okta

Okta Integration Guide for Web Access Management with F5 BIG-IP

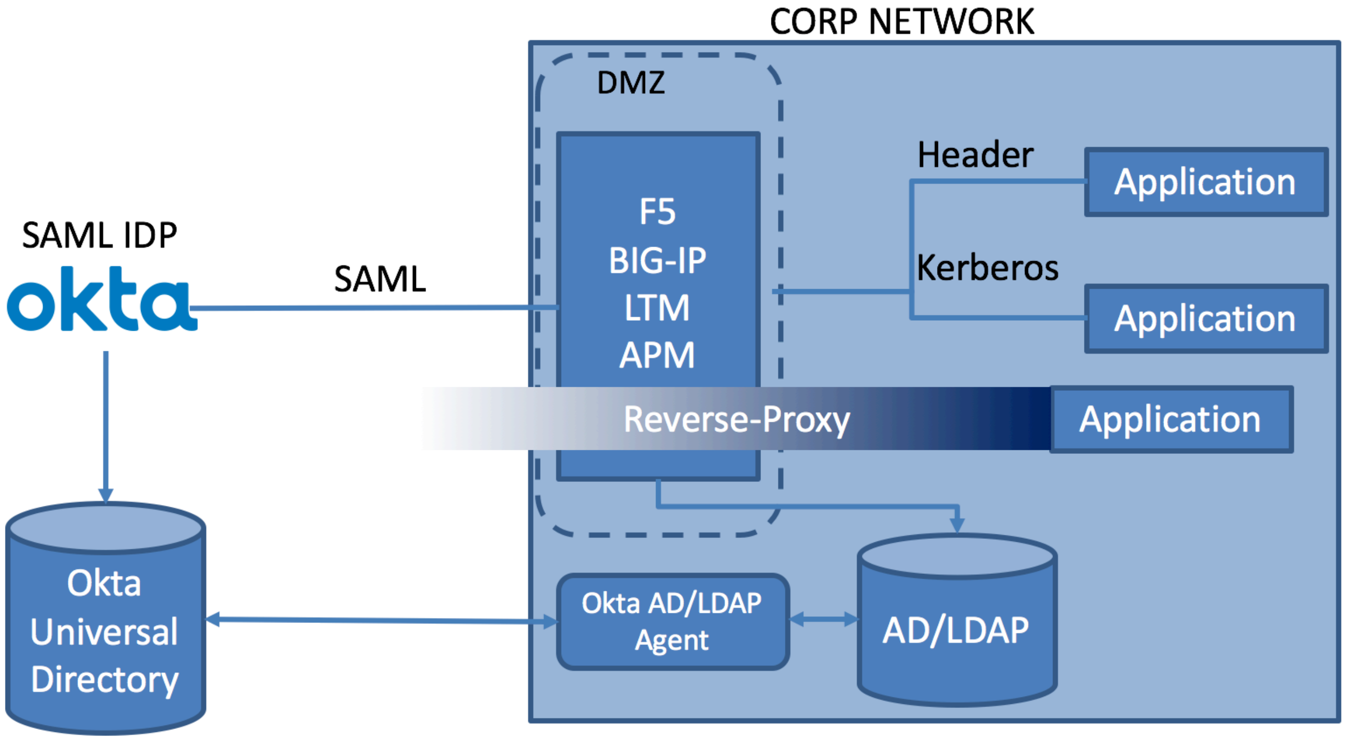
Okta Inc.
301 Brannan Street, 3rd Floor
San Francisco, CA, 94107

info@okta.com
1-888-722-7871

Contents

Introduction

F5® BIG-IP® Local Traffic Manager™ (BIG-IP LTM®) and F5 BIG-IP Access Policy Manager® (BIG-IP APM®) provide extended capabilities in conjunction with Okta identity management platform. The integration in this document allows Okta to support applications with header-based authentication, kerberos-based authentication. In addition, F5 BIG-IP also can act as a reverse proxy for publishing on-premise apps beyond the firewall where they can be accessed through Okta.



The diagram above illustrates the basic integration between the two products.

1) Okta is the identity provider. Users can be defined locally within Okta. In most cases, an on-prem Active Directory and/or LDAP is the source of identities and is integrated with Okta via Okta's AD/LDAP agent.
2) Between Okta an F5 BIG-IP, a SAML trust is built where F5 BIG-IP acts as a SAML Service Provider.
3) The target applications are protected behind F5 BIG-IP. This document covers applications that are either protected by header-based authentication or Kerberos.
4) SAML assertion from Okta is consumed by F5 BIG-IP which then "translates" the assertion appropriately for the downstream application based on their authentication scheme.

This combined solution provides best-of-breed Identity as a Service (IDaaS) deployment with full legacy and on-premise app support that is easy to deploy and configured through Okta. It also helps lower TCO by removing the need to maintain traditional on-prem identity solutions for on-premise apps.

The following table illustrates the use cases when considering using Okta and F5 BIG-IP together.

	Authentication Mechanism	Okta	F5 BIG-IP
1.	SAML	Acts as SAML Identity Provider	-
2.	WS-Fed	Acts as WS-Fed Identity Provider	-
3.	Login Page only (username/pwd)	Okta's Secure Web Authentication providing form-post capability through browser plug-in	-
4.	Header-based	Acts as identity provider	Receives SAML from Okta – generates header(s) for downstream app
5.	Kerberos	Acts as identity provider	Receives SAML from Okta – obtains Kerberos ticket for downstream Kerberos-enabled app.
6.	Reverse-Proxy to access on-prem application from outside the firewall	Acts as identity provider if only authenticated users are allowed	Acts as reverse proxy

This document will go through the following:

- Publish a sample ASP .NET IIS web application via F5 BIG-IP
- Configure Okta as SAML 2.0 IdP for F5 BIG-IP
- Configure F5 BIG-IP as SAML 2.0 SP for Okta
- Testing the SSO integration

The instructions provided here should work for F5 BIG-IP version 11.* and up. You can apply this to any production or lab edition of the product.

For an example of how to set up F5 BIG-IP environment, the Appendix presents a basic set of instructions around a VMWare example.

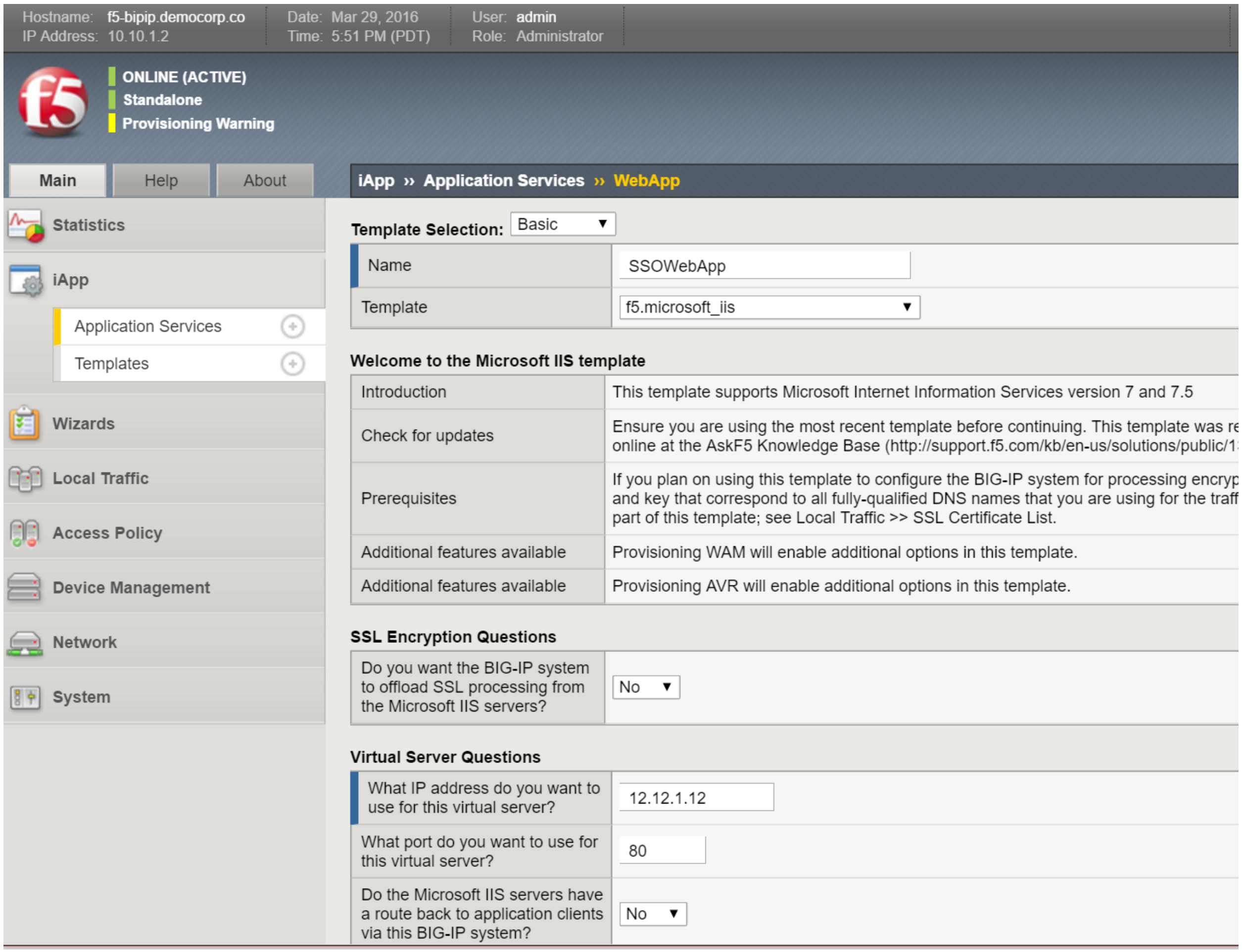
Publishing SAMPLE Web Application VIA F5 BIG-IP

We assume that you have an existing F5 BIG-IP setup where you can test the Okta integration.

If you are new to F5 BIG-IP, please refer to the F5 Support Site for download, setup and general information around F5 BIG-IP (https://support.f5.com/kb/en-us/products/big-ip_apm.html).

The instructions below assumes a Microsoft Windows Server environment with IIS enabled.

1. It is recommended to configure F5 BIG-IP to proxy requests to the test webserver by creating an iApp. Click iApp -> Application Services -> 'Create'
2. Provide a Name for this application and choose f5.microsoft_iis as the Template (use http template for generic webservers). Also provide the Virtual Server IP-Address on the external interface (e.g., 12.12.1.12)



Template Selection: Basic ▾

Name	SSOWebApp
Template	f5.microsoft_iis ▾

Welcome to the Microsoft IIS template

Introduction	This template supports Microsoft Internet Information Services version 7 and 7.5
Check for updates	Ensure you are using the most recent template before continuing. This template was re online at the AskF5 Knowledge Base (http://support.f5.com/kb/en-us/solutions/public/1
Prerequisites	If you plan on using this template to configure the BIG-IP system for processing encryp and key that correspond to all fully-qualified DNS names that you are using for the traff part of this template; see Local Traffic >> SSL Certificate List.
Additional features available	Provisioning WAM will enable additional options in this template.
Additional features available	Provisioning AVR will enable additional options in this template.

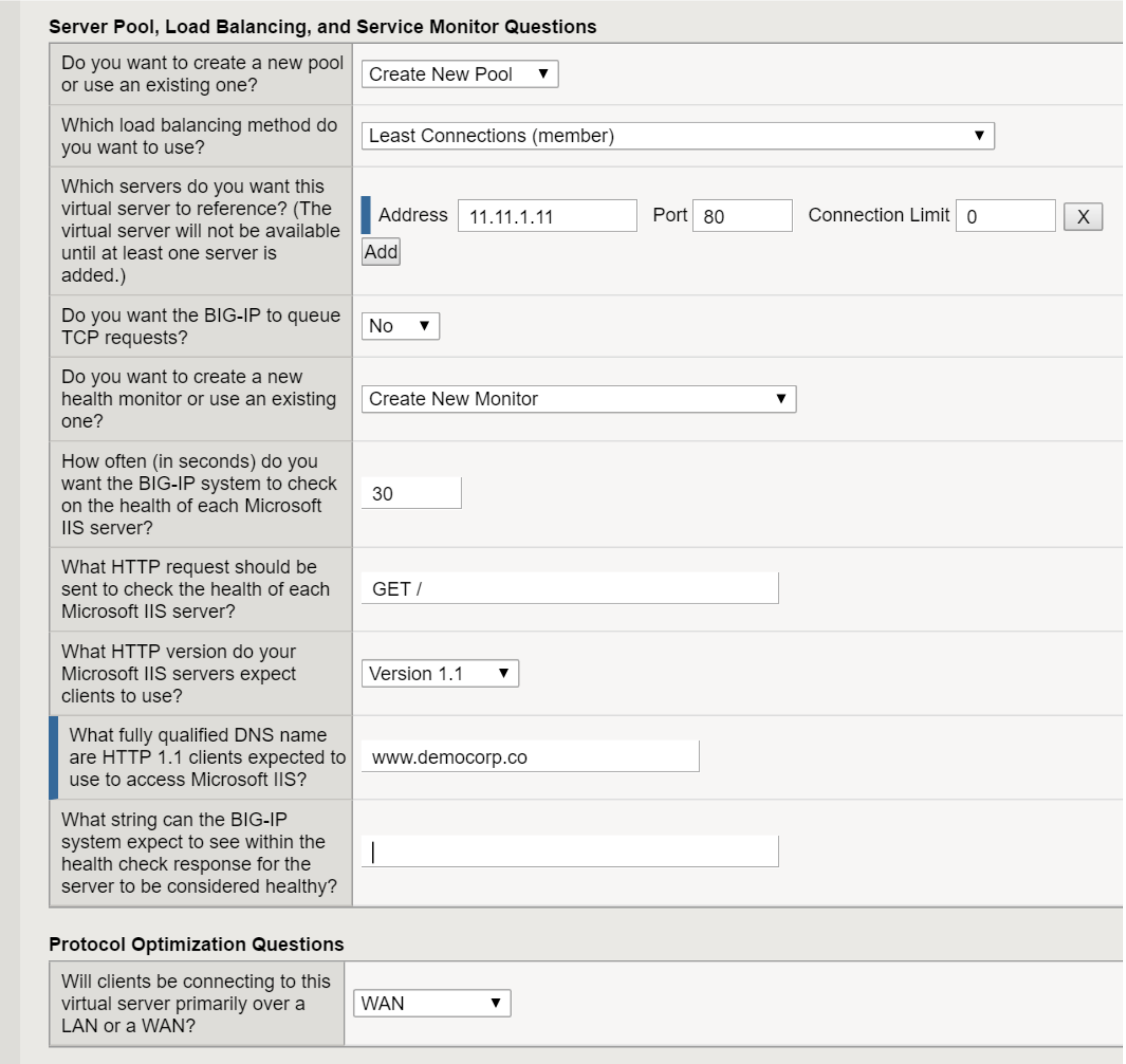
SSL Encryption Questions

Do you want the BIG-IP system to offload SSL processing from the Microsoft IIS servers?	No ▾

Virtual Server Questions

What IP address do you want to use for this virtual server?	12.12.1.12
What port do you want to use for this virtual server?	80
Do the Microsoft IIS servers have a route back to application clients via this BIG-IP system?	No ▾

3. Scroll down on the same page and under Server Pool, Load Balancing section, provide the IP-address of the test web server and port it is listening on (e.g., 11.11.1.11 and 80). Also provide an FQDN for the web server hostname (e.g., www.democorp.co) and click 'Finish'



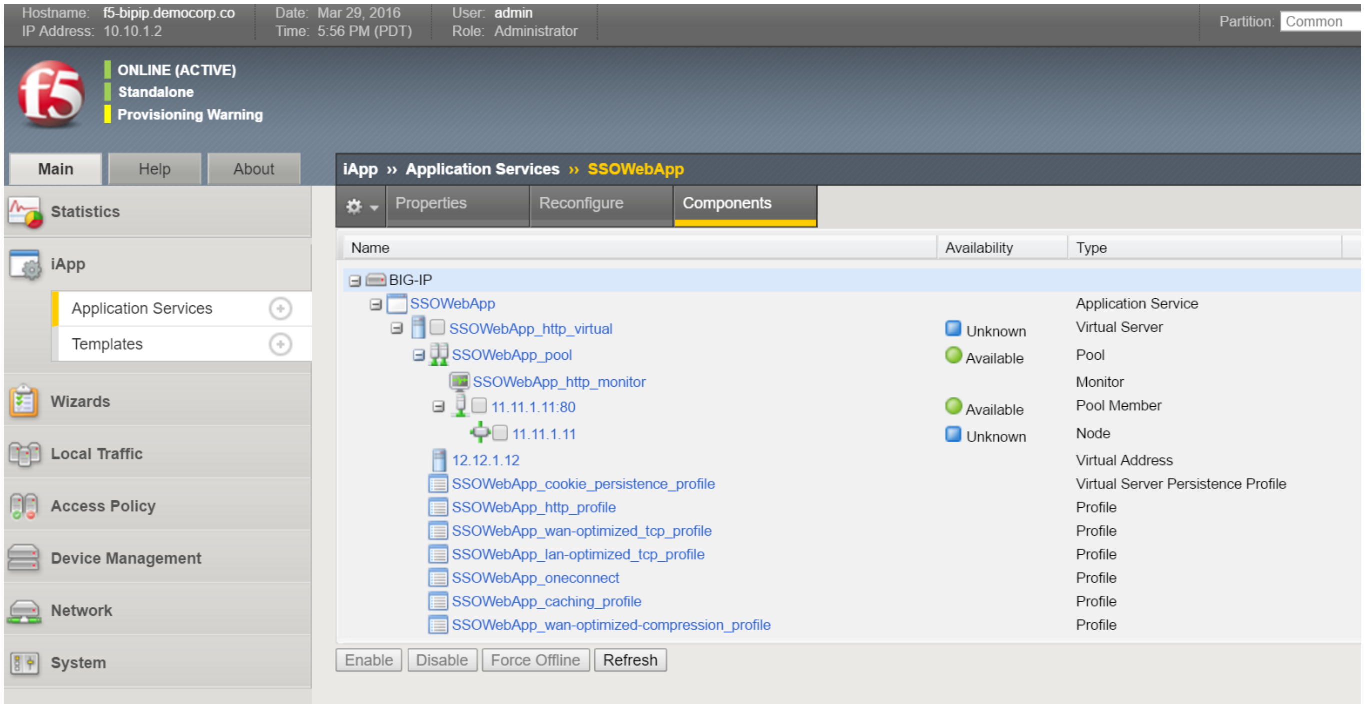
Server Pool, Load Balancing, and Service Monitor Questions

Do you want to create a new pool or use an existing one?	Create New Pool ▼
Which load balancing method do you want to use?	Least Connections (member) ▼
Which servers do you want this virtual server to reference? (The virtual server will not be available until at least one server is added.)	Address 11.11.1.11 Port 80 Connection Limit 0 X Add
Do you want the BIG-IP to queue TCP requests?	No ▼
Do you want to create a new health monitor or use an existing one?	Create New Monitor ▼
How often (in seconds) do you want the BIG-IP system to check on the health of each Microsoft IIS server?	30
What HTTP request should be sent to check the health of each Microsoft IIS server?	GET /
What HTTP version do your Microsoft IIS servers expect clients to use?	Version 1.1 ▼
What fully qualified DNS name are HTTP 1.1 clients expected to use to access Microsoft IIS?	www.democorp.co
What string can the BIG-IP system expect to see within the health check response for the server to be considered healthy?	

Protocol Optimization Questions

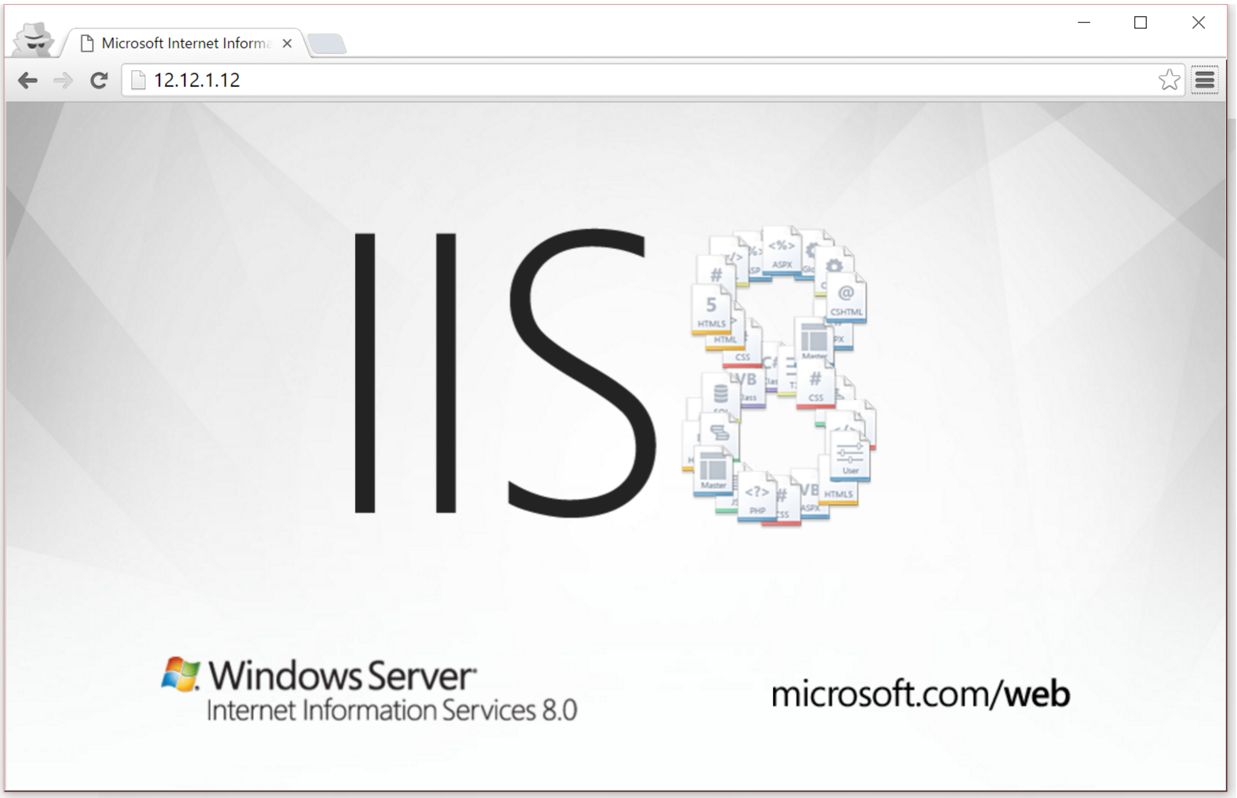
Will clients be connecting to this virtual server primarily over a LAN or a WAN?	WAN ▼

4. F5 BIG-IP will show the status of this application

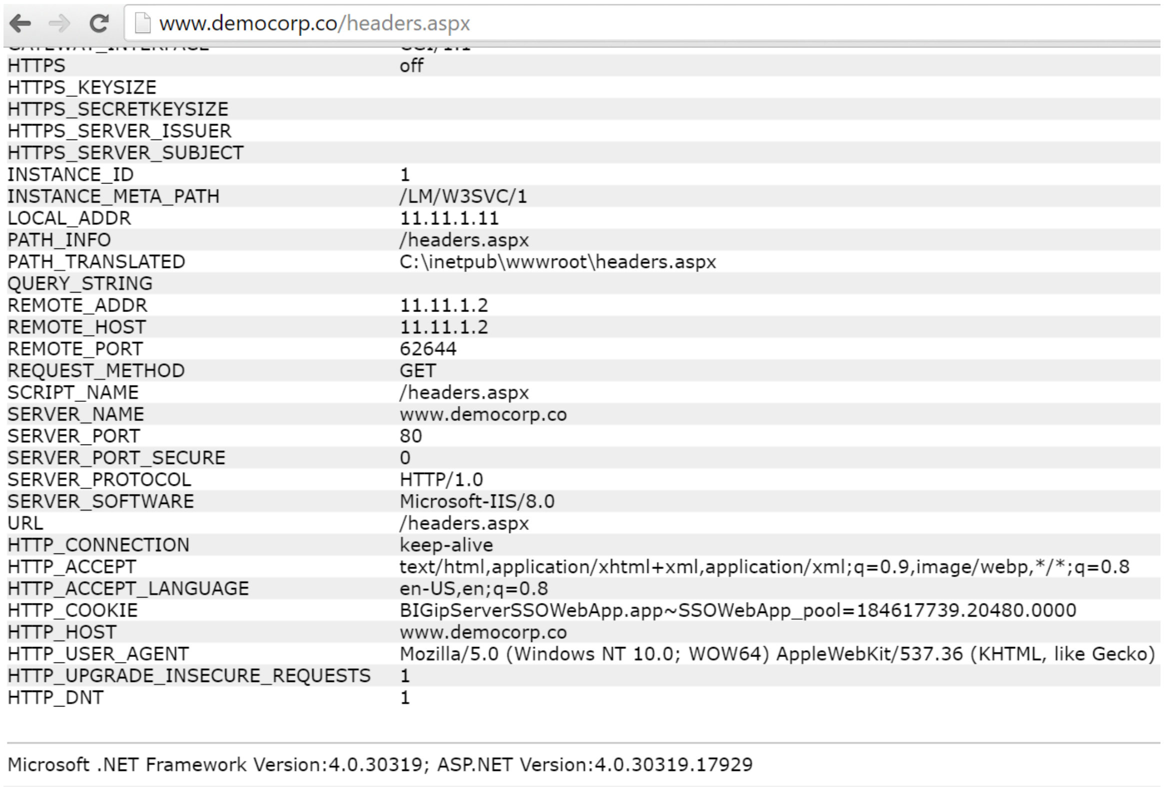


Name	Availability	Type
BIG-IP		
SSOWebApp		Application Service
SSOWebApp_http_virtual	Unknown	Virtual Server
SSOWebApp_pool	Available	Pool
SSOWebApp_http_monitor		Monitor
11.11.1.11:80	Available	Pool Member
11.11.1.11	Unknown	Node
12.12.1.12		Virtual Address
SSOWebApp_cookie_persistence_profile		Virtual Server Persistence Profile
SSOWebApp_http_profile		Profile
SSOWebApp_wan-optimized_tcp_profile		Profile
SSOWebApp_lan-optimized_tcp_profile		Profile
SSOWebApp_oneconnect		Profile
SSOWebApp_caching_profile		Profile
SSOWebApp_wan-optimized-compression_profile		Profile

5. To test the connection, launch a browser on the host machine and point it to the external IP-address chosen in the previous screen (e.g., 12.12.1.12 and it should render the backend webserver page)



6. It is recommended to put a hosts file entry to point a test hostname (e.g., www.democorp.co) to this backend app IP-address (e.g., 12.12.1.12). Also, place a file headers.aspx in the root of the webserver's folder with the following line to display all headers:
<%@ Page Language="C#" Trace="true"%>



www.democorp.co/headers.aspx

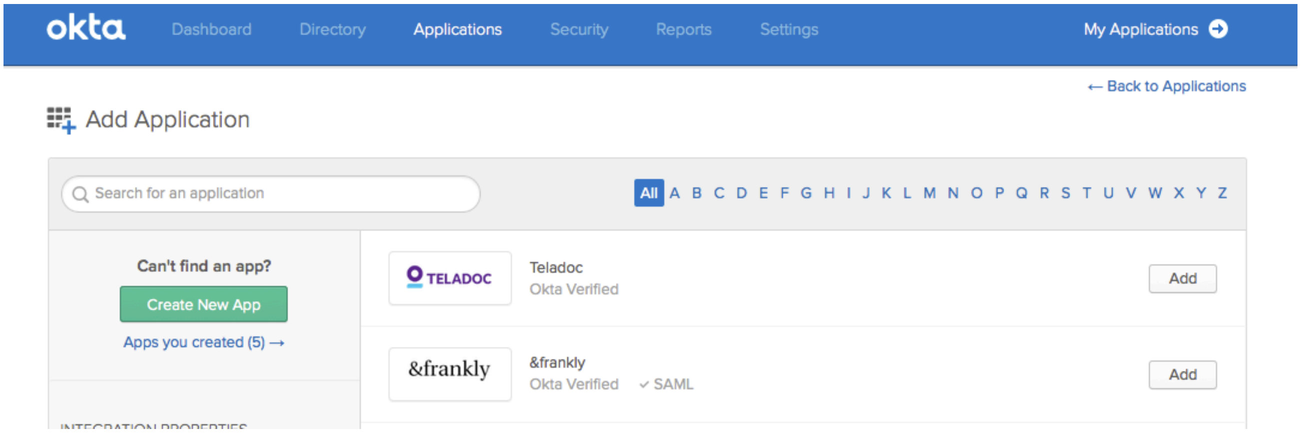
GATEWAY_INTERFACE	CGI/1.1
HTTPS	off
HTTPS_KEYSIZE	
HTTPS_SECRETKEYSIZE	
HTTPS_SERVER_ISSUER	
HTTPS_SERVER_SUBJECT	
INSTANCE_ID	1
INSTANCE_META_PATH	/LM/W3SVC/1
LOCAL_ADDR	11.11.1.11
PATH_INFO	/headers.aspx
PATH_TRANSLATED	C:\inetpub\wwwroot\headers.aspx
QUERY_STRING	
REMOTE_ADDR	11.11.1.2
REMOTE_HOST	11.11.1.2
REMOTE_PORT	62644
REQUEST_METHOD	GET
SCRIPT_NAME	/headers.aspx
SERVER_NAME	www.democorp.co
SERVER_PORT	80
SERVER_PORT_SECURE	0
SERVER_PROTOCOL	HTTP/1.0
SERVER_SOFTWARE	Microsoft-IIS/8.0
URL	/headers.aspx
HTTP_CONNECTION	keep-alive
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.8
HTTP_COOKIE	BIGipServerSSOWebApp.app~SSOWebApp_pool=184617739.20480.0000
HTTP_HOST	www.democorp.co
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_DNT	1

Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.0.30319.17929

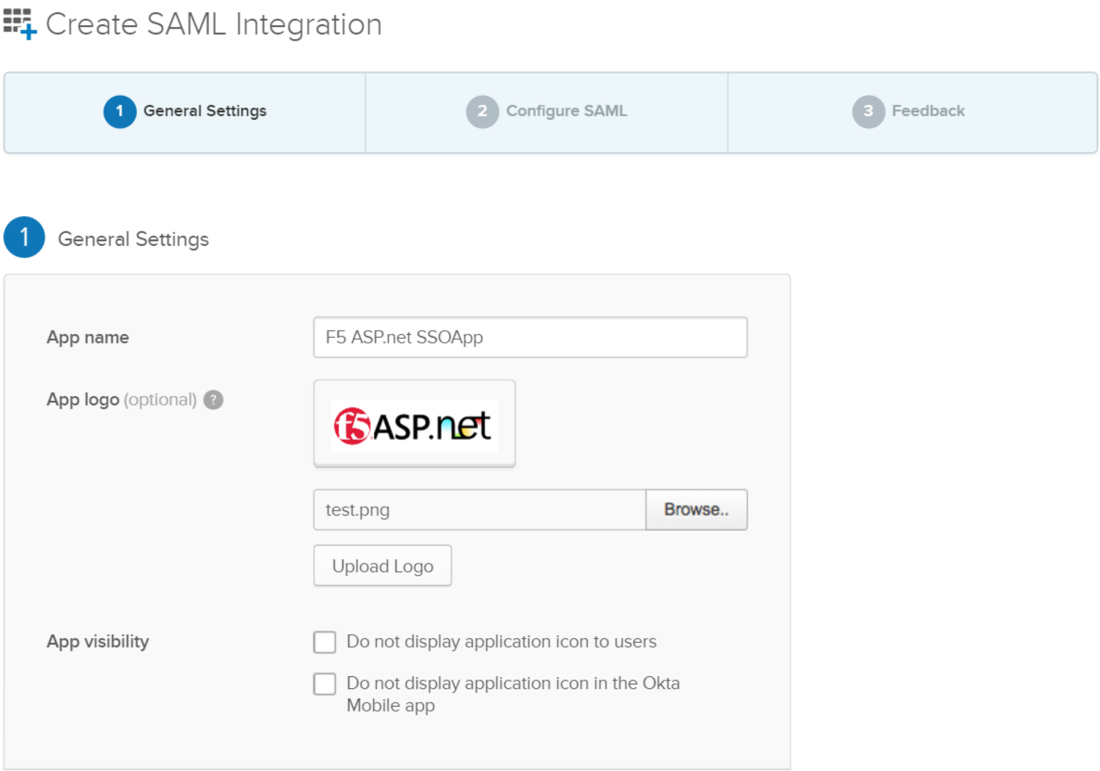
7. The page in previous step will be used to verify Okta integration in the next section

Configuring Okta as SAML 2.0 Identity Provider for F5 BIG-IP

1. Under "Applications" – choose "Add Application" option and click on "Create New App".



2. Create a new SAML 2.0 App in Okta and provide it a name and optionally choose a logo



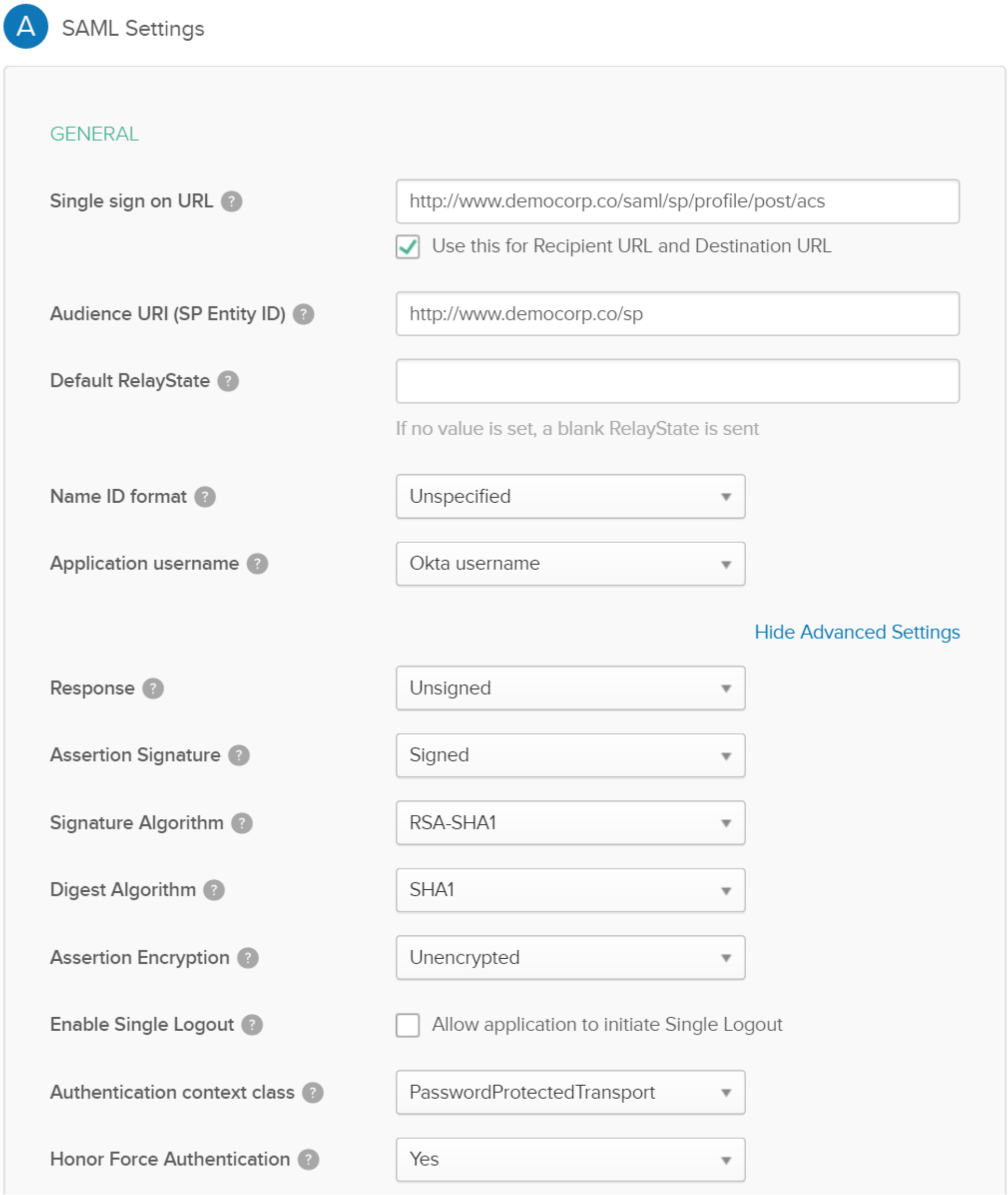
App name: F5 ASP.net SSOApp

App logo (optional): test.png

App visibility:
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile app

3. In SAML Settings, provide the Single Sign On URL (should be: <**`https://external-f5-hostname/saml/sp/profile/acs`**>), Audience URI (SP Entity ID).

   Note that F5 BIG-IP versions prior to 11.5.0 (not included) only supports SHA1 as Signature Algorithm.so it has to be set to **`RSA-SHA1`**. F5 BIG-IP version 11.5.0 and above supports RSA-SHA256. It is strongly recommended that you upgrade to a version that supports RSA-SHA256.



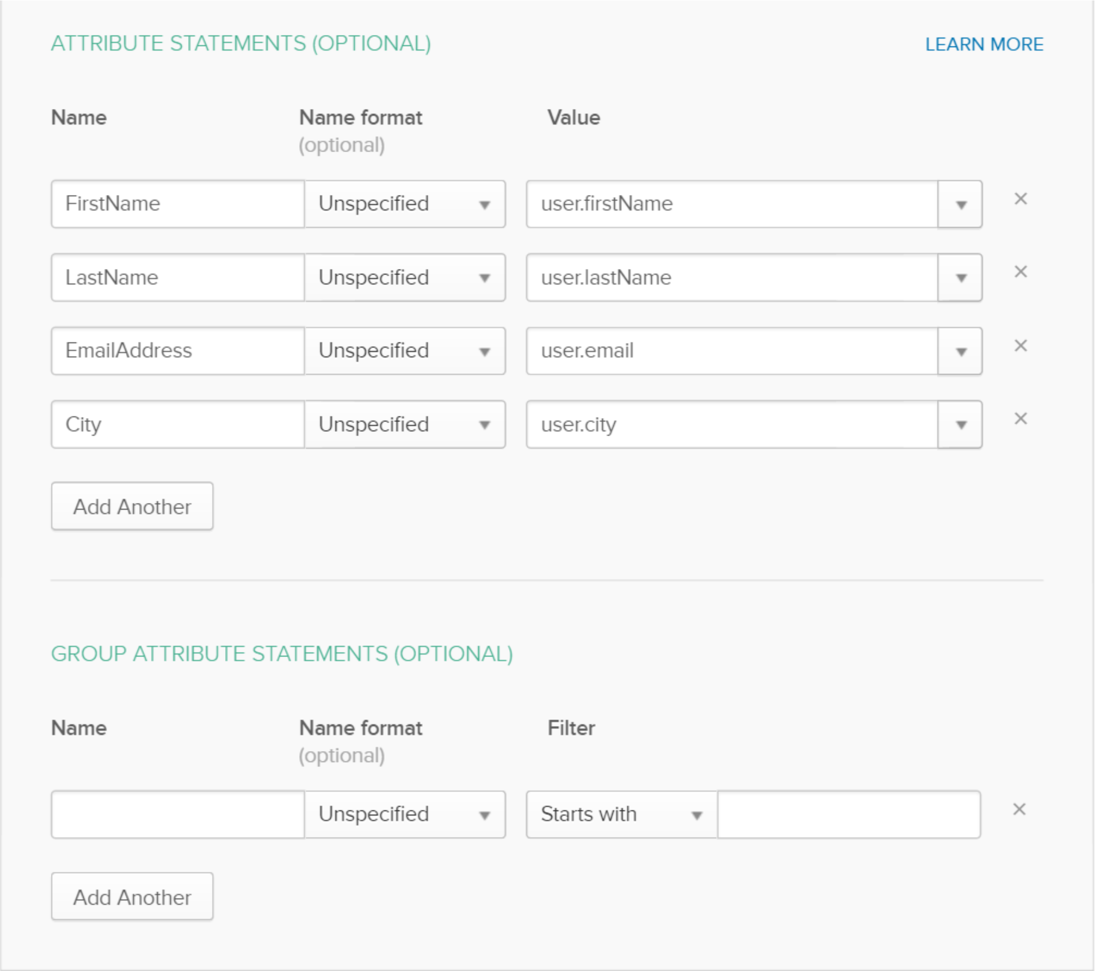
A SAML Settings

GENERAL

Single sign on URL	http://www.democorp.co/saml/sp/profile/post/acs ☑ Use this for Recipient URL and Destination URL
Audience URI (SP Entity ID)	http://www.democorp.co/sp
Default RelayState	If no value is set, a blank RelayState is sent
Name ID format	Unspecified
Application username	Okta username

Response	Unsigned
Assertion Signature	Signed
Signature Algorithm	RSA-SHA1
Digest Algorithm	SHA1
Assertion Encryption	Unencrypted
Enable Single Logout	□ Allow application to initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes

4. Scroll down on the same page and provide custom attributes to be passed in the SAML assertion to the ASP .NET application



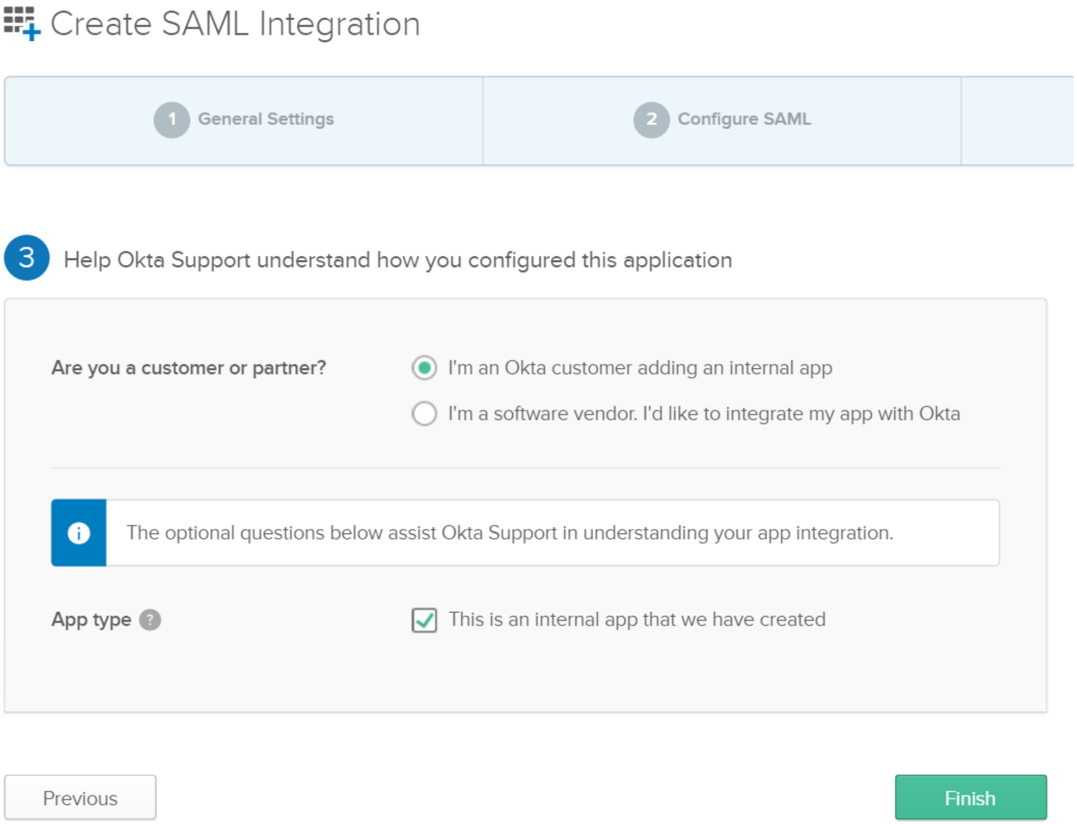
ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Value
FirstName	Unspecified	user.firstName
LastName	Unspecified	user.lastName
EmailAddress	Unspecified	user.email
City	Unspecified	user.city

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter	
	Unspecified	Starts with	

5. Click ‘Finish’ on the next screen



Create SAML Integration

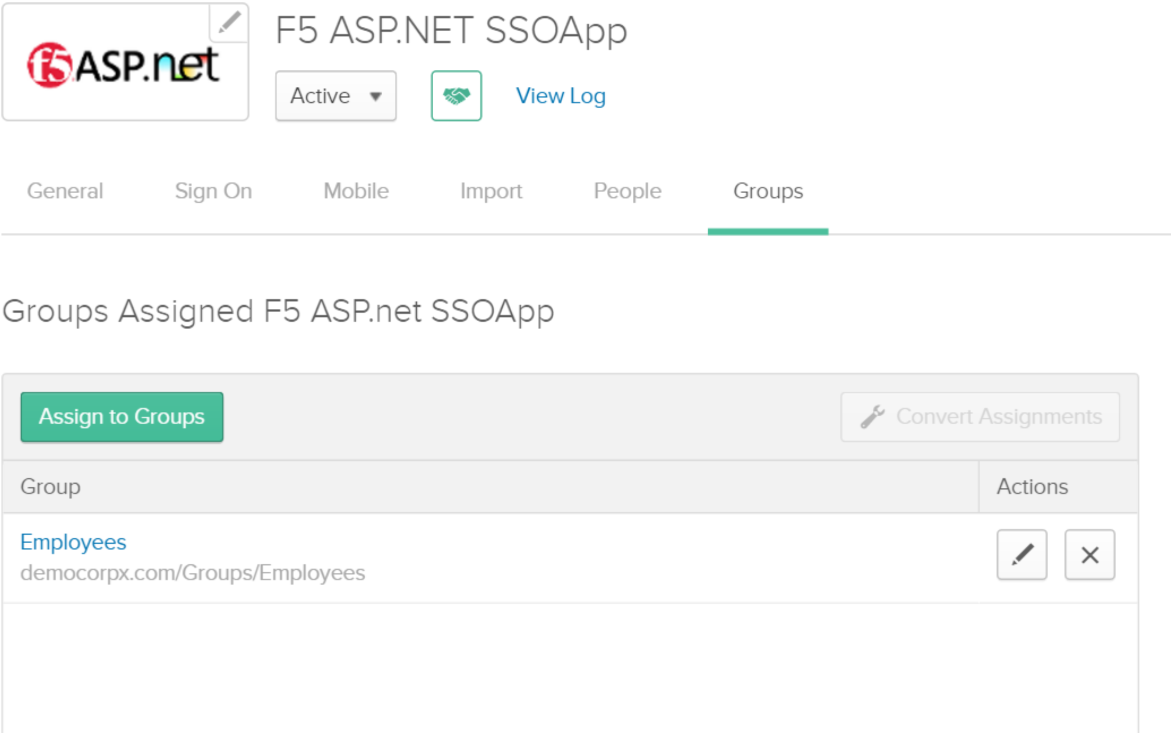
3 Help Okta Support understand how you configured this application

Are you a customer or partner? ● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type ☑ This is an internal app that we have created

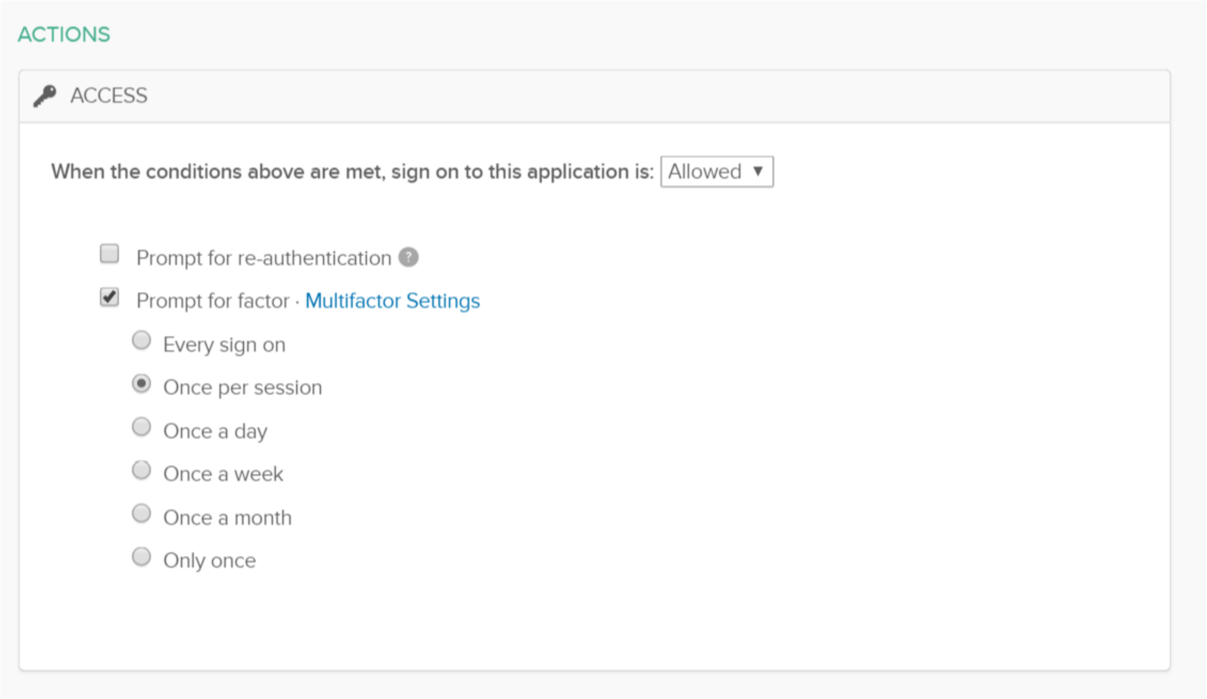
6. This app can now be assigned to authorized users or groups. Additional security options like App Sign On policy to provide MFA and granular control can be applied as well



F5 ASP.NET SSOApp

Groups Assigned F5 ASP.net SSOApp

Group	Actions
Employees democorpx.com/Groups/Employees	



ACTIONS

ACCESS

When the conditions above are met, sign on to this application is: Allowed ▼

□ Prompt for re-authentication

☑ Prompt for factor · Multifactor Settings

○ Every sign on

● Once per session

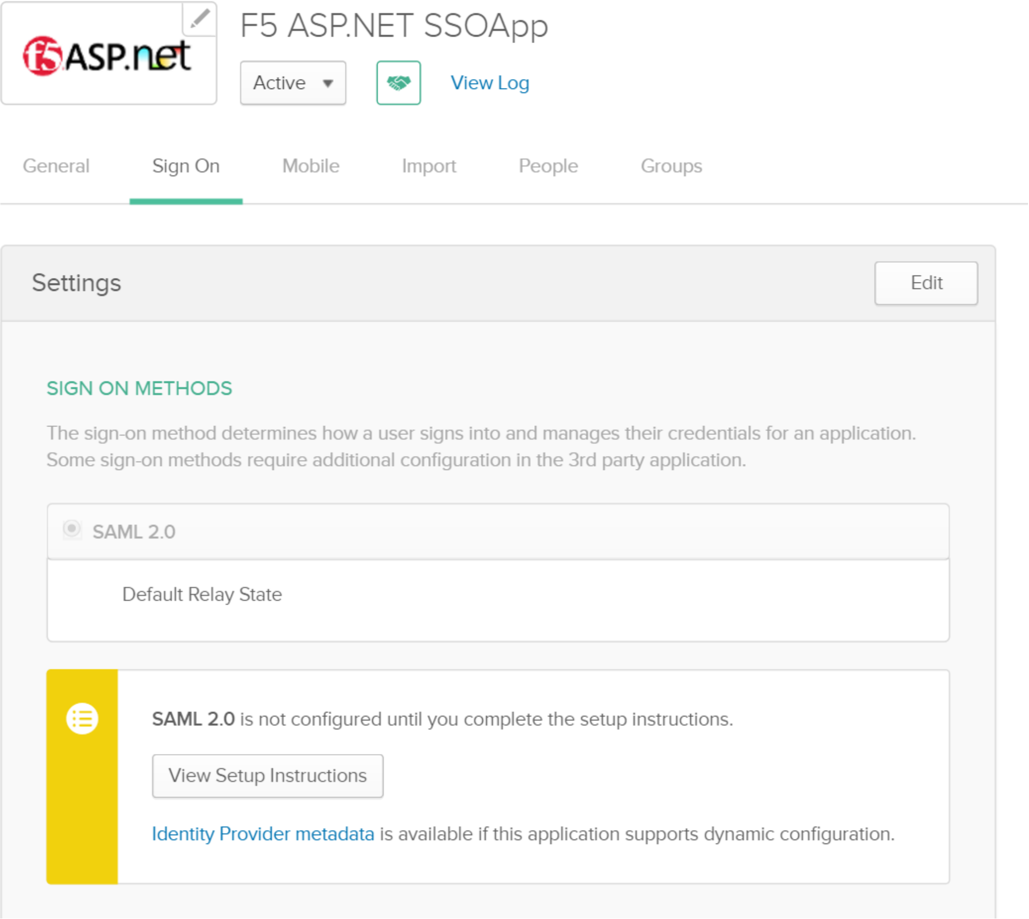
○ Once a day

○ Once a week

○ Once a month

○ Only once

7. Click on the 'Sign On' tab in the app and then click on then 'Identity Provider metadata' link to save the SAML metadata.xml that will be imported in F5 BIG-IP



F5 ASP.NET SSOApp

Active ▼ View Log

General | Sign On | Mobile | Import | People | Groups

Settings Edit

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

● SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

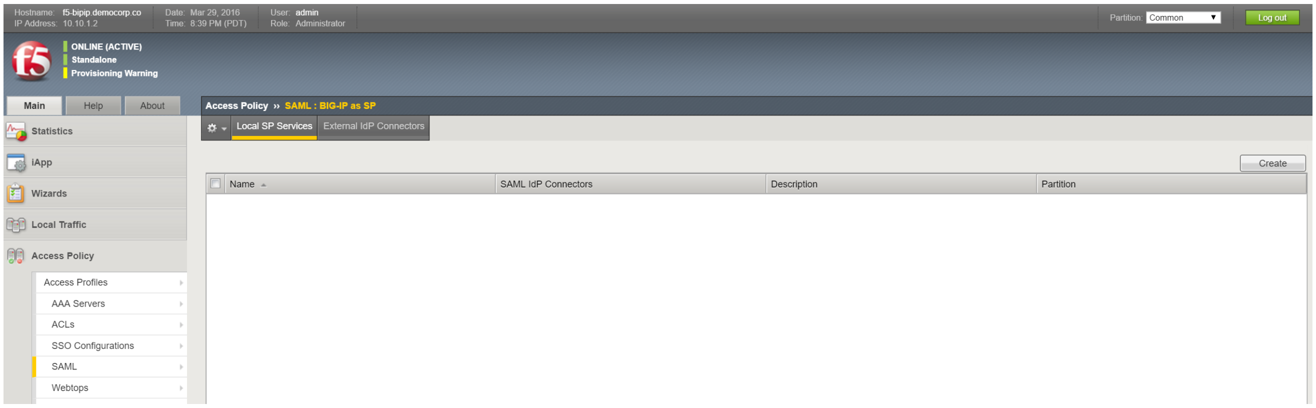
8. Okta SAML Identity Provider setup is complete.

Configuring F5 BIG-IP as SAML 2.0 Service Provider for Okta

Configure SAML SP Service

Configure a SAML SP service for F5 BIG-IP Access Policy Manager to provide AAA authentication, requesting authentication and receiving assertions from a SAML IdP.

1. On the Main tab, click Access Policy > SAML > BIG-IP as SP. The BIG-IP as SP screen opens and displays a list of local SP services



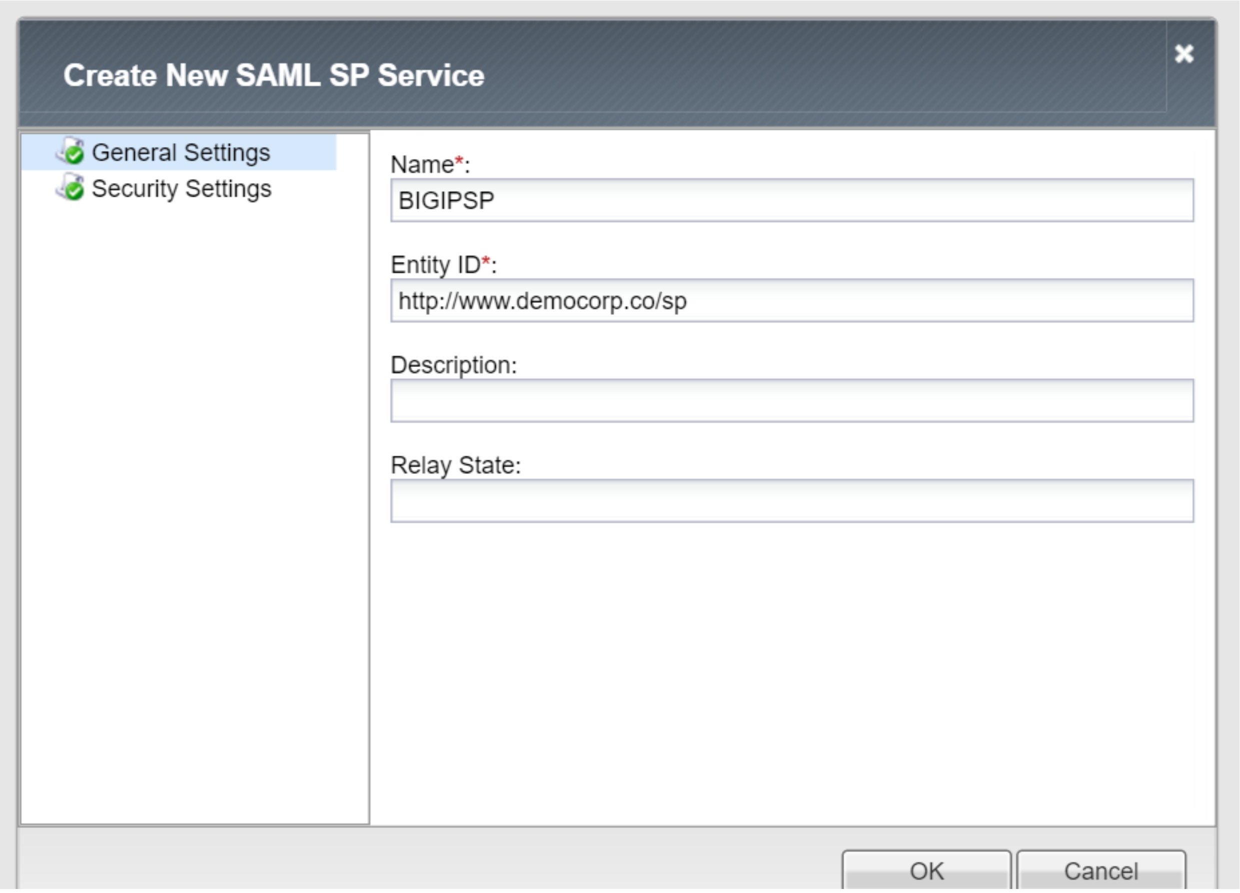
Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 8:39 PM (PDT)
User: admin
Role: Administrator
Partition: Common

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Access Policy » SAML : BIG-IP as SP

□ Name	SAML IdP Connectors	Description	Partition

2. In the Name field, type a unique name for the SAML SP service. In the Entity ID field, provide the Audience URI that was provided in Okta SAML configuration

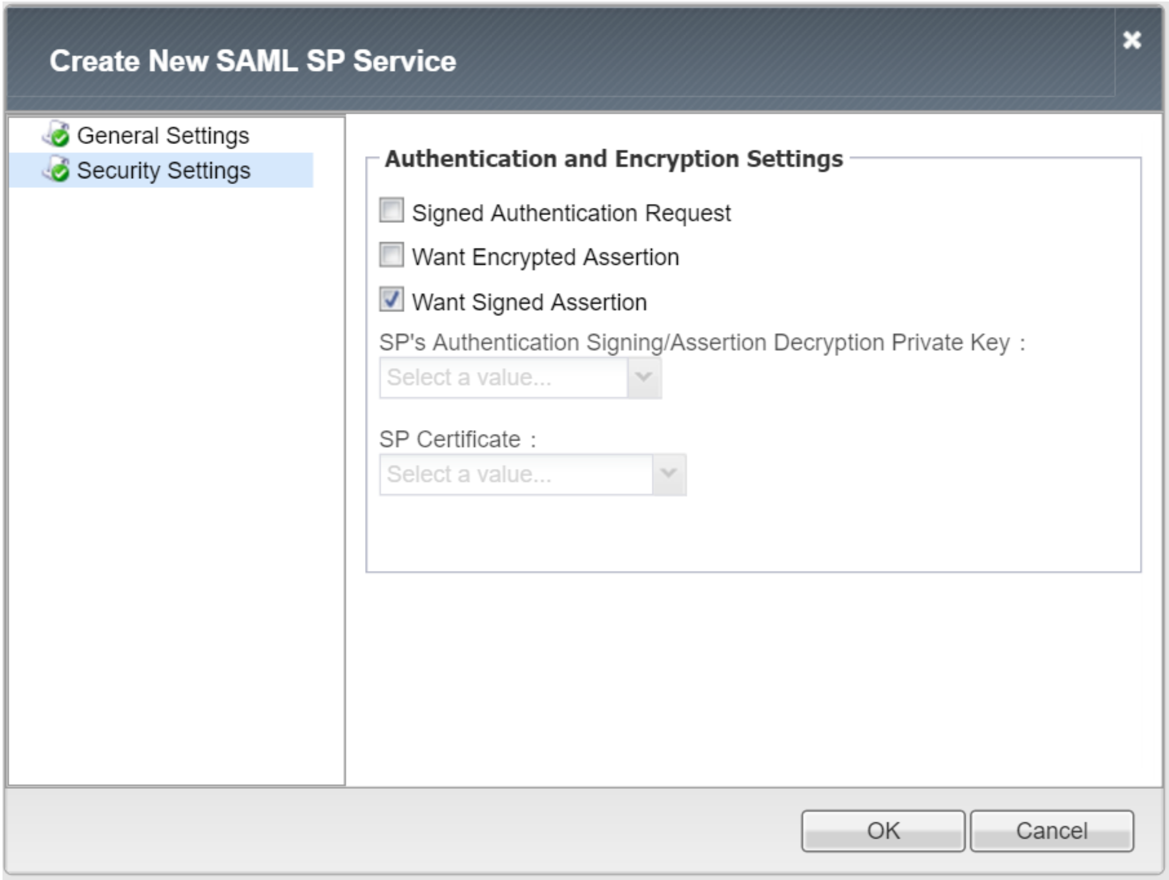


Name*: BIGIPSP

Entity ID*: http://www.democorp.co/sp

Description:

Relay State:



Create New SAML SP Service

General Settings
Security Settings

Authentication and Encryption Settings

□ Signed Authentication Request
□ Want Encrypted Assertion
☑ Want Signed Assertion

SP's Authentication Signing/Assertion Decryption Private Key : Select a value...

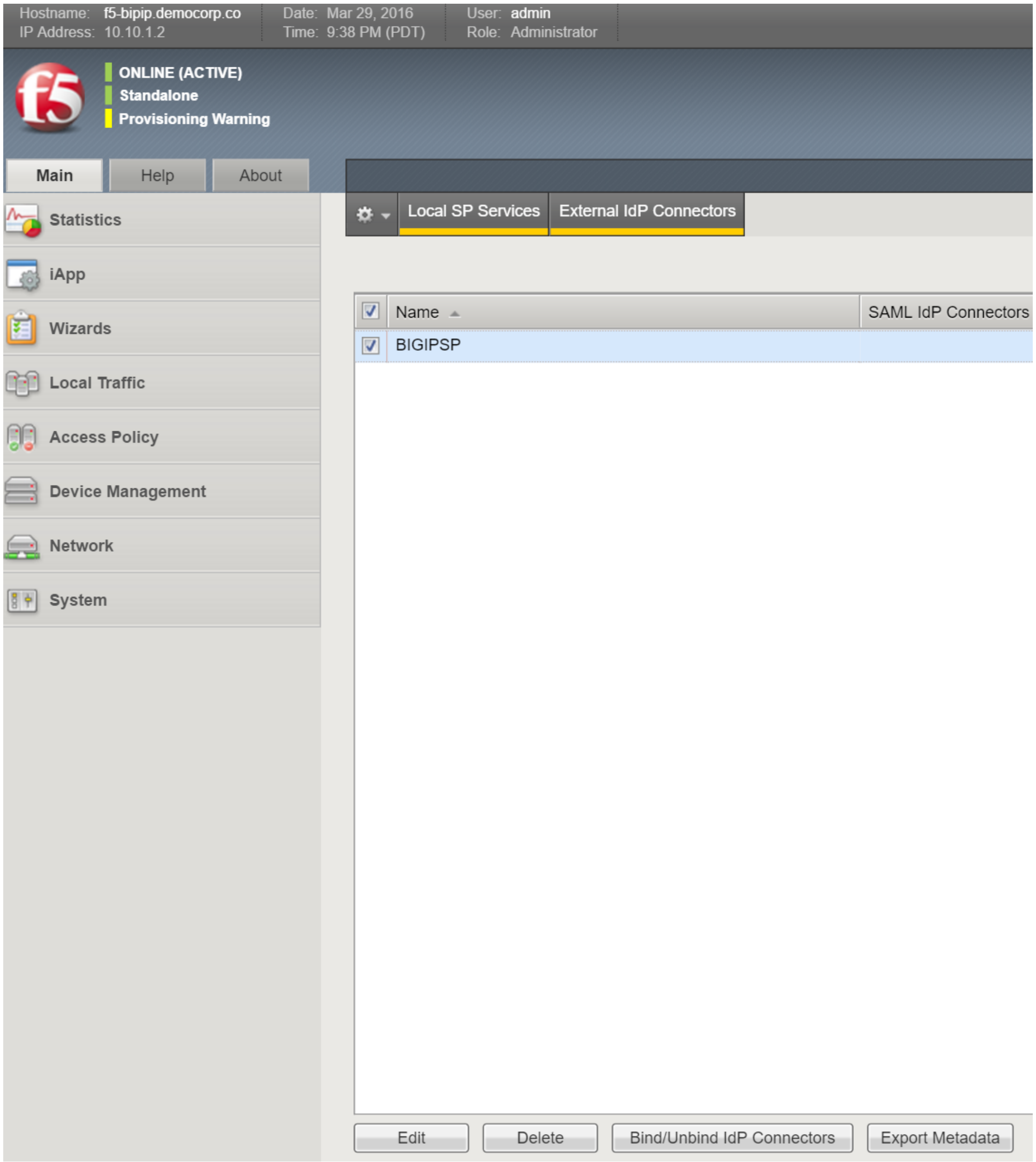
SP Certificate : Select a value...

3. Click ‘OK’

Configure SAML IdP Connector and Bind SAML SP Service to SAML IdP Connector

Configure Okta as SAML IdP connector in F5 BIG-IP so that Access Policy Manager (as a SAML service provider) can send authentication requests to Okta IdP, relying on it to authenticate users and to provide access to resources behind APM.

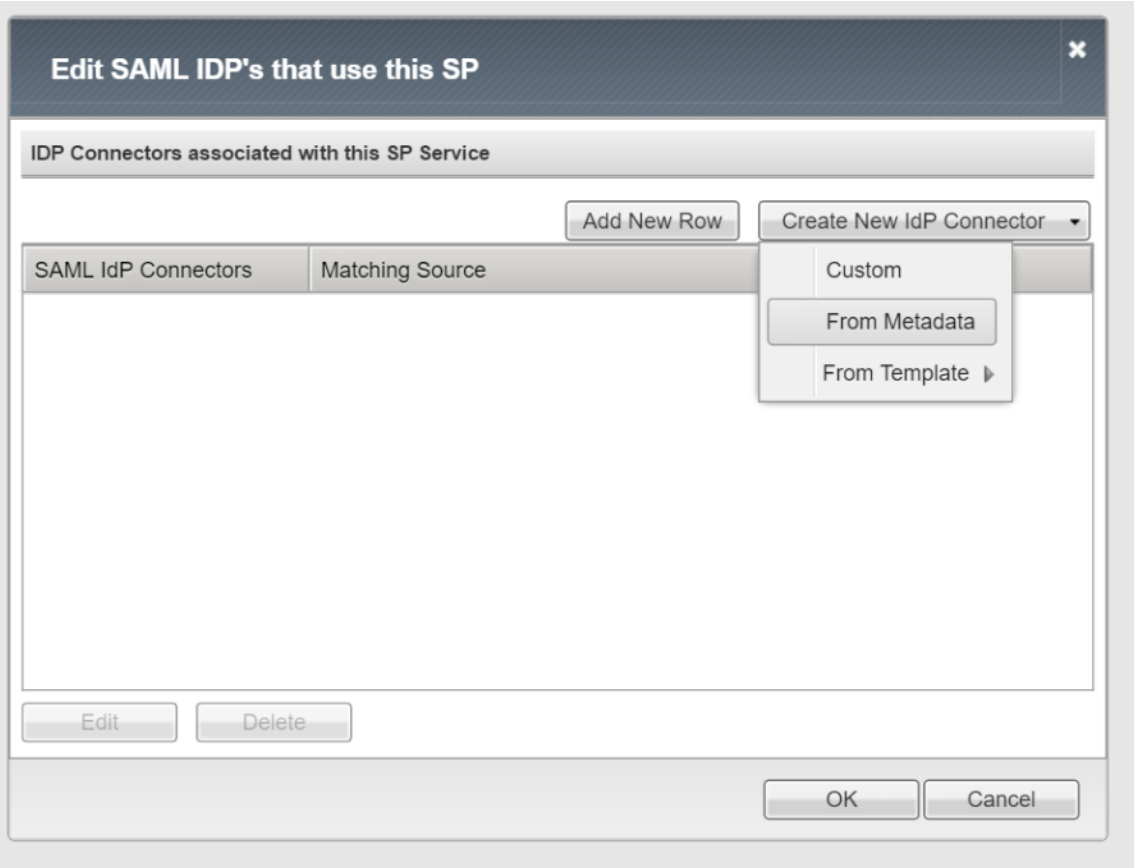
1. On the Main tab, click Access Policy > SAML > BIG-IP as SP. The BIG-IP as SP screen opens and displays a list of local SP services. Select 'BIGIPSP' SAML SP service from the list.



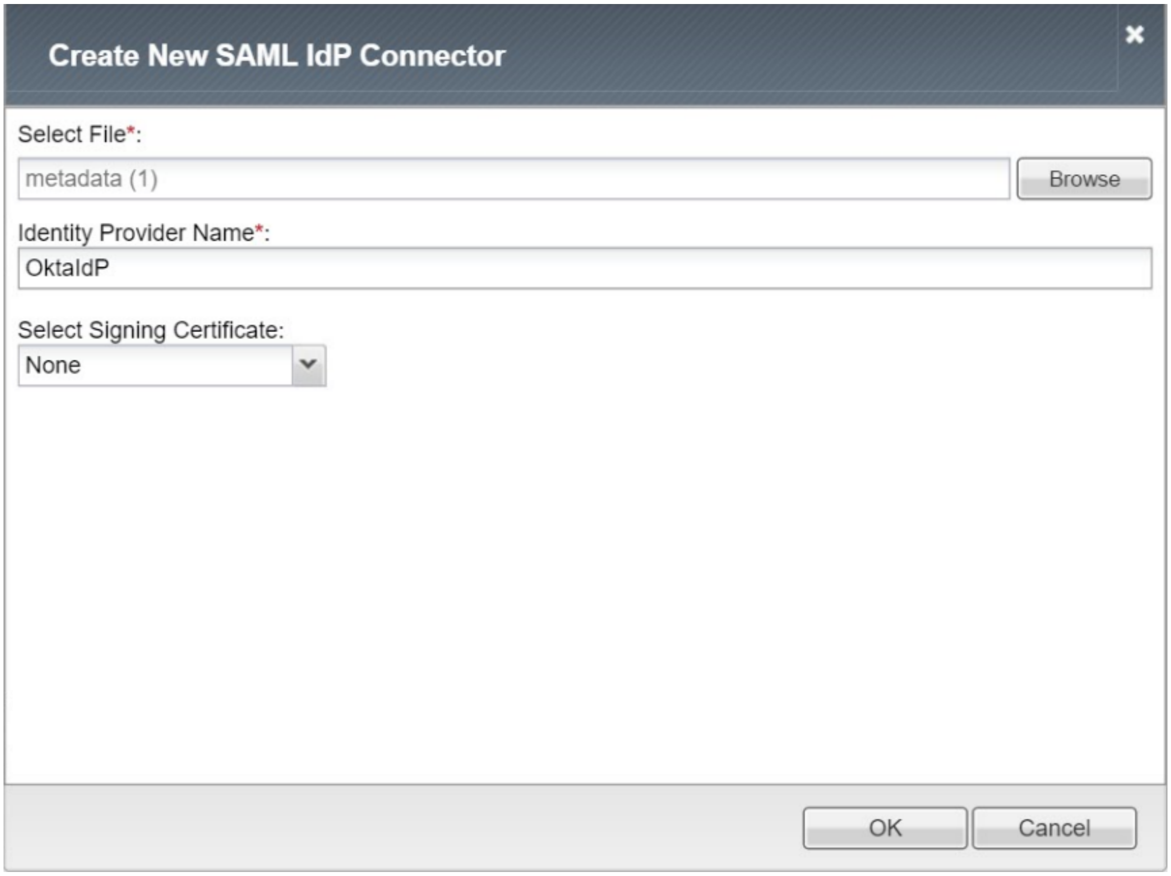
Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 9:38 PM (PDT)
User: admin
Role: Administrator

☑	Name	SAML IdP Connectors
☑	BIGIPSP	

2. Click 'Bind/Unbind IdP Connectors'. Then click 'Create New IdP Connector' and 'From Metadata'



3. Browse to metadata.xml download from Okta and enter an 'Identity Provider Name' and click 'OK'



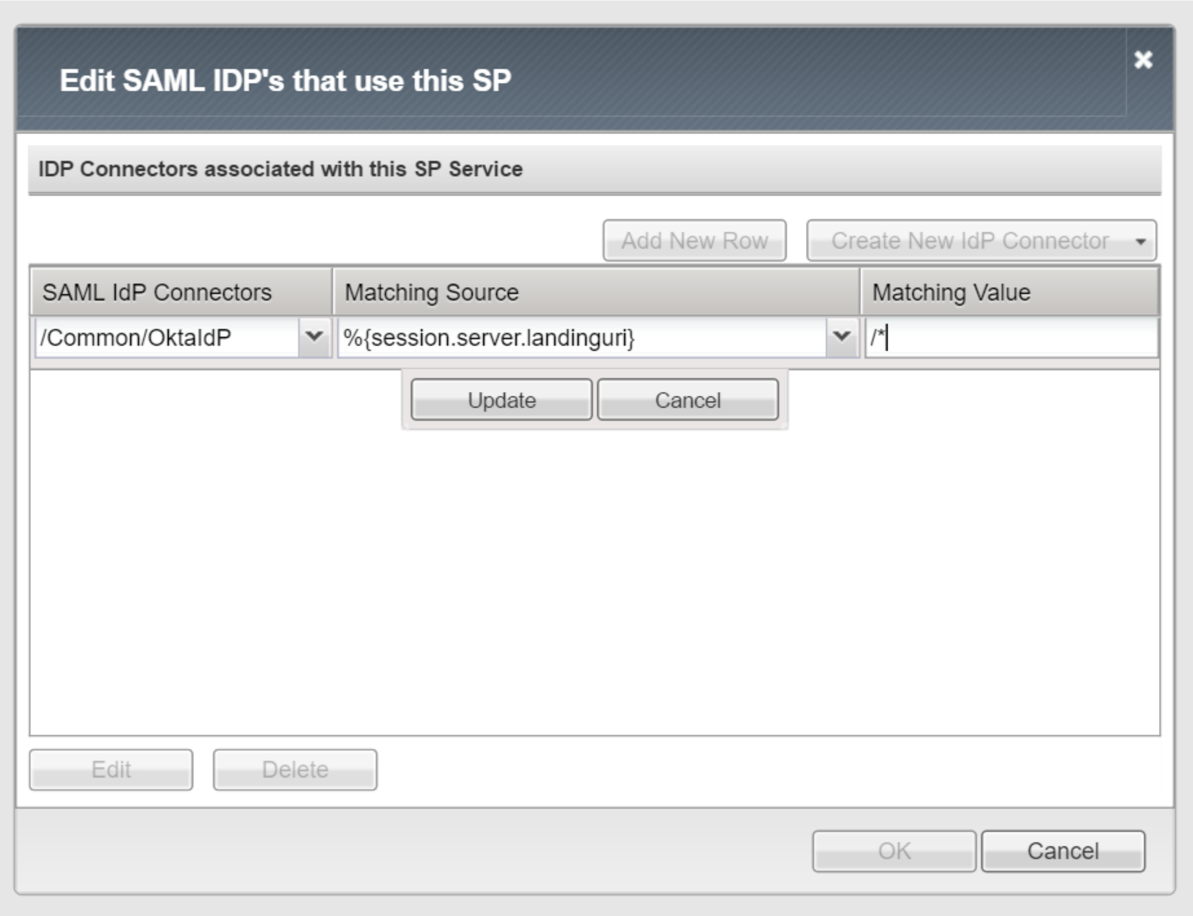
Create New SAML IdP Connector

Select File*: metadata (1)

Identity Provider Name*: OktaIdP

Select Signing Certificate: None

4. This will create an Okta IdP Connector and also import its signing certificate
5. Click ‘Add New Row’. Choose OktaIdP as the SAML IdP Connect, Matching Source as: %{session.server.landinguri} and Matching Value as /*. It tells F5 BIG-IP to use OktaIdP for all requests on this webserver. This URI can be adjusted based on specific folders or other Matching Source parameters. Click ‘OK’


Edit SAML IDP's that use this SP
IDP Connectors associated with this SP Service
Add New Row
Create New IdP Connector
Update
Cancel
Edit
Delete
OK
Cancel

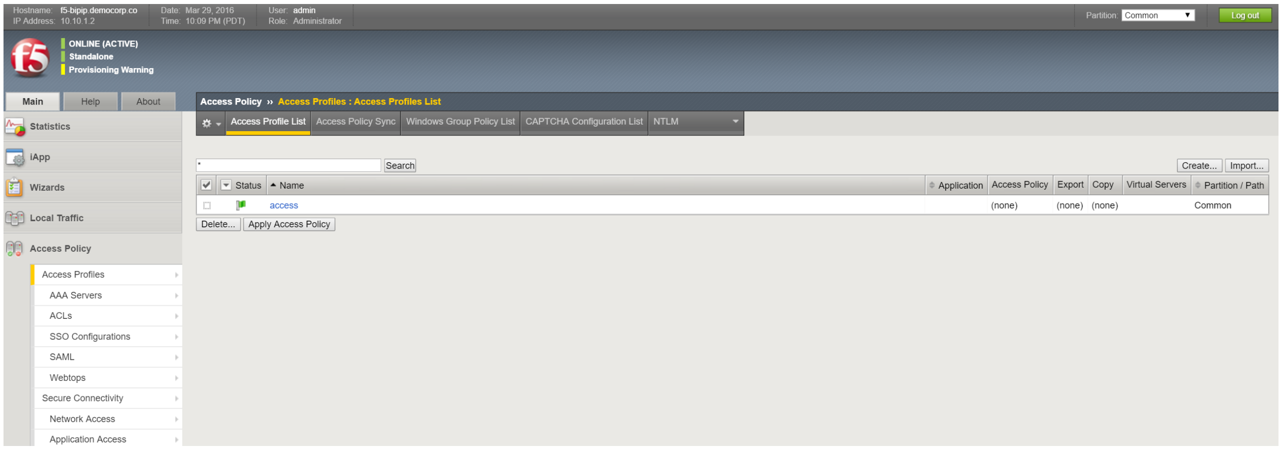
SAML IdP Connectors	Matching Source	Matching Value
/Common/OktaIdP	%{session.server.landinguri}	/*

6. SAML IdP and SP setup is complete.

Configure an F5 BIG-IP Access Policy to Authenticate with Okta SAML IdP

With the F5 BIG-IP system as a SAML service provider, configure an F5 BIG-IP access policy to direct users to Okta SAML IdP for authentication.

1. On the Main tab, click Access Policy > Access Profiles. The Access Profiles List screen opens. Click 'Create'



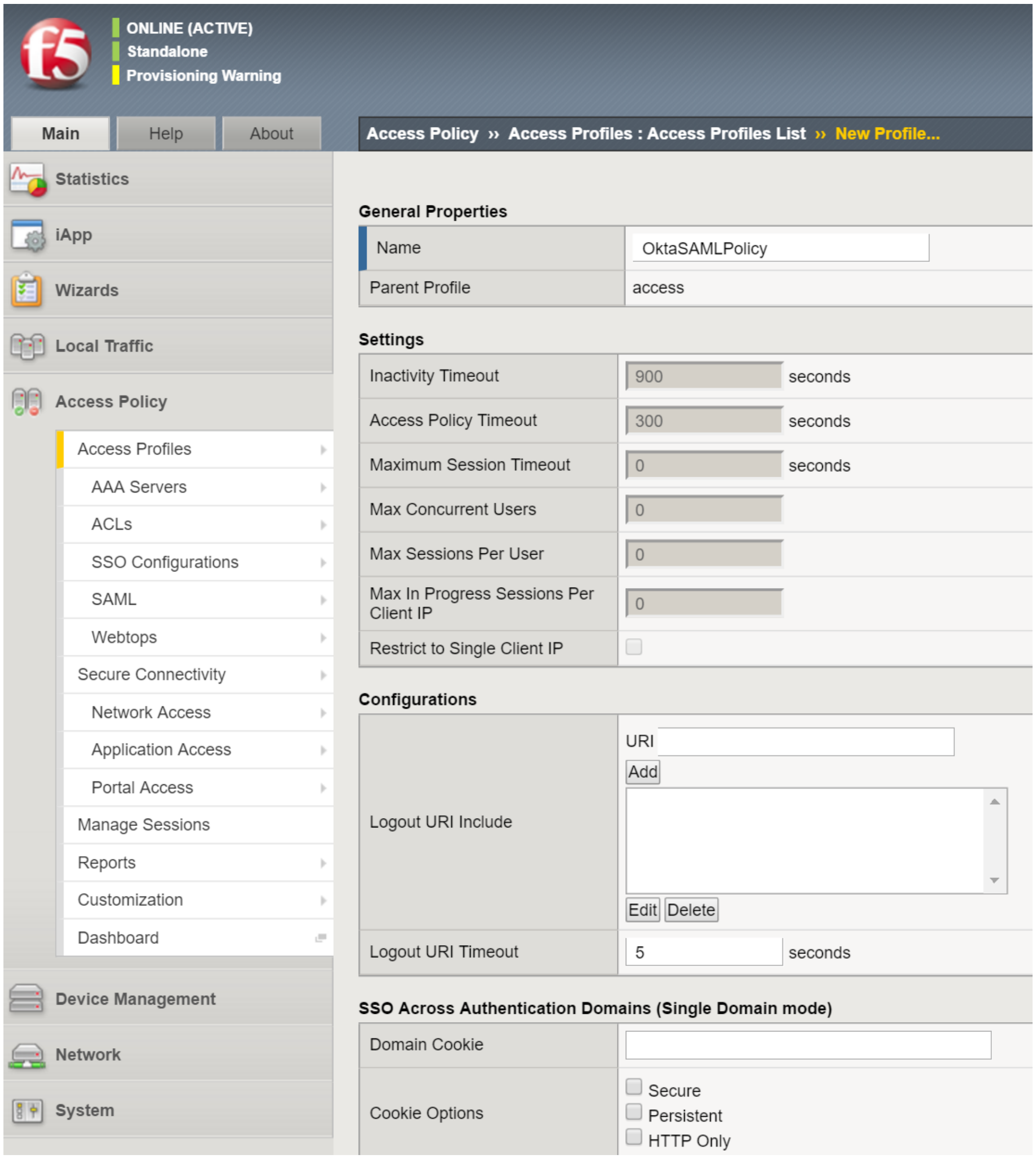
Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 10:09 PM (PDT)
User: admin
Role: Administrator
Partition: Common

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Access Policy » Access Profiles : Access Profiles List

☑	Status	Name	Application	Access Policy	Export	Copy	Virtual Servers	Partition / Path
□	🟩	access		(none)	(none)	(none)		Common

2. Provide the policy a name. In non-HTTPS test environment, make sure the "Secure" cookie option is deselected. Other custom values for timeouts and session can be optionally provided. Choose a Language and click 'Finished'



General Properties

Name	OktaSAMLPolicy
Parent Profile	access

Settings

Inactivity Timeout	900 seconds
Access Policy Timeout	300 seconds
Maximum Session Timeout	0 seconds
Max Concurrent Users	0
Max Sessions Per User	0
Max In Progress Sessions Per Client IP	0
Restrict to Single Client IP	□

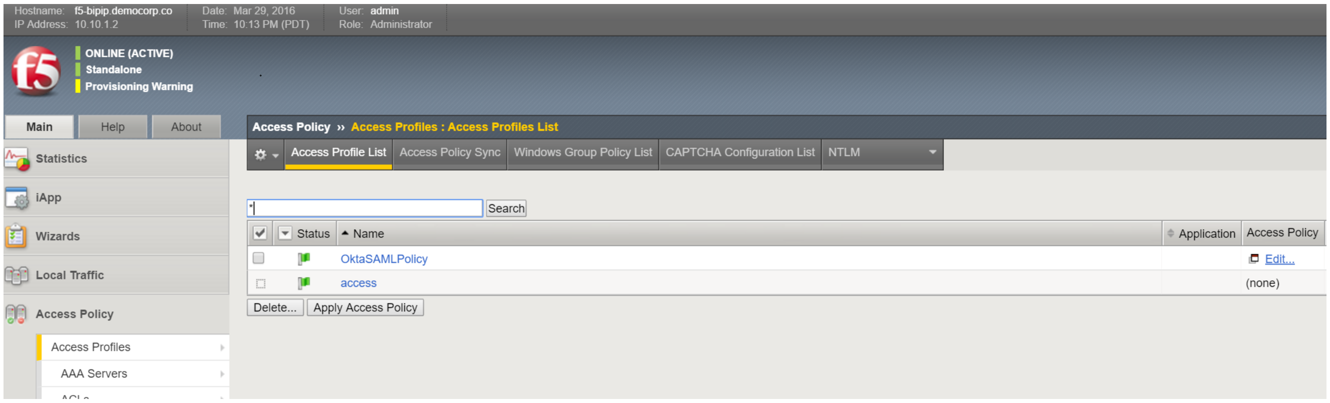
Configurations

Logout URI Include	URI
Logout URI Timeout	5 seconds

SSO Across Authentication Domains (Single Domain mode)

Domain Cookie	
Cookie Options	□ Secure □ Persistent □ HTTP Only

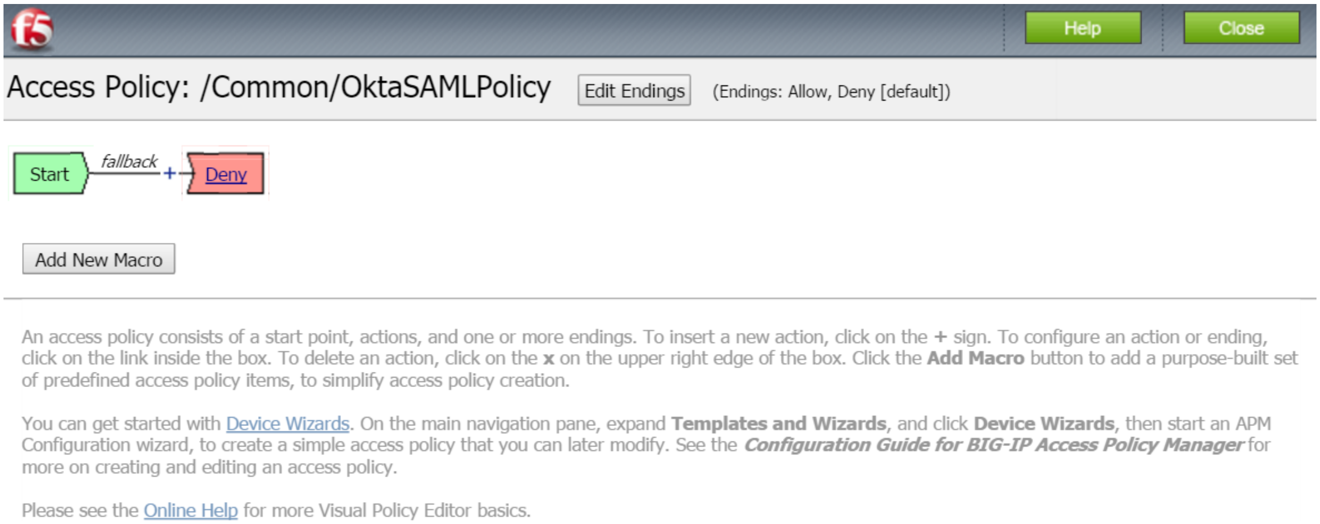
3. After the policy has been created, click on ‘Edit…’ under the ‘Access Policy’ column



Hostname: f5-bipip.democorp.co IP Address: 10.10.1.2 Date: Mar 29, 2016 Time: 10:13 PM (PDT) User: admin Role: Administrator

☑	Status	Name	Application	Access Policy
□		OktaSAMLPolicy		Edit...
□		access		(none)

4. The F5 BIG-IP APM visual policy editor opens the access policy in a separate screen displaying the default policy



Access Policy: /Common/OktaSAMLPolicy

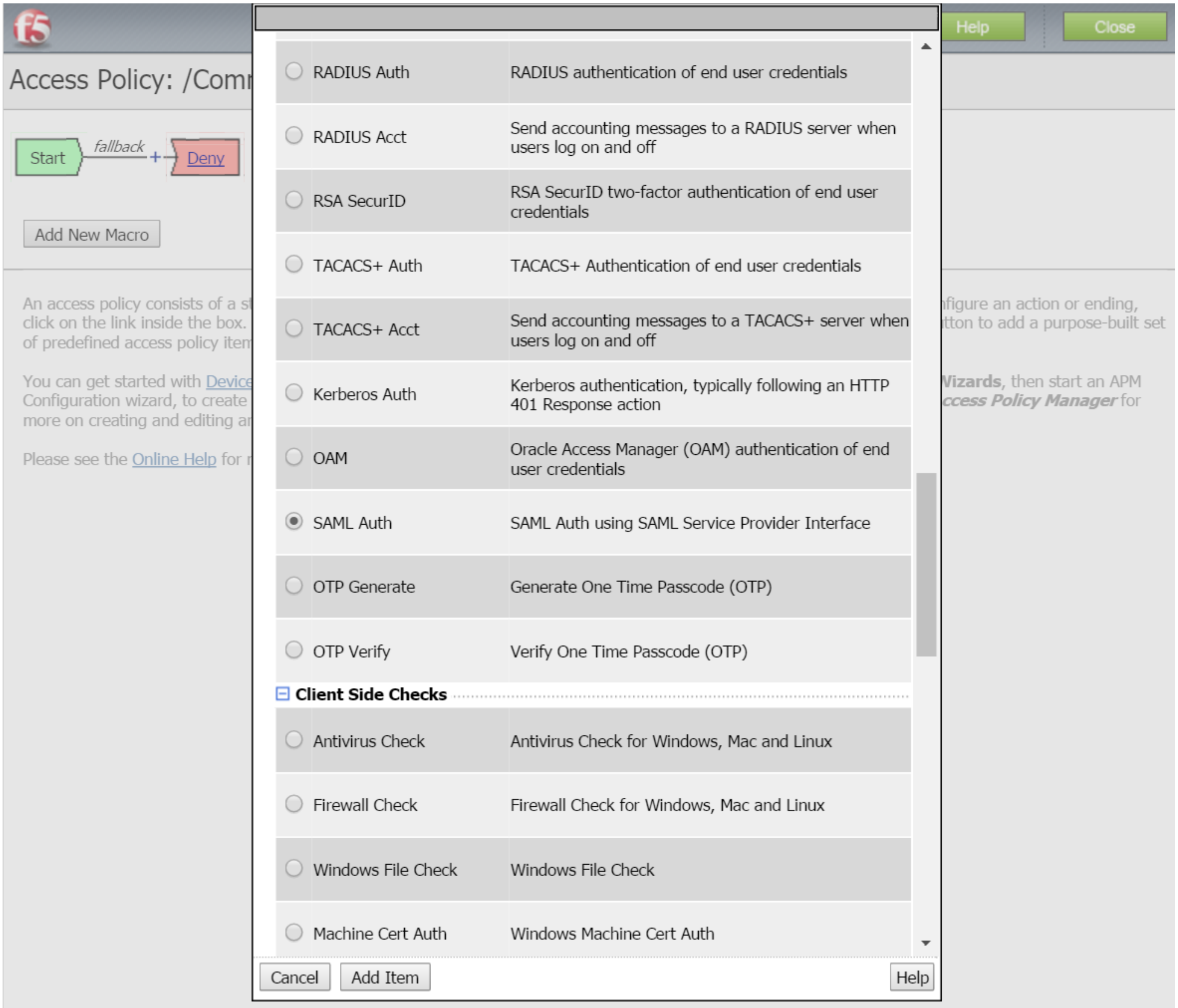
(Endings: Allow, Deny [default])

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the **+** sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the **x** on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with Device Wizards. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the ***Configuration Guide for BIG-IP Access Policy Manager*** for more on creating and editing an access policy.

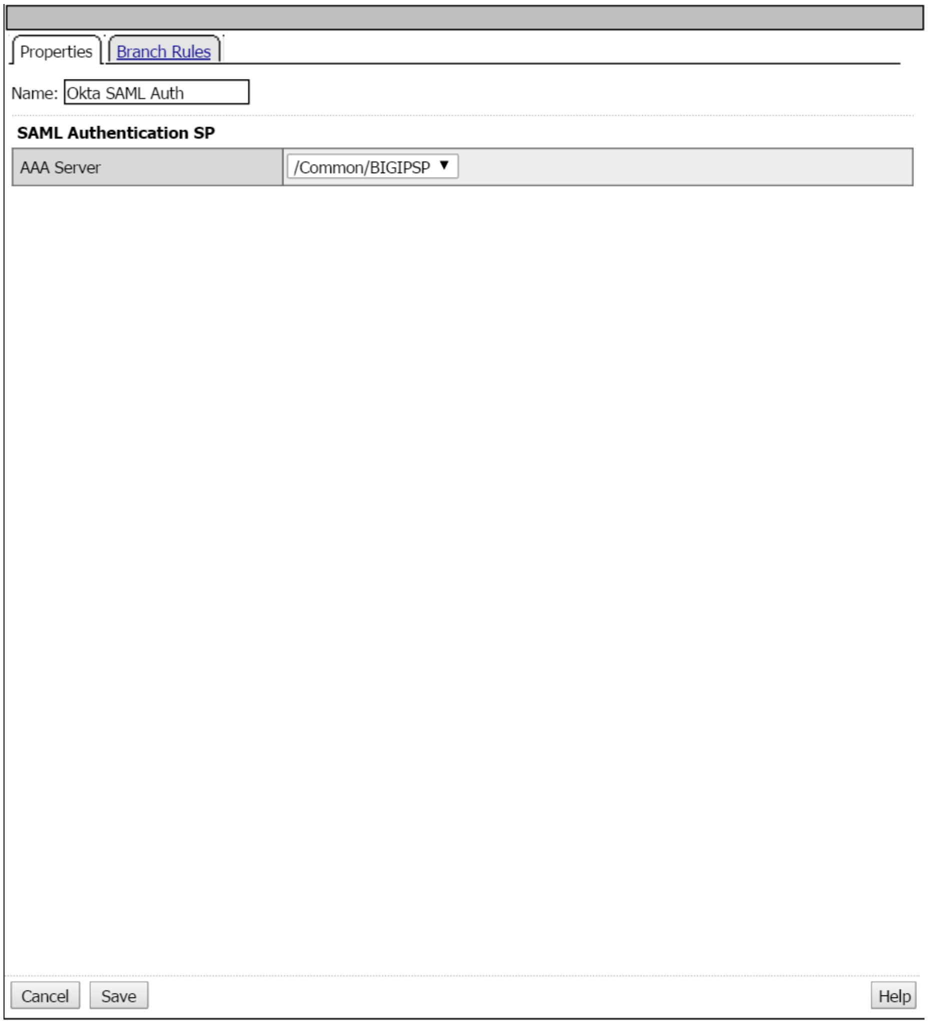
Please see the Online Help for more Visual Policy Editor basics.

5. Click on the '+' icon between Start and Deny nodes and on the pop-up window, choose 'SAML Auth'



○ RADIUS Auth	RADIUS authentication of end user credentials
○ RADIUS Acct	Send accounting messages to a RADIUS server when users log on and off
○ RSA SecurID	RSA SecurID two-factor authentication of end user credentials
○ TACACS+ Auth	TACACS+ Authentication of end user credentials
○ TACACS+ Acct	Send accounting messages to a TACACS+ server when users log on and off
○ Kerberos Auth	Kerberos authentication, typically following an HTTP 401 Response action
○ OAM	Oracle Access Manager (OAM) authentication of end user credentials
● SAML Auth	SAML Auth using SAML Service Provider Interface
○ OTP Generate	Generate One Time Passcode (OTP)
○ OTP Verify	Verify One Time Passcode (OTP)
Client Side Checks	
○ Antivirus Check	Antivirus Check for Windows, Mac and Linux
○ Firewall Check	Firewall Check for Windows, Mac and Linux
○ Windows File Check	Windows File Check
○ Machine Cert Auth	Windows Machine Cert Auth

6. On the next screen, under ‘Properties’, choose a name for the auth method and in AAA Server dropdown, select the previously configured BIG-IP SP. Click ‘Save’

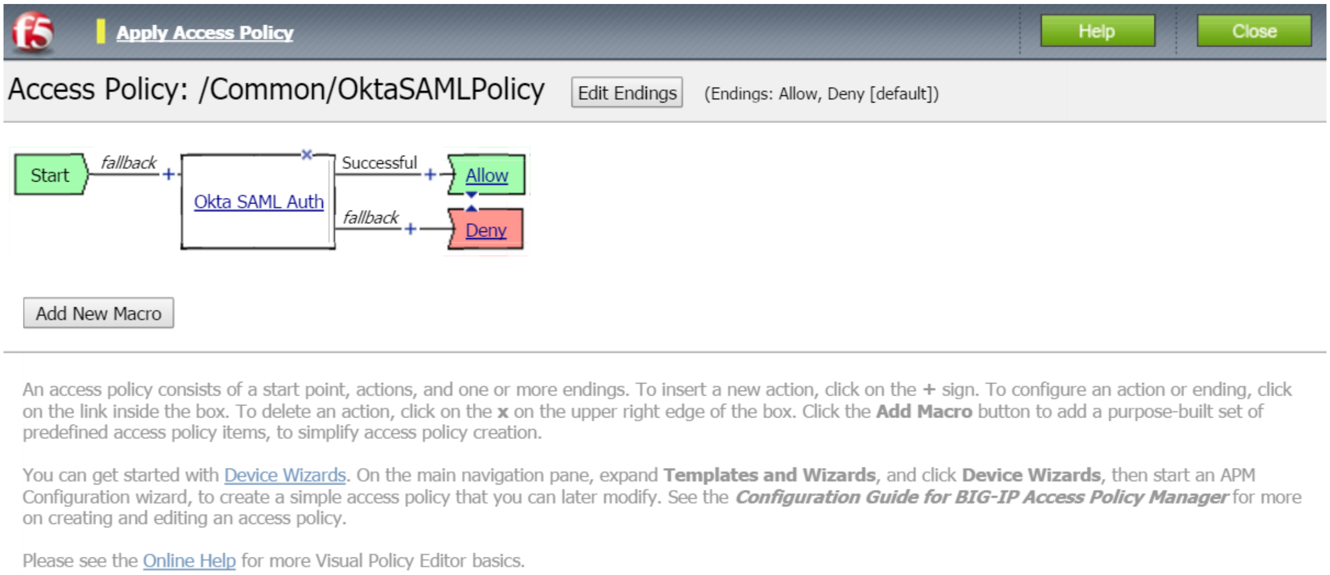


Name: Okta SAML Auth

SAML Authentication SP

AAA Server	/Common/BIGIPSP

7. The access policy looks like the following. Note that F5 BIG-IP APM is a very powerful tool and additional processing including fetching attributes from other AD/LDAP sources for insertion and additional backend authorization can be performed.



Access Policy: /Common/OktaSAMLPolicy

(Endings: Allow, Deny [default])

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the **+** sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the **x** on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with Device Wizards. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the ***Configuration Guide for BIG-IP Access Policy Manager*** for more on creating and editing an access policy.

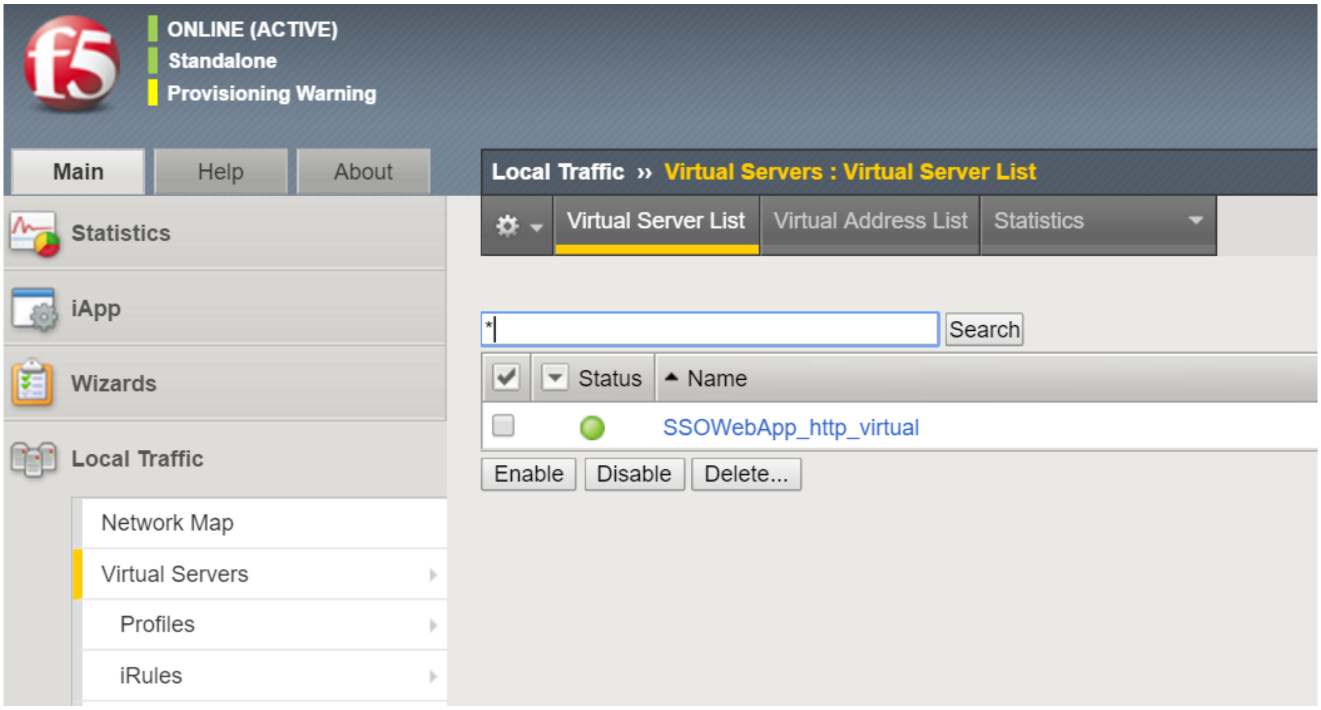
Please see the Online Help for more Visual Policy Editor basics.

8. Click ‘Apply Access Policy’. Then click ‘Close’
9. To put the access policy into effect, you must attach it to the virtual server that was created for the test ASP .NET IIS web app

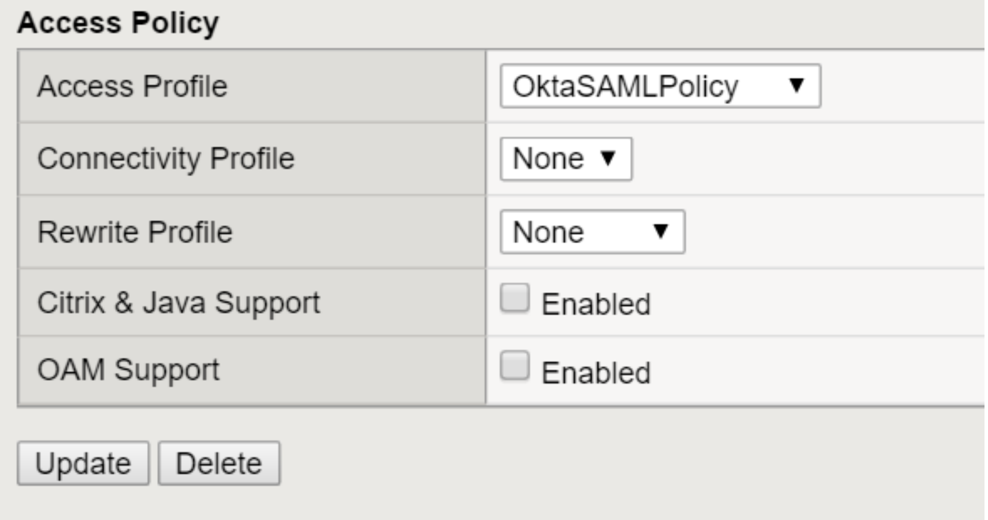
Adding the access profile to the virtual server

Associate the access profile with the virtual server so that F5 BIG-IP APM can apply the profile to incoming traffic and run the previously defined access policy

1. On the Main tab, click Local Traffic > Virtual Servers. The Virtual Server List screen opens



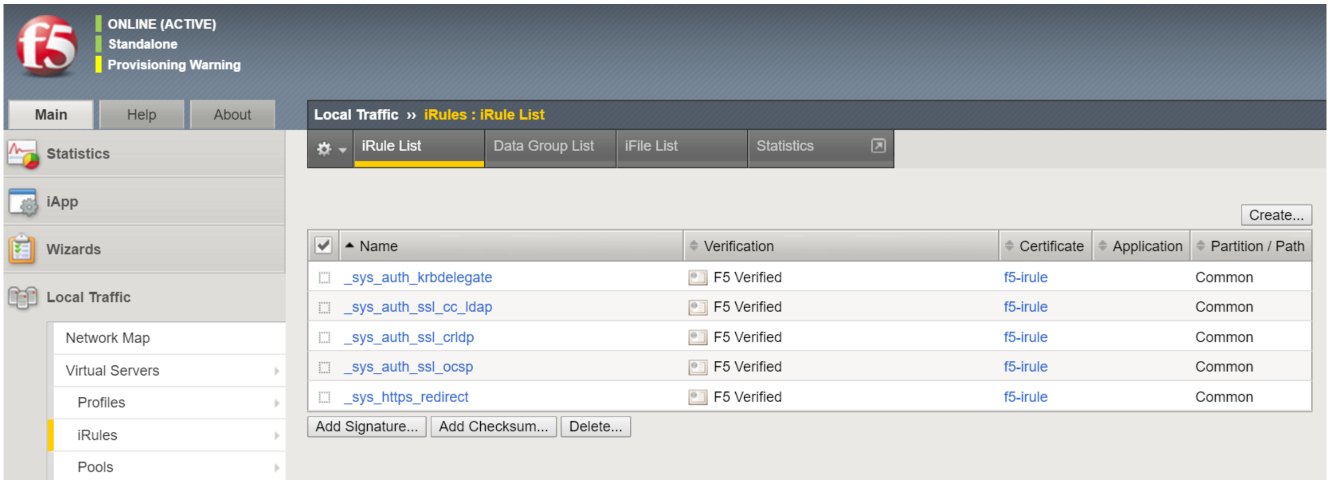
2. Click on the virtual server. Then scroll all the way to the bottom to the ‘Access Policy’ section. Select the previously defined ‘Access Profile’ and click ‘Update’



Access Policy

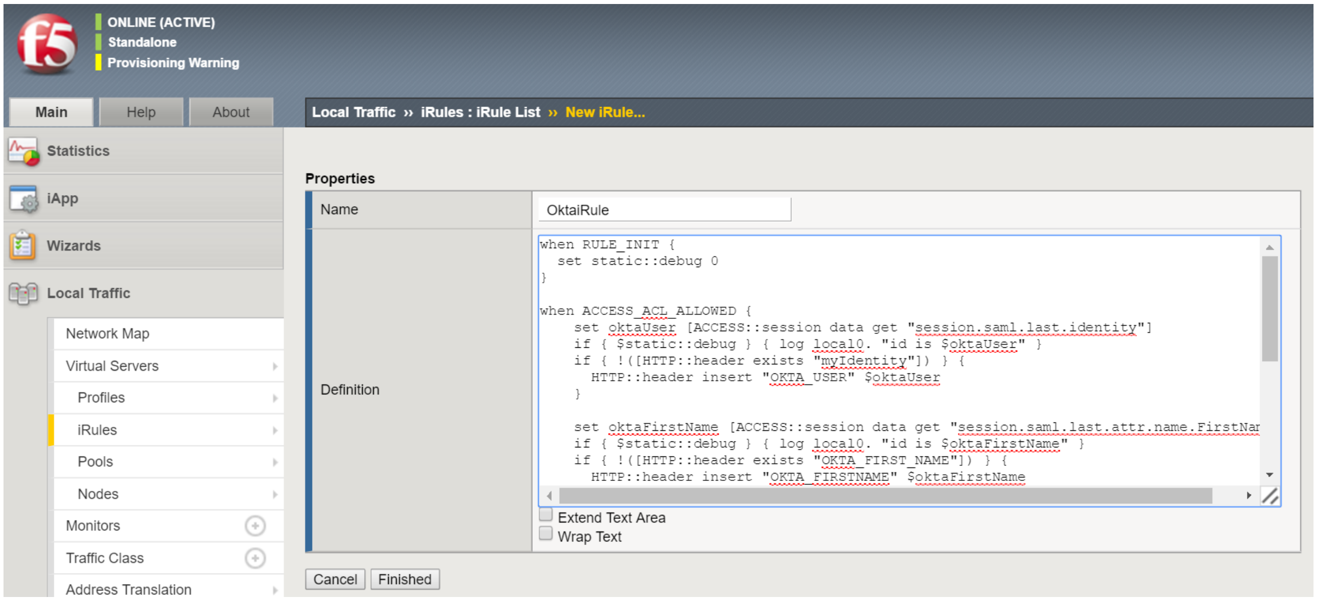
Access Profile	OktaSAMLPolicy ▼
Connectivity Profile	None ▼
Rewrite Profile	None ▼
Citrix & Java Support	□ Enabled
OAM Support	□ Enabled

3. Next create an F5 BIG-IP iRule® to extract the custom SAML attributes from the incoming assertion and pass them as HTTP headers to the backend test ASP .NET IIS application. Click ‘Create’



☑	Name	Verification	Certificate	Application	Partition / Path
□	_sys_auth_krbdelegate	F5 Verified	f5-irule		Common
□	_sys_auth_ssl_cc_ldap	F5 Verified	f5-irule		Common
□	_sys_auth_ssl_crldp	F5 Verified	f5-irule		Common
□	_sys_auth_ssl_ocsp	F5 Verified	f5-irule		Common
□	_sys_https_redirect	F5 Verified	f5-irule		Common

4. Paste the F5 BIG-IP iRule text below into the Definition window



Properties

Name: OktaiRule

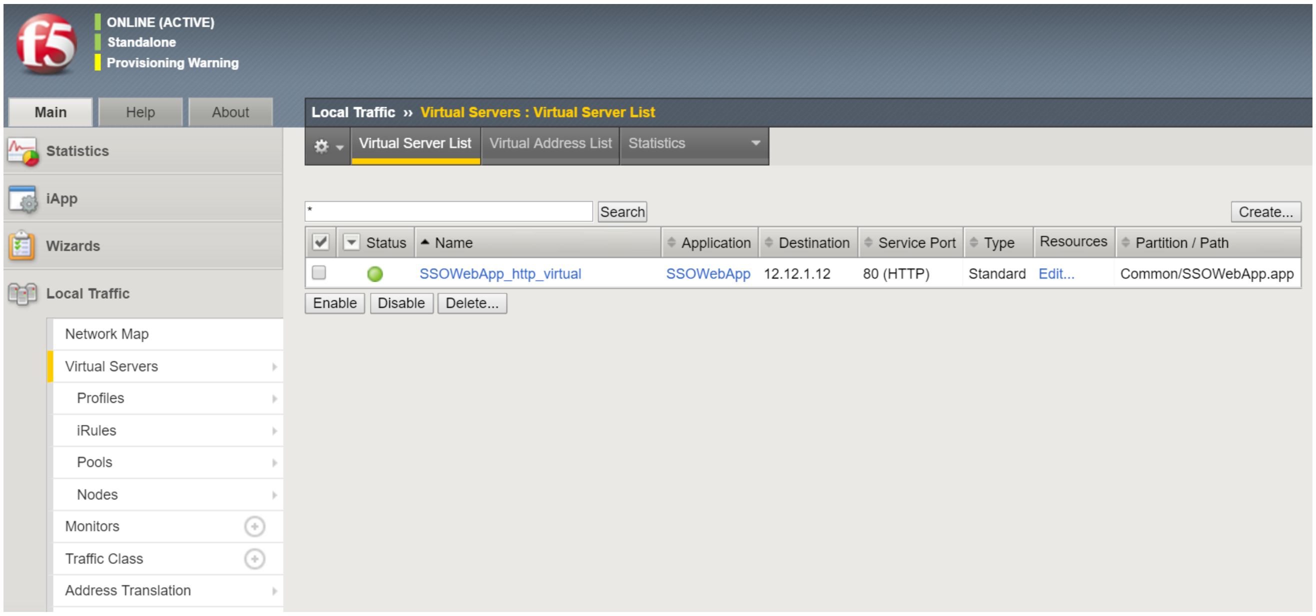
Definition:

```
when RULE_INIT {
  set static::debug 0
}

when ACCESS_ACL_ALLOWED {
    set oktaUser [ACCESS::session data get "session.saml.last.identity"]
    if { $static::debug } { log local0. "id is $oktaUser" }
    if { !([HTTP::header exists "myIdentity"]) } {
      HTTP::header insert "OKTA_USER" $oktaUser
    }

    set oktaFirstName [ACCESS::session data get "session.saml.last.attr.name.FirstNar
    if { $static::debug } { log local0. "id is $oktaFirstName" }
    if { !([HTTP::header exists "OKTA_FIRST_NAME"]) } {
      HTTP::header insert "OKTA_FIRSTNAME" $oktaFirstName
```

□ Extend Text Area
□ Wrap Text

```
when RULE_INIT {
  set static::debug 0
}

when ACCESS_ACL_ALLOWED {
    set oktaUser [ACCESS::session data get "session.saml.last.identity"]
    if { $static::debug } { log local0. "id is $oktaUser" }
    if { !([HTTP::header exists "OKTA_USER"]) } {
      HTTP::header insert "OKTA_USER" $oktaUser
    }

    set oktaFirstName [ACCESS::session data get "session.saml.last.attr.name.FirstName"]
    if { $static::debug } { log local0. "id is $oktaFirstName" }
    if { !([HTTP::header exists "OKTA_FIRSTNAME"]) } {
      HTTP::header insert "OKTA_FIRSTNAME" $oktaFirstName
    }

    set oktaLastName [ACCESS::session data get "session.saml.last.attr.name.LastName"]
    if { $static::debug } { log local0. "id is $oktaLastName" }
    if { !([HTTP::header exists "OKTA_LASTNAME"]) } {
      HTTP::header insert "OKTA_LASTNAME" $oktaLastName
    }

    set oktaCity [ACCESS::session data get "session.saml.last.attr.name.City"]
    if { $static::debug } { log local0. "id is $oktaCity" }
    if { !([HTTP::header exists "OKTA_CITY"]) } {
      HTTP::header insert "OKTA_CITY" $oktaCity
    }
}
```

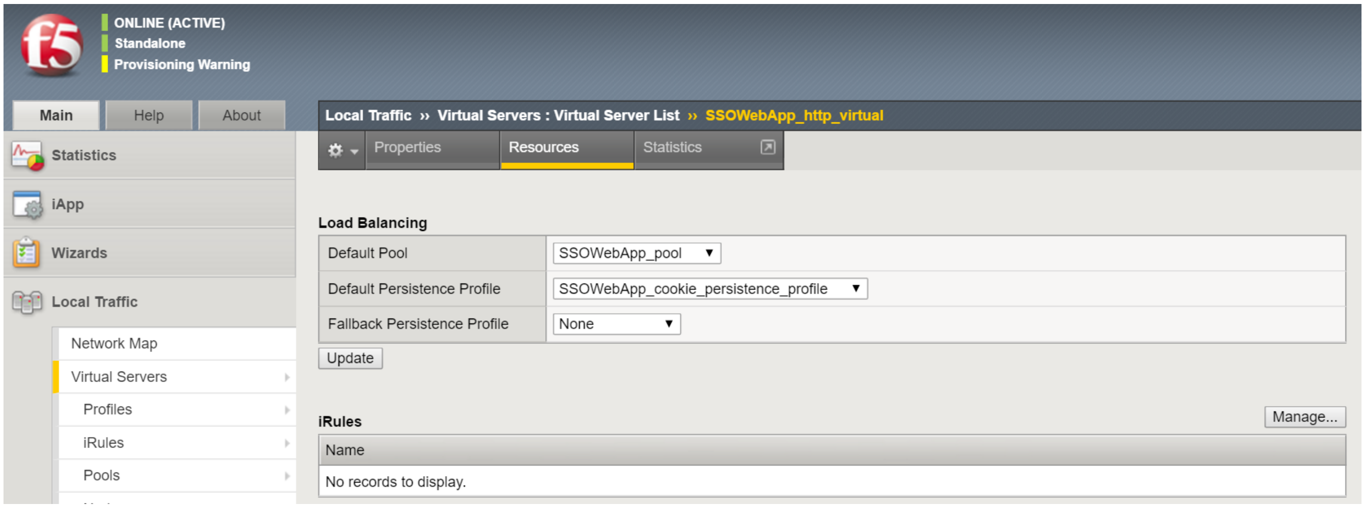
5. Next, apply this F5 BIG-IP iRule to the Virtual Server



Local Traffic » Virtual Servers : Virtual Server List

☑	Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	SSOWebApp_http_virtual	SSOWebApp	12.12.1.12	80 (HTTP)	Standard	Edit...	Common/SSOWebApp.app

6. Click 'Edit' under Resources column



Local Traffic » Virtual Servers : Virtual Server List » SSOWebApp_http_virtual

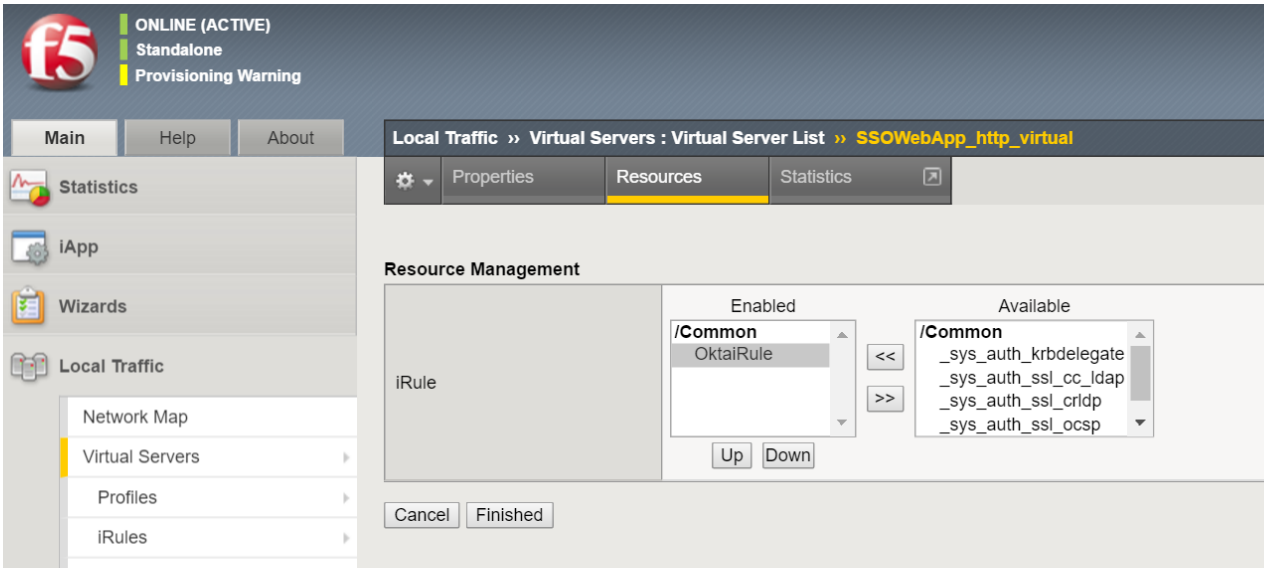
Load Balancing

Default Pool	SSOWebApp_pool
Default Persistence Profile	SSOWebApp_cookie_persistence_profile
Fallback Persistence Profile	None

iRules

Name
No records to display.

7. Click 'Manage' under iRules
8. Add OktaiRule that previously created to the Enabled list and click Finished



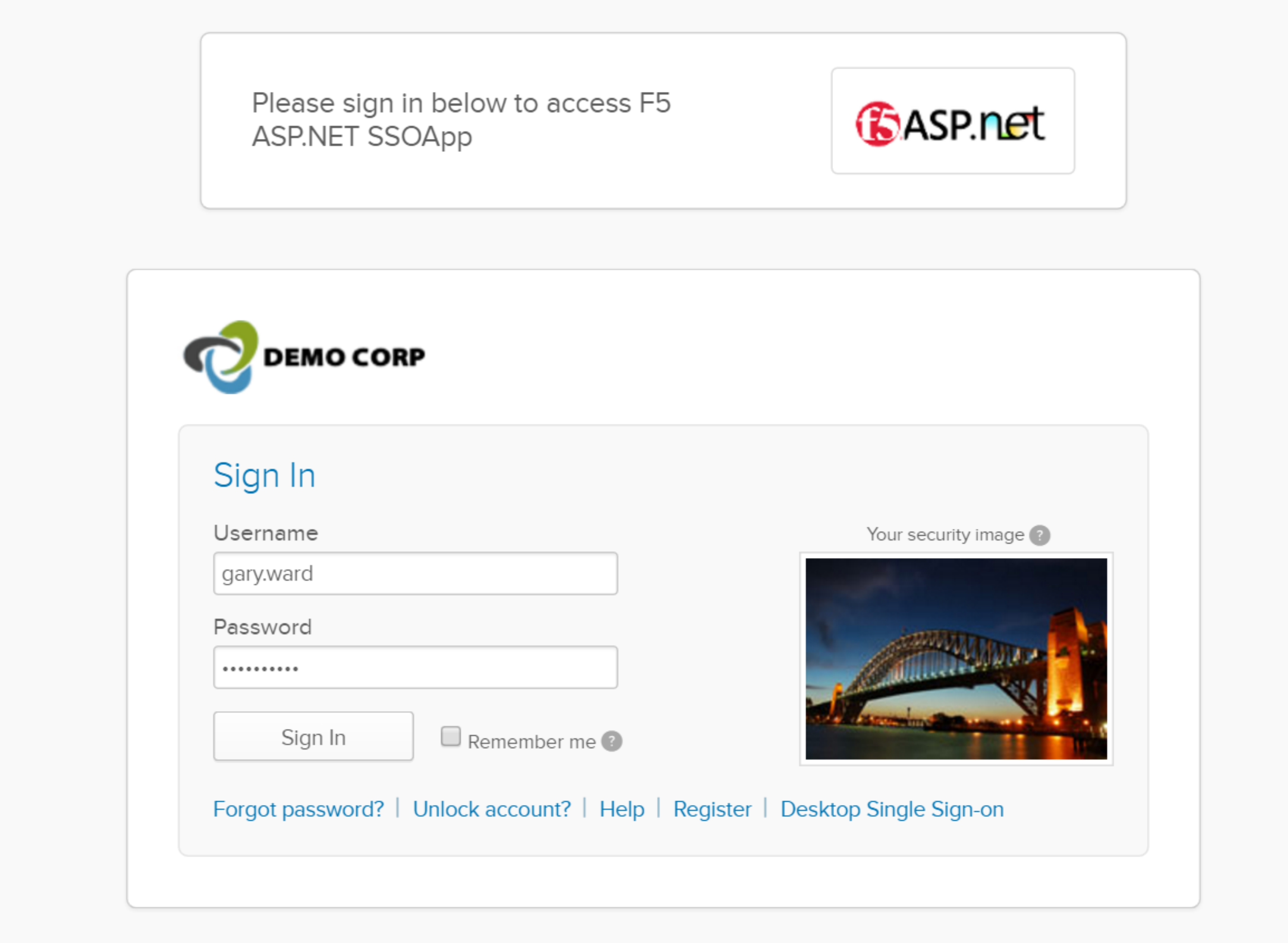
Resource Management

	Enabled	Available
iRule	/Common OktaiRule	/Common _sys_auth_krbdelegate _sys_auth_ssl_cc_ldap _sys_auth_ssl_crldp _sys_auth_ssl_ocsp

Testing the F5 BIG-IP + Okta Integration

Follow the steps below to test the integration

1. Go to the published application URL http://www.democorp.co/headers.aspx
2. F5 BIG-IP should redirect the request to Okta for authentication. Enter credentials



Please sign in below to access F5 ASP.NET SSOApp

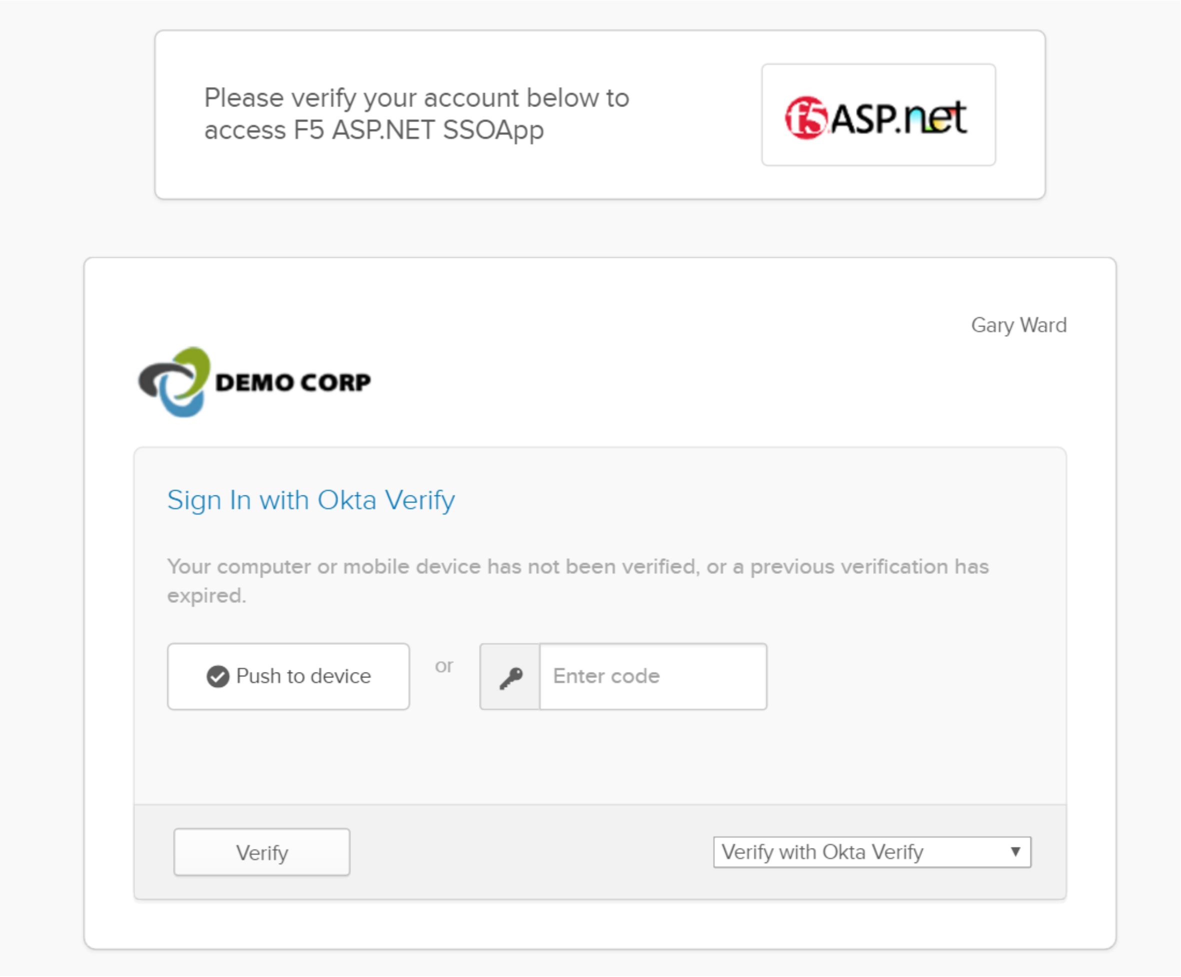
Username: gary.ward

Password: ••••••••••

□ Remember me

ASP.net
DEMO CORP
Sign In
Your security image
Sign In
Forgot password? | Unlock account? | Help | Register | Desktop Single Sign-on

3. Complete the MFA challenge



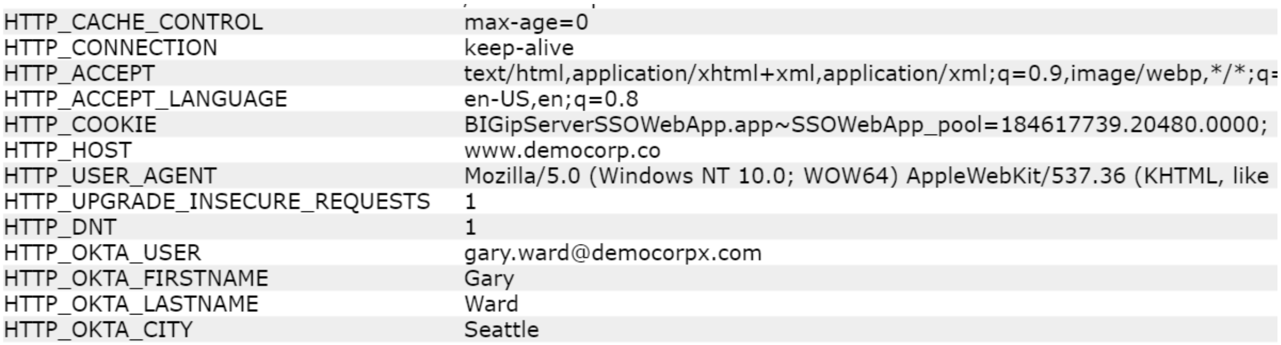
Please verify your account below to access F5 ASP.NET SSOApp

Gary Ward

Sign In with Okta Verify

Your computer or mobile device has not been verified, or a previous verification has expired.

4. Should be redirected to the published application web page



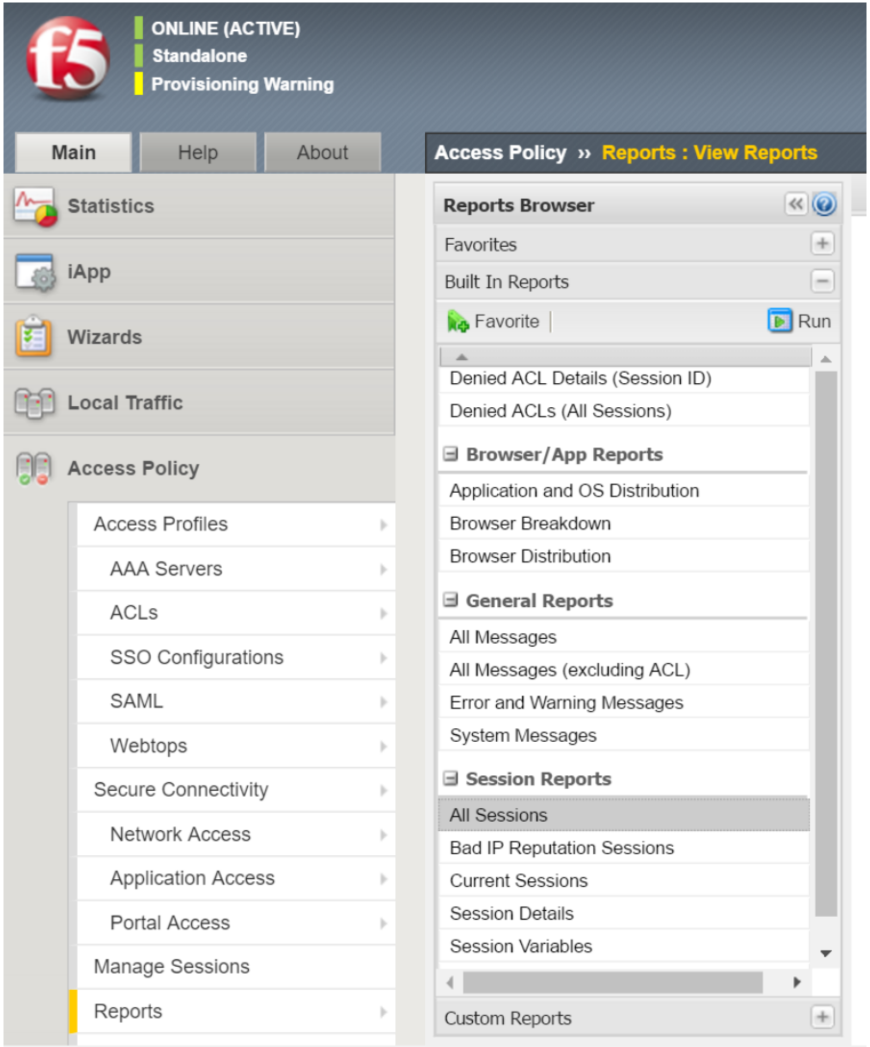
HTTP_CACHE_CONTROL	max-age=0
HTTP_CONNECTION	keep-alive
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.8
HTTP_COOKIE	BIGipServerSSOWebApp.app~SSOWebApp_pool=184617739.20480.0000;
HTTP_HOST	www.democorp.co
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_DNT	1
HTTP_OKTA_USER	gary.ward@democorpx.com
HTTP_OKTA_FIRSTNAME	Gary
HTTP_OKTA_LASTNAME	Ward
HTTP_OKTA_CITY	Seattle

5. Note the HTTP_OKTA_* headers indicating successful extraction of SAML headers

Appendix

Reports and Logs

F5 BIG-IP APM Reports -> All Sessions report and Okta System Log can provide traces of transactions that can aid in troubleshooting



For more on Okta System Log – please refer to Okta documentation here – (https://support.okta.com/help/articles/Knowledge_Article/27605453-Using-the-Okta-Reports-Page)

Additional References

Okta Company website – https://www.okta.com

Okta Customer Support – https://support.okta.com

Okta Documentation - https://support.okta.com/help/documentation

F5 BIG-IP APM Documentation - https://support.f5.com/kb/en-us/products/big-ip_apm.html

F5 BIG-IP LTM Documentation - https://support.f5.com/kb/en-us/products/big-ip_ltm.html

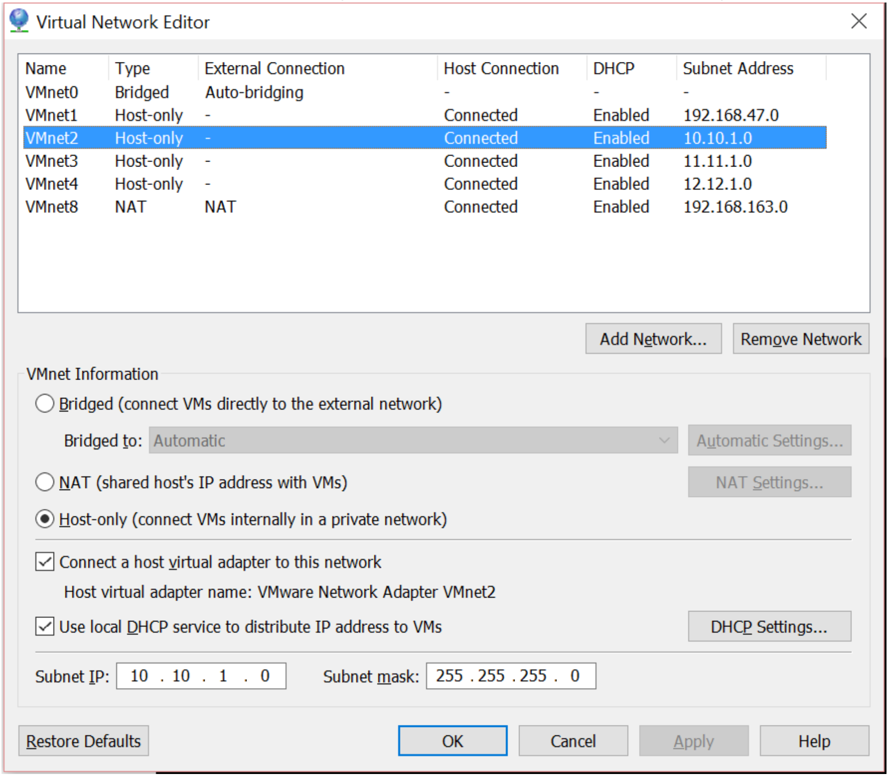
Sample F5 BIG-IP Virtual Lab Setup with VMWare

The following outlines the steps to create a basic setup of an F5 BIG-IP environment using VMWare.

NOTE: This should only be used as a sample guidance. To set up a production environment, please refer to the F5 BIG-IP documentation listed above.

1. F5 BIG-IP should be setup with three network interfaces:
   i. Management (10.10.1.1)
   ii. Internal (11.11.1.1)
   iii. External (12.12.1.1)

   It is recommended that VMWare is setup with three custom host-only networks as shown below:



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.47.0
VMnet2	Host-only	-	Connected	Enabled	10.10.1.0
VMnet3	Host-only	-	Connected	Enabled	11.11.1.0
VMnet4	Host-only	-	Connected	Enabled	12.12.1.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.163.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

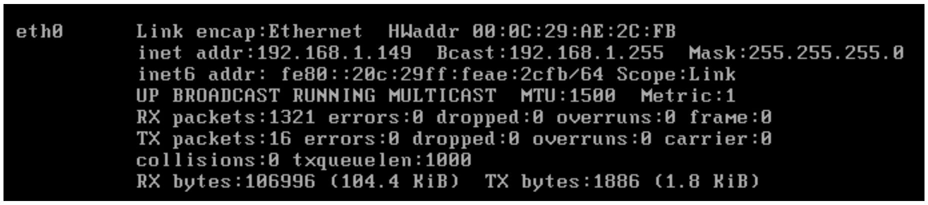
Host virtual adapter name: VMware Network Adapter VMnet2

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 10 . 10 . 1 . 0 Subnet mask: 255 . 255 . 255 . 0

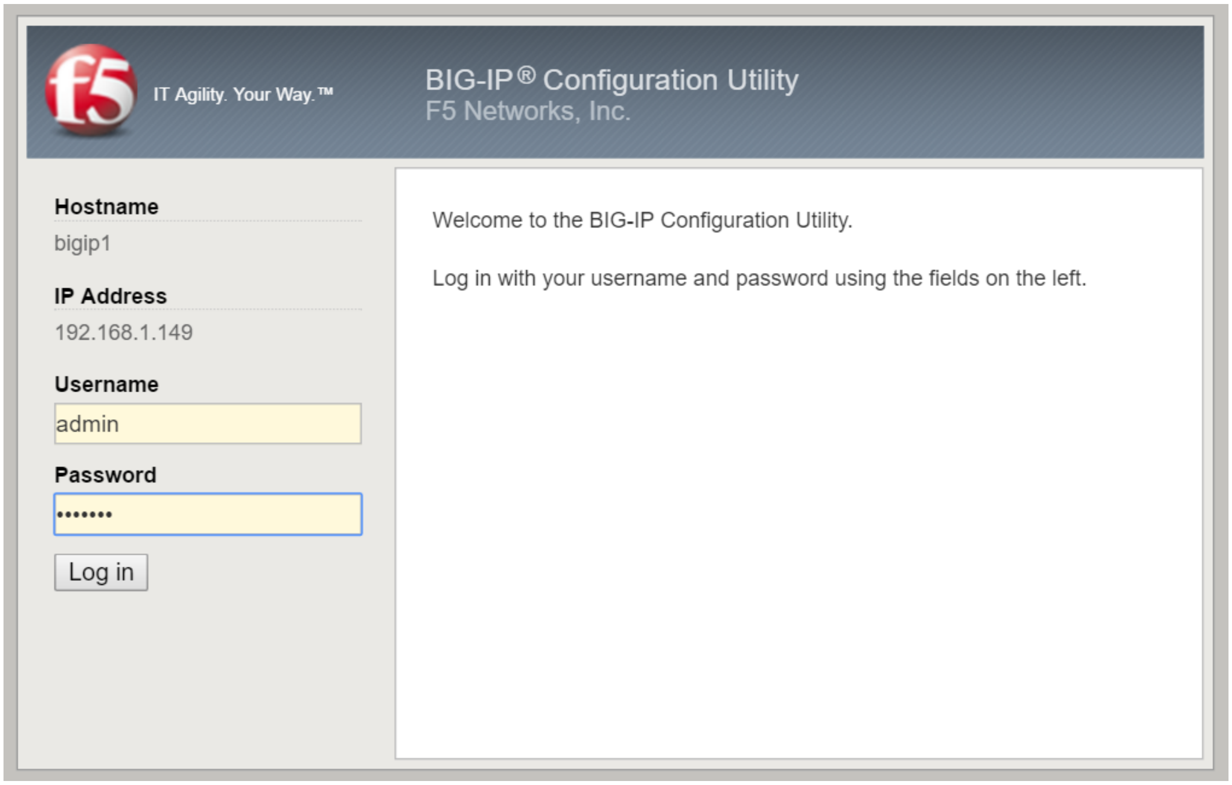
2. There should be an IIS or Apache webserver to test backend application with the suggested IP-address: 11.11.1.11
3. Open the downloaded image file in VMWare Workstation and deploy it using default options, then start the F5 BIG-IP VM

4. Switch to VM console and on login prompt, enter **`root`** as username and **`default`** as password
5. Enter **`ifconfig -a | more`** to find the DHCP assigned IP-address to this VM. For example, inet addr: 192.168.1.149 is the IP-address below:



```
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AE:2C:FB
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feae:2cfb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1321 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:106996 (104.4 KiB)  TX bytes:1886 (1.8 KiB)
```

6. Launch a browser on the host machine and enter the https://IP-address obtained in the previous step, For example: **`https://192.168.1.149`**
7. A certificate warning will be issued by the browser. This is normal, click proceed to the login page:



Hostname
bigip1

IP Address
192.168.1.149

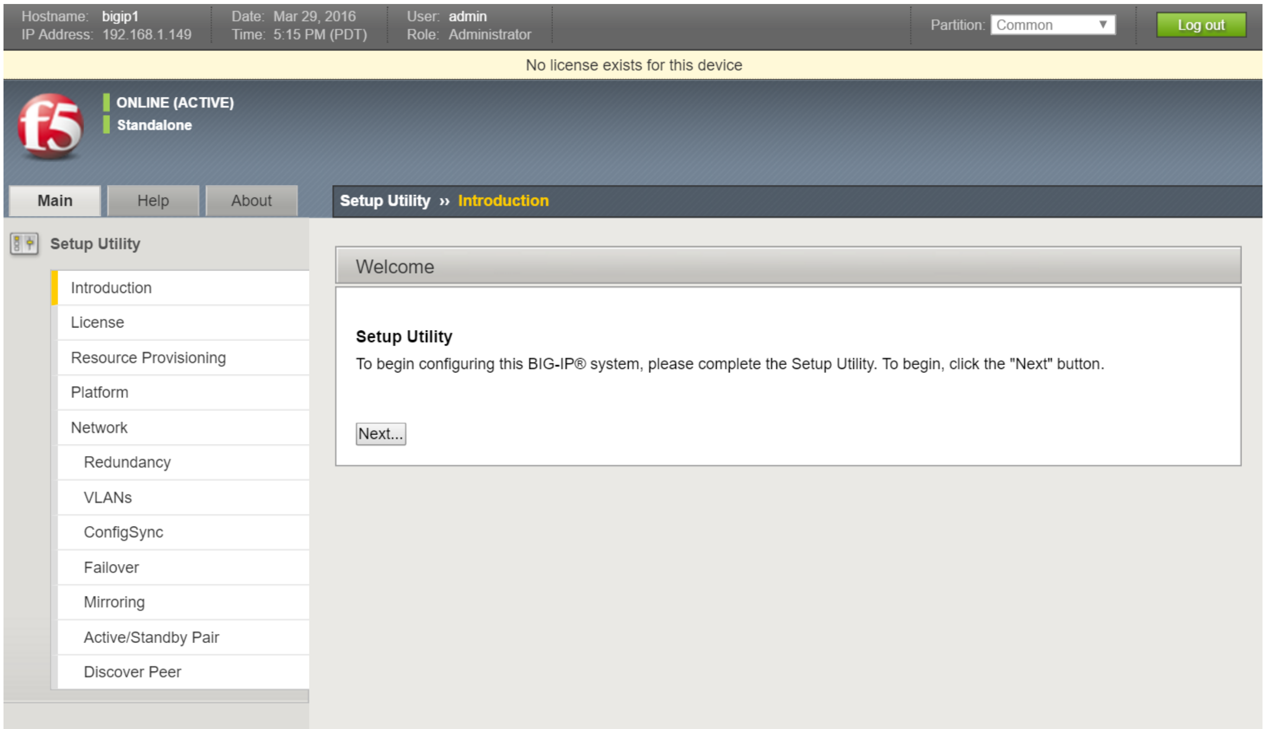
Username
admin

Password
•••••••

Welcome to the BIG-IP Configuration Utility.

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

8. Enter **`admin`** as username and **`admin`** as password and click 'Log in'
9. Click 'Next' in the Setup Utility section:



Hostname: bigip1
IP Address: 192.168.1.149
Date: Mar 29, 2016
Time: 5:15 PM (PDT)
User: admin
Role: Administrator
Partition: Common

No license exists for this device

ONLINE (ACTIVE)
Standalone

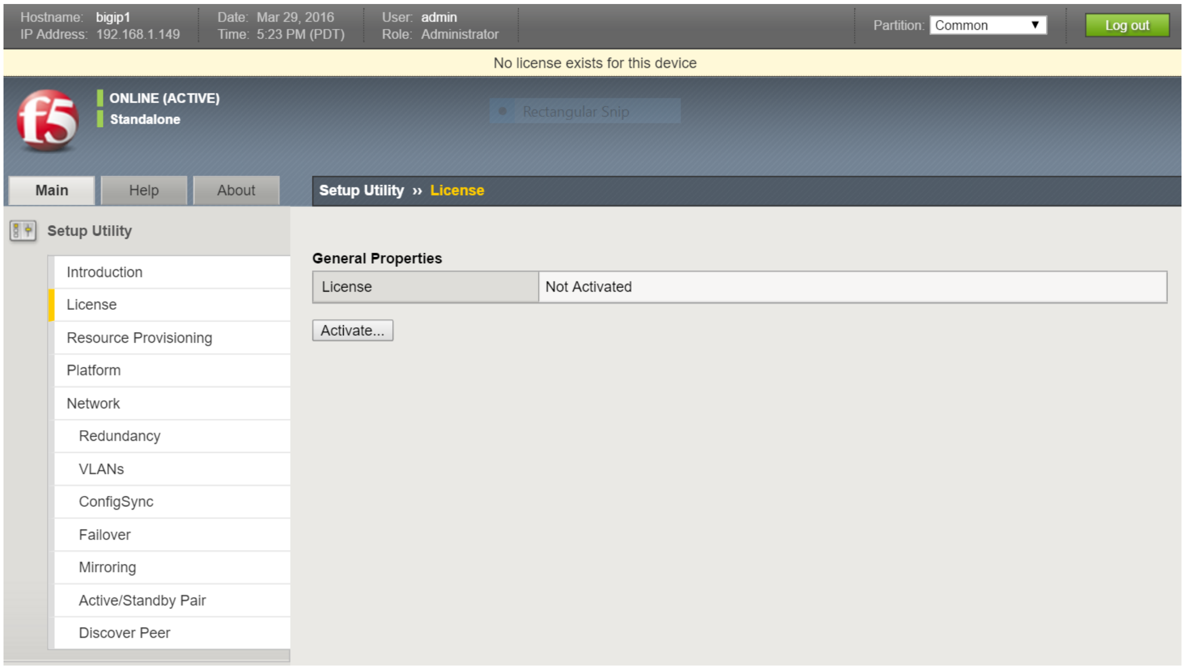
Setup Utility » Introduction

Welcome

Setup Utility

To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.

10. Click ‘Activate’ under License



Hostname: bigip1
IP Address: 192.168.1.149
Date: Mar 29, 2016
Time: 5:23 PM (PDT)
User: admin
Role: Administrator
Partition: Common

No license exists for this device

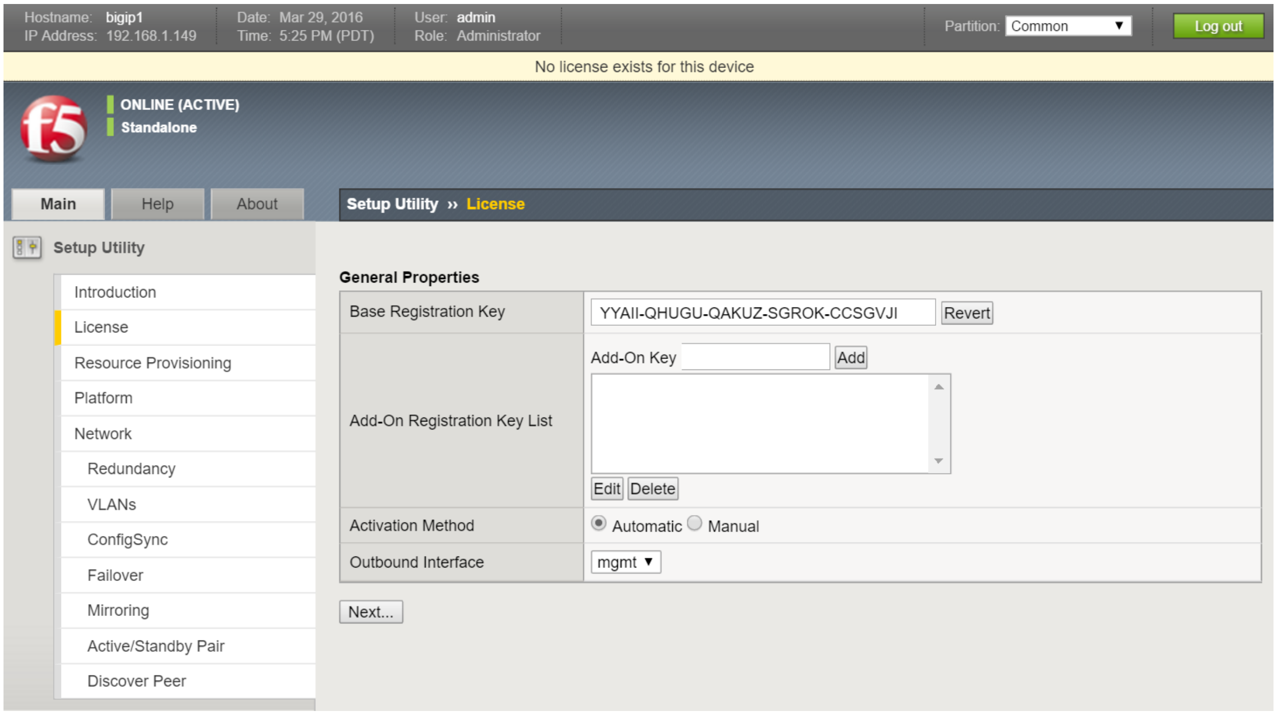
ONLINE (ACTIVE)
Standalone

Setup Utility » License

General Properties

License	Not Activated

11. Enter Registration Key received via email and click ‘Next’



Hostname: bigip1 IP Address: 192.168.1.149 | Date: Mar 29, 2016 Time: 5:25 PM (PDT) | User: admin Role: Administrator | Partition: Common | Log out

No license exists for this device

ONLINE (ACTIVE)
Standalone

Main | Help | About

Setup Utility » License

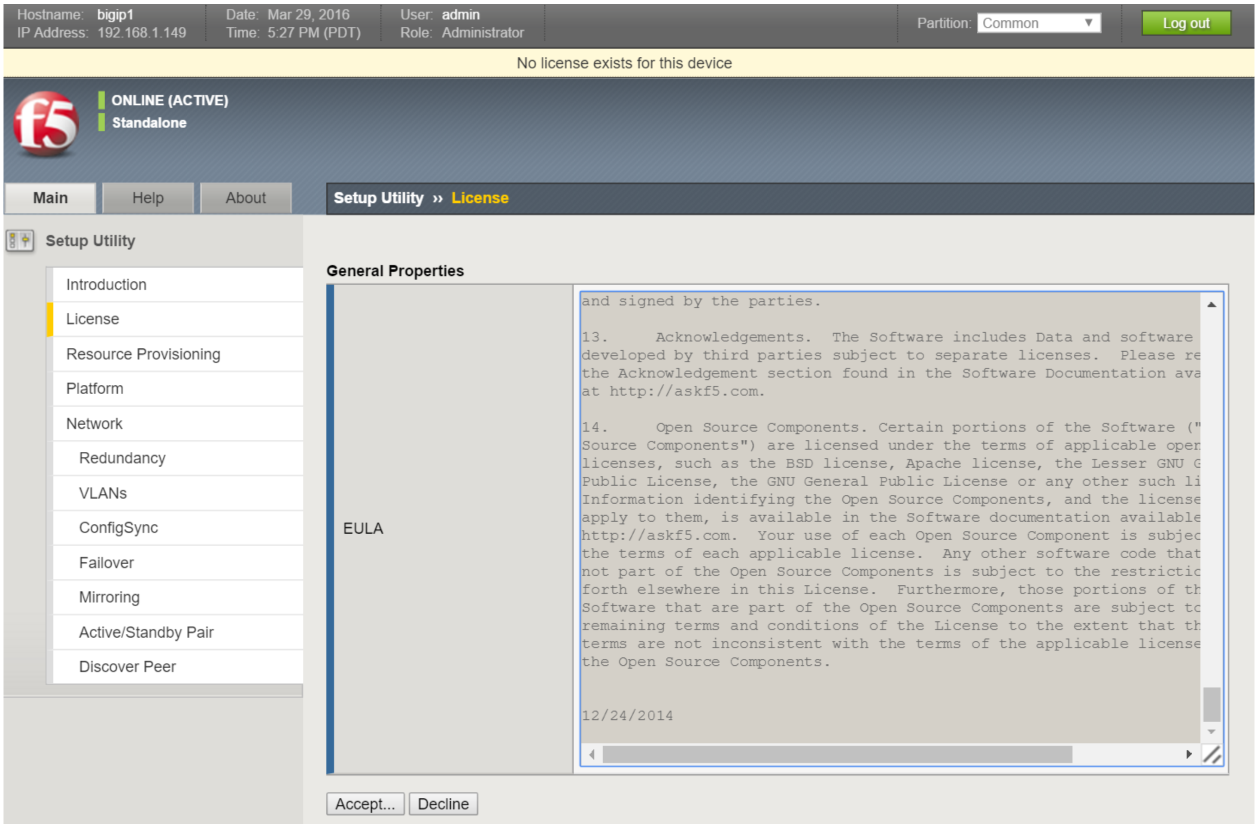
Setup Utility
- Introduction
- License
- Resource Provisioning
- Platform
- Network
  - Redundancy
  - VLANs
  - ConfigSync
  - Failover
  - Mirroring
  - Active/Standby Pair
  - Discover Peer

General Properties

Base Registration Key	YYAII-QHUGU-QAKUZ-SGROK-CCSGVJI Revert
Add-On Registration Key List	Add-On Key Add Edit Delete
Activation Method	● Automatic ○ Manual
Outbound Interface	mgmt ▾

Next...

12. Click ‘Accept’ after reviewing the license agreement



Hostname: bigip1 IP Address: 192.168.1.149 | Date: Mar 29, 2016 Time: 5:27 PM (PDT) | User: admin Role: Administrator | Partition: Common | Log out

No license exists for this device

ONLINE (ACTIVE)
Standalone

Main | Help | About

Setup Utility » License

Setup Utility
- Introduction
- License
- Resource Provisioning
- Platform
- Network
  - Redundancy
  - VLANs
  - ConfigSync
  - Failover
  - Mirroring
  - Active/Standby Pair
  - Discover Peer

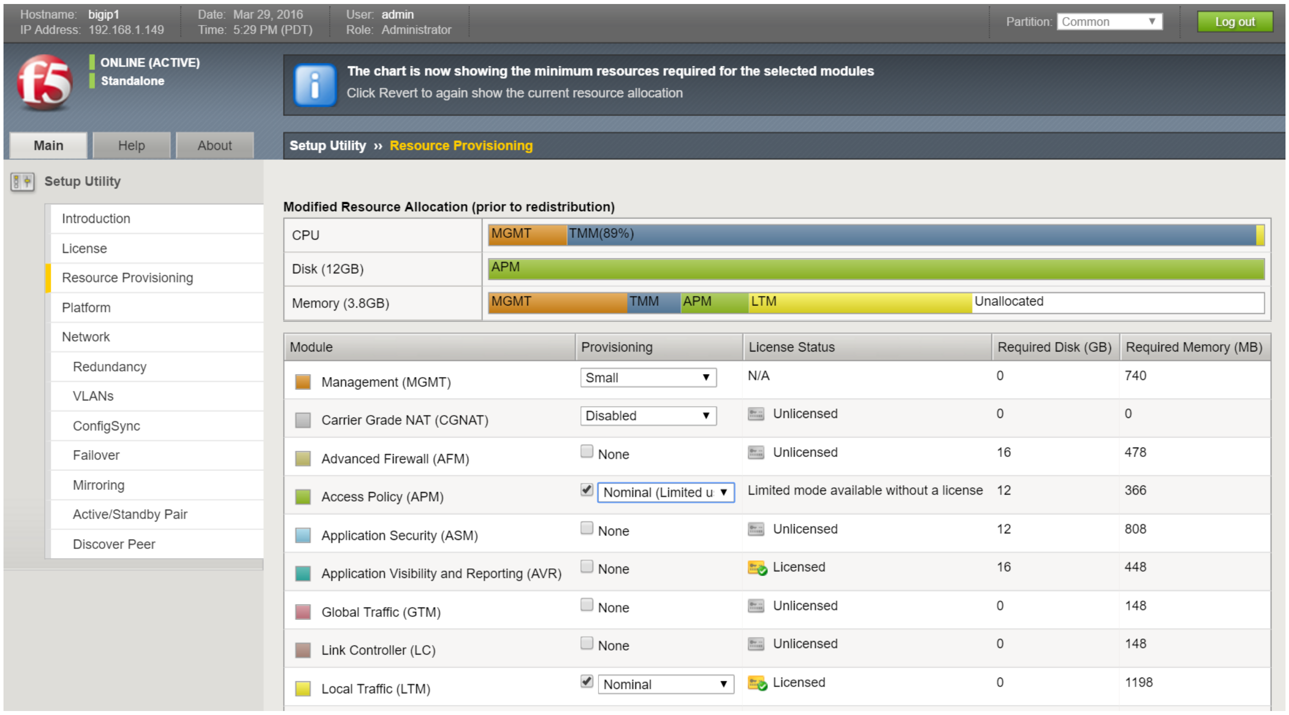
General Properties

EULA

```
and signed by the parties.

13.     Acknowledgements.  The Software includes Data and software
developed by third parties subject to separate licenses.  Please re
the Acknowledgement section found in the Software Documentation ava
at http://askf5.com.

14.     Open Source Components. Certain portions of the Software ("
Source Components") are licensed under the terms of applicable open
licenses, such as the BSD license, Apache license, the Lesser GNU G
Public License, the GNU General Public License or any other such li
Information identifying the Open Source Components, and the license
apply to them, is available in the Software documentation available
http://askf5.com.  Your use of each Open Source Component is subjec
the terms of each applicable license.  Any other software code that
not part of the Open Source Components is subject to the restrictic
forth elsewhere in this License.  Furthermore, those portions of th
Software that are part of the Open Source Components are subject tc
remaining terms and conditions of the License to the extent that th
terms are not inconsistent with the terms of the applicable license
the Open Source Components.


12/24/2014
```

Accept... Decline

13. After license activation, in the Resource Provisioning screen, select Access Policy (APM) and make sure Local Traffic (LTM) is also selected. Then click ‘Next’



Hostname: bigip1 IP Address: 192.168.1.149 | Date: Mar 29, 2016 Time: 5:29 PM (PDT) | User: admin Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)
Standalone

The chart is now showing the minimum resources required for the selected modules
Click Revert to again show the current resource allocation

Main | Help | About

Setup Utility » Resource Provisioning

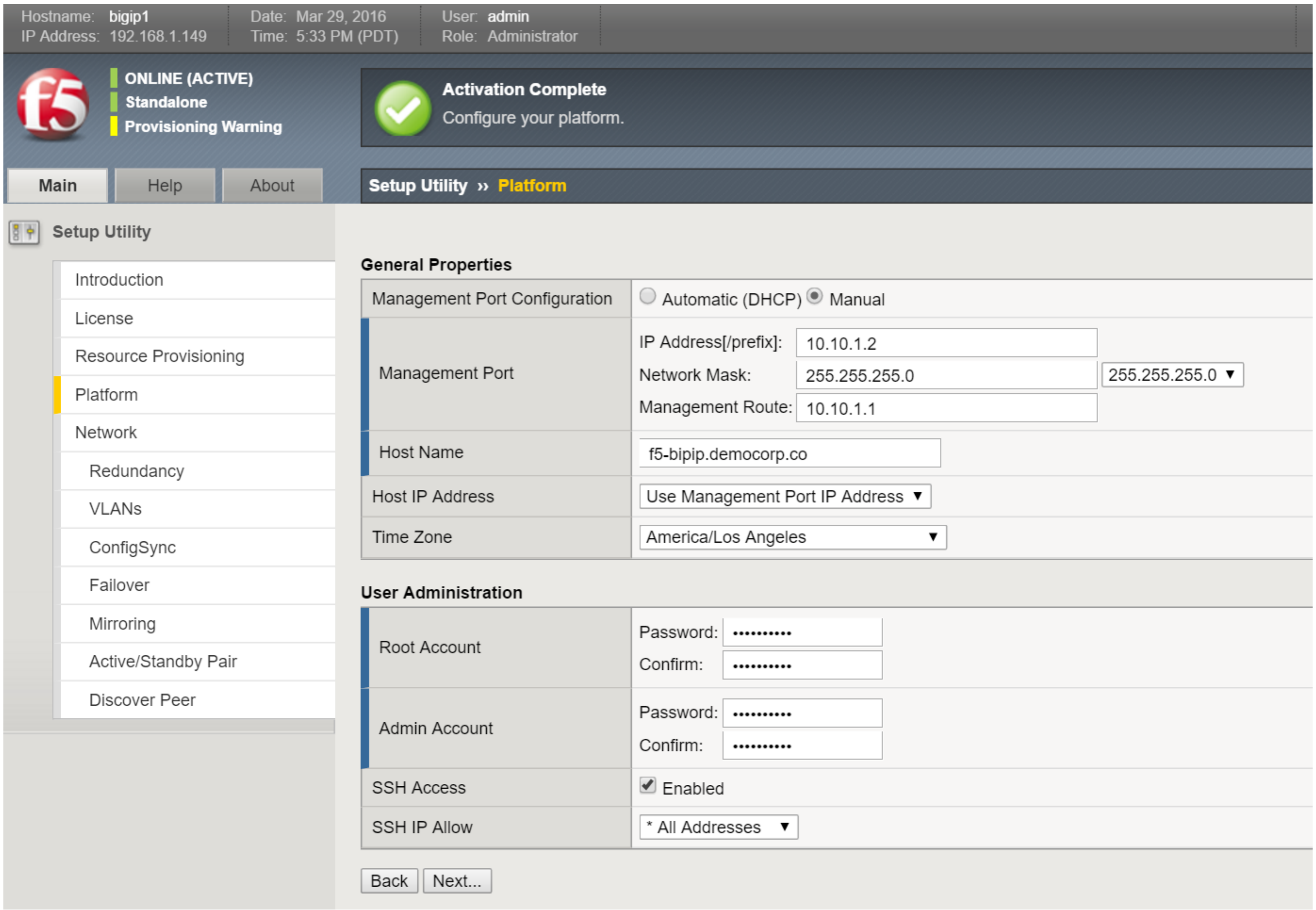
Setup Utility
- Introduction
- License
- Resource Provisioning
- Platform
- Network
  - Redundancy
  - VLANs
  - ConfigSync
  - Failover
  - Mirroring
  - Active/Standby Pair
  - Discover Peer

Modified Resource Allocation (prior to redistribution)

CPU	MGMT · TMM(89%)
Disk (12GB)	APM
Memory (3.8GB)	MGMT · TMM · APM · LTM · Unallocated

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small ▼	N/A	0	740
Carrier Grade NAT (CGNAT)	Disabled ▼	Unlicensed	0	0
Advanced Firewall (AFM)	☐ None	Unlicensed	16	478
Access Policy (APM)	☑ Nominal (Limited u ▼	Limited mode available without a license	12	366
Application Security (ASM)	☐ None	Unlicensed	12	808
Application Visibility and Reporting (AVR)	☐ None	Licensed	16	448
Global Traffic (GTM)	☐ None	Unlicensed	0	148
Link Controller (LC)	☐ None	Unlicensed	0	148
Local Traffic (LTM)	☑ Nominal ▼	Licensed	0	1198

14. In the Platform screen, enter the static IP address for Management Port and a Host Name for the F5 BIG-IP. Also choose passwords for Root and Admin accounts.



Hostname: bigip1 IP Address: 192.168.1.149 | Date: Mar 29, 2016 Time: 5:33 PM (PDT) | User: admin Role: Administrator

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Activation Complete
Configure your platform.

Main | Help | About

Setup Utility » Platform

Setup Utility
- Introduction
- License
- Resource Provisioning
- Platform
- Network
  - Redundancy
  - VLANs
  - ConfigSync
  - Failover
  - Mirroring
  - Active/Standby Pair
  - Discover Peer

General Properties

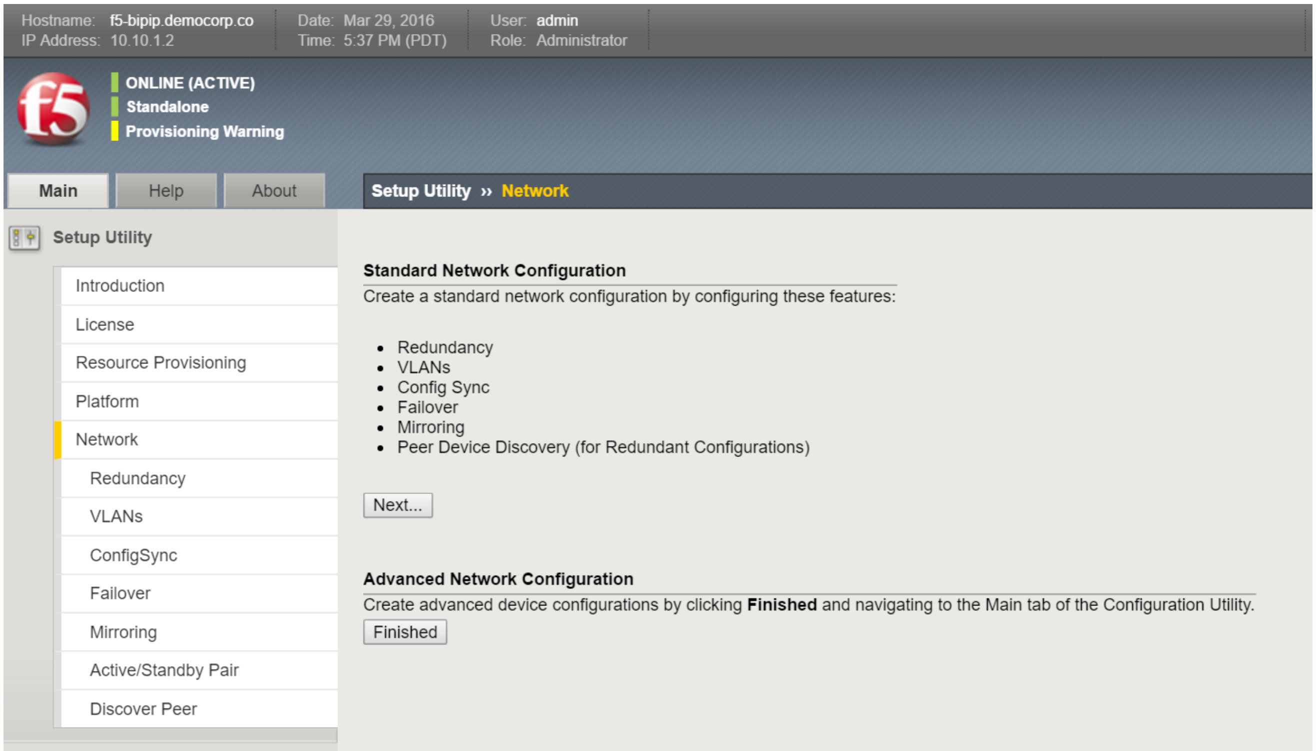
Management Port Configuration	○ Automatic (DHCP) ● Manual
Management Port	IP Address[/prefix]: 10.10.1.2 Network Mask: 255.255.255.0 (255.255.255.0 ▼) Management Route: 10.10.1.1
Host Name	f5-bipip.democorp.co
Host IP Address	Use Management Port IP Address ▼
Time Zone	America/Los Angeles ▼

User Administration

Root Account	Password: •••••••••• Confirm: ••••••••••
Admin Account	Password: •••••••••• Confirm: ••••••••••
SSH Access	☑ Enabled
SSH IP Allow	* All Addresses ▼

Back | Next...

15. The system should redirect to the new Management address and port. Log in with the new Admin password. Click ‘Next’ to configure the Network.



Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 5:37 PM (PDT)
User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Setup Utility » Network

Standard Network Configuration

Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

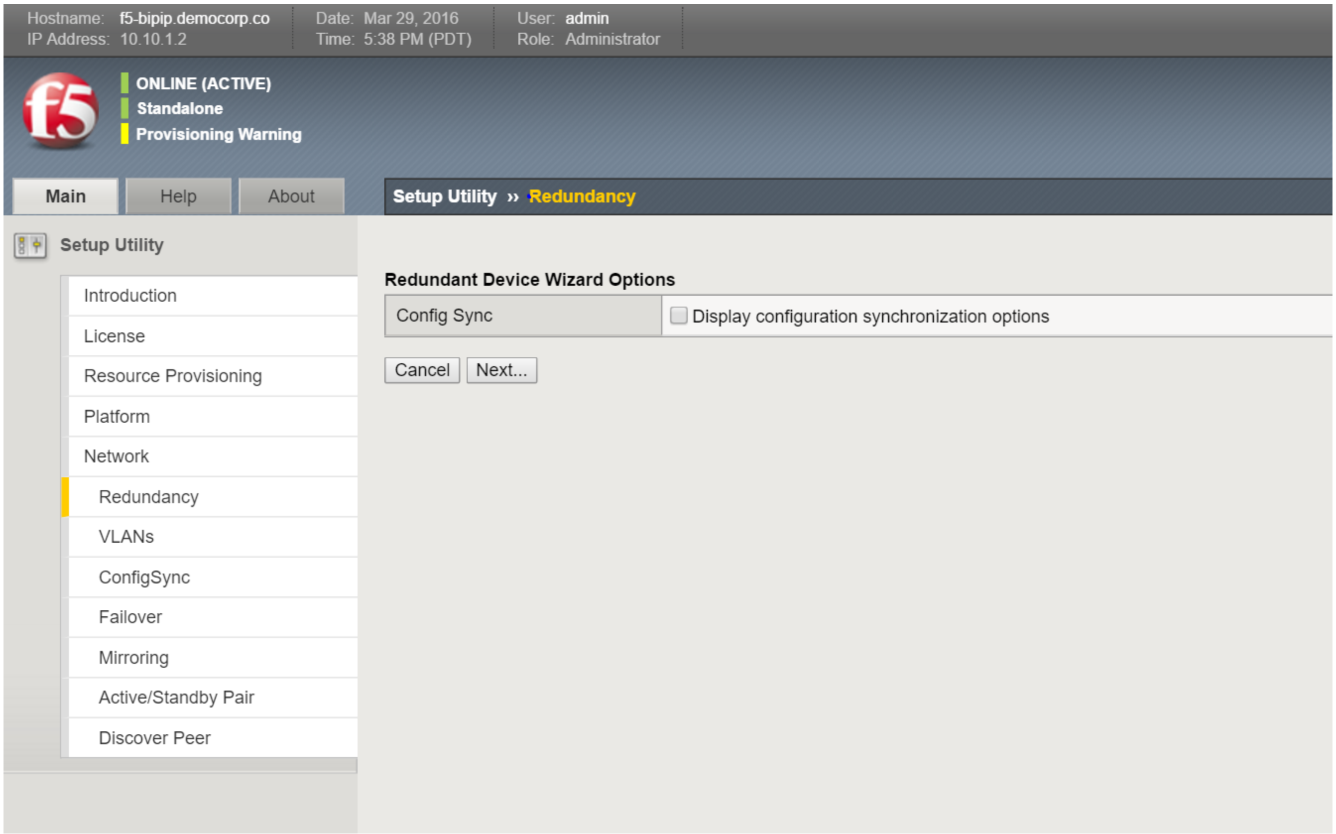
Next...

Advanced Network Configuration

Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

Finished

16. Unselect Config Sync options and click ‘Next’ as they are not needed for this lab



Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 5:38 PM (PDT)
User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone
Provisioning Warning

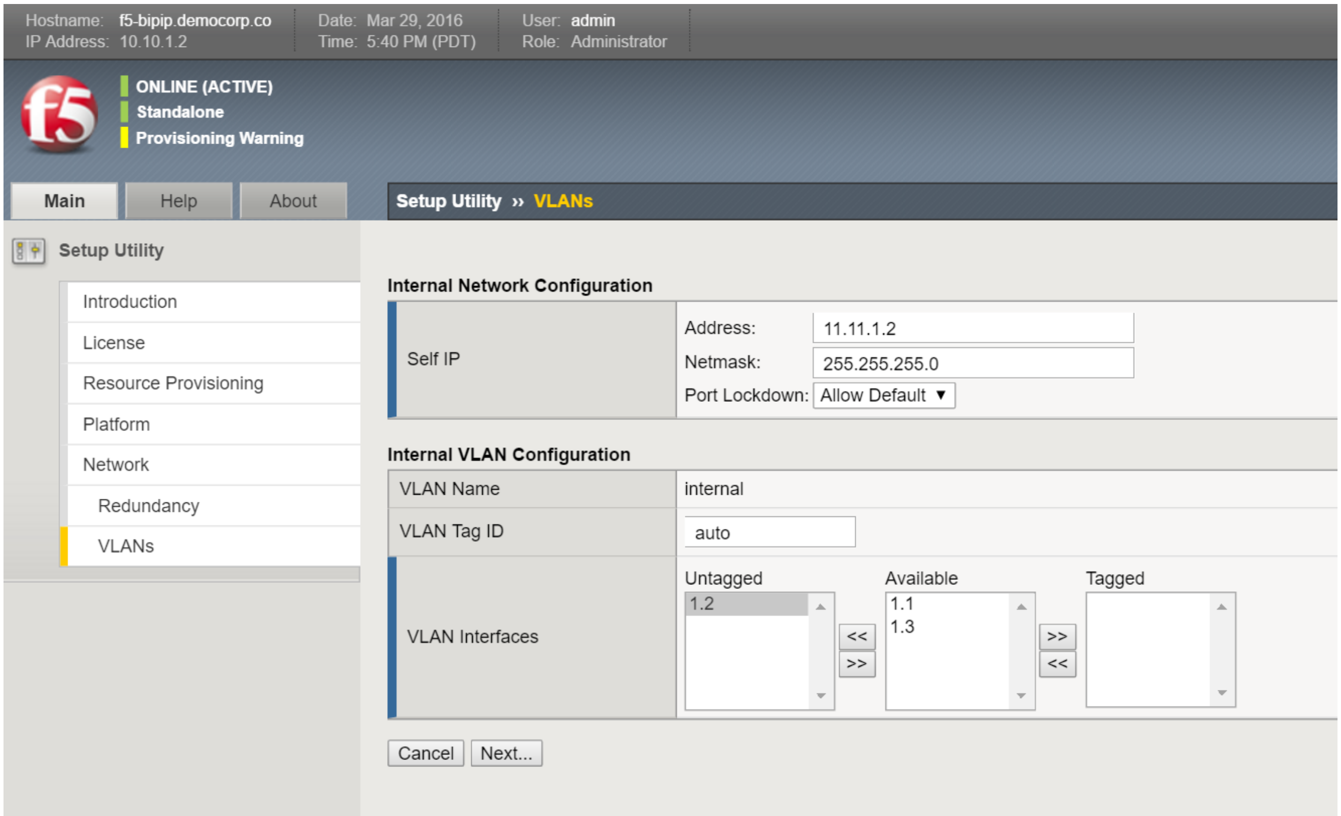
Setup Utility » Redundancy

Redundant Device Wizard Options

Config Sync	□ Display configuration synchronization options

Cancel Next...

17. Configure the Internal Network



Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 5:40 PM (PDT)
User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Setup Utility » VLANs

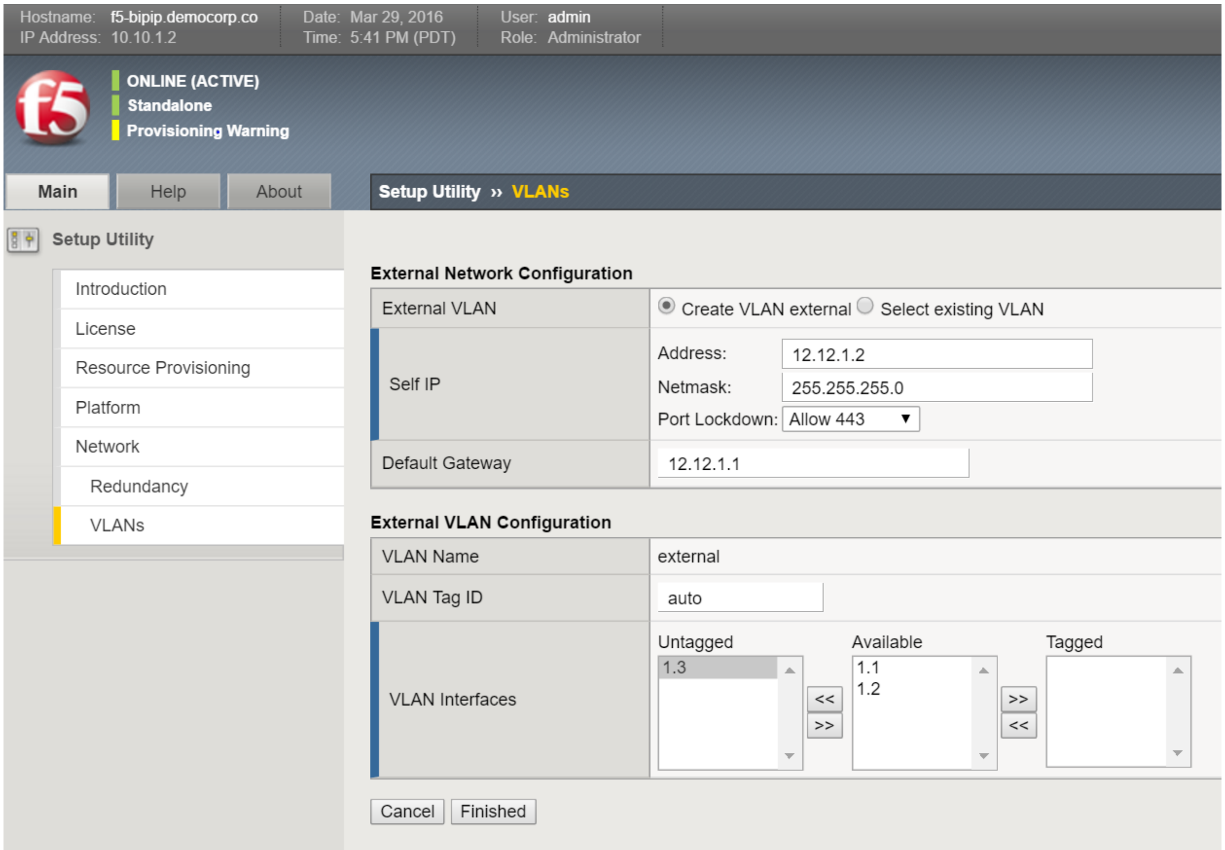
Internal Network Configuration

Self IP	Address: 11.11.1.2 Netmask: 255.255.255.0 Port Lockdown: Allow Default

Internal VLAN Configuration

VLAN Name	internal
VLAN Tag ID	auto
VLAN Interfaces	Untagged: 1.2 Available: 1.1, 1.3 Tagged:

18. Configure the External Network



Hostname: f5-bipip.democorp.co
IP Address: 10.10.1.2
Date: Mar 29, 2016
Time: 5:41 PM (PDT)
User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone
Provisioning Warning

Setup Utility » VLANs

External Network Configuration

External VLAN	● Create VLAN external ○ Select existing VLAN
Self IP	Address: 12.12.1.2 Netmask: 255.255.255.0 Port Lockdown: Allow 443
Default Gateway	12.12.1.1

External VLAN Configuration

VLAN Name	external
VLAN Tag ID	auto
VLAN Interfaces	Untagged: 1.3 Available: 1.1, 1.2 Tagged:

19. Base setup is complete at this point.