password you entered. Or can you?

12. No, you cannot because it is obscured by default.

Next, we will implement an iRule to assist the Admin in verifying what password is being entered by the user.

An iRule has been created already and supplied for you so you won't need to create it yourself you only need to apply it to the Virtual Server under the Resources Tab.

STEP 2

1. Open the properties for the Virtual Server.

2. Click the resources Tab.

3. In the iRules section, click the Manage button.

4. In the right-side box scroll down to find the iRule named **Agility-201-Troubleshooting**

5. Highlight the iRule and click the arrow button to move it to the left box.

6. Click the finished button.

TEST 2

1. Navigate to Manage Sessions and Kill all existing sessions.

2. In the console screen, hit the enter key several times to move any existing output up to the top of the window, then enter the following command **tail –F /var/log/ltm**

3. In the browser for user session testing, restart the session back to the APM VIP and logon with your username and password.

4. Click through to the end of the policy.

5. Now go back to the console session and review the log messages.

6. Do you see the username you entered in the logon page?

7. Do you see the password you entered in the logon page? If you answered yes then you were successful. Congratulations!

8.7.8 TCPDump Troubleshooting Assistance

Beginning in BIG-IP 11.2.0, you can use the "**p**" interface modifier with the "**p**" modifier to capture traffic with TMM information for a specific flow, and its related peer flow. The "**p**" modifier allows you to capture a specific traffic flow through the BIG-IP system from end to end, even when the configuration uses a Secure Network Address Translation (SNAT) or OneConnect. For example, the following command searches for traffic to or from client **10.128.10.100** on interface **0.0**:

tcpdump -ni 0.0:nnnp -s0 -c 100000 -w /var/tmp/capture.dmp host 10.128.10.100

Once **tcpdump** identifies a related flow, the flow is marked in TMM, and every subsequent packet in the flow (on both sides of the BIG-IP system) is written to the capture file.

8.8 Conclusion

In this lab, you learned how to use various tools including APM logs, ADTest, TCPDump to aid in troubleshooting common Access Policy Manager (APM) issues relating to Access Policy configuration, user authentication, and session variables.

8.8.1 Learn More

Links & Information

• **Identity & Access Management Labs**

http://clouddocs.f5.com/training/community/iam/html/

• **BIG-IP APM 13.1.0 Knowledge Center**

https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20APM&version=13.1.0

- **Manual: F5 BIG-IP Access Policy Management Operations Guide**

  https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/f5-apm-operations-guide.html

- **Manual: F5 BIG-IP Edge Client Operations Guide**

  https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/f5-edge-client-operations-guide.html

- **K13595: Frequently used tools for troubleshooting BIG-IP APM and Edge Gateway issues (11.x)**

  https://support.f5.com/csp/article/K13595

- **K14184: Troubleshooting BIG-IP APM portal applications**

  https://support.f5.com/csp/article/K14184

- **K12444: Overview of the Client Troubleshooting Utility for Windows**

  https://support.f5.com/csp/article/K12444

- **K11898: Information required when opening a support case for BIG-IP APM**

  https://support.f5.com/csp/article/K11898

Class 9: Multi-Factor Auth for Cloud Applications

This lab will teach you how to configure APM environment in order to configure multi factor authentication (MFA) using F5 Adaptive Authentication, google authenticator(GA) and DUO. Also, you will be able to configure Single Sign On (SSO) for cloud apps (AWS, Salesforce).

This class covers the following topics:

- **Create a basic APM Policy**
- **Setup AWS Connector**
- **Setup Salesforce Connector**
- **Set up Google Authenticator (GA) as Second Auth Factor**
- **Set up DUO as Second Auth Factor**

Expected time to complete: **3 hours**

9.1 Getting Started

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

Please follow the instructions provided by the instructor to start your lab and access your jump box.

Note: All work for this lab will be performed exclusively from the Windows **Jumpbox**. No installation or interaction with your local system is required.

9.1.1 Lab Topology

The following components have been included in your lab environment:

- **1 x F5 BIG-IP VE_13** (`10.1.1.245`)
    - Provisioned with APM
- **1 x Windows 7** (`10.1.1.199`)

- **–** Jumpbox machine

- **–** Jumpbox user (external_user)

- **1 X Windows Server 2008** `(10.1.1.245)`

  - **–** AAA server (Active Directory)

  - **–** User (administrator)

- **1 X Windows 7 Internal** `(10.1.1.198)`

  - **–** Internal server used to demo SSO to RDP servers

- **1 X Linux LAMP Webserver**

  - **–** Internal Portal

Lab Components

The following credentials will be utilized throughout this Lab guide:

HOST/RESOURCE	USERNAME	PASSWORD
BIG-IP Configuration Utility (GUI)	`admin`	`password`
BIG-IP CLI Access (SSH)	`root`	`password`
Jumphost Access	`external_user`	`password`
Windows Server 2008 (AD) Access	`administrator`	`password`
Sales User	`sales_user`	`sales`
Sales Manager User	`sales_manager`	`manager`
Partner User	`partner_user`	`partner`
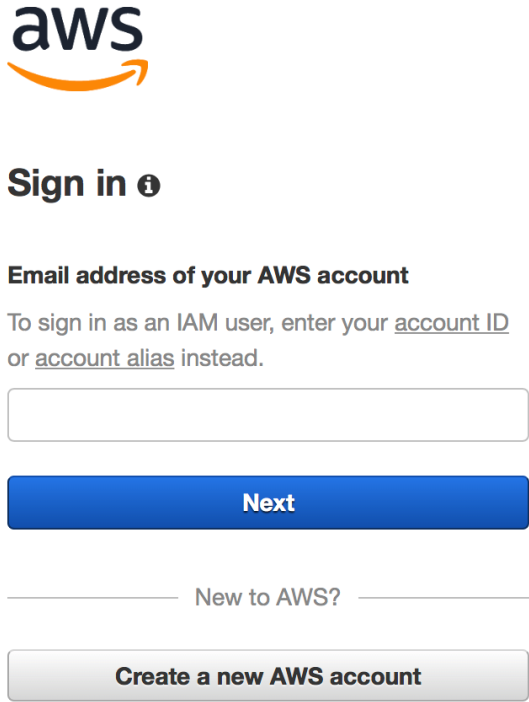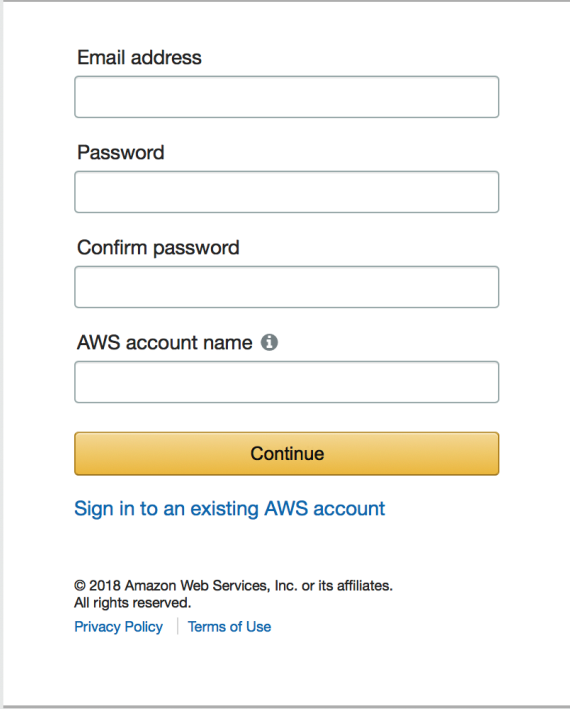
9.2 Pre-Work Activities

In this module you will create or download all the requirements to configure the **MFA for Cloud Apps Lab**

9.2.1 Lab – Pre-Work

Estimated completion time: **10 minutes**

9.2.2 Task - Create AWS Account

1. Go to AWS page	https://console.aws.amazon.com/console/home
2. Click create new AWS account	**aws** **Sign in** ⓘ **Email address of your AWS account** To sign in as an IAM user, enter your account ID or account alias instead. [_____] **Next** — New to AWS? — **Create a new AWS account**
	Create an AWS account Email address [_____] Password [_____] Confirm password [_____] AWS account name ⓘ [_____] **Continue** Sign in to an existing AWS account © 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy │ Terms of Use
440 3. Complete all of the required fields.	
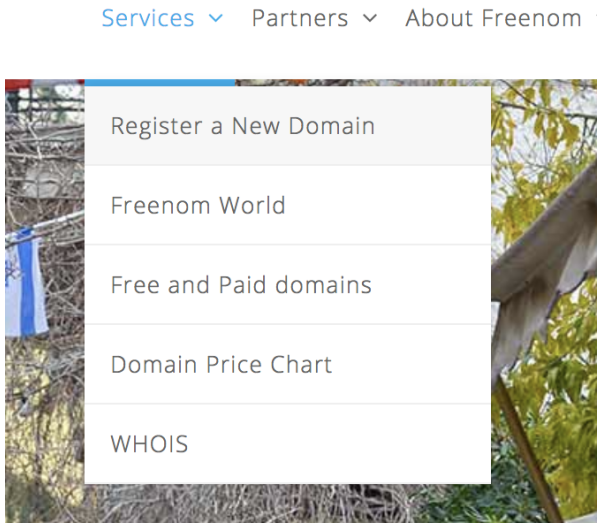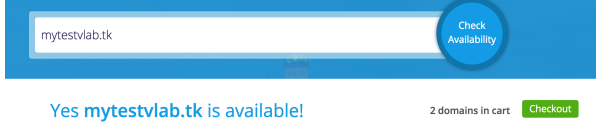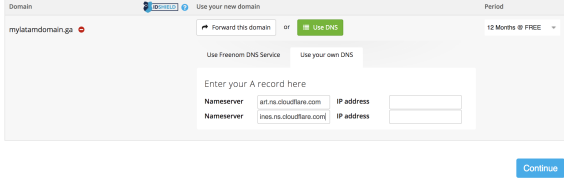
Note

Note: Payment information – Default Usage tier is **free for 1 year** with 750 hours a month compute (we will not be using any compute for this lab) and 5GB storage (`we will not be using any storage for this lab`).

9.2.3 Task - Create Salesforce Account

1. Go to Salesforce page	https://developer.salesforce.com/signup
2. Click create new Salesforce account	salesforce lightning platform Get your very own Developer Edition A full-featured copy of Lightning Platform, for FREE. **Name** First · Last **Email** Your email address **Role** Developer **Company** Company Name **Country** United States **Postal Code** **Username** Ex: name@yourcompany.com
3. Complete all of the required fields.	
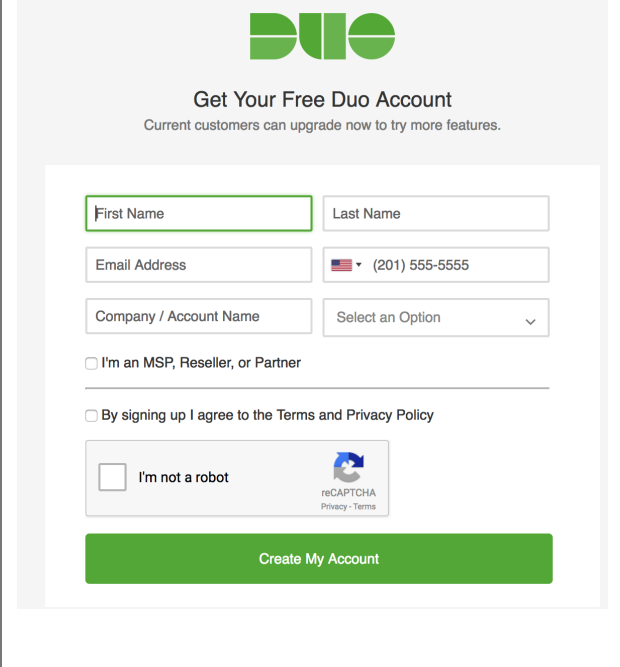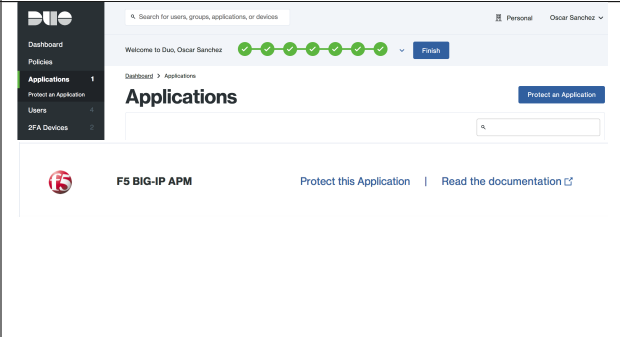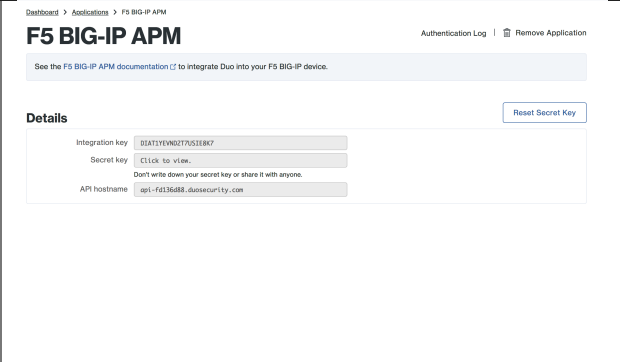
9.2.4 Task - Create (or use an existing) public domain

1. You can use **my.freenom** to create a new public domain	https://my.freenom.com
2. Go to **Services**, and then, **Register a New Domain**.	Services ∨ Partners ∨ About Freenom Register a New Domain Freenom World Free and Paid domains Domain Price Chart WHOIS
3. Introduce your new domain **mytestvlab.tk** (`select your own`), and check availability.	mytestvlab.tk — Check Availability Yes **mytestvlab.tk** is available! 2 domains in cart Checkout
4. At the bottom, click **Checkout**	1 domain in cart Checkout
5. Click in "**Use DNS**", and then "**Use your own DNS**" and introduce the hostnames : "**art.ns.cloudflare.com**" and " **ines.ns.cloudflare.com**". Select also a Period of 12 Months (`Free`)	Domain Use your new domain Period mylatamdomain.ga Forward this domain or Use DNS 12 Months @ FREE Use Freenom DNS Service Use your own DNS Enter your A record here Nameserver art.ns.cloudflare.com IP address Nameserver ines.ns.cloudflare.com IP address Continue
6. Finish the configuration signing in or registering with a personal account	**443**
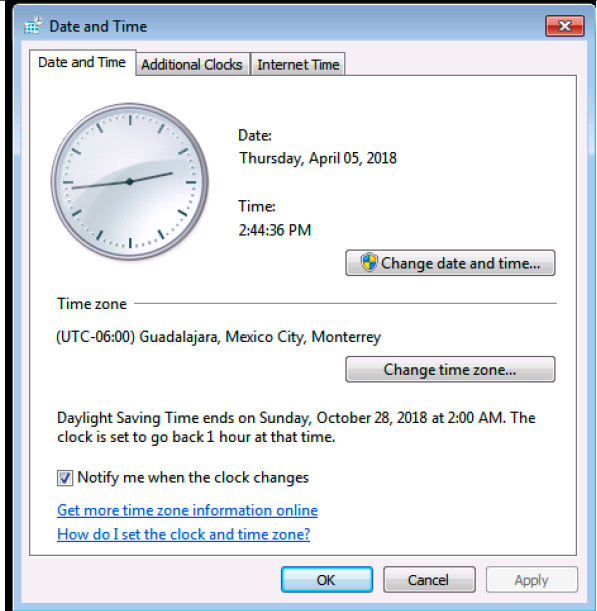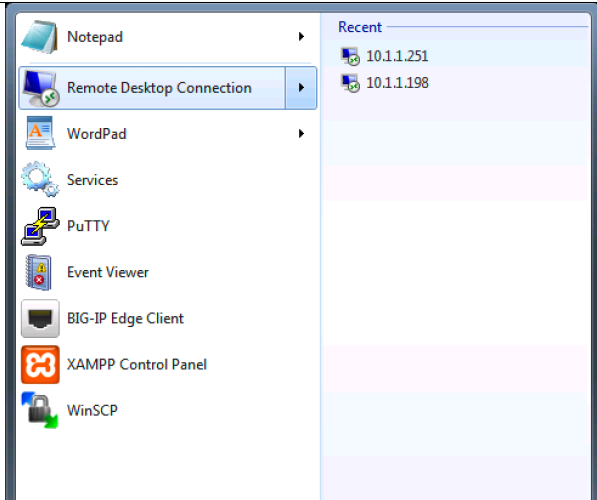
9.2.5 Task - Download Google Authenticator and DUO

1. Download **Google Authenticator** client to your smartphone.	1. Android
	   (a) https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid&hl=en
	 2. iOS
	   (a) https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

2. Download **DUO** client to your smartphone	1. iOS
	   (a) https://itunes.apple.com/us/app/duo-mobile/id422663827?mt=8
	 2. Android
	   (a) https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=en

9.2.6 Task - Create a DUO account

1. Sign up for a **DUO account**.

2. Log in to the **Duo Admin Panel** and navigate to **Applications**,
   then click **Protect an Application** and locate **F5 BIG-IP APM**
   in the applications list.

3. Click **Protect this Application** to get your `Integration Key,`
   `Secret Key,` and `API hostname.` We will use this information later.

9.2.7 Task - Log in to Ravello

1. Go to the **URL** provided by the instructor and login using the `username` and `password` assigned to you.	 1. Username = `latam_studentXX` 2. Password = `f5DEMOs4u`
2. Search **LATAM_MFA_Cloud_Apps_Agility** environment, then click on the link and verify that the VMs are running.	
3. Connect to **Windows 7 External** VM. You can use either Console shortcut or a RDP client. Then verify **time settings** and modify if it is necessary.	

9.3 Lab 1: Create a basic APM Policy

In this module you will learn how to configure a basic APM Policy

9.3.1 Lab – Create an APM Policy

This lab will teach you how to create a basic APM Policy using the GUI. Estimated completion time: **20 minutes**

9.3.2 Task - Setup Virtual Server

1. Go to **Local Traffic** -> **Virtual Servers** -> **Create**	
2. Enter the following values (leave others default) **Name:** `webtop_demo_vs` **Destination Address:** `10.1.10. 47` **Service Port:** `443` **HTTP Profile:** `http` **SSL Profile (Client):** `f5demo_client_ssl` **Source Address Translation:** `Àutomap`	

9.3.3 Task - Create a Connectivity Profile

1. Go to **Access** -> **Connectivity/VPN** -> **Profiles -> Add**	
2. Enter the following values (leave others default) **Name:** `webtop_demo_cp` **Parent Profile:** `/Common/connectivity`	

9.3.4 Task - Create an AD Server as AAA

1. Go to **Access** -> **Authentication** -> **Active Directory** -> **Create**	
2. Enter the following values (leave others default) **Name:** `webtop_demo_aaa_srvr` **Domain Name:** `f5demo.com` **Server Connection:** `Direct` **Domain Controller:** `10.1.20.251` **Admin Name:** `service_account` **Admin Password:** `password`	

9.3.5 Task - Create a container (webtop)

1. Go to **Access** -> **Webtop** -> **Webtop Lists** -> **Create**	
2. Enter the following values (leave others default) **Name:** `webtop_demo_webtop` **Type:** `Full`	

9.3.6 Task - Create a Portal Access

1. Go to **Access** -> **Connectivity/VPN: Portal Access List** -> **Create**	
2. Enter the following values (leave others default) **Name:** `portal_intranet` **Link Type:** `Application URI` **Application URI:** `http://10.1.20.32` **Caption:** `INTRANET`	

9.3.7 Task - Setup APM Profile

1. Go to **Access** -> **Profiles / Policies** -> **Access Profiles (Per Session Policies)** -> **Create**	
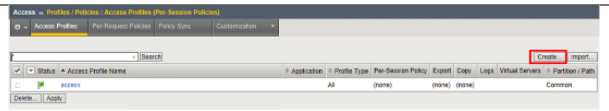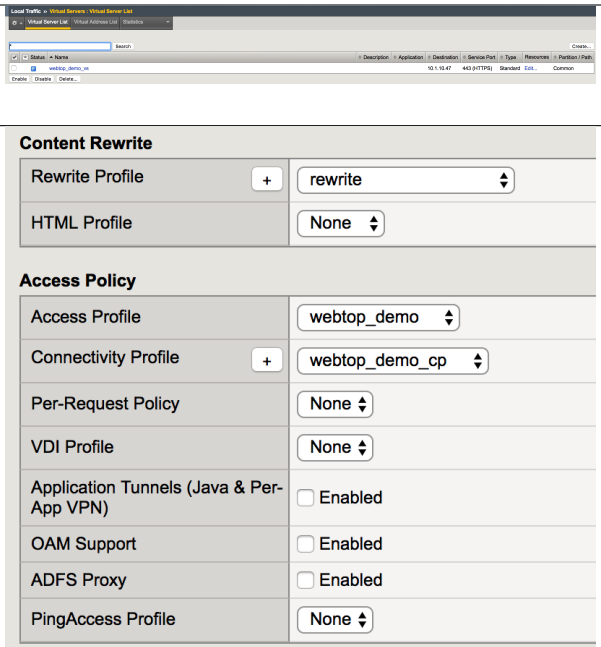
2. Enter the following values (leave others default) then click **Finished**
    Name: webtop_demo
    Profile Type: All
    Profile Scope: Profile
    Languages: English	
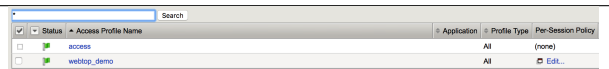
3. Click **Edit** for **webtop_demo**, a new browser tab will open	
4. Click the + between **Start** and **Deny**, select **Logon Page** from the **Logon** tab, click **Add Item**	

9.3.8 Task - Add the Access Policy to the Virtual Server

1. Go to **Local Traffic** -> **Virtual Servers** -> **webtop__demo_vs**	
2. Modify the **Rewrite Profile** setting to rewrite, **Access Profile** to `webtop_demo` and **Connectivity Profile** to `webtop_demo_cp`, then click **Update**	
3. Test access to `https://webtop.vlab.f5demo.com` (you can use the bookmark in Chrome) from the jump host, you should see a logon page. You can login with any user: • **sales_user** • **sales_manager** • **partner_user**	

9.4 Lab 2: Setup an AWS Connector

In this module you will learn how to configure an AWS Connector

9.4.1 Lab – Setup AWS Connector

This lab will teach you how to create a SAML AWS connector. Estimated completion time: **30 minutes**

9.4.2 Task - Download AWS metadata

1. From the jumpbox machine (**Win7**) , open new window browser tab to `https://signin.aws.amazon.com/static/saml-metadata.xml` and **download** de xml file to the **Desktop**. This file will be used to create and AWS external SP Connector on the BIG-IP.	
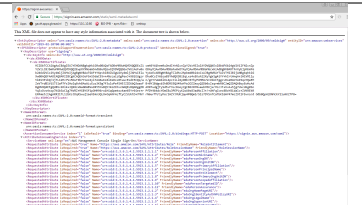
9.4.3 Task - Create an external SP connector to AWS

1. Logon onto BIG-IP, then go to **Access** -> **Federation: SAML Identity Provider** -> **External SP Connectors** -> **Create** -> **From Metadata**	
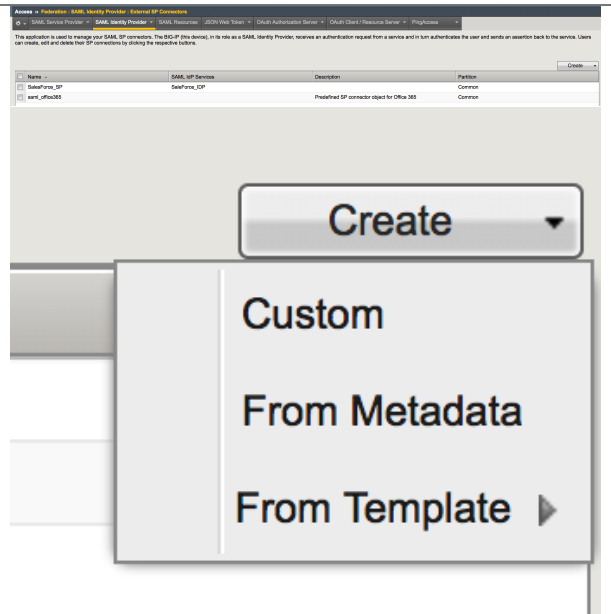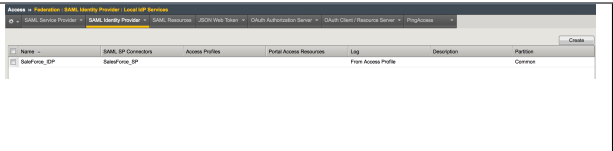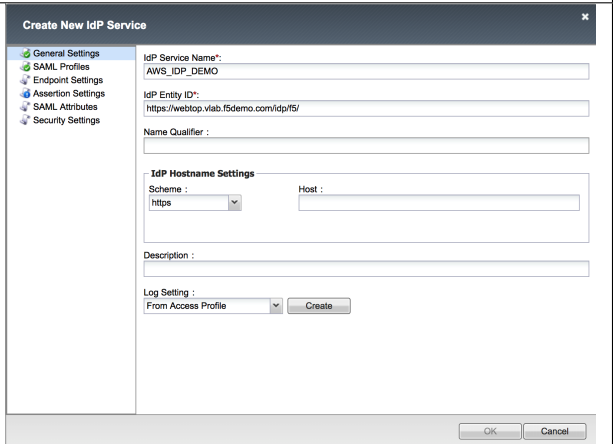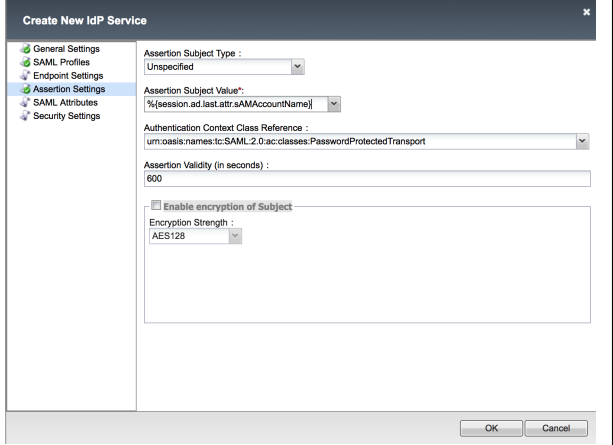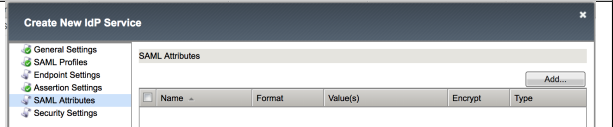
2. Enter the following values (leave others default) then click **OK**
    Select File: `saml-metadata.xml`
    Service Provider Name: `AWS_EXT_SP`	
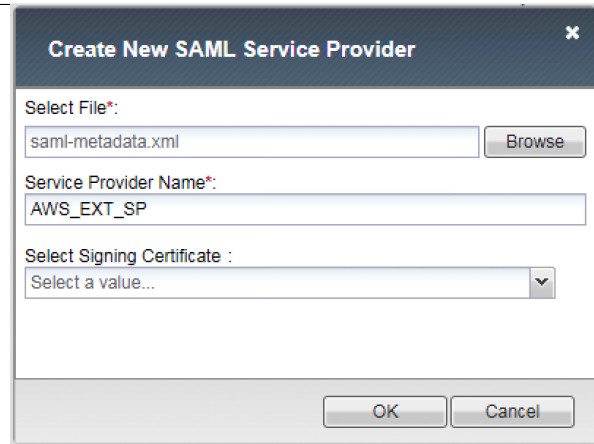
9.4.4 Task - Create a local IDP Service to AWS

1. Logon onto BIG-IP, then go to **Access** -> **Federation: SAML Identity Provider** -> **Local Idp Services** -> **Create**

2. Enter the following values (leave others default) on the **General Settings**
   Idp Service Name: `AWS_IDP_DEMO`
   IdP Entity ID: `https://webtop.vlab.f5demo.com/idp/f5/`

3. Enter the following values (leave others default) on the **Assertion Settings**.
   Assertion Subject Type: `Unspecified`
   Assertion Subject Value: `%{session.ad.last.attr.sAMAccountName}`
   Authentication Context Class Reference:
   `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`

9.4.5 Task - Download IdP metadata from BIG-IP for AWS

1. Go to **Access** -> **Federation: SAML Identity Provider** -> **Local IdP Services**, select the `AWS_IDP_DEMO` object, then click **Export Metadata**. Leave the **Sign Metadata** to **No**, and then click **Download**.

9.4.6 Task - Bind IdP and SP Connector to AWS

1. Go to **Access** -> **Federation: SAML Identity Provider** -> **Local IdP Services**, select the `AWS_IDP_DEMO` object, then click **Bind/Unbind SP Connector**. Then select `/Common/AWS_EXT_SP` as SP connector and click **OK**.
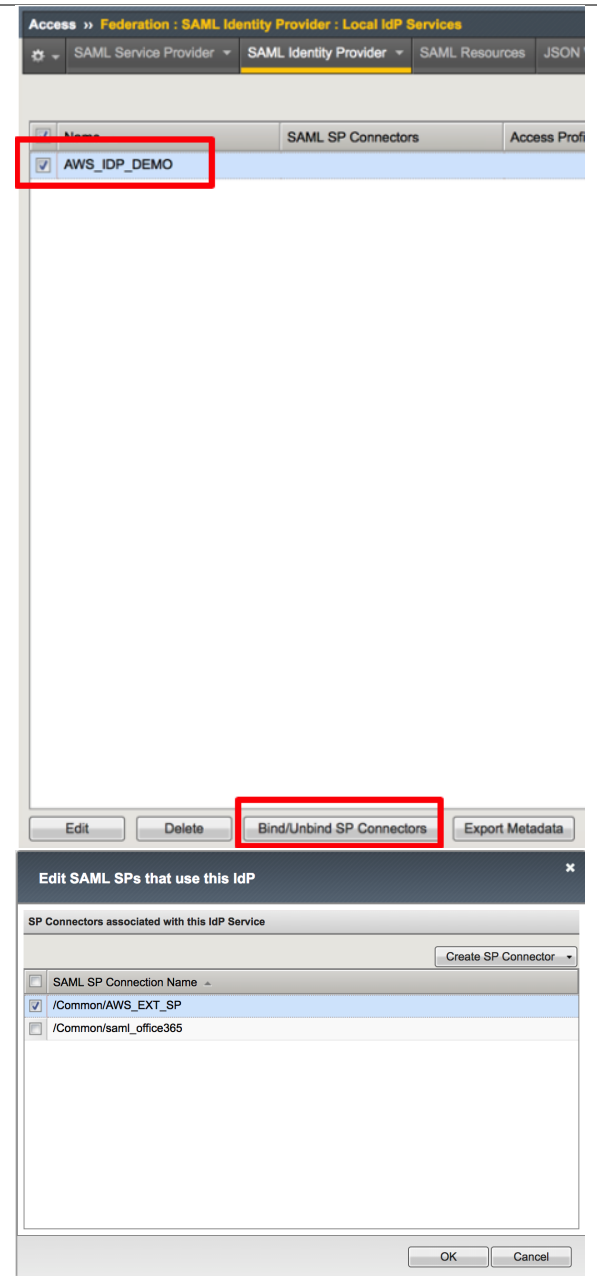
9.4.7 Task - Create an IdP provider in AWS

1. Sign in to the AWS Management Console and open the **IAM console** at `https://console.aws.amazon.com/iam/` then click **Identity Provider**	**Welcome to Identity and Access Management** IAM users sign-in link: https://572542488750.signin.aws.amazon.com/console | Customize IAM Resources Users: 0 Roles: 0 Groups: 0 Identity Providers: 0 Customer Managed Policies: 0 Security Status 1 out of 5 complete. ☑ Delete your root access keys ⚠ Activate MFA on your root account ⚠ Create individual IAM users ⚠ Use groups to assign permissions ⚠ Apply an IAM password policy
2. Click **Create Provider**	**Create Provider** **Delete Providers** Filter ☐ Provider Name ⇕ No records found.

3. Enter the following values (leave others default) on the **Configure Provider** tab, then click **Next Step**
 	
    Provider Type: `SAML`
    Provider Name: `f5demo`
    Metadata Document: `PATH\\AWS_IDP_DEMO_metadata.xml`
    For the `metadata` document choose the file that you already downloaded.
	Configure Provider
	Choose a provider type.
	Provider Type* SAML ▼
	Provider Name* f5demo
	  Maximum 128 characters. Use alphanumeric and '._-' characters.
	Metadata Document* C:\fakepath\AWS_IDP_DEMO_n **Choose File**

4. `Verify the information` you have provided, and then click **Create**.	**Verify Provider Information** Verify the following provider information. Click **Create** to finish. **Provider Name** f5demo **Type** SAML

9.4.8 Task - Create a new Role in AWS

1. In the left navigation pane, click **Roles**.	
2. Click **Create Role**	
3. Enter the following values (leave others default) on the **Select type of trusted entity** tab, then click **Next: Permisions** **Type of trusted entity:** `SAML 2.0` **SAML provider:** `f5demo` **Select:** `Allow programmatic and AWS Management Console` **Attribute:** `SAML:aud` **Value:** `https://signing.aws.amazon.com/saml`	

9.4.9 Task - Create a AWS SAML resource in BIG-IP

<table>
<tr>
<td>1. Go to Access -> Federation: SAML Resources -> Create.</td>
<td></td>
</tr>
<tr>
<td>2. Enter the following values (leave others default) on the New SAML Resource tab, then click Finished.

Name: AWS_SAML_DEMO
SSO Configuration: AWS_IDP_DEMO
Caption: AWS (SAML)</td>
<td></td>
</tr>
</table>

9.4.10 Task - Assign the AWS SAML resource

1. Go to **Access** -> **Profiles**/**Policies** -> **Access Profiles**, then click **Edit** for **webtop_demo**, a new browser tab will open
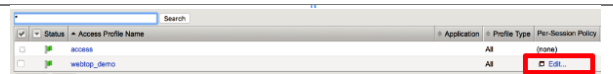
2. Click the + between **AD Auth** and **Advanced Resource Assign**, select **AD Query** from the **Authentication** tab, click **Add Item**

3. Enter the following values (leave others default) then click **Save**

> **Server:** `/Common/webtop_demo_aaa_srvr`
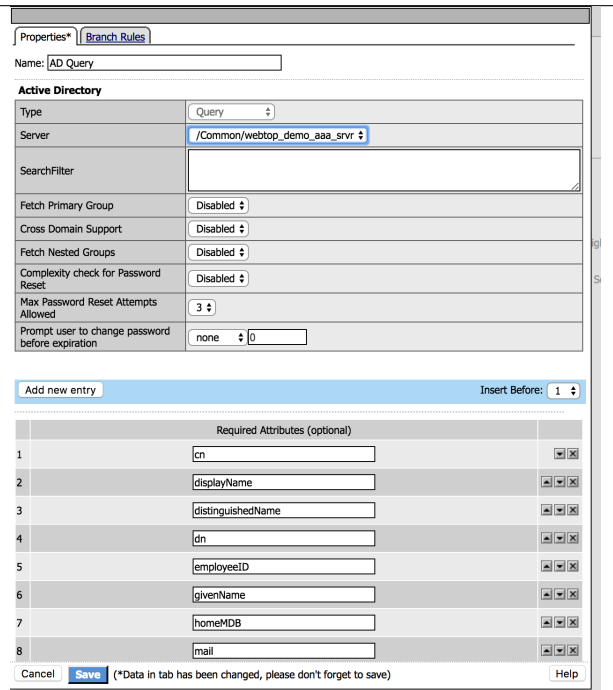
4. Click on the **AD Query** object, a new window will open. Click on the **Branch Rules** tab
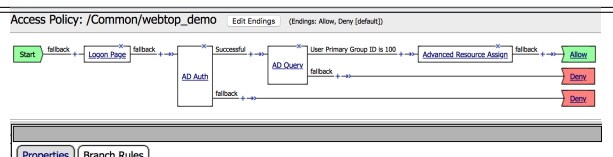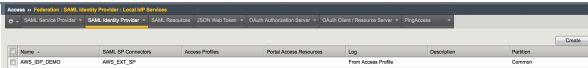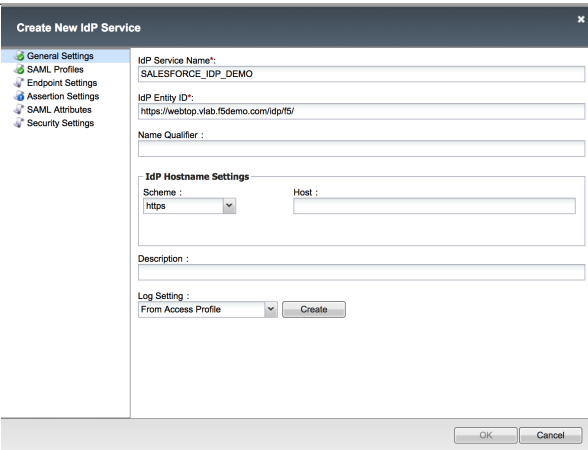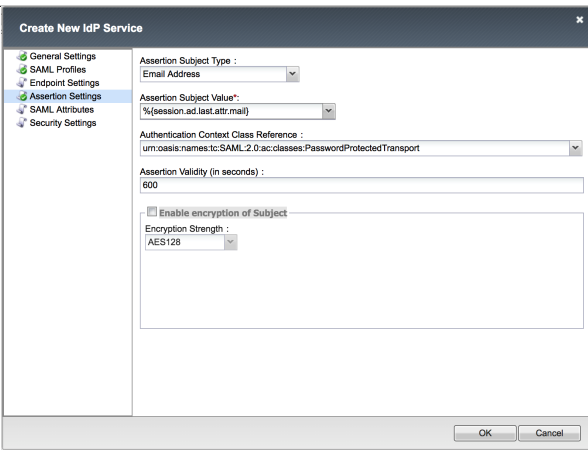
9.5 Lab 3: Setup a Salesforce Connector

In this module you will learn how to configure a Salesforce Connector.

9.5.1 Lab – Setup Salesforce Connector

This lab will teach you how to create a SAML Salesforce connector. Estimated completion time: **30 minutes**

9.5.2 Task - Create a local IDP Service to Salesforce

<table>
<tr>
<td>1. Logon onto BIG-IP, then go to Access -> Federation: SAML Identity Provider -> Local Idp Services -> Create</td>
<td></td>
</tr>
<tr>
<td>2. Enter the following values (leave others default) on the General Settings
Idp Service Name: <code>SALESFORCE_IDP_DEMO</code>
IdP Entity ID: <code>https://webtop.vlab.f5demo.com/idp/f5/</code></td>
<td></td>
</tr>
<tr>
<td>3. Enter the following values (leave others default) on the Assertion Settings.
Assertion Subject Type: <code>Email Address</code>
Assertion Subject Value: <code>%{session.ad.last.attr.mail}</code>
Authentication Context Class Reference:
<code>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</table>

9.5.3 Task - Download IdP metadata from BIG-IP for Salesforce

1. Go to **Access** -> **Federation: SAML Identity Provider** -> **Local IdP Services**, select the **SALESFORCE_IDP_DEMO** object, then click **Export Metadata**. Leave the **Sign Metadata** to **No**, and then click **Download**.

9.5.4 Task - Create an IdP provider in Salesforce

1. Log in to Salesforce `https://login.salesforce.com`

2. In Quick Find search box, type **single**, and then click **Single Sign-On Settings.** After that click the **Edit** button and check the **SAML Enabled** box, and then click **Save**.

3. Click **New from Metadata file**.Then click **Choose File**, select `SALESFORCE_IDP_DEMO_metadata.xml` export file you downloaded from BIG-IP, and then click **Create.**

9.5.5 Task - Create a new user in Salesforce

1. Log in to Salesforce `https://login.salesforce.com`

2. Under Administration, click **Users** -> **Users** -> **New User.**

3. Enter the following values (leave others default) on the **New User**.
   First Name: `Sales`
   Last Name: `Manager`
   E mail: `sales_manager@yourdomain`
   Username:
   `sales_manager@yourdomain`
   Nickname: `sales_manager`
   Role: `VP, North American Sales`
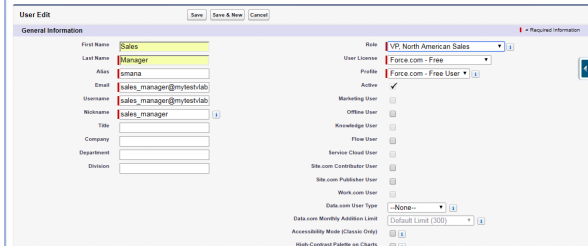
   User License: `Free`
   Repeat steps to the following users and change the
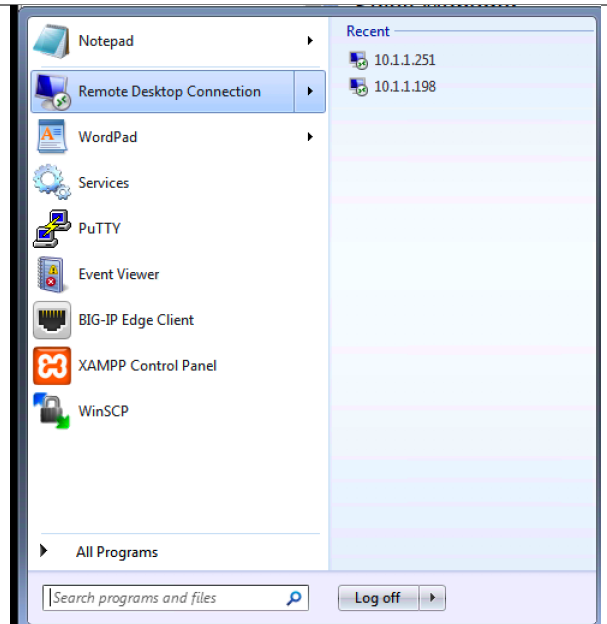   **Role** as you want:
   Sales User = `sales_user@yourdomain`
   Partner User = `partner_user@yourdomain`

9.5.6 Task - Modify the users in Active Directory

1. From the **Win 7** Jumpbox open a **Remote Desktop Connection** to Win 2008 server `10.1.1.251` Log in using **username:** `administrator` and **password:** `password`.

2. Open the **Active Directory Users and Computers**console, then **right-click on the **Sales Manager** user and then click **Properties**, modify the `E-mail` parameter according to the user that you already created at Salesforce. (`sales_manager@yourdomain`). Repeat steps to the following users:

Sales User = `sales_user@yourdomain`
Partner User = `partner_user@yourdomain`
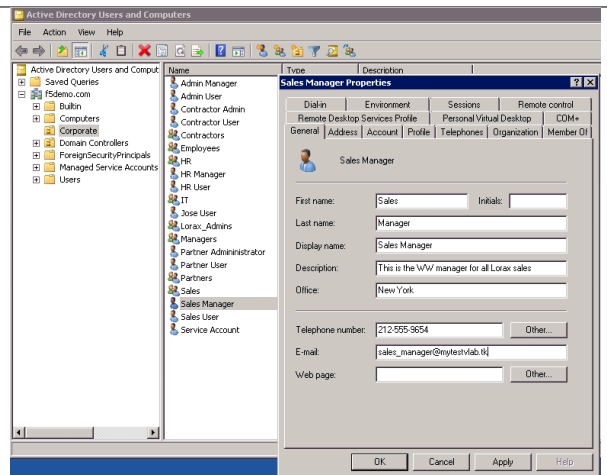
9.5.7 Task - Create an external SP connector to Salesforce

1. Logon onto BIG-IP, then go to **Access** -> **Federation: SAML Identity Provider** -> **External SP Connectors** -> **Create** -> **From Metadata**	
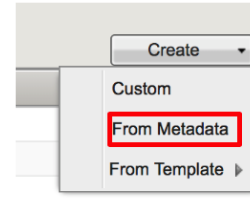
2. Enter the following values (leave others default) then click **OK**
 	
    Select File: `SAMLSP-XXXX.xml`
    Service   Provider   Name: `SALESFORCE_EXT_SP`
Use the `XML file` that you downloaded from **TASK 3**.	

9.5.8 Task - Bind IdP and SP Connector to Salesforce

1. Go to **Access** -> **Federation: SAML Identity Provider** -> **Local IdP Services**, select the `SALESFORCE_IDP_DEMO` object, then click **Bind/Unbind SP Connector**. Then select `Common/SALESFORCE_EXT_SP` as SP connector, and click **OK**.

9.5.9 Task - Create a Salesforce SAML resource in BIG-IP

1. Go to **Access** -> **Federation: SAML Resources** -> **Create.**	
2. Enter the following values (leave others default) on the **New SAML Resource** tab, then click **Finished.** **Name:** `SALESFORCE_SAML_DEMO` **SSO Configuration:** `SALESFORCE_IDP_DEMO` **Caption:** `SALESFORCE (SAML)`	

9.5.10 Task - Assign the SALESFORCE SAML resource

1. Go to **Access** -> **Profiles/Policies** -> **Access Profiles**, then click **Edit** for `webtop_demo`, a new browser tab will open	
2. Click on the **Advanced Resource Assign** object, a new window will open. Click **Add/Delete**, then choose `/Common/AWS_SAML_DEMO` and `/Common/SALESFORCE_SAML_DEMO` from the **SAML** tab and click **Update**, then **Save**.	
3. Click **Apply Access Policy** in the top left and then close the browser tab	
4. Go to `https://webtop.vlab.f5demo.com` from the jump host, You can login with any user: • **sales_user** • **sales_manager** • **partner_user** You should see two `SAML` resources **AWS** and **SALESFORCE**	
5. Click on the **AWS** and **SALESFORCE** links. You should be able to access **both** because of **SSO** (`SAML`).	

9.6 Lab 4: Set up Google Authenticator (GA)

In this module you will learn how to configure Google Authenticator as Second Auth Factor

9.6.1 Lab – Set up Google Authenticator (GA)

This lab will teach you how to configure Google Authenticator as Second Auth Factor. Estimated completion time: **30 minutes**

9.6.2 Task - Create the VS used to generate GA tokens

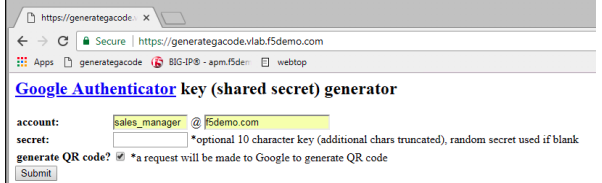|	
1. Log in to the BIG IP then go to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List**. Click on **Create**.	
2. Enter the following values (leave others default) and then **finished.** **Name:** VS_GENERATE_TOKEN **Destination Address:** 10.1.10.80 **Service Port:** 443 **HTTP Profile:** http **SSL Profile (Client):** f5demo_client_ssl **iRules:** generate_ga_code	

9.6.3 Task - Generate a token

1. Open a **Chrome** browser and click on **generate-gacode bookmark.** You should see the **GA generator App**.	
2. Enter the **account:** `sales_manager` and **domain:** `f5demo.com`. Also **check** the **generate QR code**, and then click **Submit**	
3. Open up your **Google Authenticator** app and touch the **"plus sign"**, select scan barcode and **scan** the **QR code**. Save the **secret**, we will need it soon.	 account: sales_manager@f5demo.comkey (secret): G4ZEIWDJLBJE4ZCM
4. Go to **Local Traffic** -> **iRules** -> **Data Group List** .Click on **google_auth_keys**.	
5. Create a new record, using the info saved in **step 3**. Click **Add** and then **Update.** **String:** `sales_manager`	
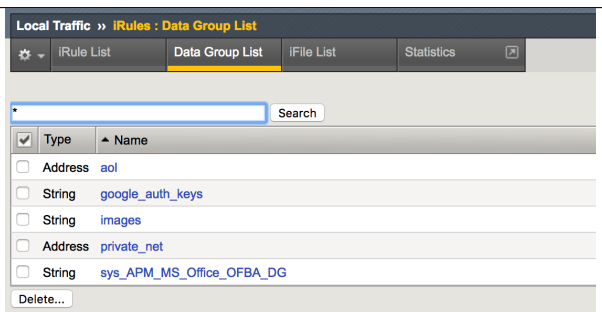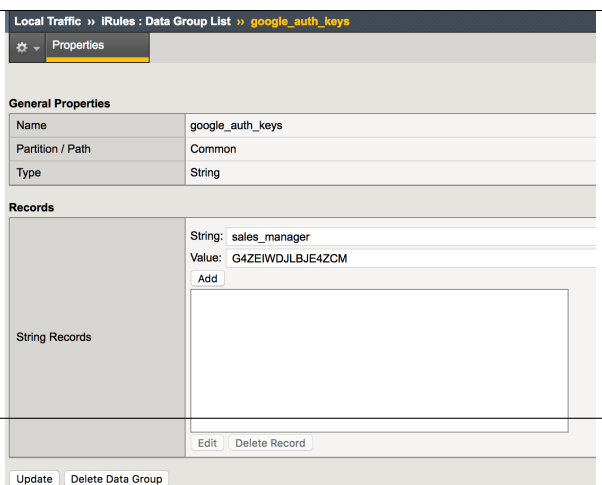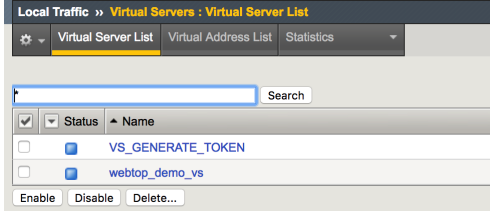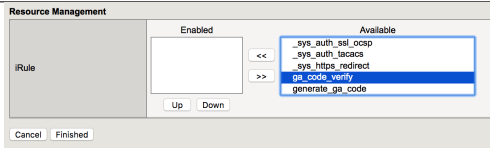
9.6.4 Task - Update the VS with the verification iRule

1. Go to **Local Traffic** -> **Virtual Servers** -> **Virtual Server List**, then find the Virtual Server **webtop_demo_vs** and **click on** it.	
2. In the following page, choose **Resources** and click on **manage** in the **iRules** section	
3. Find the **ga_code_verify** irule in the right list and **click on the arrows** pointing left. The irule should now moved to the left side. Then Click **finished**.	

9.6.5 Task - Update the Access Policy

1. Go to **Access** -> **Profiles/Policies** -> **Access Profiles.** Find the **webtop_demo** policy and click on **Edit**.	
2. In the **VPE** (Visual Policy Editor), click the + between **AD Auth** and **AD Query.**	
3. In the **Logon tab**, choose **Logon Page** and then **Add Item**	
4. **Modify** the values according to the picture (leave others default) and then **Save.** **Name:** `Get Ga Code`	
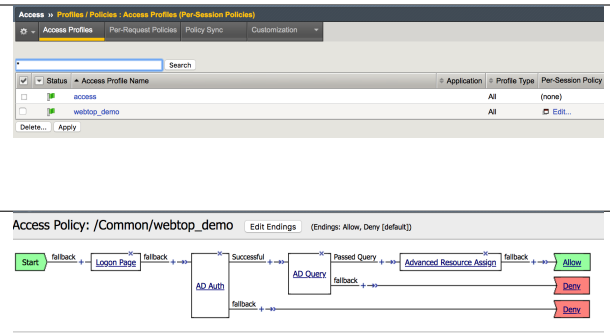
Post Variabl:e `ga_code_attempt`
Session Variable: `ga_code_attempt`
Form Header Text: `Empty`
Logon Page Input Field: `Google`
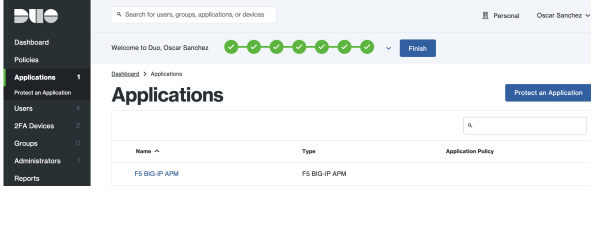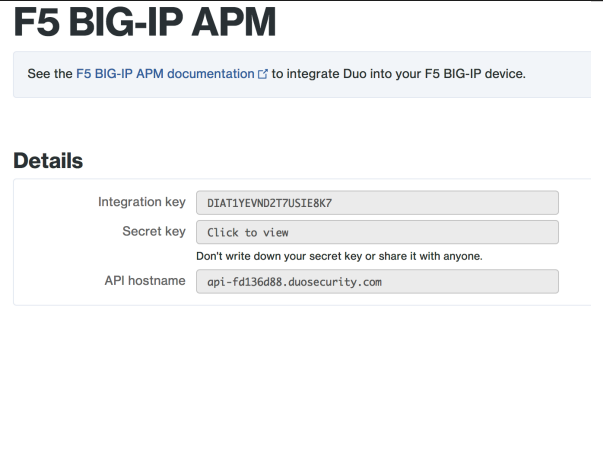
9.7 Lab 5: Set up DUO

In this module you will learn how to configure DUO as Second Auth Factor.
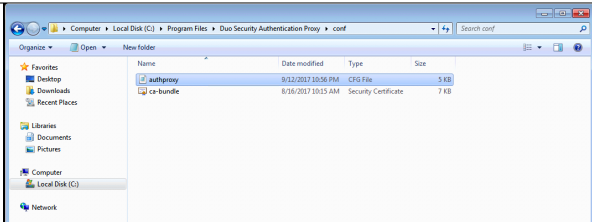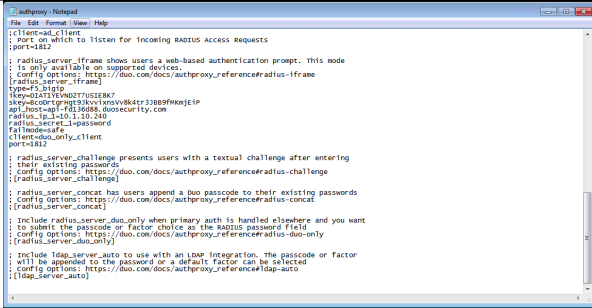
9.7.1 Lab – Set up DUO as Second Auth Factor

This lab will teach you how to configure DUO as Second Auth Factor. Estimated completion time: **30 minutes**
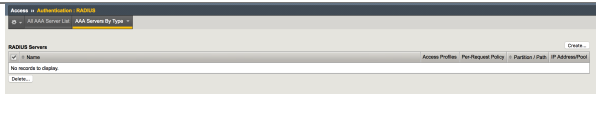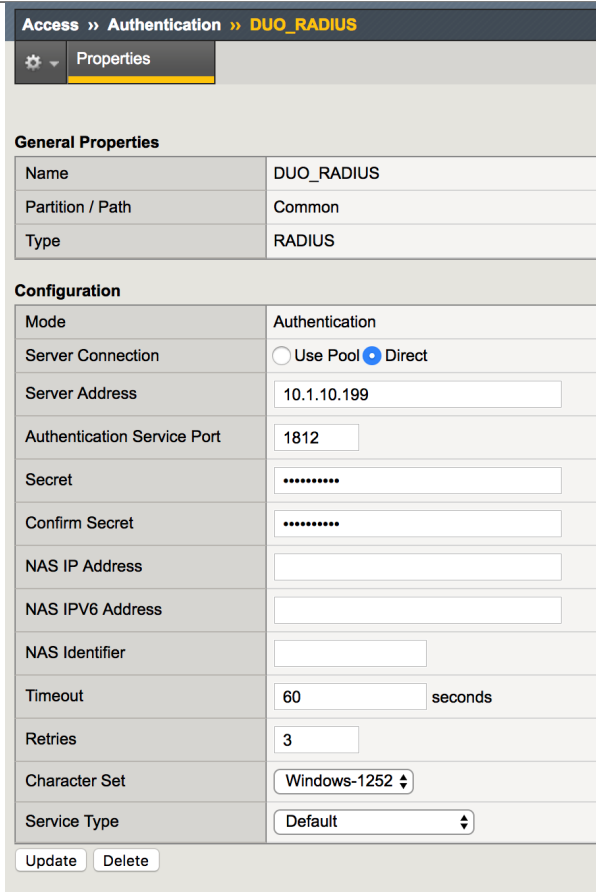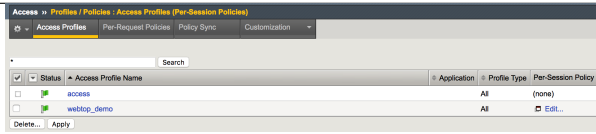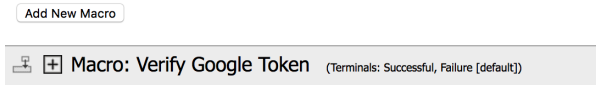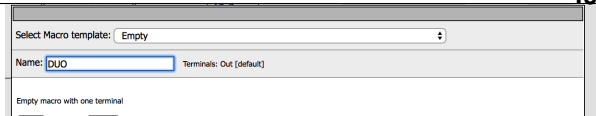
9.7.2 Task - Get the values from DUO Admin Panel

1. Log in to the **Duo Admin Panel** and navigate to **Applications**. Then click on `F5 BIG-IP APM`.	

2. **Copy** the values for:
`Integration key`
`Secret key`
`API hostname`	
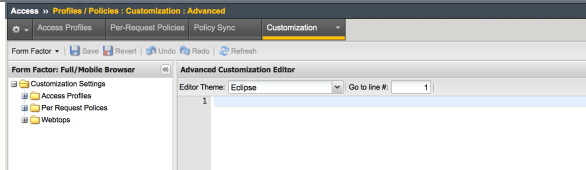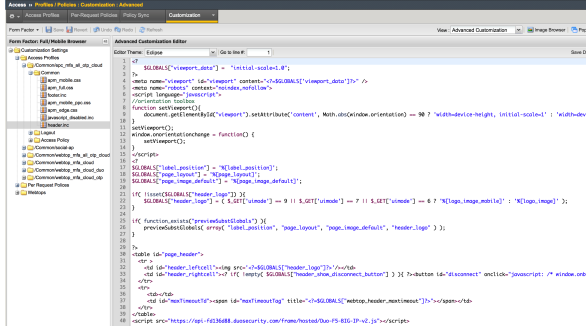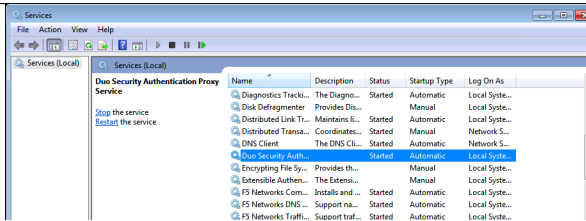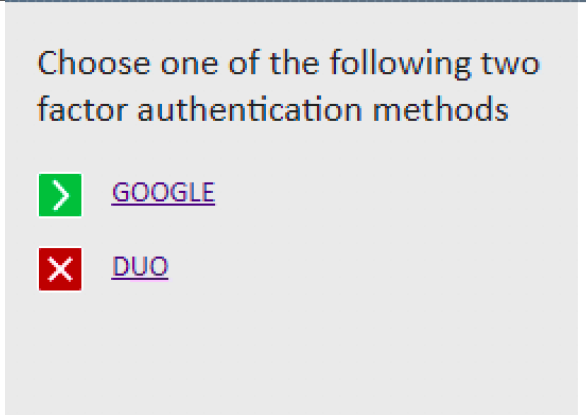
9.7.3 Task - Configure the Proxy for APM

1. In the **Win 7 External** open (as administrator) the file **C:Program Files-Duo Security Authentication Proxyconfauth-proxy.cfg**	
1. Search the section **[radius_server_iframe]** and modify the following values according to your **DUO account** • `ikey` • `skey` • `api`	

9.7.4 Task - Modify the Access Policy to include DUO

1. Go to **Access** -> **Authentication** -> **RADIUS** -> **Create.**	

2. Create a new record, using the following info and then **Finished.**
    Name: DUO_RADIUS
    Mode: Authentication
    Server Connection: Direct
    Server Address: 10.1.10.199
    Authentication Service Port: 1812
    Secret: password
    Confirm Secret: password
    Timeout: 60	

3. Go to **Access** -> **Profile / Policies** -> **Access Profile** then locate the **webtop_demo** profile and click **Edit**.	
4. Click on **Add New Macro**	

9.7.5 Task - Configure the APM to use the DUO Service

1. Go to **Access** -> **Profiles** / **Policies** -> **Customization** -> **Advanced**	
2. Navigate to **Access Profiles** -> /**Common**/**webtop_demo** -> **Common** -> **header.inc** and insert the line `<script src="https://api-XXXXXXXX.duosecurity.com/frame/hosted/Duo-F5-BIG-IP-v2.js"></script>` at the end of file and then **Save**. **NOTE:** Use the `api URL` from your `DUO account`.	
3. Click on **Apply Access Policy**	ONLINE (ACTIVE) Standalone Apply Access Policy
4. Restart the Proxy DUO Service. Go to **Start** -> **Services** and then click `Restart`	
	Choose one of the following two factor authentication methods GOOGLE DUO
5. Go to `https://webtop.vlab.f5demo.com`. You should see the **Google Authenticator** and **DUO** options to use as `Second Factor`. Try to log in with any user:	**493**

Class 10: Privileged User Access

Welcome to the Self Guided Priviledged User Access Hands-on Lab Guide. The following labs and exercises will instruct you on how to configure the IrulesLX Priviledged User Access Solution.

10.1 Lab Network Setup

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

- Cloud-based lab environment complete with Virtual BIG-IP.

- The Virtual BIG-IP has been pre-licensed and provisioned with Access Policy Manager (APM).

- Pre-staged configurations to speed up lab time, reducing repetitive tasks to focus on key learning elements.

If you wish to replicate these labs in your environment you will need to perform these steps accordingly.

Note: All work for this lab will be performed within the BIG-IP GUI and CLI. No installation or interaction with your local system is required.

10.1.1 Authentication – Credentials

The following credentials will be utilized throughout this Lab guide. All other credentials will be indicated at the time of use.

Credential Use	User ID	Password
BIG-IP Configuration Utility (GUI)	admin	4g1L17Y2018
BIG-IP CLI Access (SSH)	root	4g1L17Y2018

10.1.2 Utilized Browsers

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

10.1.3 General Notes

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

10.1.4 Acknowledgements

This lab is built upon the work of prior F5 Agility's and the work of many individuals behind the scenes in addition the 2018 Agility Lab Team. Many thanks to Michael Coleman and Bill Church.

10.1.5 Presented by

No Presenter, but written by Michael Coleman & stolen mostly from Bill Church.

10.2 Lab 1: WebSSH and APM

The Privileged User Authentication (PUA) solution is made up of three parts.

1. WebSSH2 Client Plugin

2. Ephemeral Authentication Plugin

3. Access Policy Manager (APM) policy configuration

10.2.1 Requirements

- BIG-IP with TMOS v13.1.0.2 or greater.

- 1-5 IP addresses for virtual servers (see Resource Table)

10.2.2 Prerequisites

BIG-IP with at least APM and iRules LX licensed and provisioned

The *build_pua.zip* or *build_pua_offline.zip* installation script found here:

> https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua.zip
>
> https://raw.githubusercontent.com/billchurch/f5-pua/master/build_pua_offline.zip

---

Note: These requirements, and prerequisites have all been provisioned ahead of time for you.

10.2.3 Installation Overview

The installation will consist of installing and testing (in order)

1. BIG-IP Preparation

2. Script download and execution

---

3. Customization of APM policy

10.2.4 Resource Table

Resource	Description	Value
WebSSH_proxy_vs_IP	Virtual server IP Address of WebSSH2 service.	10.1.10.240
APM_Portal_vs_IP	Virtual server IP Address of APM portal for authentication	10.1.10.240
RADIUS_proxy_vs_IP	Virtual server IP address of RADIUS proxy service	10.1.10.240
LDAP_proxy_vs_IP	Virtual server IP address of LDAP proxy service	10.1.10.240
LDAPS_proxy_vs_IP	Virtual server IP address of LDAPS proxy service	10.1.10.240
LDAP_server_IP	IP Address of site LDAP or AD server (required for LDAP use)	10.1.10.240
RADIUS_server_IP	IP Address of site RADIUS server (if RADIUS bypass is used)	10.1.10.240

10.2.5 Installation

This script will configure a reference implementation of the F5 Privileged User Authentication solution. The only requirements are a running and licensed system ("Active"), initial configuration complete (licensed, VLANs, self IPs), and preferably already provisioned for LTM+APM+ILX. The script will check for and can enable it for you if you wish.

You will be prompted for IP addresses for 5 services:

- WebSSH Proxy - This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/2222) do not conflict. This proxy is ultimately called by the APM web top. It's also important to note that SNAT may not be used on this virtual server. (webssh_proxy)

- RADIUS Proxy – This runs the RADIUS Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (udp/1812) do not conflict. (radius_proxy)

- LDAP Proxy – This runs the LDAP Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/389) do not conflict. (ldap_proxy)

- LDAPS Proxy – This runs the LDAPS (ssl) Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/636) do not conflict. (ldaps_proxy)

- Web top – This runs the LDAP Ephemeral Authentication Service. This IP may be shared with other IPs on the BIG-IP system if the protocol/port (tcp/443) do not conflict. By default SNAT is disabled for this vs as the WebSSH proxy may not interoperate with SNAT. If you change this option be sure to institute some sort of selective disable option (iRule) when connecting to the webssh_proxy as a portal resource.

WebSSH, LDAPS, and web top will all be initially configured with a default client-ssl profile, after testing this should be changed to use a legitimate certificate.

A blank APM policy is created and attached to the web top vs "pua_webtop", this policy will need to be built out for the pua_webtop service to operate correctly.

Note: For this lab, the scripts have been preloaded to /tmp, and we will be using build_pua_offline.sh and using Offline Installation Method. The online instructions, in the event you wish to deploy in your own environment, can be located here: https://raw.githubusercontent.com/billchurch/f5-pua/master/docs/PUA% 20Solution%20Install%20Guide.docx If the scripts do not appear in /tmp, they have also been copied to /root.

10.2.6 Offline Installation Method

This method utilizes the *build_pua_offline.sh/zip* method to install the PUA solutions from a closed network or a BIG-IP with limited or no Internet connectivity.

10.2.7 Run Installation Script

Note: This lab utilizes the Non-Interactive Install mode. A file called pua_config.sh may be placed in the same directory as build_pua.sh or build_pua_offline.sh to fully automate the install, or provide defaults for a "semi-automatic" deployment. See pua_config.sh as an example.

When started, build_pua.sh or build_pua_offline.sh both check for the existence of this file.

Additionally, most of the variables set in the top of pua_config.sh and pua_config_offline.sh may be overridden by this file.

---

1. Run **/tmp/build_pua_offline.sh** or **/root/build_pua_offline.sh**
2. Win.

10.3 Validation

10.3.1 WebSSH2 Client

1. Open a web browser and DO NOT navigate to the first URL given by the script. The IP show in the script is internal and will not be accessible externally. Instead, you will have to use the IP from the Student Portal "Webtop" link.

example: https://{[}VS_IP{]}:2222/ssh/host/10.1.0.240

2. Enter the username **testuser** with any password and click login.
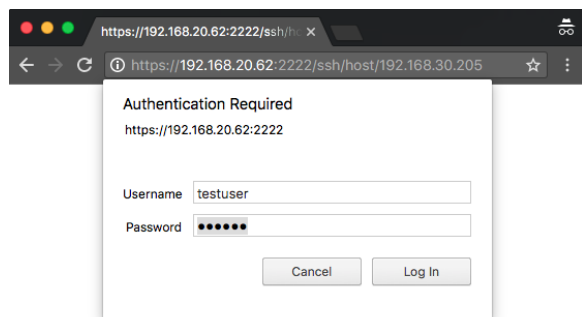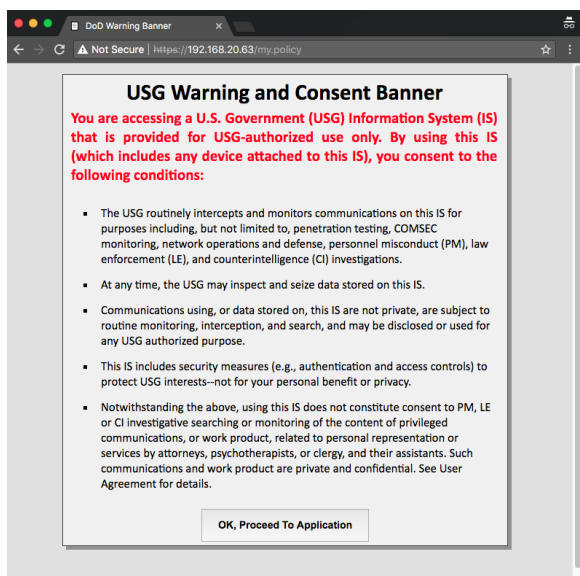

3. You should be greeted with a tmsh prompt to the BIG-IP the script was installed on, logged in as the user ***testuser***.
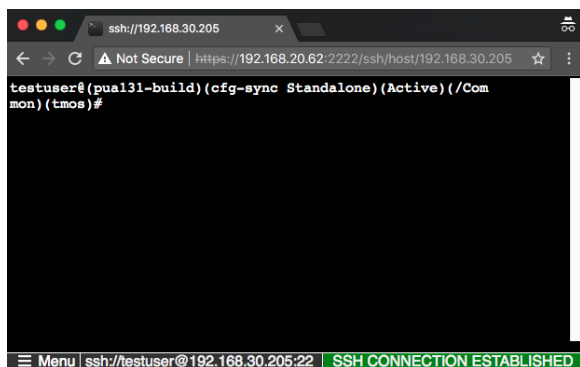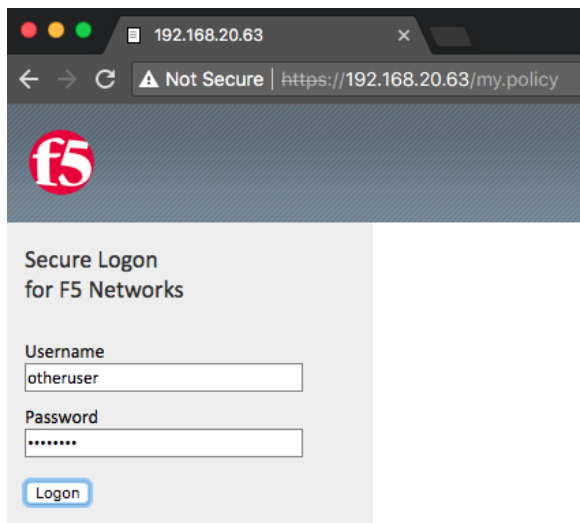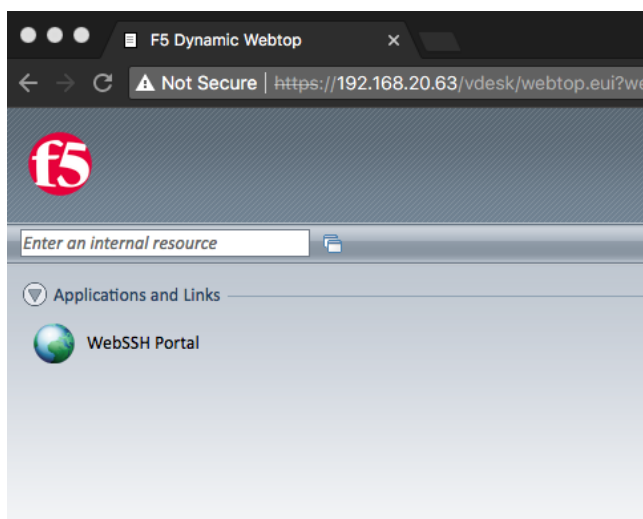
10.3.2 APM Policy and Portal Mode

1. Open a web browser and navigate to the second URL given by the script.

example: *https://[Public IP of Virtual Server]*

2. The sample USG Warning and Consent Banner should appear, click **OK**.

3. Enter a random username other than *testuser* and any password. Click **Logon**.

4. You should be directed to the webtop, click the **WebSSH Portal** icon.

5. You should be presented with another WebSSH2 screen, logged into the BIG-IP the script was installed on as the user you provided in step 3.