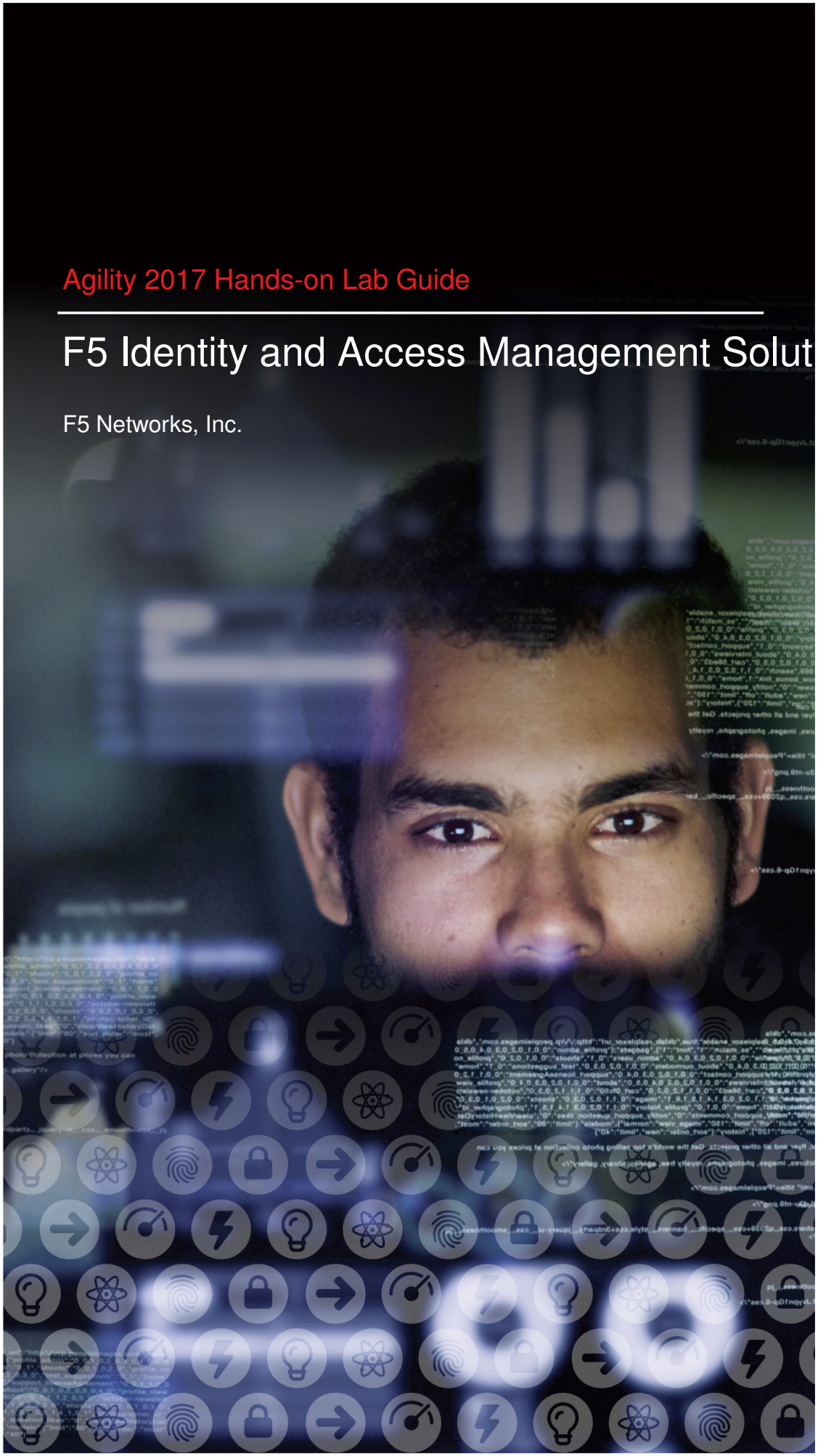


Agility 2017 Hands-on Lab Guide

F5 Identity and Access Management Solut

F5 Networks, Inc.

Contents:

1

Class 1: SAML Federation with F5

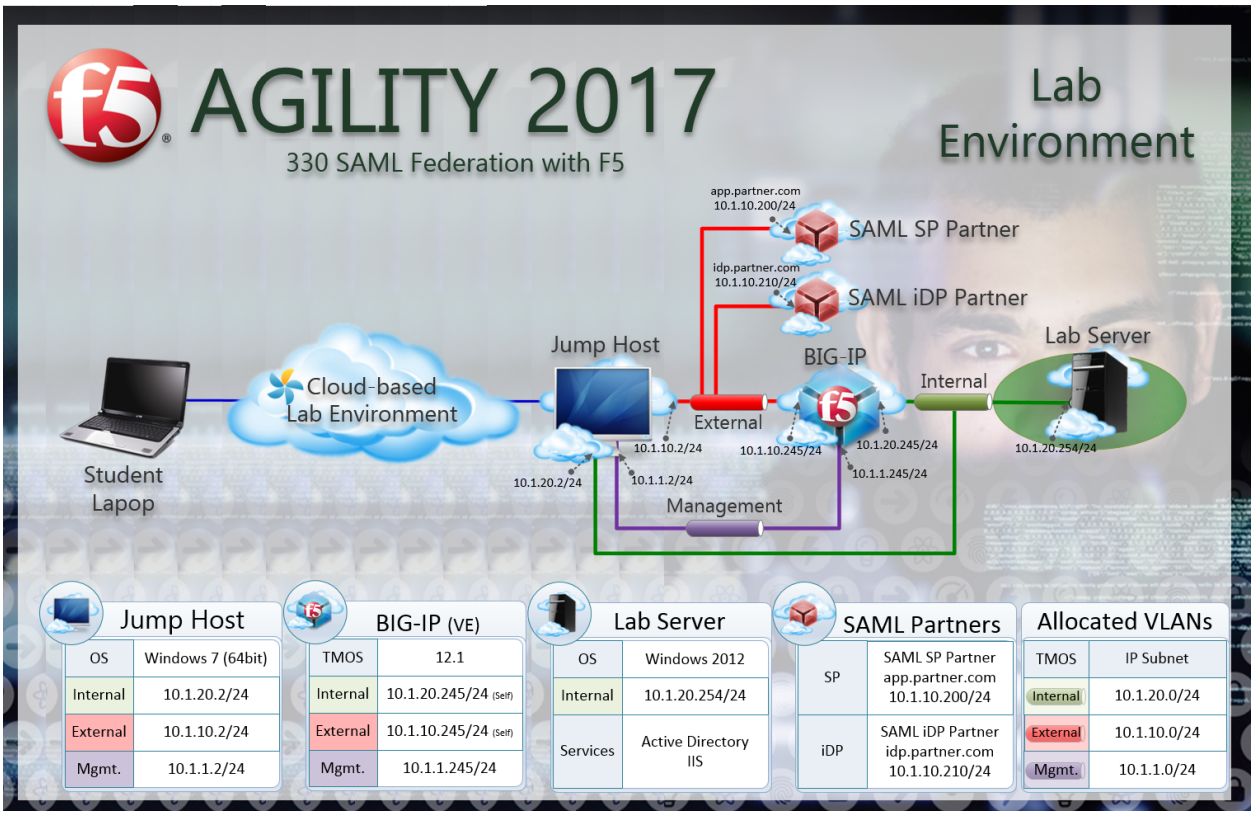
1.1 Getting Started

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:

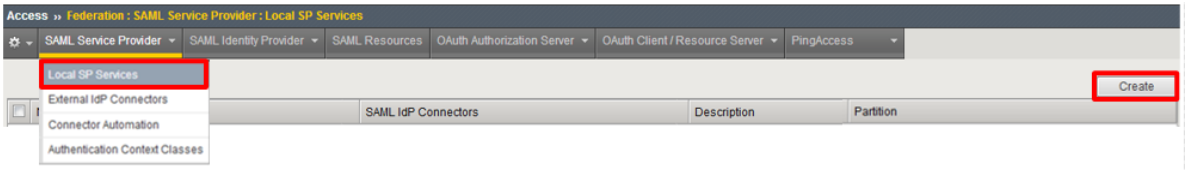
- All Lab requirements will be noted in*f* the tasks that follow

Estimated completion time: 25 minutes

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

SP Service

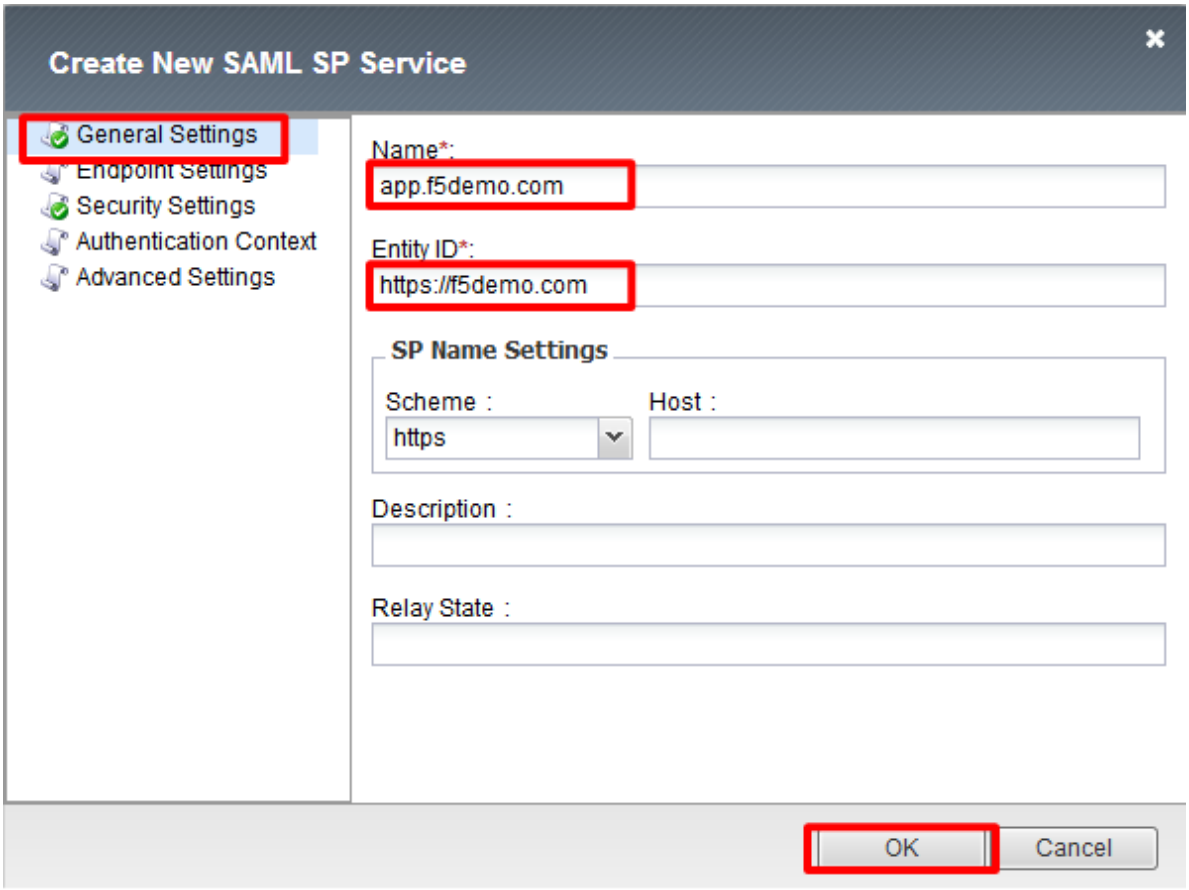
1. Begin by selecting: **Access -> Federation -> SAML Service Provider -> Local SP Services**
2. Click the **Create** button (far right)



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`

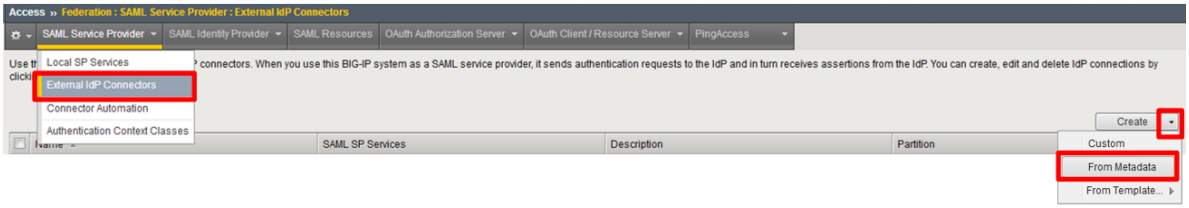
4. Click **OK** on the dialogue box



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

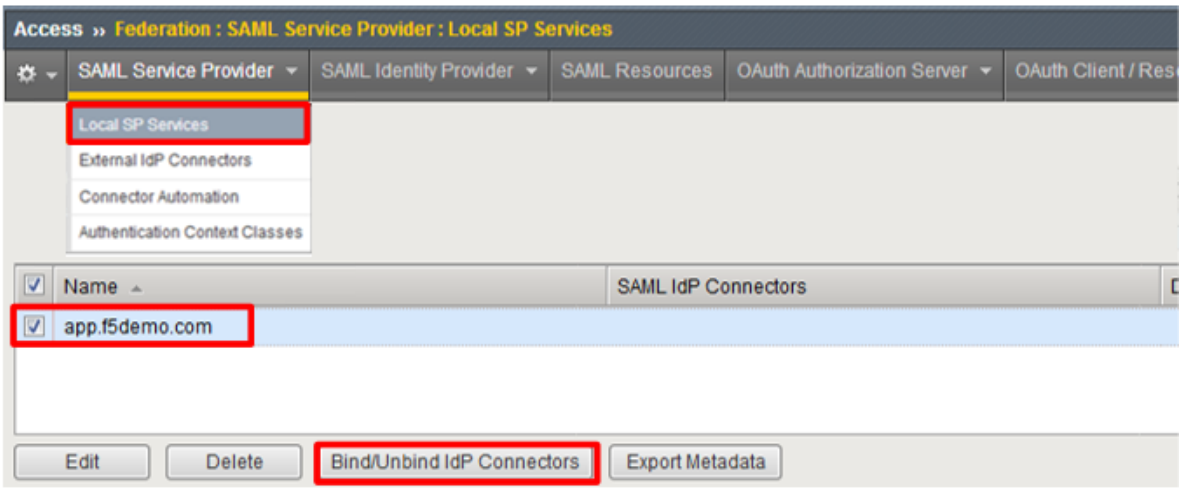


4. In the **Create New SAML IdP Connector** dialogue box, click **Browse** and select the **idp.partner.com?app_metadata.xml** file from the Desktop of your jump host.
5. In the **Identity Provider Name** field enter *idp.partner.com*:
6. Click **OK** on the dialog box

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

---

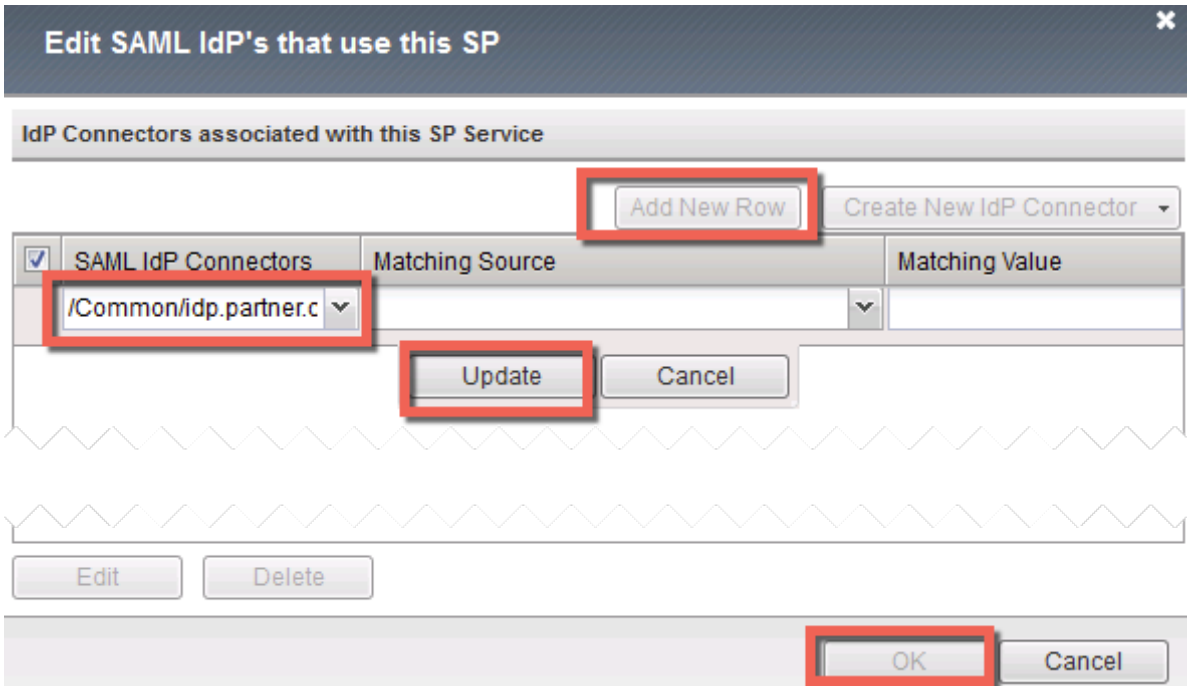
7. Click on the **Local SP Services** from the **SAML Service Providers** tab in the horizontal navigation menu
8. Click the **checkbox** next to the previously created *app.f5demo.com* and click **Bind/Unbind IdP Connectors** at the bottom of the GUI



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-*

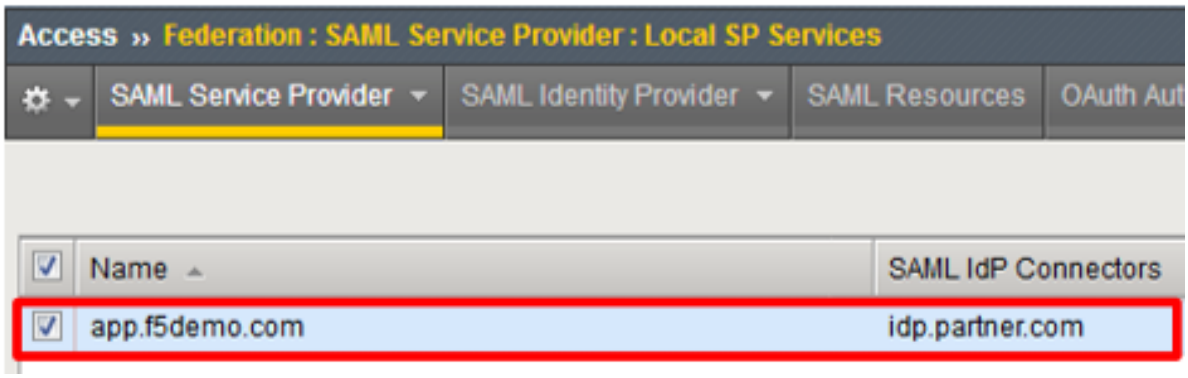
mon/idp.partner/com SAML IdP Connector previously created

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



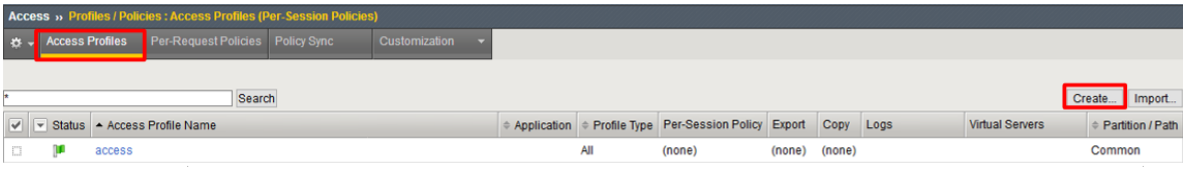
12. Under the **Access ?> Federation ?> SAML Service Provider ?> Local SP Services** menu you should now see the following (as shown):

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



1.2.2 TASK 2 ? Configure the SAML SP Access Policy

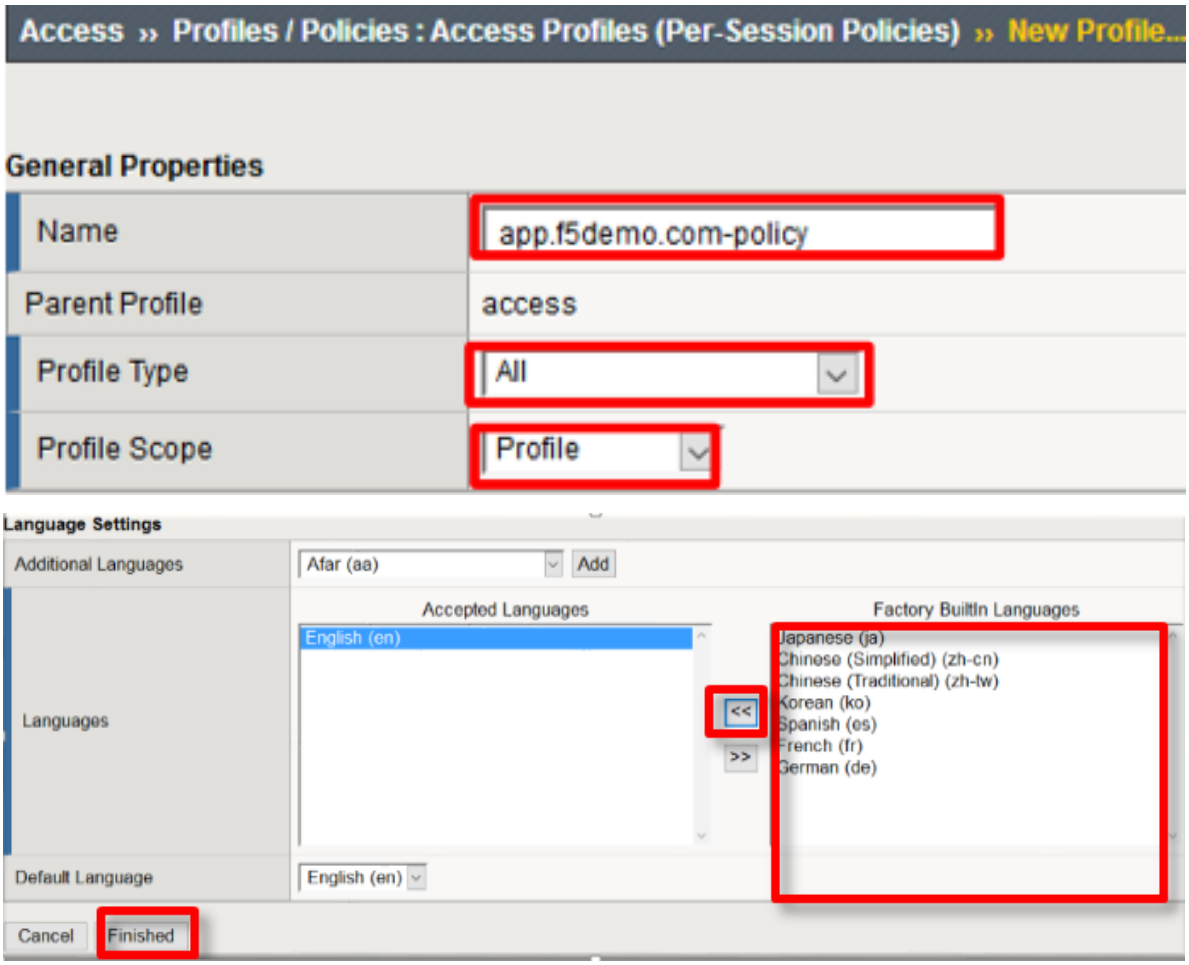
1. Begin by selecting **Access ?> Profiles/Policies ?> Access Profiles (Per?Session Policies)**
2. Click the **Create** button (far right)



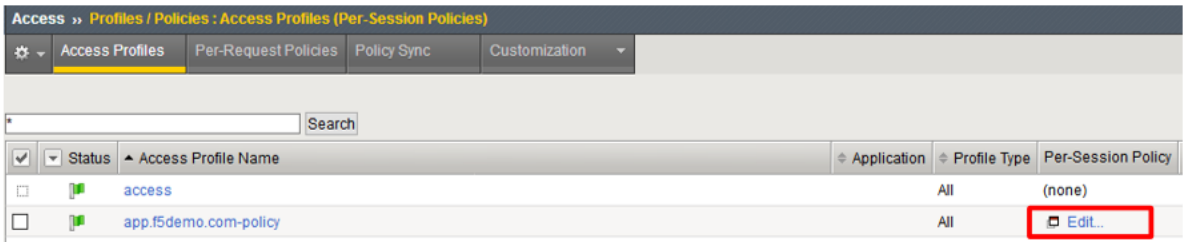
3. In the **New Profile** window, key in the following:

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.

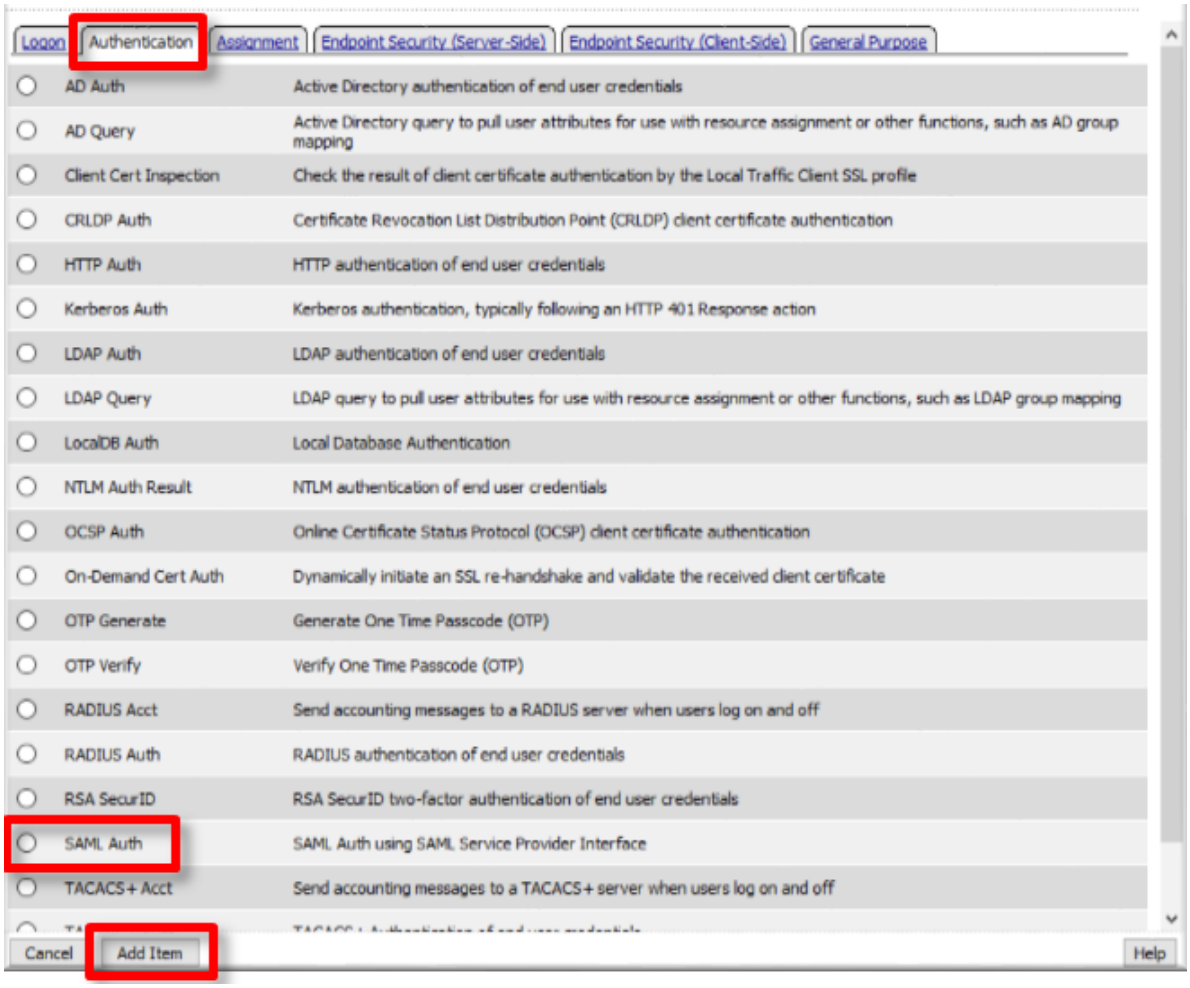


6. From the **Access ?> Profiles/Policies ?> Access Profiles (Per?Session Policies)** screen, click the **Edit** link on the previously created `app.f5demo.com?policy` line

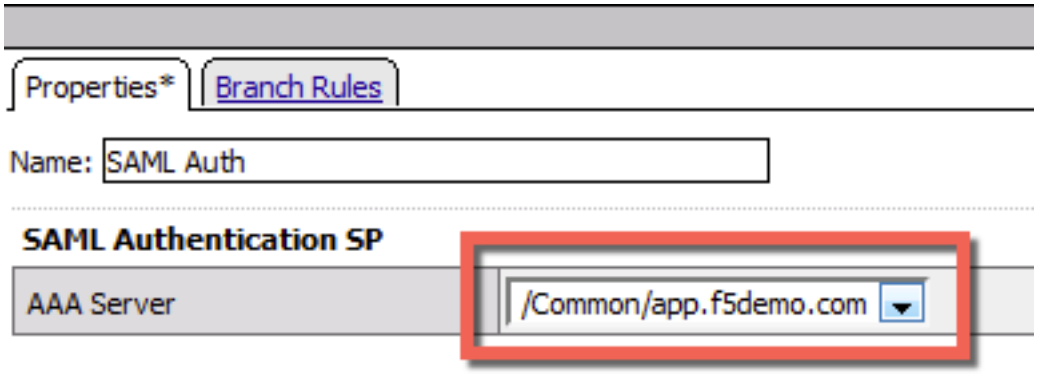


7. In the Visual Policy Editor window for `/Common/app.f5demo.com?policy`, click the **Plus (+) Sign** between **Start** and **Deny**

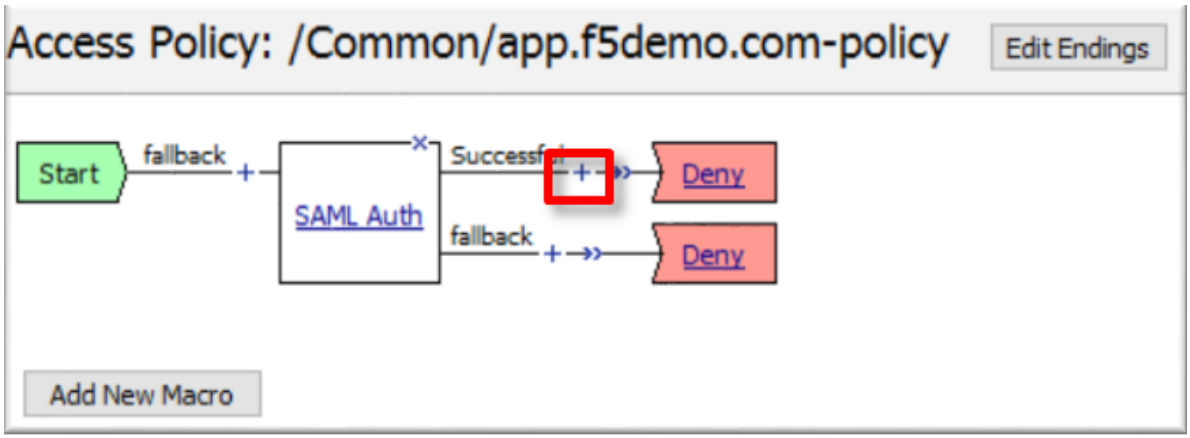
8. In the pop?up dialog box, select the **Authentication** tab and then click the **Radio Button** next to **SAML Auth**
9. Once selected, click the **Add Item** button



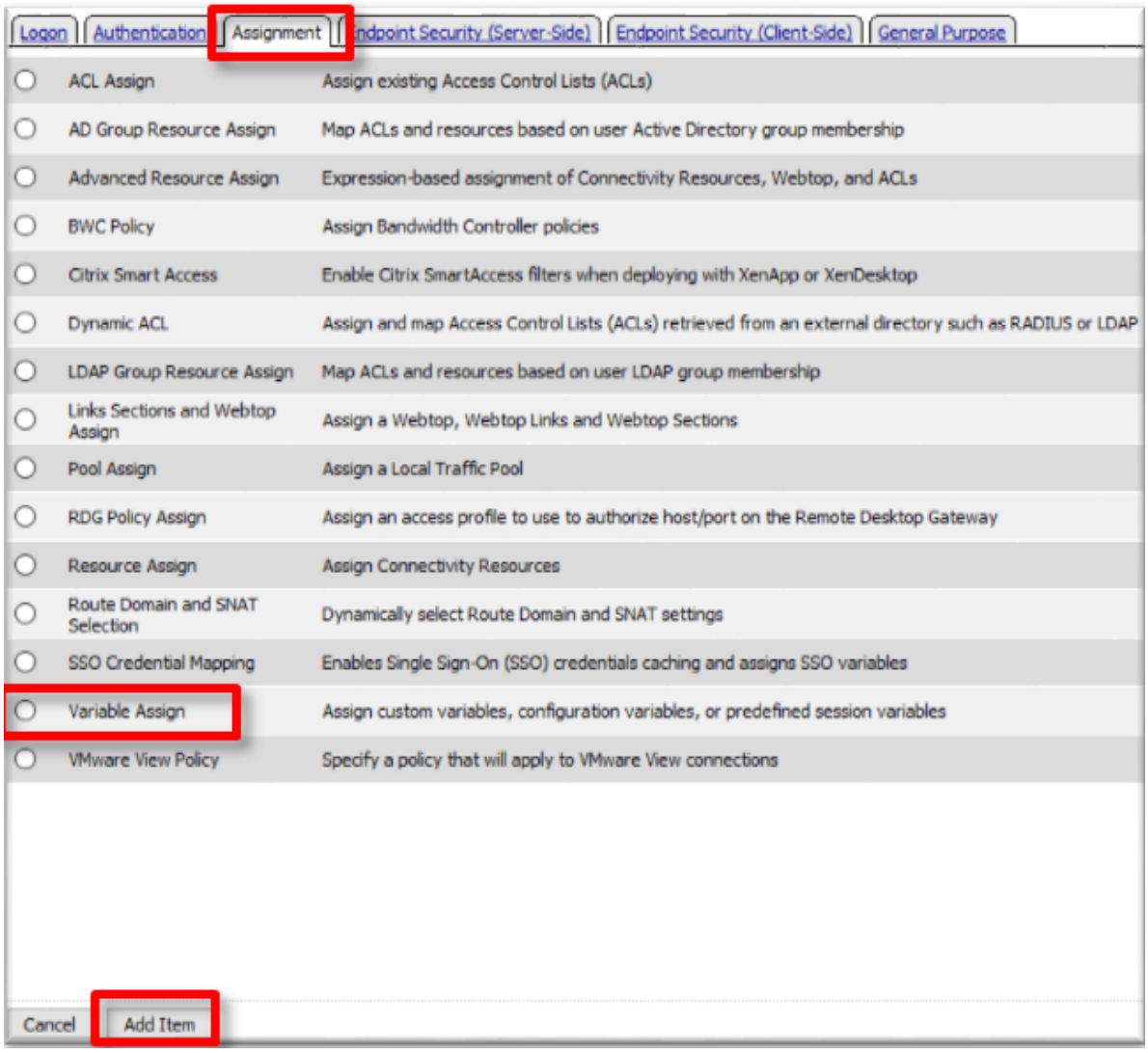
10. In the **SAML Auth** configuration window, select `/Common/app.f5demo.com` from the **AAA Server** drop down menu
11. Click the **Save** button at the bottom of the window



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



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



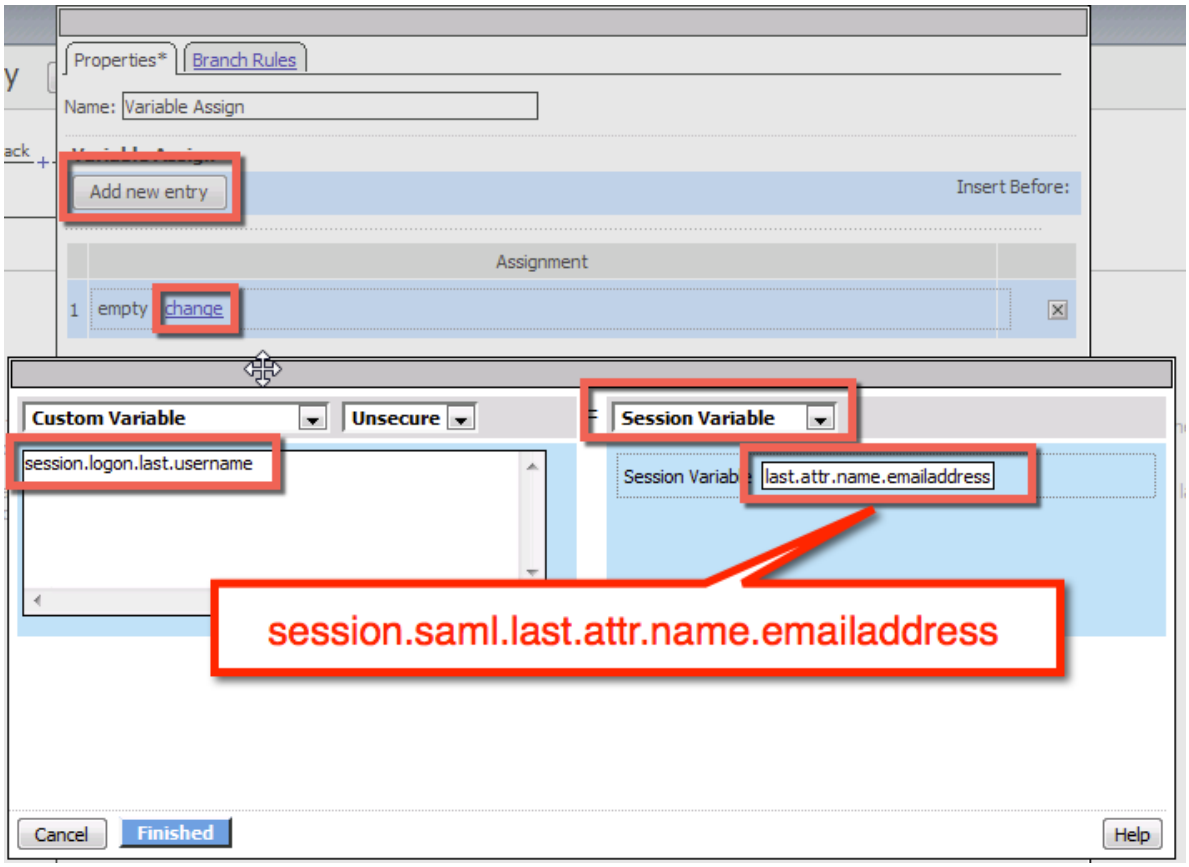
15. In the **Variable Assign** configuration window, click the **Add New Entry** button

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

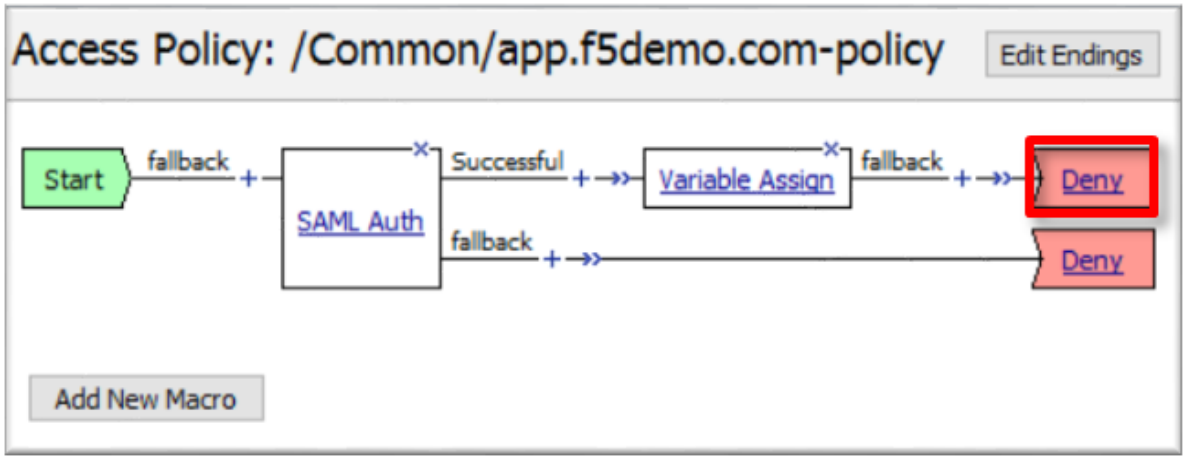
Left Pane	
Variable Type:	`Custom Variable`
Security:	`Unsecure`
Value:	`session.logon.last.username`

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**

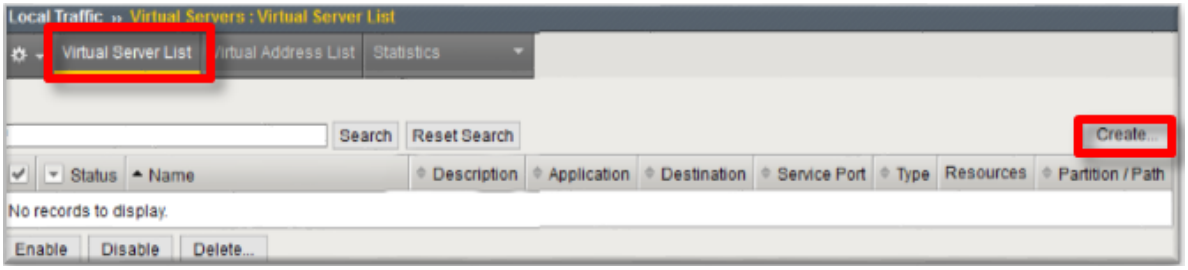


21. From the **Select Ending** dialog box, select the **Allow** button and then click **Save**

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:

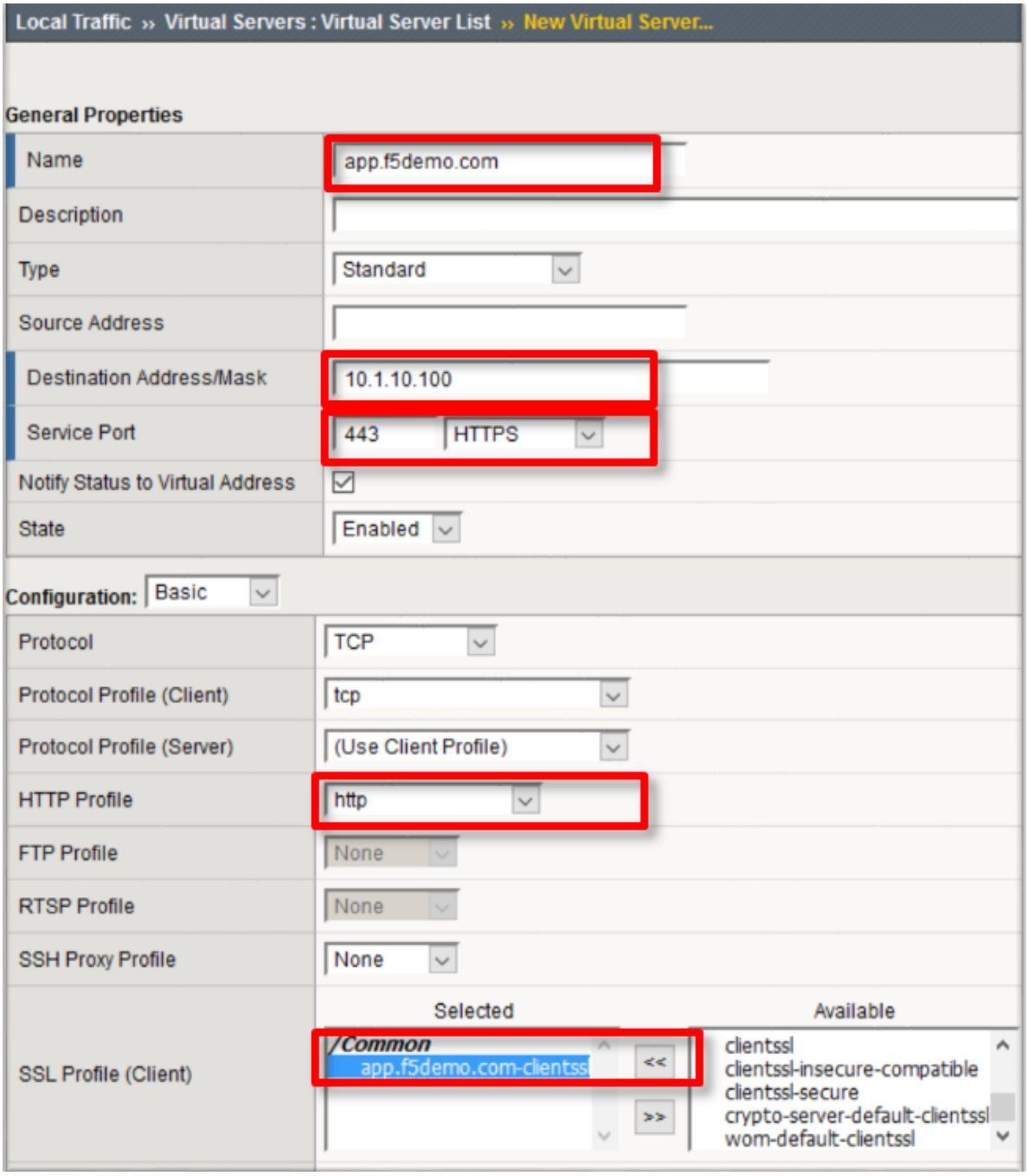
General Properties	
Name:	`app.f5demo.com`
Destination Address/Mask:	`10.1.10.100`
Service Port:	`443`

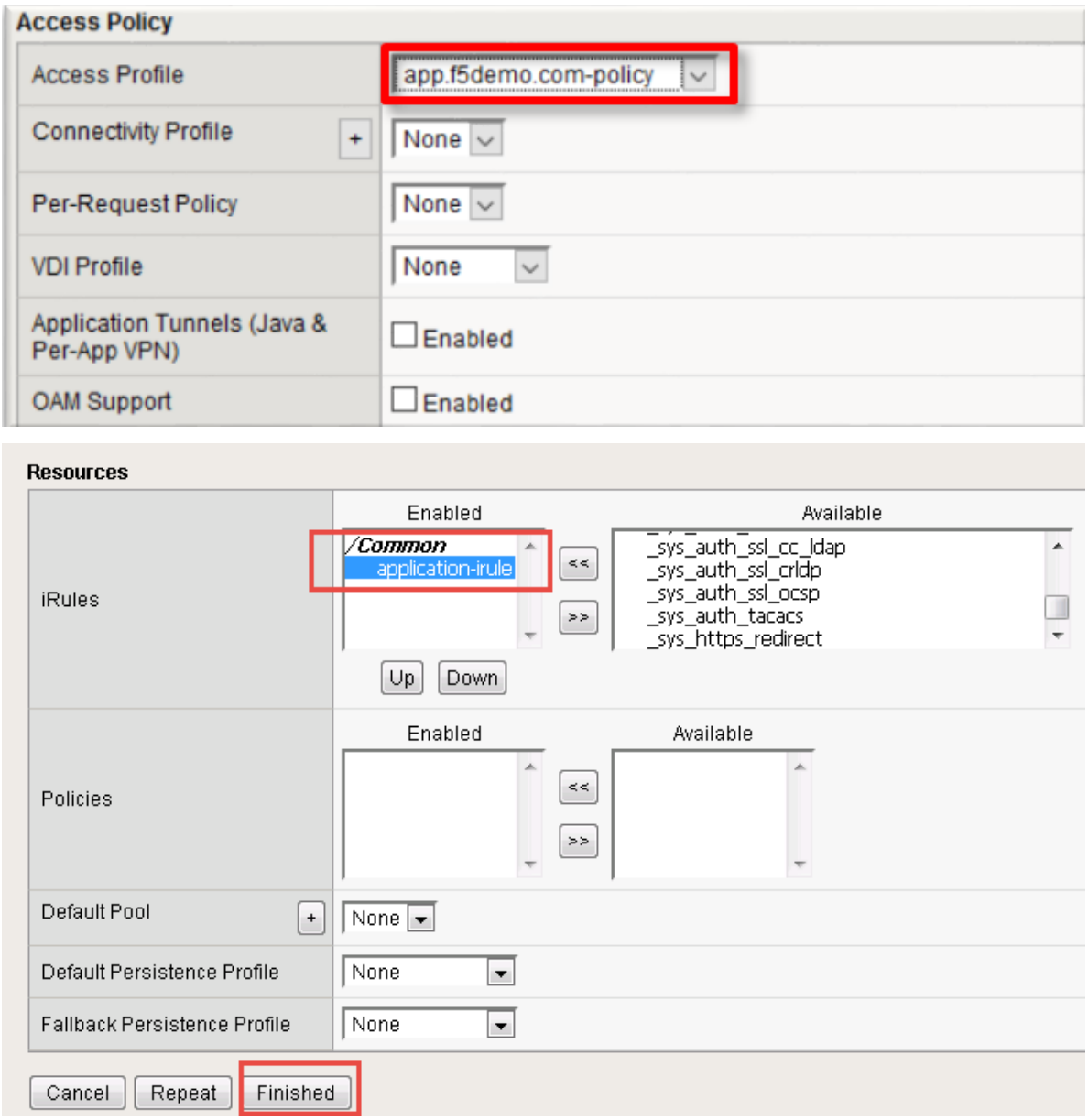
Configuration	
HTTP Profile:	`http` (drop down)
SSL Profile (Client)	`app.f5demo.com?clientssl`

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

Resources	
iRules:	`application?irule`

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

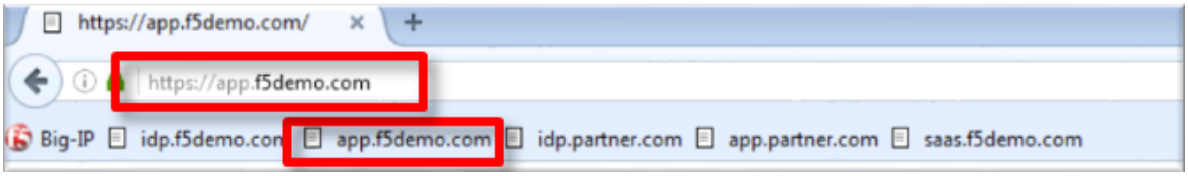

Local Traffic ›› Virtual Servers : Virtual Server List ›› New Virtual Server...
General Properties
Name
app.f5demo.com
Description
Type
Standard
Source Address
Destination Address/Mask
10.1.10.100
Service Port
443
HTTPS
Notify Status to Virtual Address
State
Enabled
Configuration:
Basic
Protocol
TCP
Protocol Profile (Client)
tcp
Protocol Profile (Server)
(Use Client Profile)
HTTP Profile
http
FTP Profile
None
RTSP Profile
None
SSH Proxy Profile
None
Selected
Available
SSL Profile (Client)
/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:

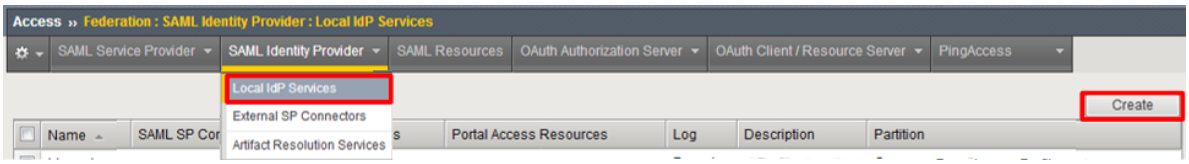
- All Lab requirements will be noted in the tasks that follow

Estimated completion time: 25 minutes

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

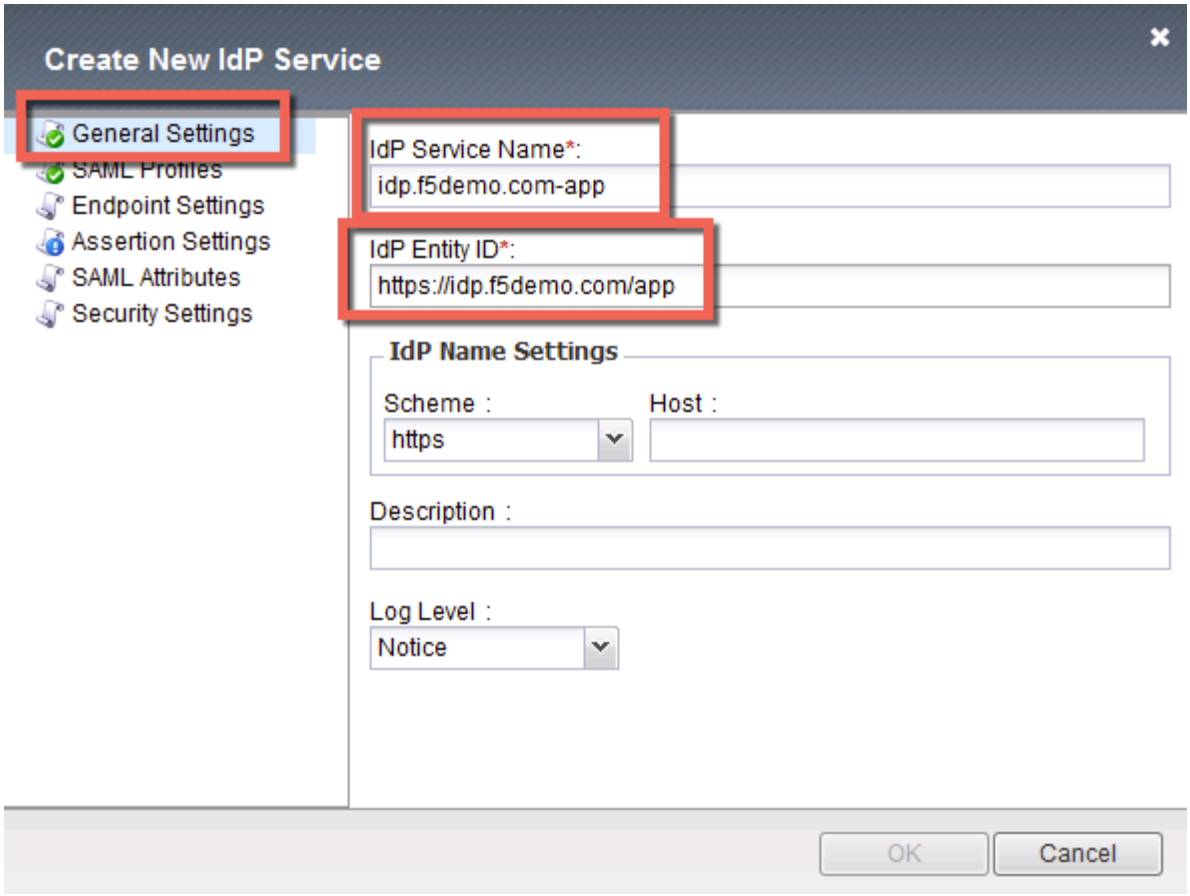
IdP Service

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:

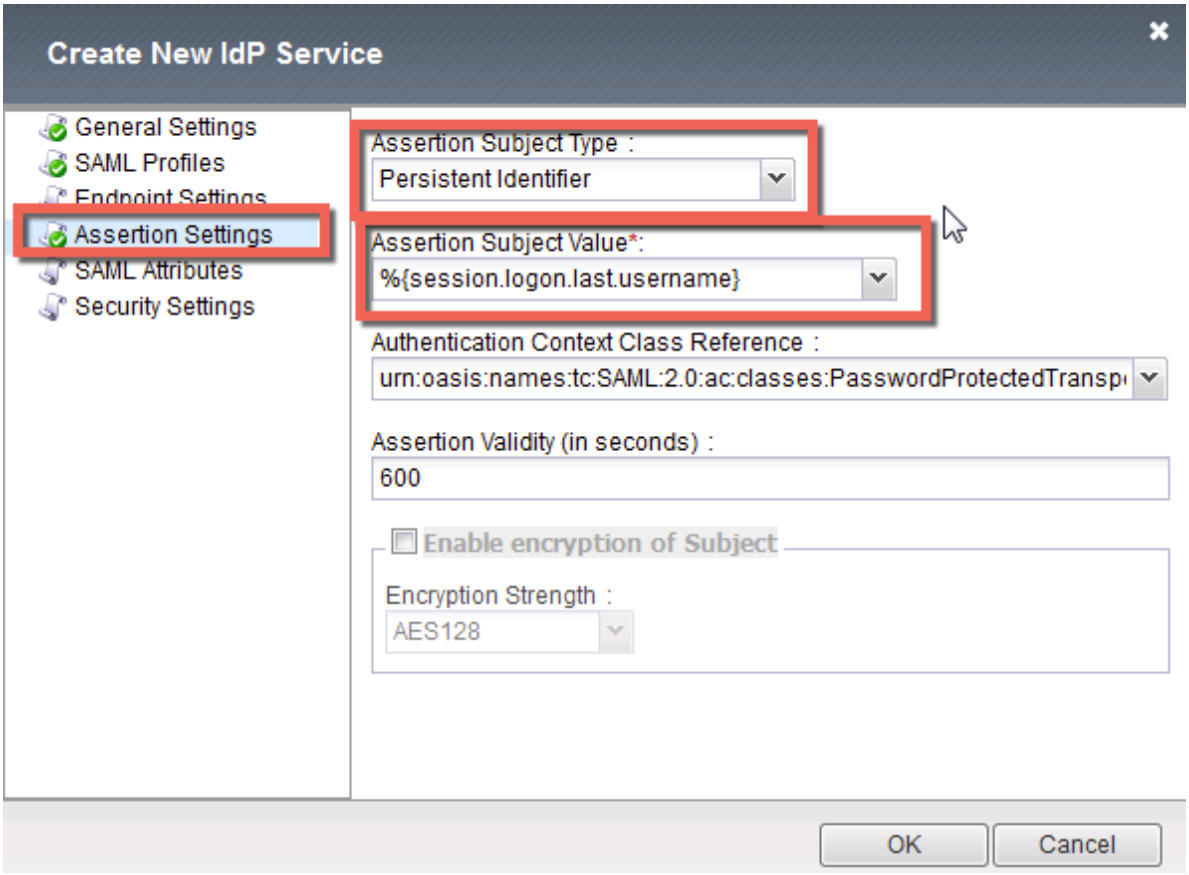
IdP Service Name:	`idp.f5demo.com?app`
IdP Entity ID:	`https://idp.f5demo.com/app`



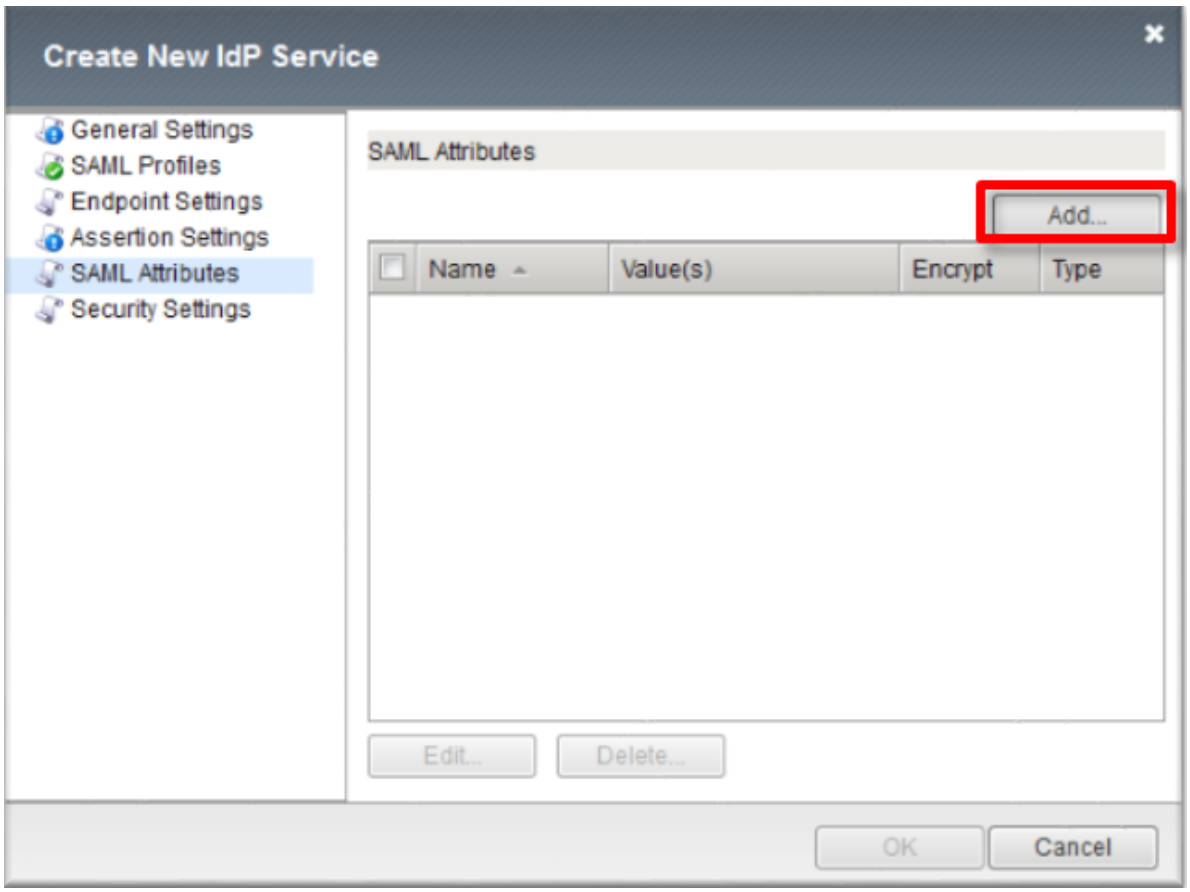
Note: The yellow box on “Host” will disappear when the Entity ID is entered

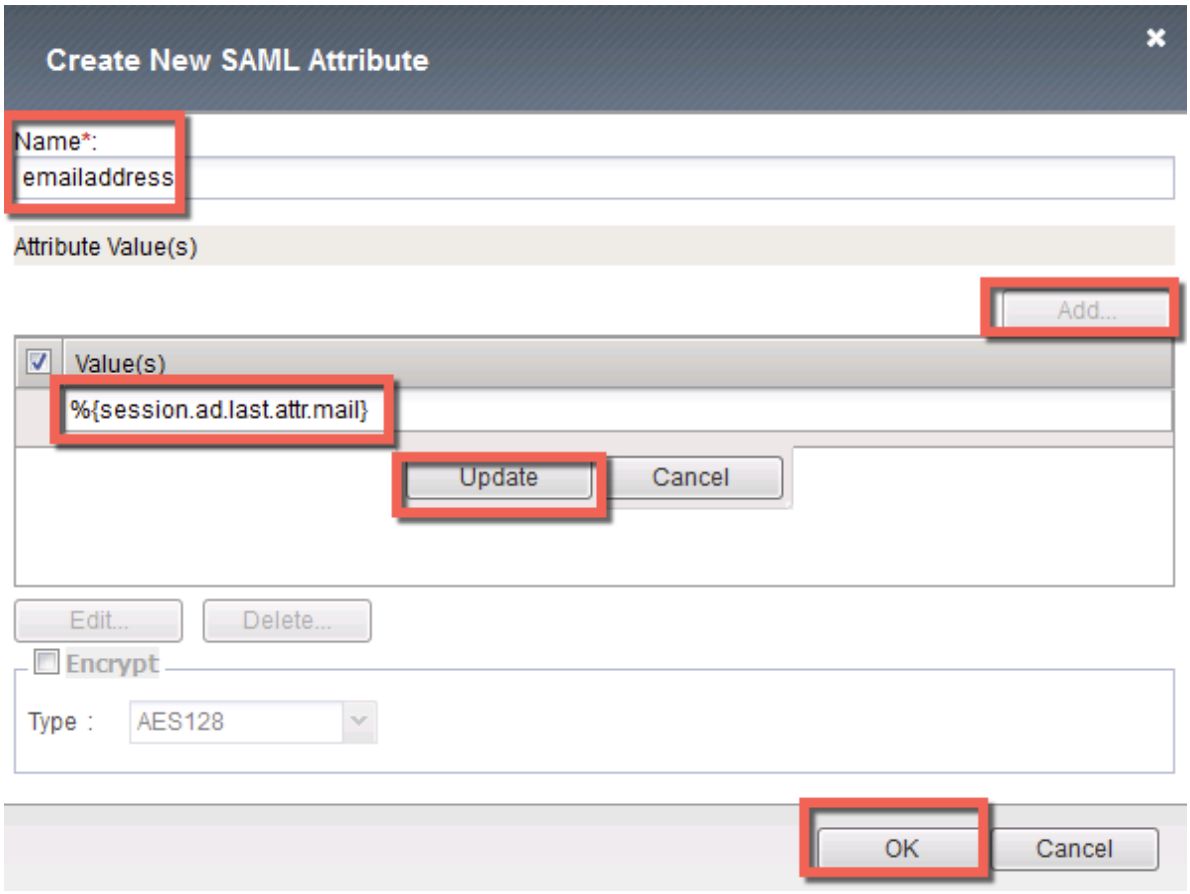
4. In the **Create New SAML IdP Service** dialog box, click **Assertion Settings** in the left navigation pane and key in the following:

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

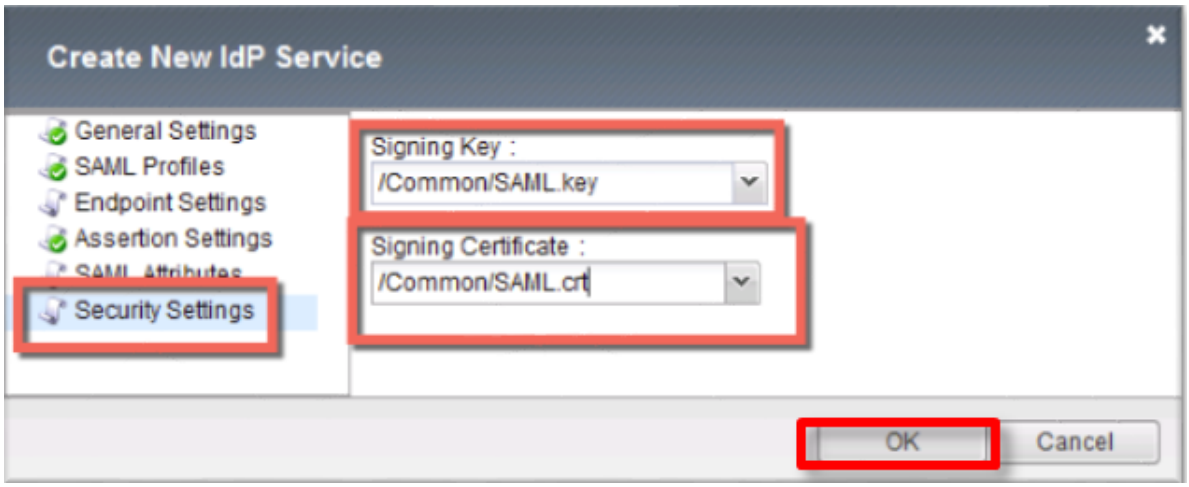


11. In the **Create New SAML IdP Service** dialog box, click **Security Settings** in the left navigation pane and key in the following:

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

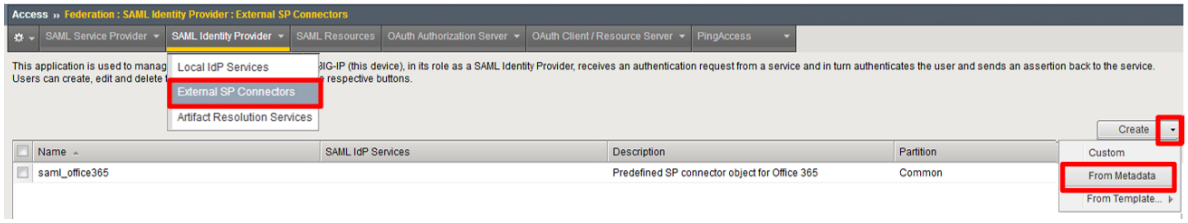
Note: The certificate and key were previously imported

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



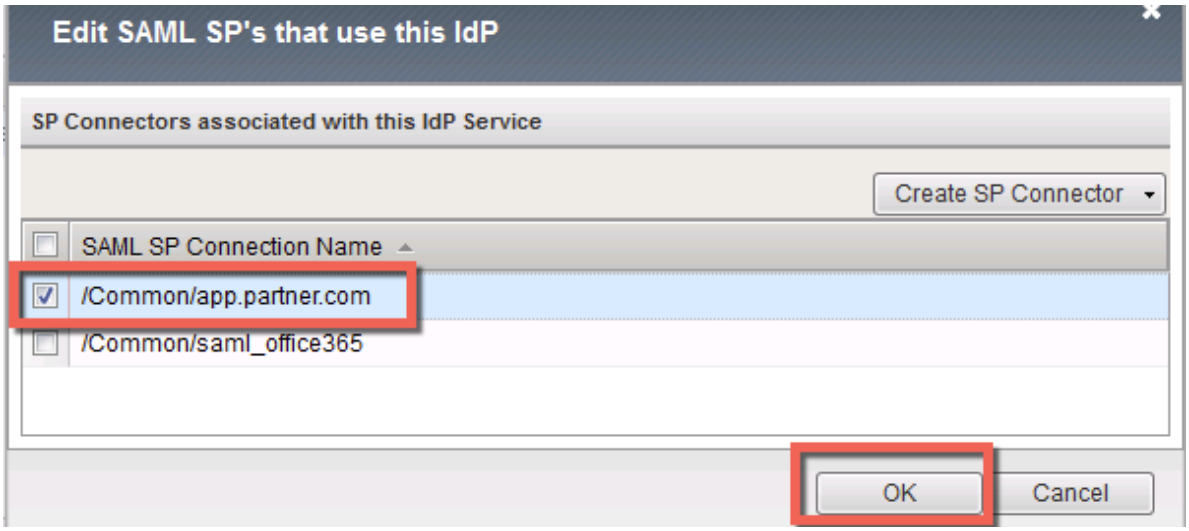
4. In the **Create New SAML Service Provider** dialogue box, click **Browse** and select the *app.partner.com_metadata.xml* file from the Desktop of your jump host
5. In the **Service Provider Name** field, enter the following: `app.partner.com`
6. Click **OK** on the dialog box

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

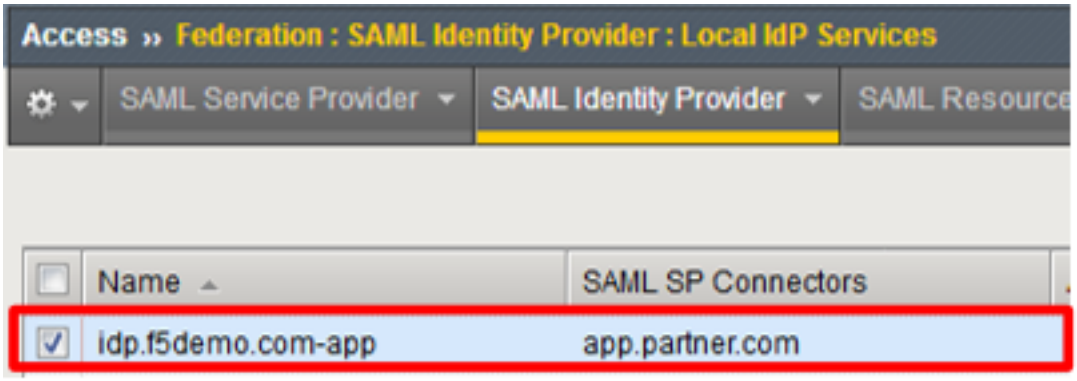
9. In the **Edit SAML SP's that use this IdP** dialog, select the `/Common/app.partner.com` SAML SP Connection Name created previously

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`



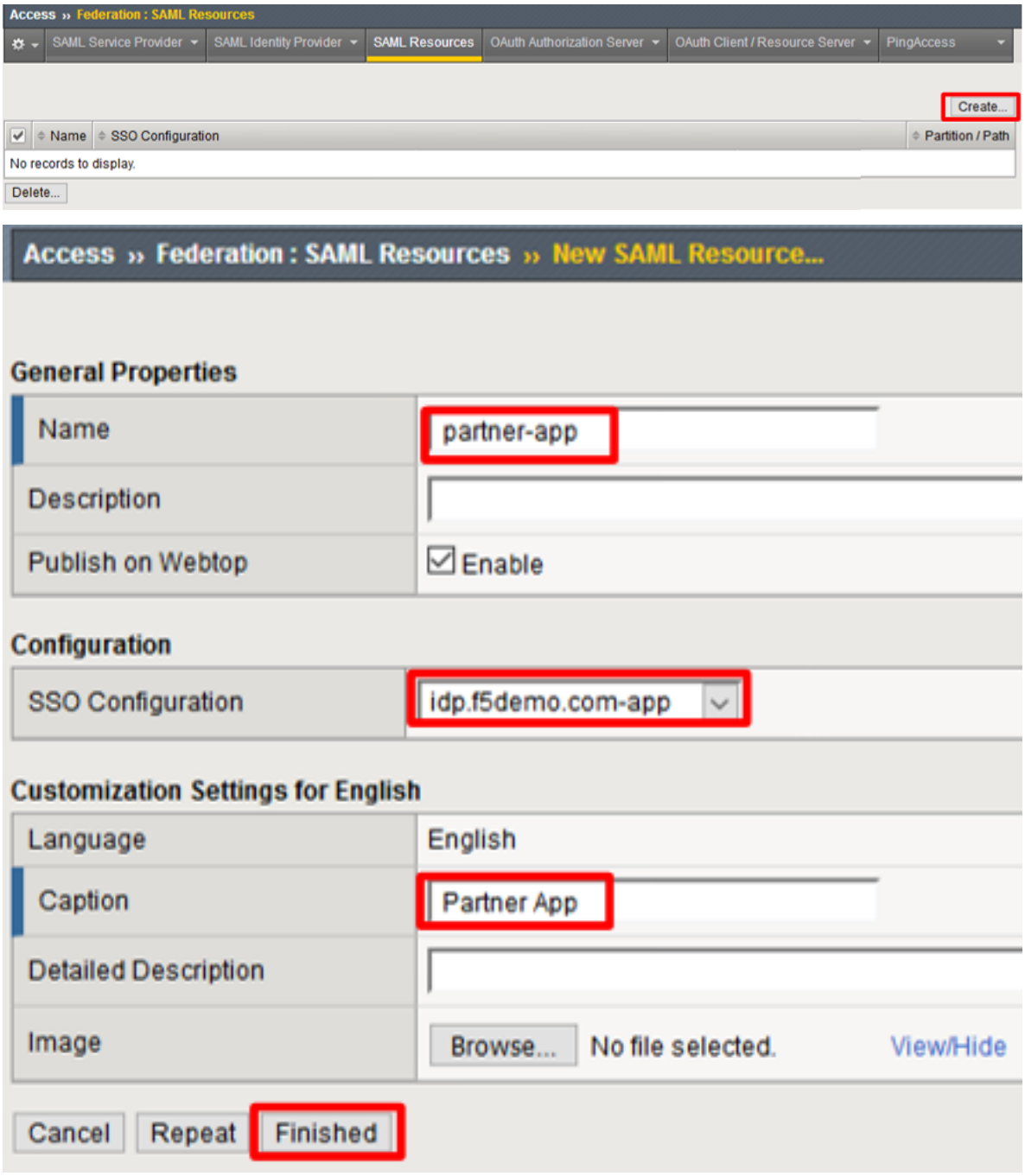
1.3.2 TASK 2 ? Create SAML Resource, Webtop, and SAML IdP Access Policy

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:

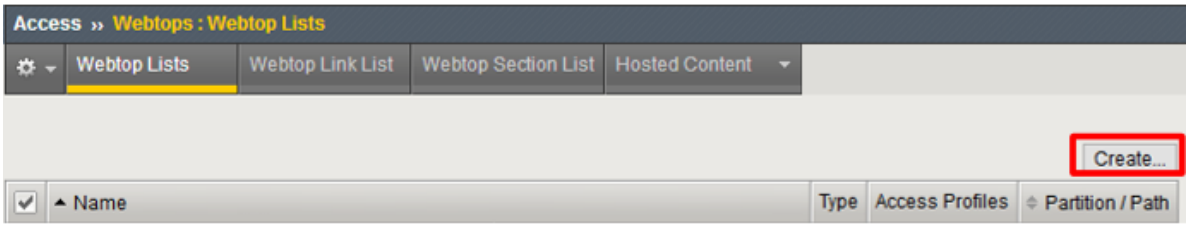
Name:	`partner?app`
SSO Configuration:	`idp.f5demo.com?app`
Caption:	`Partner App`

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



Webtop

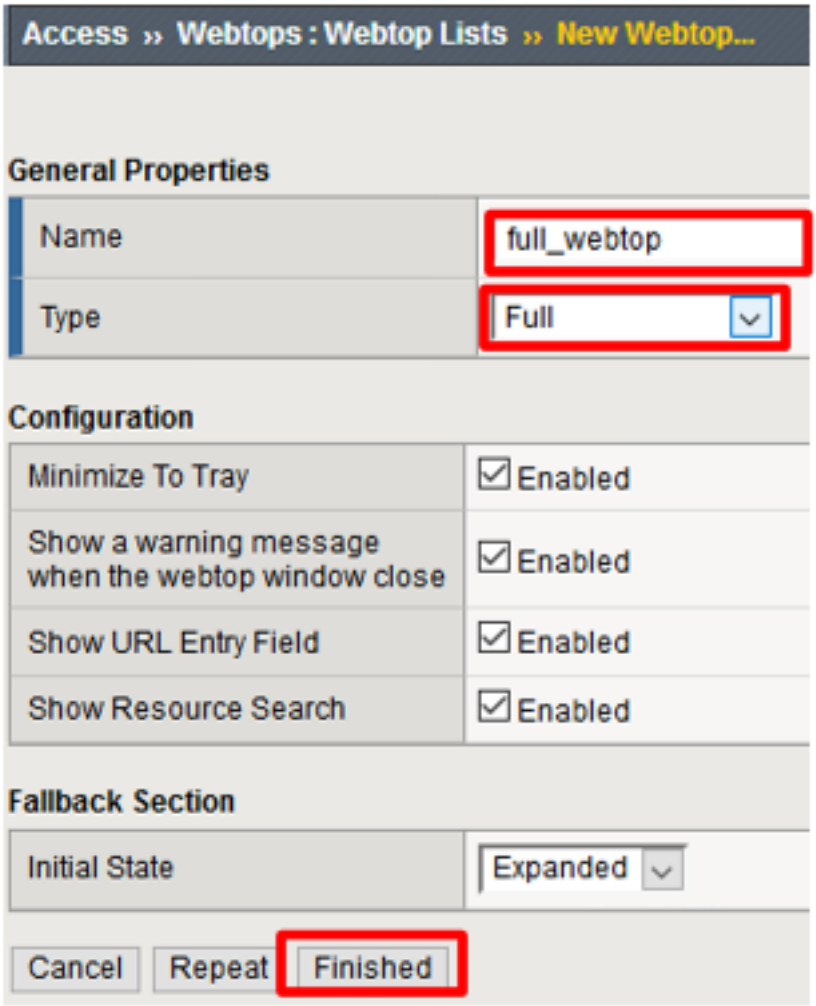
1. Select **Access ?> Webtops ?> Webtop List**
2. Click the **Create** button (far right)



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

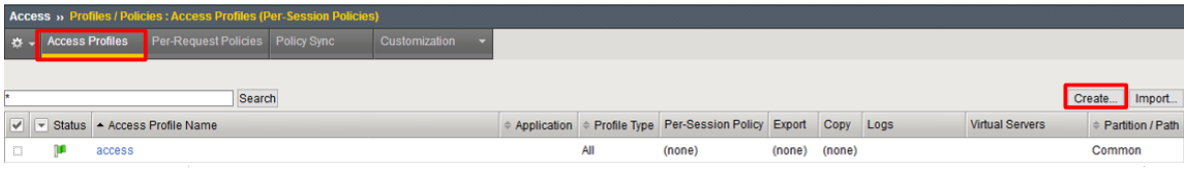
Name:	`full_webtop`
Type:	`Full` (drop down)

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



SAML IdP Access Policy

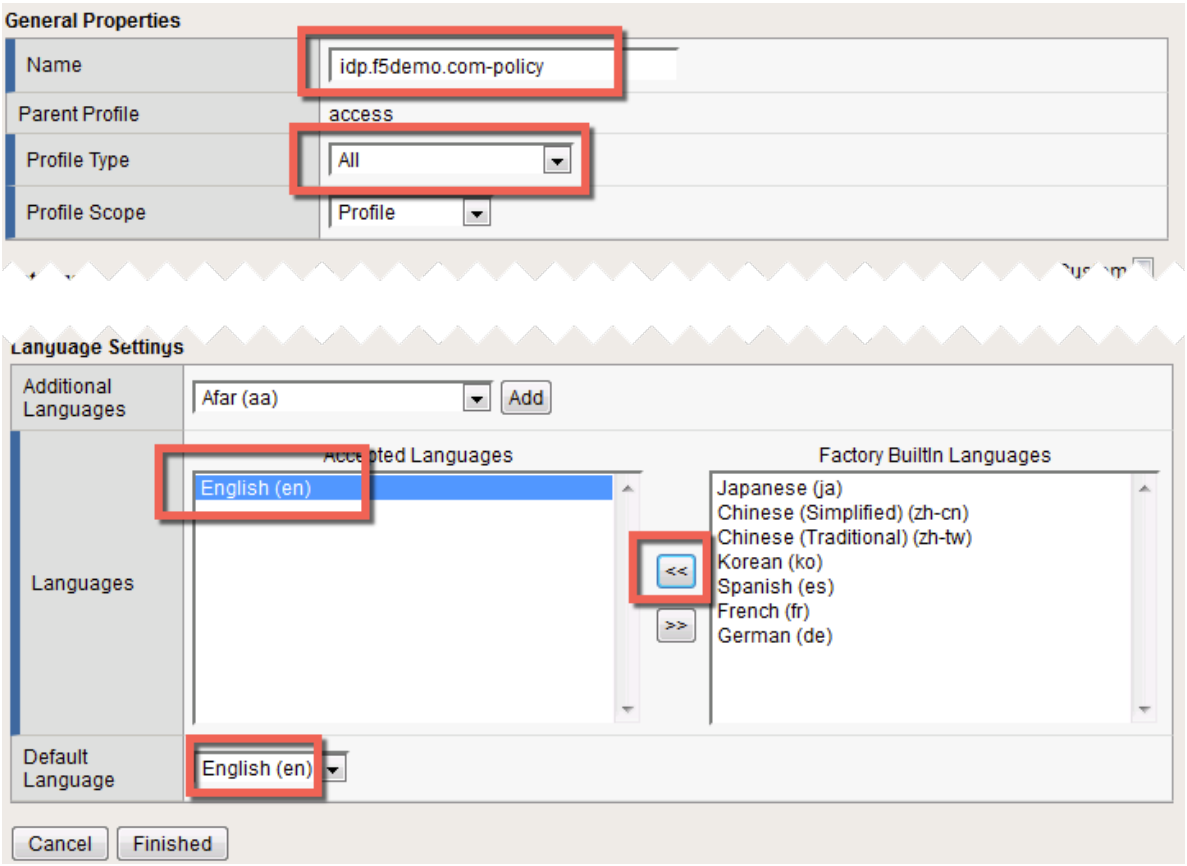
1. Select **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)**
2. Click the **Create** button (far right)



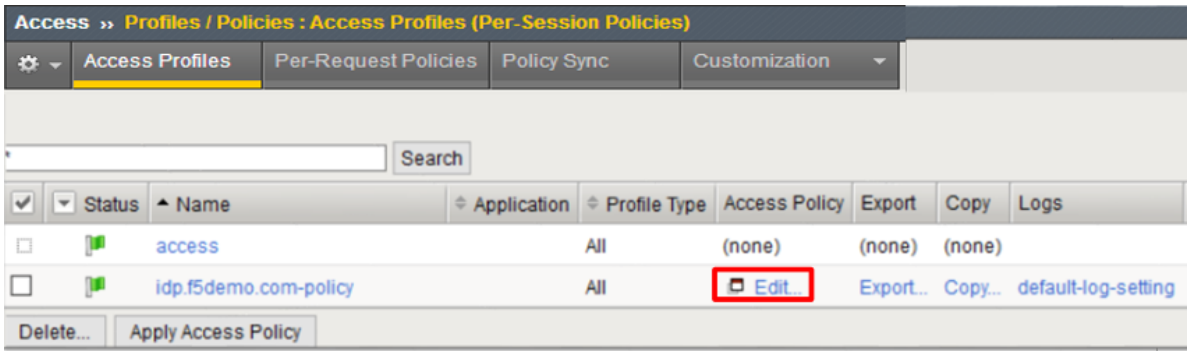
3. In the **New Profile** window, enter the following information:

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

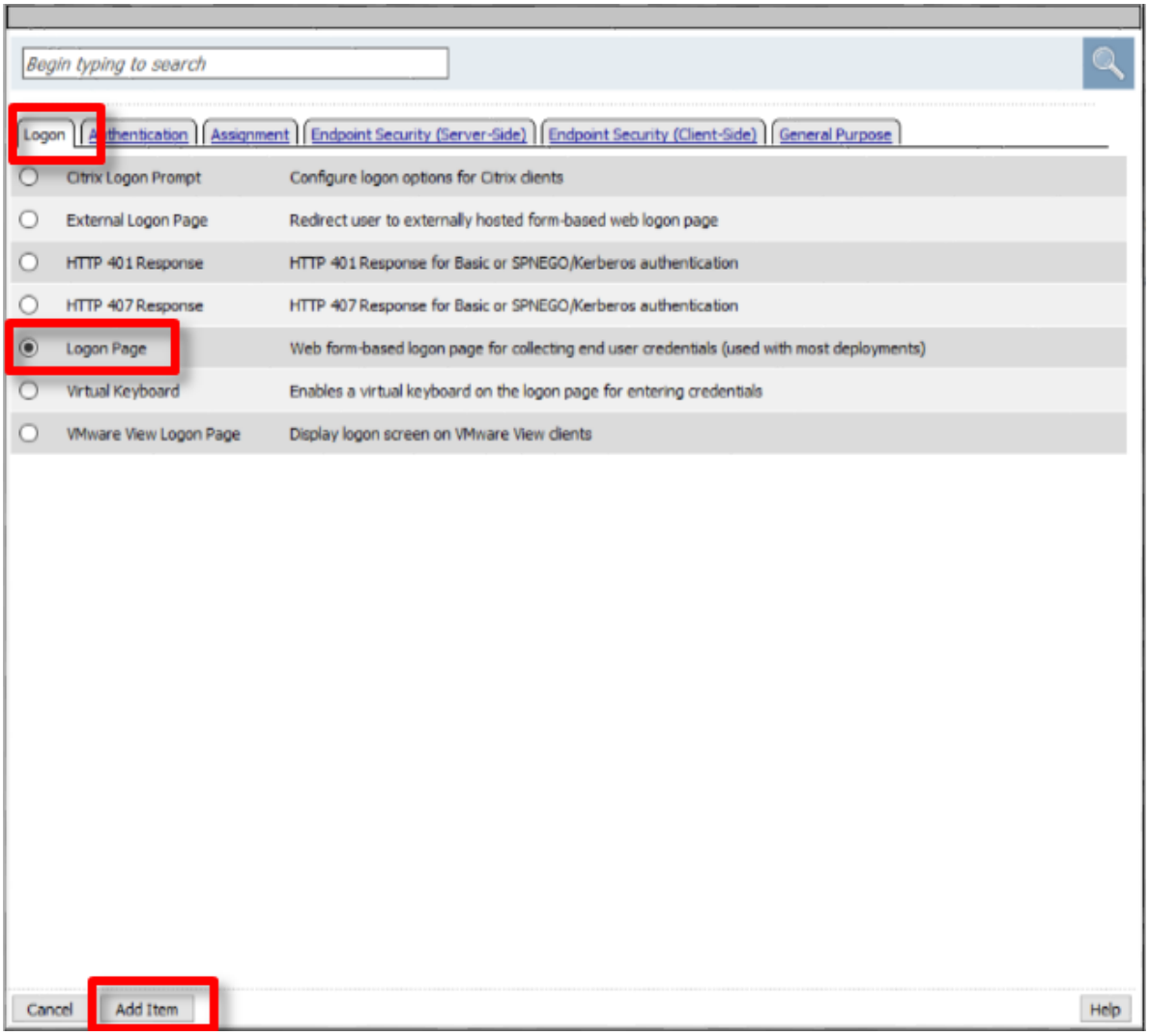


7. From the **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies) screen**, click the **Edit** link on the previously created `idp.f5demo.com?policy` line

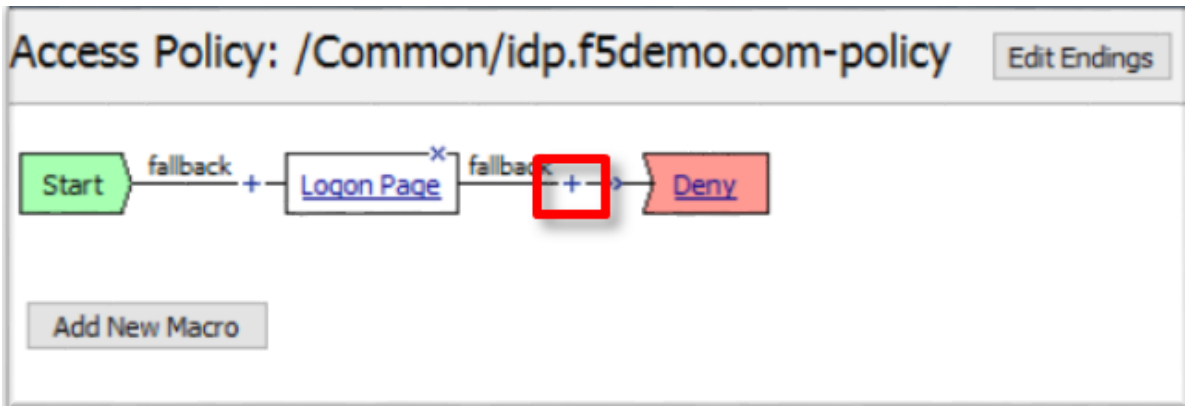


8. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** between **Start** and **Deny**

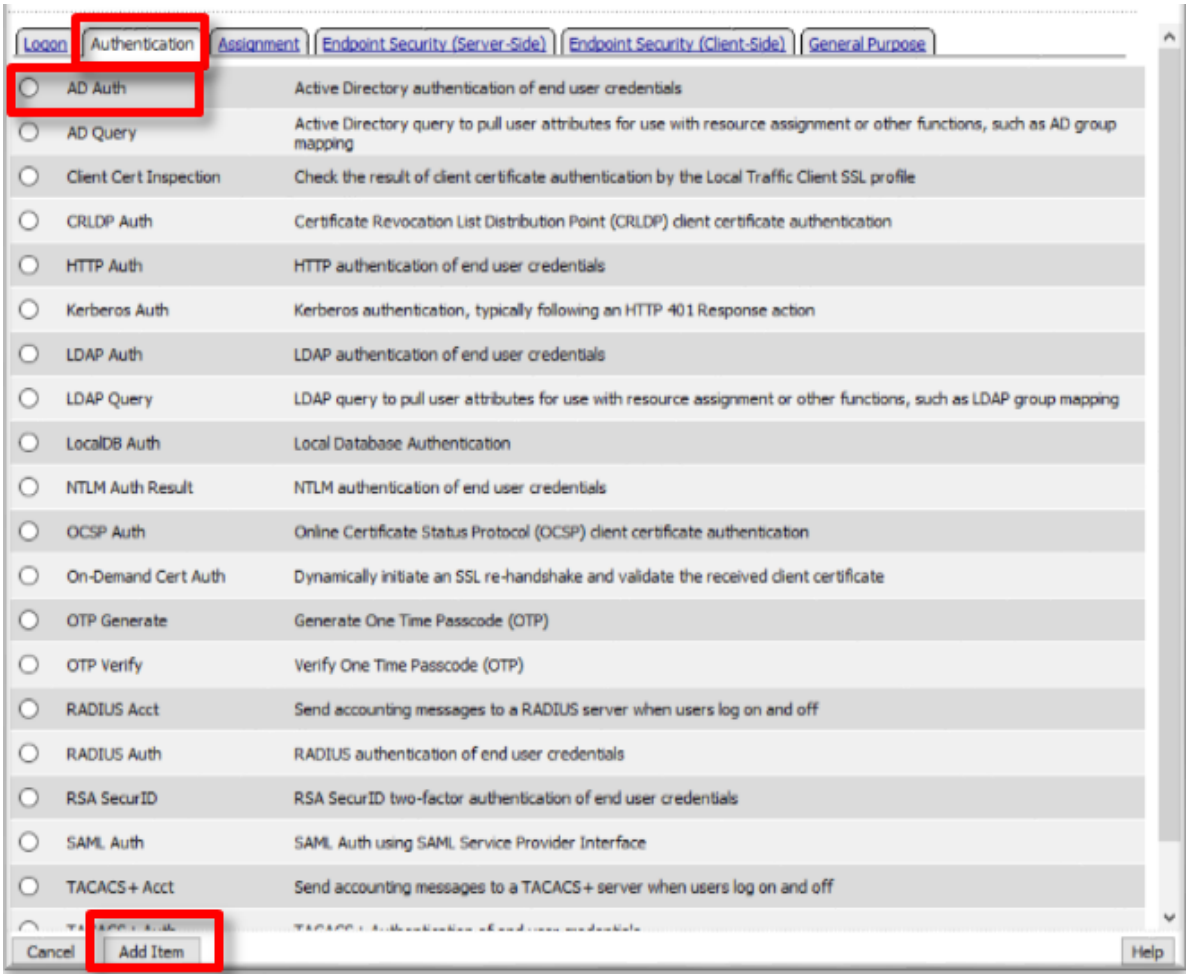
9. In the pop-up dialog box, select the **Logon** tab and then select the **Radio** next to **Logon Page**, and click the **Add Item** button
10. Click **Save** in the resulting Logon Page dialog box



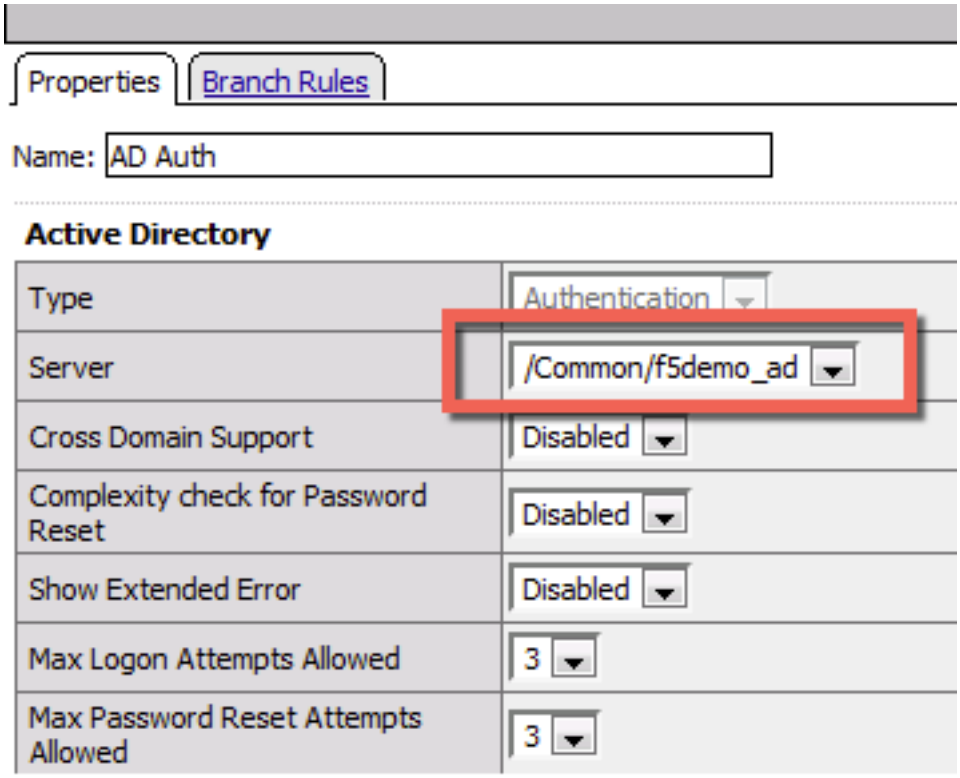
11. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** between **Logon Page** and **Deny**



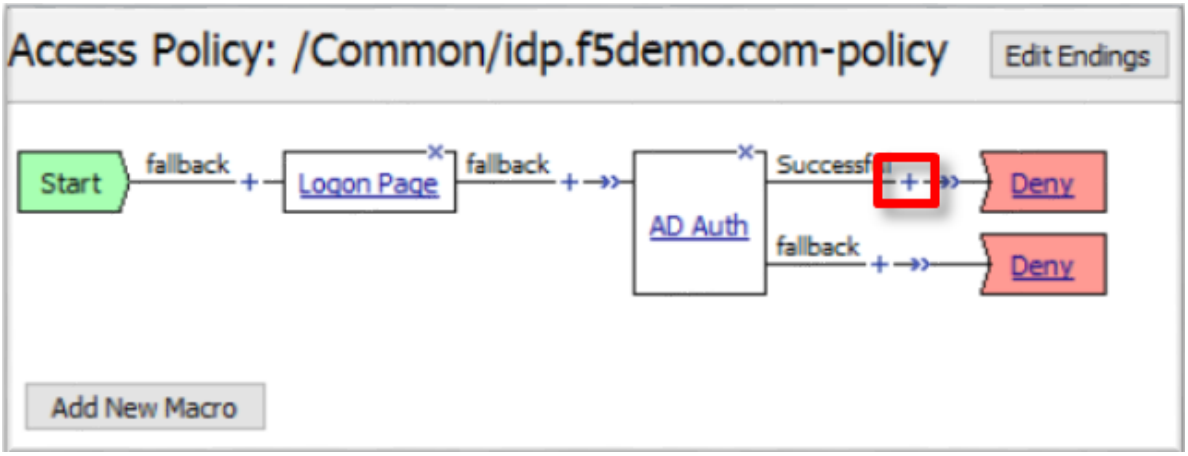
12. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Auth**, and click the **Add Item** button



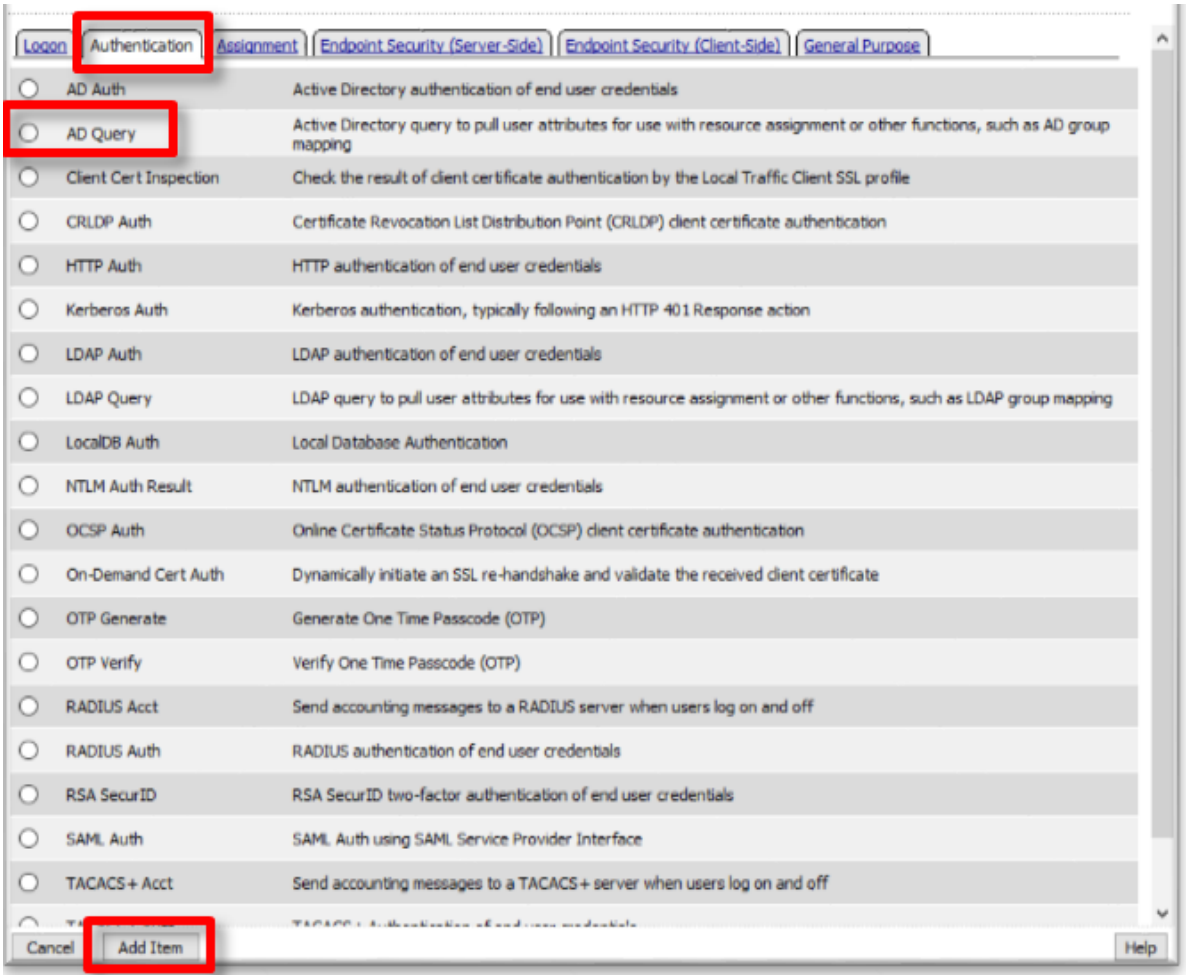
13. In the resulting **AD Auth** pop-up window, select `/Common/f5demo_ad` from the **Server** drop down menu
14. Click **Save** at the bottom of the window



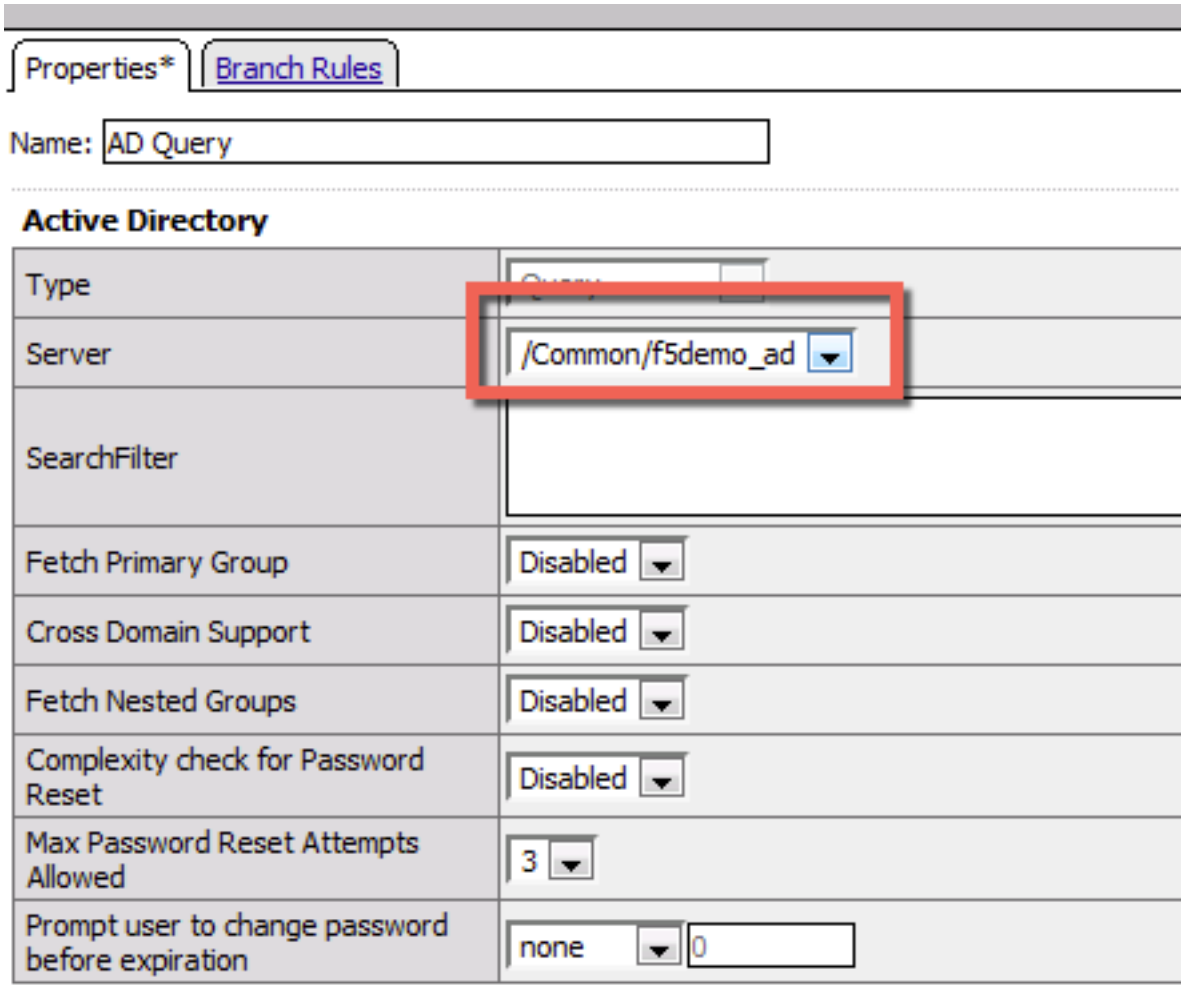
15. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** on the successful branch between **AD Auth** and **Deny**



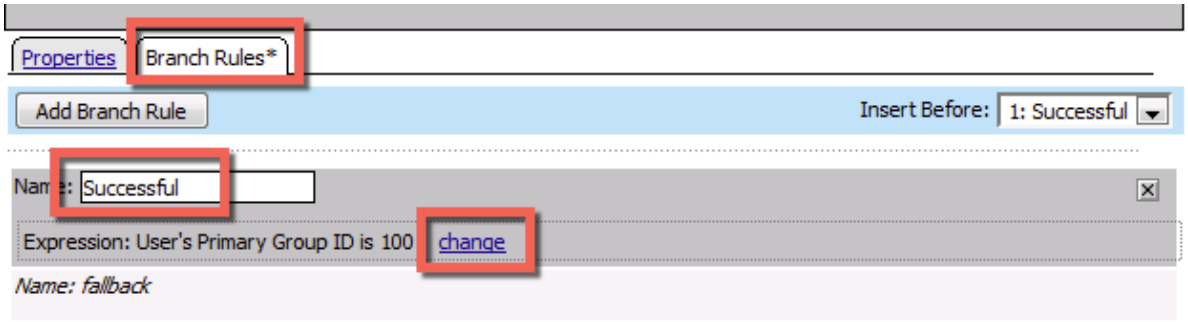
16. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button



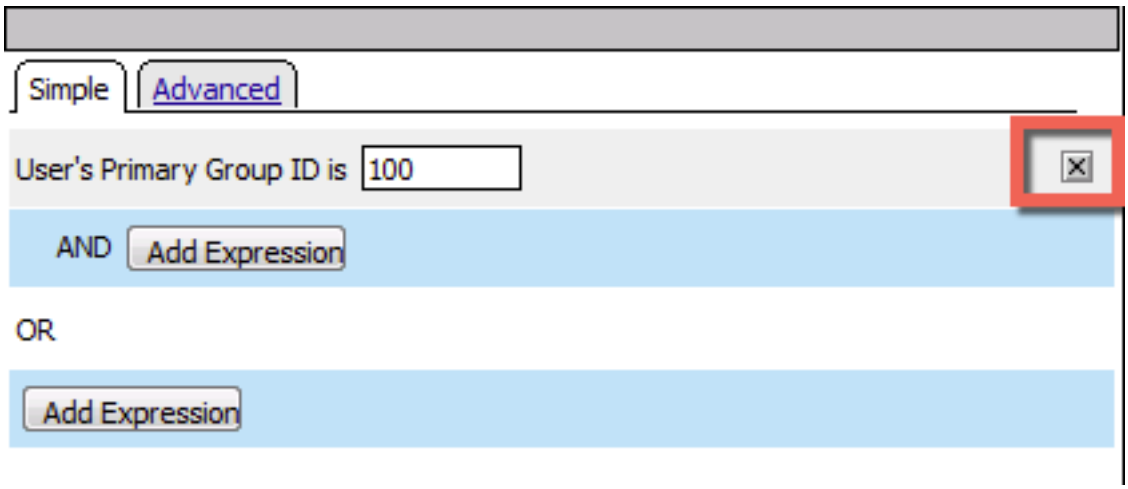
17. In the resulting **AD Query** pop-up window, select `/Common/f5demo_ad` from the **Server** drop down menu



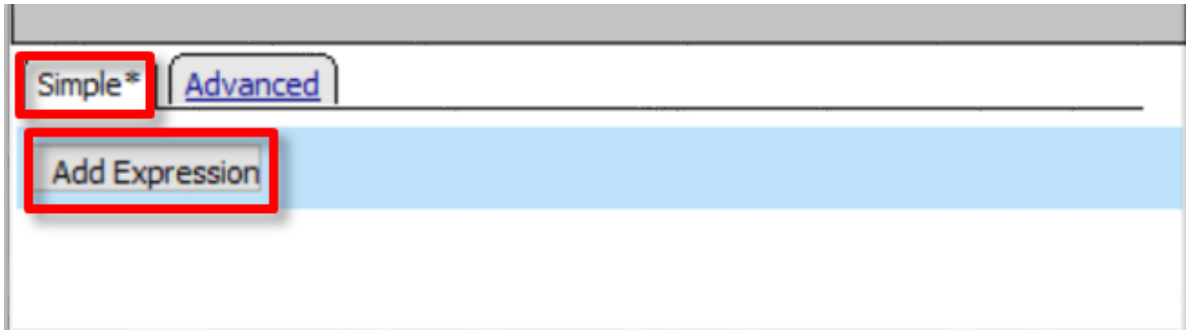
18. In the **AD Query** pop?up window, select the **Branch Rules** tab
19. Change the **Name** of the branch to *Successful*.
20. Click the **Change** link next to the **Expression**



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



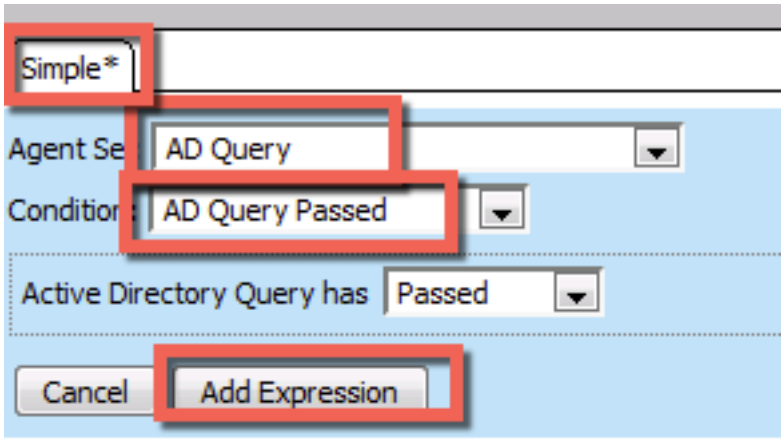
22. Create a new **Simple** expression by clicking the **Add Expression** button



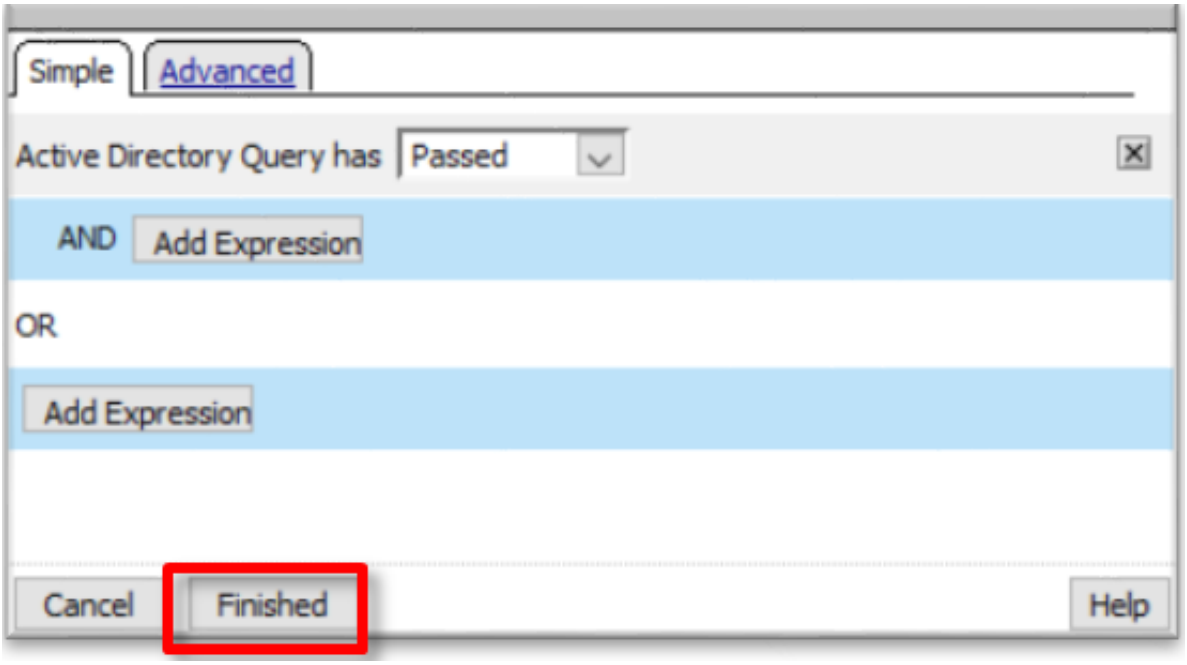
23. In the resulting menu, select the following from the drop down menus:

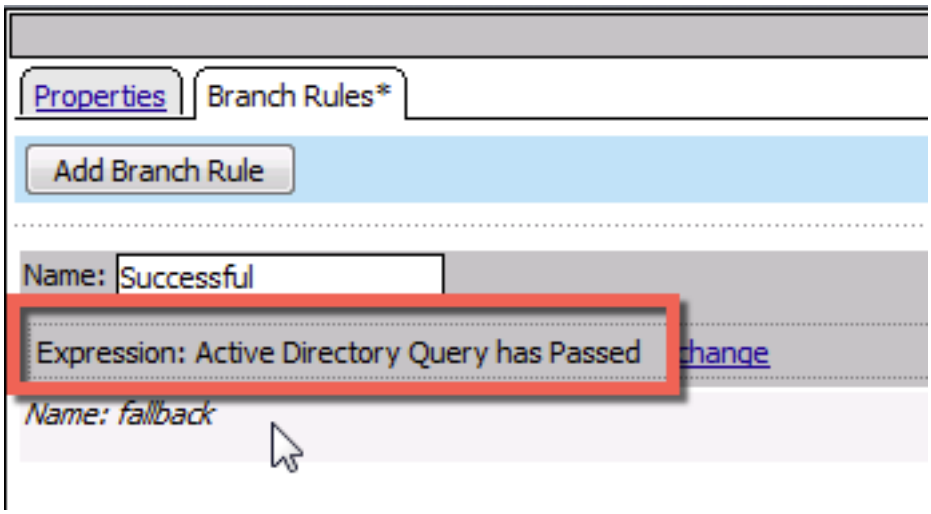
Agent Sel:	AD Query
Condition:	AD Query Passed

24. Click the **Add Expression** Button

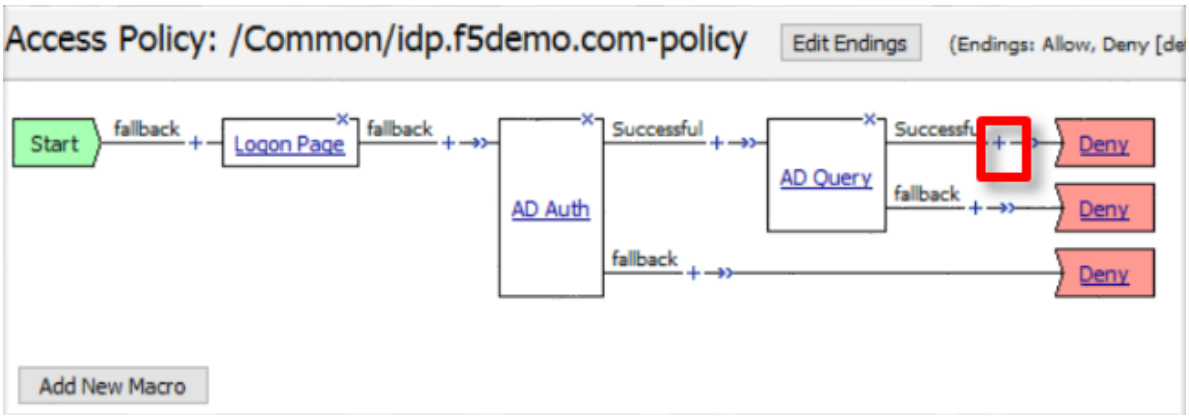


25. Click the **Finished** button to complete the expression

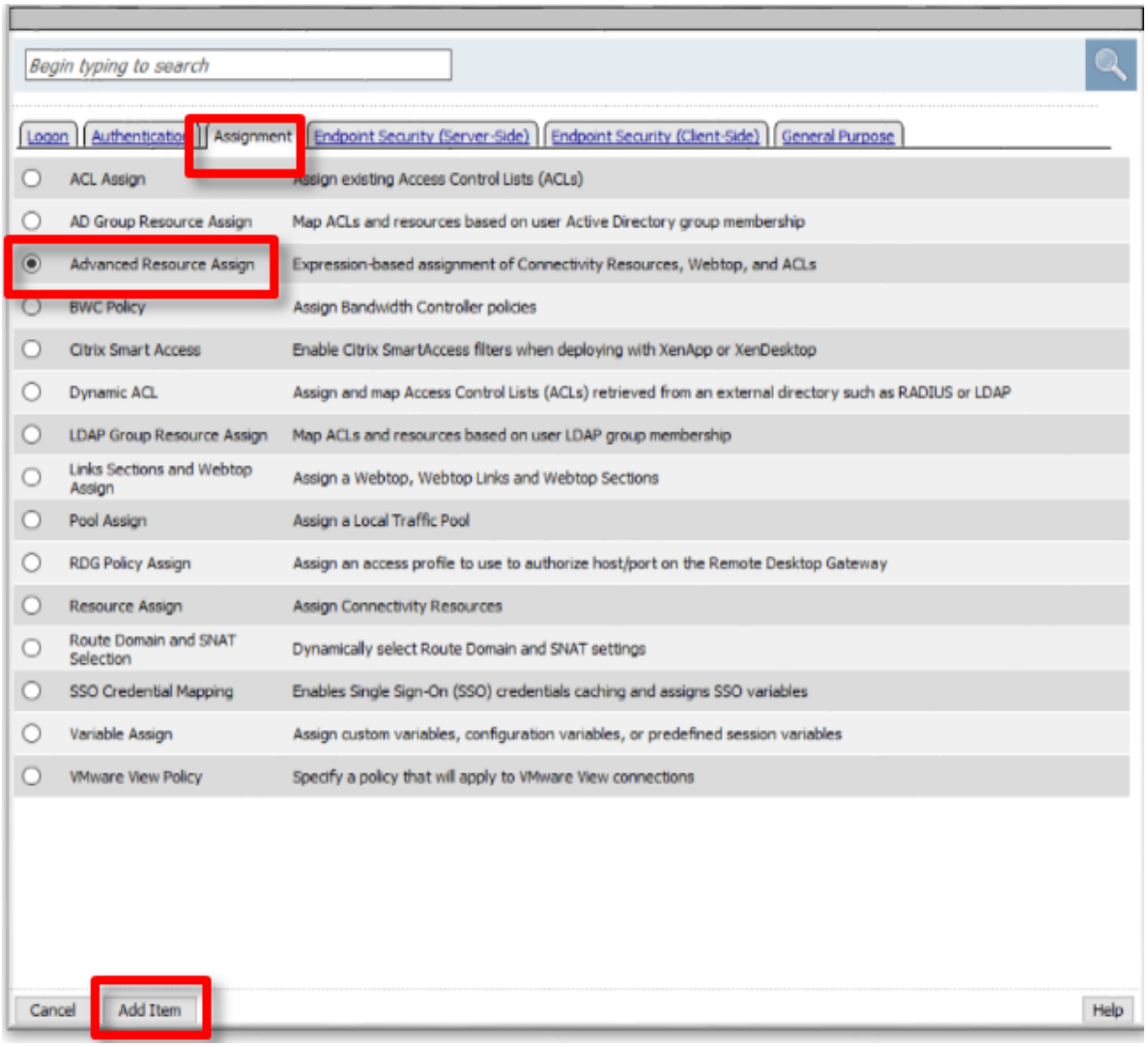




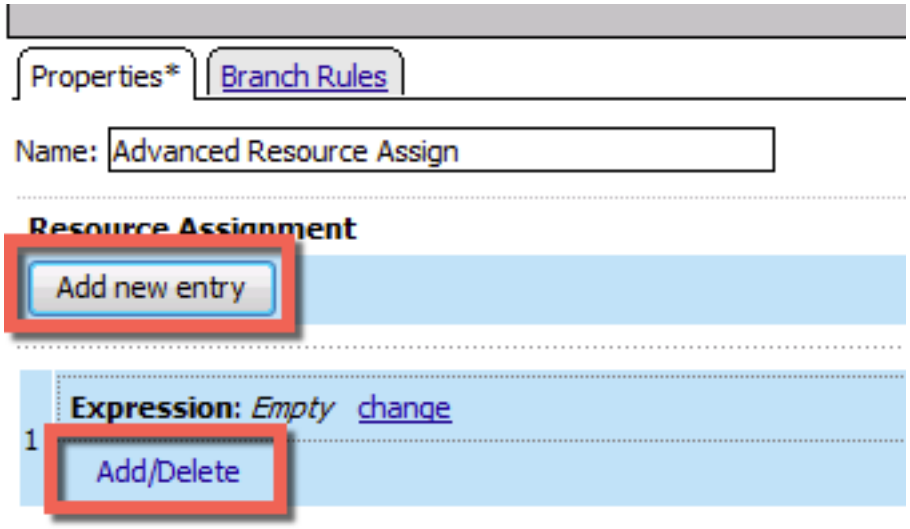
26. Click the **Save** button to complete the **AD Query**
27. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** on the successful branch between **AD Query** and **Deny**



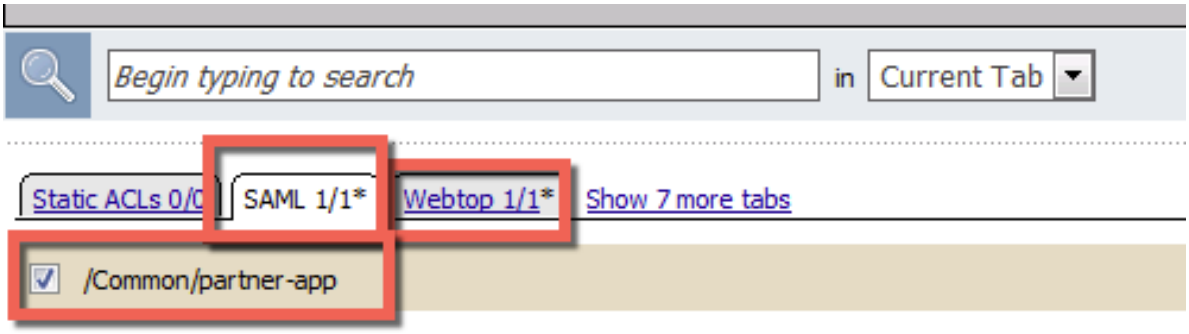
28. In the pop-up dialog box, select the **Assignment** tab and then select the **Radio** next to **Advanced Resource Assign**, and click the **Add Item** button



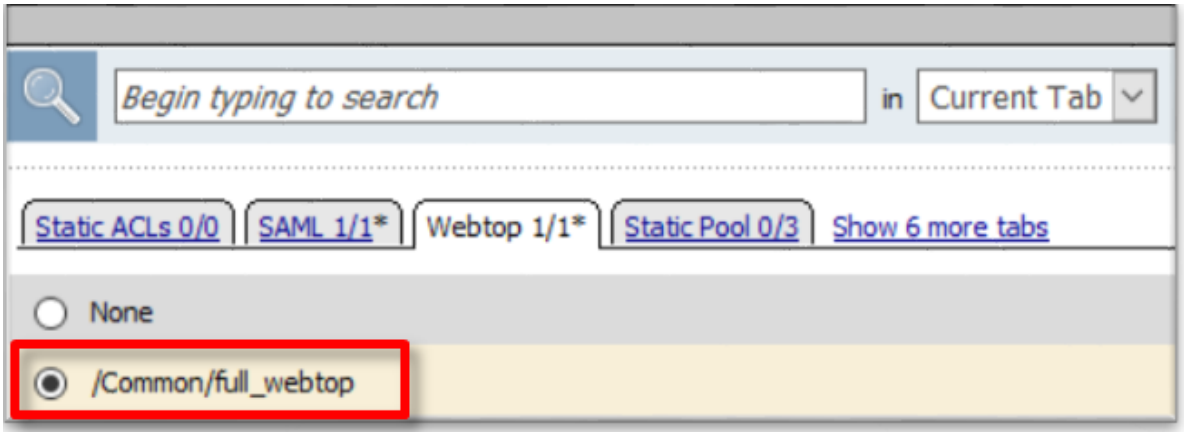
29. In the resulting **Advanced Resource Assign** pop-up window, click the **Add New Entry** button
30. In the new Resource Assignment entry, click the **Add**/**Delete** link



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

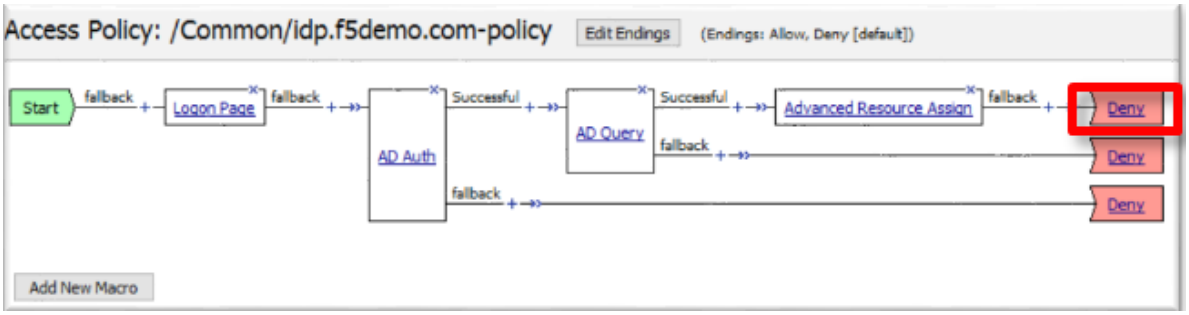


32. Click the **Webtop** tab, and select the **Checkbox** next to `/Common/full_webtop`



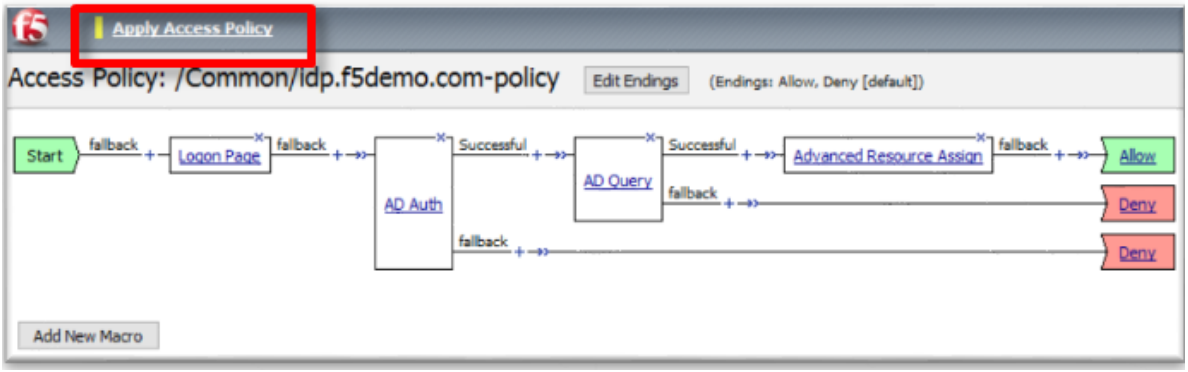
33. Click the **Update** button at the bottom of the window to complete the Resource Assignment entry
34. Click the **Save** button at the bottom of the **Advanced Resource Assign** window

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



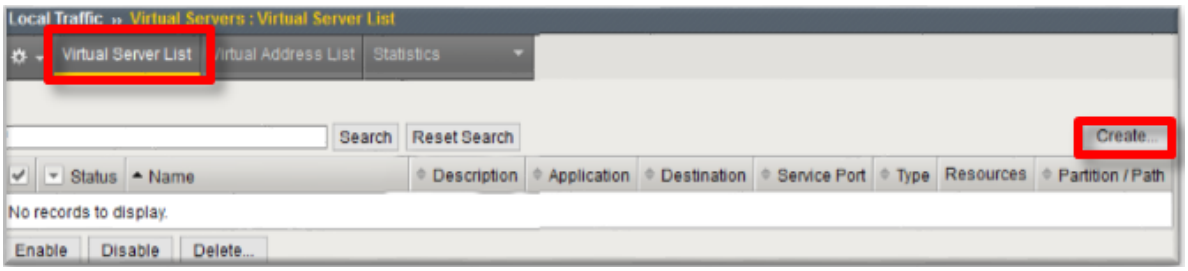
36. In the **Select Ending** dialog box, selet the **Allow** radio button and then click **Save**

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)

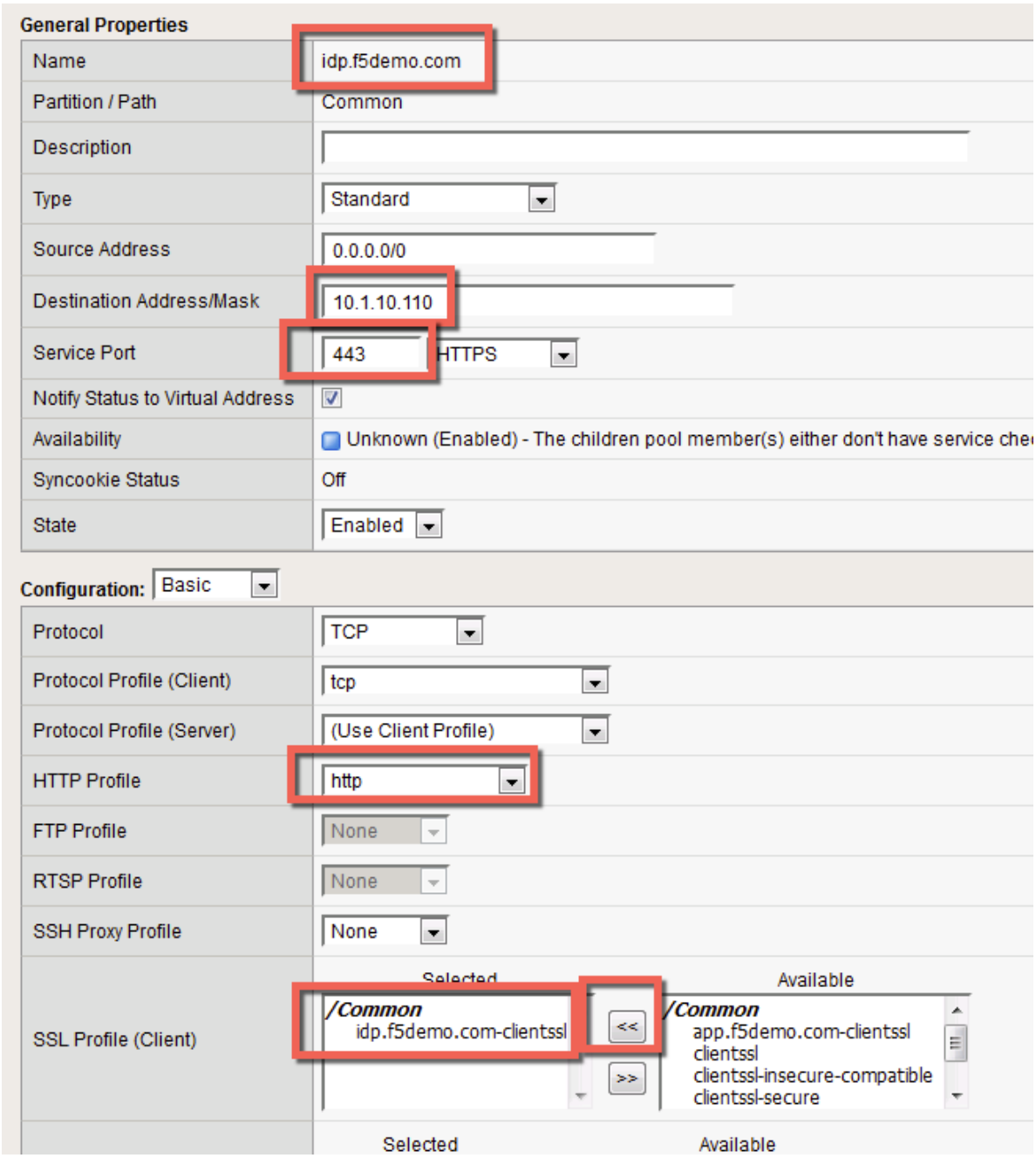


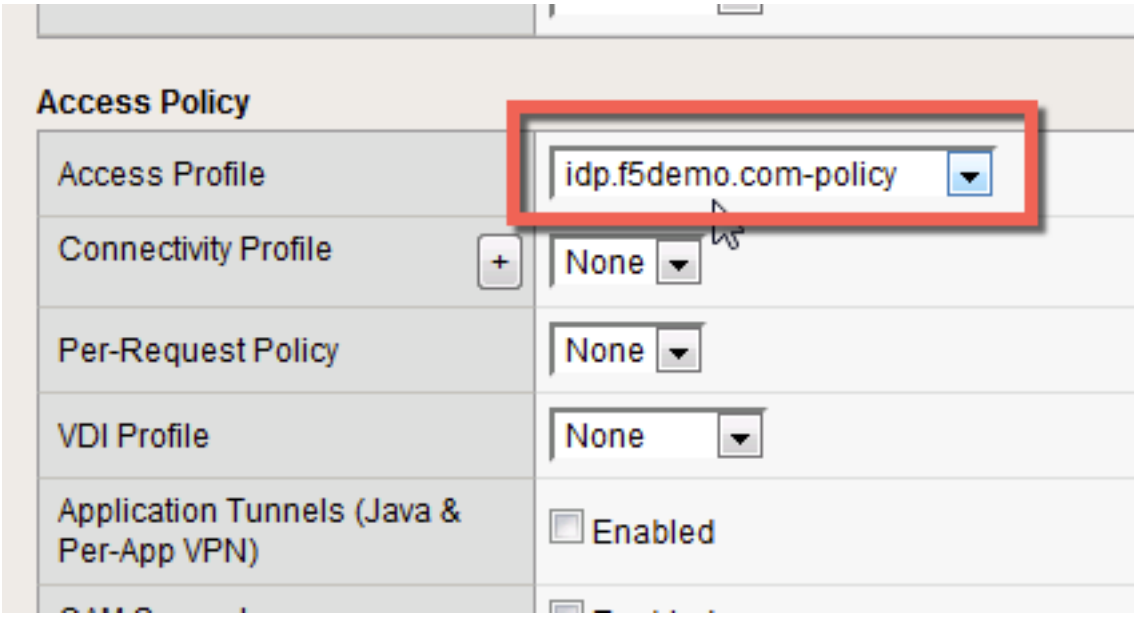
3. In the **New Virtual Server** window, enter the following information:

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`

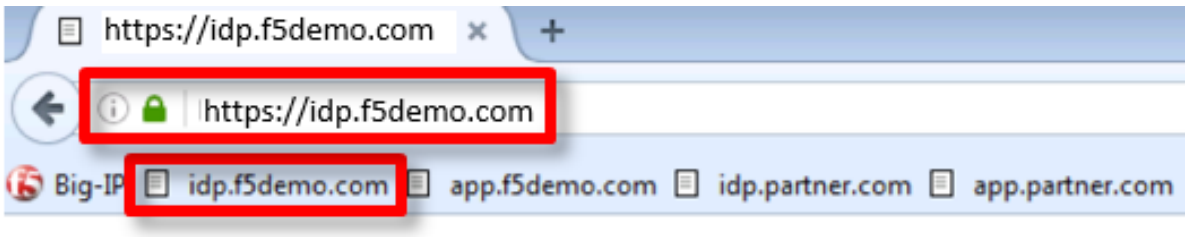

General Properties
Name
idp.f5demo.com
Partition / Path
Common
Description
Type
Standard
Source Address
0.0.0.0/0
Destination Address/Mask
10.1.10.110
Service Port
443
HTTPS
Notify Status to Virtual Address
Availability
Unknown (Enabled) - The children pool member(s) either don't have service che
Syncookie 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
Selected
Available
SSL Profile (Client)
/Common
idp.f5demo.com-clientssl
<<
>>
/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

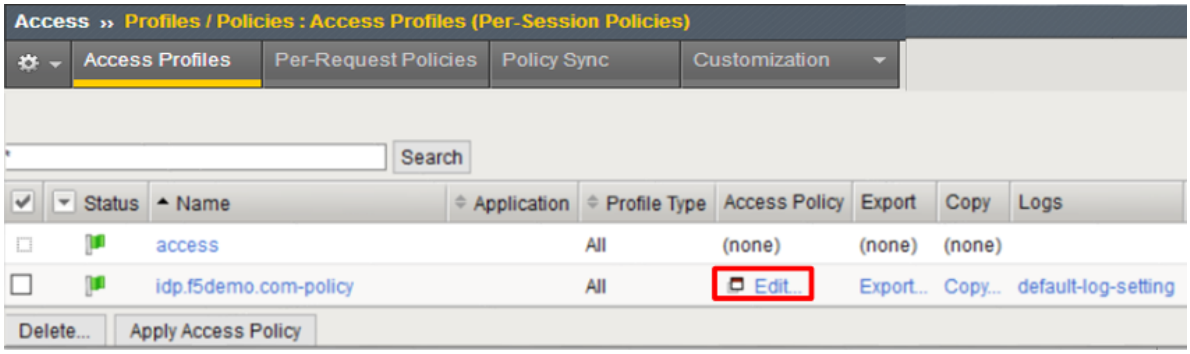
Lab Requirements:

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

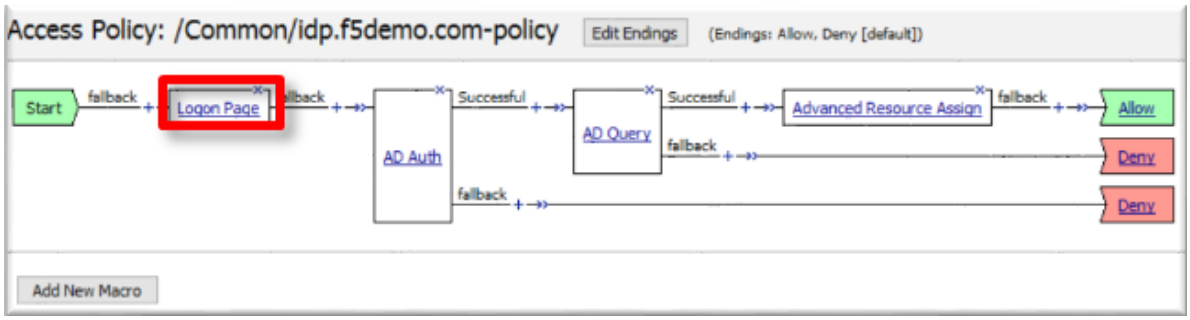
Estimated completion time: 25 minutes

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

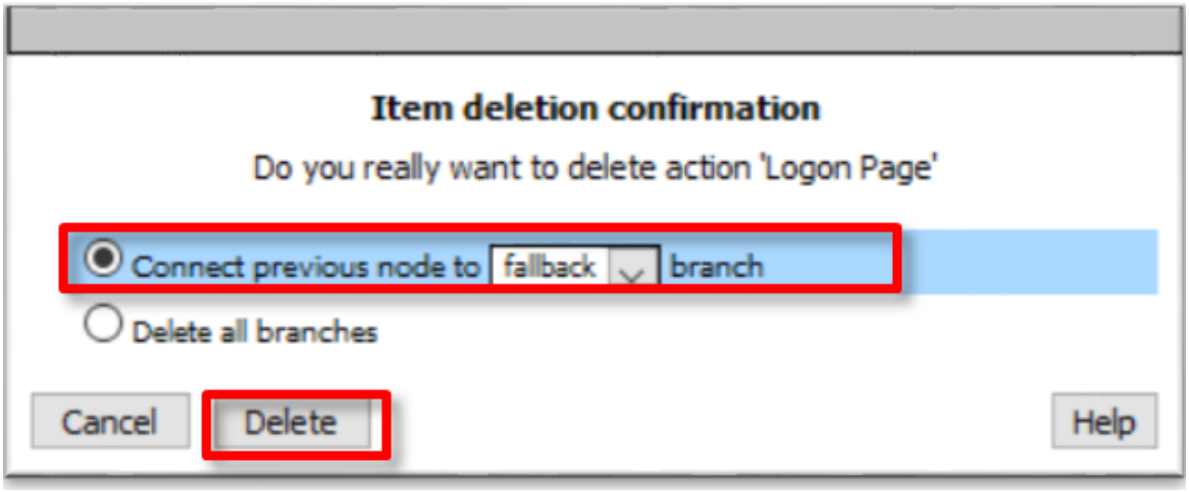
1. Using the existing Access Policy from Lab 2, navigate to **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)**, and click the **Edit** link next to the previously created *idp.f5demo.com-policy*



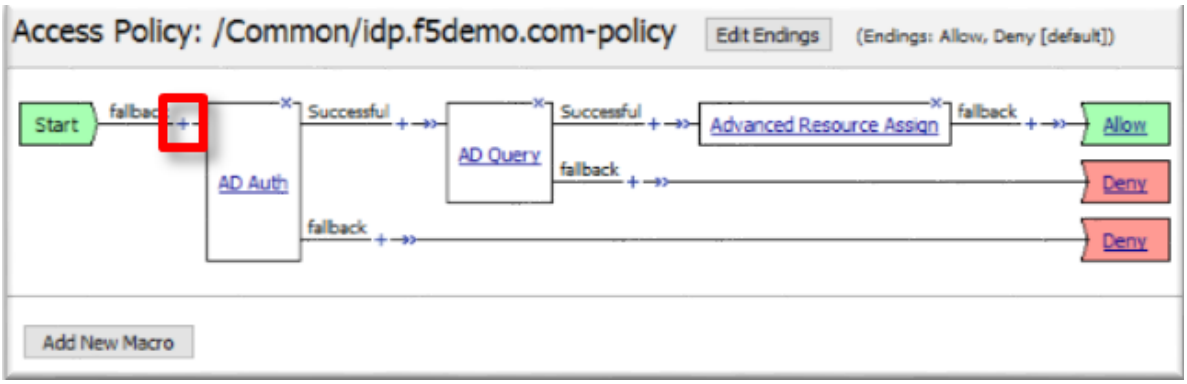
2. Delete the **Logon Page** object by clicking on the **X** as shown



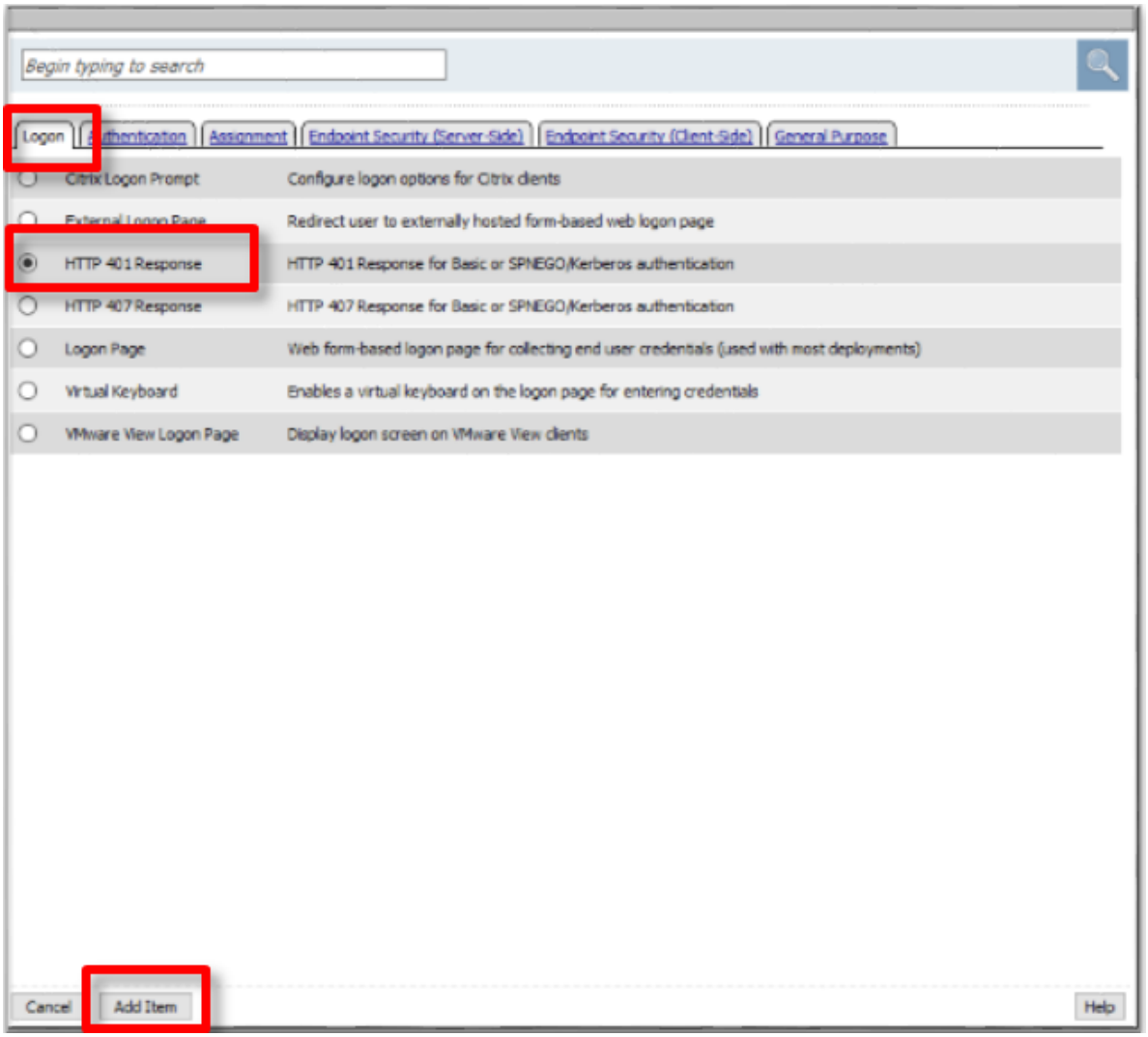
3. In the resulting **Item Deletion Confirmation** dialog, ensure that the previous node is connect to the **fallback** branch, and click the **Delete** button



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



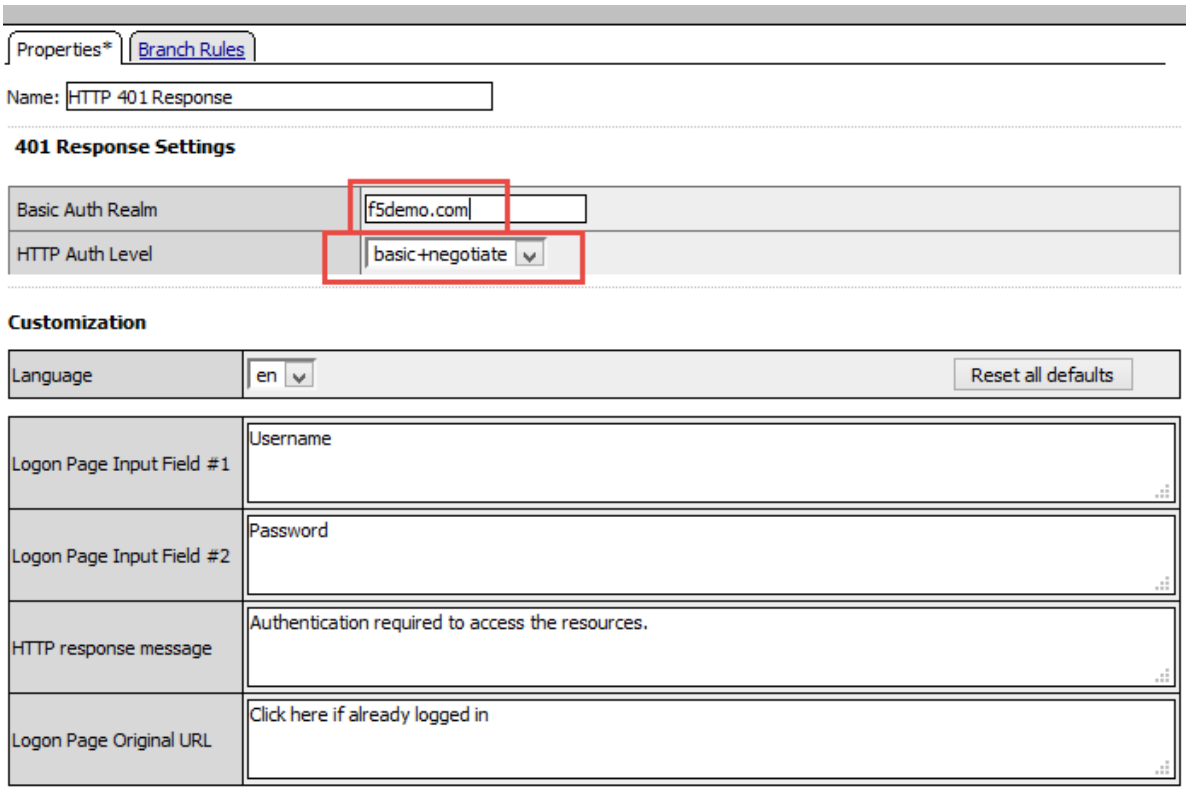
5. In the pop-up dialog box, select the **Logon** tab and then select the **Radio** next to **HTTP 401 Response**, and click the **Add Item** button



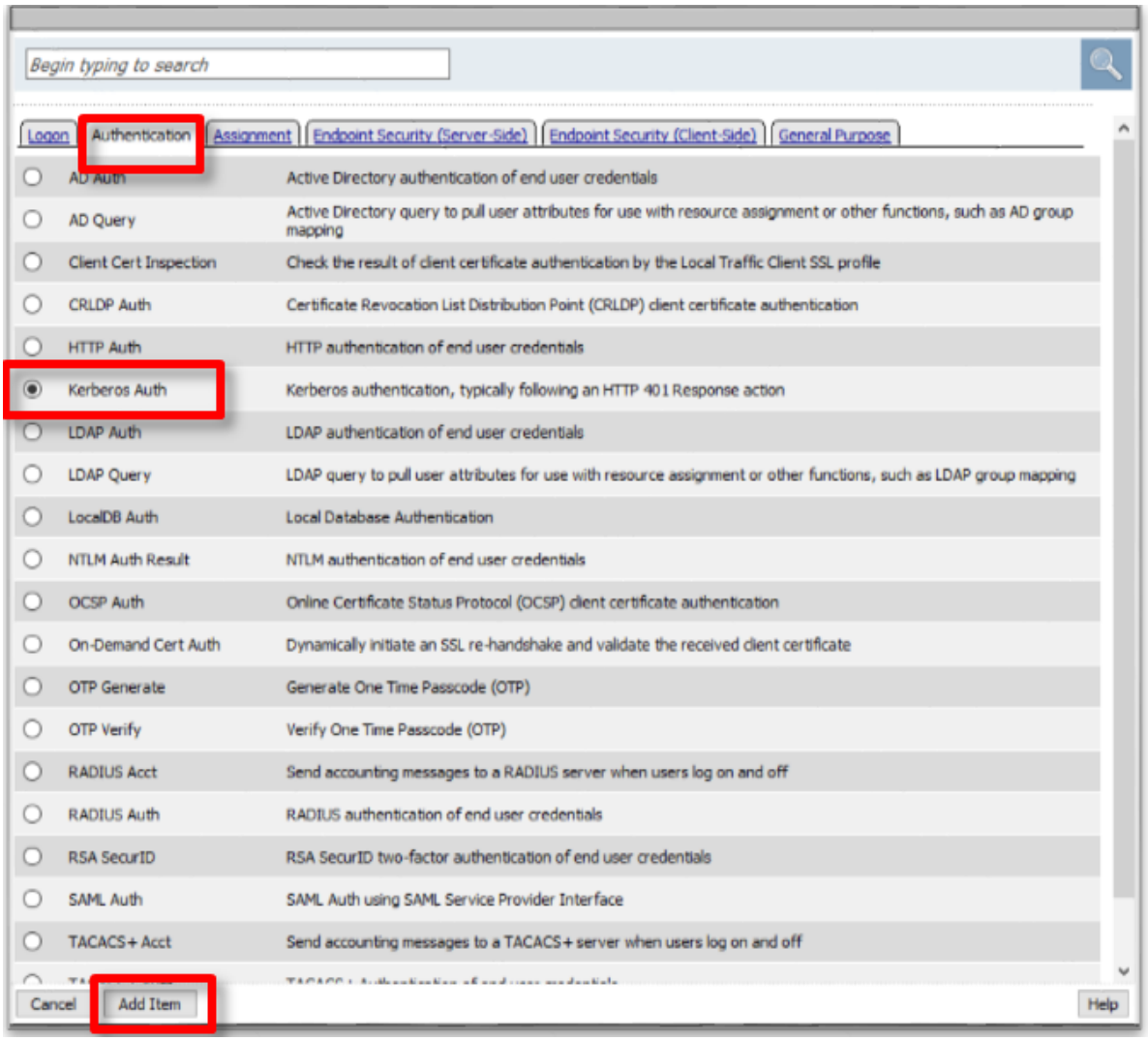
6. In the **HTTP 401 Response** dialog box, enter the following information:

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

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



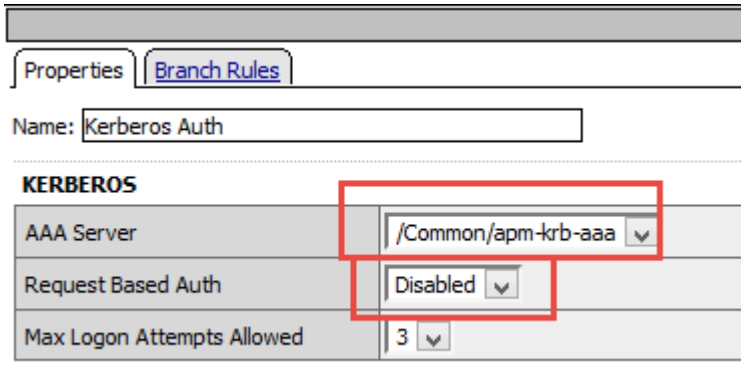
8. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** on the **Negotiate** branch between **HTTP 401 Response** and **Deny**
9. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **Kerberos Auth**, and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



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

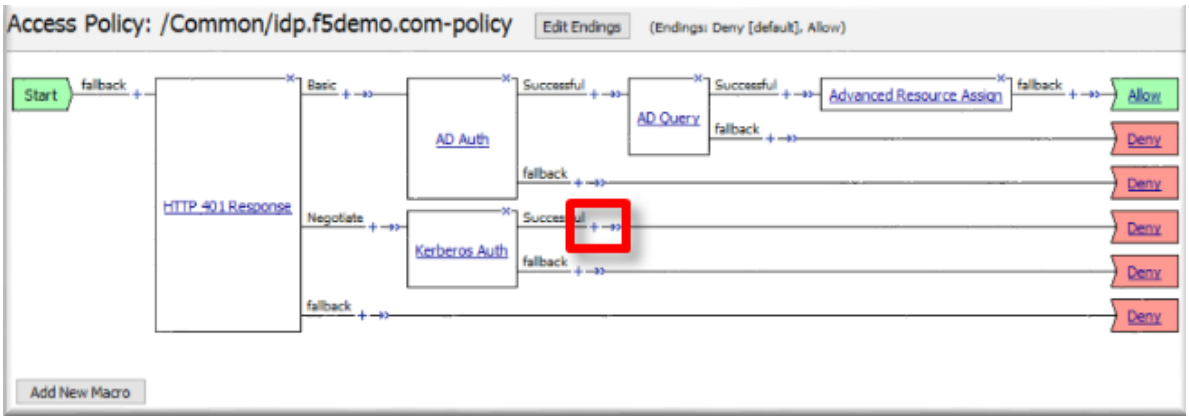
AAA Server:	`/Common/apm-krb-aaa` (drop down)
Request Based Auth:	`Disabled` (drop down)

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

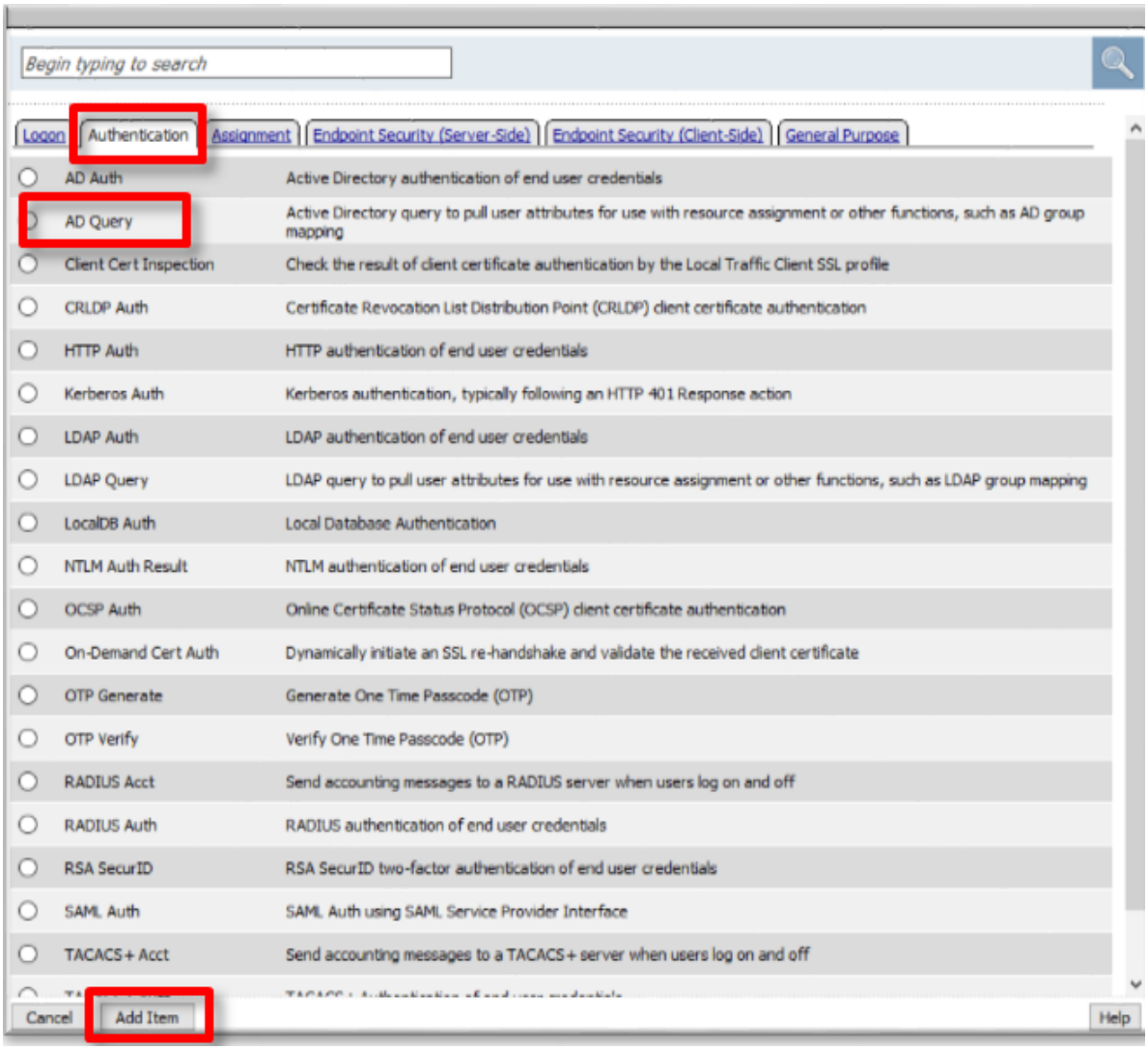


Note: The *apm-krb-aaa* object was pre-created for you in this lab. More details on the configuration of Kerberos AAA are included in the Learn More section at the end of this guide.

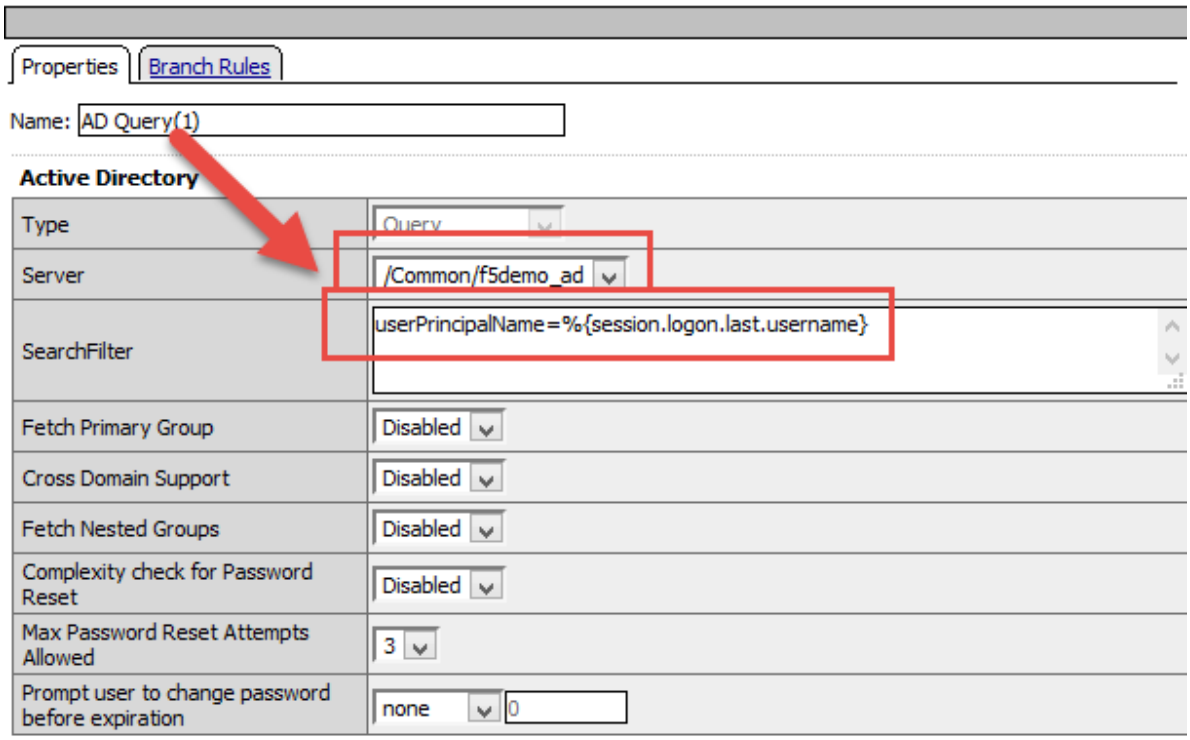
12. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** on the **Successful** branch between **Kerberos Auth** and **Deny**



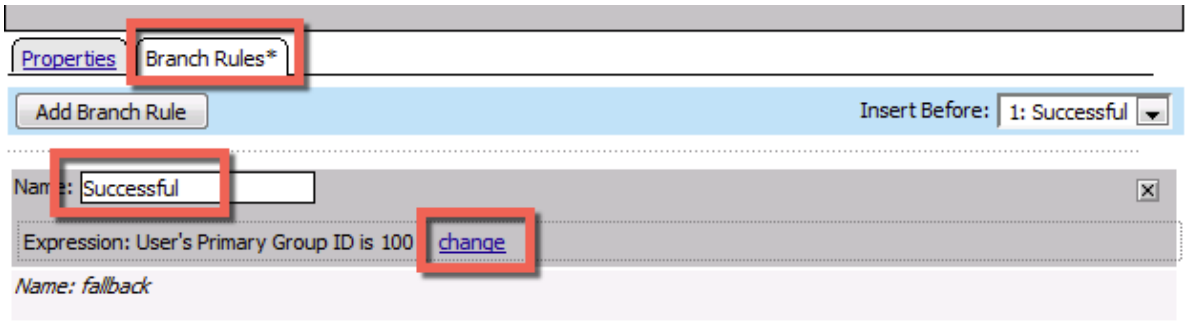
13. In the pop-up dialog box, select the **Authentication** tab and then select the **Radio** next to **AD Query**, and click the **Add Item** button



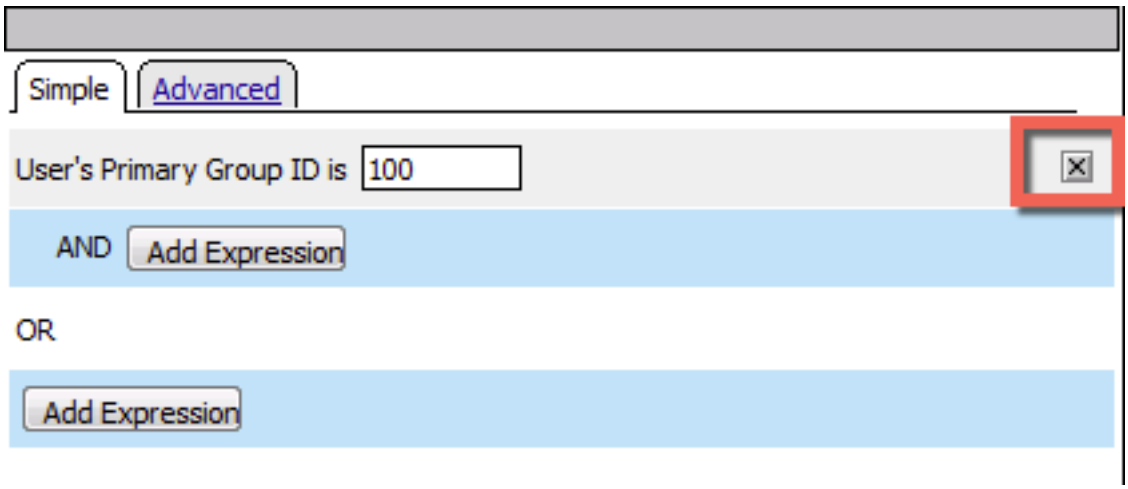
14. In the resulting **AD Query(1)** pop-up window, select `/Commmon/f5demo_ad` from the **Server** drop down menu
15. In the **SearchFilter** field, enter the following value: `userPrincipalName=%{session.logon.last.username}`



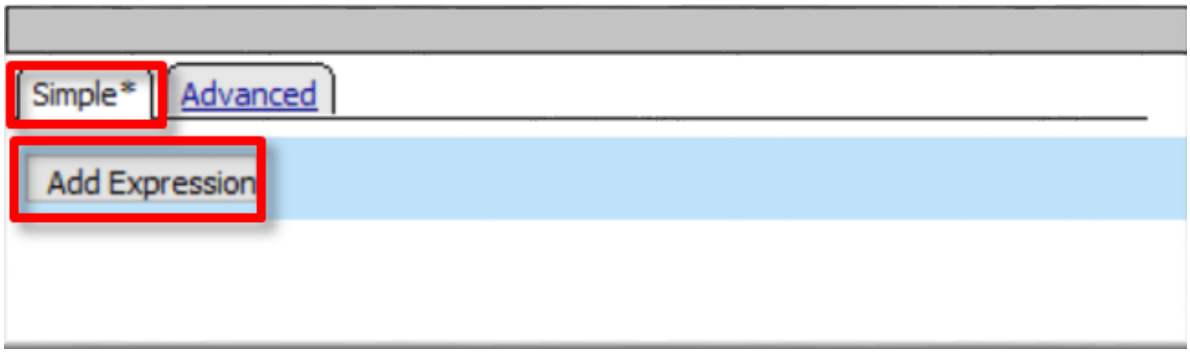
16. In the **AD Query(1)** window, click the **Branch Rules** tab
17. Change the **Name** of the branch to *Successful*.
18. Click the **Change** link next to the **Expression**



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



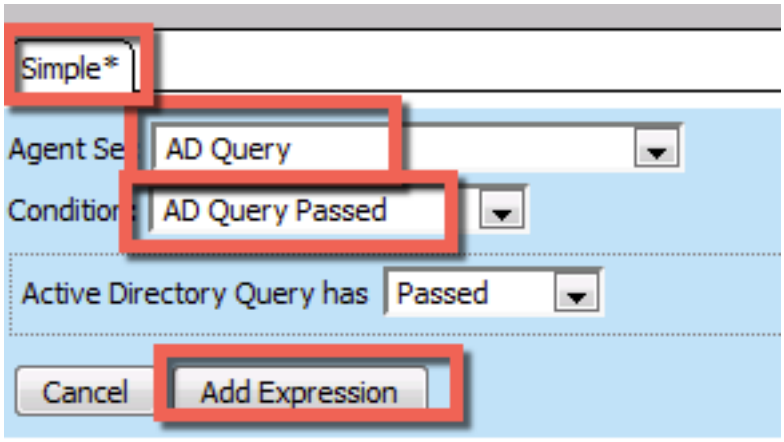
20. Create a new **Simple** expression by clicking the **Add Expression** button



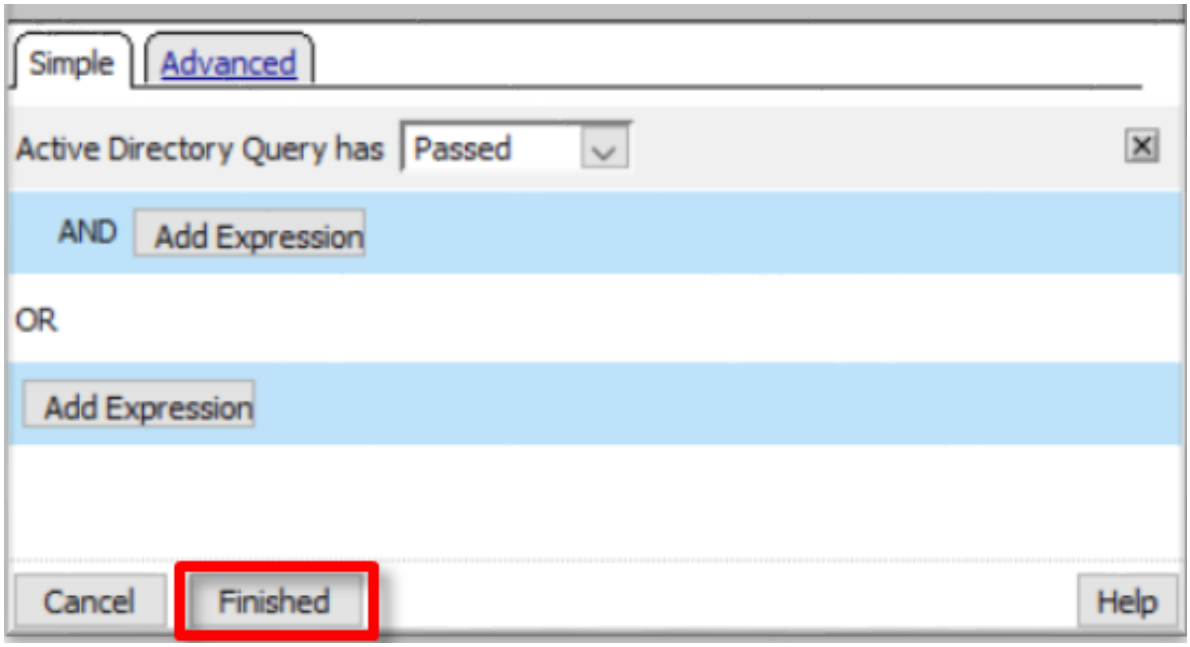
21. In the resulting menu, select the following from the drop down menus:

Agent Sel:	AD Query
Condition:	AD Query Passed

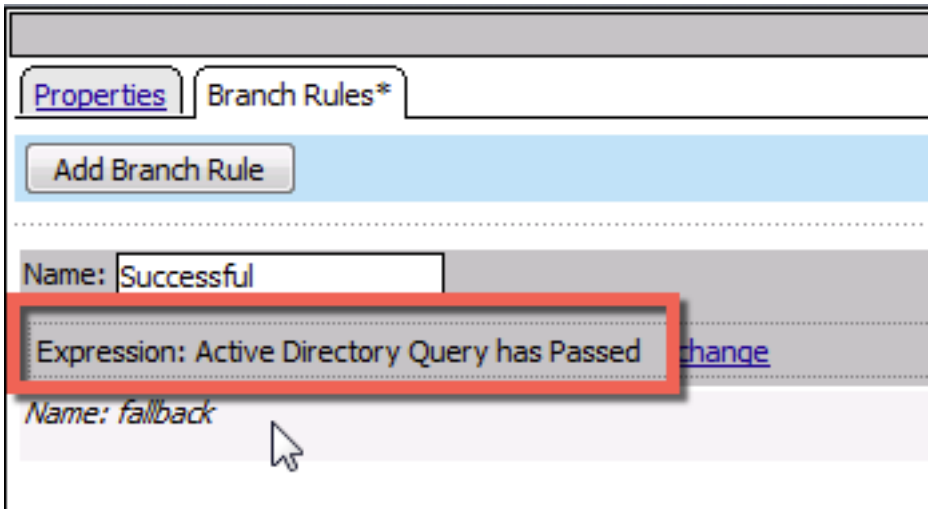
22. Click the **Add Expression** Button



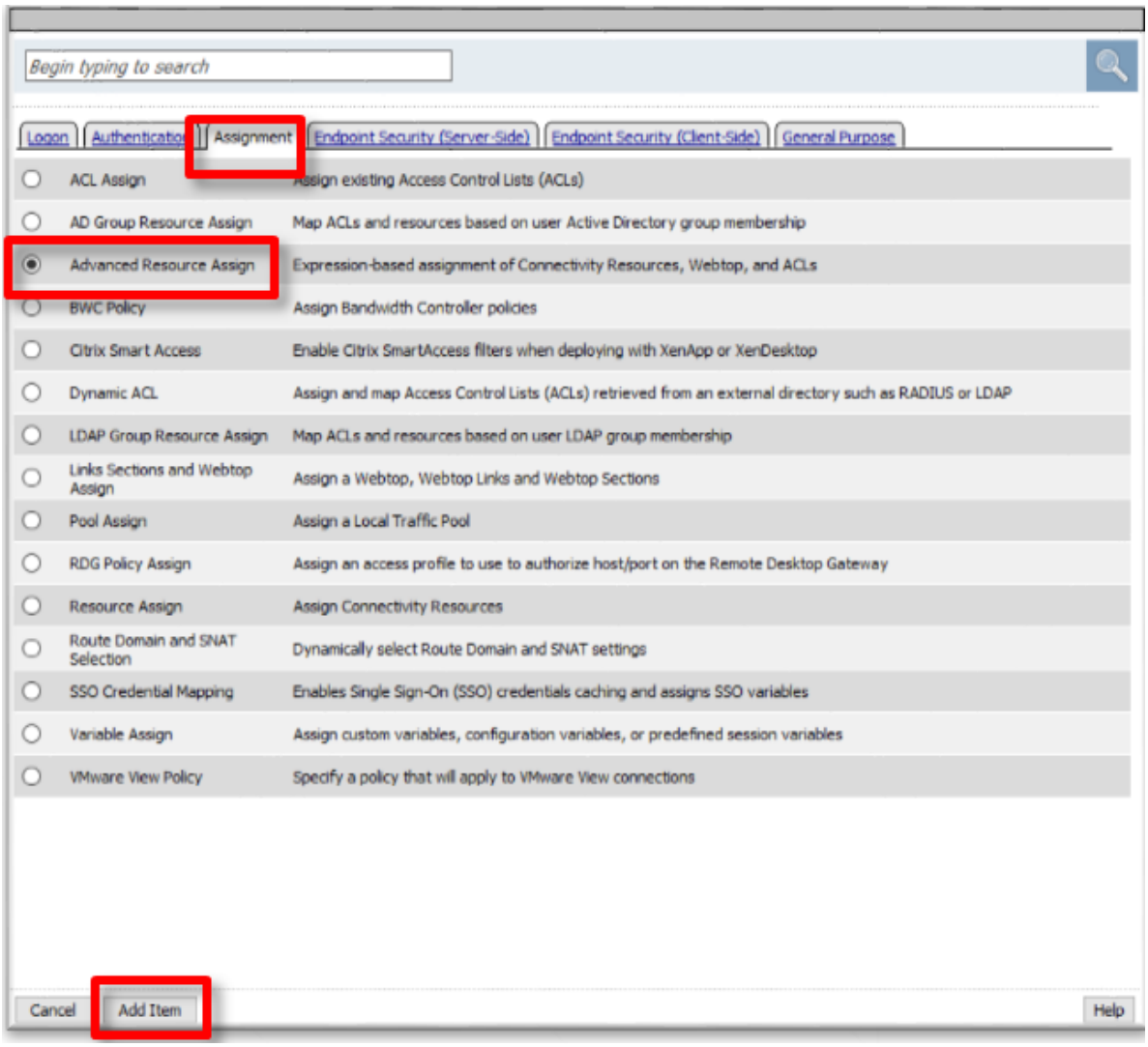
23. Click the **Finished** button to complete the expression



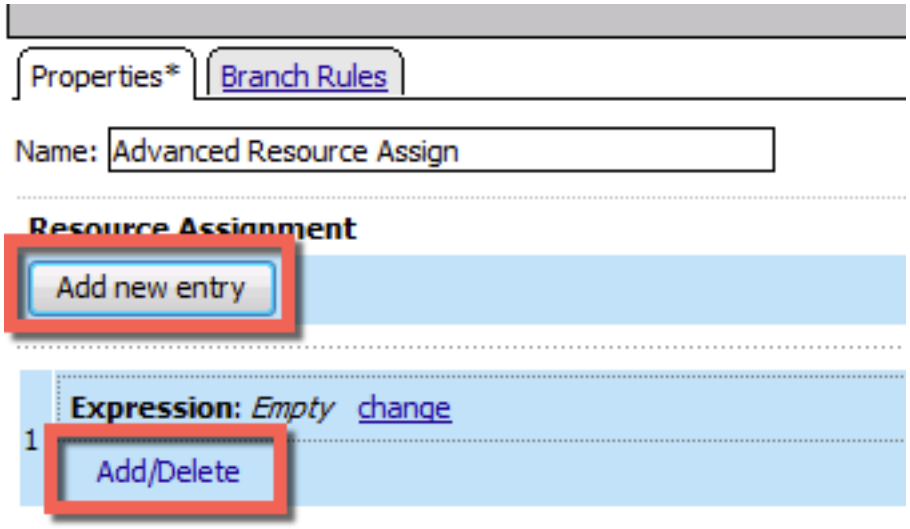
24. Click the **Save** button to complete the **AD Query**



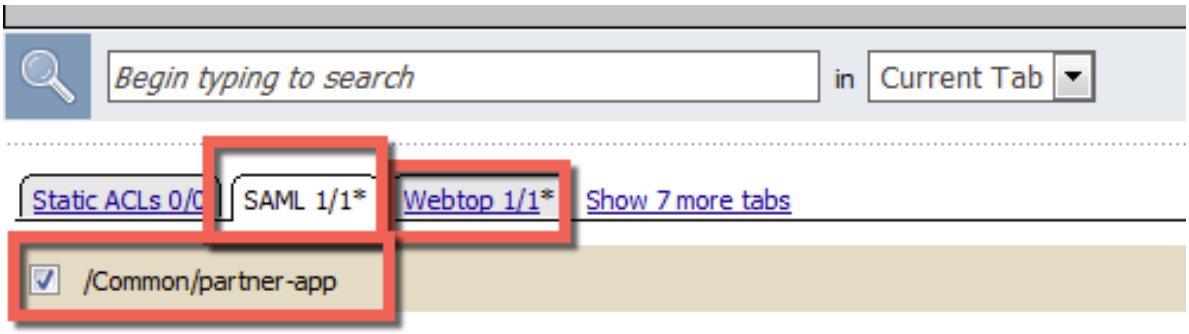
25. In the **Visual Policy Editor** window for `/Common/idp.f5demo.com?policy`, click the **Plus (+) Sign** on the **Successful** branch between **AD Query(1)** and **Deny**
26. In the pop-up dialog box, select the **Assignment** tab and then select the **Radio** next to **Advanced Resource Assign**,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



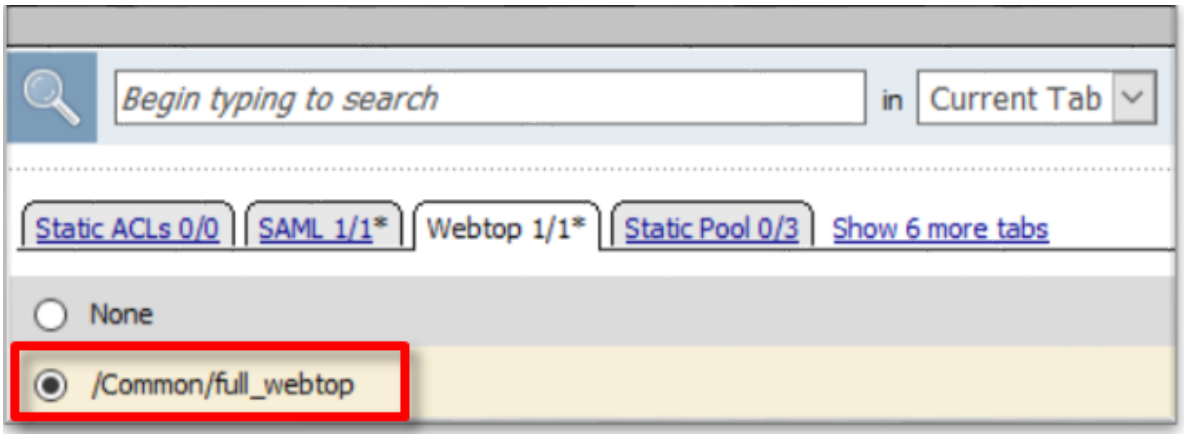
27. In the resulting **Advanced Resource Assign(1)** pop-up window, click the **Add New Entry** button
28. In the new Resource Assignment entry, click the **Add/Delete** link



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

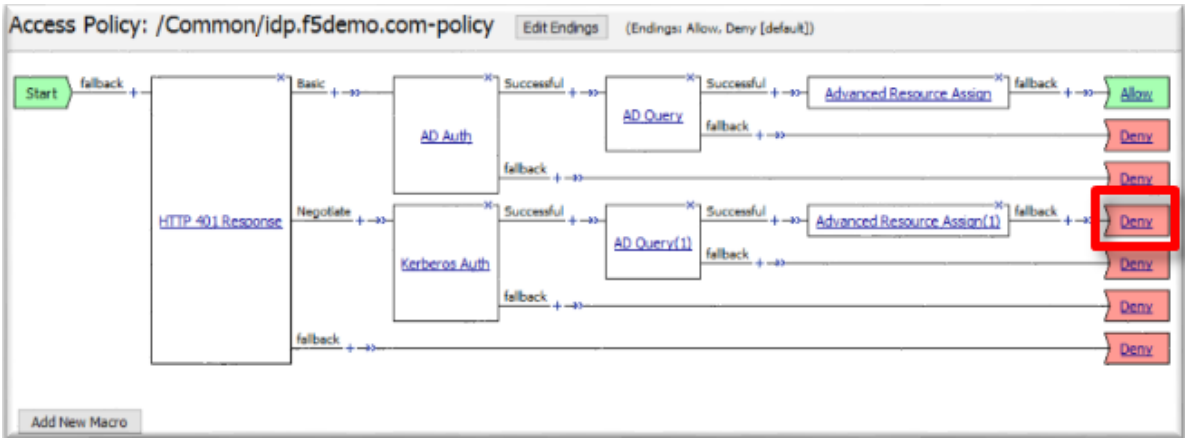


30. Click the **Webtop** tab, and select the **Checkbox** next to `/Common/full_webtop`



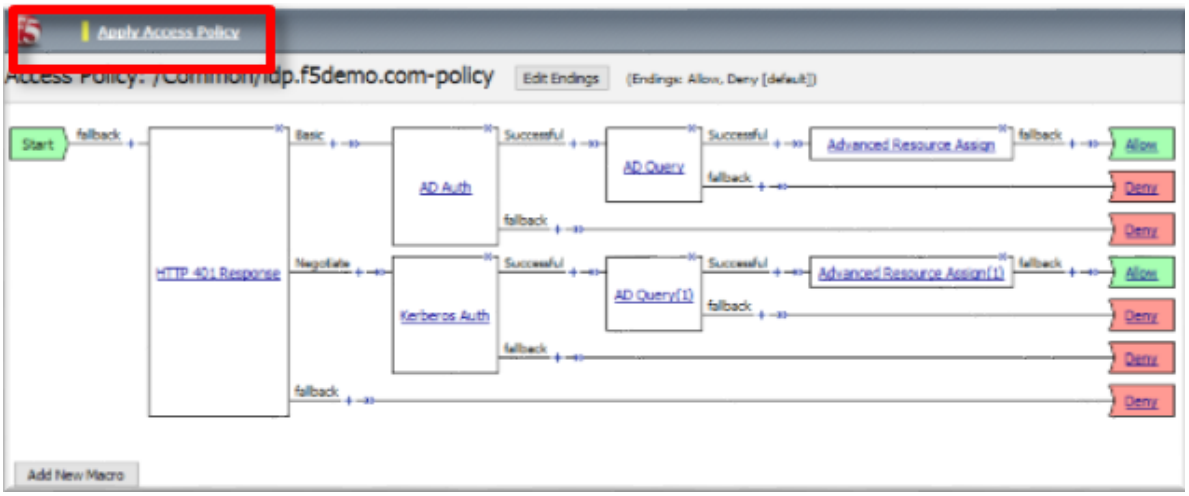
31. Click the **Update** button at the bottom of the window to complete the Resource Assignment entry
32. Click the **Save** button at the bottom of the **Advanced Resource Assign(1)** window

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



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

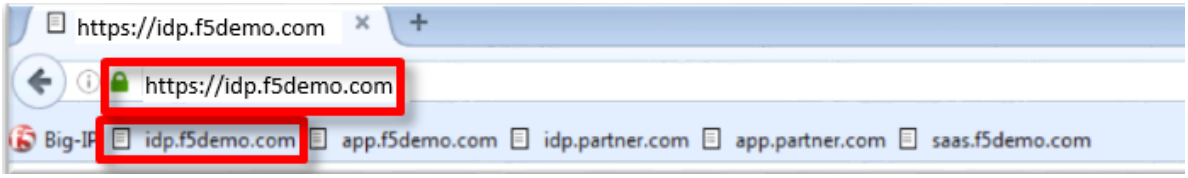
35. In the **Visual Policy Editor**, click **Apply Access Policy** (top left), and close the **Visual Policy Editor**



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

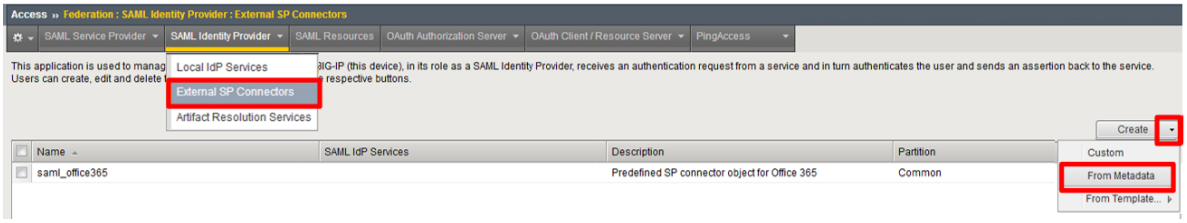
Lab Requirements:

- All lab requirements will be noted in the tasks that follow

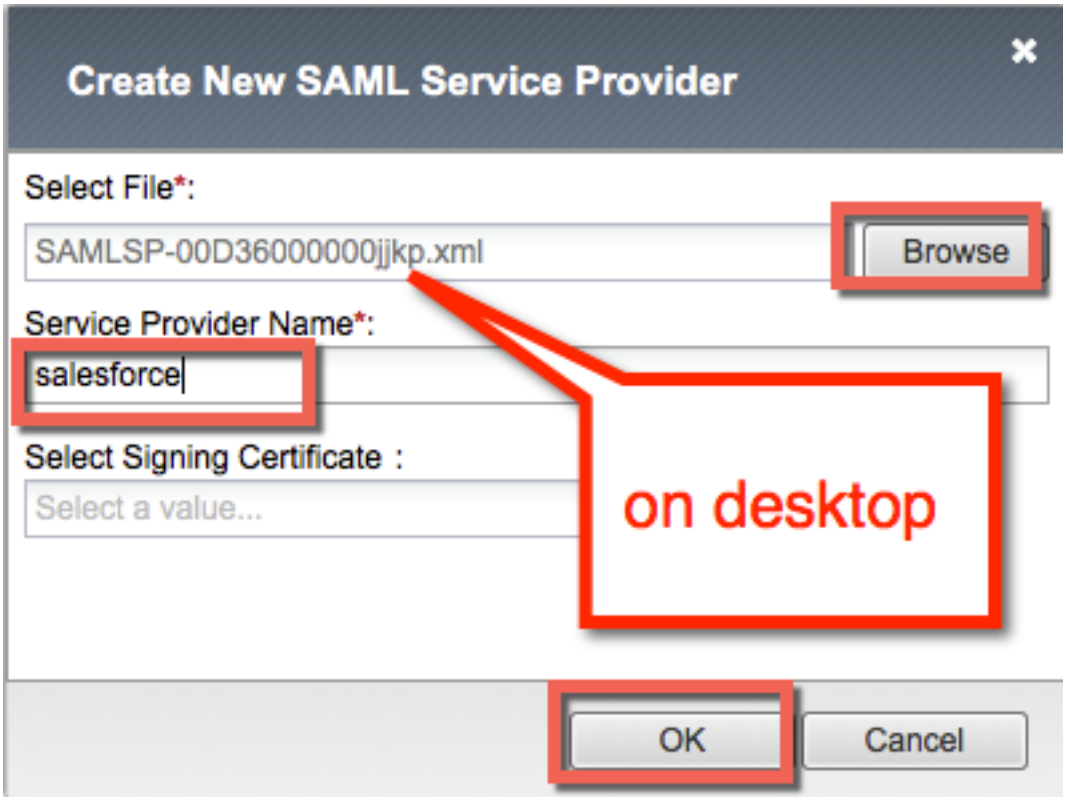
Estimated completion time: 25 minutes

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

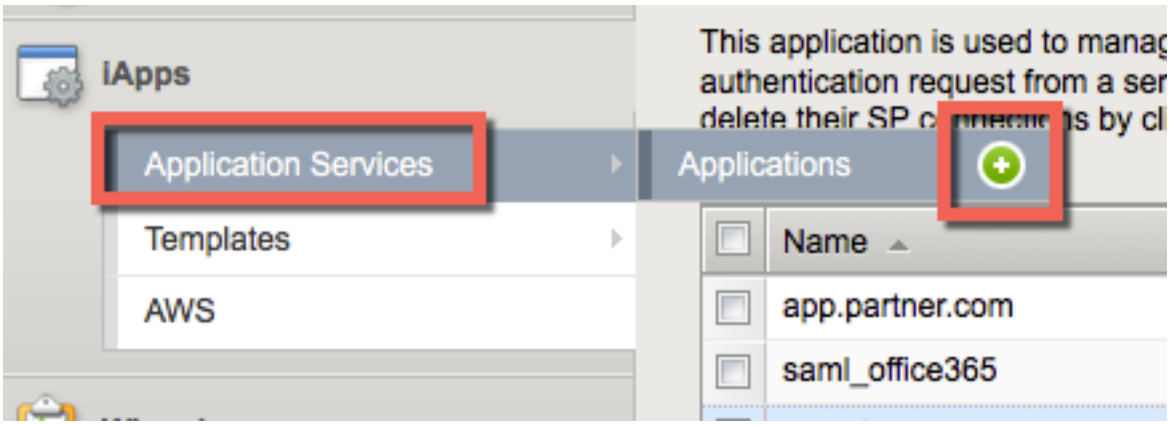


4. In the **Create New SAML Service Provider** dialogue box, click **Browse** and select the `SAMLSP-00D36000000jjkp.xml` file from the Desktop of your jump host
5. In the **Service Provider Name** field, enter: `salesforce`
6. Click **OK** on the dialog box

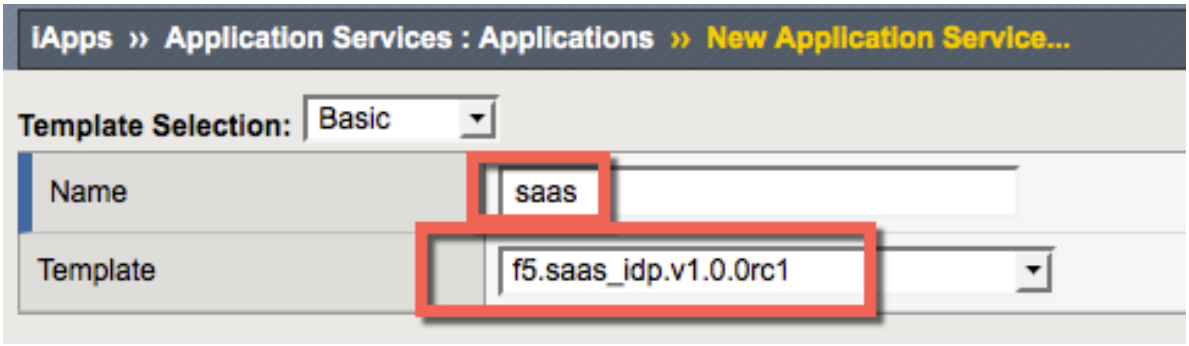


1.5.2 TASK 2 - Deploy the SaaS Federation iApp

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



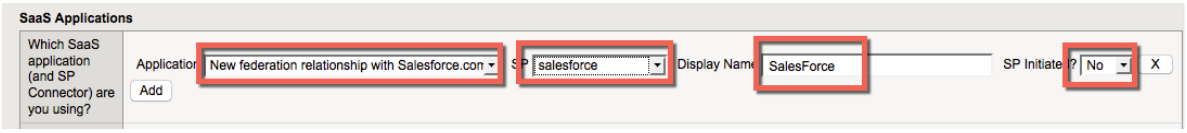
2. In the resulting **New Application Service** window, enter *saas* as the *Name*
3. Select `f5.saas_idp.v1.0.rc1` from the **Template** drop down menu



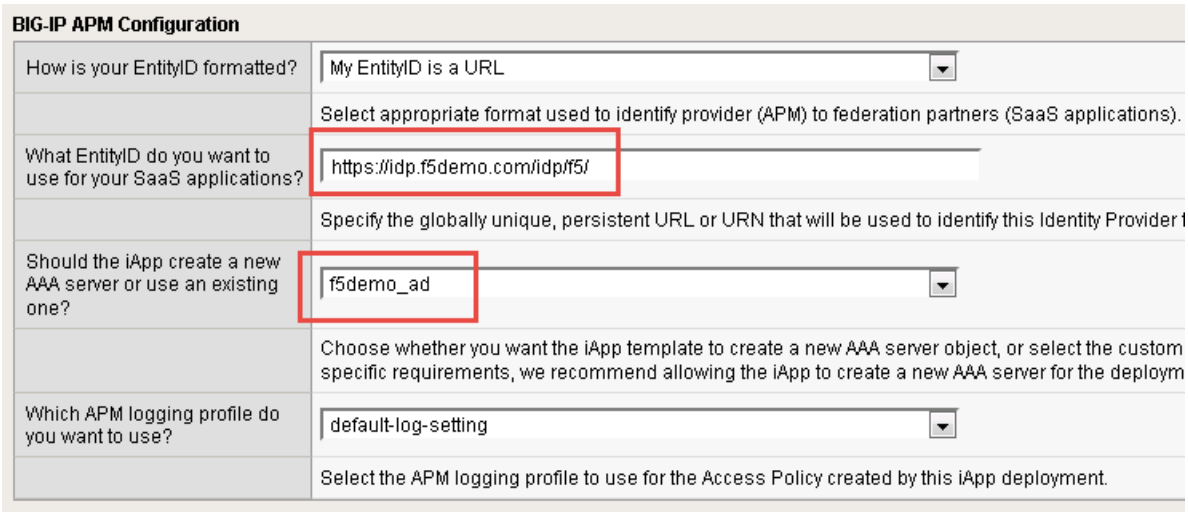
Note: The iApp template has already been downloaded and imported for this lab. You can download the latest iApp templates from https://downloads.f5.com/

4. Configure the iApp template as follows:

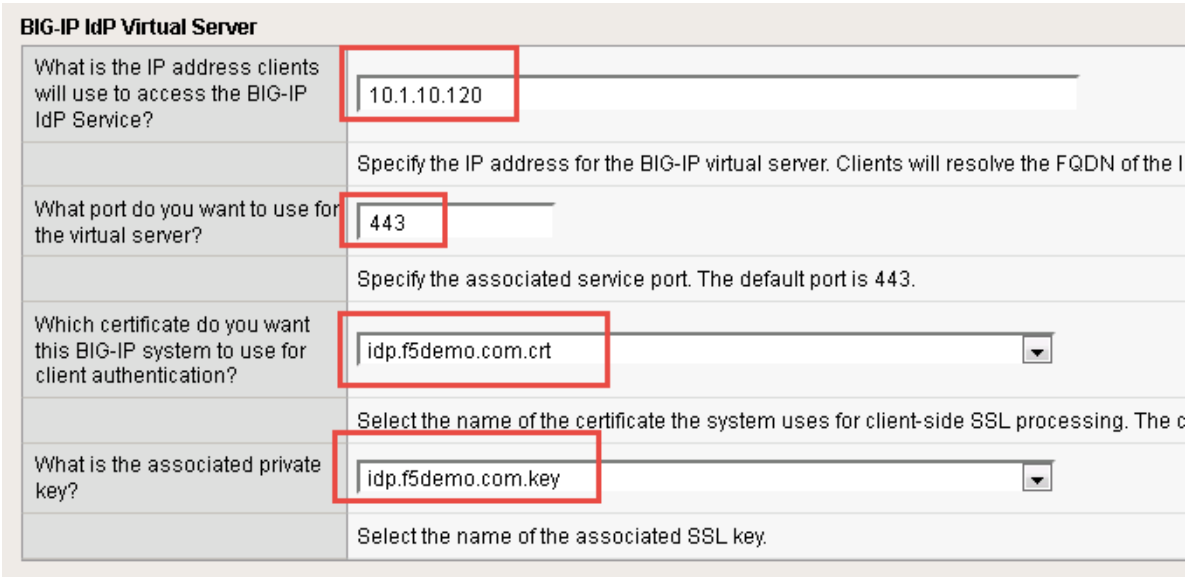
SaaS Applications	
Application:	`New federation relationship with salesforce.com`
SP:	`salesforce`
Display Name:	`SalesForce`
SP Initiated:	`No`



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`

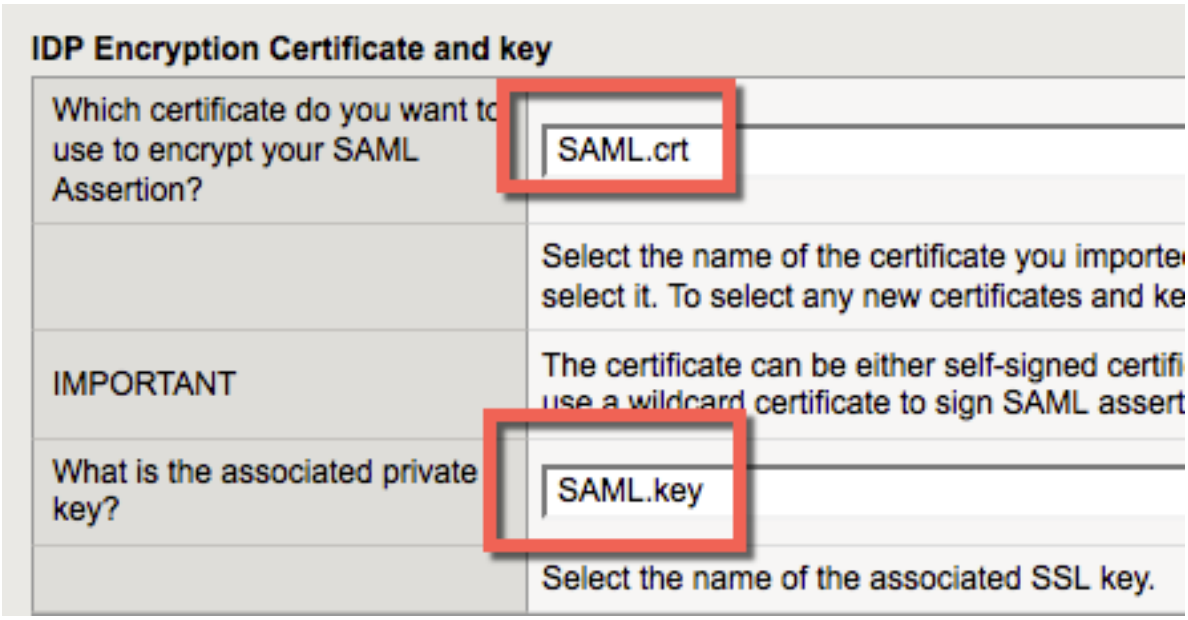


BIG-IP Virtual Server	
What is the IP address clients will use to access the BIG-IP IdP Service?	`10.1.10.120`
What port do you want to use for the virtual server?	`443`
Which certificate do you want this BIG-IP system to use for client authentication?	`idp.f5demo.com.crt`
What is the associated private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

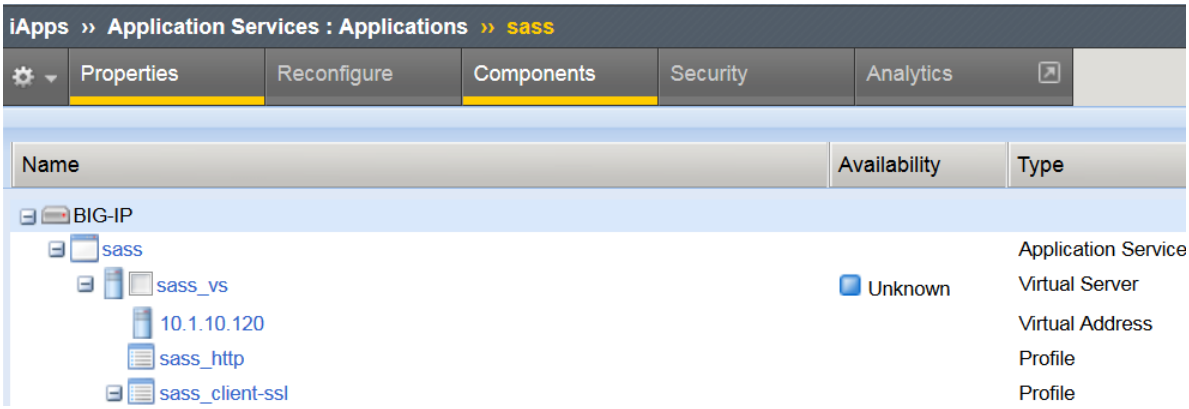


Note: We are deploying the iApp on a different IP so that you can see how everything is built out; however, this IdP will not work, as the `idp.f5demo.com` FQDN resolves to another IP. We are going to use the iApp to create the SAML resource that we will assign to our existing access policy from Lab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

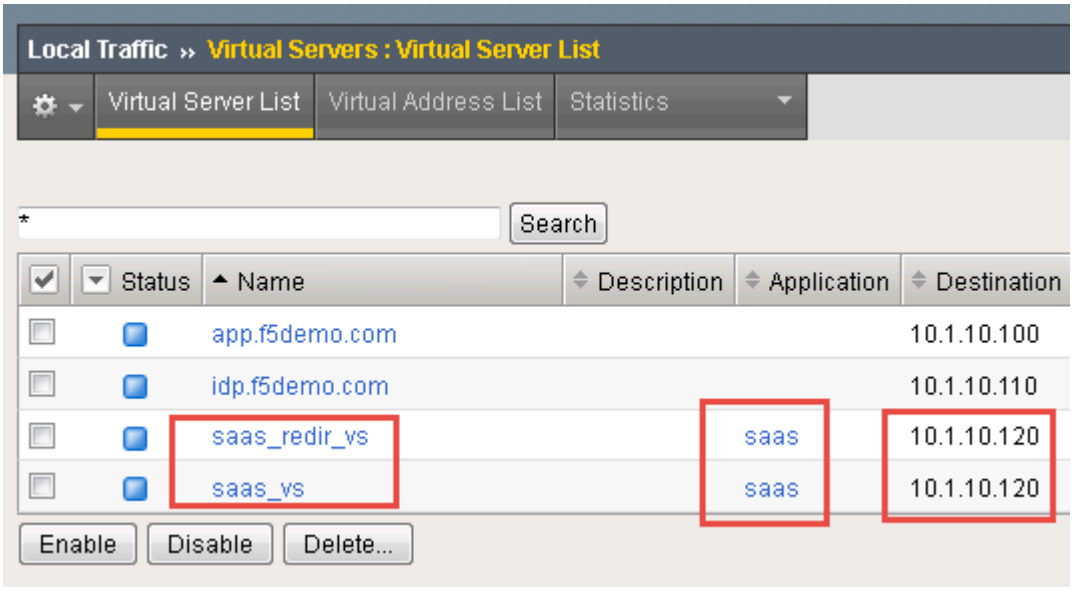
IdP Encryption Certificate and Key	
Which certificate do you want to use to encrypt your SAML Assertion?	`SAML.crt`
What is the associated private key?	`SAML.key`



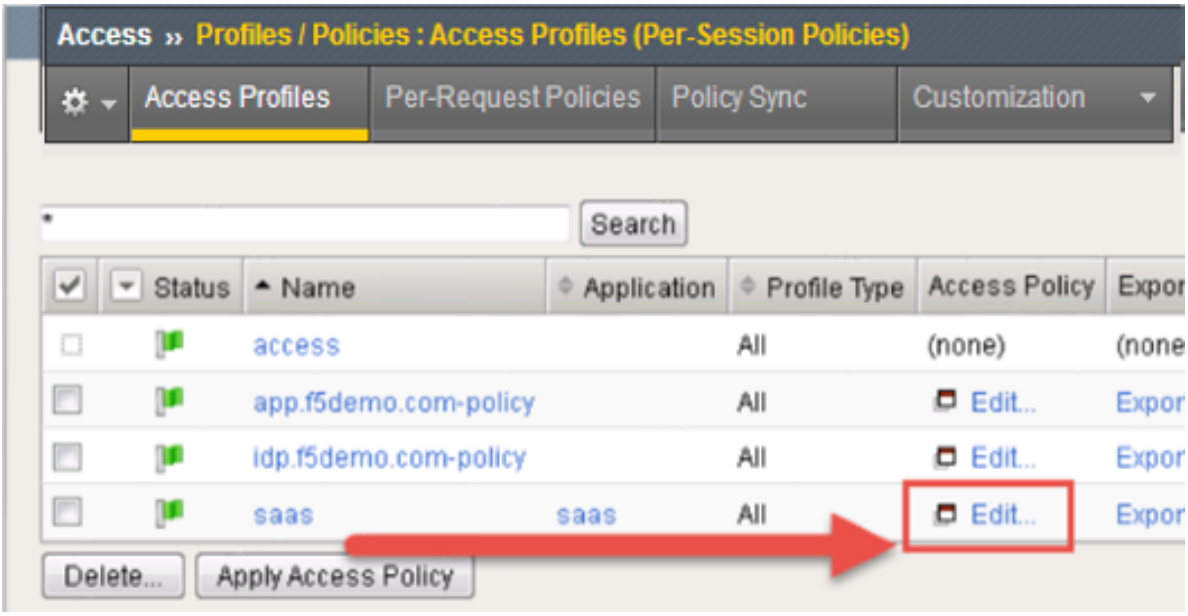
5. Scroll to the bottom of the configuration template and click **Finished**
6. Once deployed, you can review the built out SaaS Federation iApp at **iApps ?> Application Services ?> Applications ?> saas**



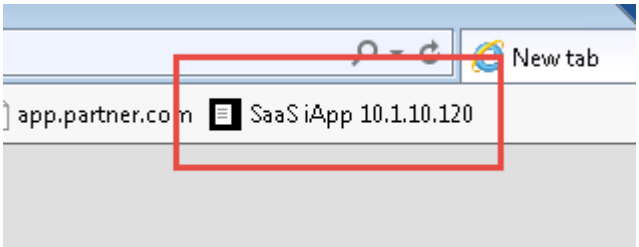
7. Review the new virtual servers created by the iApp at **Local Traffic ?> Virtual Server ?> Virtual Server List**



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

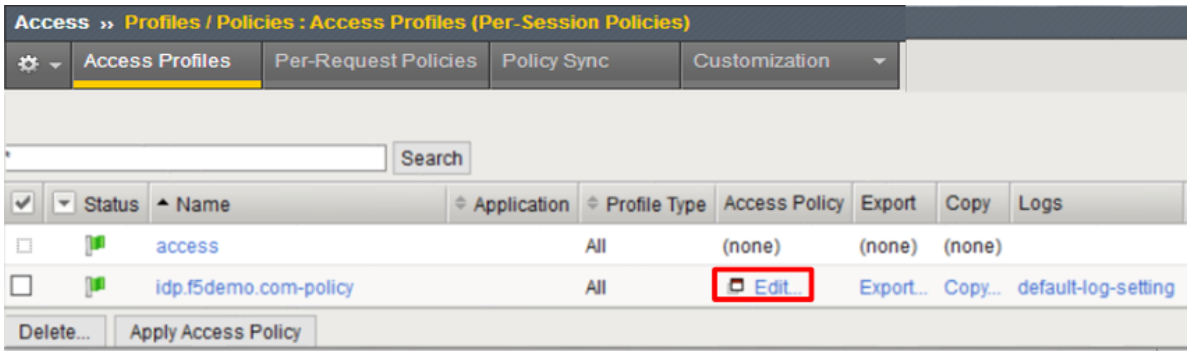
through the warning to see the resulting page.

1.5.3 TASK 3 - Modify the SAML IdP Access Policy

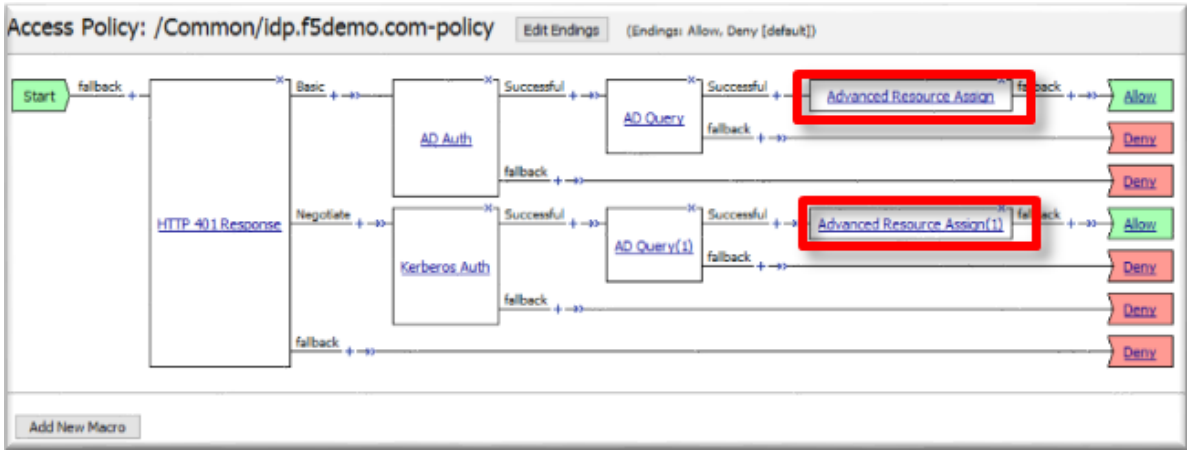
The previous task, Task 2, was to provide you an understanding of how the SaaS Federation iApp can automatically build a configuration for you.

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.

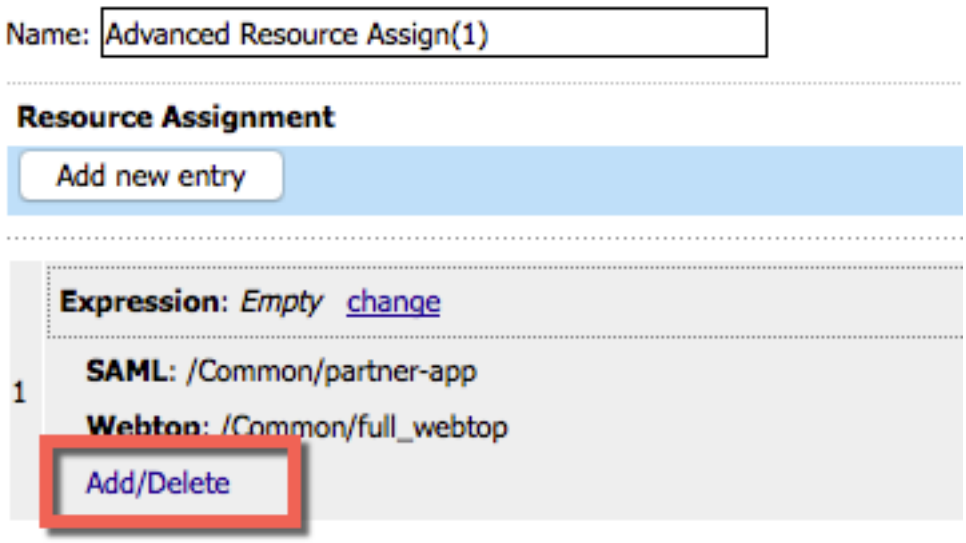
1. Using the same Access Policy from Lab 3, navigate to **Access ?> Profiles/Policies ?> Access Profiles (Per-Session Policies)** and click the **Edit** link next to the previously created `idp.f5demo.com-policy`



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

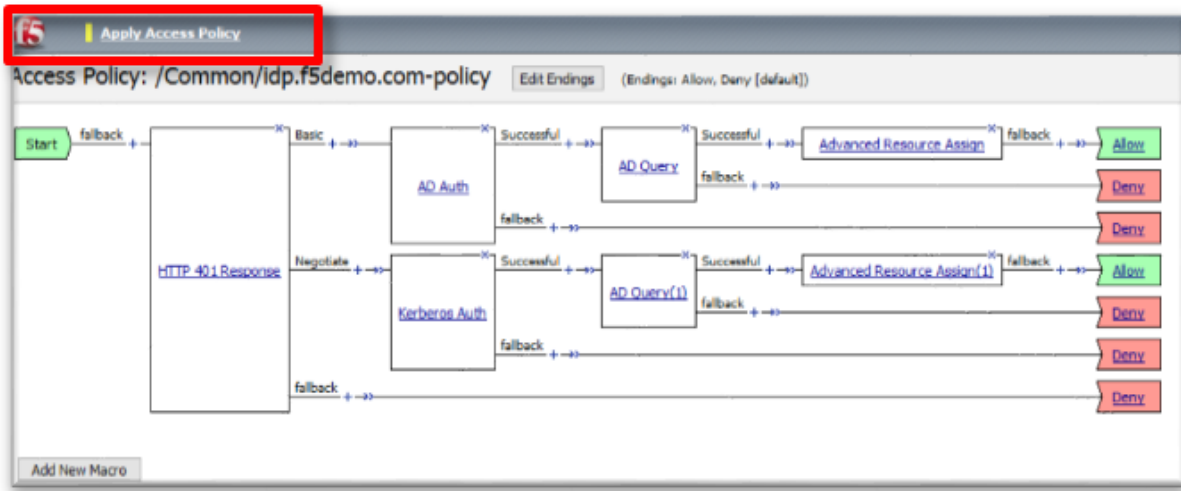


3. Click the **Add/Delete** link on the Resource Assignment item



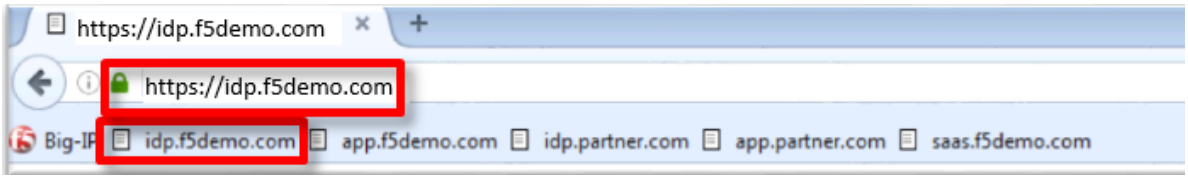
4. Click the **SAML** tab, and select the checkbox next to `/Common/saas.app/saas_SalesForce_saml_resource_sso`

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

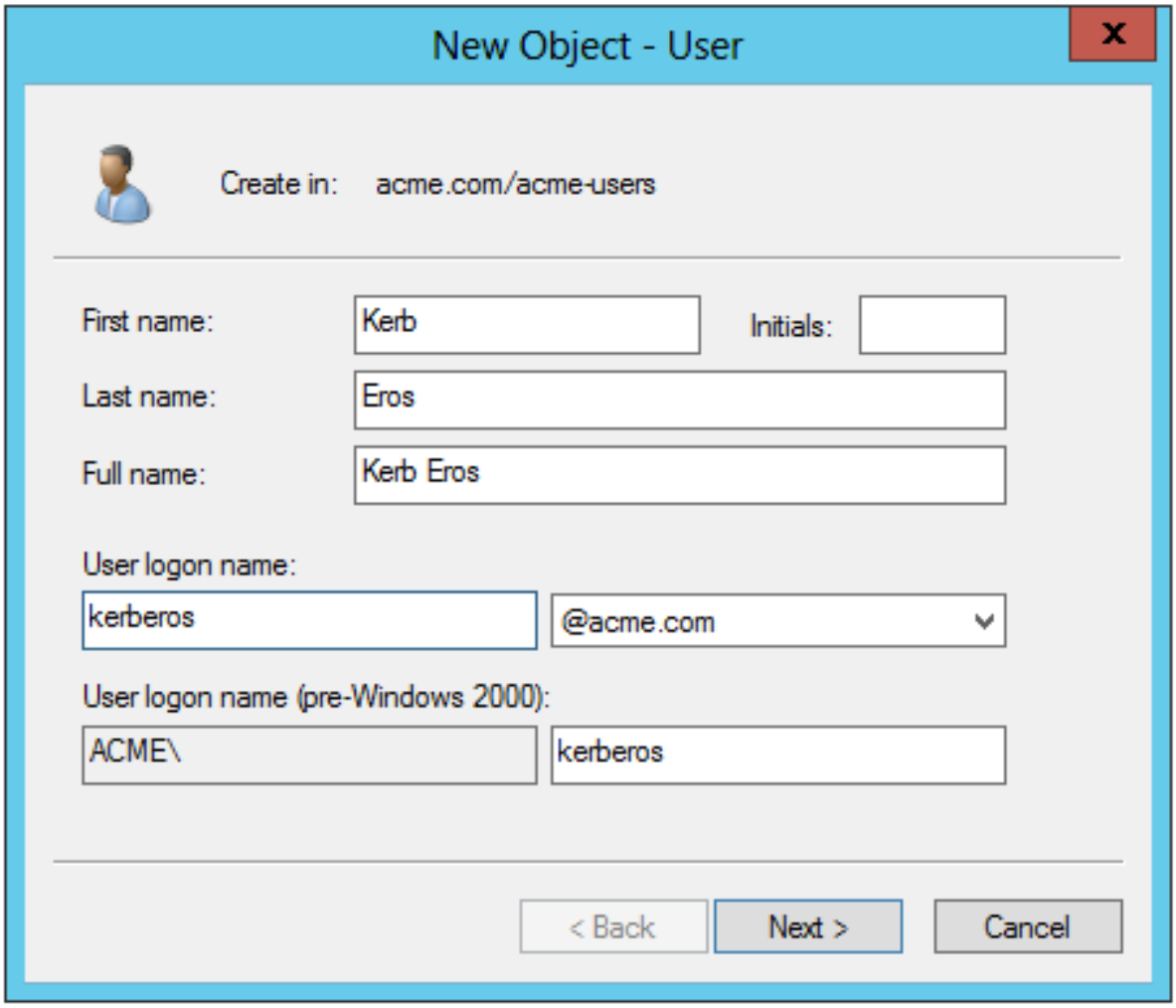
- **F5 Deployment Guide for Microsoft SharePoint 2010/2013:** https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2010-and-2013-new-supported-iapp-big-ip-v114-ltm-apm-asm-aam
- **F5 Deployment Guide for Microsoft SharePoint 2016:** https://f5.com/solutions/deployment-guides/microsoft-sharepoint-2016-big-ip-v114-v12-ltm-apm-asm-afm-aam
- **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

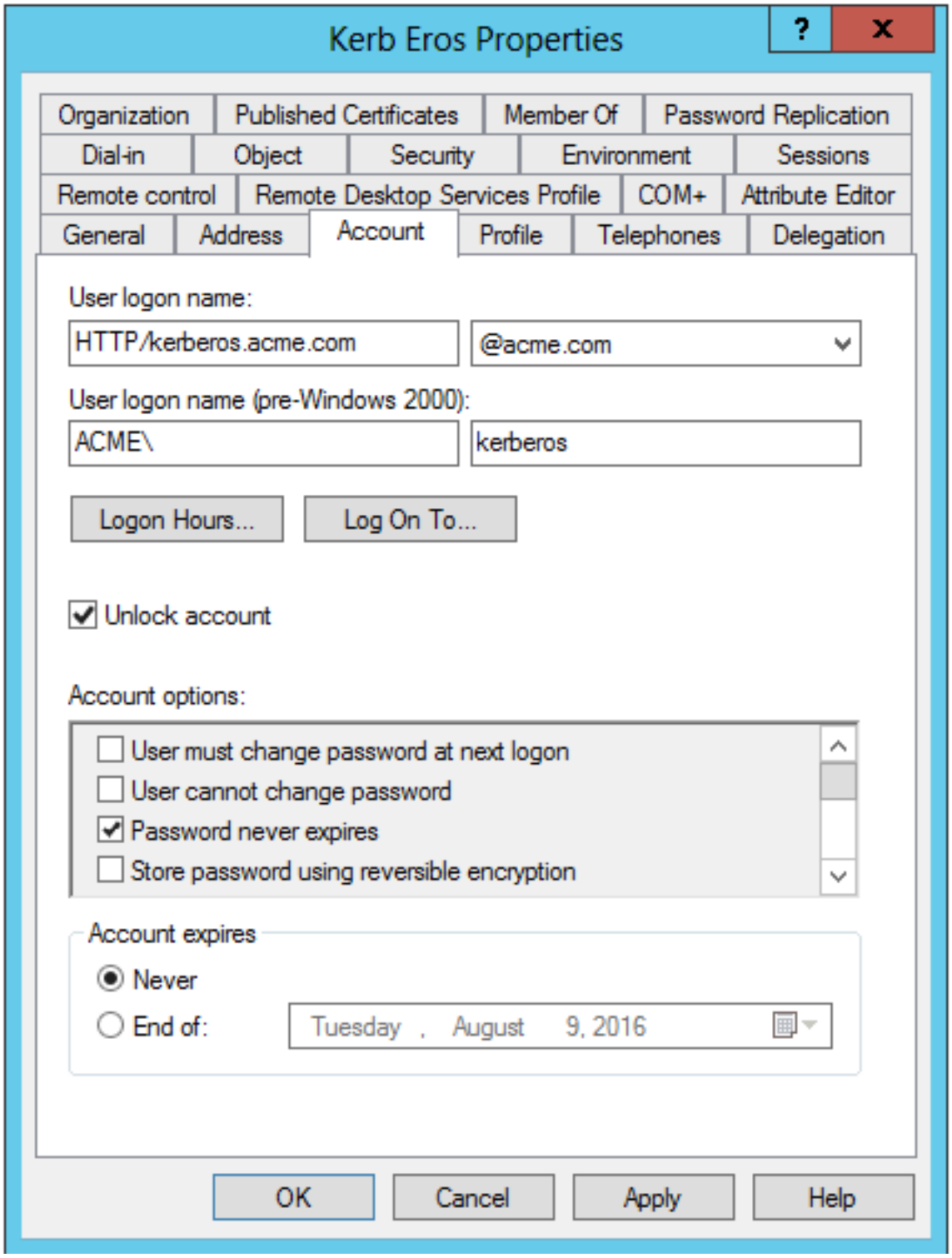


3. From the Windows command line, run the KTPASS command to generate a keytab file for the previously created user object

```
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`

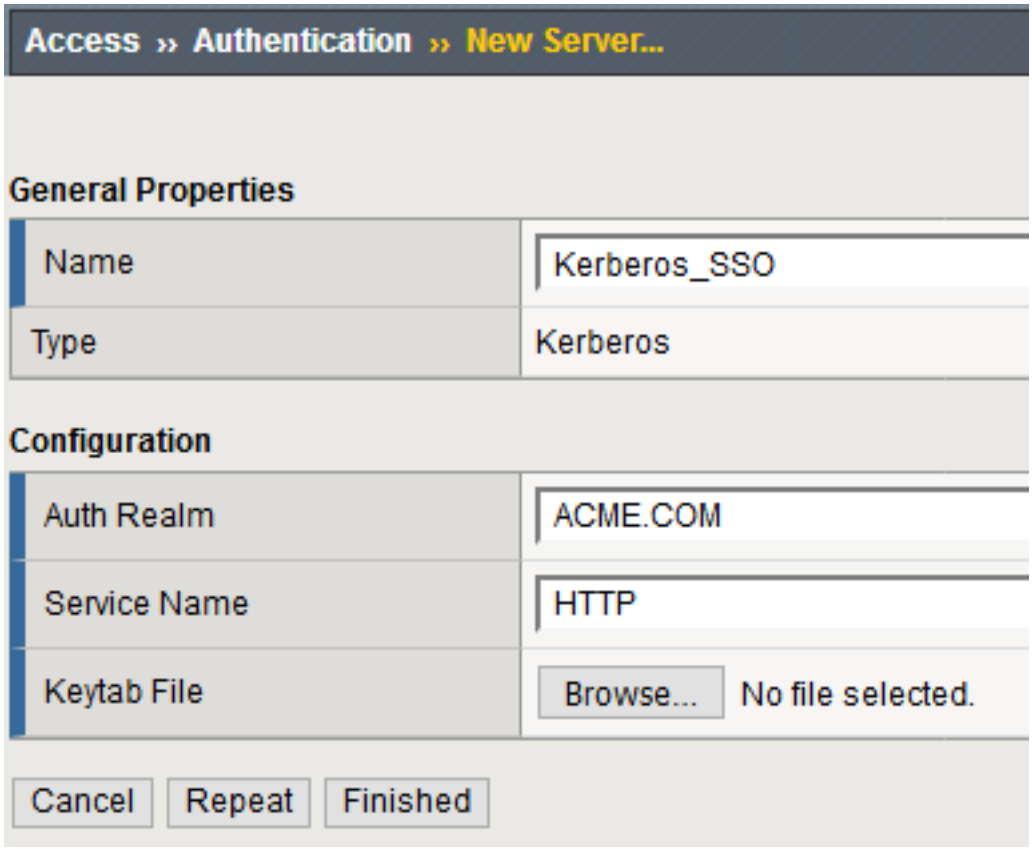
4. Review the changes to the AD User object



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



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

2

Class 2: OAuth Federation with F5

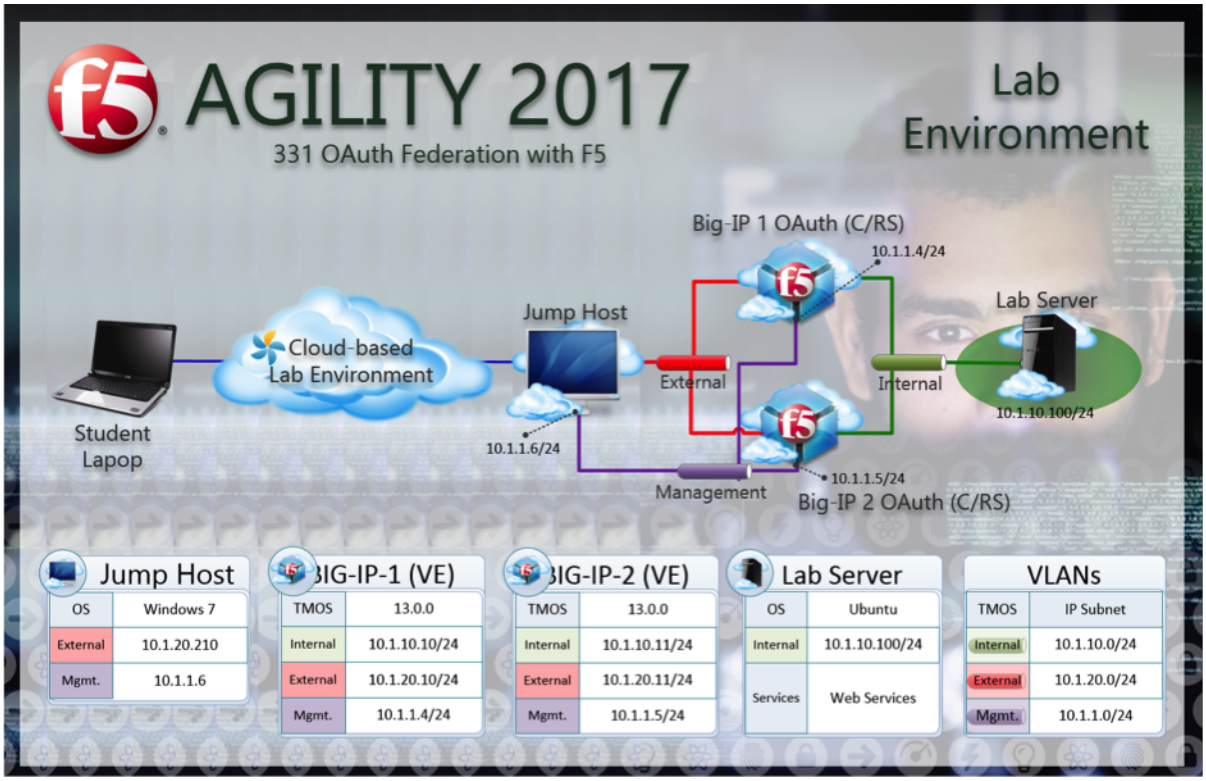
2.1 Lab Environment

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

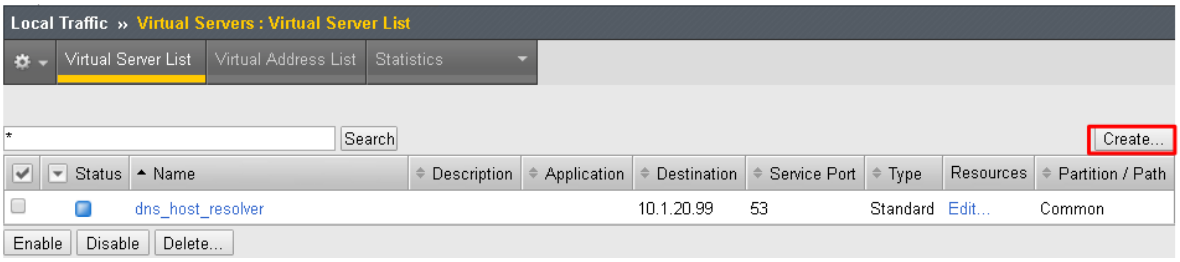
Note: The entire module covering Social Login is performed on BIG-IP 1 (OAuth C/RS)

2.2.1 Purpose

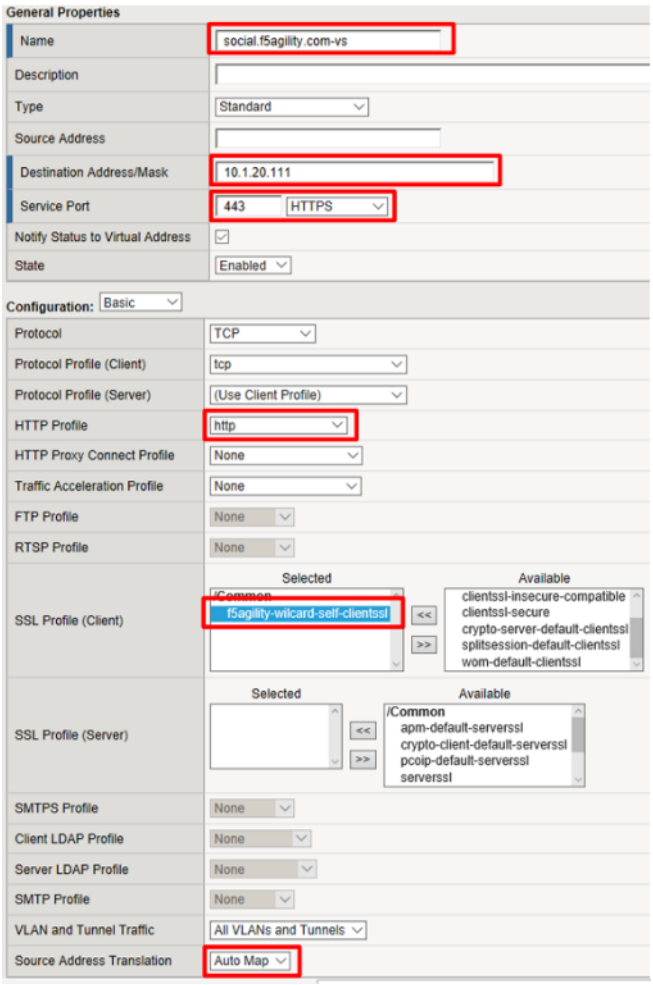
This module will teach you how to configure a Big-IP as a client and resource server enabling you to integrate with social login providers like Facebook, Google, and LinkedIn to provide access to a web application. You will inject the identity provided by the social network into a header that the backend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

2.2.2 Task 1: Setup Virtual Server

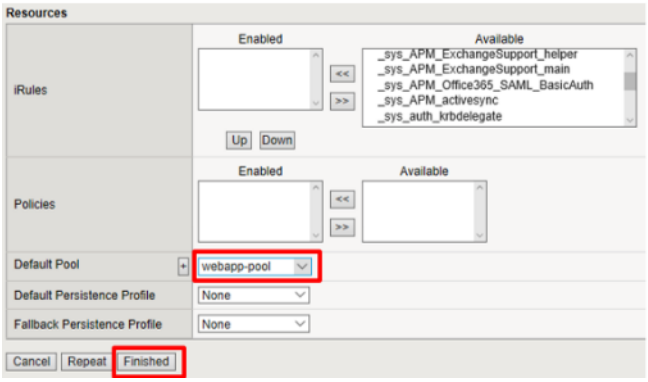
1. Go to **Local Traffic -> Virtual Servers -> Create**



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`

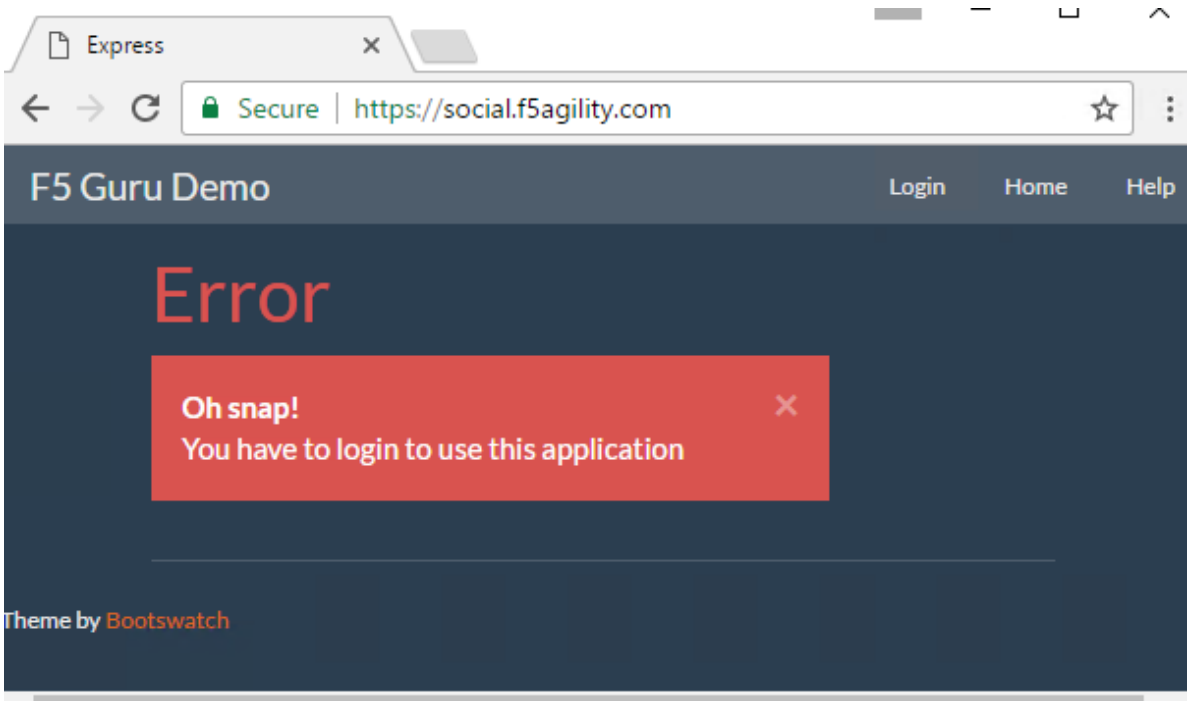


3. Select webapp-pool from the Default Pool drop down and then click **Finished**



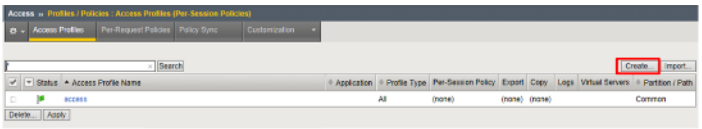
4. Test access to `https://social.f5agility.com` from the jump host's browser.

   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.



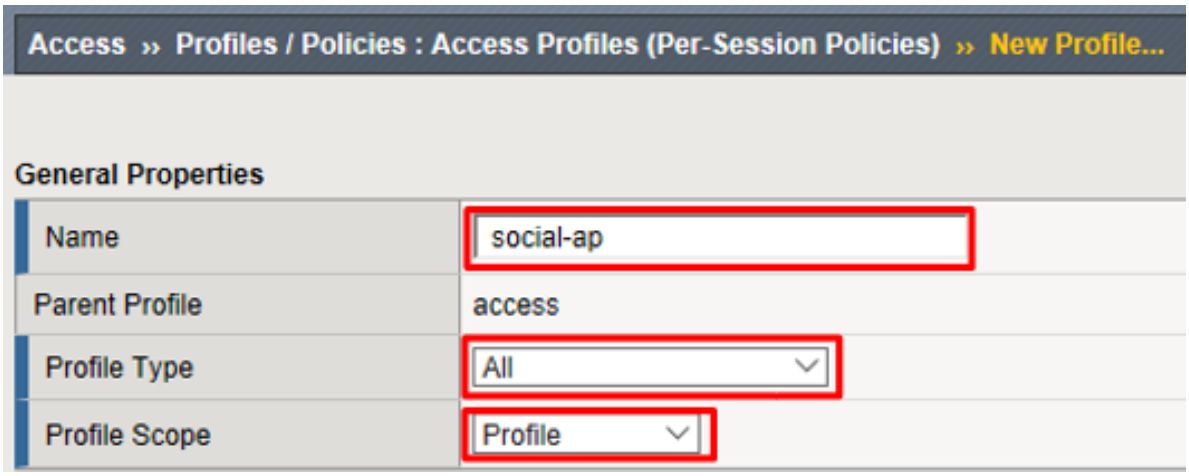
2.2.3 Task 2: Setup APM Profile

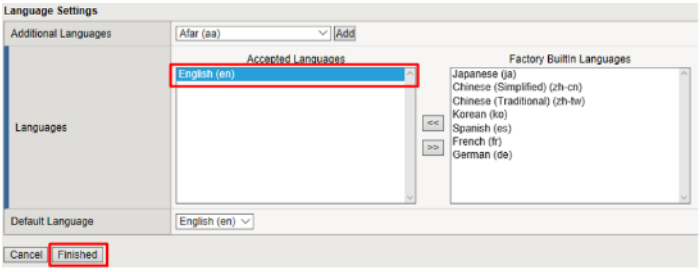
1. Go to **Access -> Profiles / Policies -> Access Profiles (Per Session Policies) -> Create**



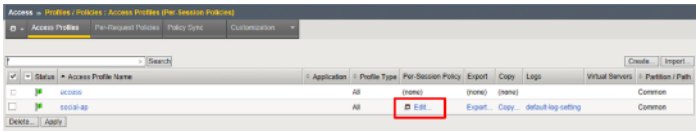
2. Enter the following values (leave others default) then click **Finished**
   - **Name:** `social-ap`
   - **Profile Type:** `All`
   - **Profile Scope:** `Profile`

- **Languages:** English

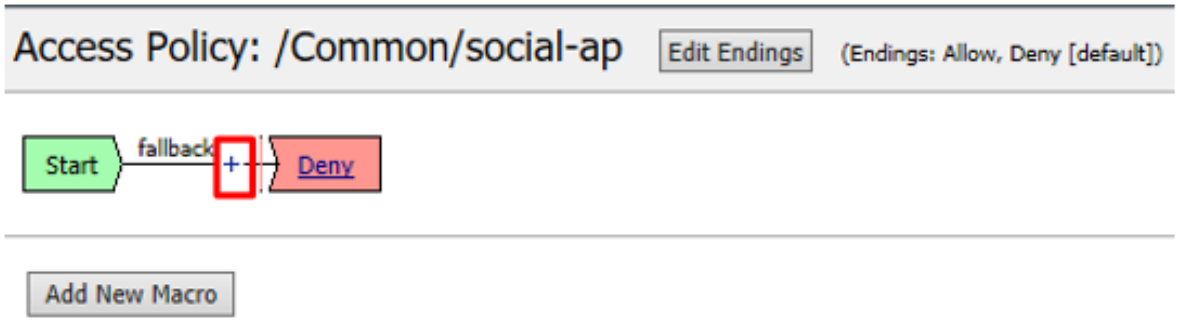


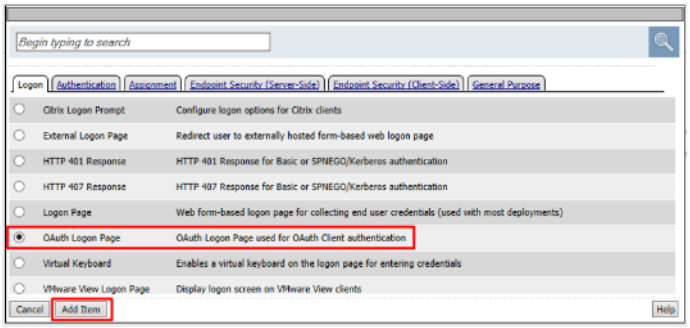


3. Click **Edit** for social-ap, a new browser tab will open

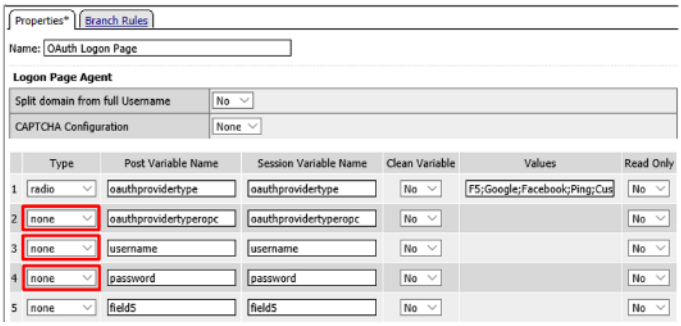


4. Click the **+** between **Start** and **Deny**, select **OAuth Logon Page** from the **Logon** tab, click **Add Item**

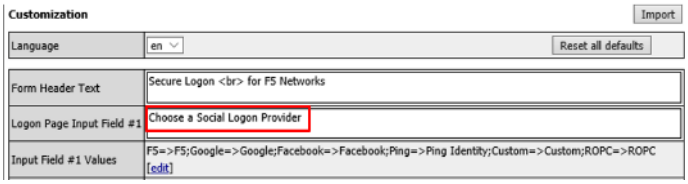




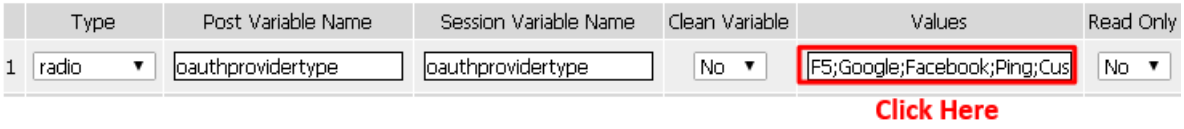
5. Set the **Type** on **Lines 2, 3, and 4** to none



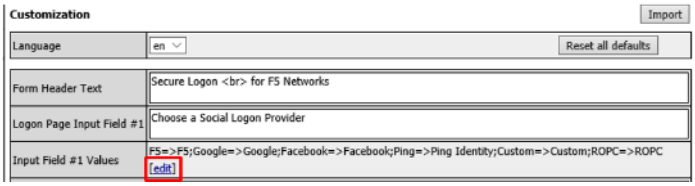
6. Change the **Logon Page, Input Field #1** to “Choose a Social Logon Provider”



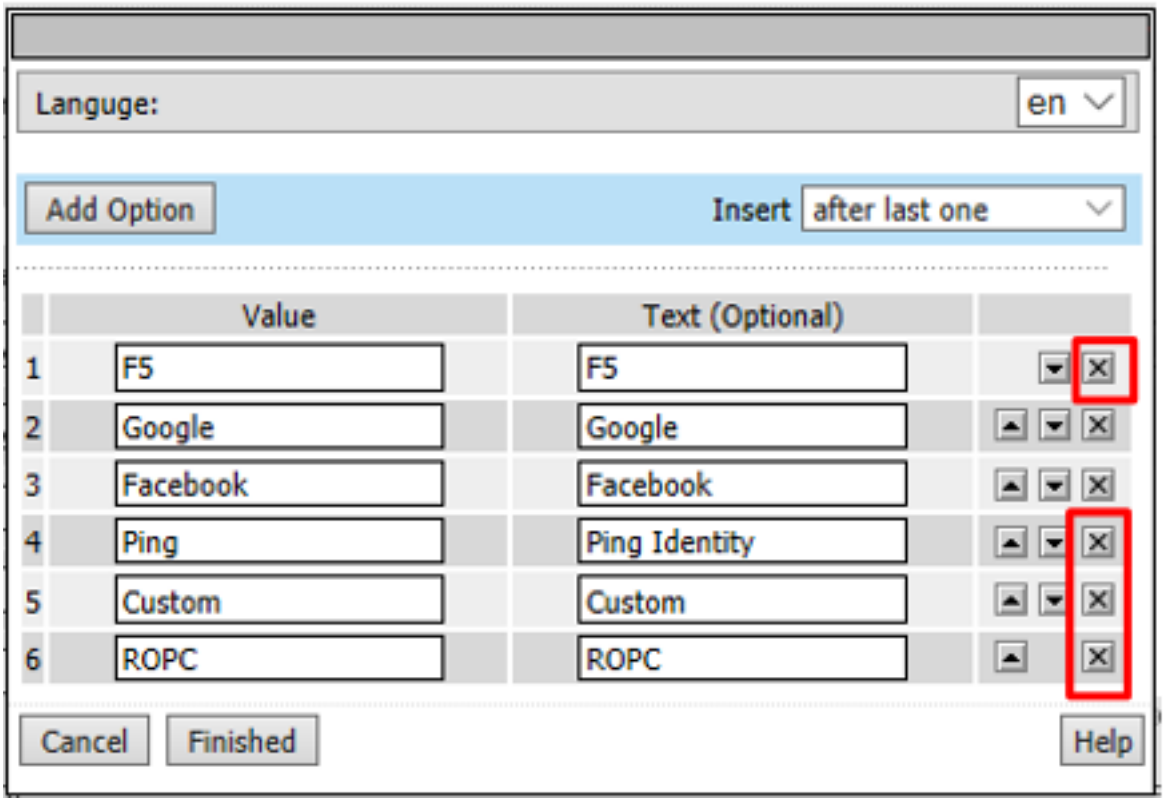
7. Click the **Values** column for **Line 1**, a new window will open.



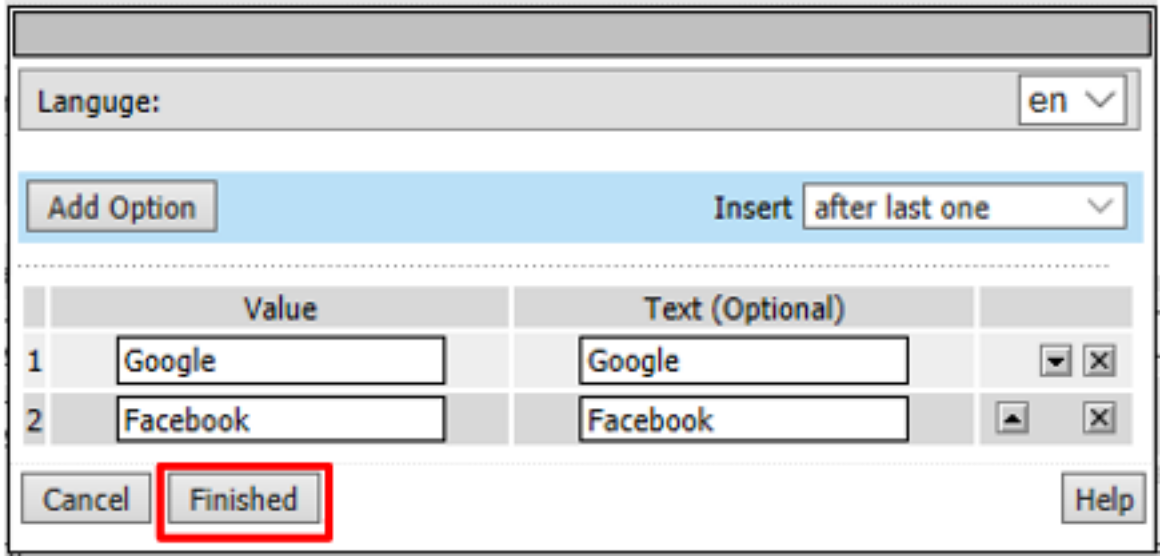
Alternatively, you may click **[Edit]** on the **Input Field #1 Values** line. Either item will bring you to the next menu.

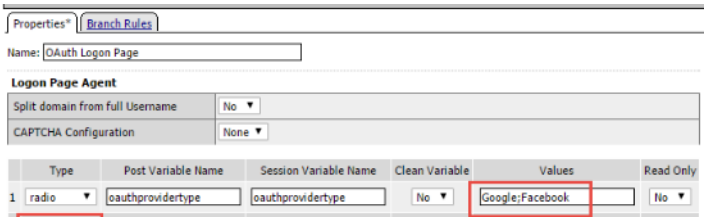


8. Click the **X** to remove **F5, Ping, Custom, and ROPC**



9. Click **Finished**

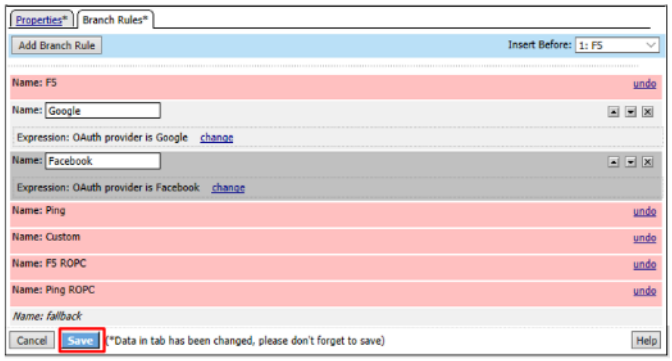




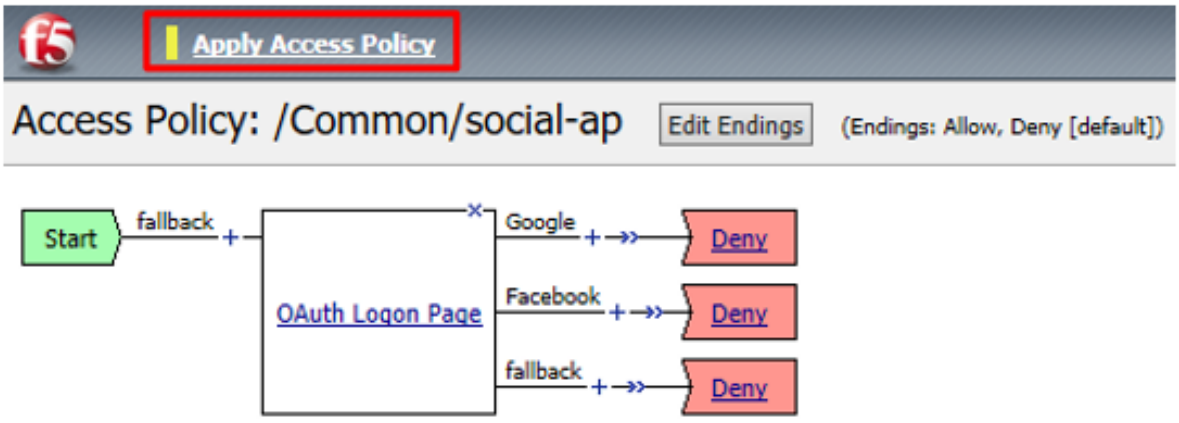
Note: The resulting screen is shown

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

11. Click **Save**

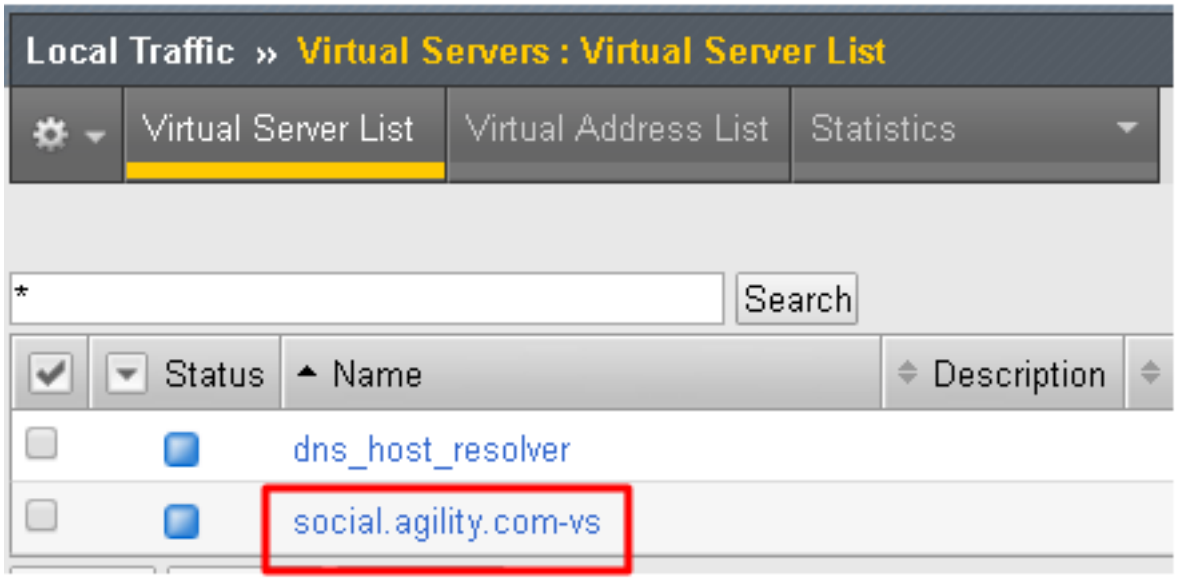


12. Click **Apply Access Policy** in the top left and then close the browser tab

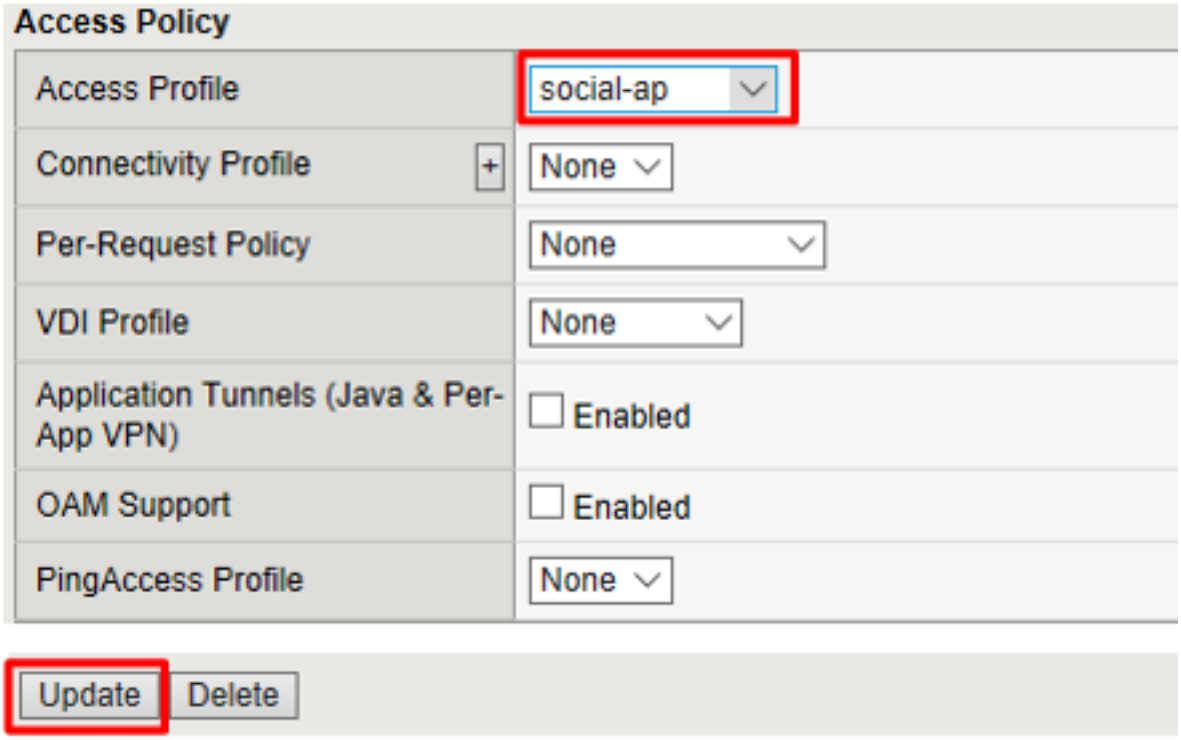


2.2.4 Task 3: Add the Access Policy to the Virtual Server

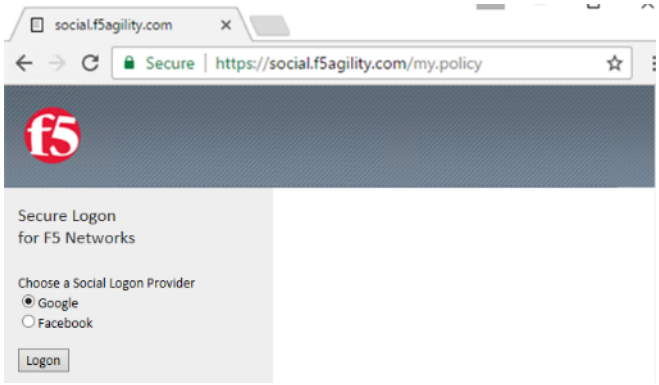
1. Go to **Local Traffic -> Virtual Servers -> social.f5agility.com-vs**



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



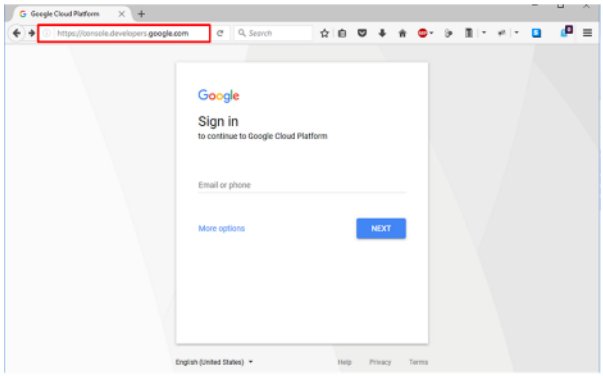
3. Test access to https://social.f5agility.com from the jump host again, you should now see a logon page requiring you to select your authentication provider. Any attempt to authenticate will fail since we have only deny endings.



2.2.5 Task 4: Google (Built-In Provider)

Setup a Google Project

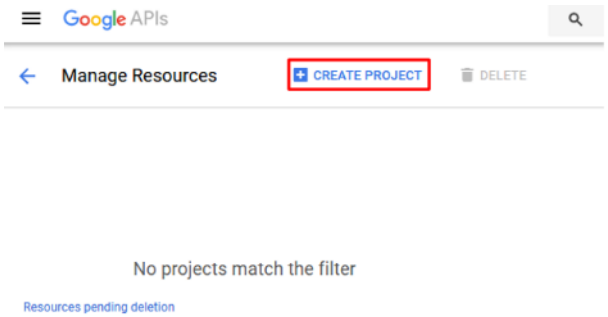
1. Login at https://console.developers.google.com

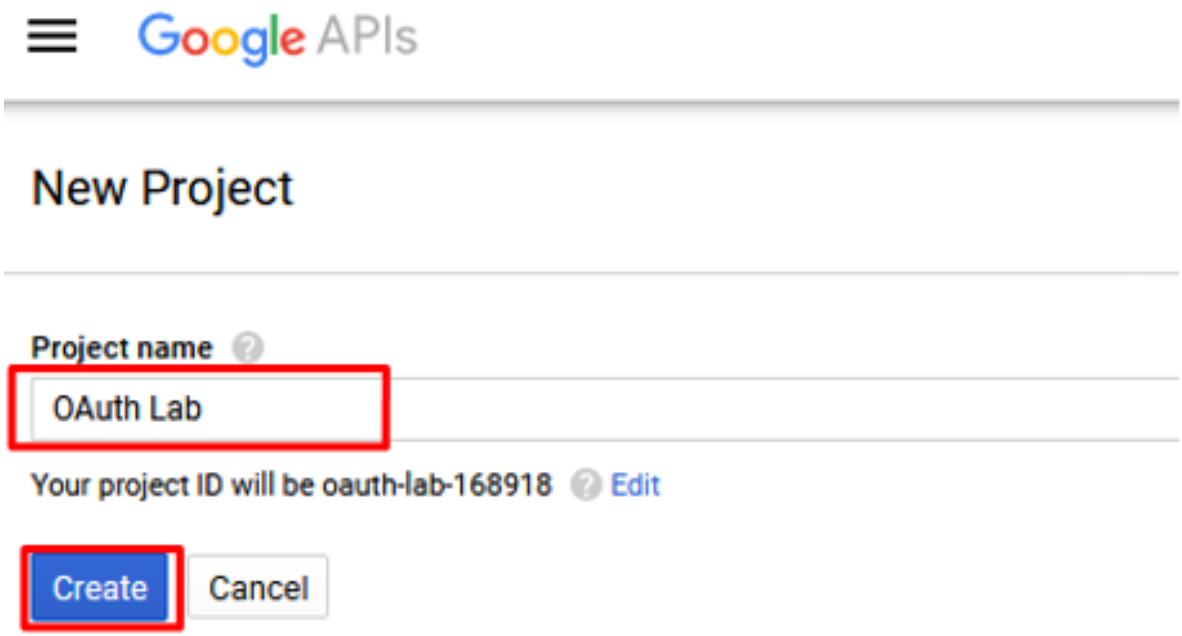


Note: This portion of the exercise requires a Google Account. You may use an existing one or create one for the purposes of this lab

---

2. Click **Create Project** and give it a name like “OAuth Lab” and click **Create**

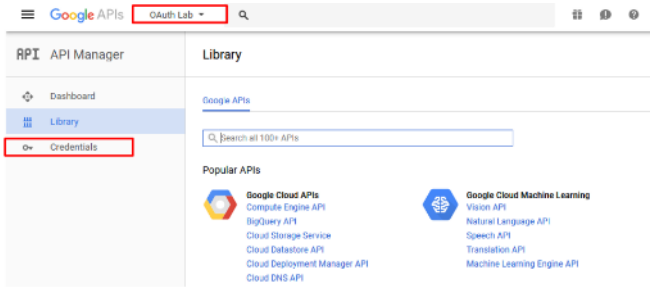




Note: You may have existing projects so the menus may be slightly different.

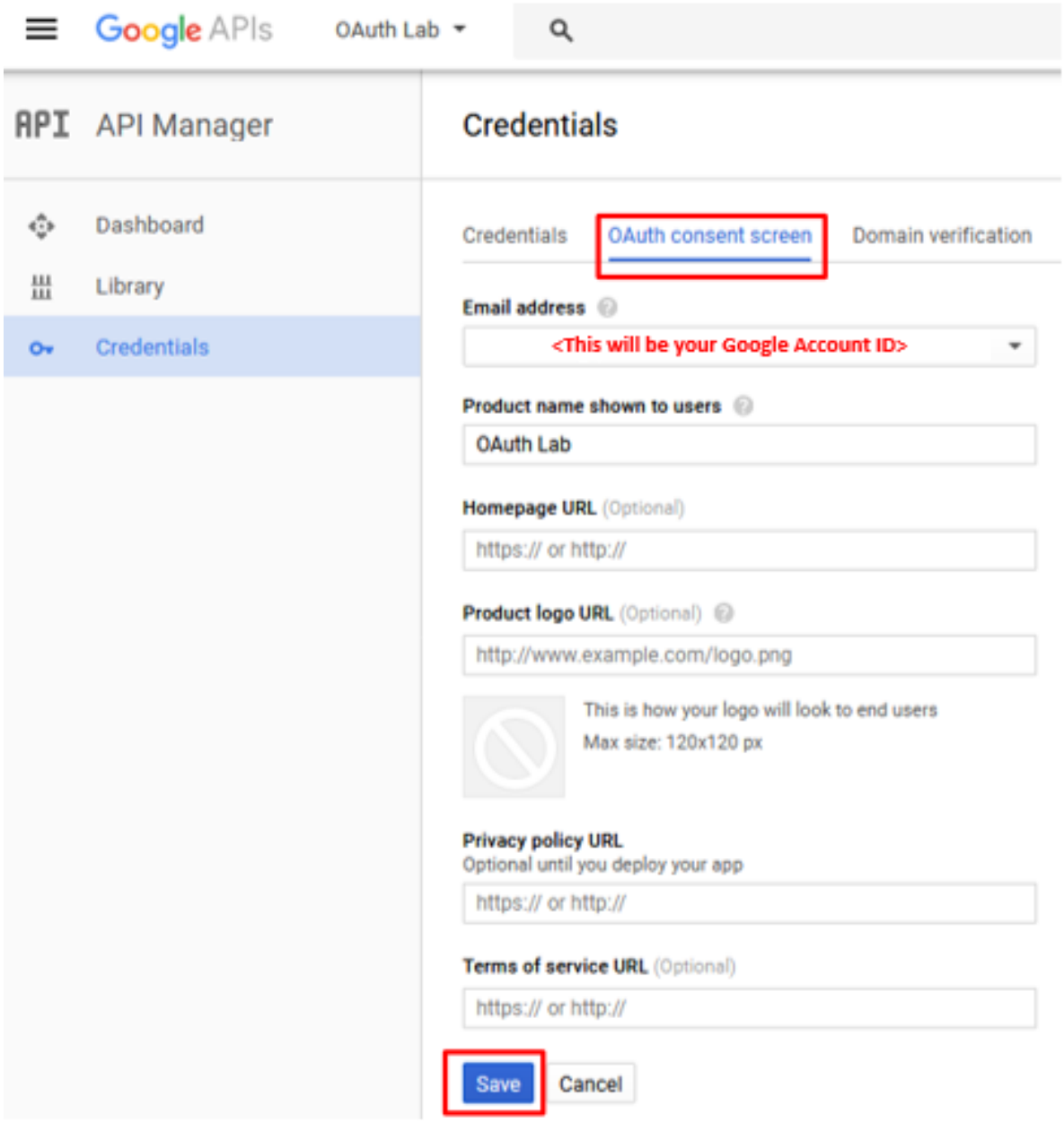
Note: You may have to click on Google+ API under Social APIs

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

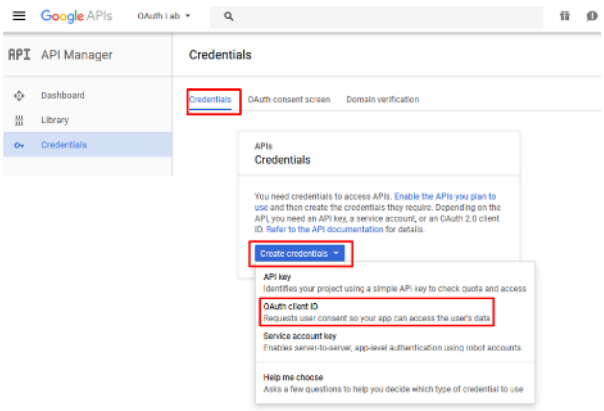


Note: You may have navigate to your OAuth Lab project depending on your browser or prior work in Google Developer

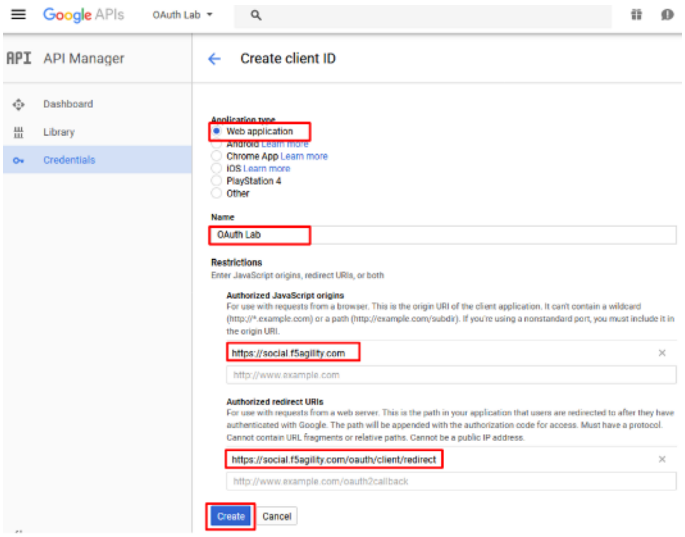
4. Click **OAuth Consent Screen** tab, fill out the product name with “OAuth Lab”, then click save



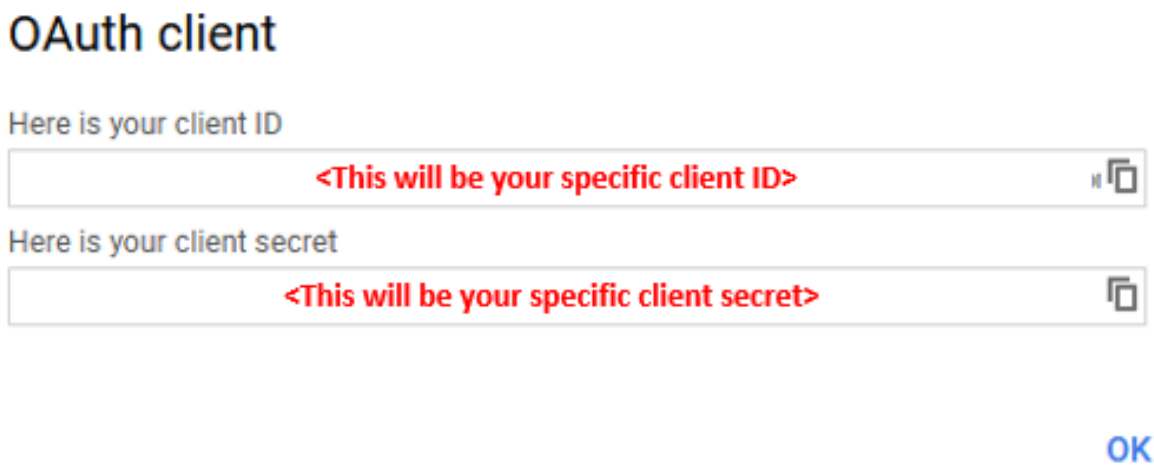
5. Go to the **Credentials** tab (if you are not taken there), click **Create Credentials** and select **OAuth Client ID**



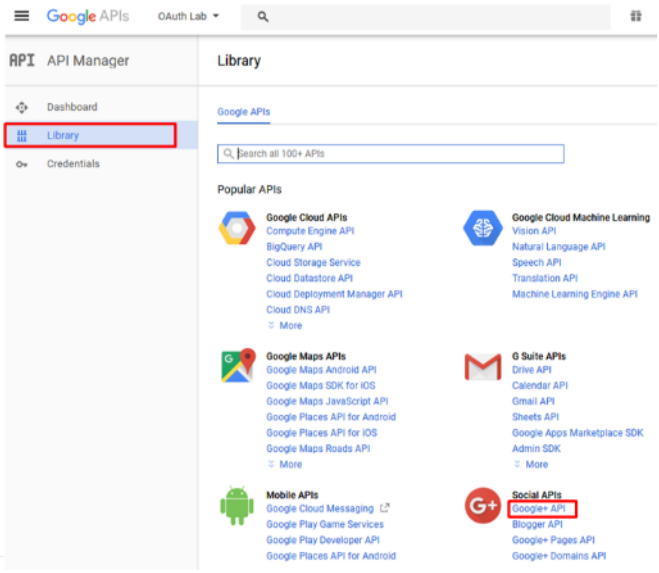
6. Under the **Create Client ID** screen, select and enter the following values and click **Create**
   - **Application Type:** `Web Application`
   - **Name:** `OAuth Lab`
   - **Authorized Javascript Origins:** `https://social.f5agility.com`
   - **Authorized Redirect URIs:** `https://social.f5agility.com/oauth/client/redirect`



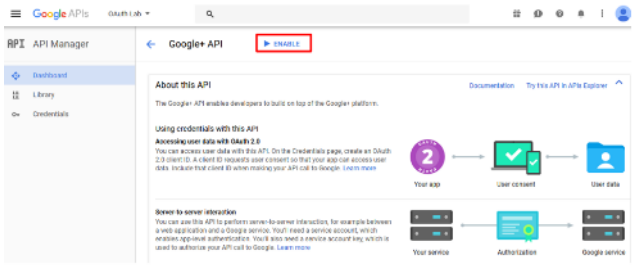
7. Copy the **Client ID** and **Client Secret** to notepad, or you can get it by clicking on the **OAuth Lab Credentials** section later if needed. You will need these when you setup Access Policy Manager (APM).

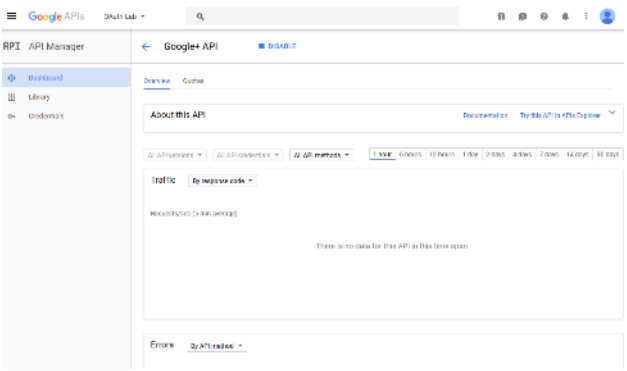


8. Click **Library** in the left-hand navigation section, then select **Google+ API** under **Social APIs** or search for it

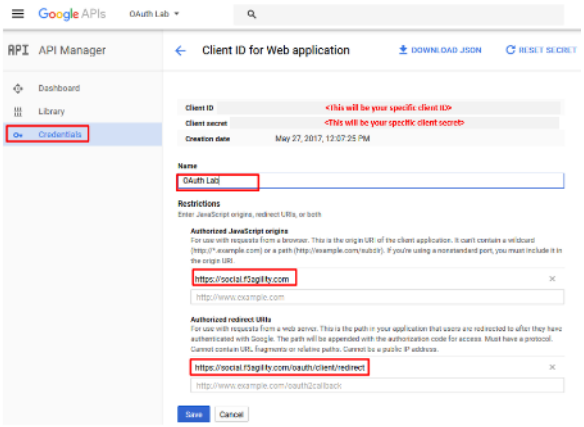


9. Click **Enable** and wait for it to complete, you will now be able to view reporting on usage here



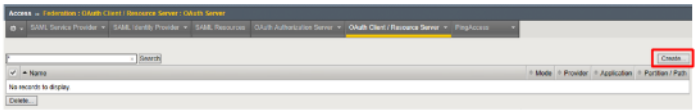


10. For Reference: This is a screenshot of the completed Google project:



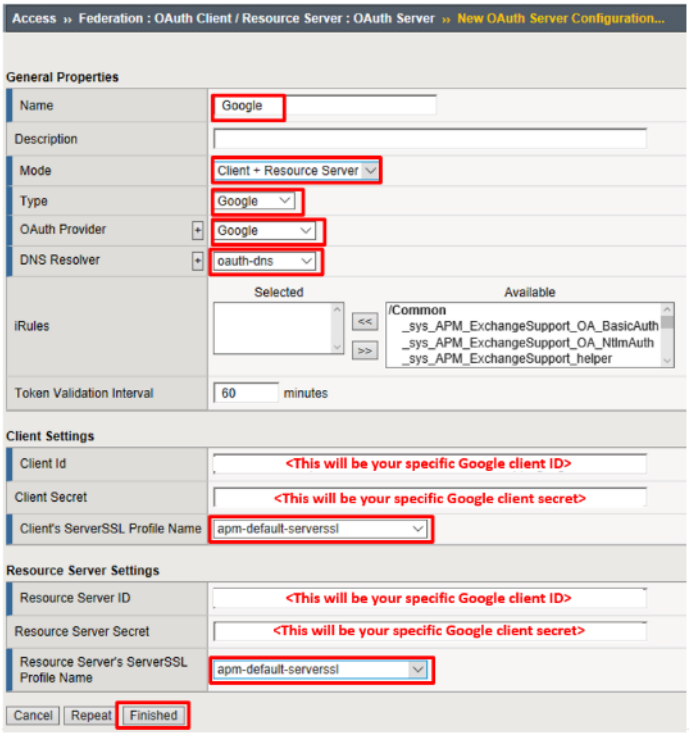
Configure Access Policy Manager (APM) to authenticate with Google

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

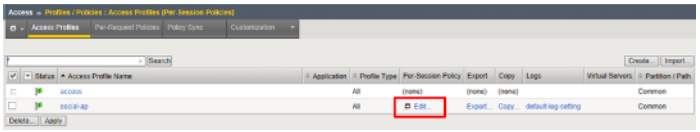


2. Enter the values as shown below for the **OAuth Server** and click **Finished**
    - **Name:** Google
    - **Mode:** `Client + Resource Server`
    - **Type:** `Google`
    - **OAuth Provider:** `Google`
    - **DNS Resolver:** `oauth-dns *(configured for you)*`
    - **Client ID:** `<Client ID 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>`

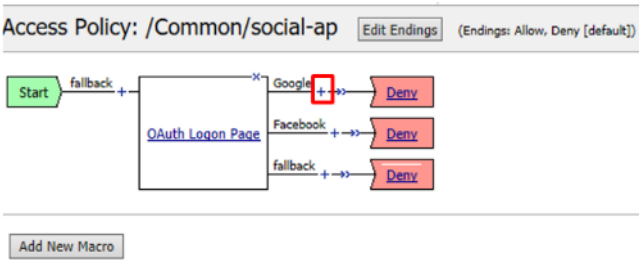
- **Resource Server's ServerSSL Profile Name:** `apm-default-serverssl`



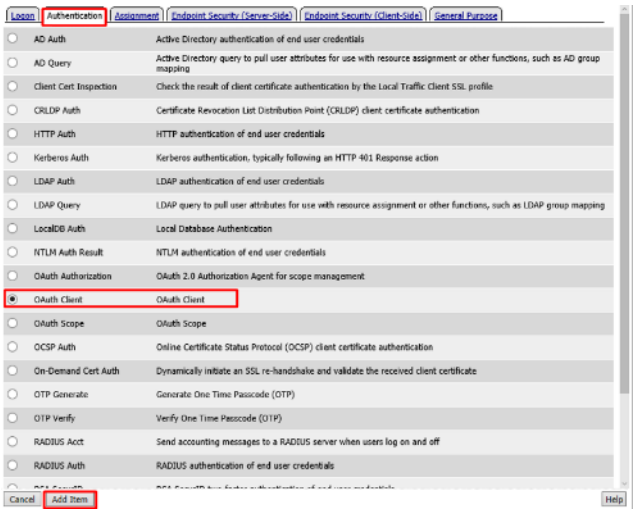
3. Configure the VPE for Google: Go to **Access -> Profiles / Policies -> Access Profiles (Per Session Policies)** and click **Edit** on `social-ap`, a new browser tab will open



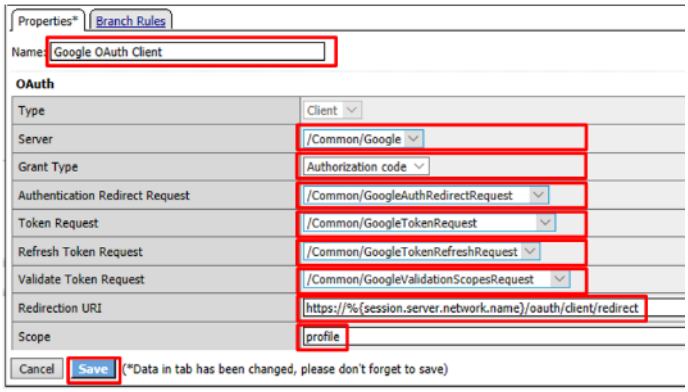
4. Click the + on the **Google** provider's branch after the **OAuth Logon Page**



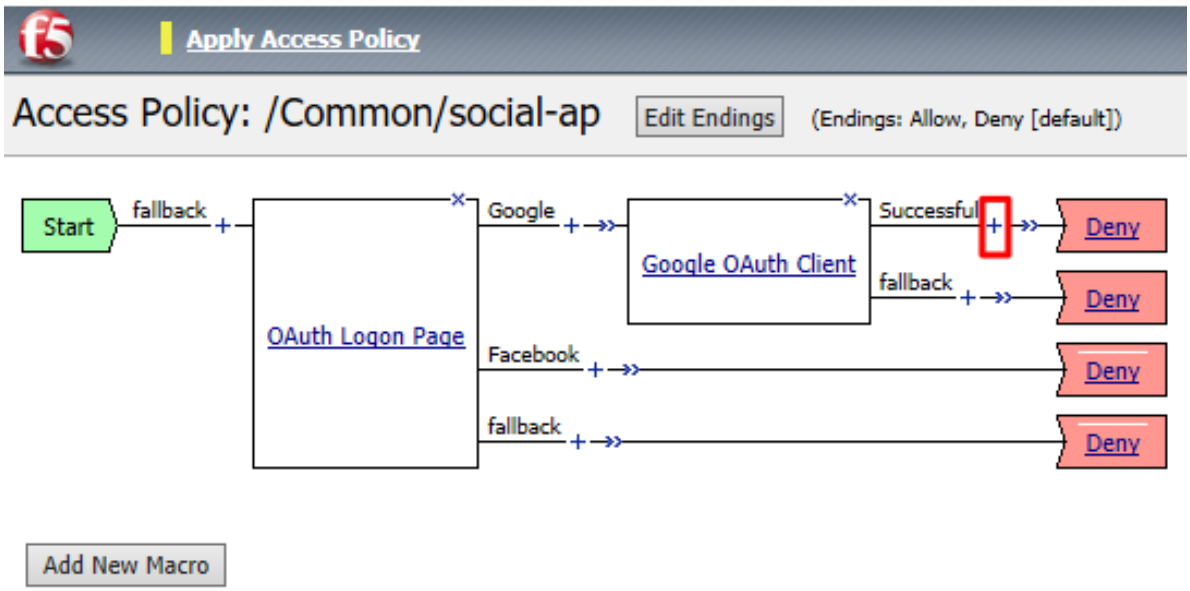
5. Select **OAuth Client** from the **Authentication** tab and click **Add Item**



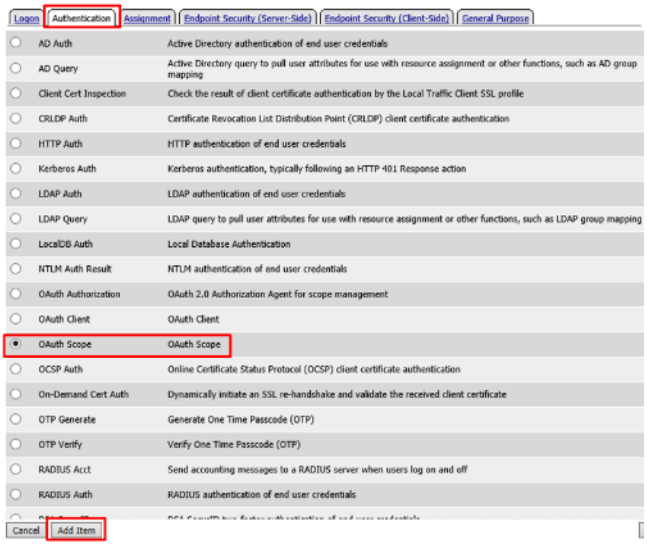
6. Enter the following in the **OAuth Client** input screen and click **Save**
    - **Name:** `Google OAuth Client`
    - **Server:** `/Common/Google`
    - **Grant Type:** `Authorization Code`
    - **Authentication Redirect Request:** `/Common/GoogleAuthRedirectRequest`
    - **Token Request:** `/Common/GoogleTokenRequest`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



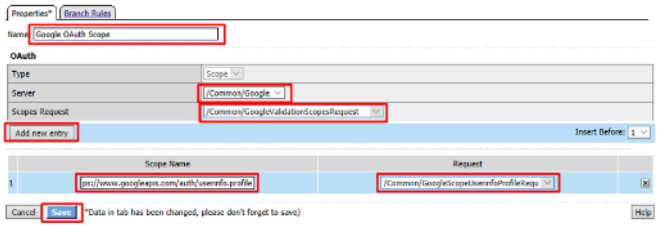
7. Click **+** on the **Successful** branch after the **Google OAuth Client**



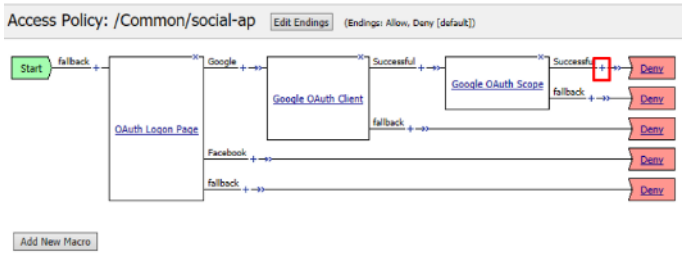
8. Select **OAuth Scope** from the **Authentication** tab, and click **Add Item**



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`

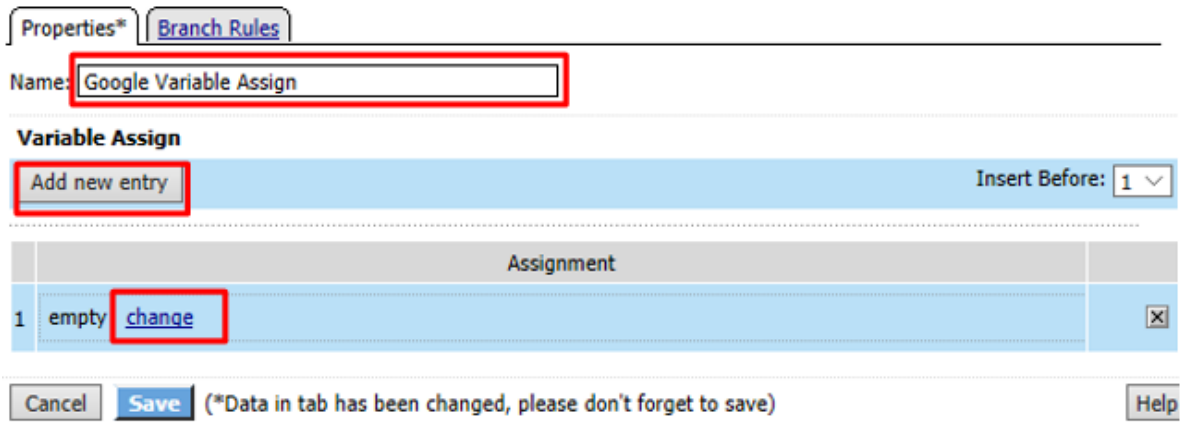


1. **Click the + on the Successful branch after the Google OAuth Scope** object



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**

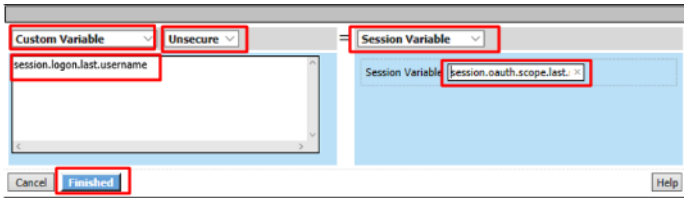
   Left Side:

   - **Type:** `Custom Variable`

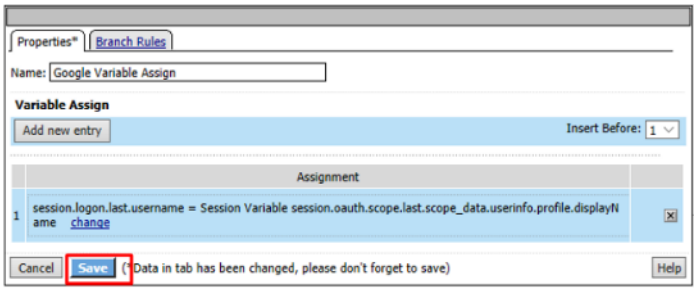
- **Security:** `Unsecure`
- **Value:** `session.logon.last.username`

Right Side:

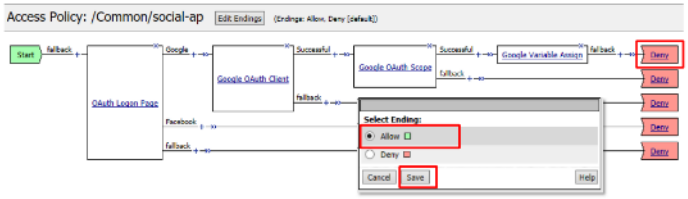
- **Type:** `Session Variable`
- **Session Variable:** `session.oauth.scope.last.scope_data.userinfo.profile.displayName`



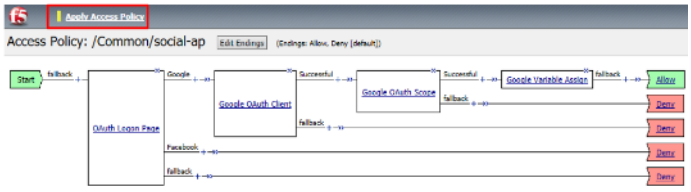
5. Review the **Google Variable Assign** object and click **Save**



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

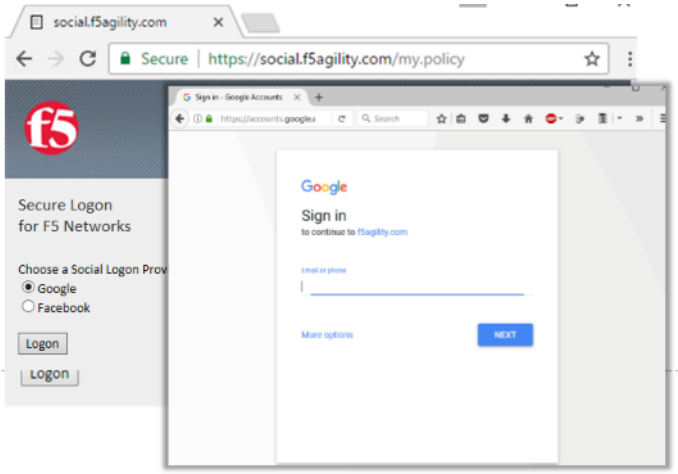


7. Click **Apply Access Policy** in the top left and then close the tab



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.

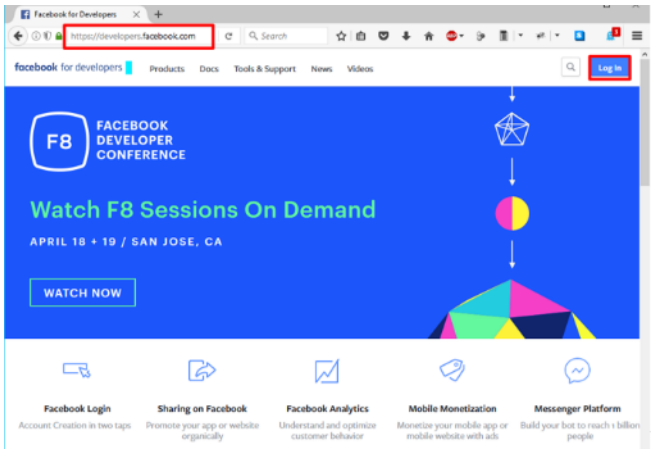
Note: You may also be prompted for additional security measures as you are logging in from a new location.

2.2.6 Task 5: Facebook (Built-In Provider)

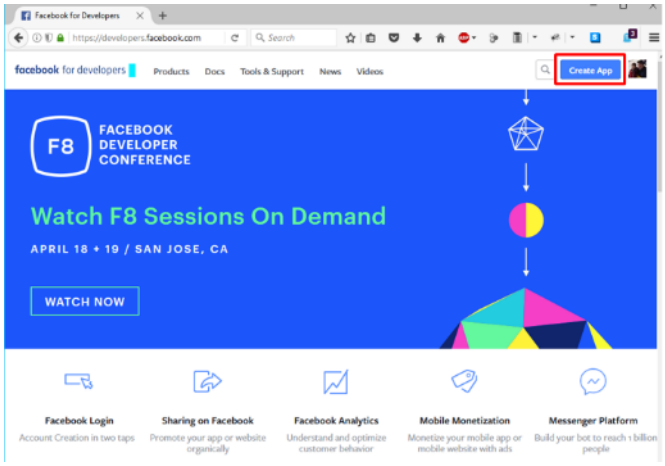
Setup a Facebook Project

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



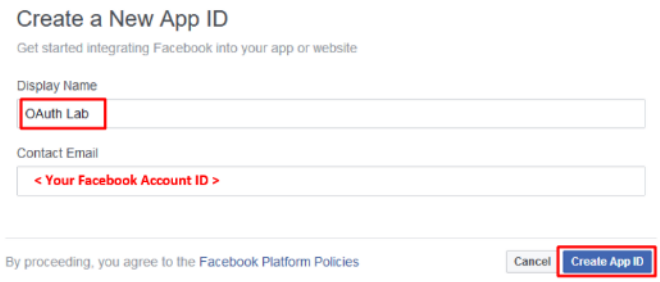
2. If prompted click, **Get Started** and accept the **Developer Policy.** Otherwise, click **Create App**



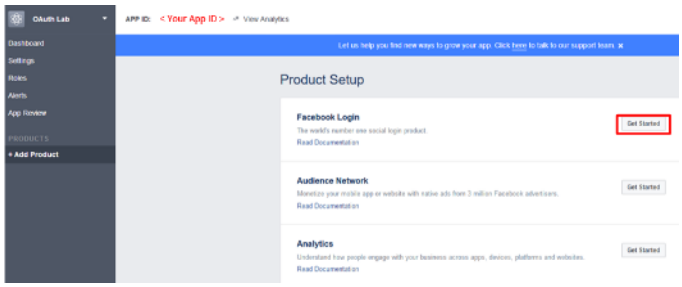
3. Click **Create App** and name (**Display Name**) your app (Or click the top left project drop down and create a new app, then name it). Then click **Create App ID**.

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

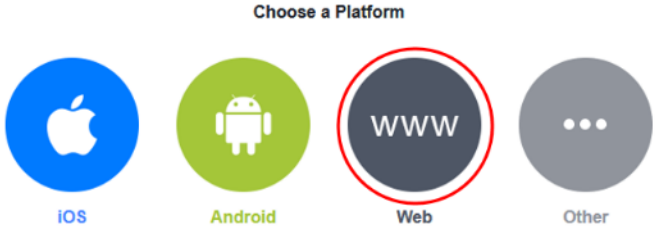
---



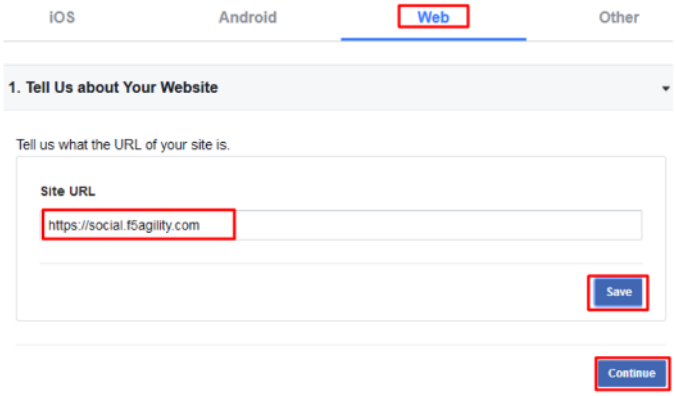
4. Click **Get Started** in the **Facebook Login** section (*Or click + Add Product and then Get Started for Facebook*)



5. From the *“Choose a Platform”* screen click on **WWW (Web)**



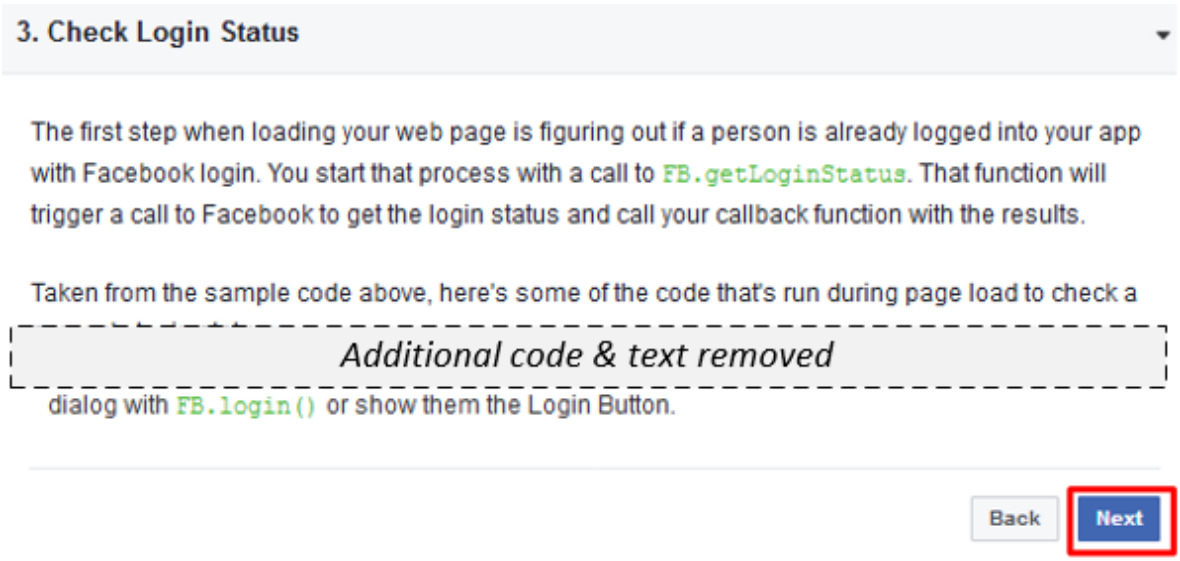
6. In the *"Tell Us about Your Website"* prompt, enter `https://social.f5agility.com` for the **Site URL** and click **Save** then click **Continue**



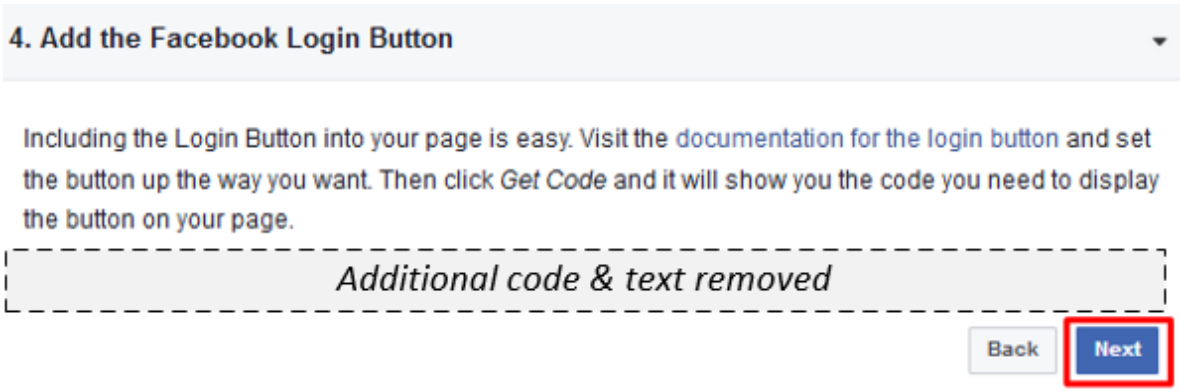
7. Click **Next** on the *"Set Up the Facebook SDK for Javascript"* screen

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

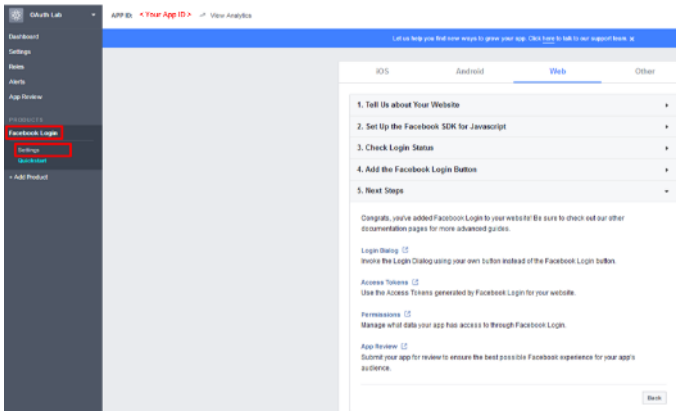
Note: Additional screen content removed.



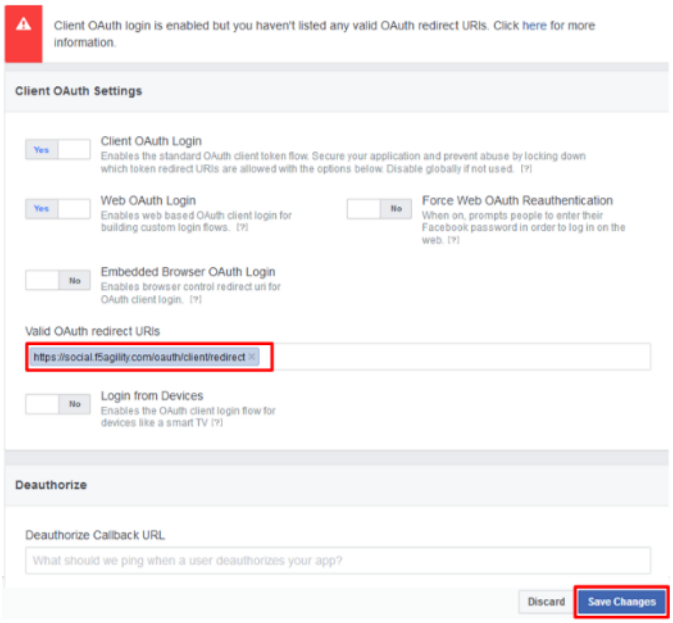
9. Click **Next** on the *"Add the Facebook Login Button"* screen



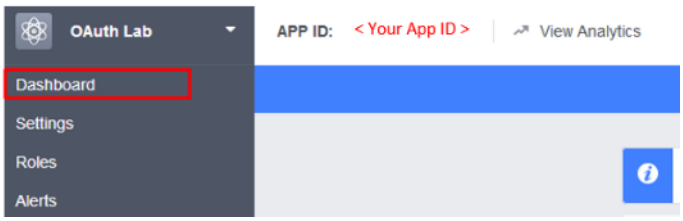
10. Click **Facebook Login** on the left side bar and then click **Settings**



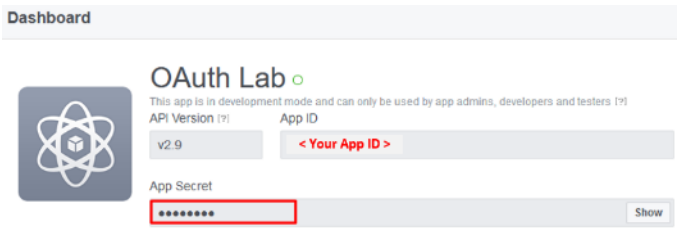
11. For the **Client OAuth Settings** screen in the **Valid OAuth redirect URIs** enter `https://social.f5agility.com/oauth/client/redirect` and then click enter to create it, then **Save Changes**



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).



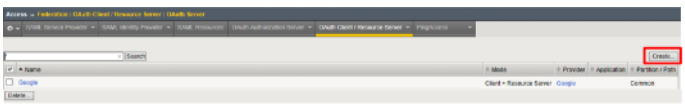
Screenshot of completed Facebook project

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

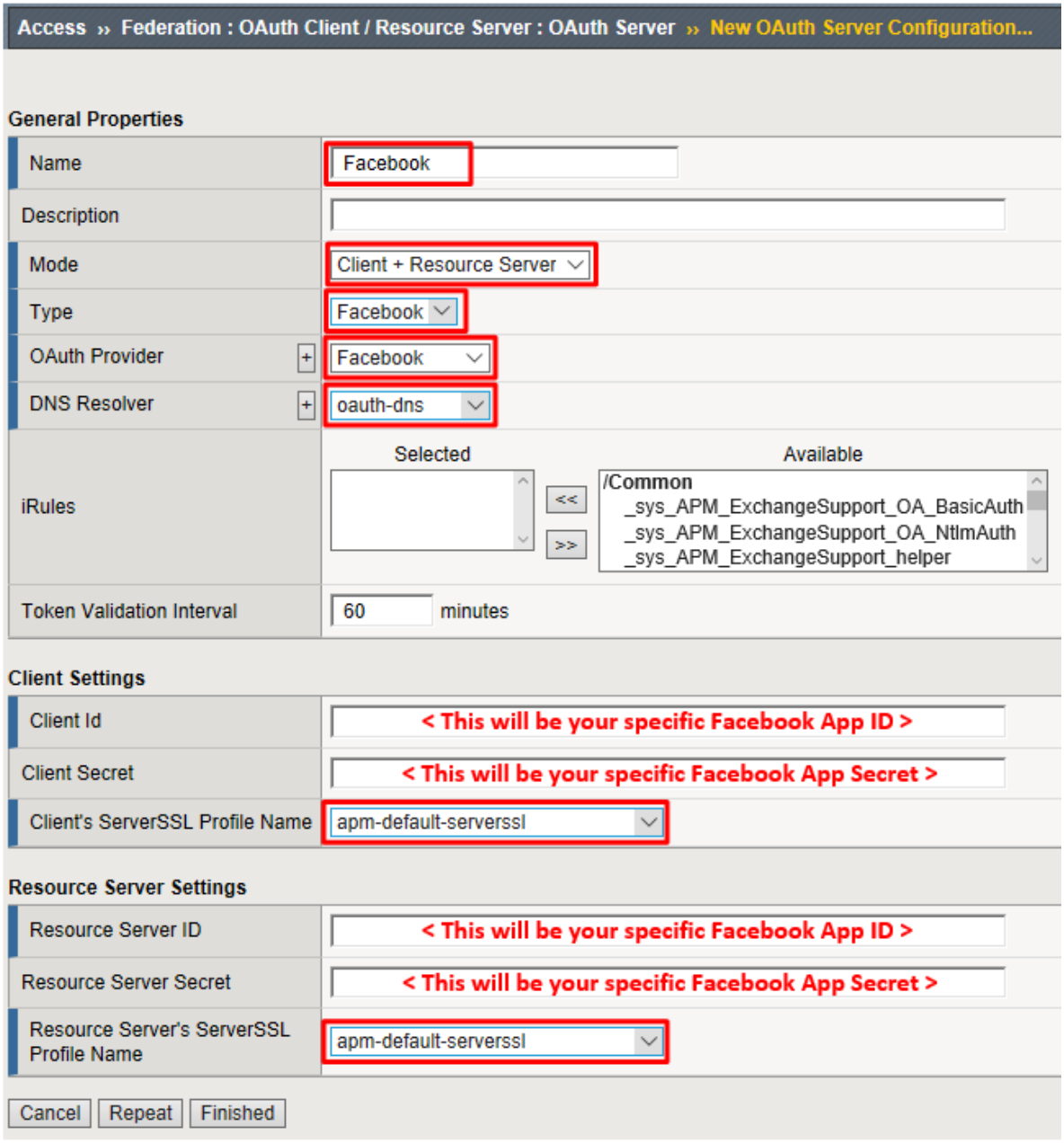
---

Configure Access Policy Manager (APM) to authenticate with Facebook

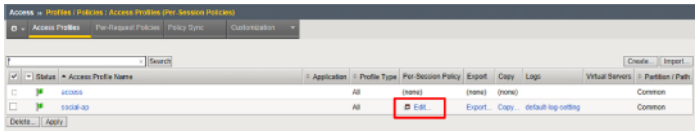
1. Configure the **OAuth Server** Object: Go to **Access -> Federation -> OAuth Client / Resource Server -> OAuth Server** and click **Create**



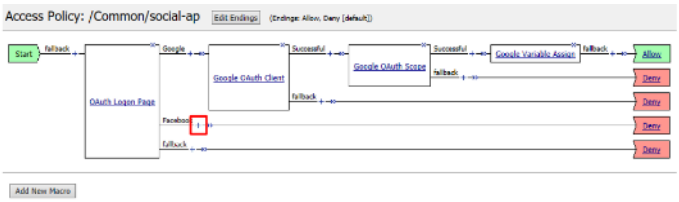
2. Enter the values as shown below for the **OAuth Server** and click **Finished**
    - **Name:** `Facebook`
    - **Mode:** `Client + Resource Server`
    - **Type:** `Facebook`
    - **OAuth Provider:** `Facebook`
    - **DNS Resolver:** `oauth-dns` *(configured for you)*
    - **Client ID:** `<App 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`



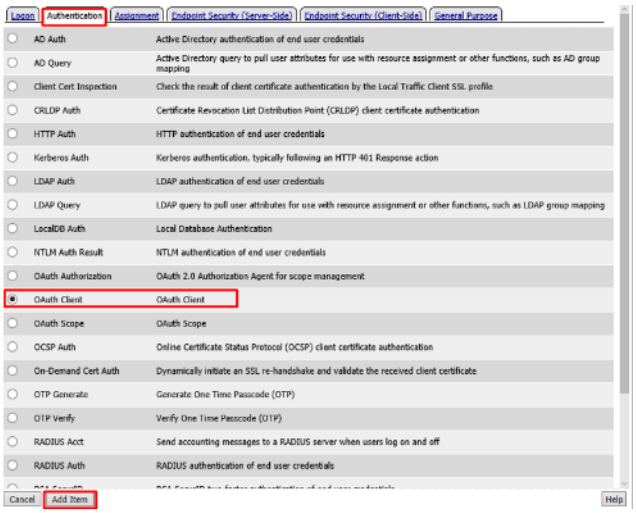
3. Configure the VPE for Facebook: Go to **Access -> Profiles / Policies -> Access Profiles (Per Session Policies)** and click **Edit** on `social-ap`, a new browser tab will open



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

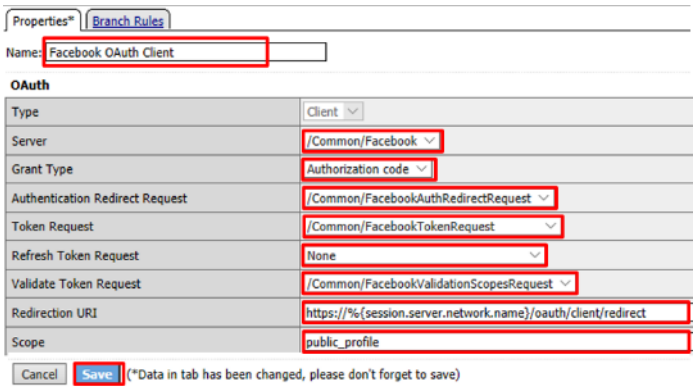


5. Select **OAuth Client** from the **Authentication** tab and click **Add Item**

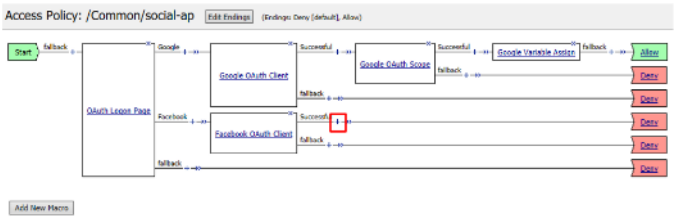


6. Enter the following in the **OAuth Client** input screen and click **Save**

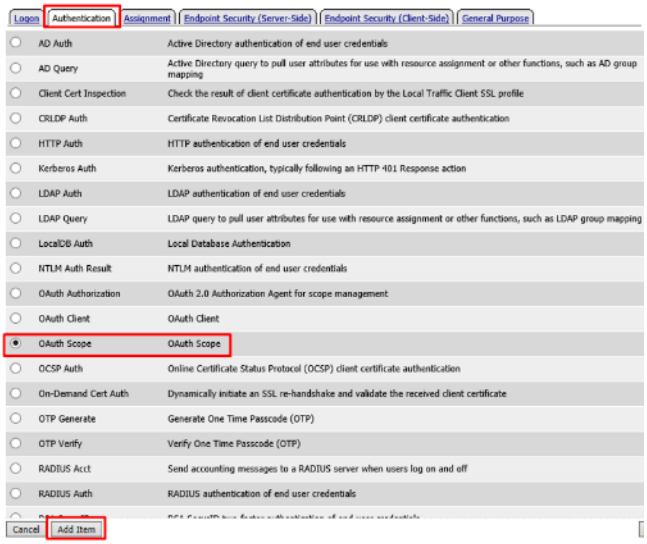
   - **Name:** `Facebook OAuth Client`
   - **Server:** `/Common/Facebook`
   - **Grant Type:** `Authorization Code`
   - **Authentication Redirect Request:** `/Common/FacebookAuthRedirectRequest`
   - **Token Request:** `/Common/FacebookTokenRequest`
   - **Refresh Token Request:** `None`
   - **Validate Token Request:** " /Common/FacebookValidationScopesRequest"
   - **Redirection URI:** `https://%{session.server.network.name}/oauth/client/redirect`
   - **Scope:** `public_profile` *(Note underscore)*



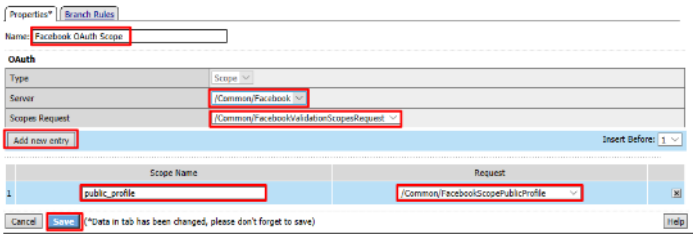
7. Click **+** on the **Successful** branch after the **Facebook OAuth Client**



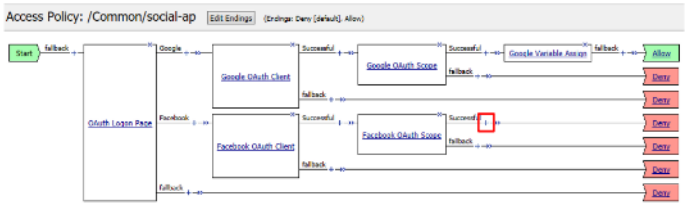
8. Select **OAuth Scope** from the **Authentication** tab, and click **Add Item**



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`

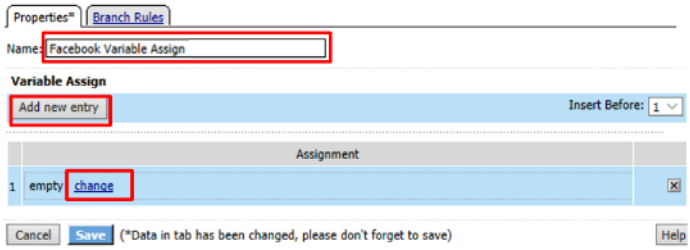


10. Click the **+** on the **Successful** branch after the **Facebook OAuth Scope** object



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**



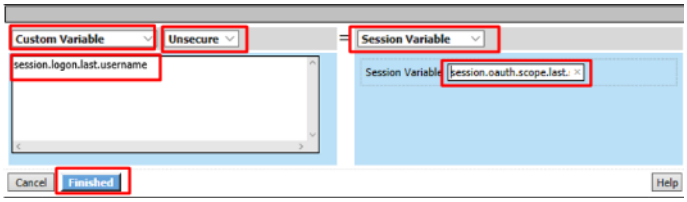
13. Enter the following values and click **Finished**

    Left Side:

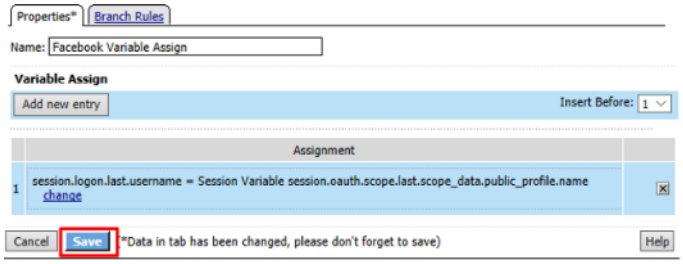
    - **Type:** `Custom Variable`
    - **Security:** `Unsecure`
    - **Value:** `session.logon.last.username`

    Right Side:

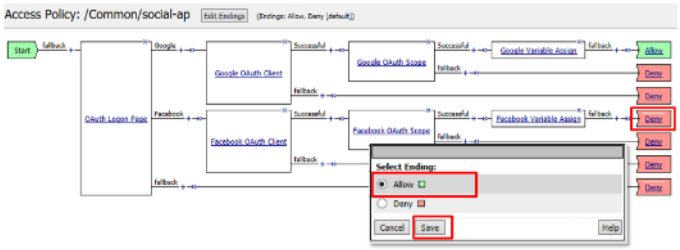
    - **Type:** `Session Variable`
    - **Session Variable:** `session.oauth.scope.last.scope_data.public_profile.name`



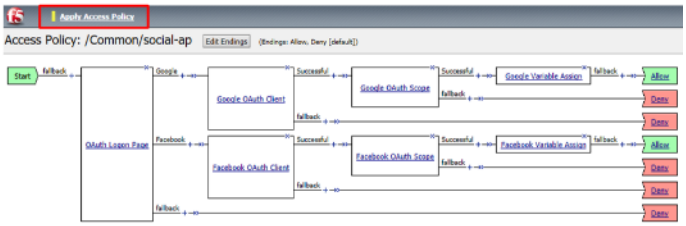
14. Review the **Facebook Variable Assign** object and click **Save**



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

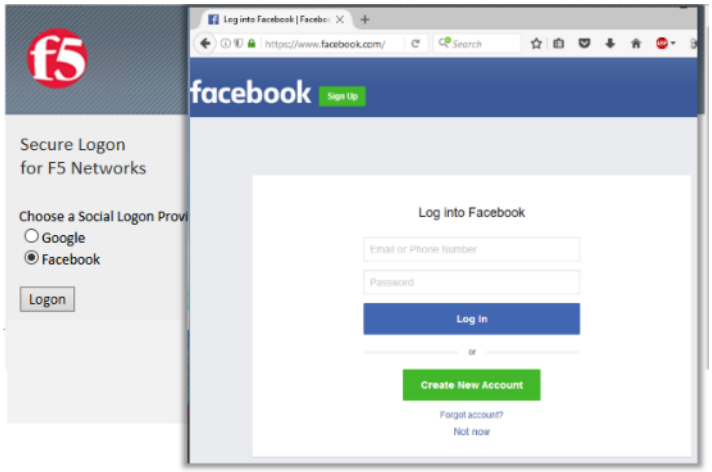


16. Click **Apply Access Policy** in the top left and then close the tab



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.



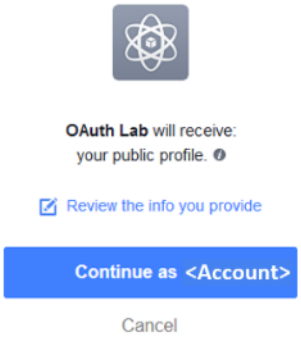
Note: You are able to login and reach the app now, but SSO to the app has not been setup so you

get an application error.

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

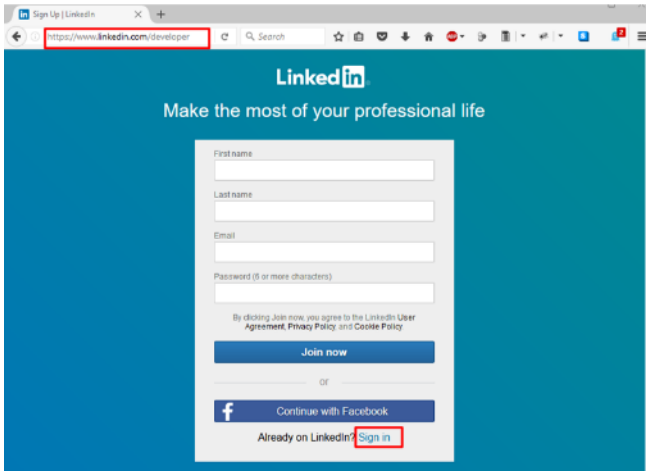
Note: You may need to start a Chrome New Incognito Window so no session data carries over.

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



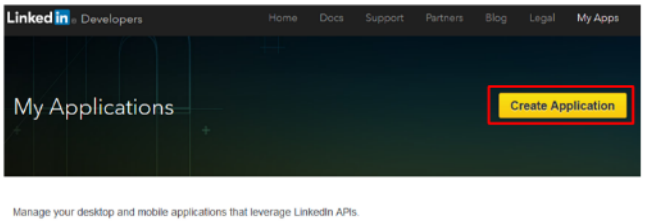
2.2.8 Task 6: LinkedIn (Custom Provider)

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

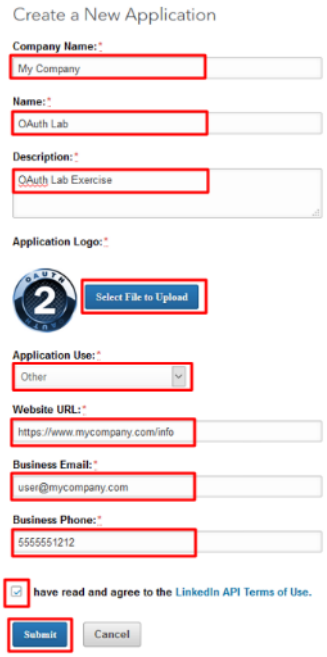


Note: This portion of the exercise requires a LinkedIn Account. You may use an existing one or create one for the purposes of this lab*

2. Click **Create Application**



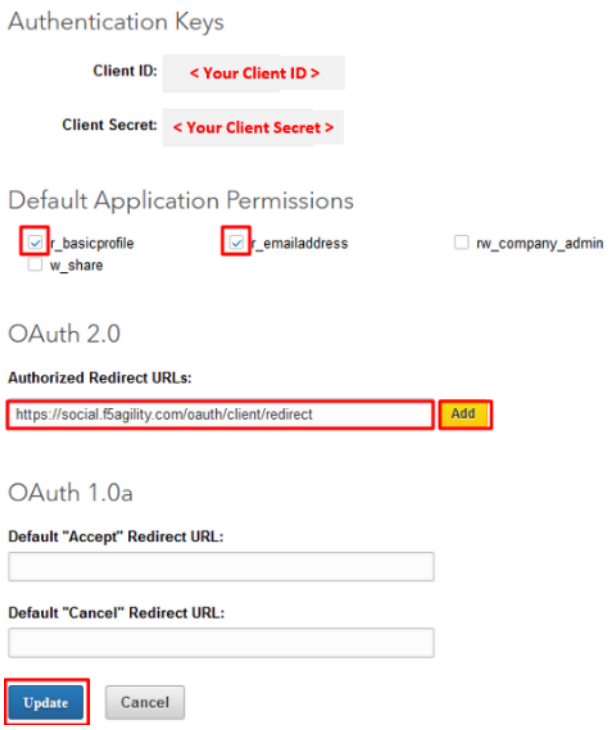
3. In the **Create a New Application** screen fill in the required values and click **Submit**



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

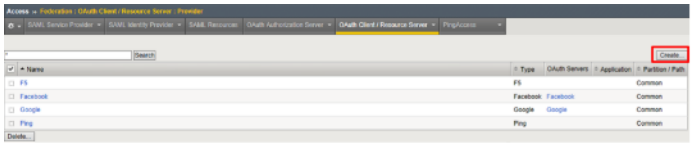
Note: An Application logo has been provided on your desktop 'OAuth2.png'

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

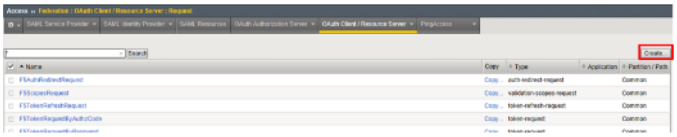
1. Configure the **OAuth Server** Object: Go to **Access -> Federation -> OAuth Client / Resource Server -> Provider** and click **Create**



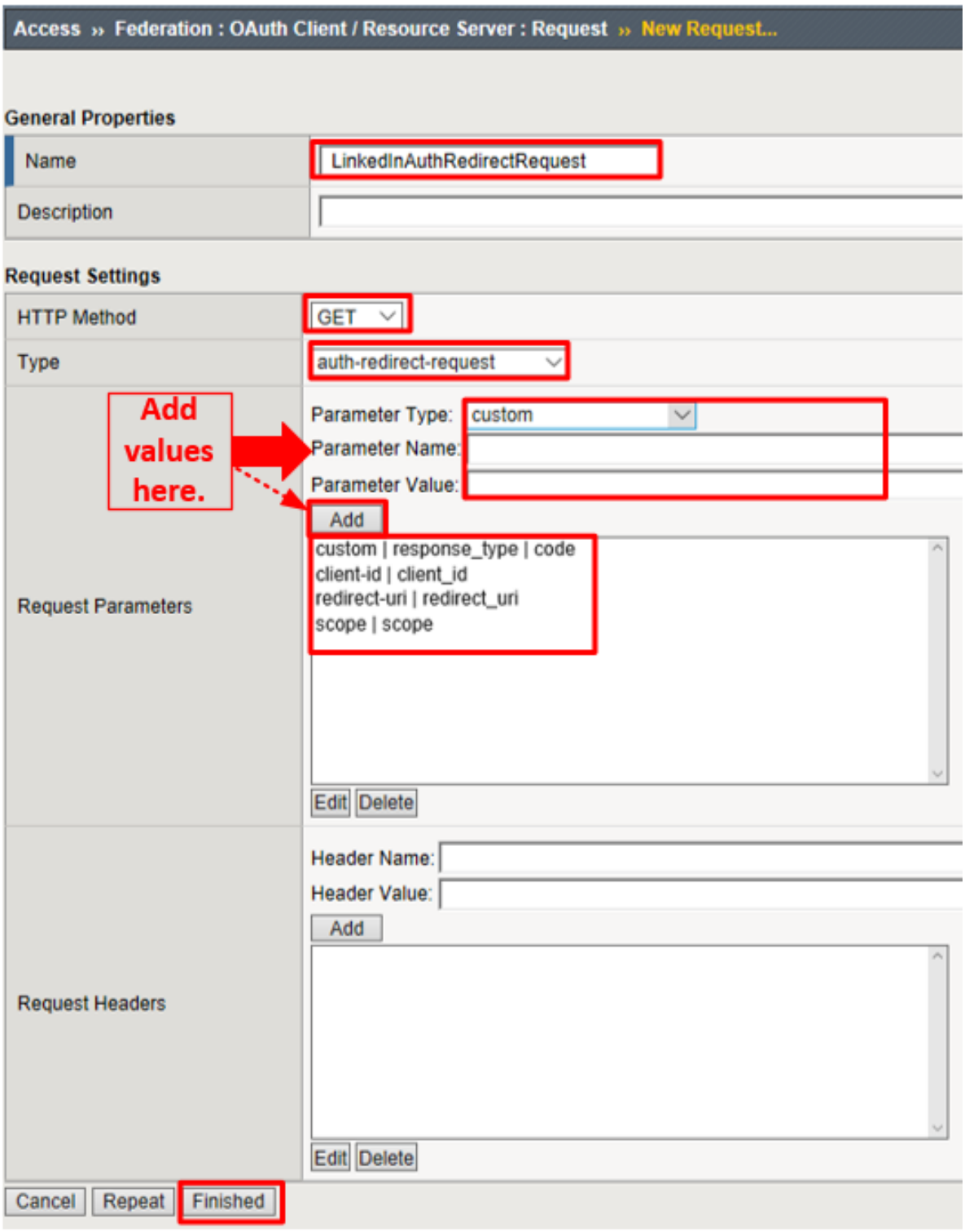
Note: You are creating a “Provider”

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/~`

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



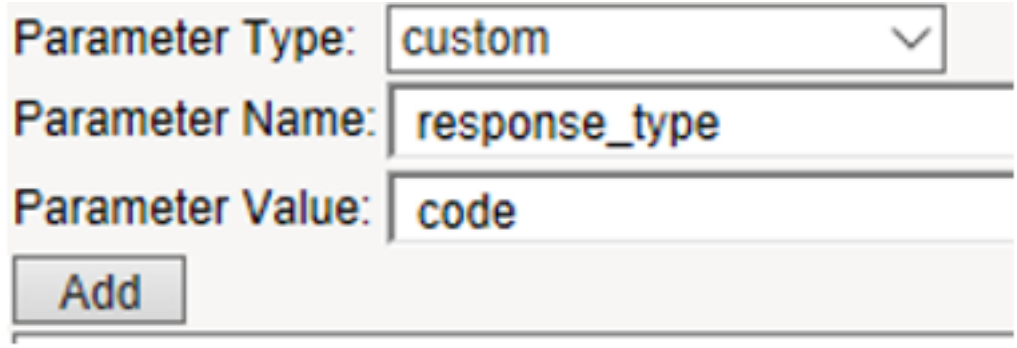
4. Enter the values as shown for the **OAuth Request** and click **Finished**
    - **Name:** `LinkedInAuthRedirectRequest`
    - **HTTP Method:** `GET`
    - **Type:** `auth-redirect-request`

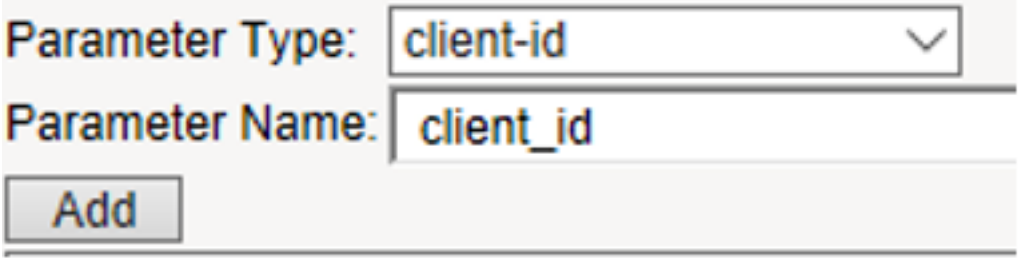


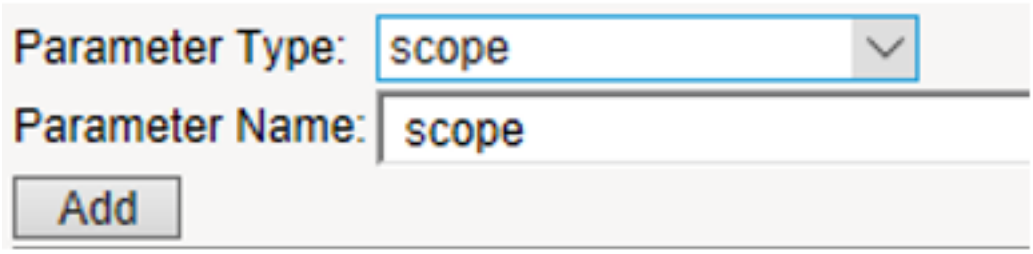
5. Add the following request parameters and click **Add** after entering the values for each:
    - **Parameter Type:** `custom`
    - **Parameter Name:** `response_type`
    - **Parameter Value:** `code`

- **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.

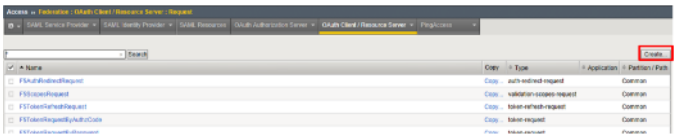




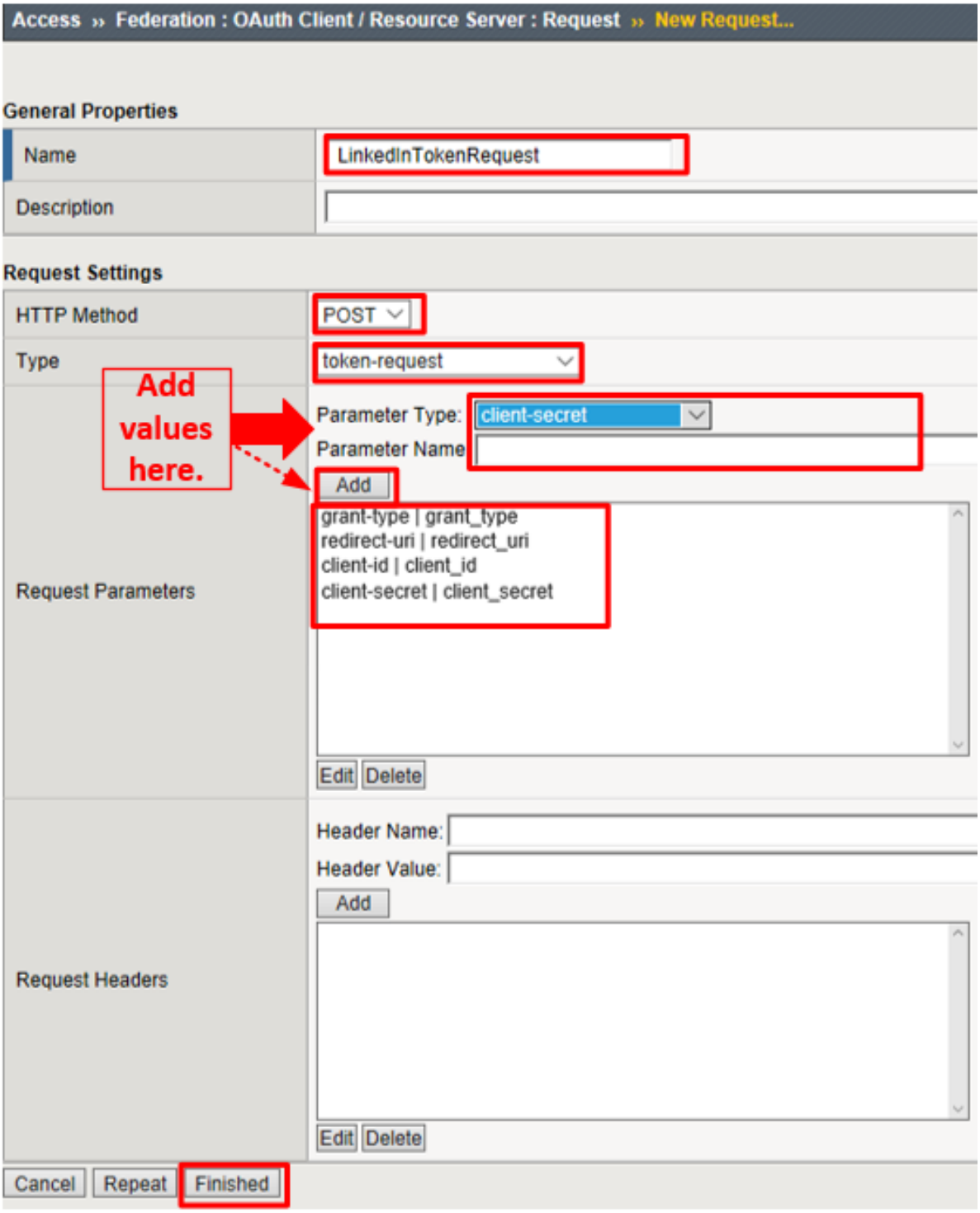


6. Configure the **OAuth Token Request** Profile Object: Go to **Access -> Federation -> OAuth Client** /

Resource Server -> Request and click **Create**

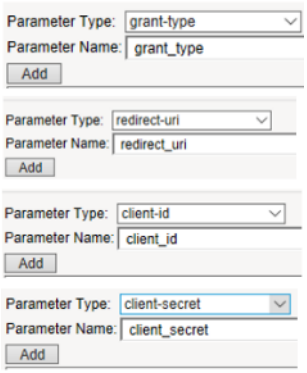


7. Enter the values as shown for the **OAuth Request** and click **Finished**
    - **Name:** `LinkedInTokenRequest`
    - **HTTP Method:** `POST`
    - **Type:** `token-request`

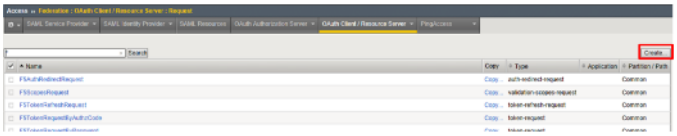


8. Add the following request parameters and click **Add** after entering the values for each:
   - **Parameter Type:** `grant-type`
   - **Parameter Name:** `grant_type`
   - **Parameter Type:** `redirect-uri`
   - **Parameter Name:** `redirect_uri`

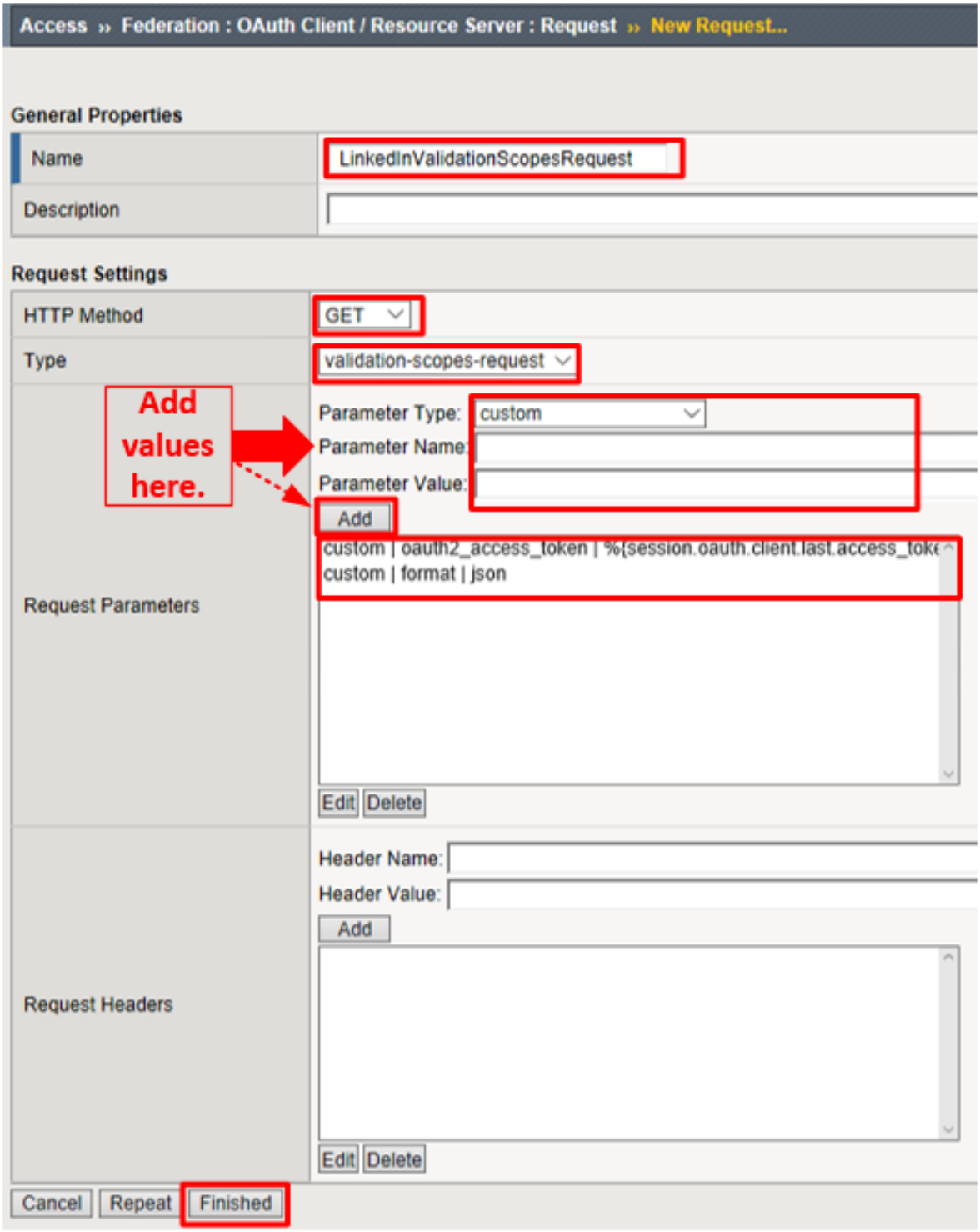
- **Parameter Type:** `client-id`
- **Parameter Name:** `client_id`
- **Parameter Type:** `client-secret`
- **Parameter Name:** `client_secret`



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

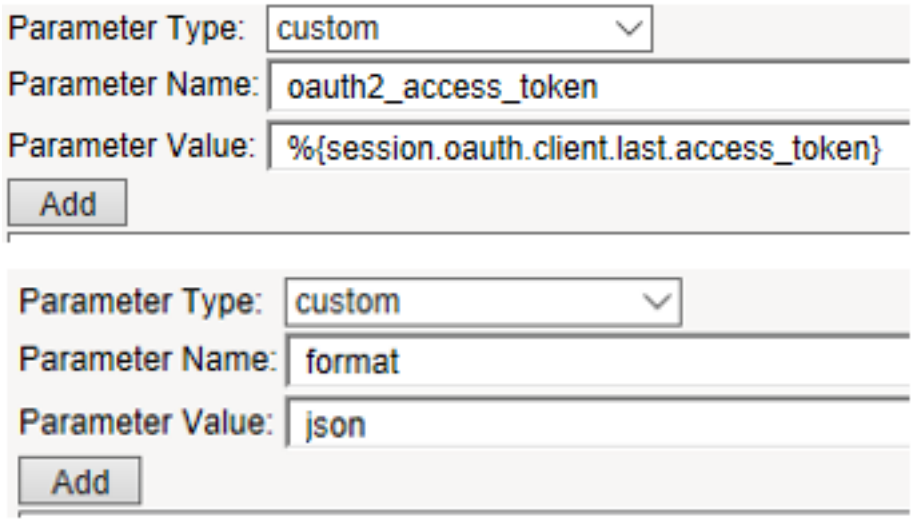


10. Enter the values as shown for the **OAuth Request** and click **Finished**
    - **Name:** `LinkedInValidationScopesRequest`
    - **HTTP Method:** `GET`
    - **Type:** `validation-scopes-request`

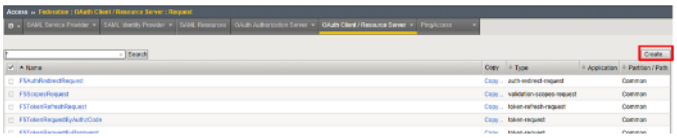


11. Add the following request parameters and click **Add** after entering the values for each:
    - **Parameter Type:** `custom`
    - **Parameter Name:** `oauth2_access_token`
    - **Parameter Value:** `%{session.oauth.client.last.access_token}`
    - **Parameter Type:** `custom`

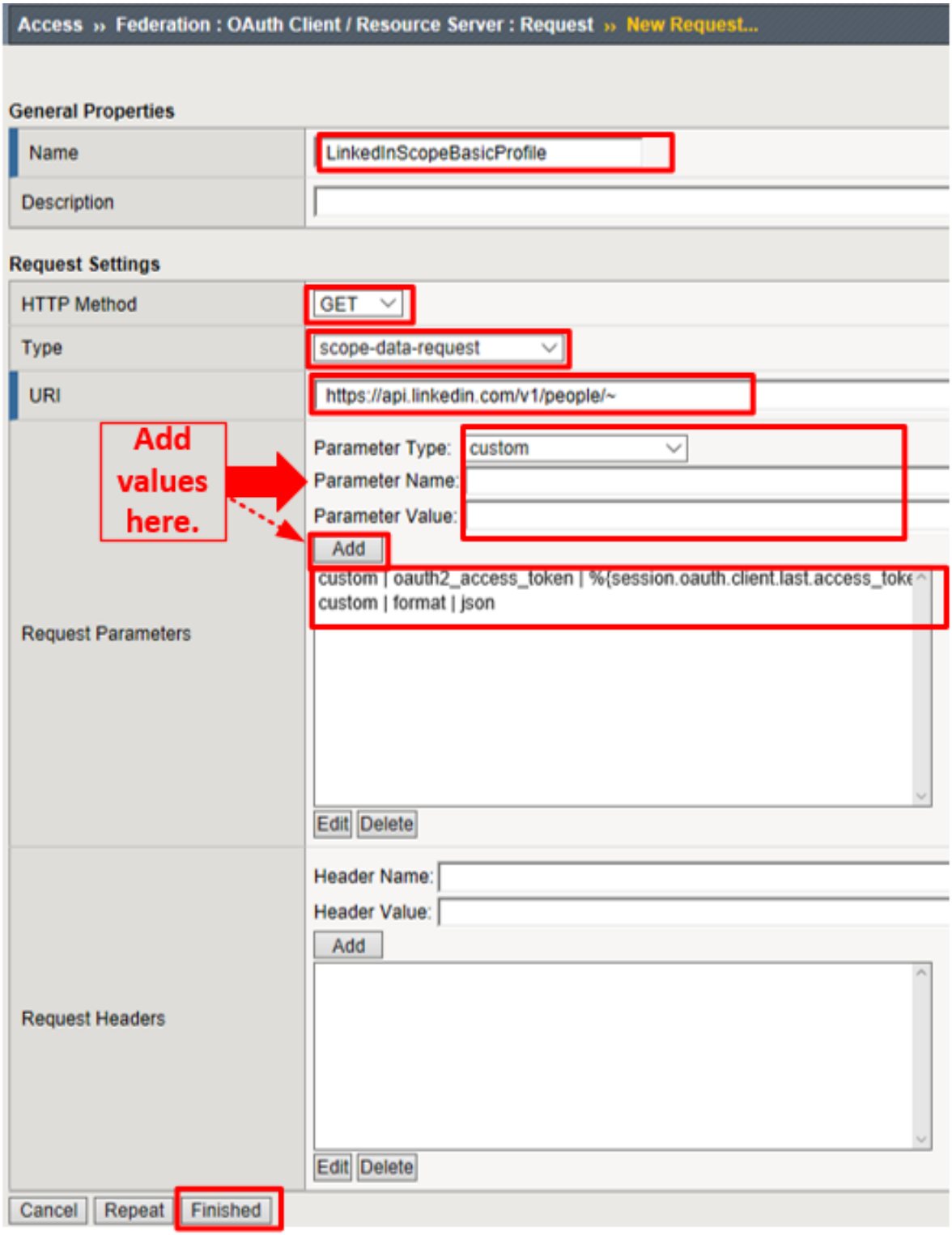
- **Parameter Name:** `format`
- **Parameter Value:** `json`



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

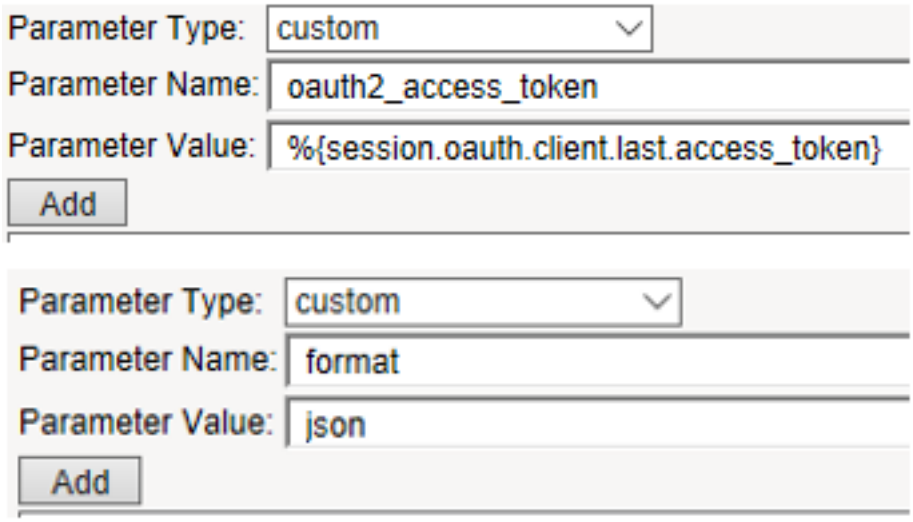


13. Enter the values as shown for the **OAuth Request** and click **Finished**
    - **Name:** `LinkedInScopeBasicProfile`
    - **HTTP Method:** `GET`
    - **URI:** `https://api.linkedin.com/v1/people/~`
    - **Type:** `scope-data-request`

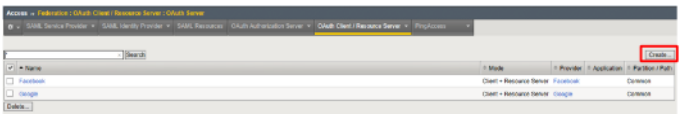


14. Add the following request parameters and click **Add** after entering the values for each:
    - **Parameter Type:** `custom`
    - **Parameter Name:** " oauth2_access_token"
    - **Parameter Value:** `%{session.oauth.client.last.access_token}`

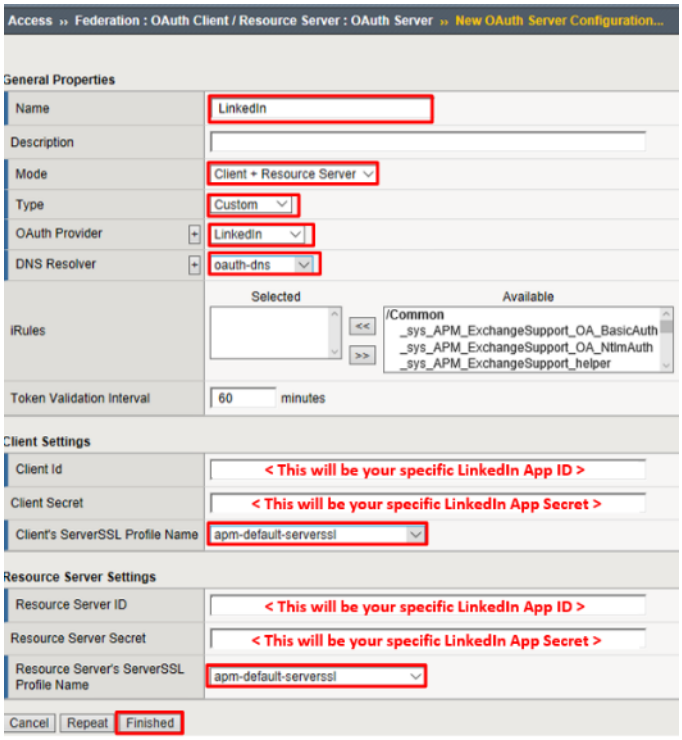
- **Parameter Type:** `custom`
- **Parameter Name:** `format`
- **Parameter Value:** `json`



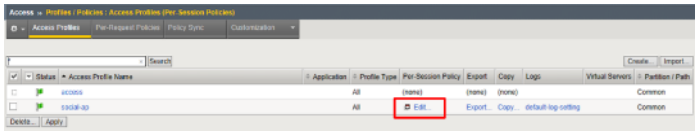
15. Configure the **OAuth Server** Object: Go to **Access -> Federation -> OAuth Client / Resource Server -> OAuth Server** and click **Create**



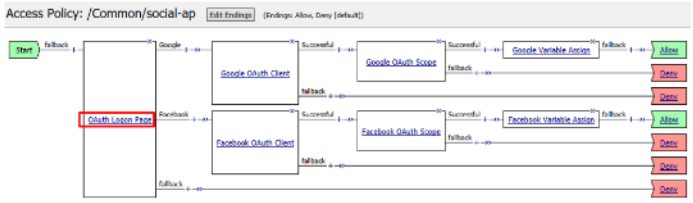
16. Enter the values as shown below for the **OAuth Server** and click **Finished**
    - **Name:** `LinkedIn`
    - **Mode:** `Client + Resource Server`
    - **Type:** `Custom`
    - **OAuth Provider:** `LinkedIn`
    - **DNS Resolver:** `oauth-dns *(configured for you)*`
    - **Client ID:** `<App 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`



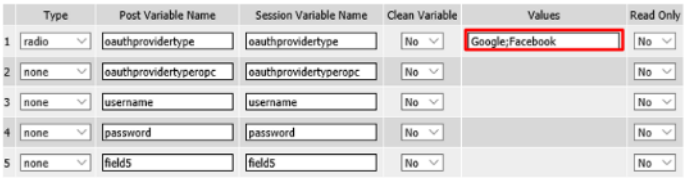
17. Configure the VPE for LinkedIn: Go to **Access -> Profiles / Policies -> Access Profiles (Per Session Policies)** and click **Edit** on `social-ap`, a new browser tab will open



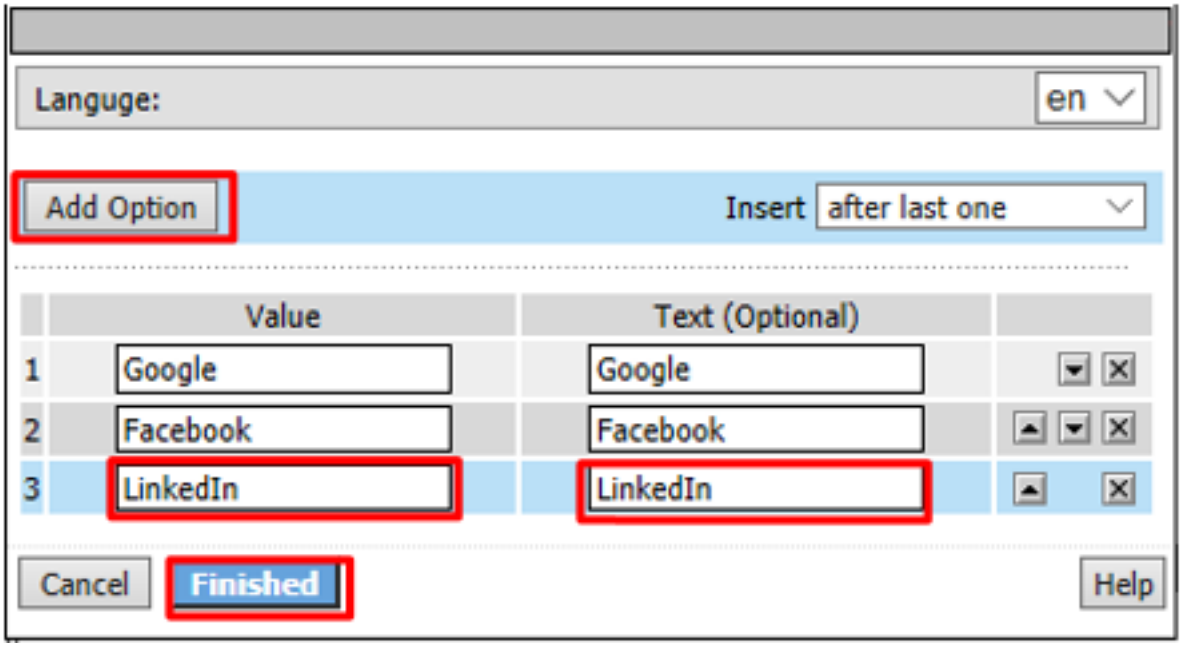
18. Click on the link **OAuth Logon Page** as shown



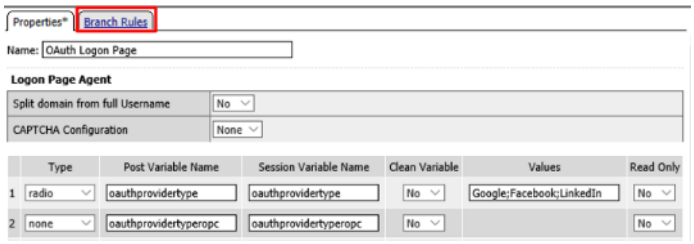
19. Click on the **Values** area of **Line #1** as shown. A pop-up window will appear



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

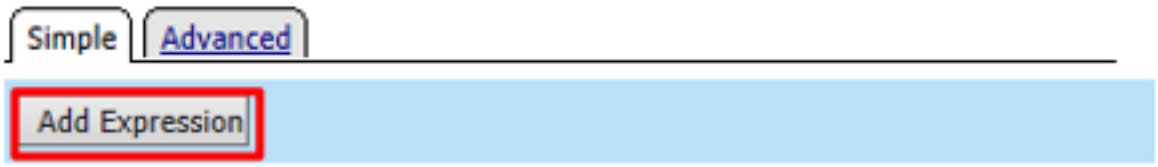


21. Click on the **Branch Rules** tab of the **OAuth Logon Page** screen

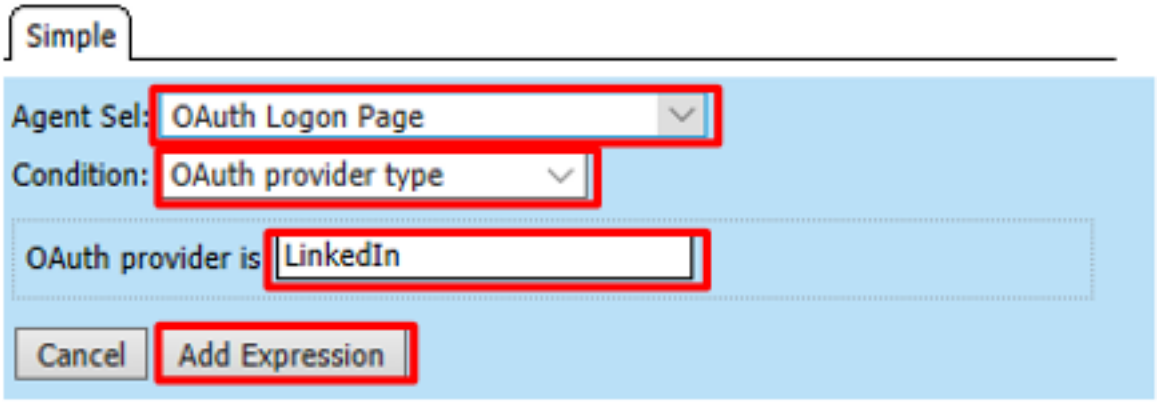


22. Click **Add Branch Rule**. In the resulting new line enter LinkedIn for the **Name** field and click the **Change** link on the **Expression** line

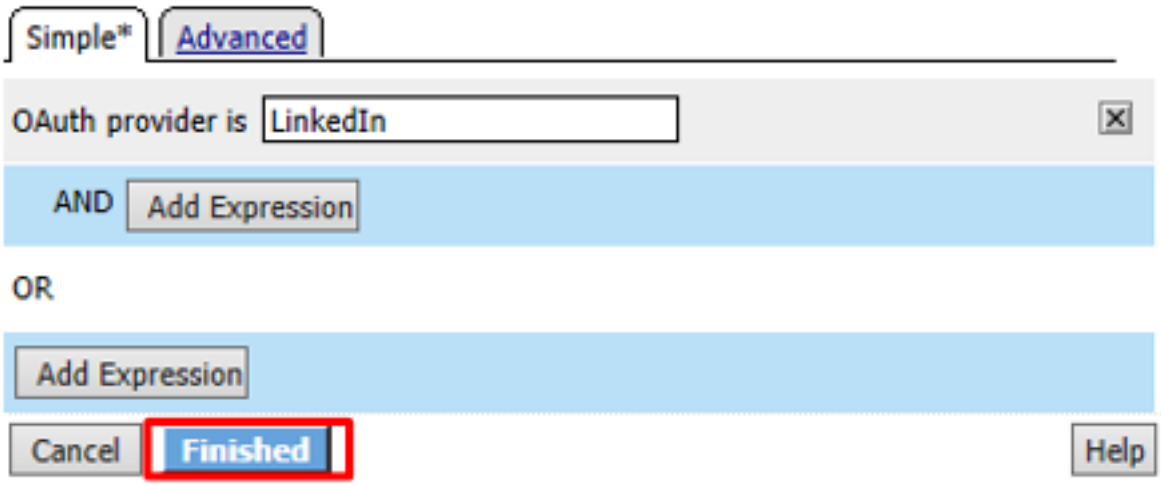
23. Click **Add Expression** on the **Simple** tab



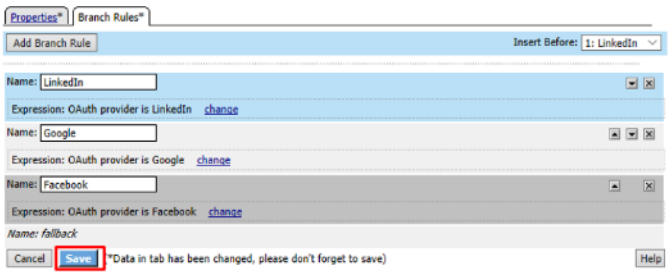
24. Select OAuth Logon Page in the **Agent Sel:** drop down. Select OAuth provider type from the **Condition** drop down. In the **OAuth provider** field enter LinkedIn and then click **Add Expression**



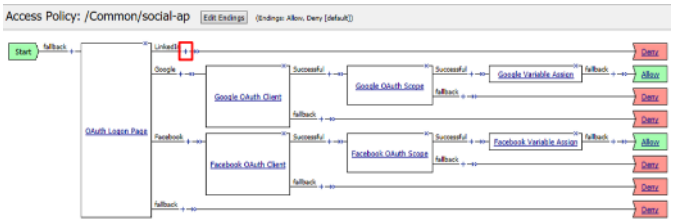
25. Click **Finished** on the **Simple** Expression tab



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



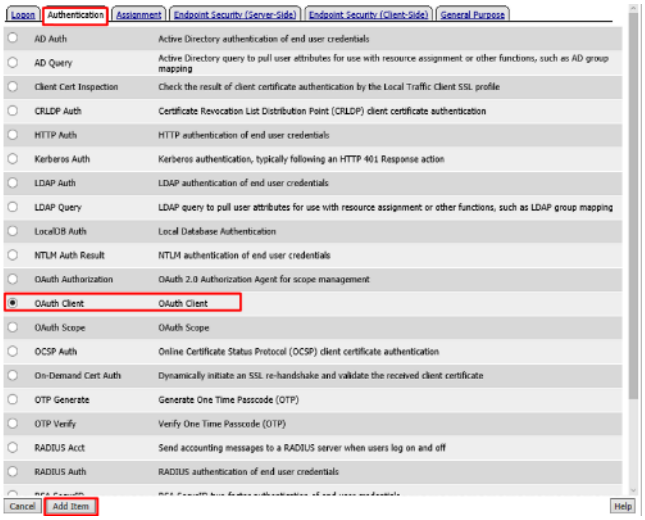
27. Click the + on the **LinkedIn** provider's branch after the **OAuth Logon Page**



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

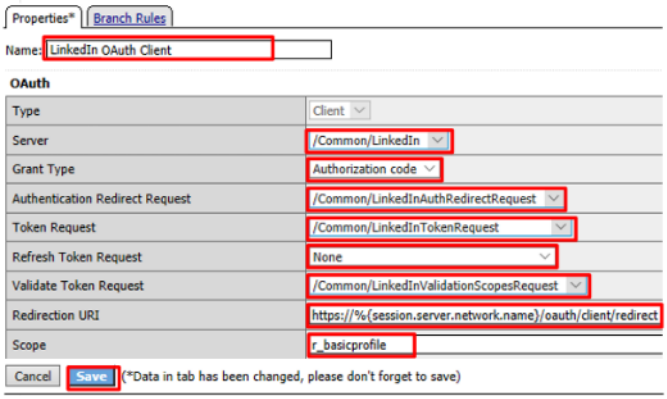
Policies). Click **Edit** on **social-ap**, a new browser tab will open*

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

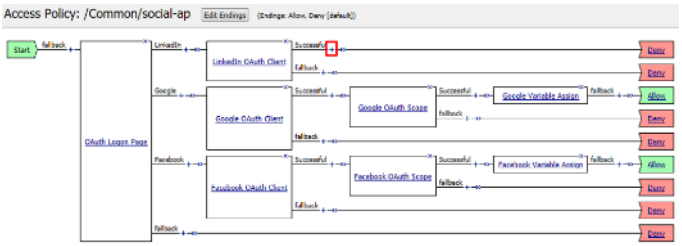


29. Enter the following in the **OAuth Client** input screen and click **Save**

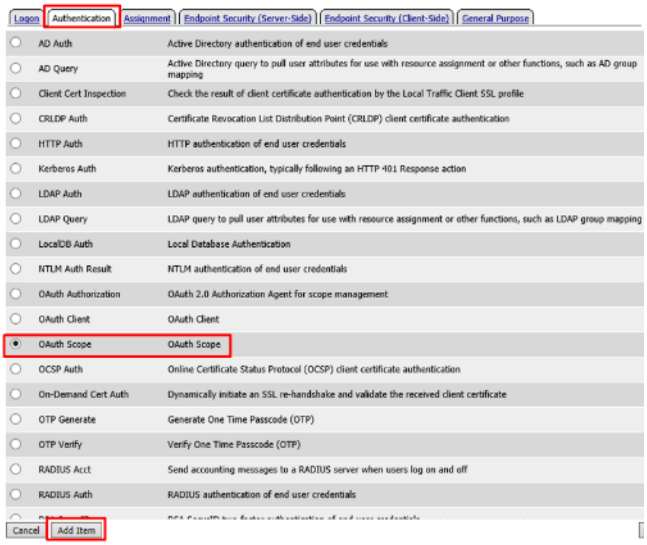
- **Name:** `LinkedIn OAuth Client`
- **Server:** `/Common/LinkedIn`
- **Grant Type:** `Authorization Code`
- **Authentication Redirect Request:** `/Common/LinkedInAuthRedirectRequest`
- **Token Request:** `/Common/LinkedInTokenRequest`
- **Refresh Token Request:** `None`
- **Validate Token Request:** `/Common/LinkedInValidationScopesRequest`
- **Redirection URI:** `https://%{session.server.network.name}/oauth/client/redirect`
- **Scope:** `r_basicprofile *(Note underscore)*`



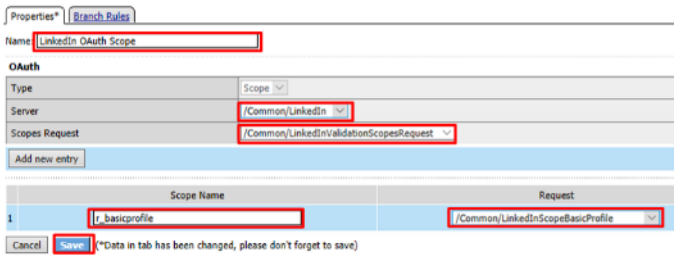
30. Click **+** on the **Successful** branch after the **LinkedIn OAuth Client**



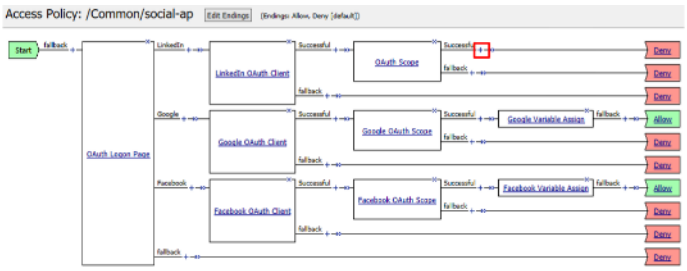
31. Select **OAuth Scope** from the **Authentication** tab, and click **Add Item**



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`

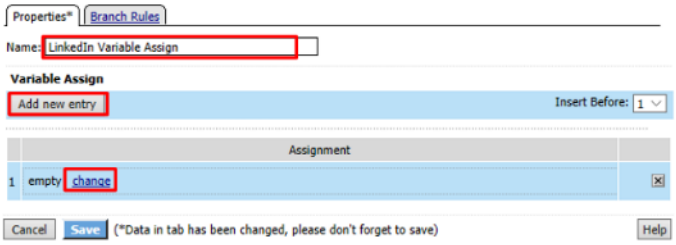


33. Click the **+** on the **Successful** branch after the **LinkedIn OAuth Scope** object



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**



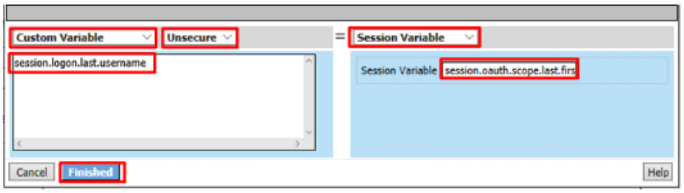
36. Enter the following values and click **Finished**

    Left Side:

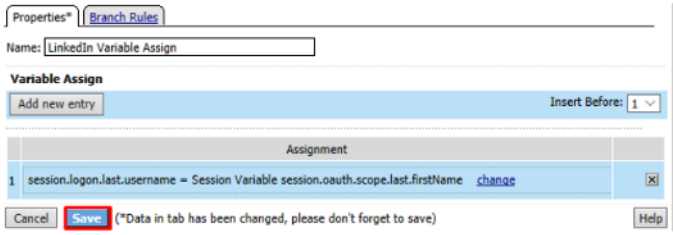
    - **Type:** `Custom Variable`
    - **Security:** `Unsecure`
    - **Value:** `session.logon.last.username`

    Right Side:

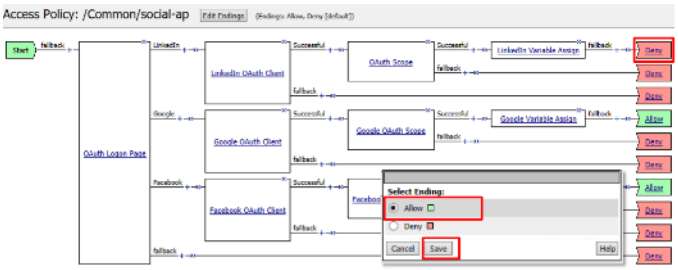
    - **Type:** `Session Variable`
    - **Session Variable:** `session.oauth.scope.last.firstName`



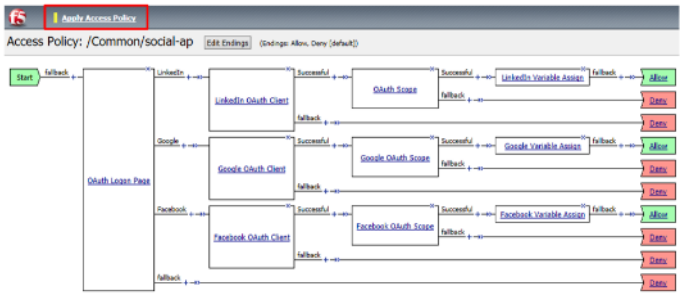
37. Review the **LinkedIn Variable Assign** object and click **Save**



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

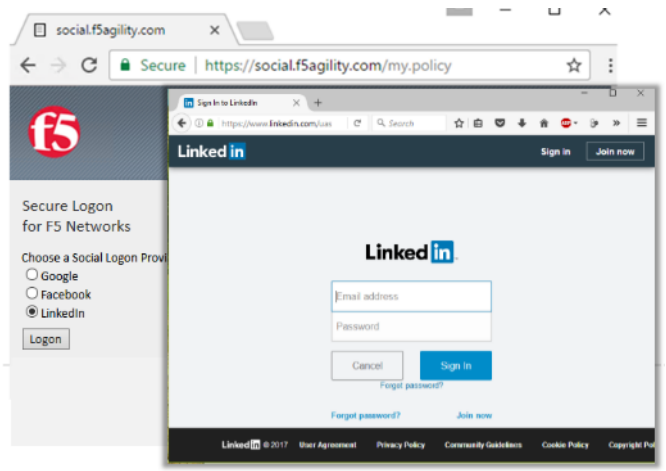


39. Click **Apply Access Policy** in the top left and then close the tab



Test Configuration

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

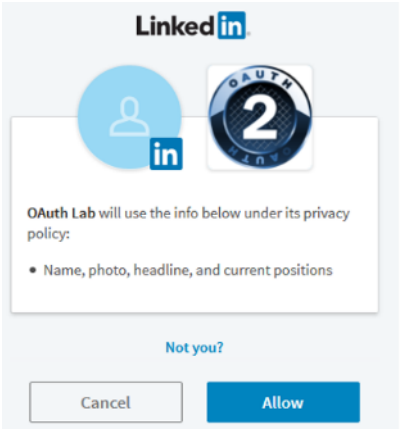


Note: You are able to login and reach the app now, but SSO to the app has not been setup so you get an application error.

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.**

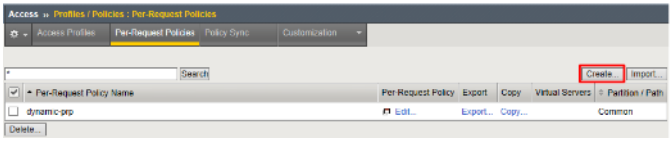


2.2.9 Task 7: Add Header Insertion for SSO to the App

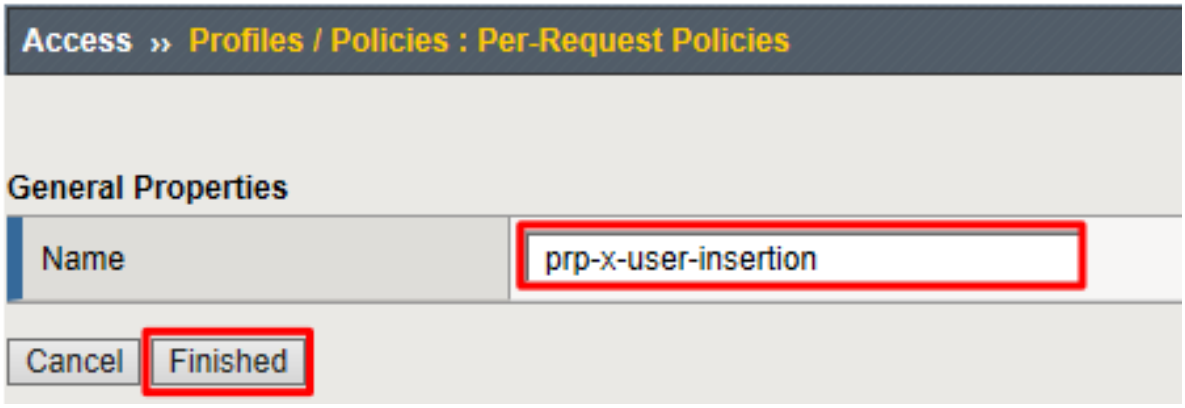
In this task you will create a policy that runs on every request. It will insert a header into the serverside HTTP Requests that contains the username. The application will use this to identify who the user is, providing Single Sign On (SSO).

Configure the Per Request Policy

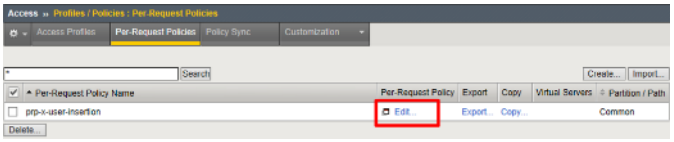
1. Go to **Access** -> **Profiles/Policies** -> **Per Request Policies** and click **Create**



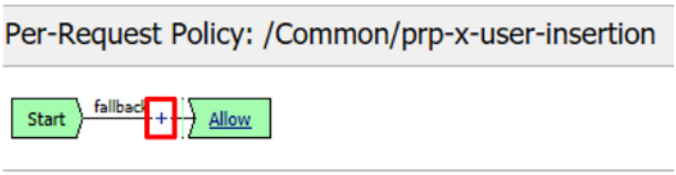
2. Enter prp-x-user-insertion the Name field and click **Finished**



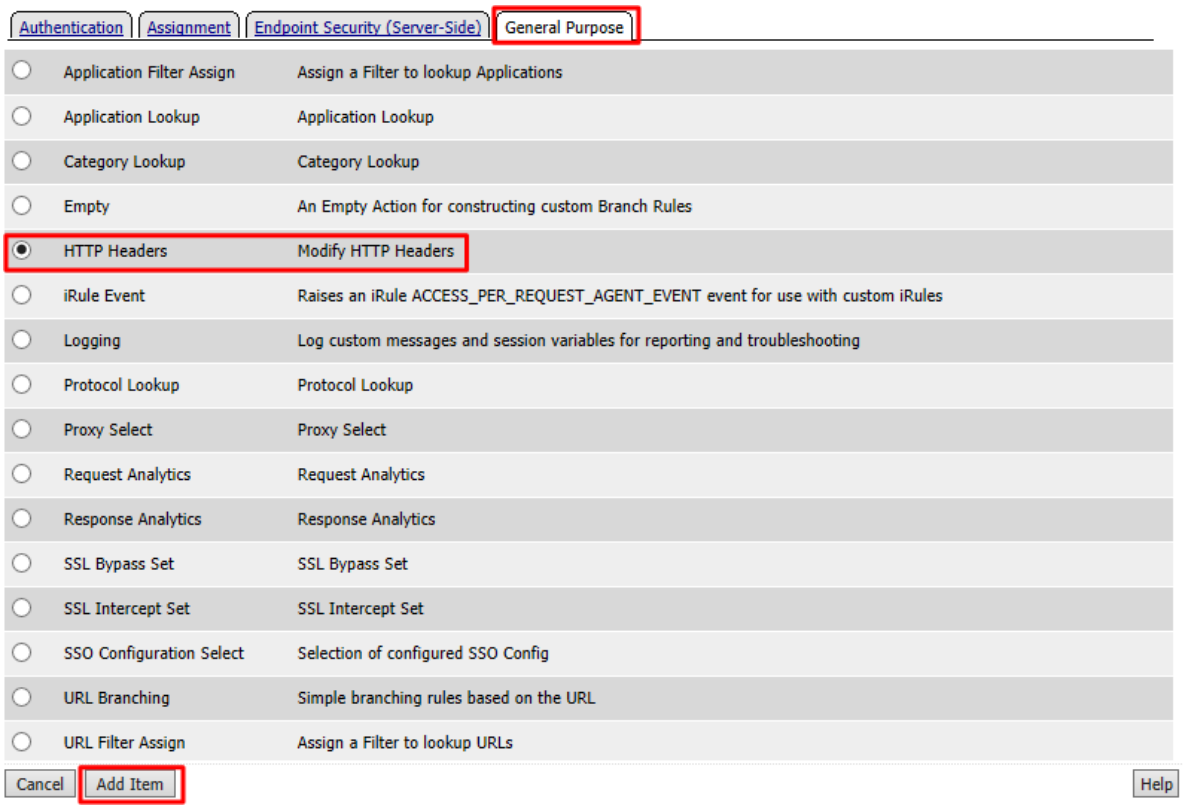
3. Click **Edit** on the **prp-x-user-insertion policy** line



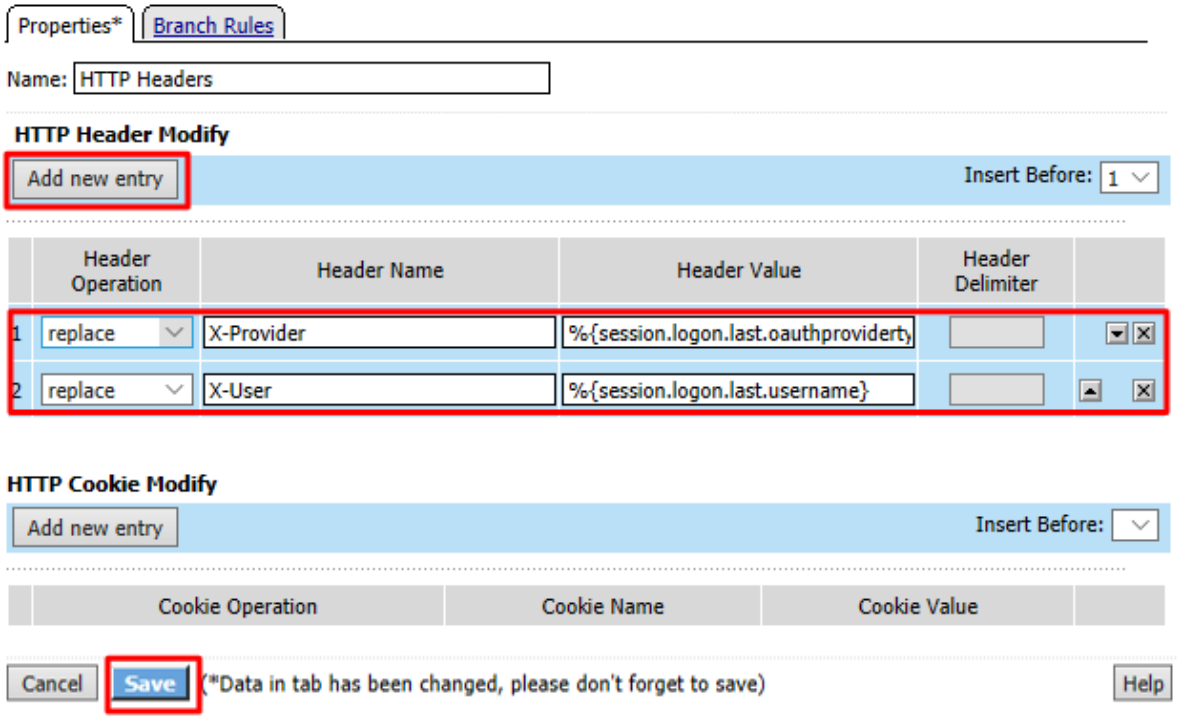
4. Click the **+** symbol between **Start** and **Allow**



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

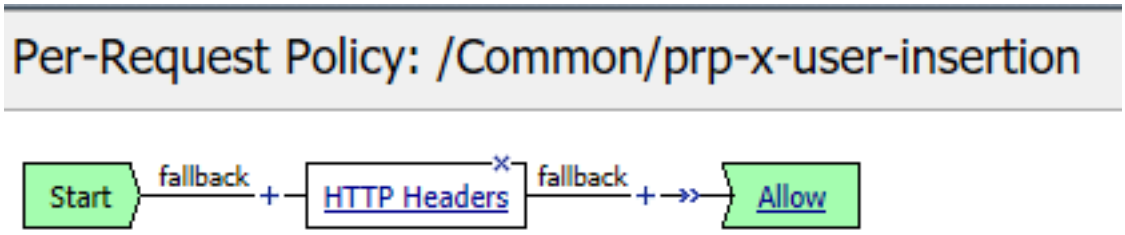


6. Under the HTTP Header Modify section, click Add New Entry to add the following two headers and then click Save
    - **Header Operation:** `replace`
    - **Header Name:** `X-User`
    - **Header Value:** `%{session.logon.last.username}`
    - **Header Operation:** `replace`
    - **Header Name:**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



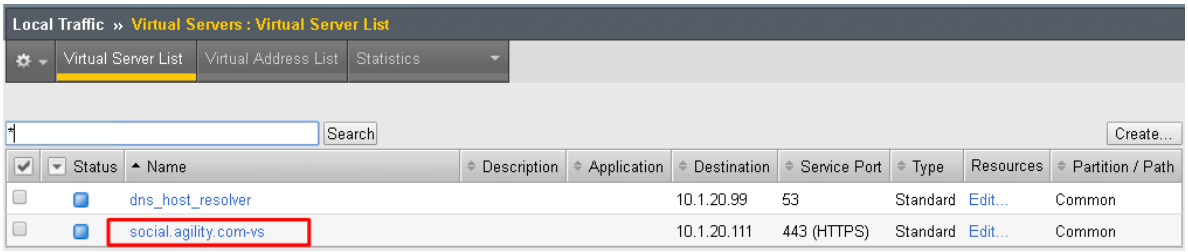
Note: Replace instead of Insert has been selected for Header Operation to improve security. A malicious user might insert their own X-User header. As using Insert would simply add another header. Using Replace will add a header if it does not exist, or replace one if it does.

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

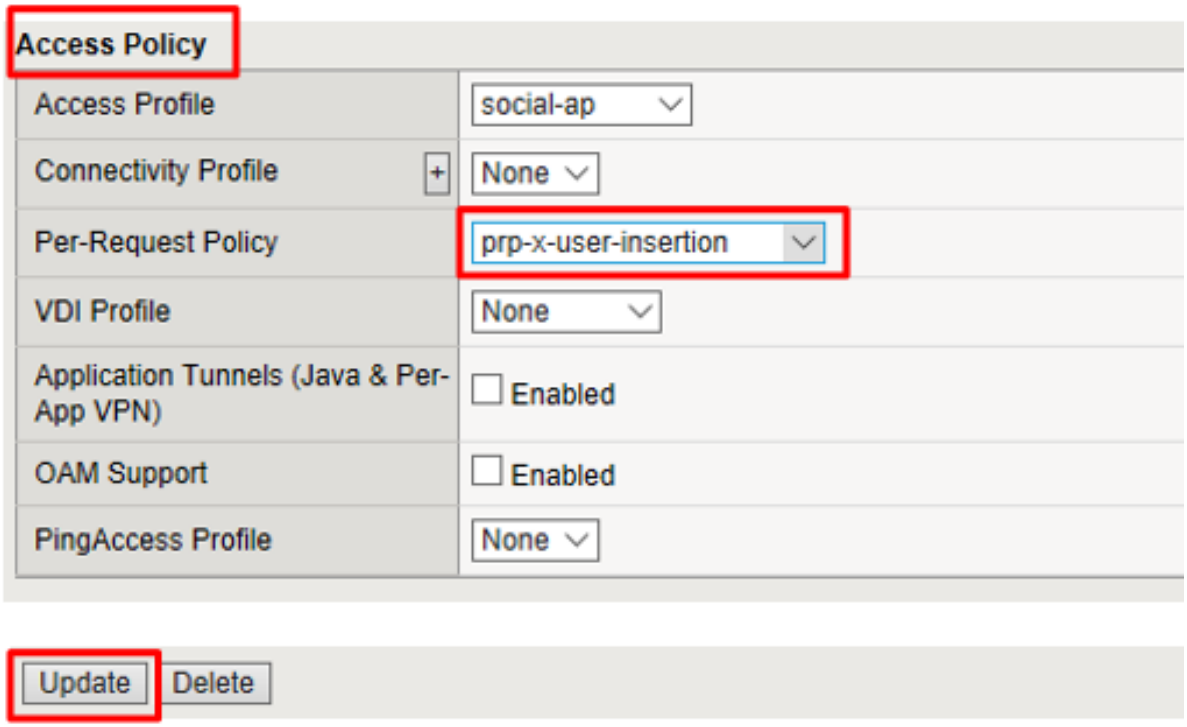


Add the Per Request Policy to the Virtual Server

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

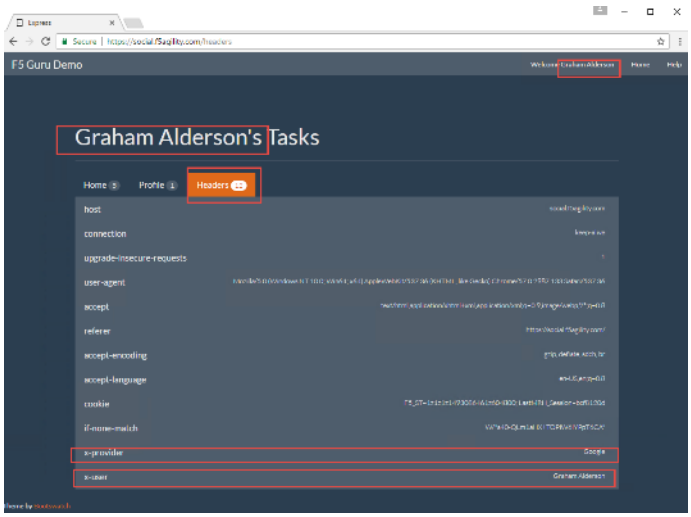


2. Scroll to the **Access Policy** section of the Virtual Server and select `prp-x-user-insertion` from the **Per-Request Policy** drop down. Scroll to the bottom of the page and click **Update**



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

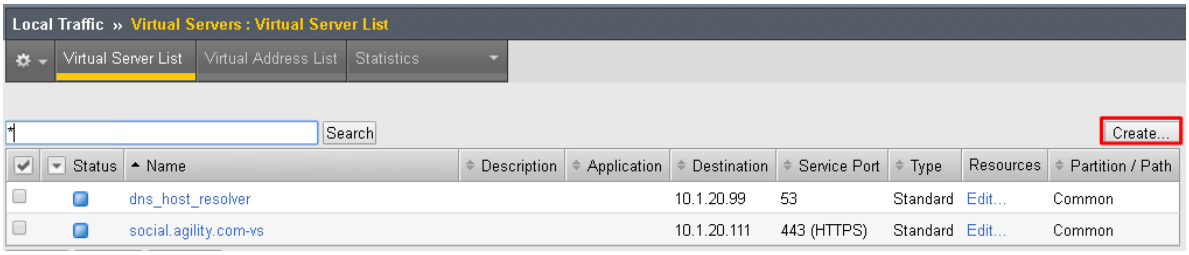
2.3.1 Purpose

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.

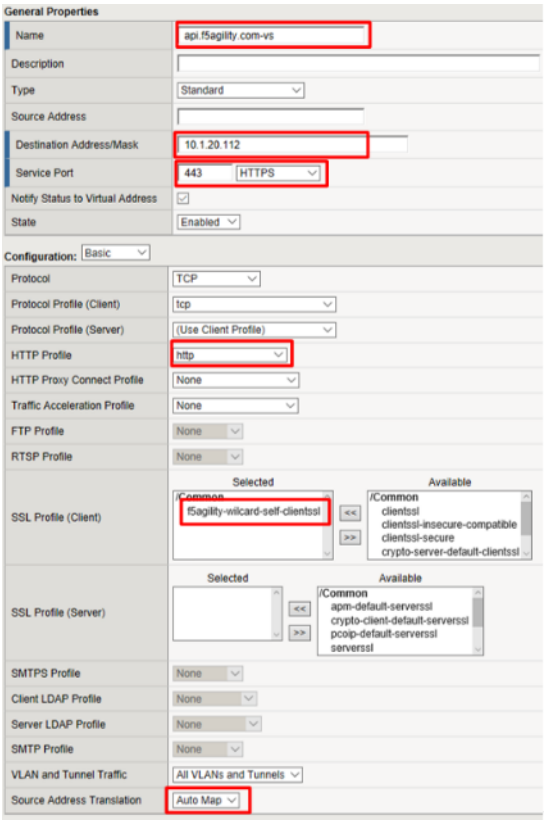
2.3.2 Task 1: Setup Virtual Server for the API

Create the Virtual Server

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

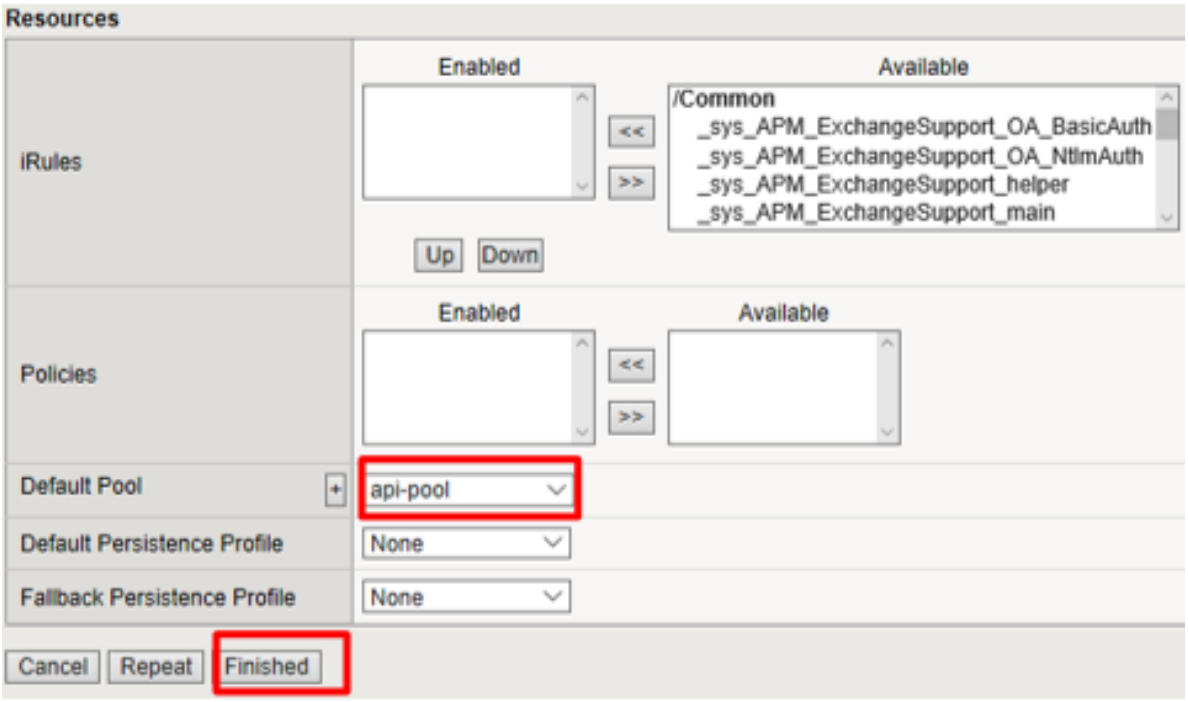


2. Enter the following values *(leave others default)* then scroll down to **Resources**
   - **Name:** `api.f5agility.com-vs`
   - **Destination Address:** `10.1.20.112`
   - **Service Port:** `443`
   - **HTTP Profile:** `http`
   - **SSL Profile (Client):** `f5agility-wildcard-self-clientssl`
   -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

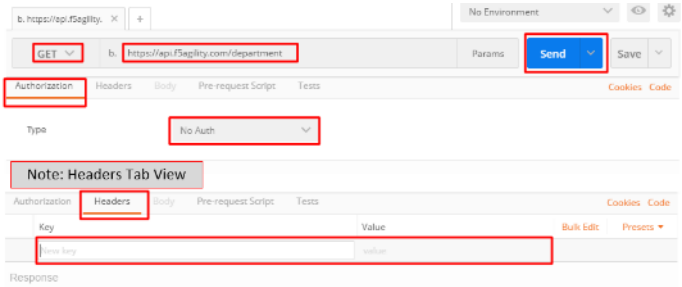
2. The request should be prefilled with the settings below. If not change as needed or select **TEST API Call** from the **API Collection** and click **Send**

   Method: `GET`

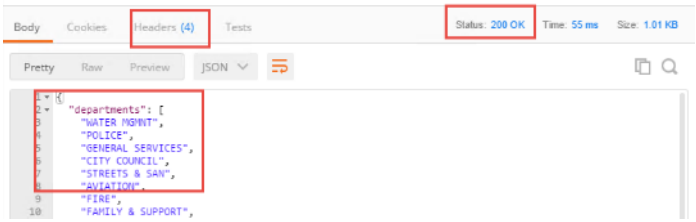
   Target: `https://api.f5agility.com/department`

   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.



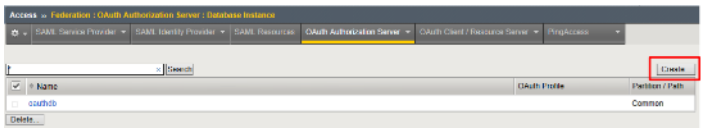
Note: This request is working because we have not yet provided any protection for the API.*

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**.*

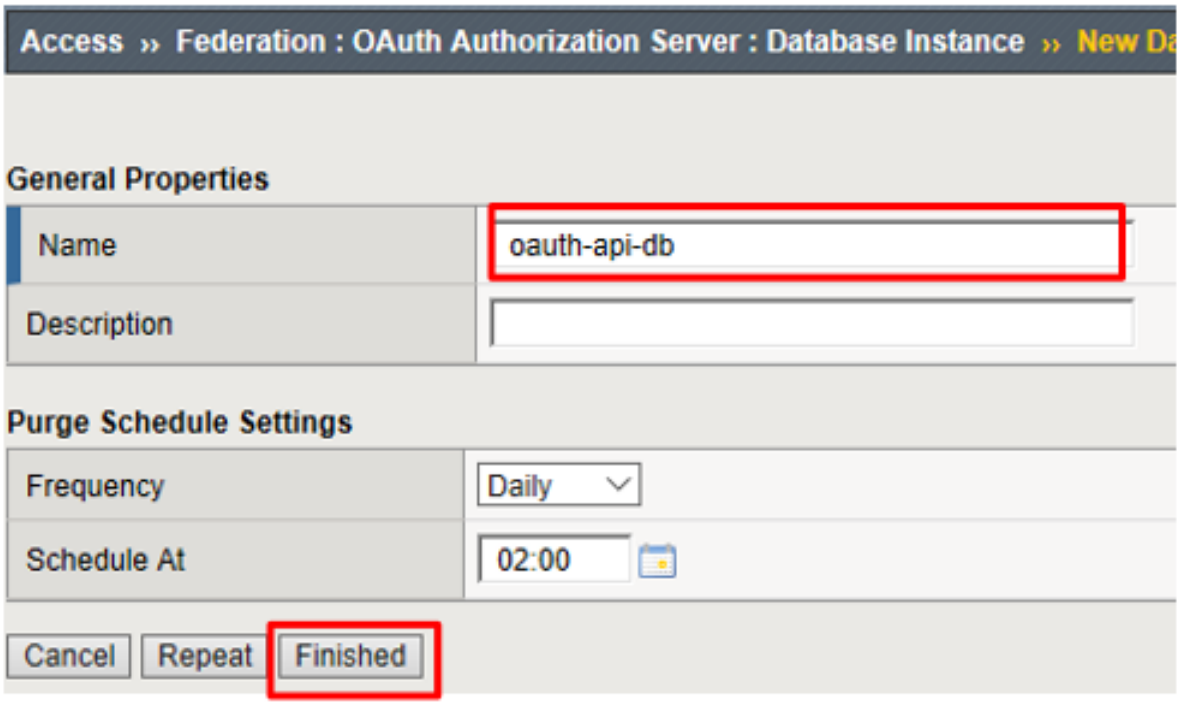
2.3.3 Task 2: Authorization Server

Configure the Database Instance

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

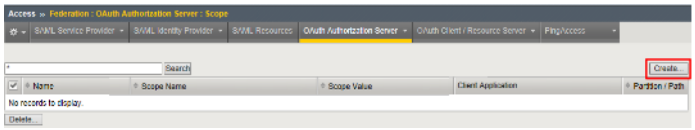


2. Enter oauth-api-db for the **Name** field and click **Finished**.

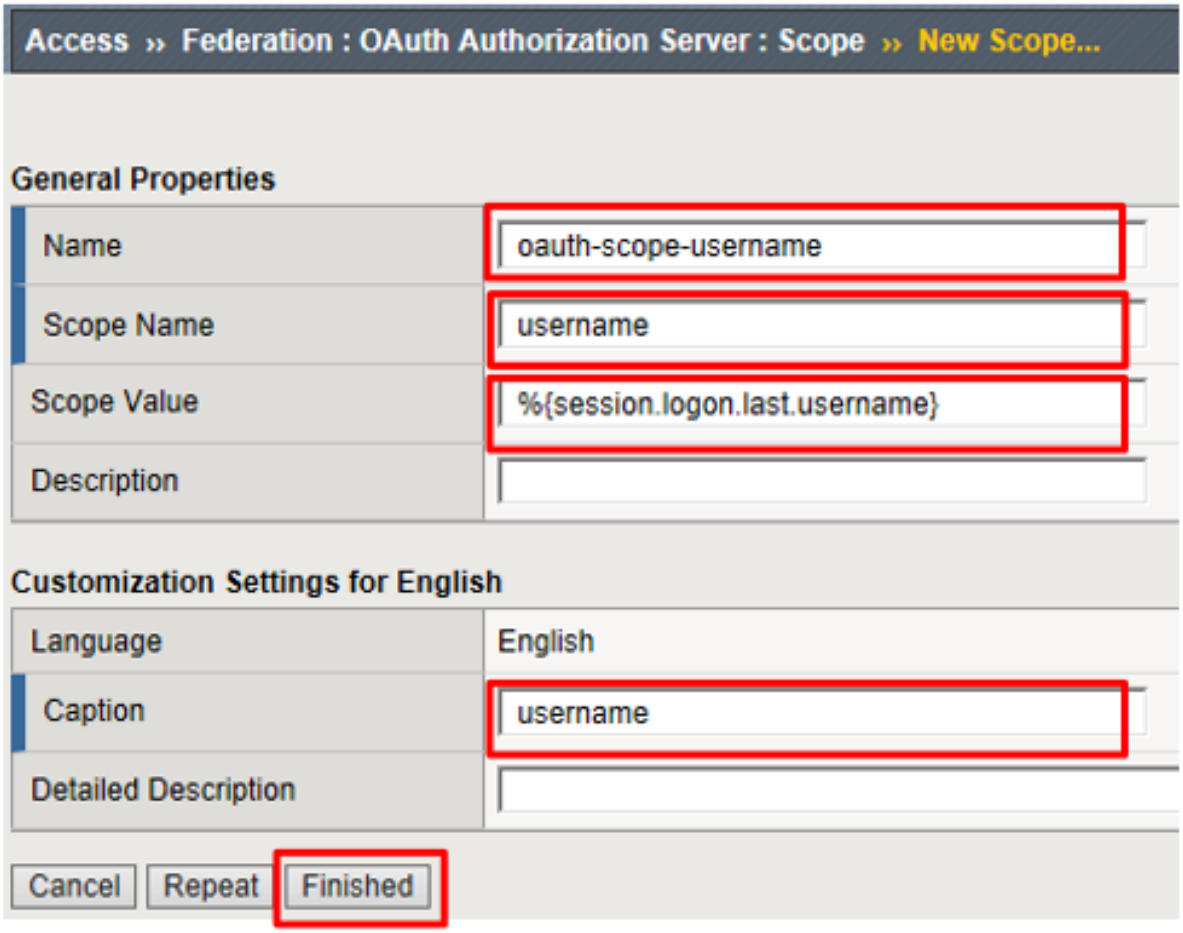


Configure the Scope

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



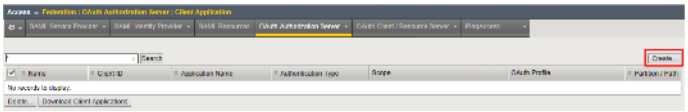
2. Enter the following values and and click **Finished**.
    - **Name:** `oauth-scope-username`
    - **Scope Name:** `username`
    - **Scope Value:** `%{session.logon.last.username}`
    - **Caption:** `username`



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

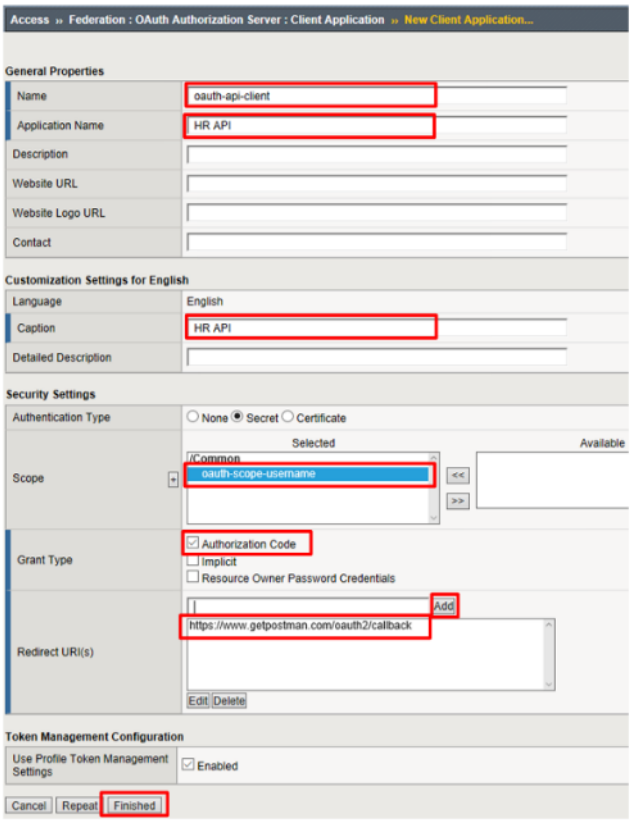
1. Go to **Access** -> Federation -> **OAuth Authorization Server -> Client Application** and click **Create**



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`

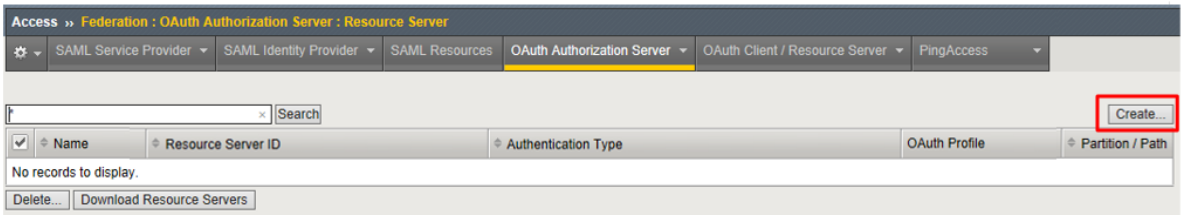
Remember to click Add



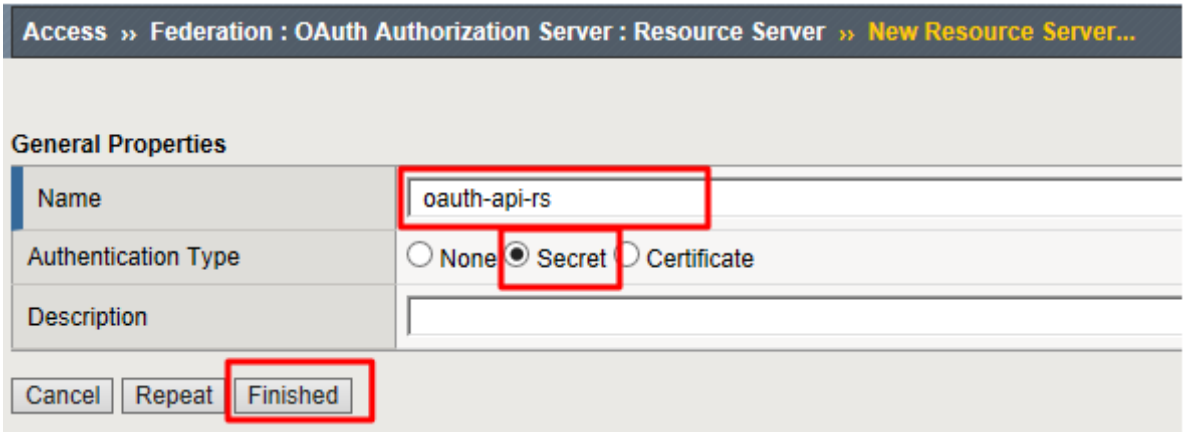
Note: The Redirect URI above is a special URI for the Postman client you'll be using. This would normally be a specific URI to your client

Configure the Resource Server

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

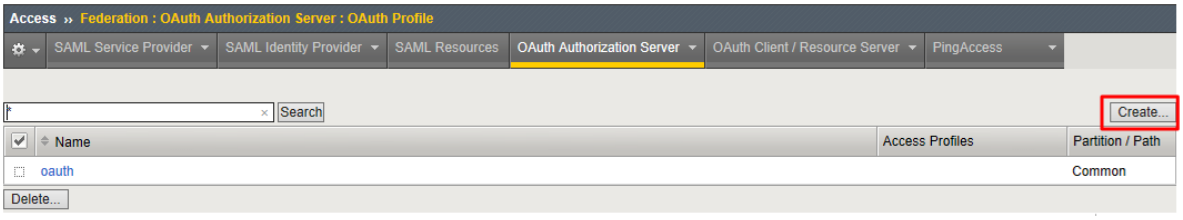


2. Enter the following values and click **Finished**.
   - **Name:** `oauth-api-rs`
   - **Application Type:** `Secret`

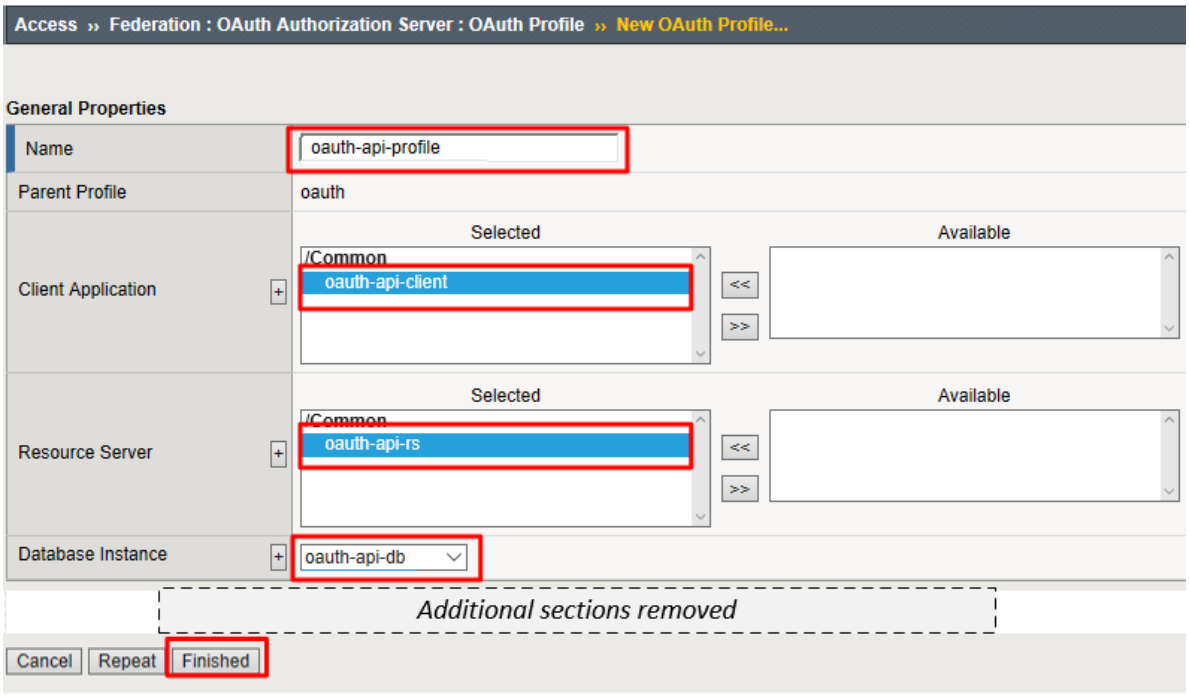


Configure the OAuth Profile

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

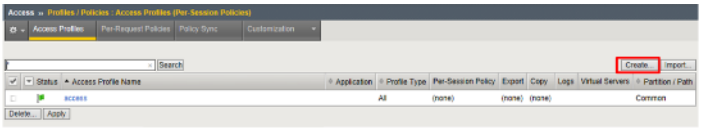


2. Enter the following values and click **Finished**.
    - **Name:** `oauth-api-profile`
    - **Client Application:** `oauth-api-client`
    - **Resource Server:** `oauth-api-rs`
    - **Database Instance:** `oauth-api-db`

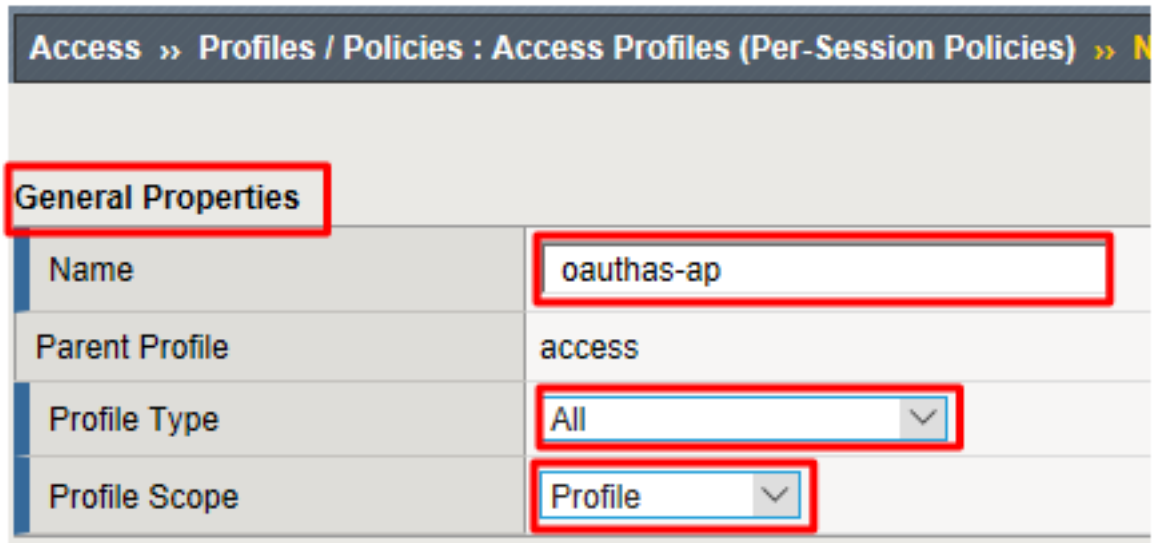


Configure the APM Per Session Policy

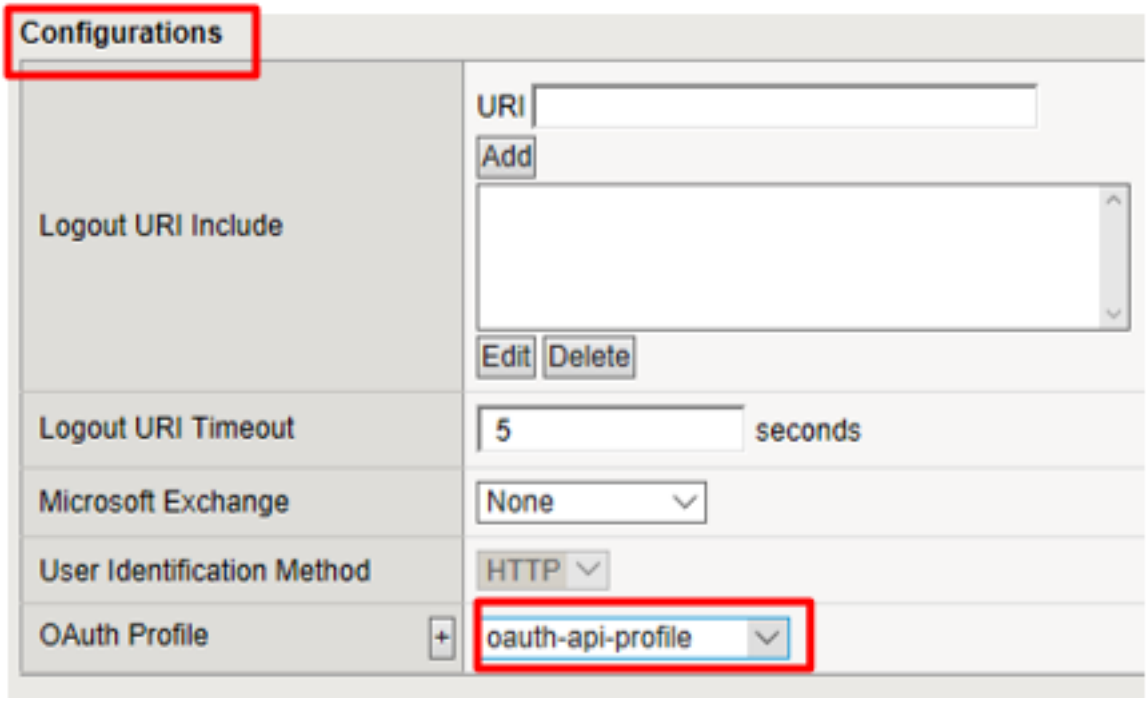
1. Go to **Access -> Profiles/Policies -> Access Profiles (Per Session Policies)** and click **Create**



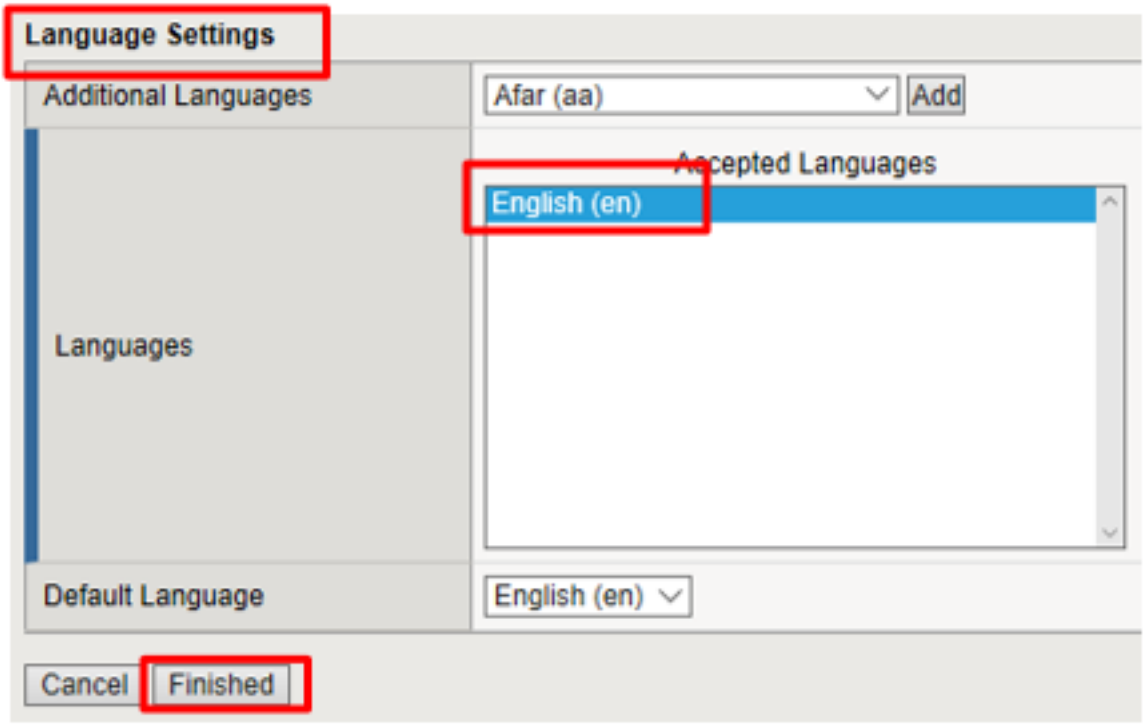
2. In the **General Properties** section enter the following values
   - **Name:** `oauthas-ap`
   - **Profile Type:** `All`
   - **Profile Scope:** `Profile`



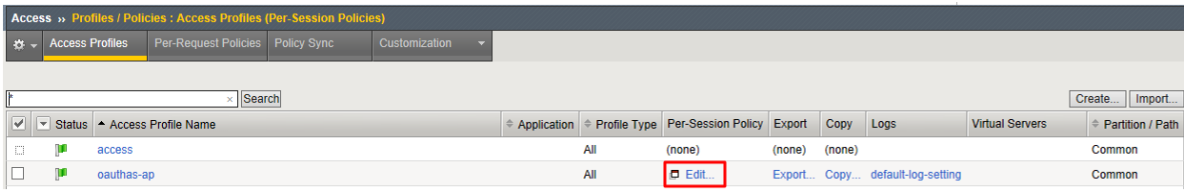
3. In the **Configurations** section select the following value from the **OAuth Profile** drop down menu.
   - **OAuth Profile:** `oauth-api-profile`



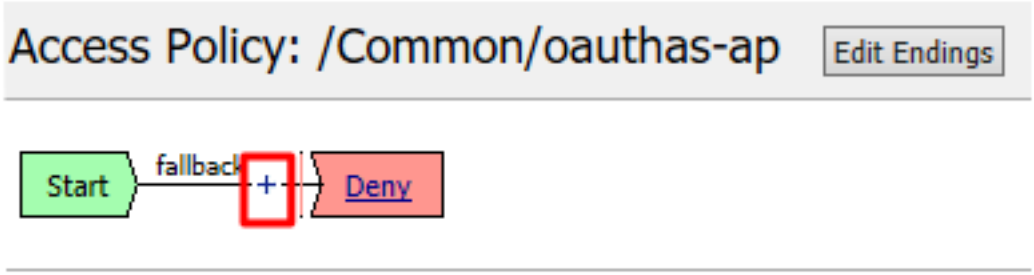
4. In the **Language Settings** section enter the following value and then click **Finished**.
   - **Languages:** `English`



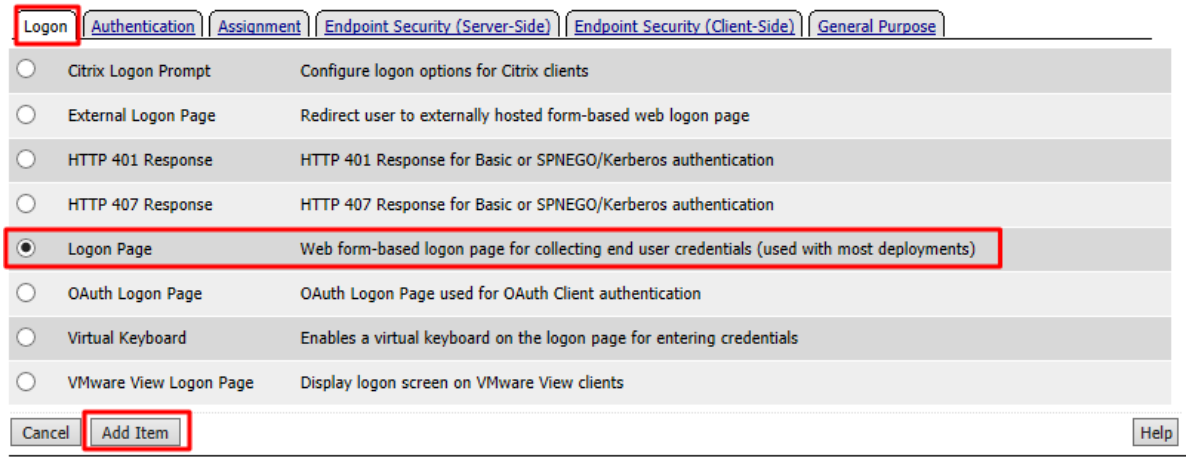
5. Click **Edit** on the **oauthas-ap** policy, a new browser tab will open.



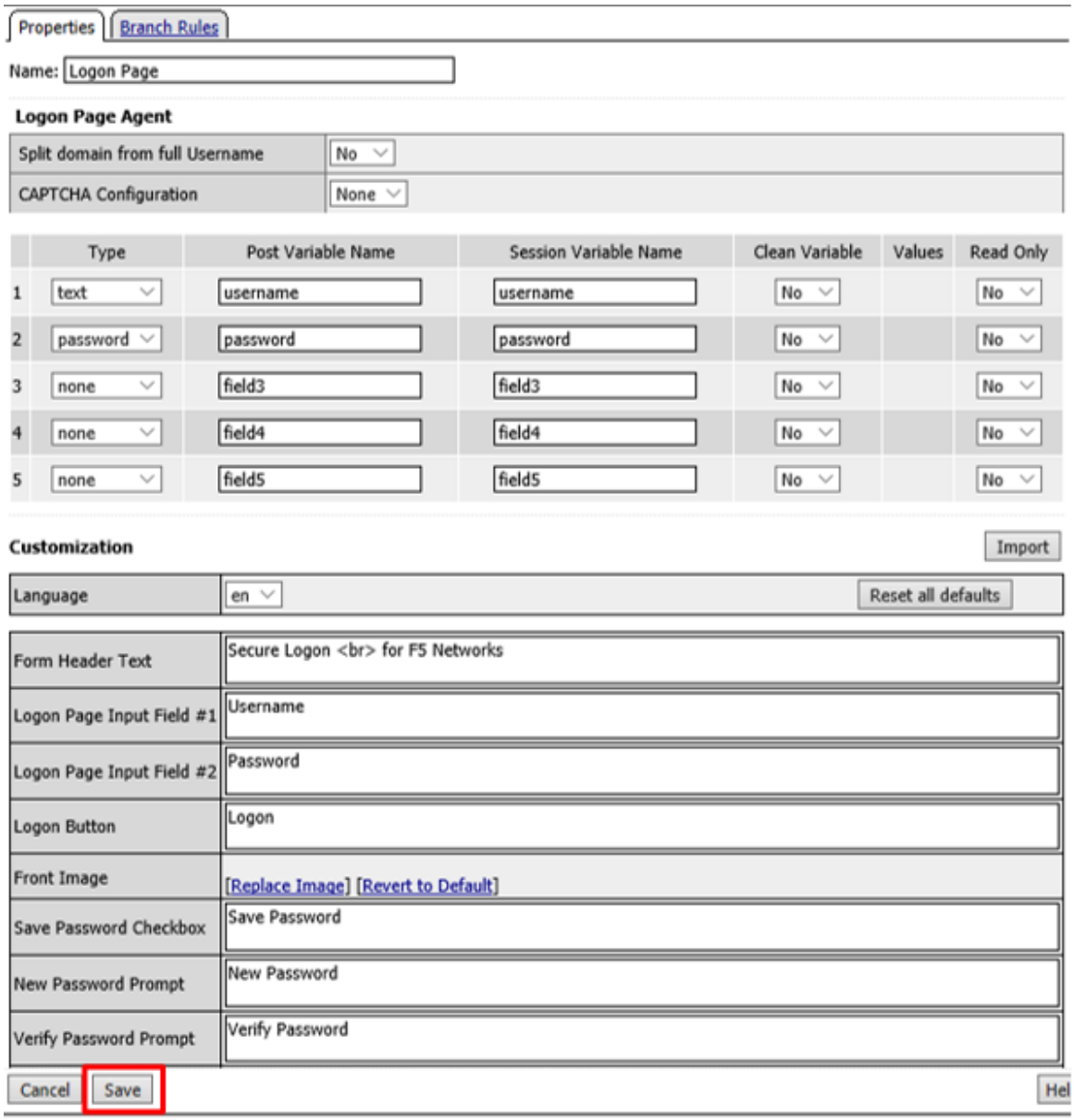
6. Click the **+** between **Start** and **Deny**



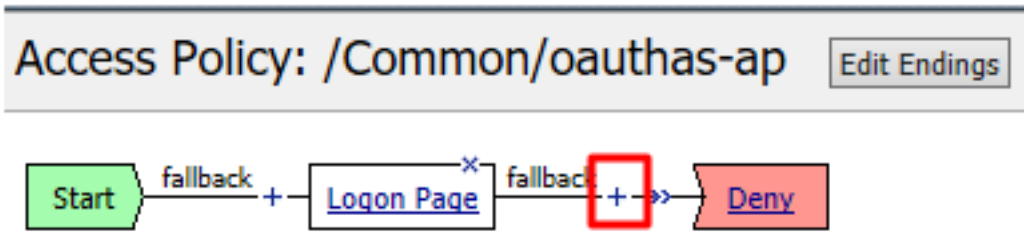
7. Select **Logon Page** from the **Logon** tab, and click **Add Item**



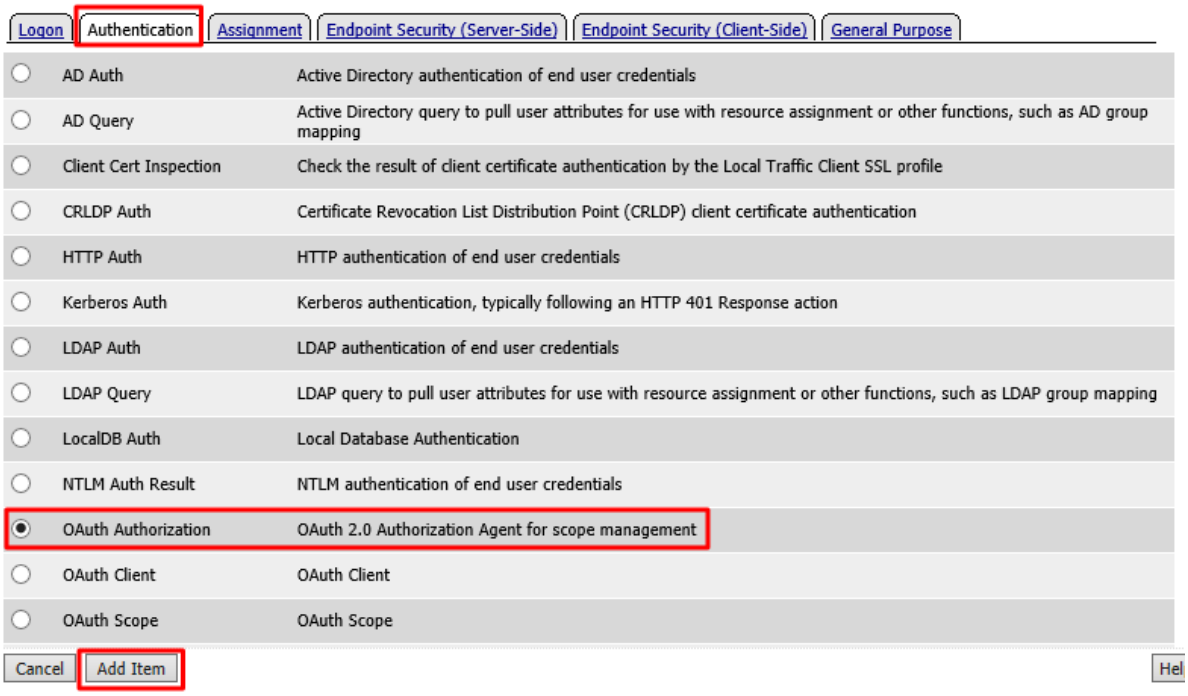
8. Accept the defaults on the **Logon Page** and click **Save**



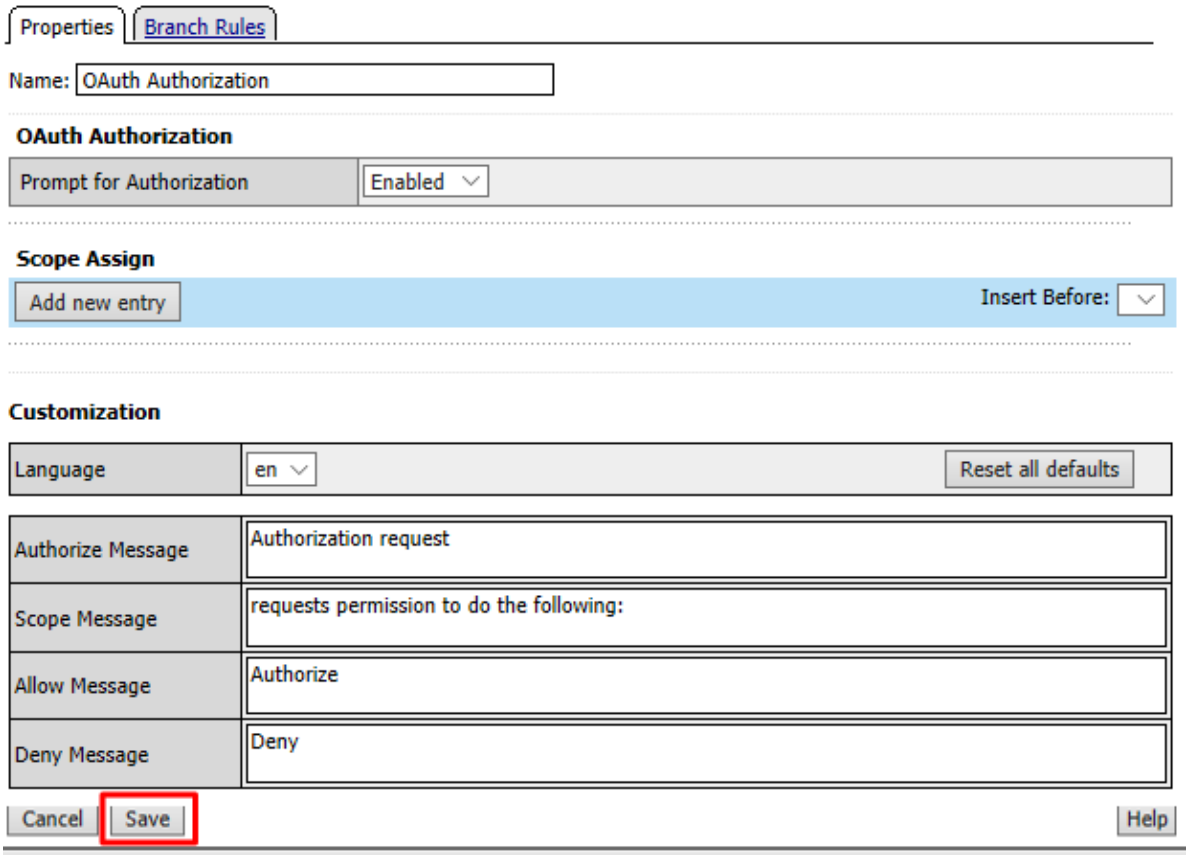
9. Click the **+** between **Logon Page** and **Deny**



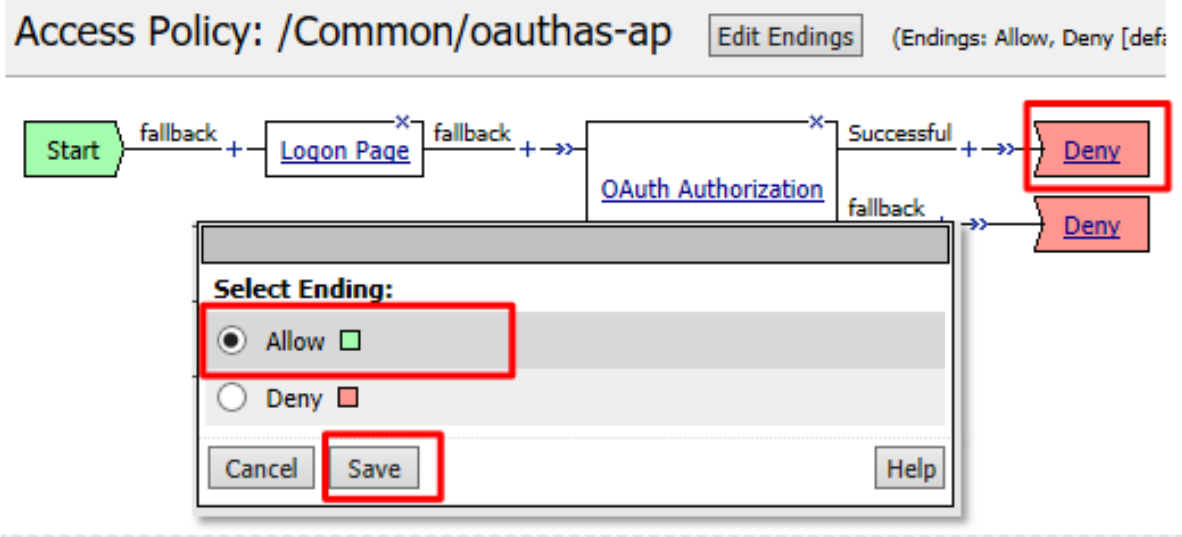
10. Select **OAuth Authorization** from the **Authentication** tab and click **Add Item**



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

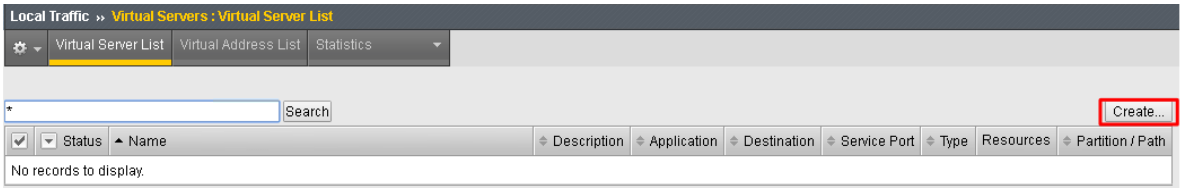
Note: We are not validating the credentials entered on the Logon Page, so you can enter anything you want. In a production deployment you would most likely include some process for validating credentials such as an LDAP Auth or AD Auth object, or perhaps limiting access by IP or client certificate

---

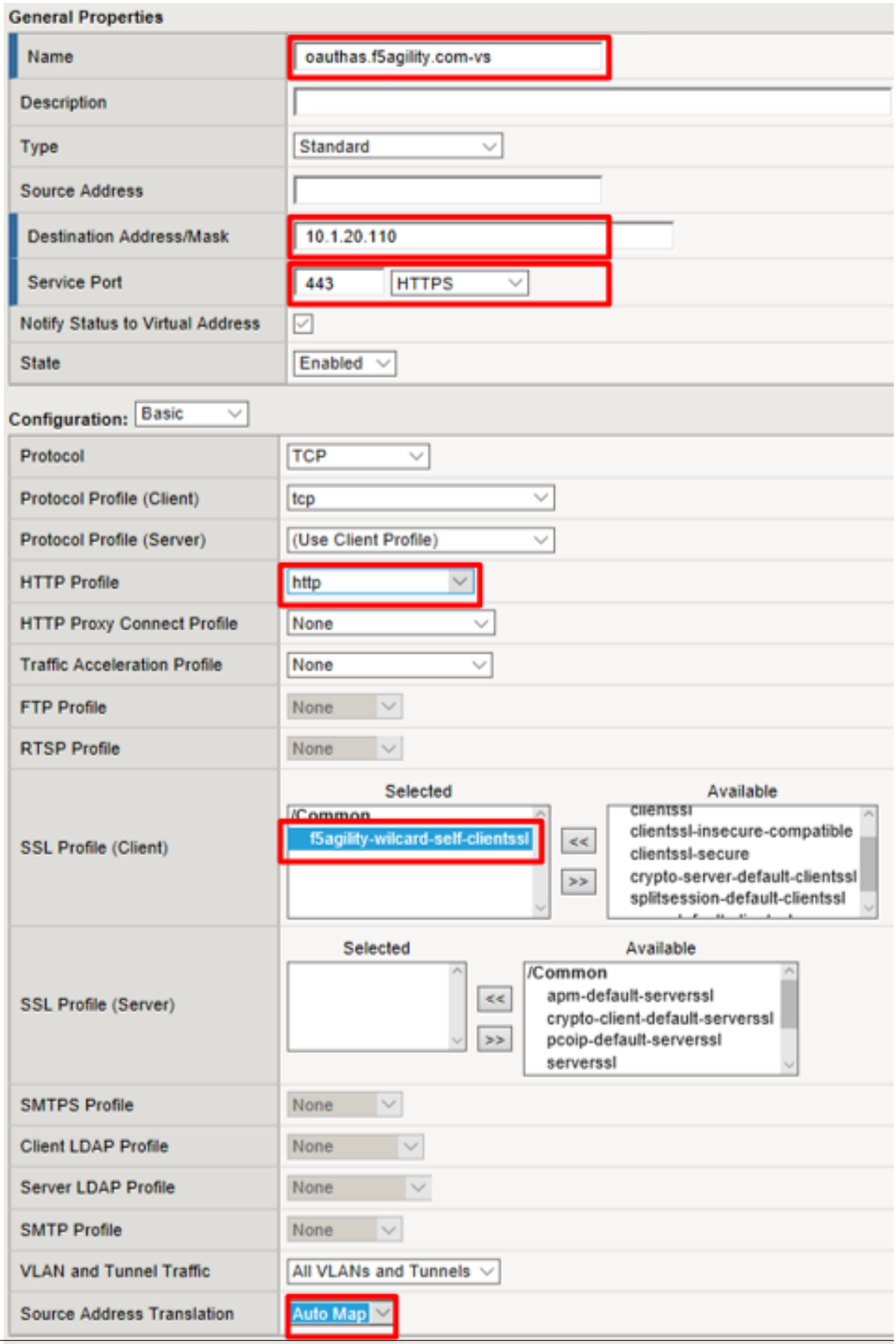
Note: This policy might also set some variables that get used as scope values. Thus, you could determine what the scope values are by utilizing the policy here.*

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`

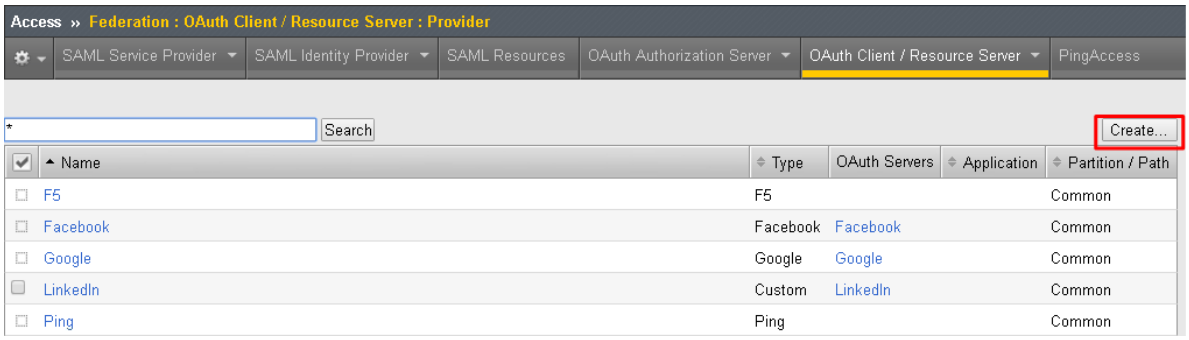

General Properties
Name
oauthas.f5agility.com-vs
Description
Type
Standard
Source Address
Destination Address/Mask
10.1.20.110
Service Port
443
HTTPS
Notify Status to Virtual Address
State
Enabled
Configuration:
Basic
Protocol
TCP
Protocol Profile (Client)
tcp
Protocol Profile (Server)
(Use Client Profile)
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-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

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.

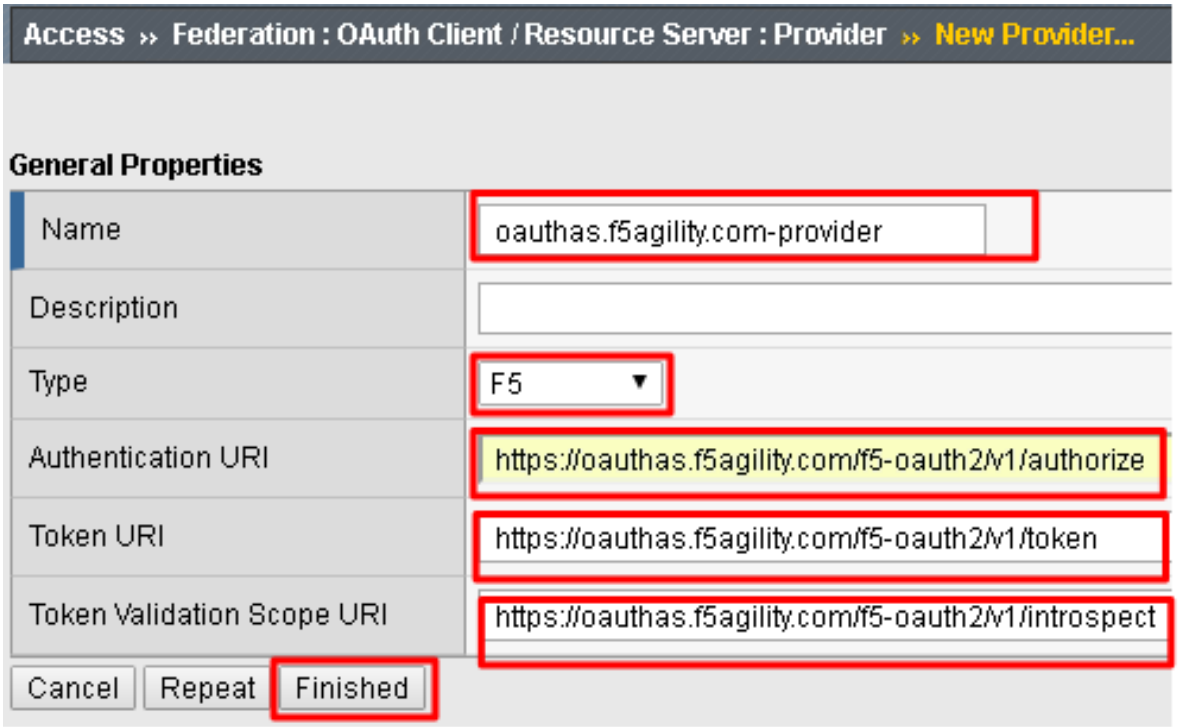
2.3.4 Task 3: Resource Server

Configure the OAuth Provider

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

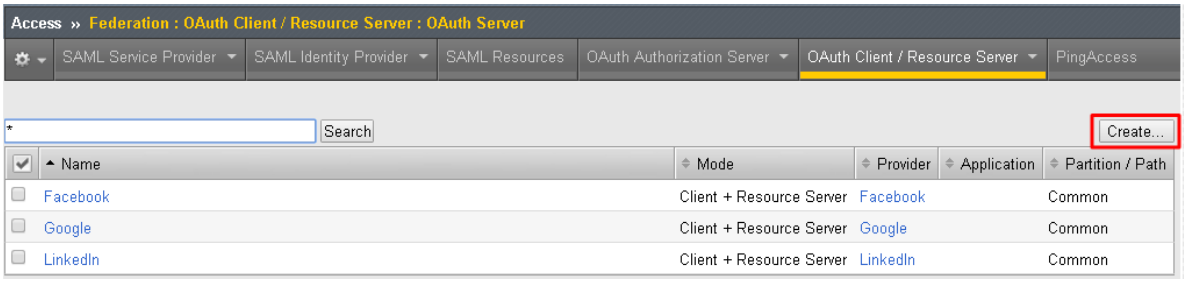


2. Enter the following values for the Authorization Server Virtual Server and then click **Finished**
   - **Name:** `oauthas.f5agility.com-provider`
   - **Type:** `F5`
   - **Authentication URI:** `https://oauthas.f5agility.com/f5-oauth2/v1/authorize`
   - **Token URI:** `https://oauthas.f5agility.com/f5-oauth2/v1/token`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

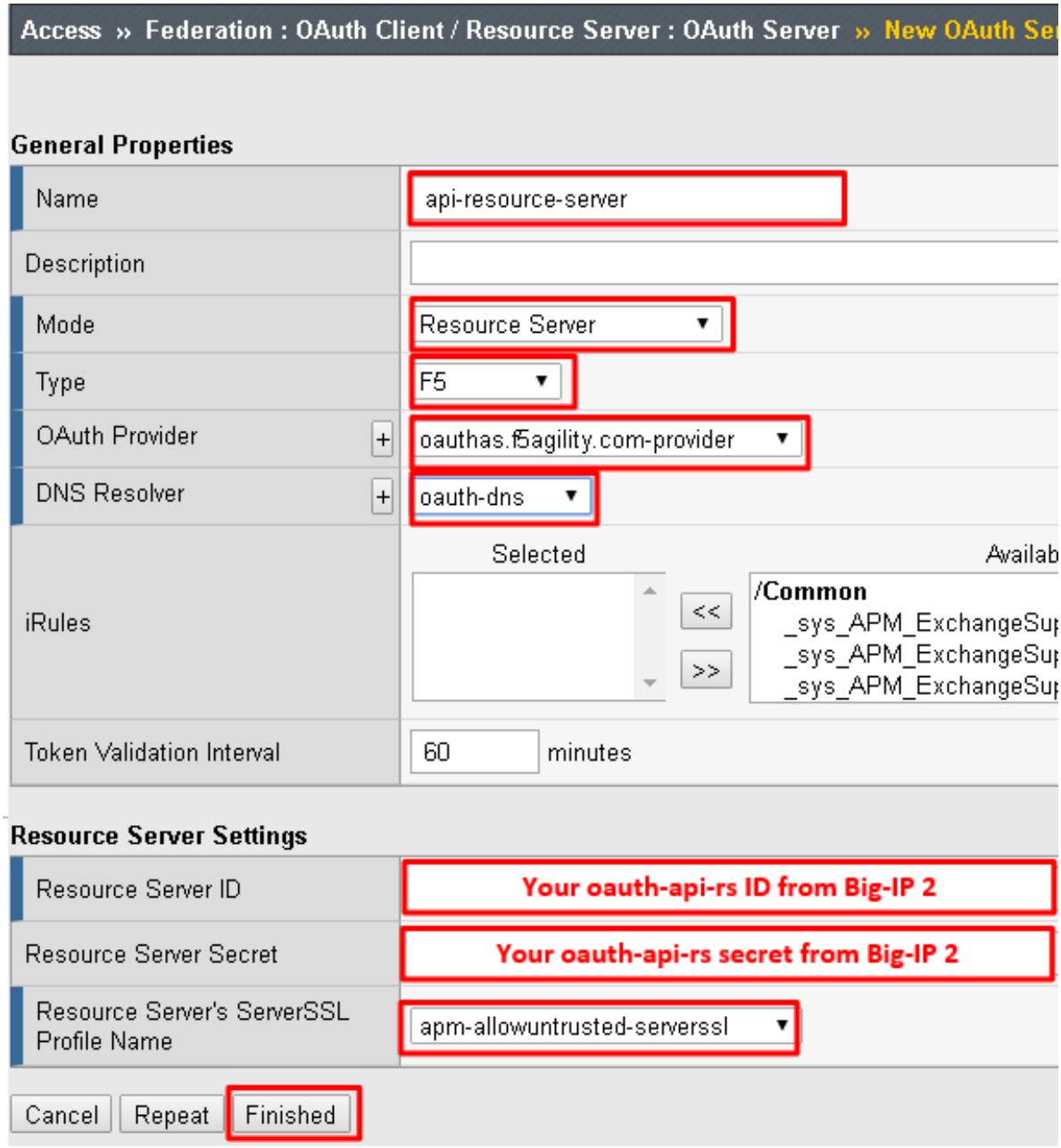


Configure the OAuth Server

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



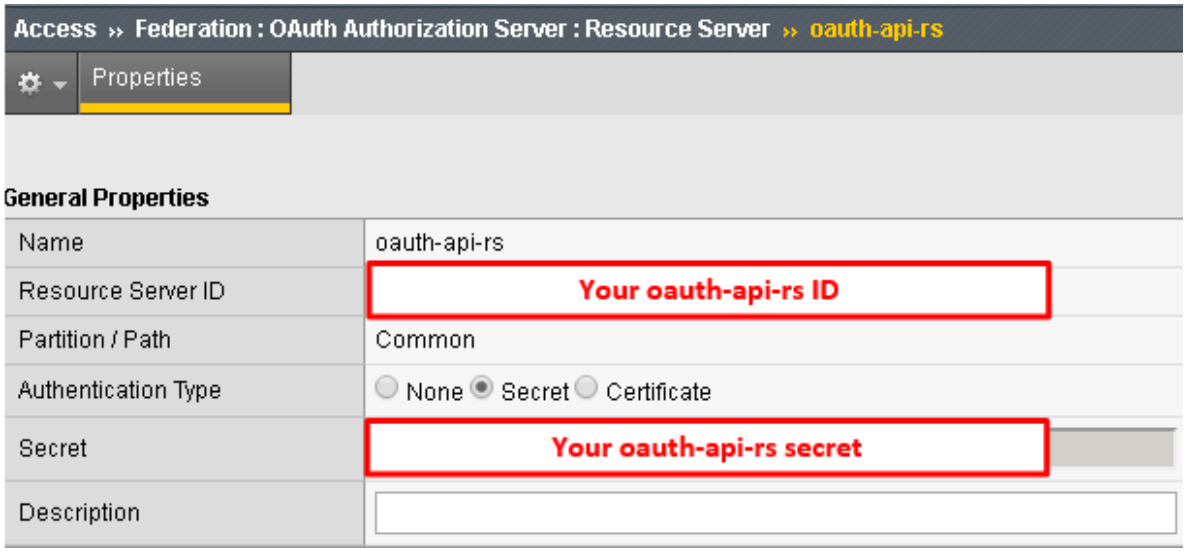
2. Enter the following values for the Authorization Server Virtual Server and then click **Finished**
   - **Name:** `api-resource-server`
   - **Mode:** `Resource Server`
   - **Type:** `F5`
   - **OAuth Provider:** `oauthas.f5agility.com-provider`
   - **DNS Resolver:** `oauth-dns`
   - **Resource 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



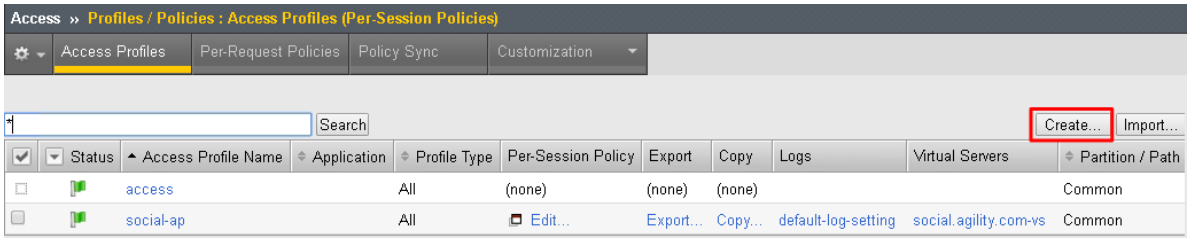
Note: We are using a custom serverssl profile to allow negotiation with an untrusted certificate. This is needed because our Authorization Server is using a self-signed certificate. In production for proper security you should leverage a trusted certificate (most likely publicly signed) and the apm-default-serverssl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

---

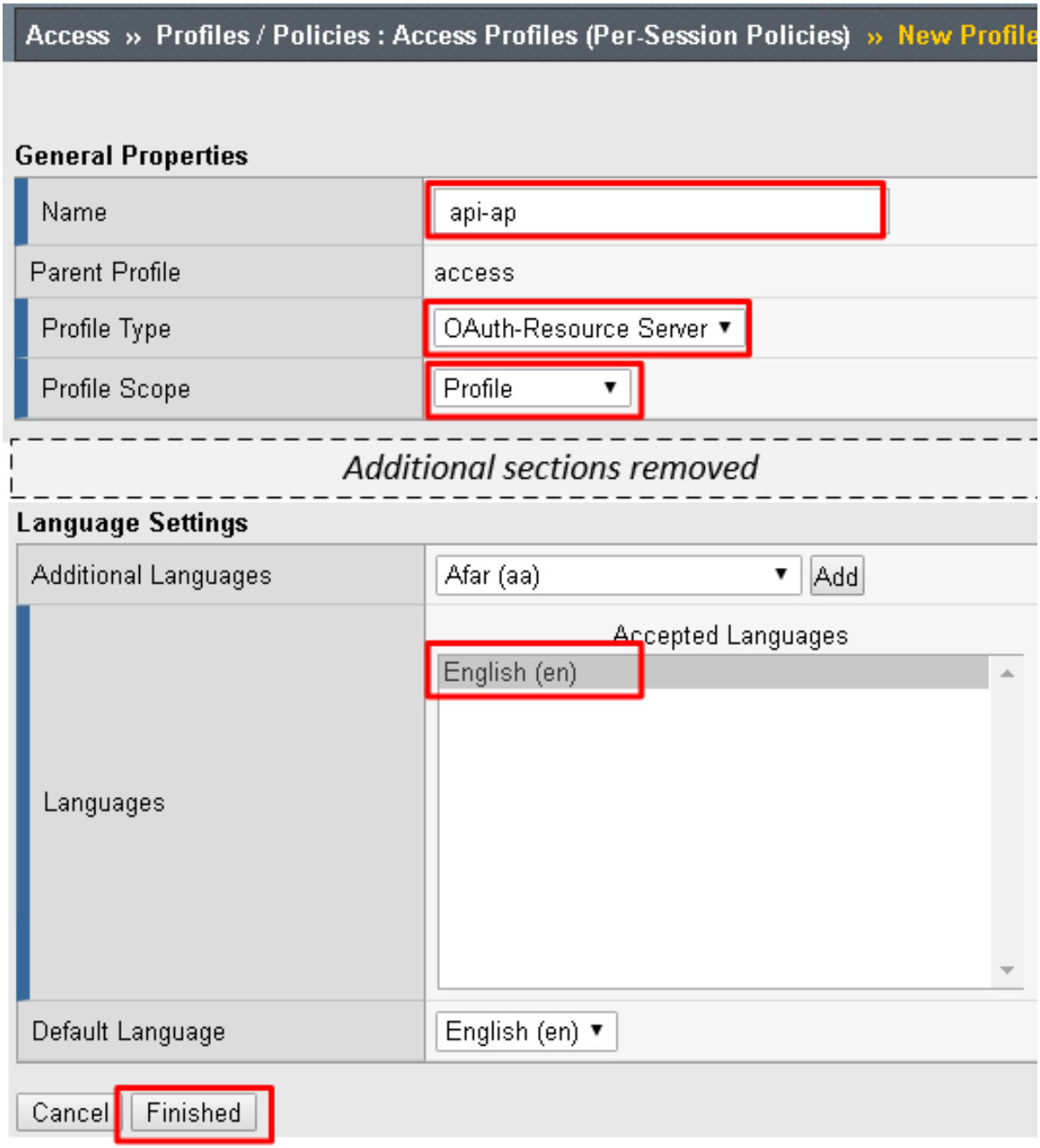
3. The values for step 4 above can be obtained by accessing Big-IP 2 and navigating to **Access -> Federation -> OAuth Authorization Server -> Resource Server -> oauth-api-rs** as shown.



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



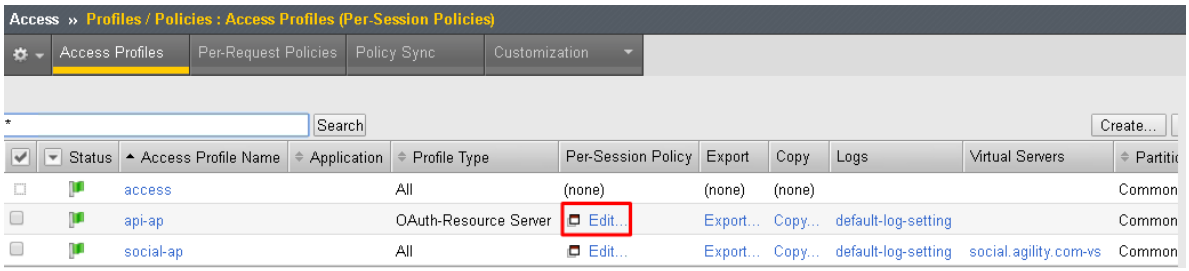
5. Enter the following values and then click **Finished**



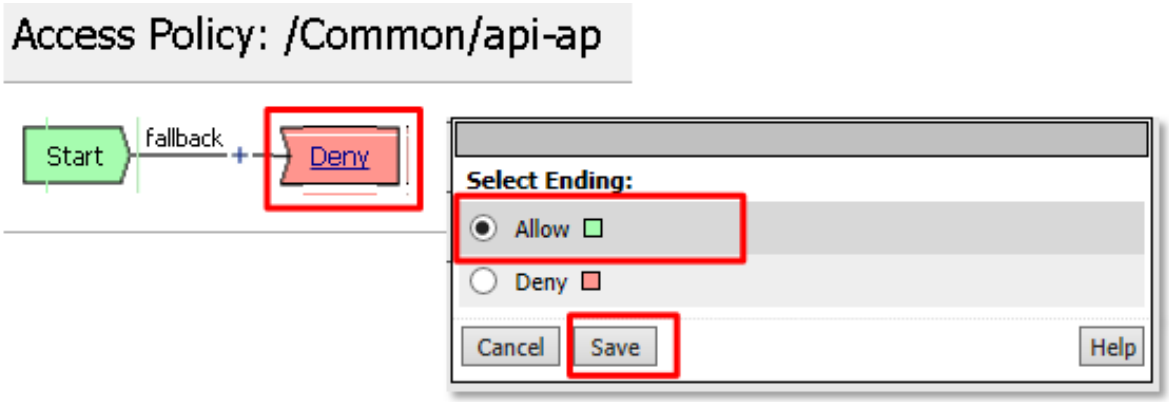
- **Name:** `api-ap`
- **Profile Type:** `OAuth-Resource-Server`
- **Profile Scope:** `Profile`
- **Languages:** `English`

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

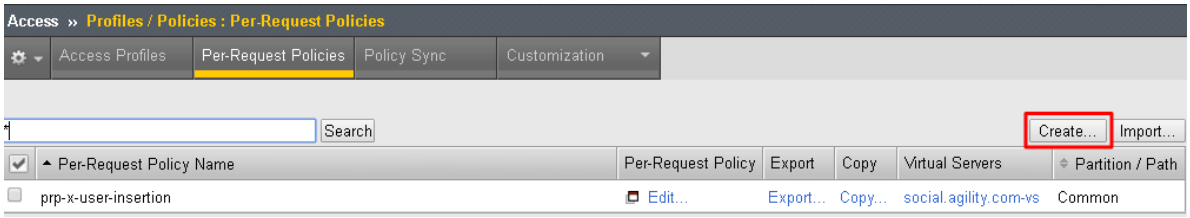


7. Click **Deny** on the fallback branch after **Start**, select **Allow** and click **Save**

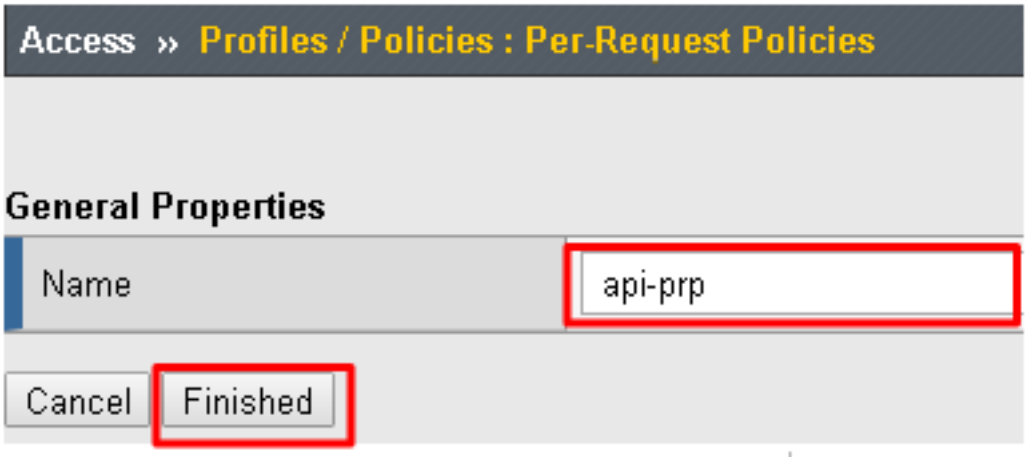


8. Click **Apply Access Policy** in the top left and then close the tab

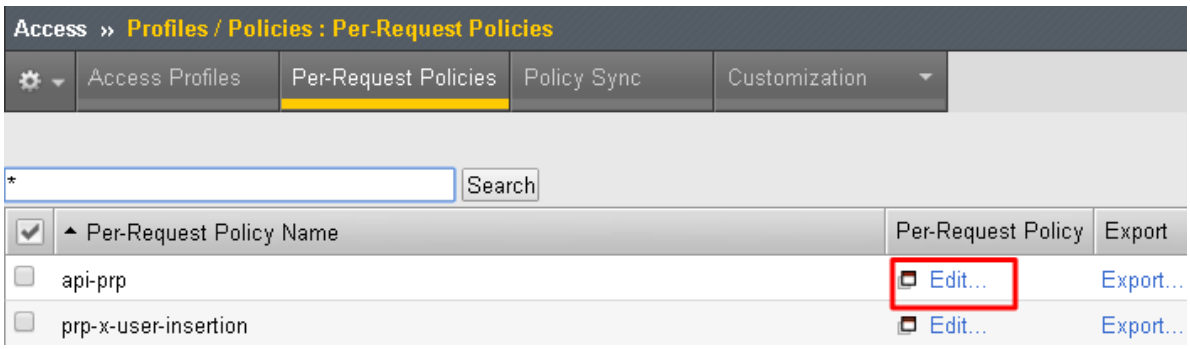
9. To configure the **APM Per Request Policy** go to **Access -> Profiles / Policies -> Per Request Policies** and then click **Create**



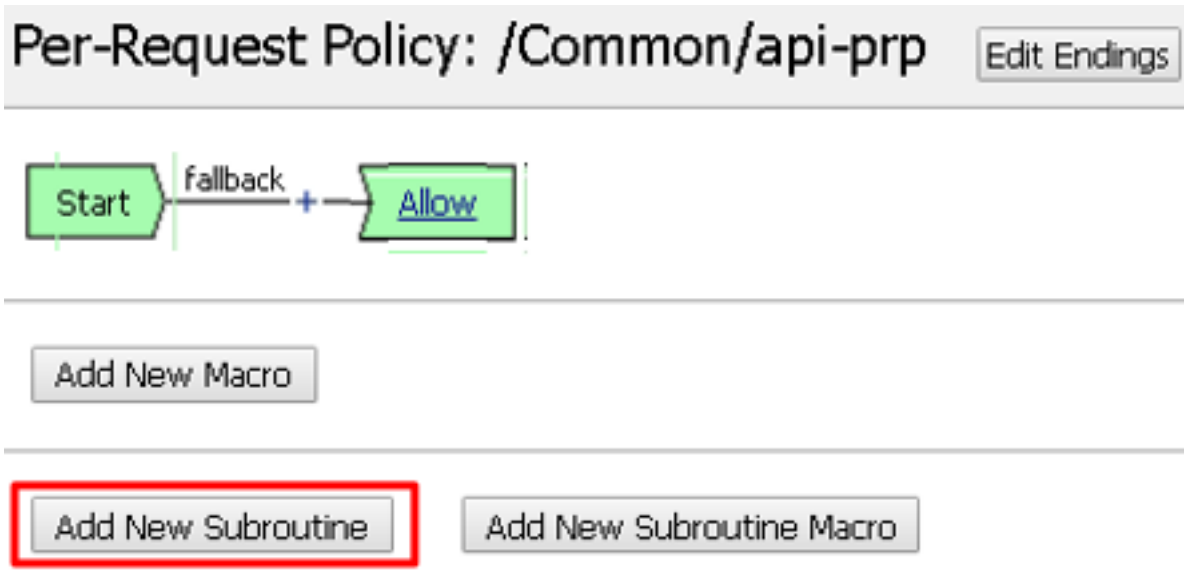
10. Enter api-prp for the **Name** and click **Finished**



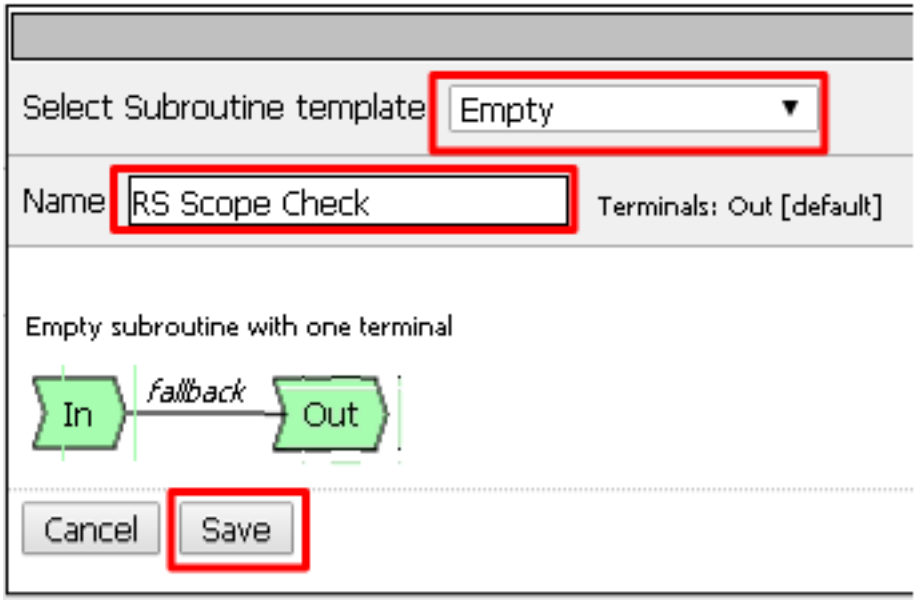
11. Click **Edit** on the **api-prp** policy and a new window will appear



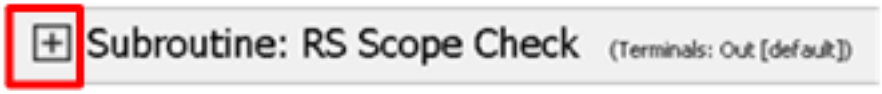
12. Click **Add New Subroutine**



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

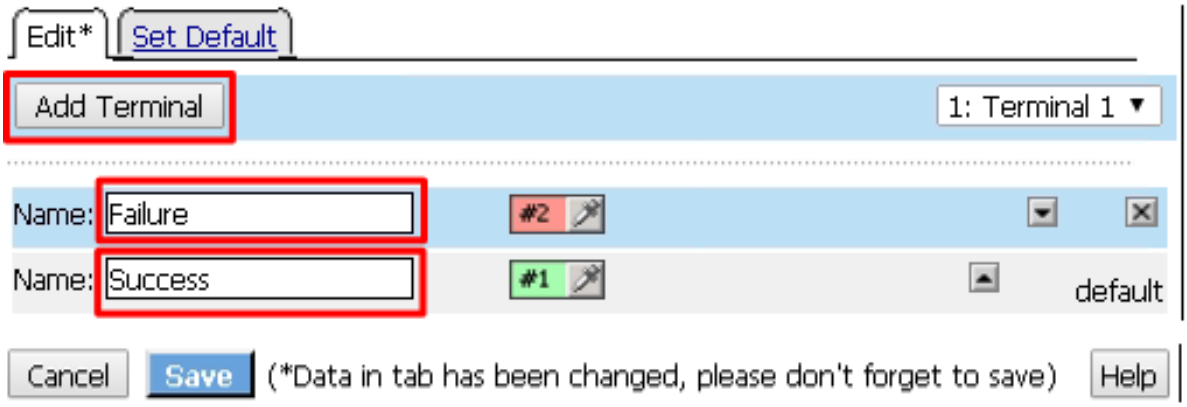


14. Click the **+** next to the **RS Scope Check**

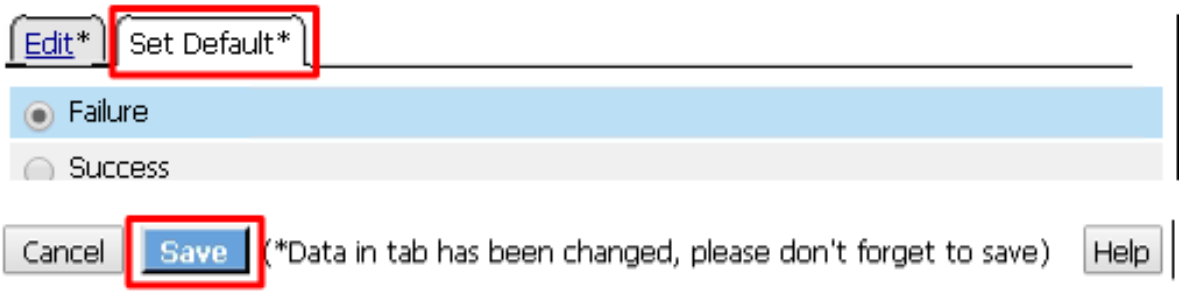


15. Click Edit Terminals on the RS Scope Check Subroutine

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

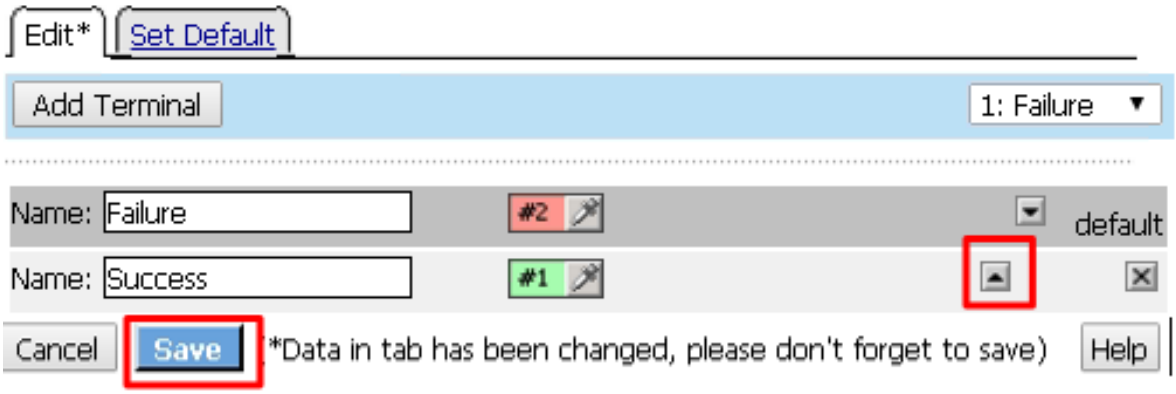


17. Go to the **Set Default** tab and select **Failure** then click Save

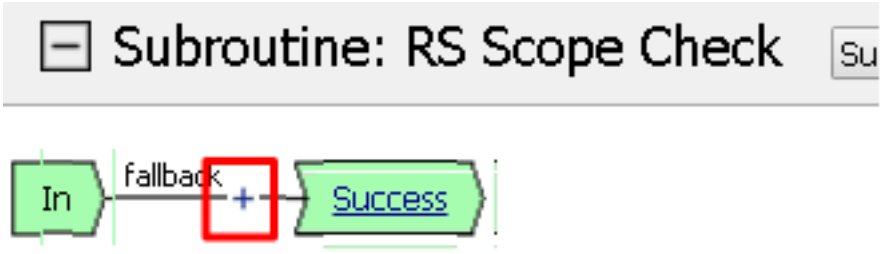


18. Click **Edit Terminals** again *(it will ignore the order settings if you do this in one step without saving in between)*

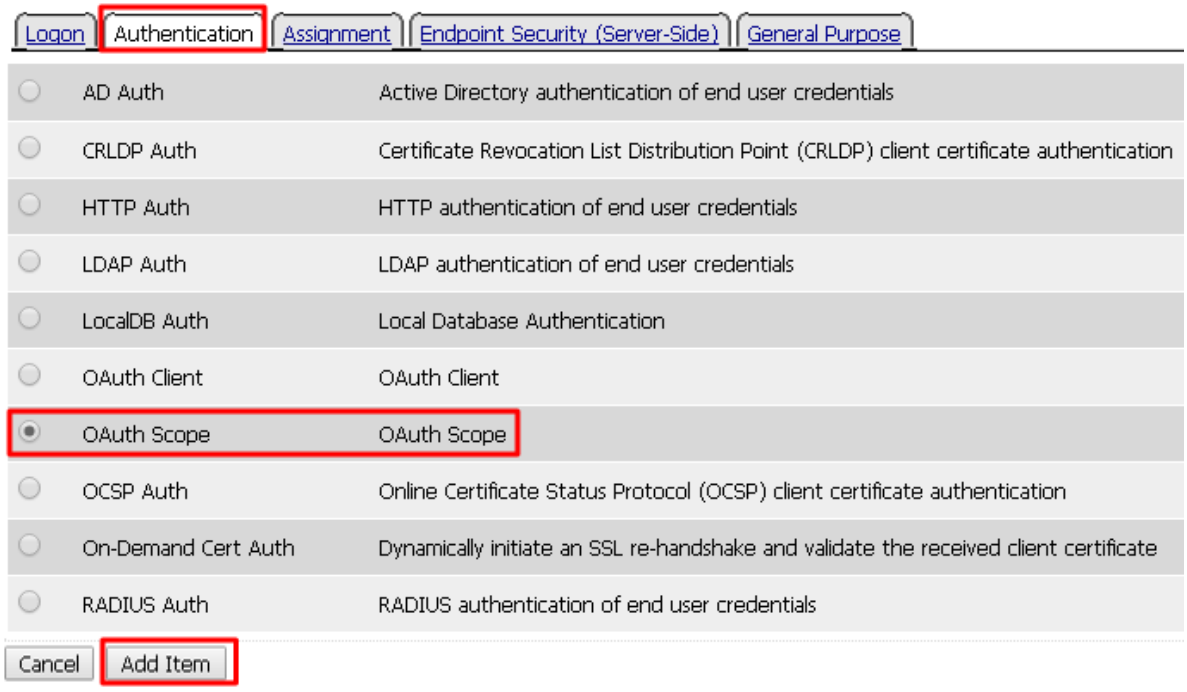
19. Move **Success** to the top using the up arrow on the right side then click **Save**



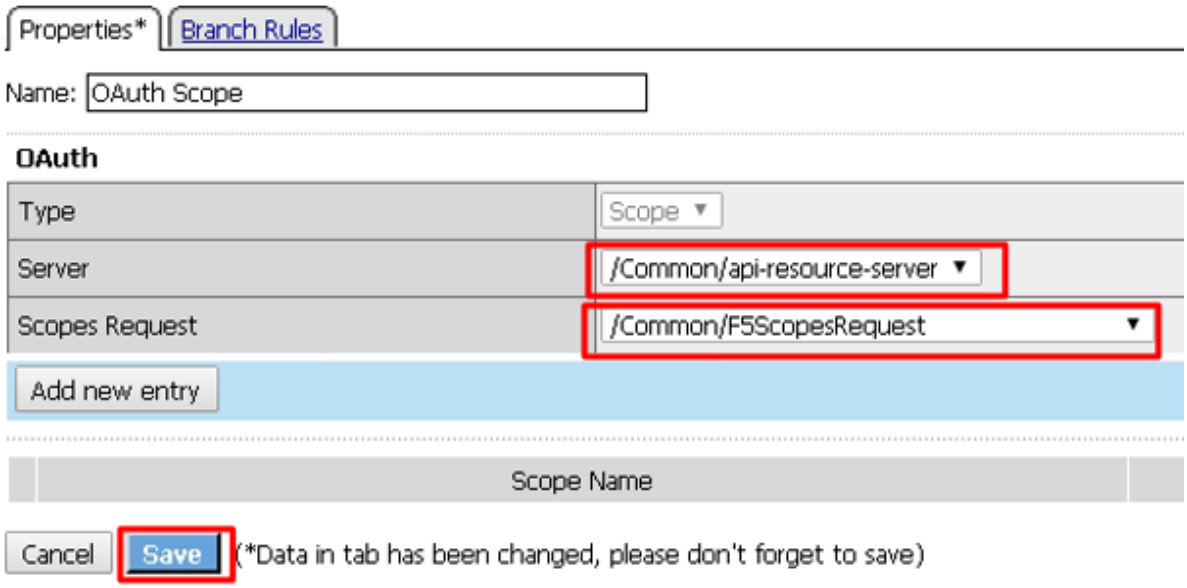
20. Click the **+** between **In** and **Success**, a new window will appear



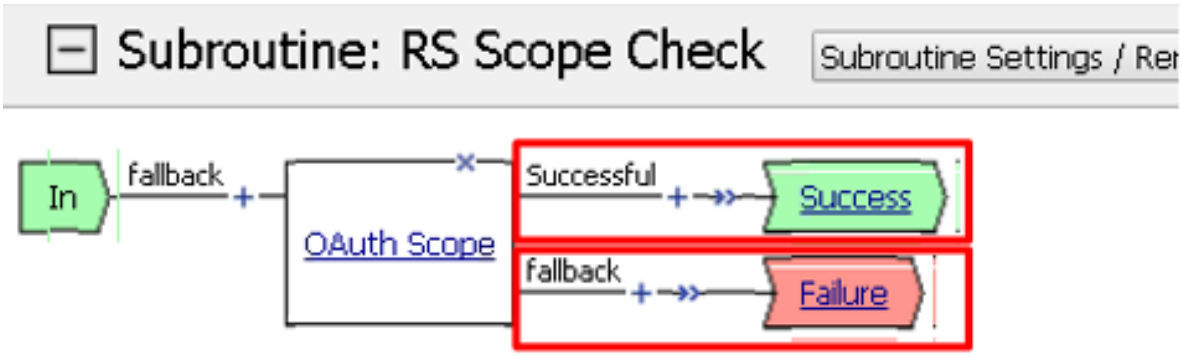
21. Select **OAuth Scope** from the **Authentication** tab and click **Add Item**



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

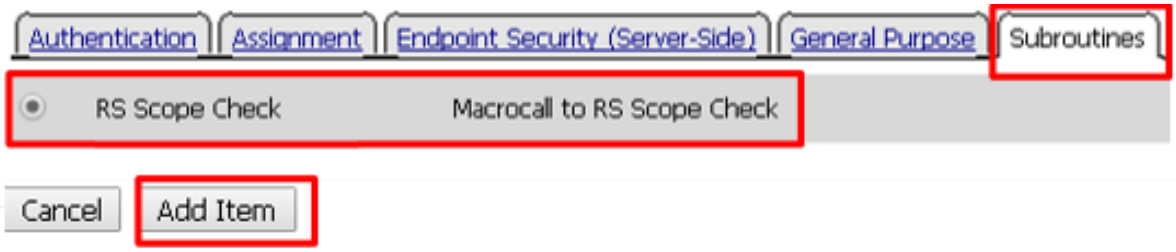


23. Verify that the **Successful** branch terminates in **Success** and the **Fallback** branch terminates in **Failure**

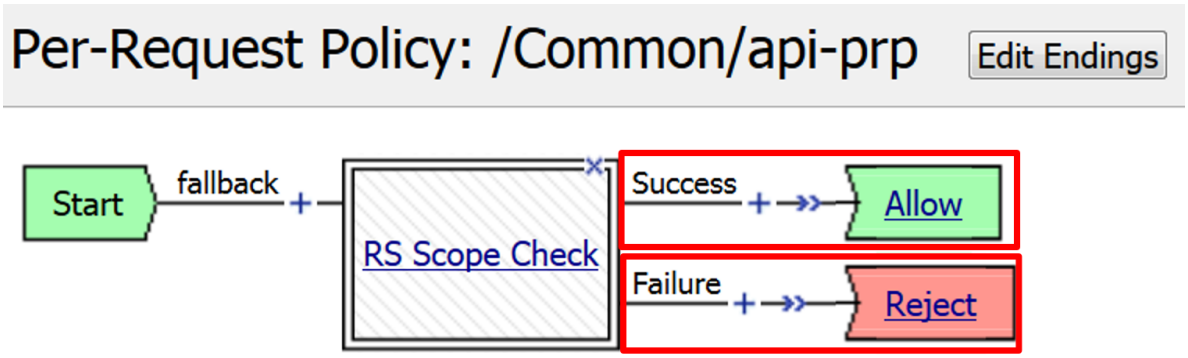


24. In the main policy, click **+** between the **Start** and **Allow**

25. Select **RS Scope Check** from the **Subroutines** tab and click **Add Item**

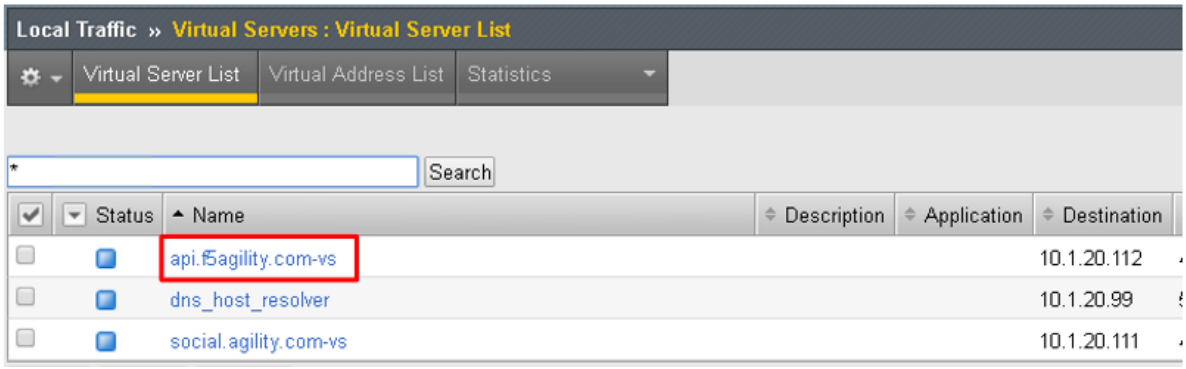


26. Verify that the Success branch terminates in Allow and the Fallback branch terminates in Reject

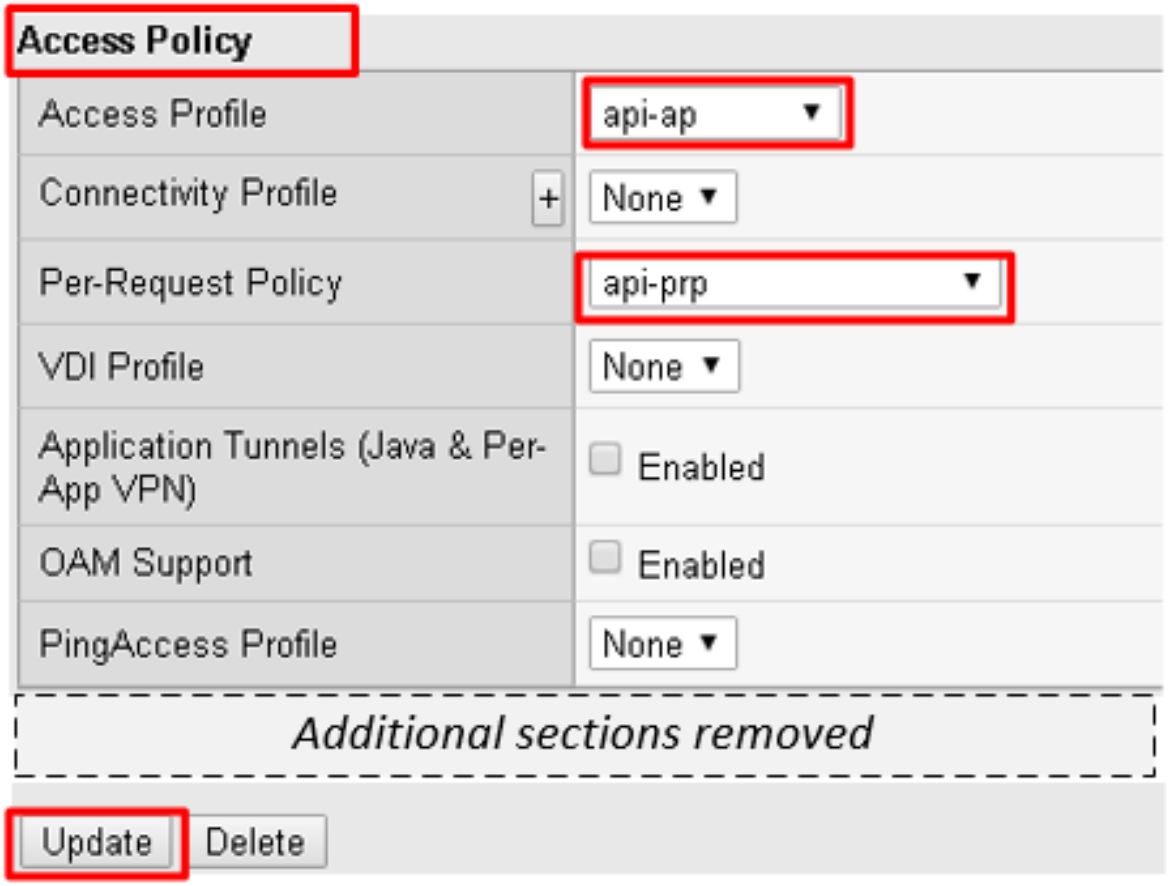


Note: You do not need to “Apply Policy ” on Per Request Policies*

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

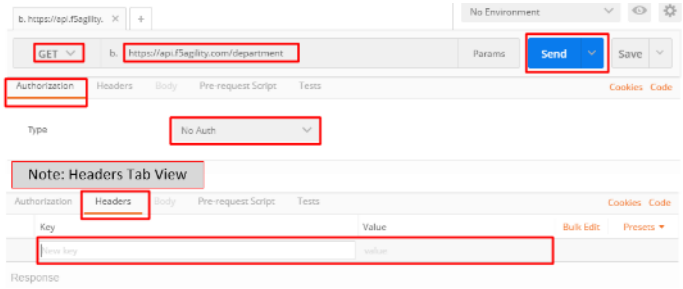


29. Change **Per-Request Policy** from **None** to api-prp and then click **Update**

2.3.5 Task 3: Verify

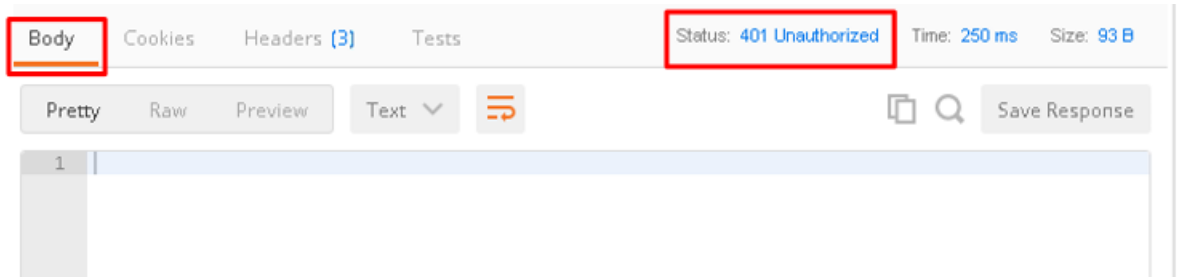
1. On the Jump Host, launch **Postman** from the desktop icon

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**

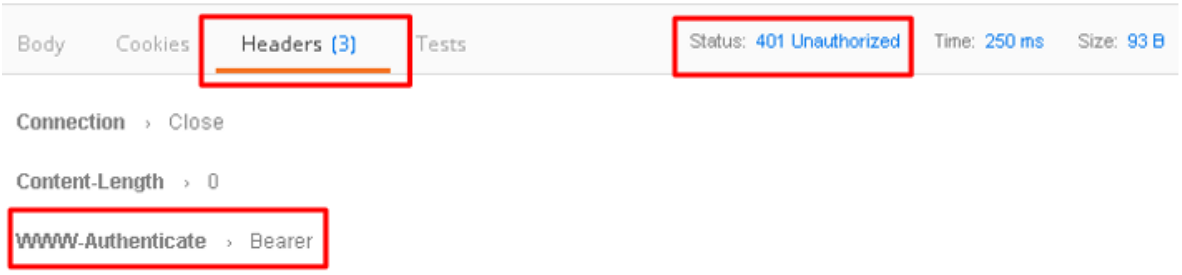


- **Method:** `GET`
- **Target:** `https://api.f5agility.com/department`
- **Authorization:** `No Auth`
- **Headers:** `(none should be set)`

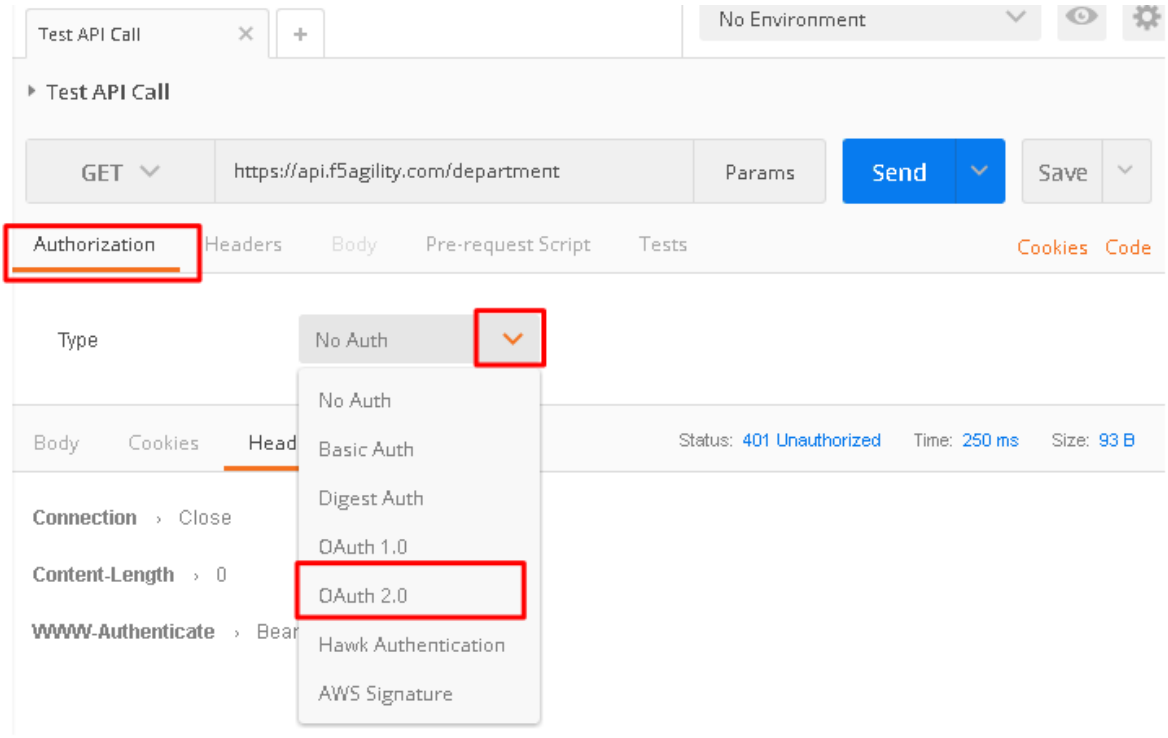
3. You should receive a `401 Unauthorized` and **3 headers**, including `WWW-Authenticate: Bearer`. The body will be empty.



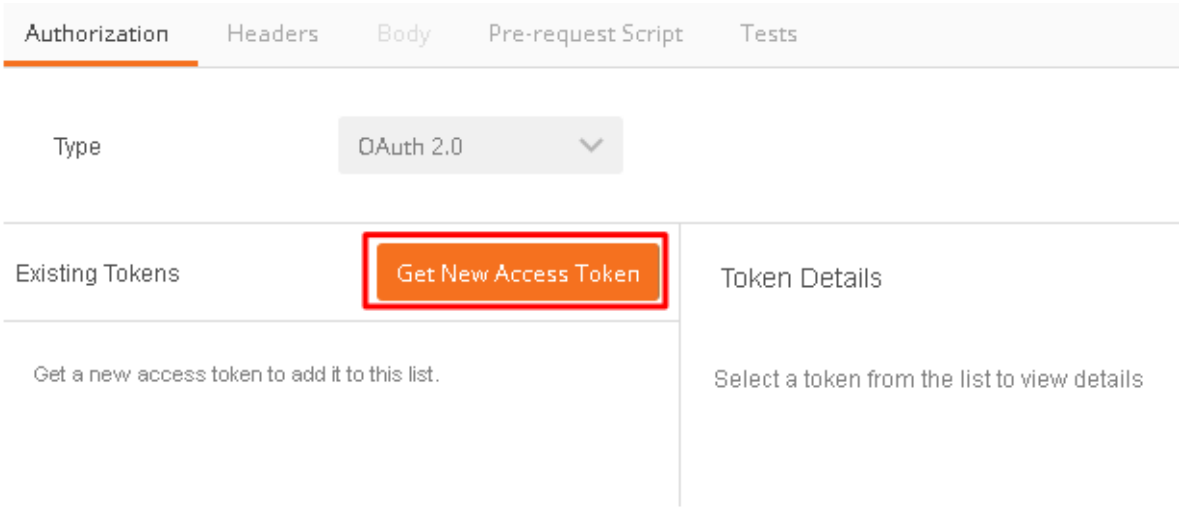
Note: Your API call failed because you are not providing an OAuth token. Both tabs shown



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**

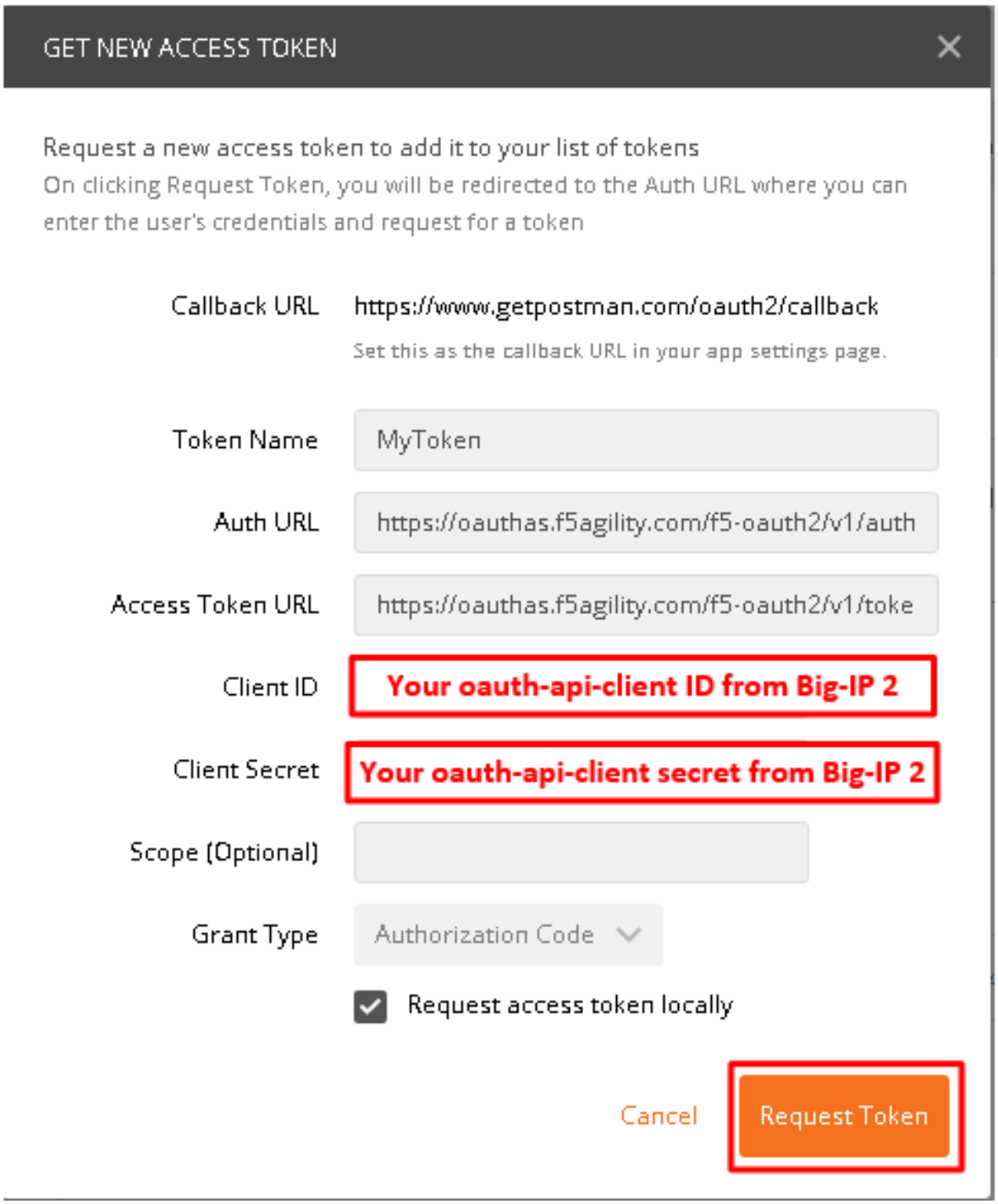


6. In the **Get New Access Token** window, if the values do not match then adjust as needed, and click **Request Token**
   - **Token Name:** <Anything is fine here>

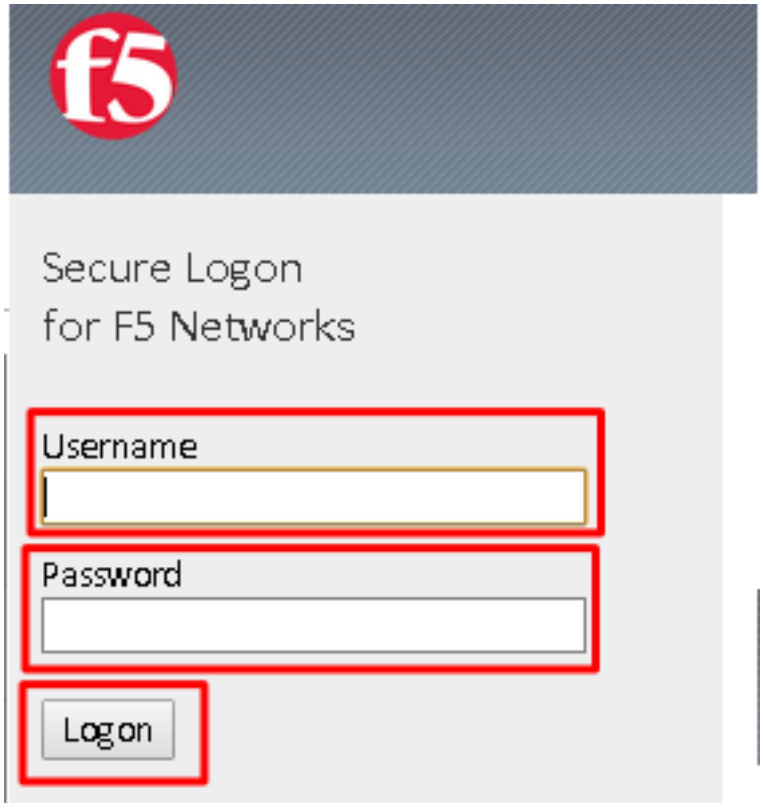
Note: If you're doing this lab on your own machine and using self signed certificates you must add the certs to the trusted store on your computer. If you've just done this, you must close Postman and reopen. You also need to go to File -> Settings in Postman and turn SSL certificate validation to off.

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

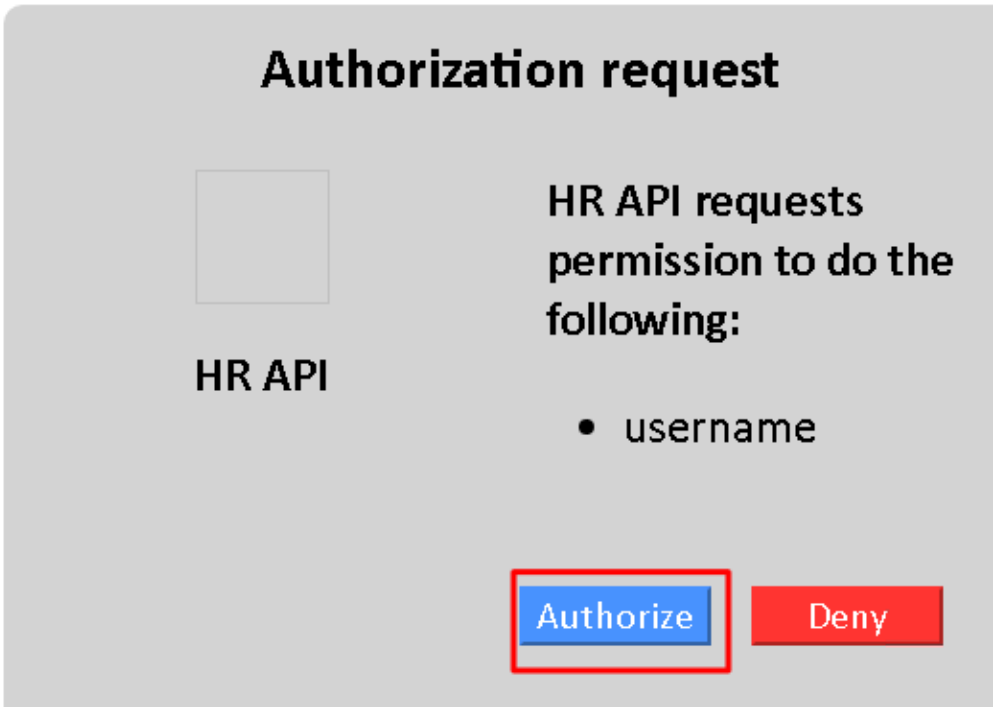
- **Access Token URL:** `https://oauthas.f5agility.com/f5-oauth2/v1/token`
- **Client ID:** <Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization Server -> Client Application -> oauth-api-client>
- **Client Secret:** <Get this from Big-IP 2 -> Access -> Federation -> OAuth Authorization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



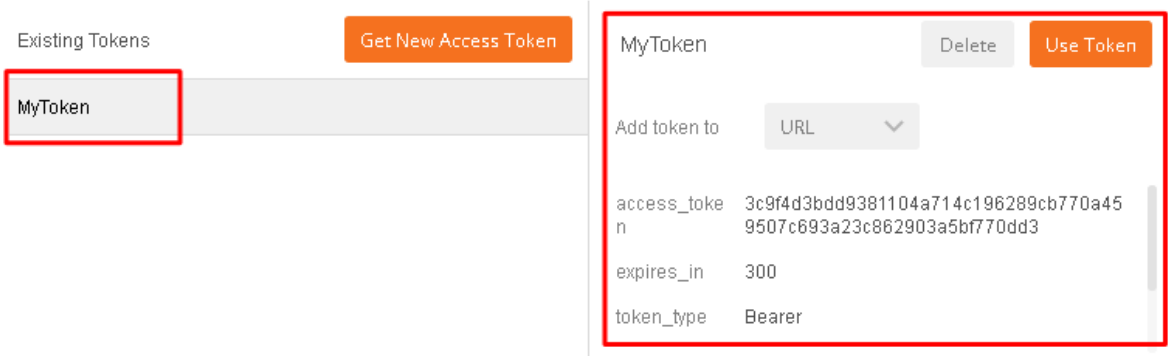
7. Logon with any credentials, such as user/password



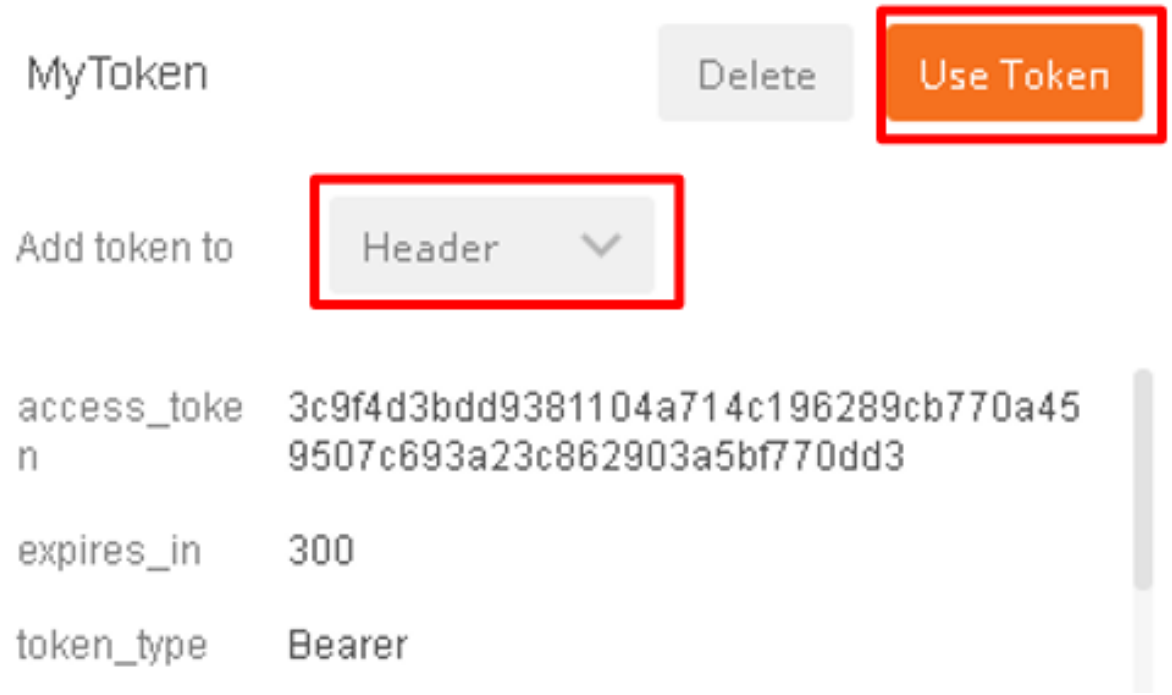
8. Authorize the HR API by clicking **Authorize**



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

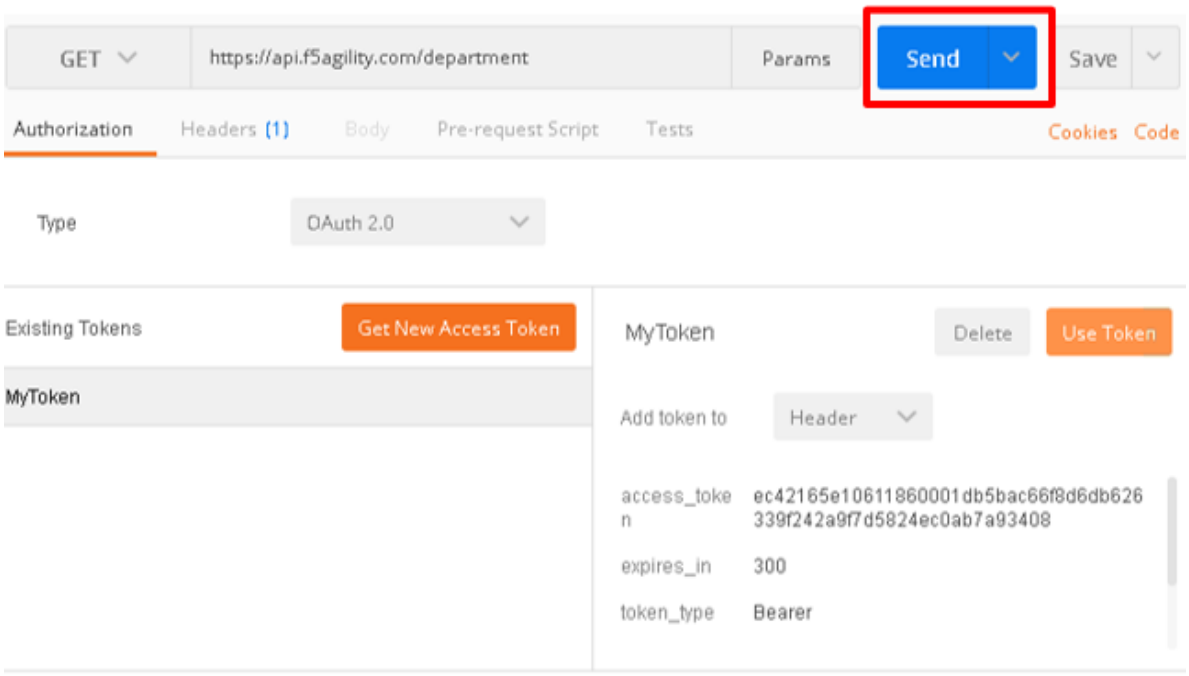


10. Change the **Add token to** drop down to Header and the click **Use Token**. You will note that the **Header** tab (in the section tabs just above) now has one header in the **Header** tab which contains your **Authorization Header** of type **Bearer** with a string value.

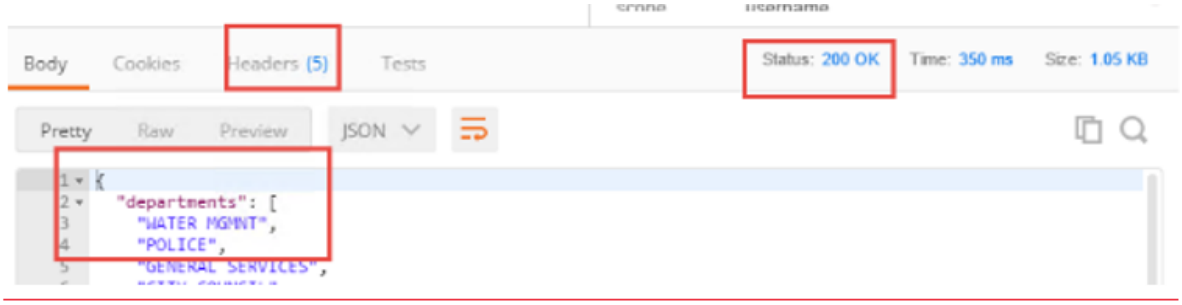


The Header tab data is shown in the screenshot

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

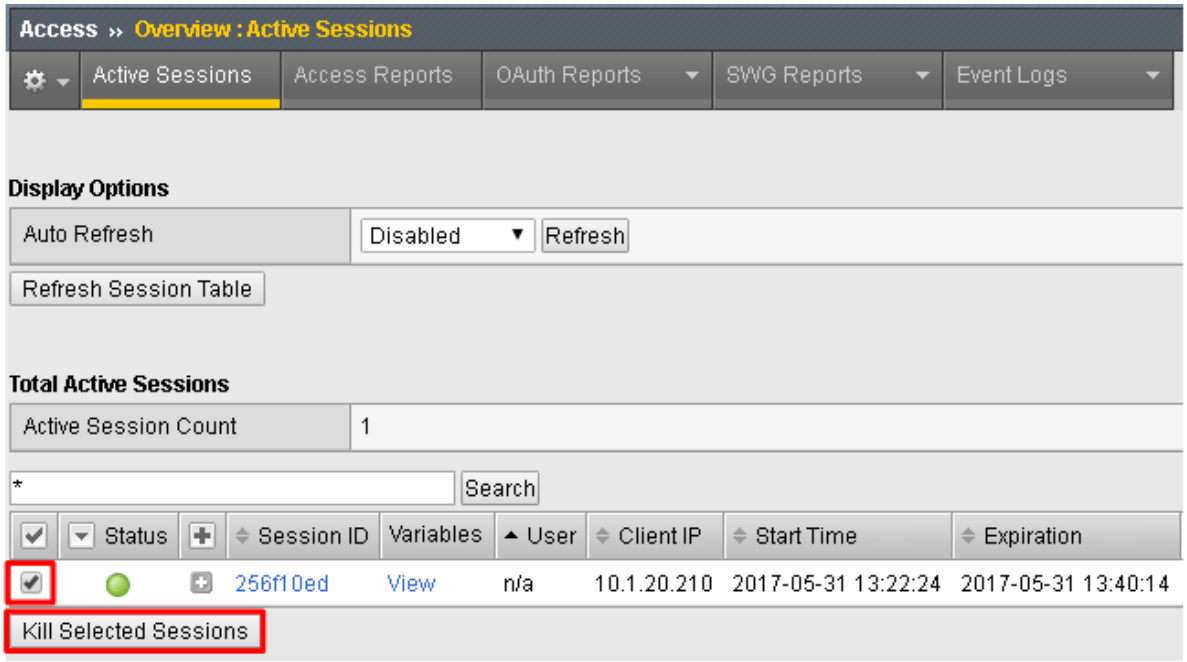


Note: This time the request was successful because you presented a valid OAuth token to the resource server (the Big-IP), so it allowed the traffic to the API server on the backend.

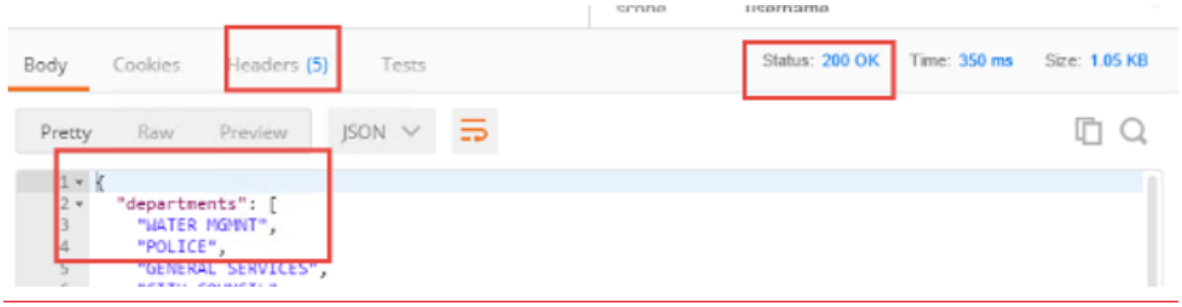
2.3.6 Task 4: Testing Session and Token States

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**



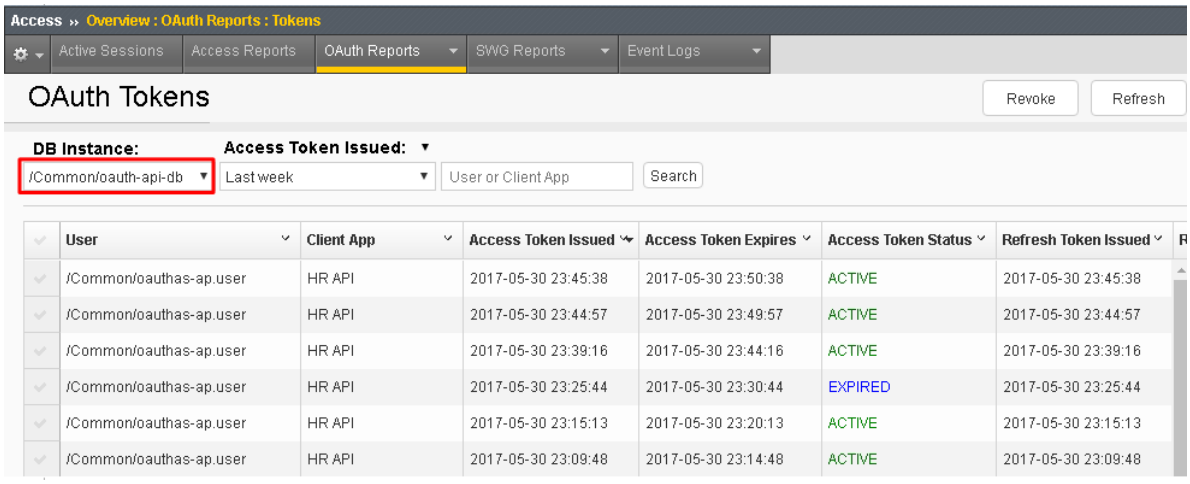
2. Go back to **Postman** and click **Send** with your current OAuth token still inserted into the header. You should still receive a 200 OK, 5 headers and the body should contain a list of departments.



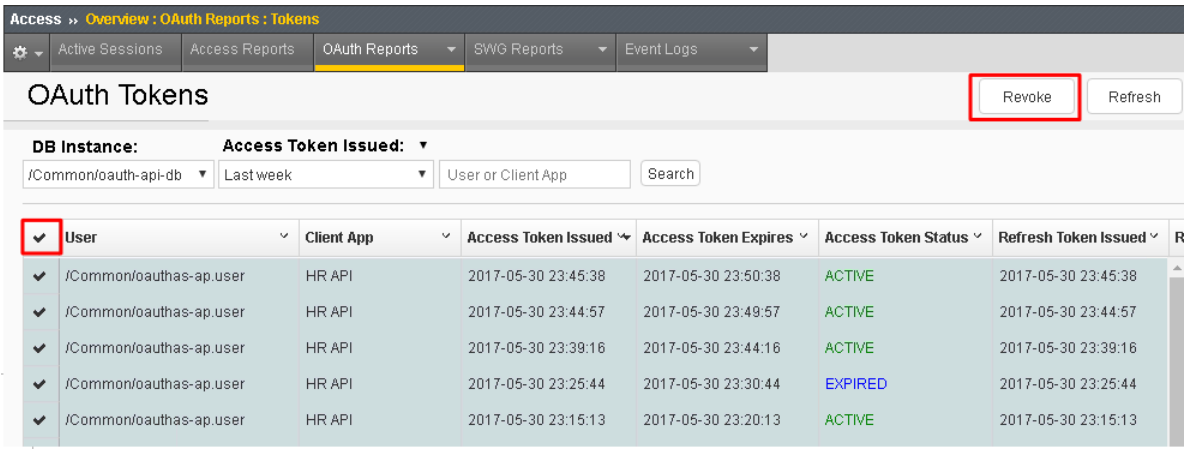
Note: You were still able to reach the API because you were able to establish a new session with your existing valid token*.

Invalidate both the Current Session and Token

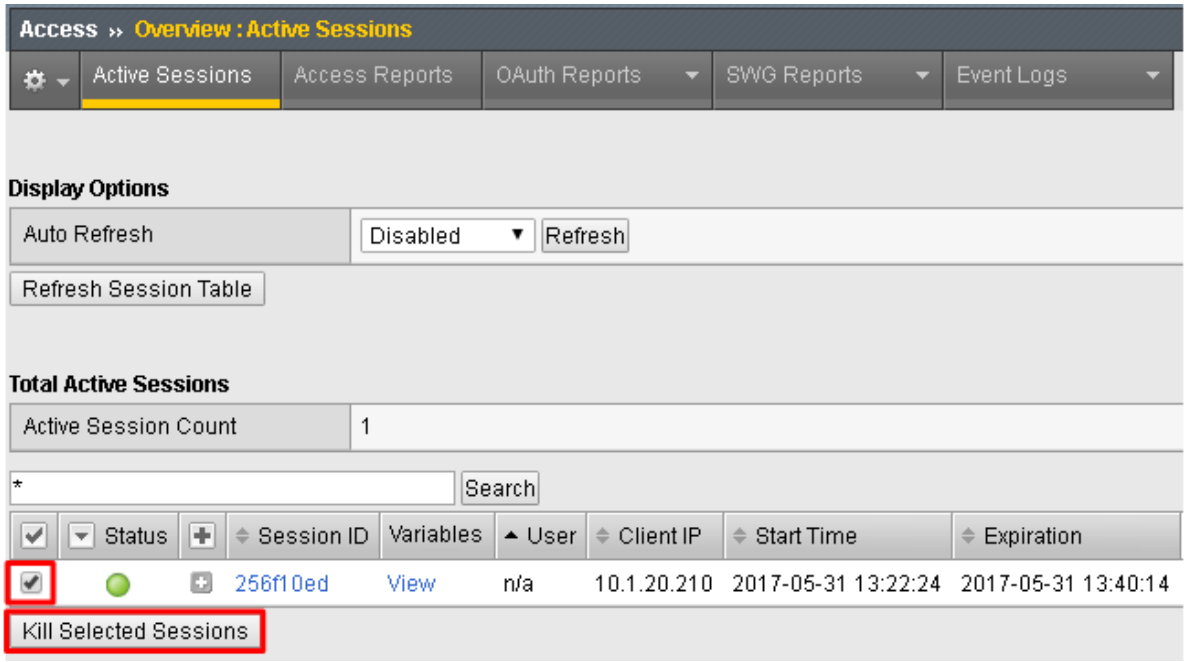
1. Go Big-IP 2 (OAuth AS) -> **Access -> Overview -> OAuth Reports -> Tokens**. Change the **DB Instance** to oauth-api-db.



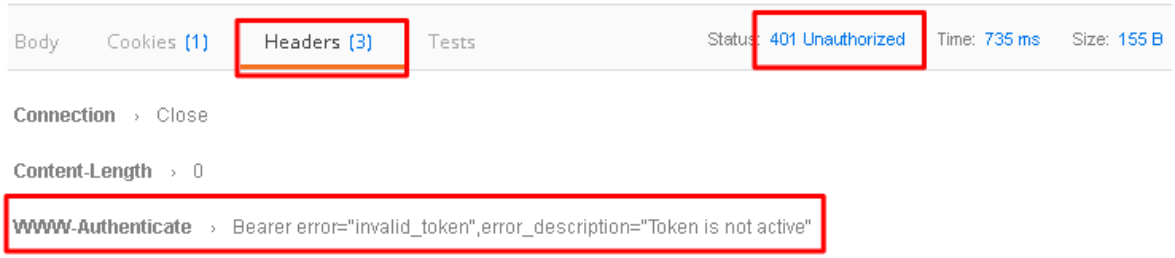
2. Select all tokens, click **Checkbox** left in title bar and the click **Revoke** in the top right



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.



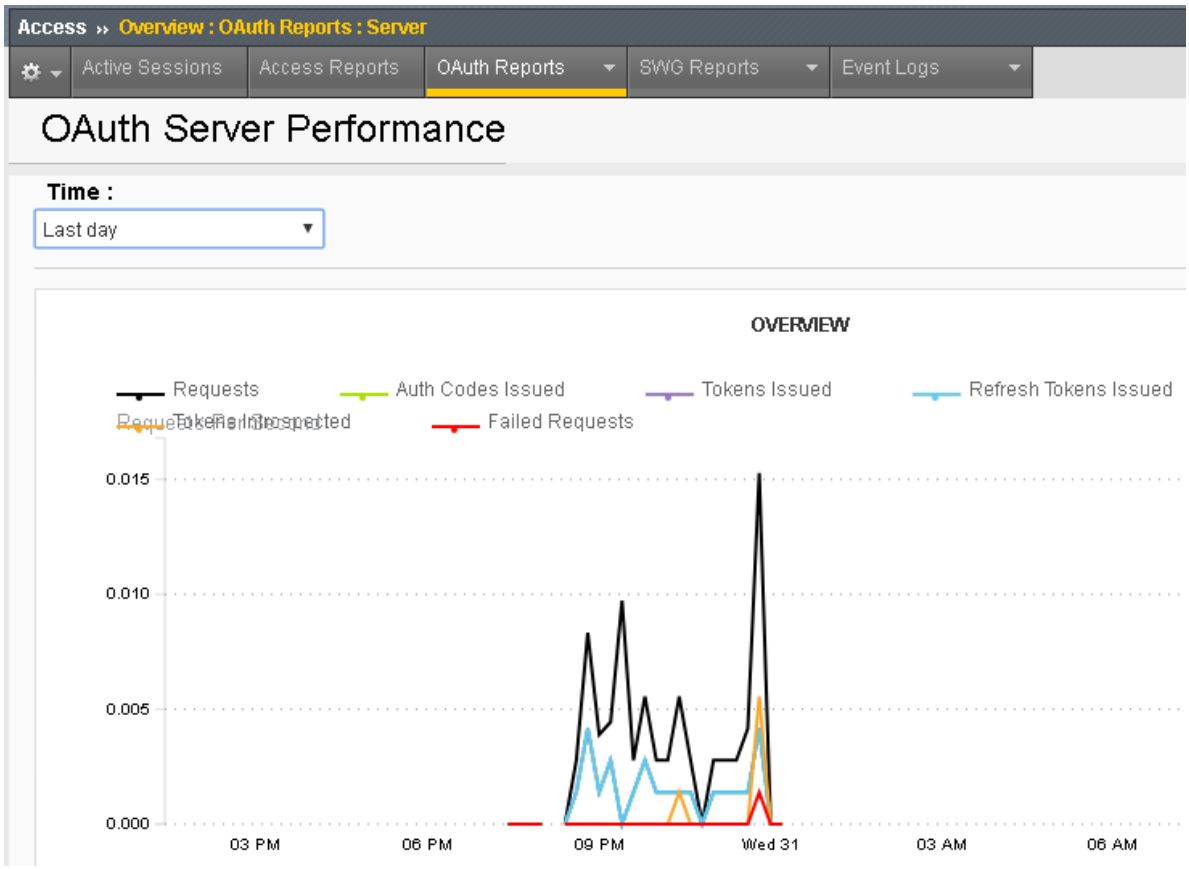
Note: You can remove the header, delete the token, and start over getting a new token and it will work once again.*

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.

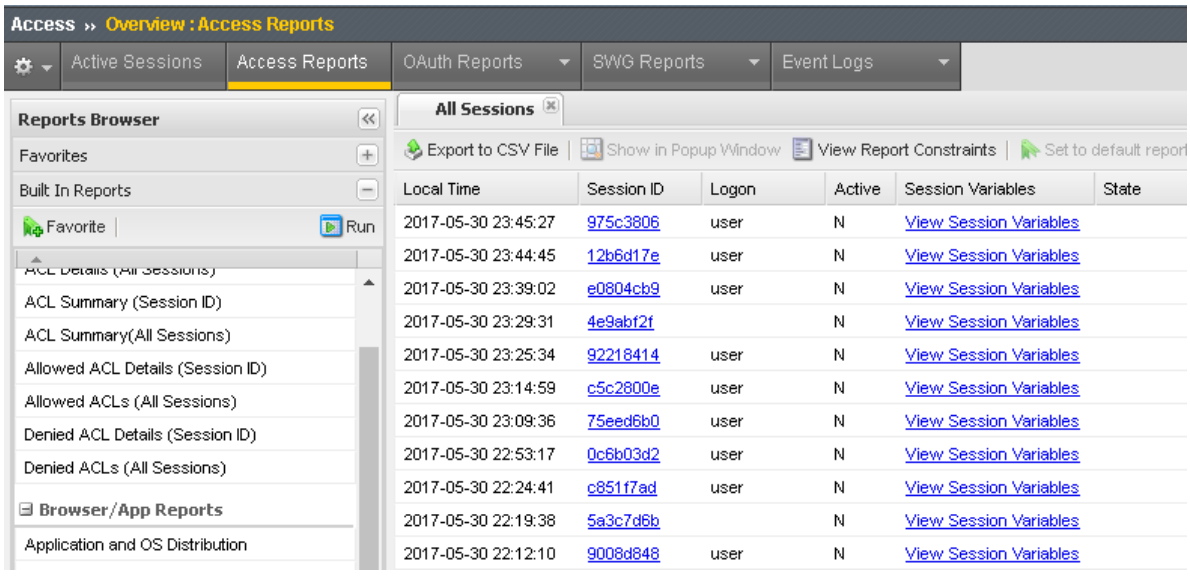
2.4 Lab 3: Reporting and Session Management

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**

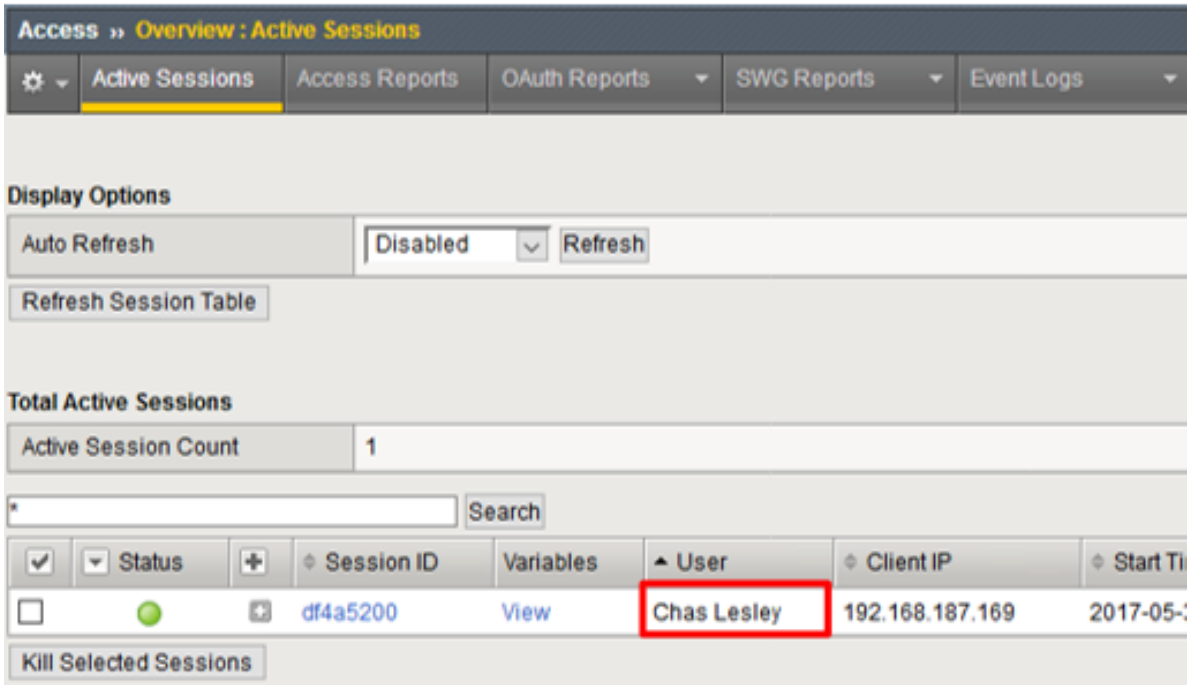


2. You can see the session logs by going to **Access**-> **Overview**-> **Active Sessions** and click on the active session, or for past sessions under **Access -> Overview -> Access Reports -> All Sessions Report** *(it runs by default and asks for a time period)*

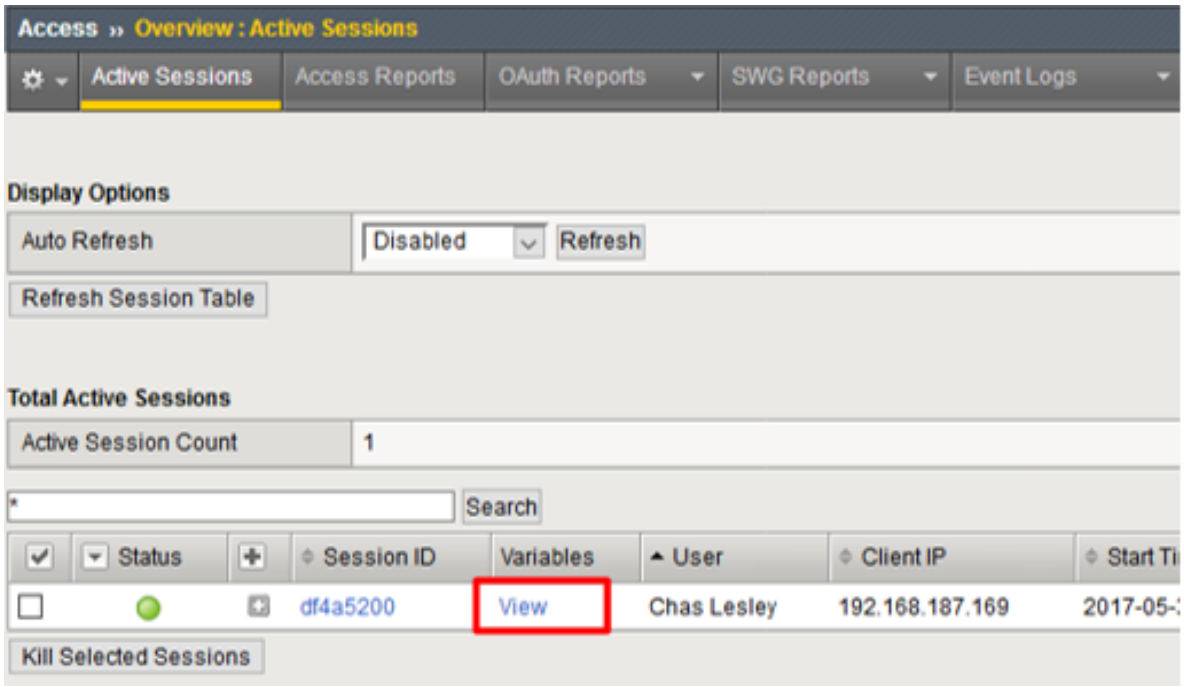


2.4.2 Task 2: Big-IP as Client / Resource Server (Big-IP 1)

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*.



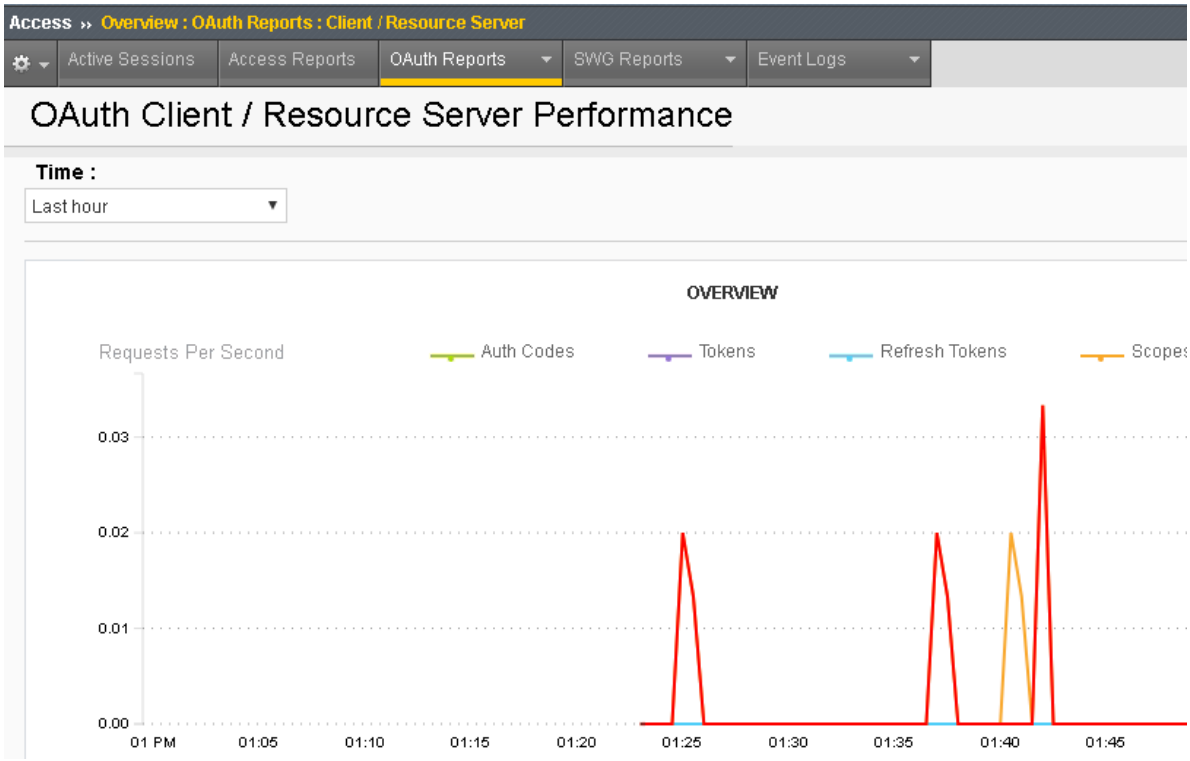
2. There are more session variables retrieved from the provider you can examine. To see them click on **View** under **Variables** for the session. Search for variables that start with "session.oauth.scope.last". The scope will determine what the Authorization Server returns to you.



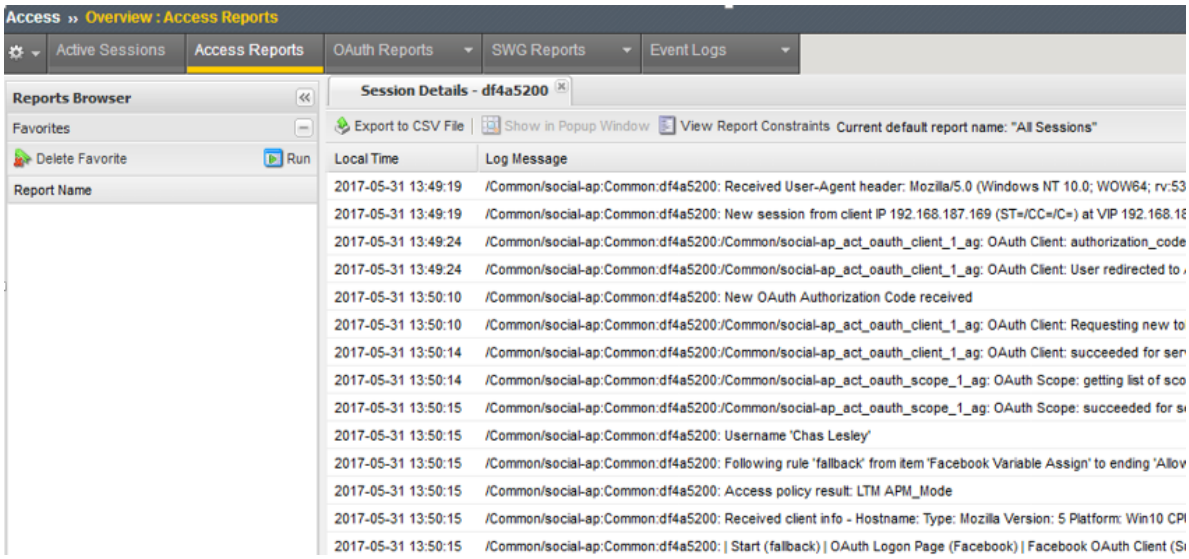
Note: You can terminate this session if desired at the Active Sessions screen*

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**



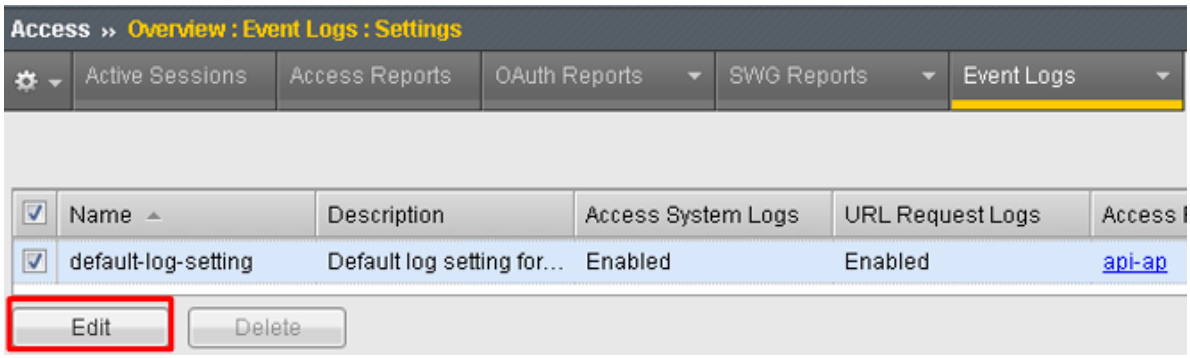
4. You can see the session logs by going to **Access**-> **Overview**-> **Active Sessions** and click on the active session, or for past sessions under **Access -> Overview -> Access Reports -> All Sessions Report** *(it runs by default and asks for a time period)*

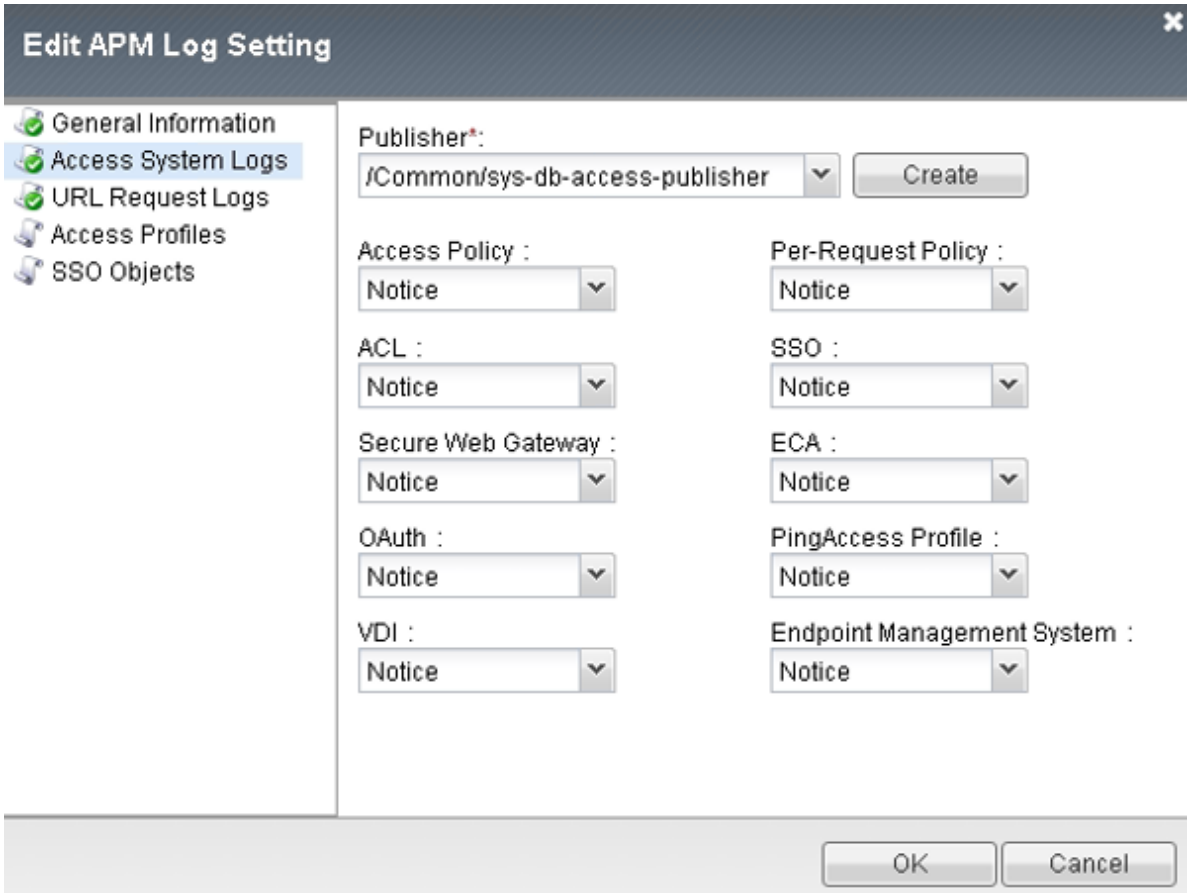


2.5 Lab 4: Troubleshooting

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
   ```

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

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

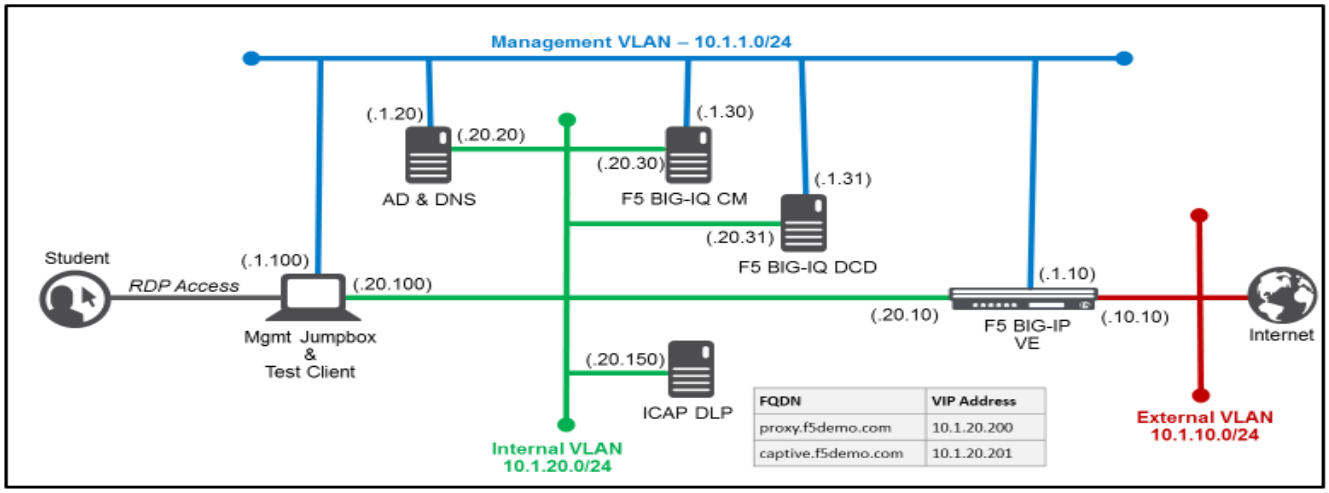
In the interest of time, the following components have been set up with basic configurations for you in a cloud-based virtual lab environment with:

- **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 SWG: Securing Outbound Internet Access

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

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

Estimated completion time: 30 minutes

Objectives:

- Create an Explicit Proxy configuration by deploying the SWG iApp template
- Test web browsing behavior

Lab Requirements:

- BIG-IP with SWG licensed
- BIG-IP must have access to the public Internet
- BIG-IP must have access to a DNS server that can resolve queries for public Internet web site names
- The latest iApp for SWG can be downloaded from **https://downloads.f5.com/** (browse to BIG-IP **iApp Templates**) Note: The iApp has already been downloaded and imported for you.

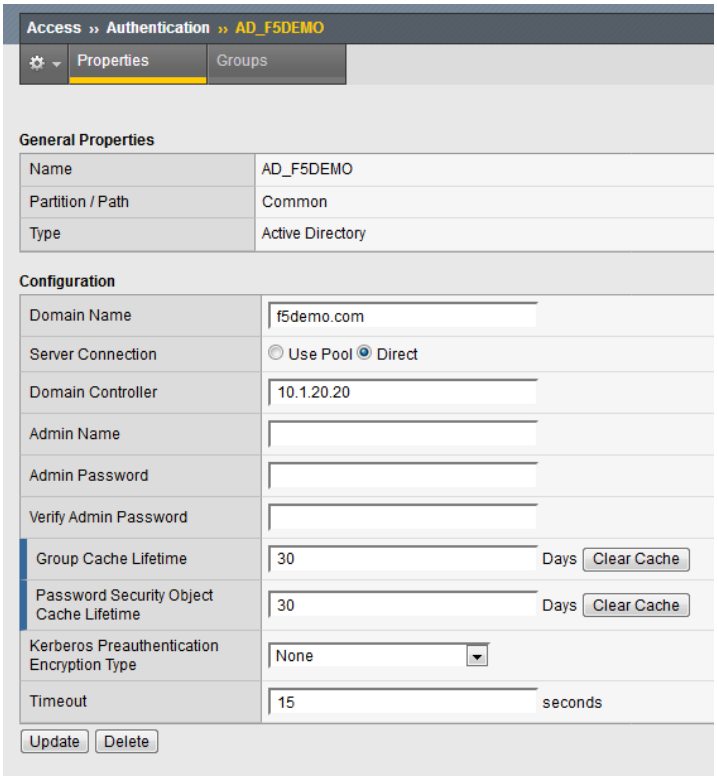
Before you can deploy the SWG iApp template, you must have the following objects configured:

- AD AAA server
- SWG-Explicit Access Policy
- Custom URL Filter
- Per-Request Access Policy

Task 1 – Create an “SWG-Explicit” Access Policy for Authentication

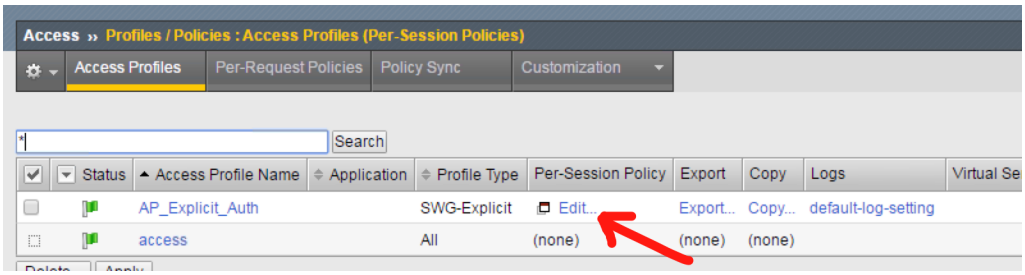
Create an AD AAA Server

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

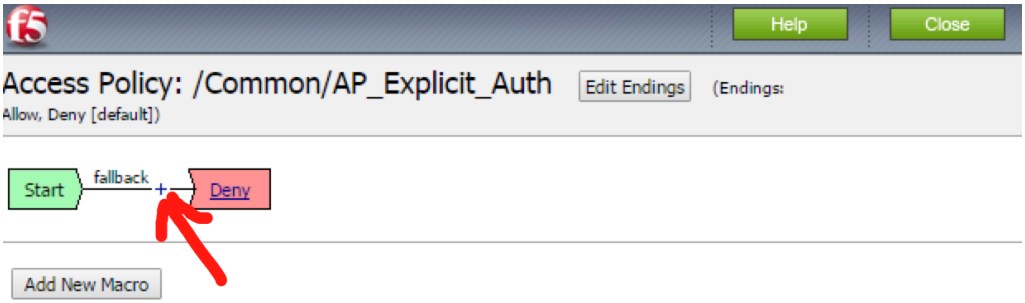


Create a Per-Session Access Policy

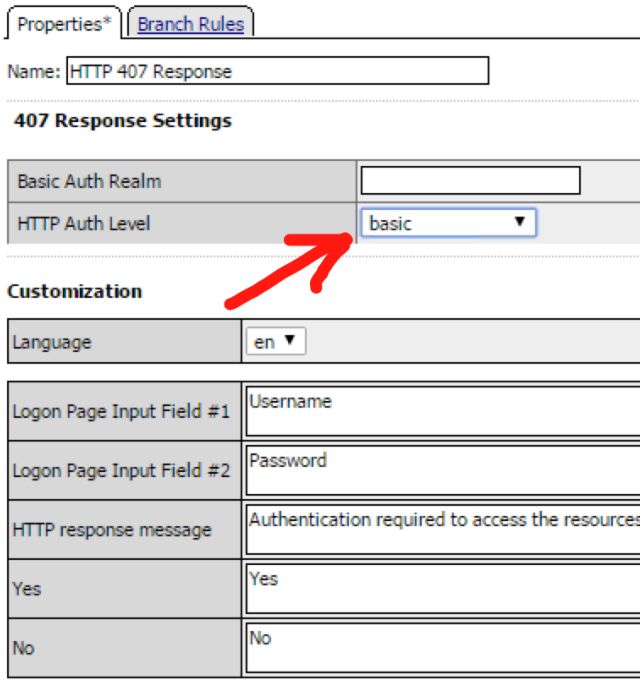
- Browse to **Access >> Profiles / Policies >> Access Profiles (Per-Session Policies)** and click **Create...***
- Name the profile **AP_Explicit_Auth**
- Change the **Profile Type** to **SWG-Explicit**
- Add **English** to the **Accepted Languages** list
- Accept all other default settings and click **Finished**
- Click on the **Edit...** link for the appropriate Access Policy created above



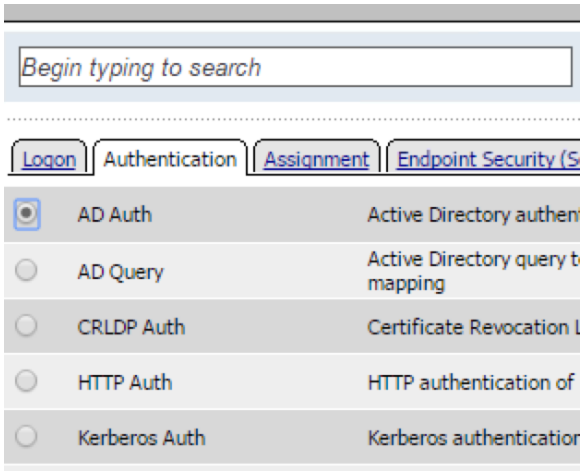
- Select the **+** between Start and Deny and **Add** an **HTTP 407 Response** object



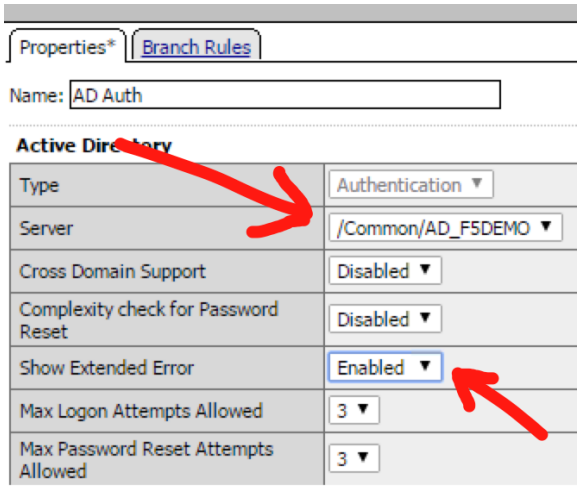
- Change the **HTTP Auth Level** to **basic**



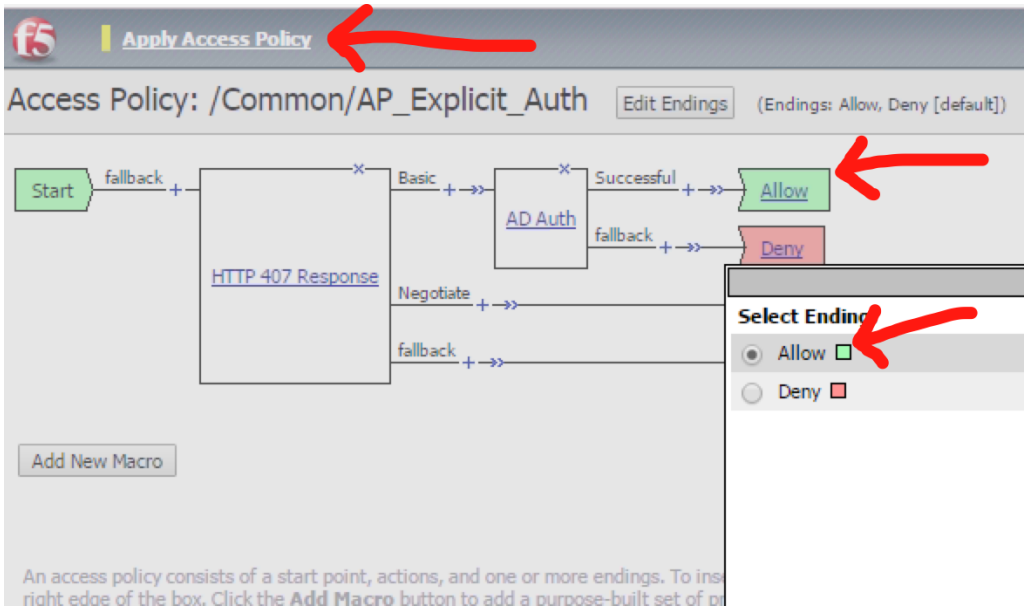
- Click **Save**
- On the **Basic** branch of the **HTTP 407** Object, **Add** an **AD Auth** Object



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

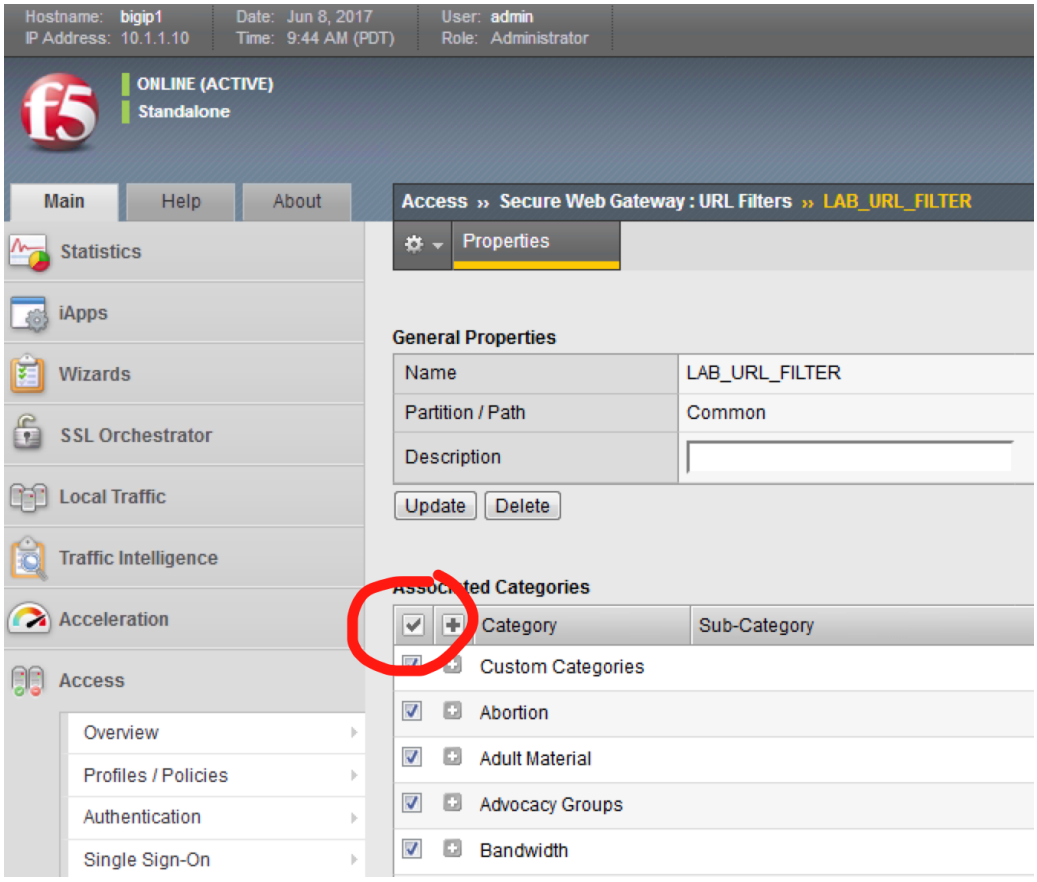


- Click **Save**
- On the **Successful** branch of the **AD Auth** Object, click on the **Deny** Ending and change it to **Allow**
- Click **Save**
- Click on the **Apply Access Policy** link



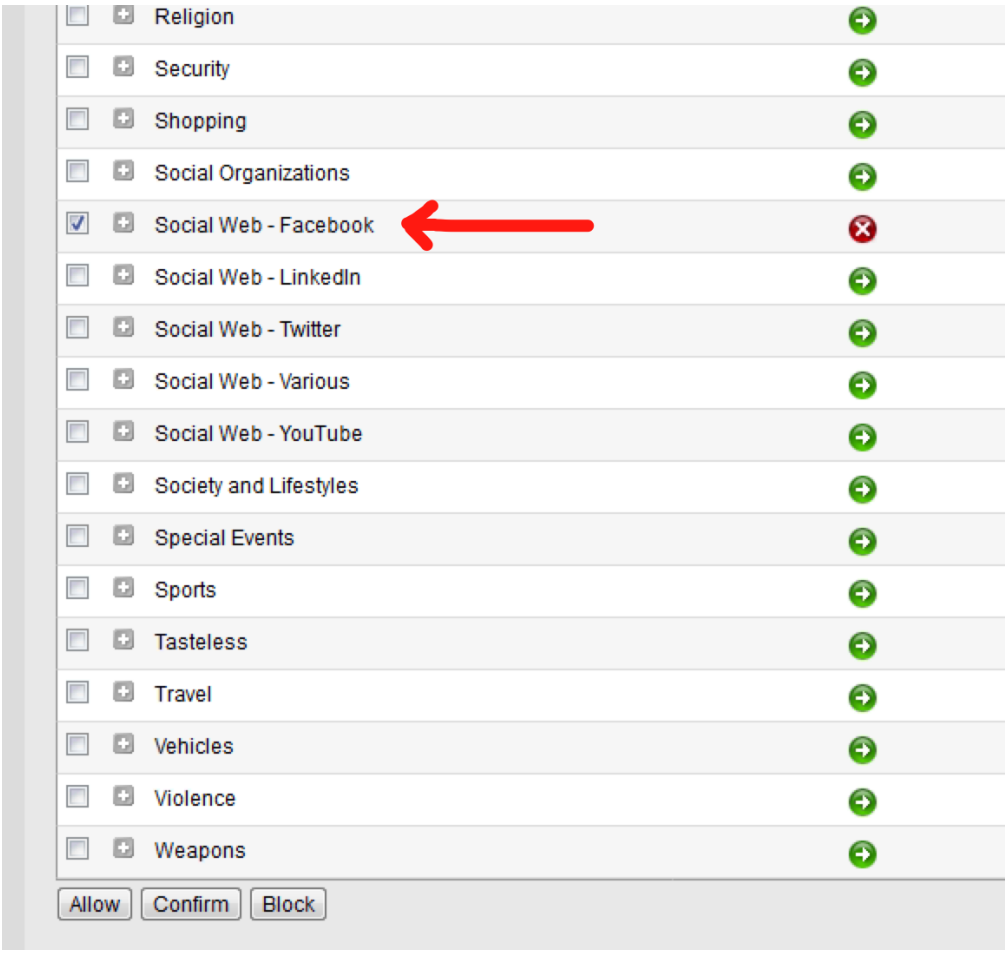
Task 2 – Create a custom URL Filter

- 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



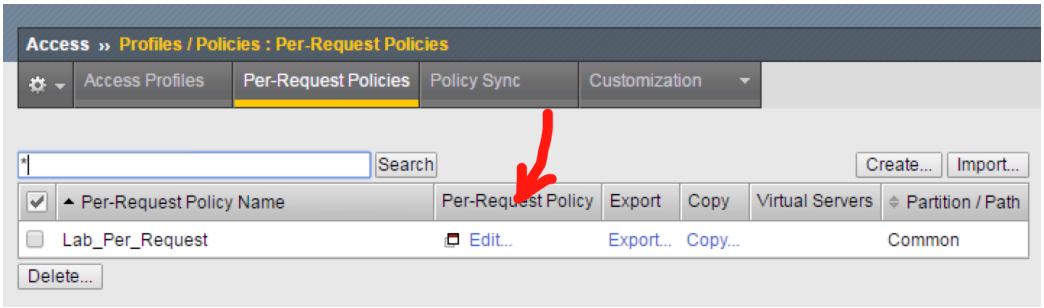
- Click **Allow** at the bottom of the page

- Click the check box to select **Social Web – Facebook** and then click **Block** (for this lab, our URL filter will only block Facebook)

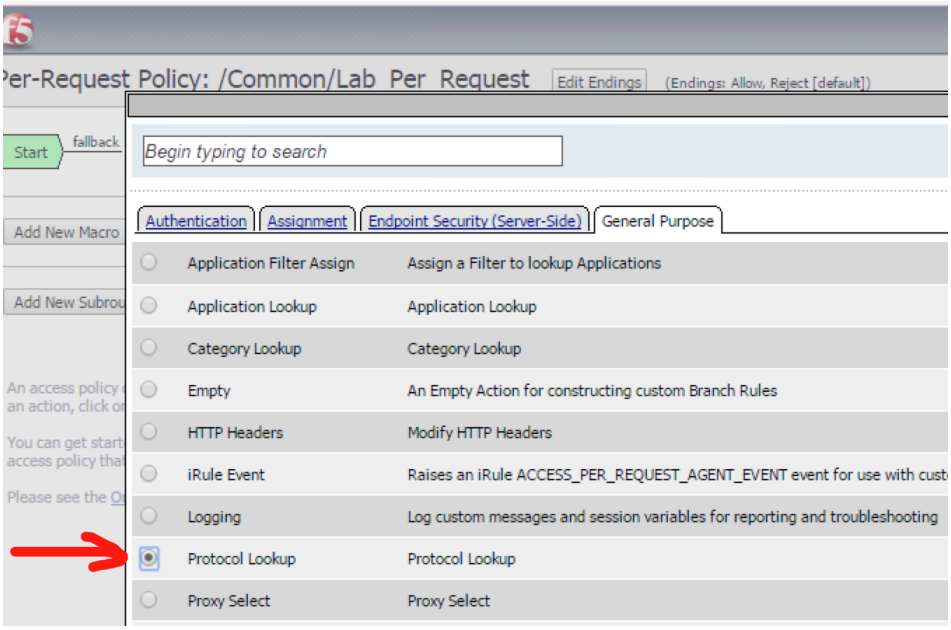


Task 3 – Create a "Per-Request" Access Policy

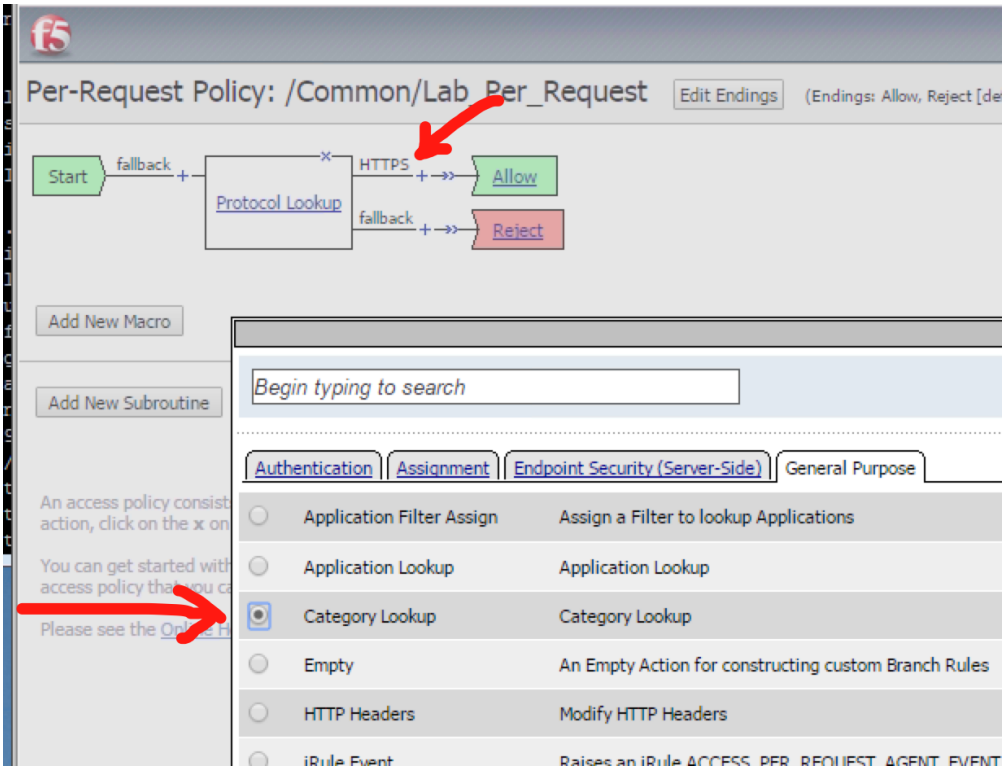
- Browse to **Access >> Profiles / Policies >> Per-Request Policies** and click **Create...**
- Name your policy **Lab_Per_Request**
- Click **Finished**
- Click on the **Edit...** link for the appropriate Per-Request Policy created above, then go back to the VPE tab in your browser



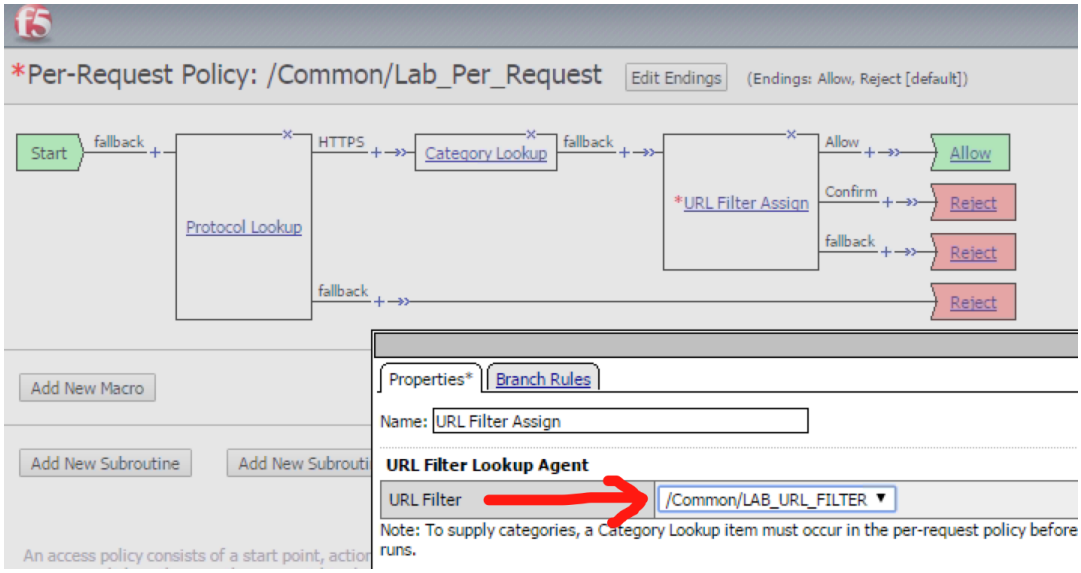
- Click on the **+** symbol between **Start** and **Allow**
- Go to the **General Purpose** tab and add a **Protocol Lookup** object



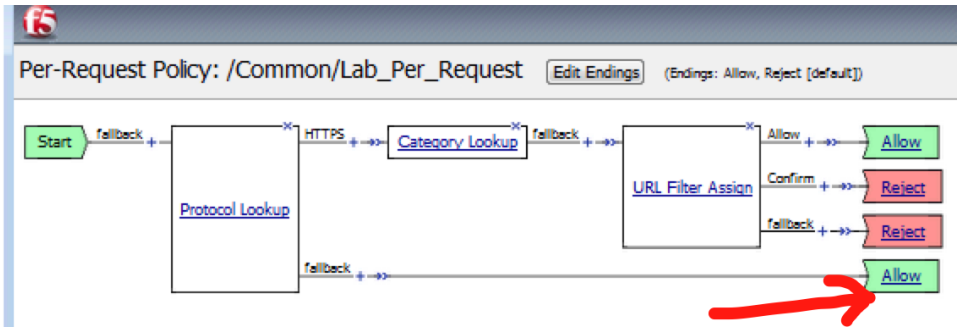
- Click **Add Item**
- Click **Save**
- On the HTTPS branch, click the **+** and **Add** a **Category Lookup** object (**General Purpose** tab)



- 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**



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:

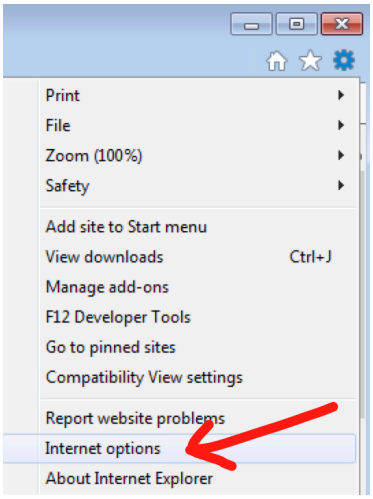
Question | Answer	
Do you want to see inline help? | Yes, show inline help	
Do you want to enable advanced options?	No, do not enable advanced options
Which type of SWG configuration do you want to deploy	Explicit Proxy
Do you want to use ICAP to forward requests for inspection by DLP servers?	No, do 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.

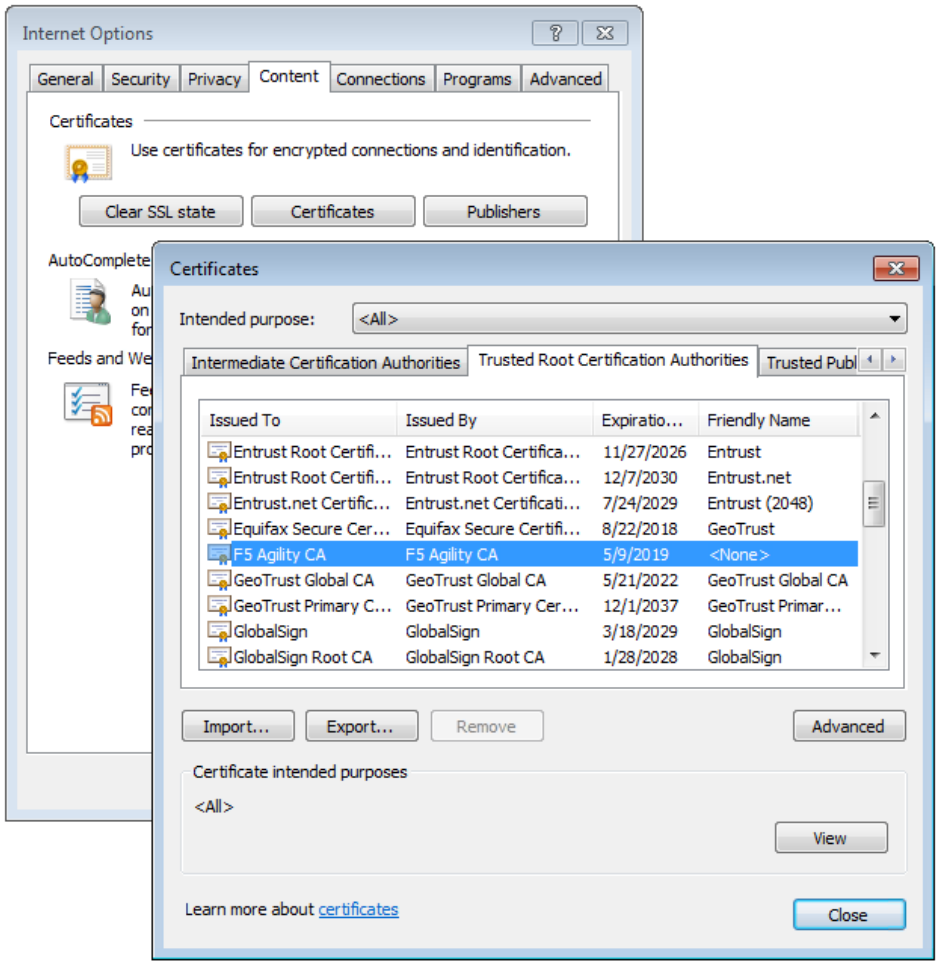
Task 5 – Verify that the "F5 Agility CA" certificate is trusted

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.

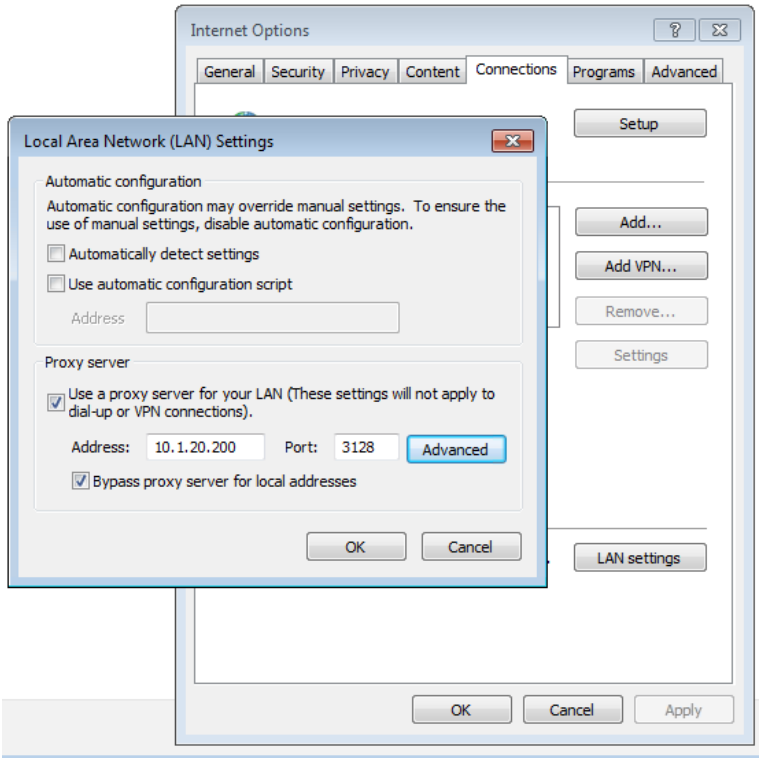


- Double-click on the certificate to view its properties, then close this window and the Certificates window.

Task 6 – Testing

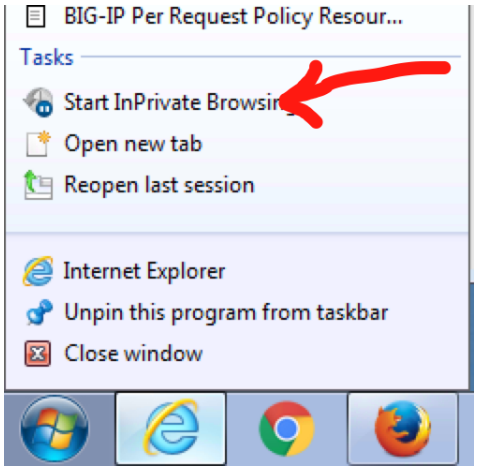
Configure your browser with a “Proxy Server”

- 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.

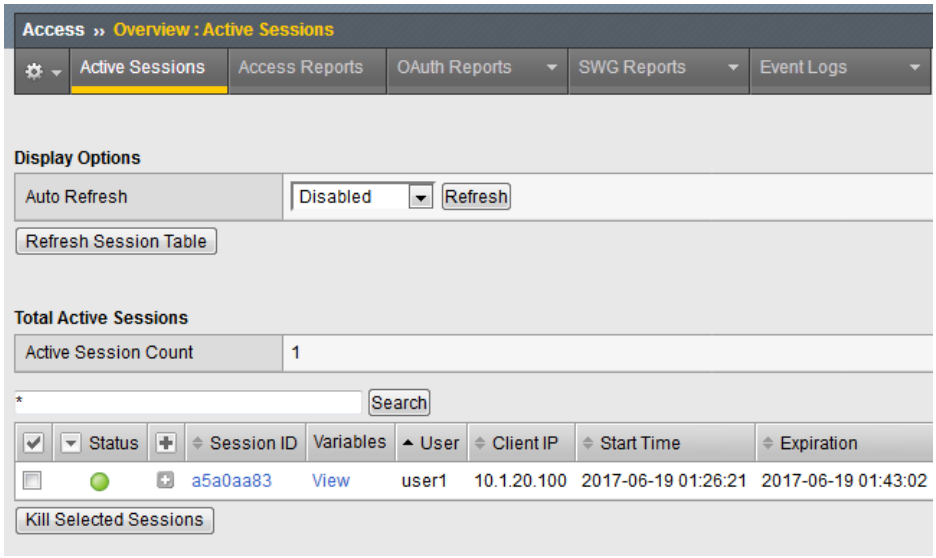


Test 1:

- Open a new Internet Explorer “InPrivate” browser window on your Jump Host client machine
- Browse to **https://www.google.com**

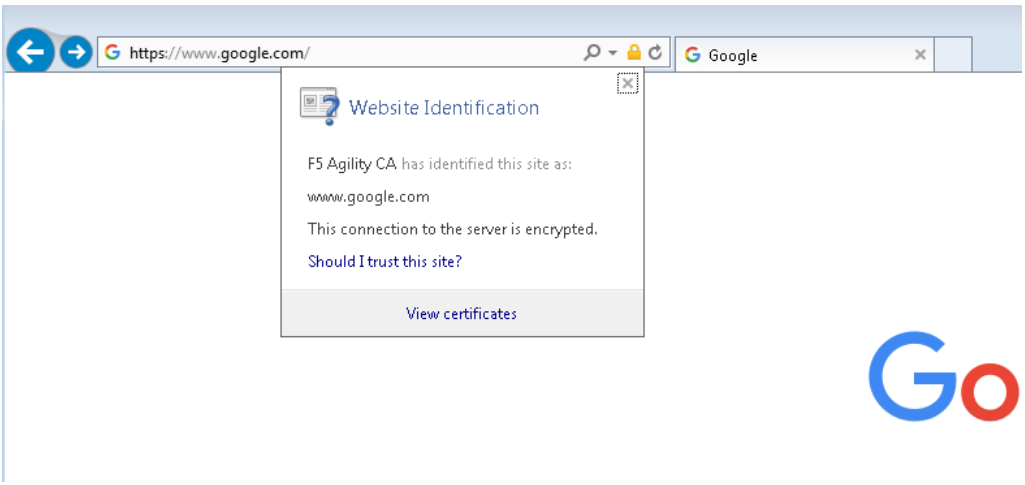


- The browser should prompt you for authentication. Submit your credentials:
  - User: `user1`
  - Password: `AgilityRocks!`
- Verify defined user has an Access Session ID
- Browse to **Access > Overview > Active Sessions**

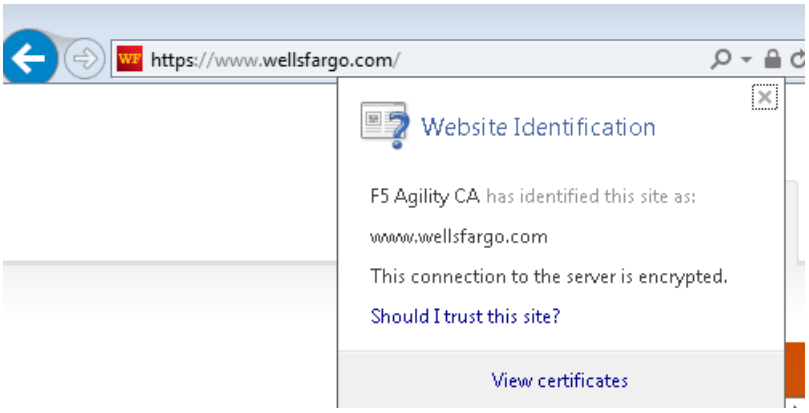


Test 2:

- 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

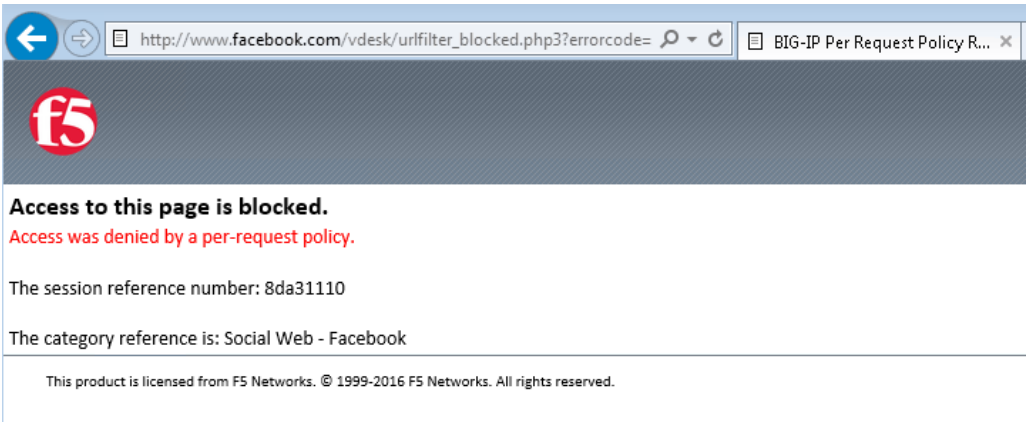


- Using an InPrivate browser window from the client test machine, go to https://www.wellsfargo.com and examine the certificate to verify that it is signed by the same **F5 Agility CA** you configured in Lab 1



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.



3.2.2 Lab 2: URL Category-based Decryption Bypass

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

Estimated completion time: 25 minutes

Objectives:

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

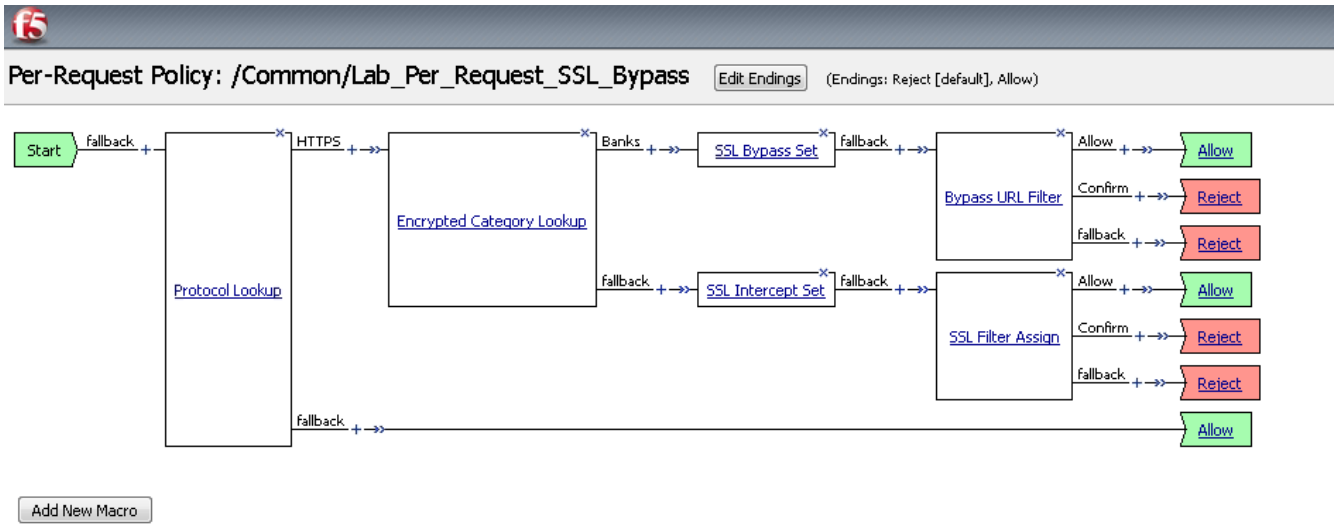
Lab Requirements:

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

Task 1 – Copy and configure new Per-Request Policy

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

- Change the **Allow** branch to an ending of **Allow**



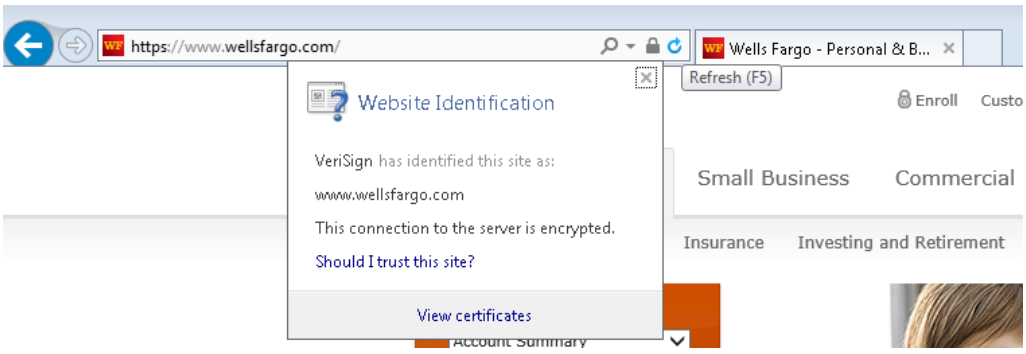
Task 2 – Reconfigure SWG iApp to assign New Per-Request Policy

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

Task 3 – Testing

Test 1:

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



3.2.3 Lab 3: Explicit Proxy Authentication – NTLM

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

Estimated completion time: 25 minutes

Objectives:

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

Lab Requirements:

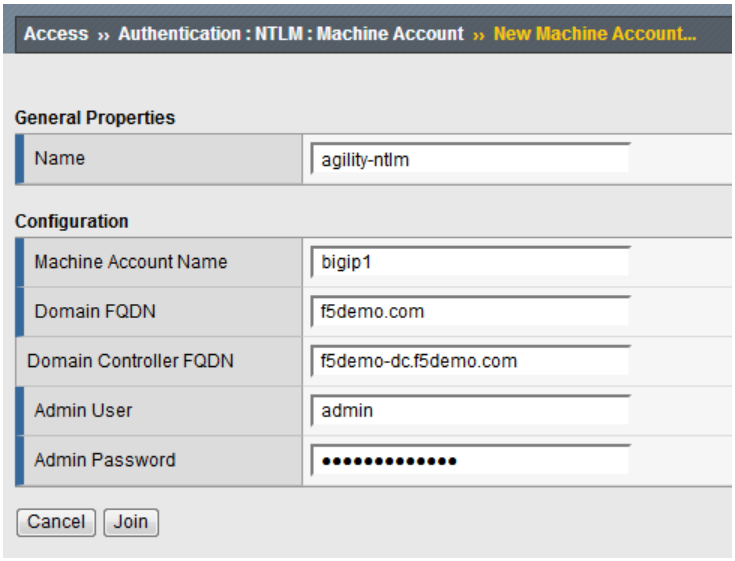
- Lab 1 previously completed successfully (working SWG iApp deployment)

Task 1 – Logout and log back in as domain user

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

Task 2 – Join BIG-IP to Domain

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



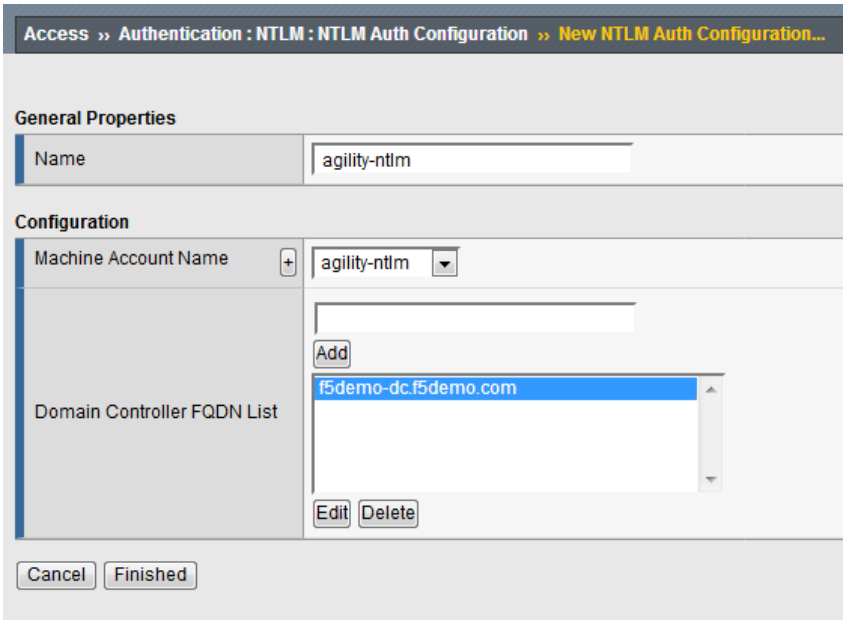
- Click **Join**
- Create a new NTLM Auth Configuration
- Browse to Access ›› Authentication : NTLM : NTLM Auth Configuration
- Click **Create**

  Name: `agility-ntlm`

  Machine Account Name: `agility-ntlm`

  Domain controller FQDN: `f5demo-dc.f5demo.com`

  Click **Add**



- Click Finished

Task 3 – Create a new Access Policy

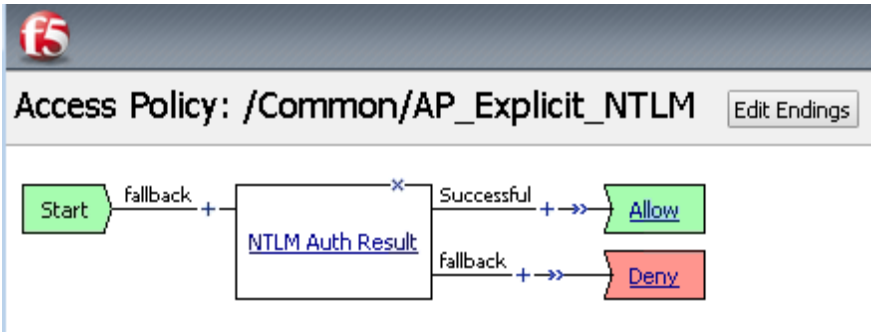
- Browse to **Access >> Profiles** / **Policies >> Access Profiles (Per-Session Policies)** and click **Create...**
- Name the profile **AP_Explicit_NTLM**
- Change the Profile Type to **SWG-Explicit**

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**



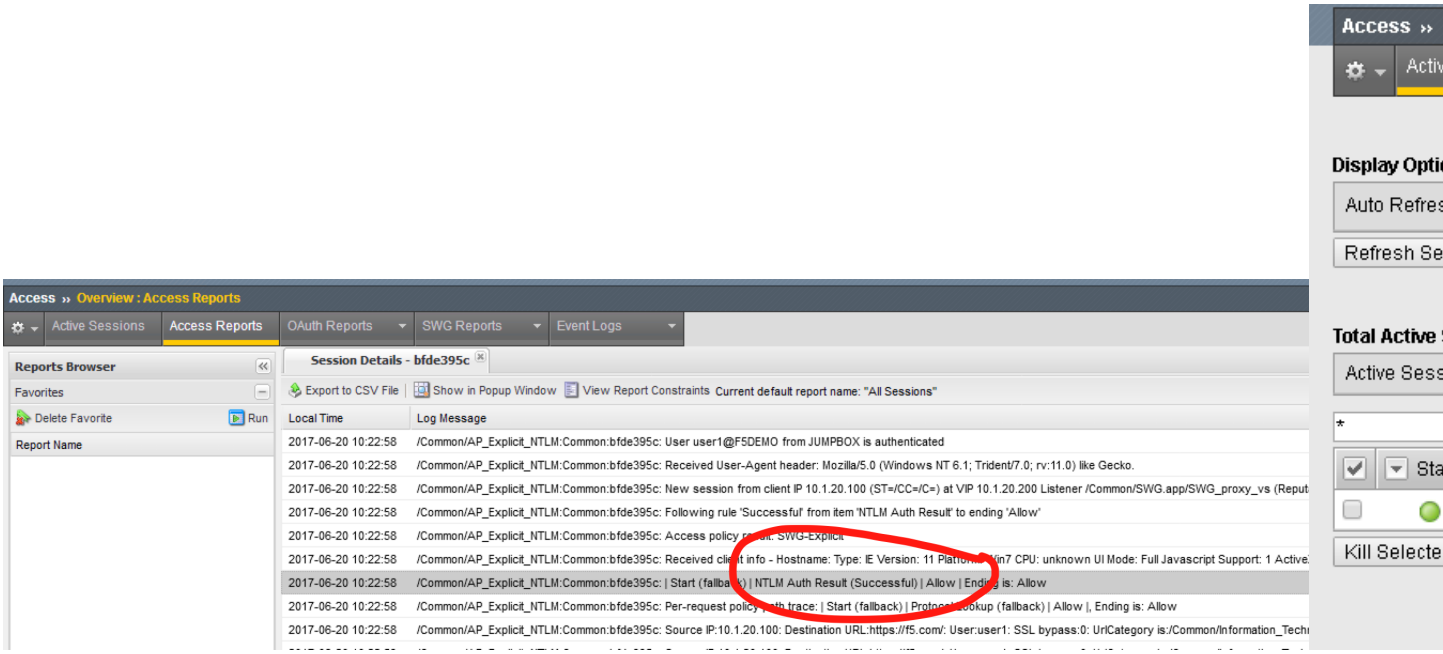
Task 4 – Reconfigure SWG iApp to apply NTLM Access Policy

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

Task 5 – Testing

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

- Open **Internet Explorer** on your Jump Host client machine
- Browse to https://www.f5.com. The browser should not prompt you for authentication since NTLM authentication is happening in the background (transparent to the user).
- Examine the user session details under **Access > Overview > Active Sessions**. Click on the session ID for details. You can see that NTLM authentication was performed.



3.2.4 Lab 4: SWG Reporting with BIG-IQ

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

Estimated completion time: 15 minutes

Objectives:

- View SWG activity reports using BIG-IQ Access
- Test web browsing behavior

Lab Requirements:

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

Task 1 – Generate New Web Browsing Traffic

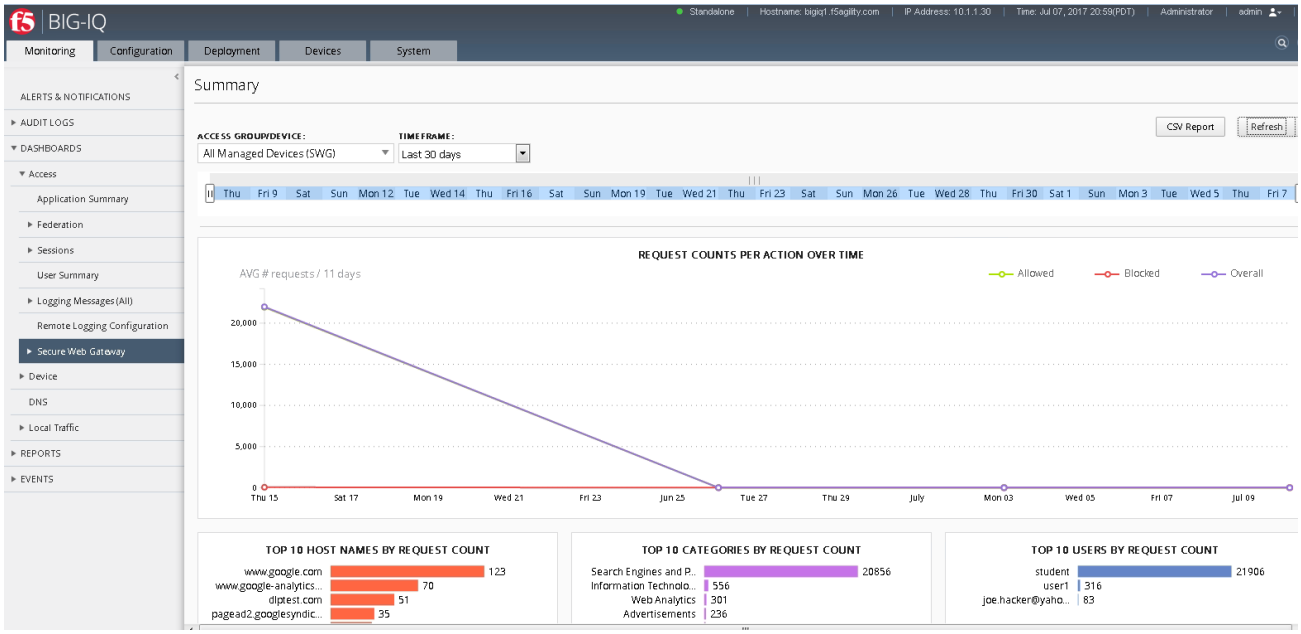
- Open Internet Explorer on your Jump Host machine and browse to several web sites, including facebook.com and banking sites to generate reporting data for traffic that is allowed, decrypted, SSL bypassed, and blocked by SWG.

Task 2 – View SWG Reporting Data

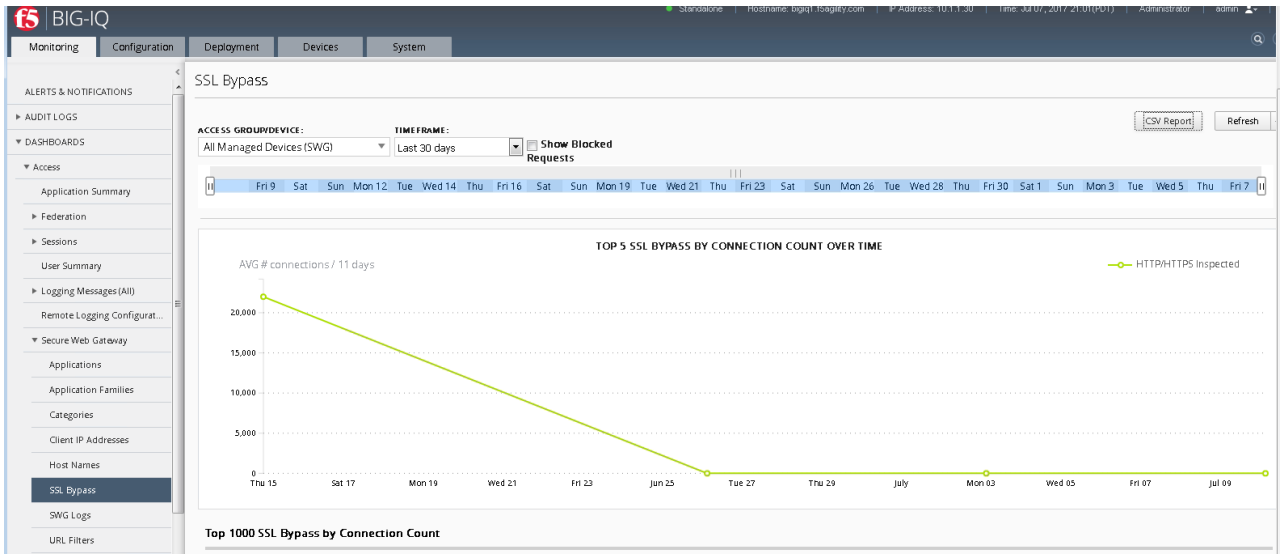
- Using Firefox, browse to the BIG-IQ Management GUI **https://10.1.1.30**
- Login with the following credentials:

  Username: **admin**

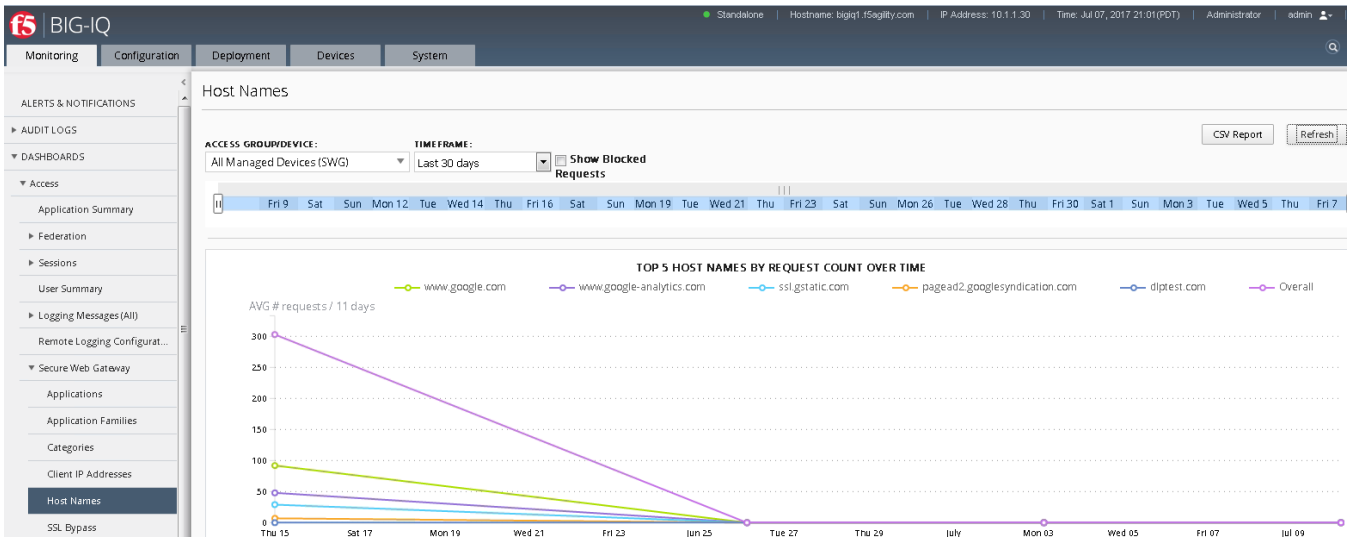
  Password: **admin**
- Browse to **Monitoring > Dashboards > Access > Secure Web Gateway > Users** to see the activity by users
- Click on **Categories** to view category information,
- Adjust the time period to **30 days or less**



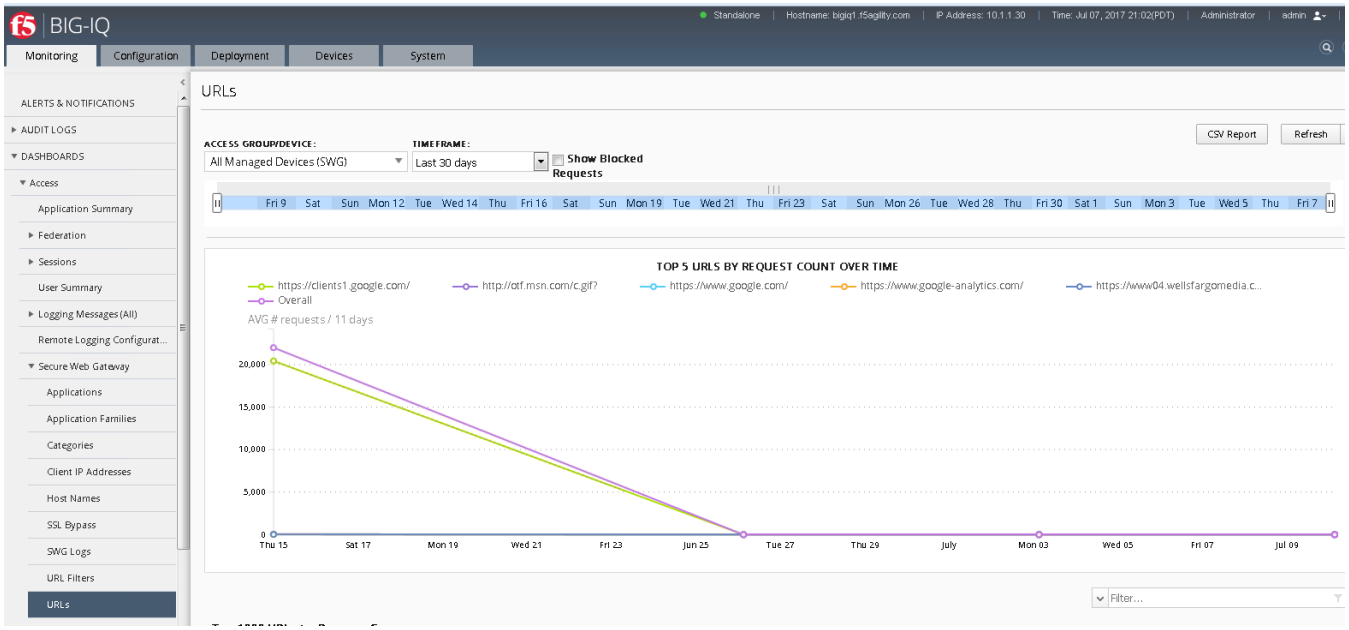
- Click on **SSL Bypass** and view the breakdown between **HTTPS Inspected** and **Bypassed** Content



- 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



3.2.5 Lab 5: SWG iApp - Transparent Proxy for HTTP and HTTPS

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

Estimated completion time: 15 minutes

Objectives:

- Deploy SWG in transparent proxy mode
- Test web browsing behavior

Lab Requirements:

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

Task 1 – Create a new Access Policy

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

Task 2 – Reconfigure SWG iApp to apply Transparent Access Policy

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

Task 3 – Testing

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

3.2.6 Lab 6: Captive Portal Authentication

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

Estimated completion time: 25 minutes

Objectives:

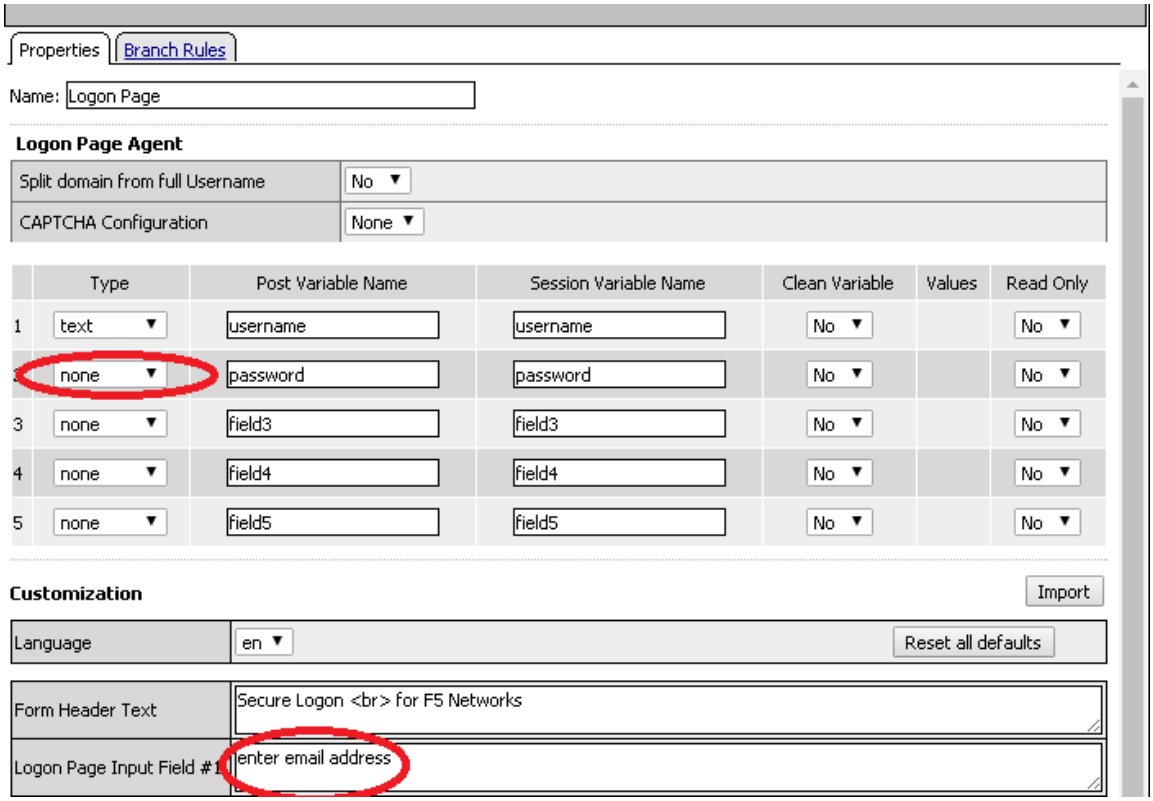
- Configure SWG with a Captive Portal to facilitate client authentication
- Test web browsing behavior

Lab Requirements:

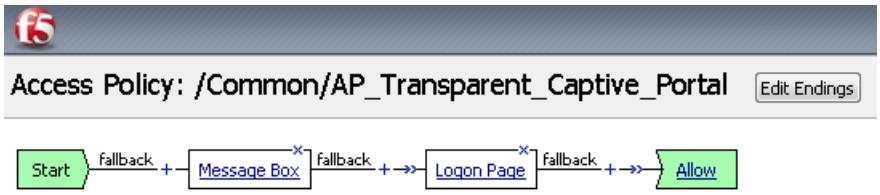
- Lab 5 previously completed successfully (working SWG transparent proxy deployment)

Task 1 – Create a new Access Policy

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



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



Task 2 – Reconfigure SWG iApp to enable Transparent Capture Portal

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

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

Task 3 – Testing

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

3.2.7 Lab 7: SSL Visibility for DLP (ICAP)

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

Estimated completion time: 15 minutes

Objectives:

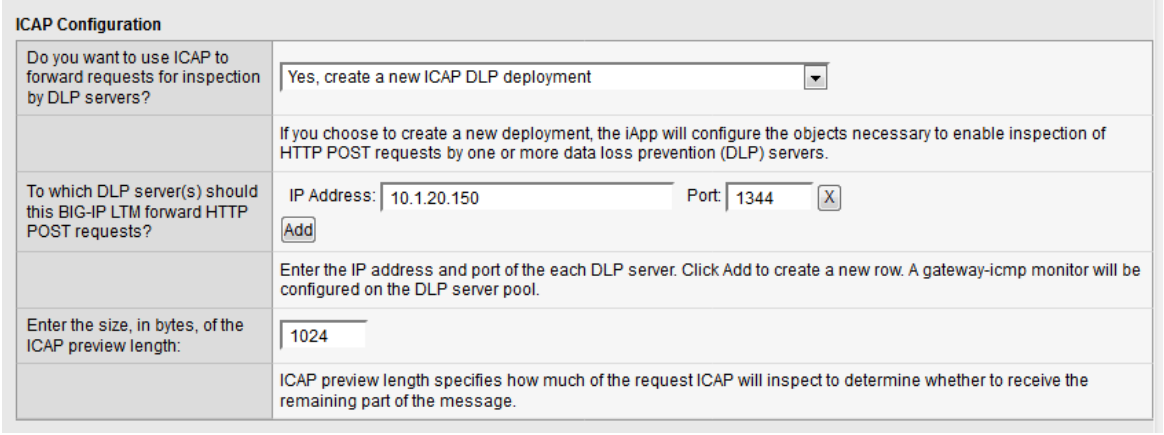
- Re-configure the SWG iApp to send unencrypted HTTP and decrypted HTTPS traffic to an ICAP (DLP) server
- Verify that the DLP service is able to see SWG proxy traffic and block if a policy violation occurs

Lab Requirements:

- Working SWG iApp deployment

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

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



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

Task 2 – Testing

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

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com