Fisher Enterprise Integration Platform

***VPC/VPN Assessment and Requirements Report***

***Table of Contents***

[***1. Purpose***](#_3dy6vkm) ***3***

[***2. Intended Audience***](#_4d34og8) ***3***

[**3. Anypoint Virtual Private Cloud (VPC)**](#_2s8eyo1) **3**

[3.1 Overview](#_17dp8vu) 3

[3.2 VPC architecture diagram](#_3rdcrjn) 3

[3.3 Advantages](#_lnxbz9) 4

[3.4 Considerations](#_35nkun2) 4

[3.5 Anypoint VPC characteristics](#_1ksv4uv) 4

[3.6 Steps to setup Anypoint VPC](#_44sinio) 4

[**4. Anypoint VPN**](#_2jxsxqh) **7**

[4.1 Overview](#_hhoze6wf8hn) 7

[4.2 VPN (IPsec Tunnel) diagram](#_3j2qqm3) 7

[4.3 Checklist for Creating an Anypoint VPN](#_1y810tw) 7

[4.4 Steps to setup Anypoint VPN](#_4i7ojhp) 7

[4.5 How to generate interesting traffic for Anypoint VPN (verify vpc-vpn connectivity)?](#_1ci93xb) 12

[**5. Dedicated Load Balancer (DLB)**](#_3whwml4) **12**

[5.1 Overview](#_wnzvq8a9wf2u) 12

[5.2 Benefits](#_qsh70q) 12

[5.3 Steps to setup Load Balancer](#_3as4poj) 13

[**6. Okta Integration**](#_49x2ik5) **14**

[6.1 Overview](#_2p2csry) 14

[6.2 Steps to Set Up Okta Integration](#_147n2zr) 15

Introduction

# 1. Purpose

This document sets the context and provides guidelines as to how to gather VPC/VPN requirements and set up the VPN and VPC.

# 2. Intended Audience

The primary audience for these guidelines are:

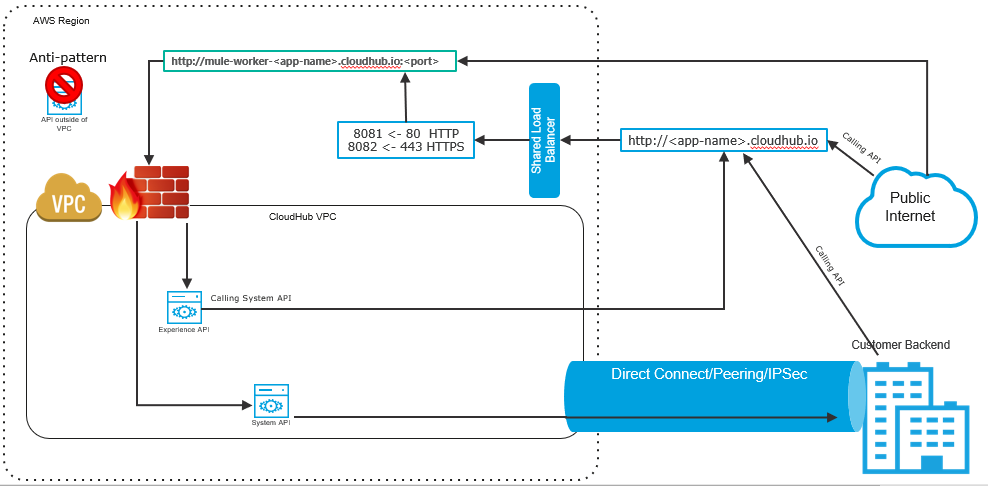
* Enterprise Architects
* Solution Architects
* Application Designers, Developers and Team leads
* Application Technical Design Architects (TDAs)

# 3. Anypoint Virtual Private Cloud (VPC)

## 3.1 Overview

Anypoint VPC allows to create a private isolated network in the cloud to host cloudhub workers. Basically, it is an isolated network segment specific to a customer & it is hosted in the AWS account which is being managed by MuleSoft. Mule applications deployed to the VPC can communicate with each other using the VPCs private network addresses. MuleSoft VPC is a customized/extended version of AWS VPC.

## 3.2 VPC architecture diagram

****

## 

## 3.3 Advantages

* It’s an enabler to securely connect with corporate data centers and on-premise applications
* It creates secure virtual networks within CloudHub
* It provides an option to choose industry standard encryption standards IPSec or SSL, and secure the network at the hardware or software levels

## 3.4 Considerations

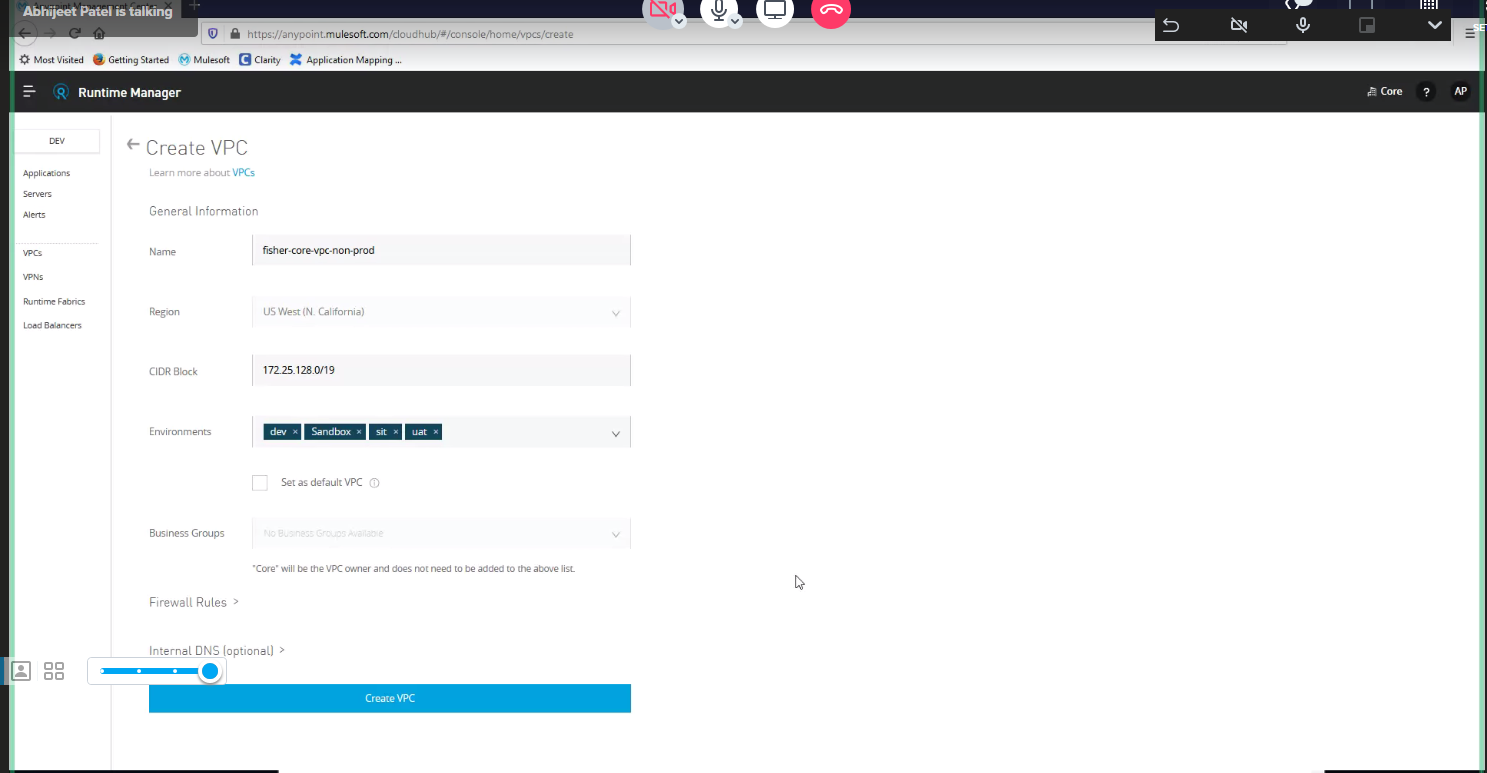
* VPCs cannot be readjusted once it is created. CIDR range & Location will not be allowed to change
  + *Note: Only Firewall rules, DNS, & associated environments are configurable*
* 2 VPN connections are included in the Subscription
* At the time of VPC creation, it is recommended to specify a CIDR block from the private IPv4 address ranges as specified in RFC 1918
* The safe rule of thumb for deciding the size of your Anypoint VPC subnet is to **calculate 10 times the maximum number of expected apps** to deploy in the VPC

## 3.5 Anypoint VPC characteristics

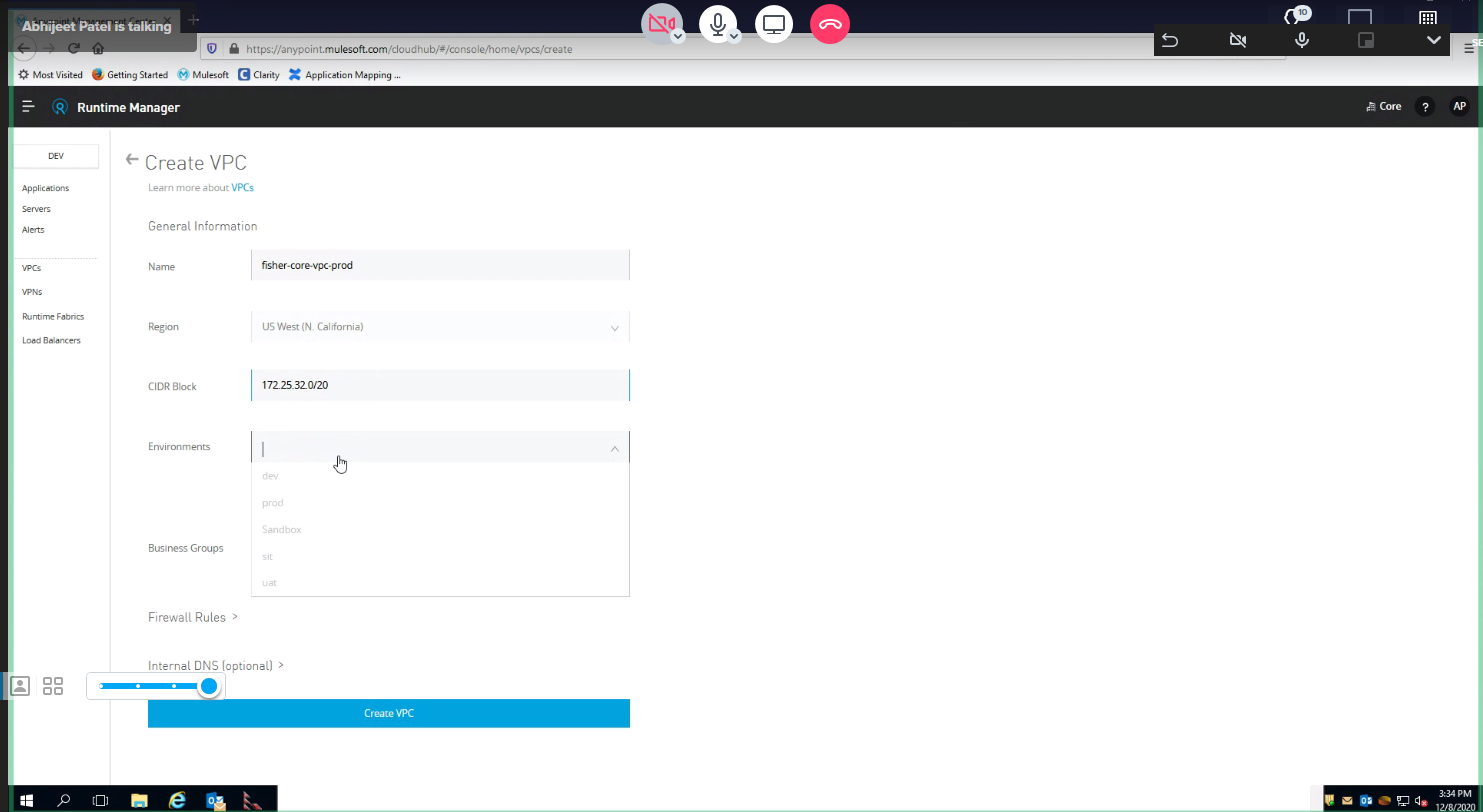
* Multiple VPC can be created in the same region
* Always create VPC in the same region or near to your datacenter or AWS region
* All non-prod environments DEV, SIT,UAT can be mapped to “non prod” VPC and production environment to “prod” VPC
* Multiple environments can be mapped to the same VPC

## 3.6 Steps to setup Anypoint VPC

* Sign into Anypoint Platform account with the Organization Administrators role
* Under Management Center, click Runtime Manager & navigate to VPC section
* Click Create VPC, and enter the following information to define and configure the Anypoint VPC:
  + **Name**: The name to identify your Anypoint VPC
  + **Region**: The region to which the Anypoint VPC is bound
  + **CIDR Block:** The size of the Anypoint VPC in Classless Inter-Domain Routing (CIDR) notation
    - For example, if you set it to 10.111.0.0/24, the Anypoint VPC is granted 256 IP addresses from 10.111.0.0 to 10.111.0.255
    - Ideally, the CIDR Blocks you choose for the Anypoint VPC come from a private IP space, and should not overlap with any other Anypoint VPC’s CIDR Blocks, or any CIDR Blocks in use in your corporate network
  + **Environments:** Select an environment to which the Anypoint VPC is bound
  + **Business Groups:** Bind the Anypoint VPC with a business group
  + **Configure Firewall Rules:** Click on it to expand the fields and configure firewall rules
    - By default, all inbound traffic is blocked and you need to configure firewall rules to allow traffic to your worker
      * You can configure these rules at a later time
      * The UI is pre-filled with suggestions of the most commonly used firewall rules

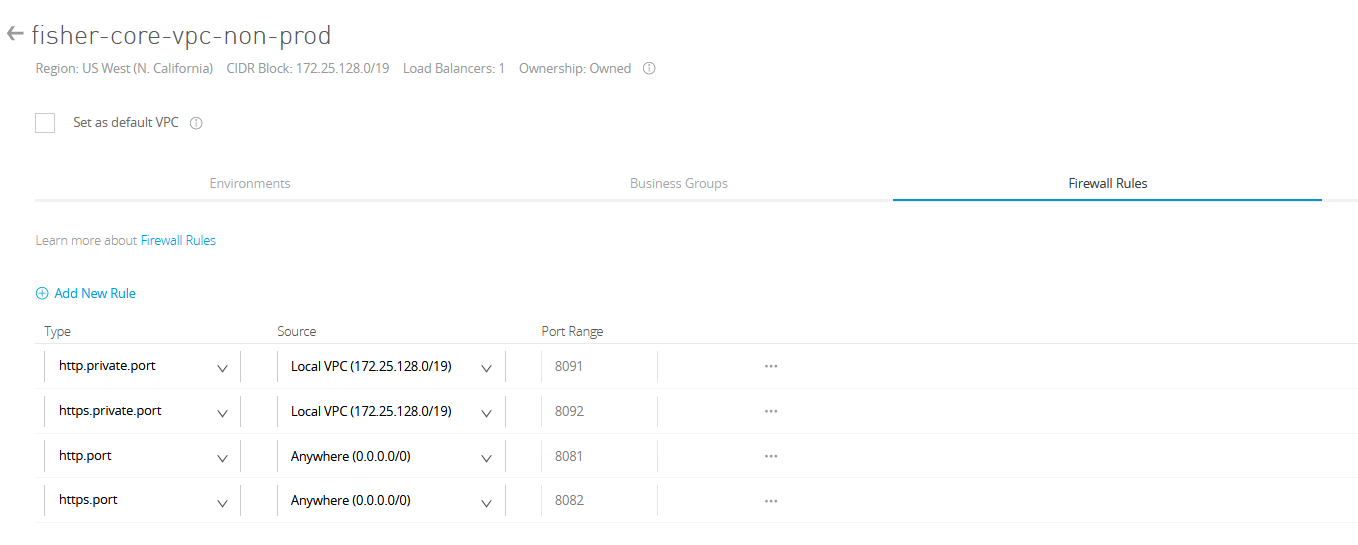


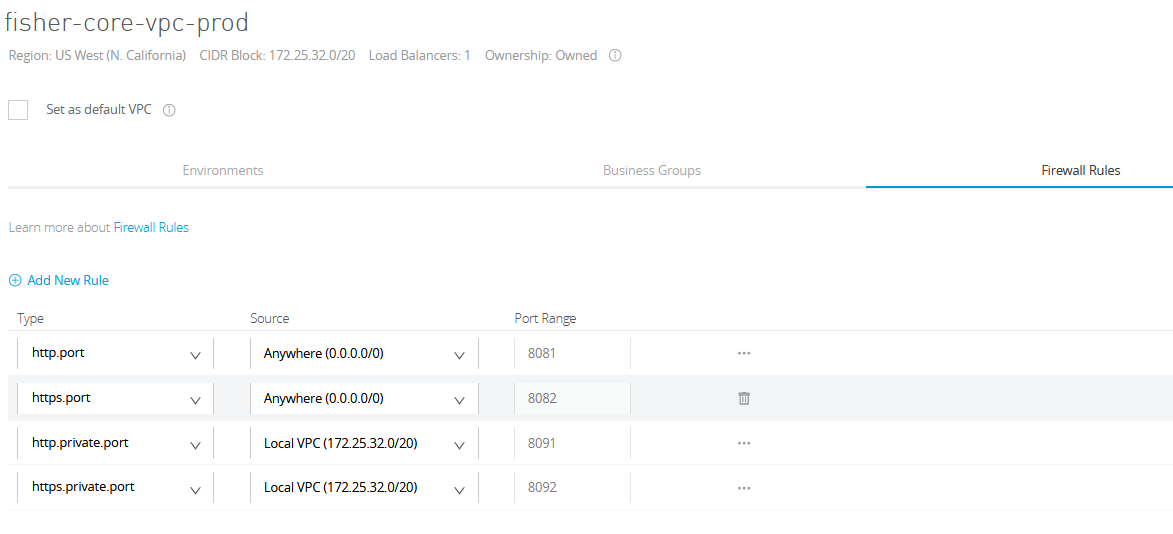
**Fig**: Non-Prod VPC Configuration



**Fig**: Prod VPC Configuration

* + - In general, we can configure 4 different rules as shown in the images below:
      * **Rule 1:** Any application running on 8081 can be reached from anywhere via http
      * **Rule 2:** Any application running on 8082 can be reached from anywhere via https
      * **Rule 3:** Any application running on 8091 can be reached from any application running inside the same Anypoint VPC
        + If these applications need to be exposed outside the Anypoint VPC they can be exposed using Dedicated Load Balancer
      * **Rule 4:** Any application running on 8092 can be reached from any application running inside the same Anypoint VPC
        + If these applications need to be exposed outside the Anypoint VPC, they can be exposed using Dedicated Load Balancer
  + **Internal DNS**: Click on it to set up internal DNS servers to resolve your private host names





All set, click on the “**Create VPC**” button to complete the setup process.

# 4. Anypoint VPN

## 4.1 Overview

Anypoint VPN helps to create a secure connection between MuleSoft VPC and customer hosted on-premises networks. It supports site-to-site Internet Protocol security (IPsec) connections.

Each Anypoint VPN connection consists of two tunnels that help to connect to a single public IP address at a remote location.

VPN licenses are bundled with the VPC license, so each VPC license also entitles the organization to 1 VPN gateway, with a connection to 1 public IP address in a remote location.

That is to say, 1 VPC License = 1 VPC entitlement + 1 VPN entitlement.

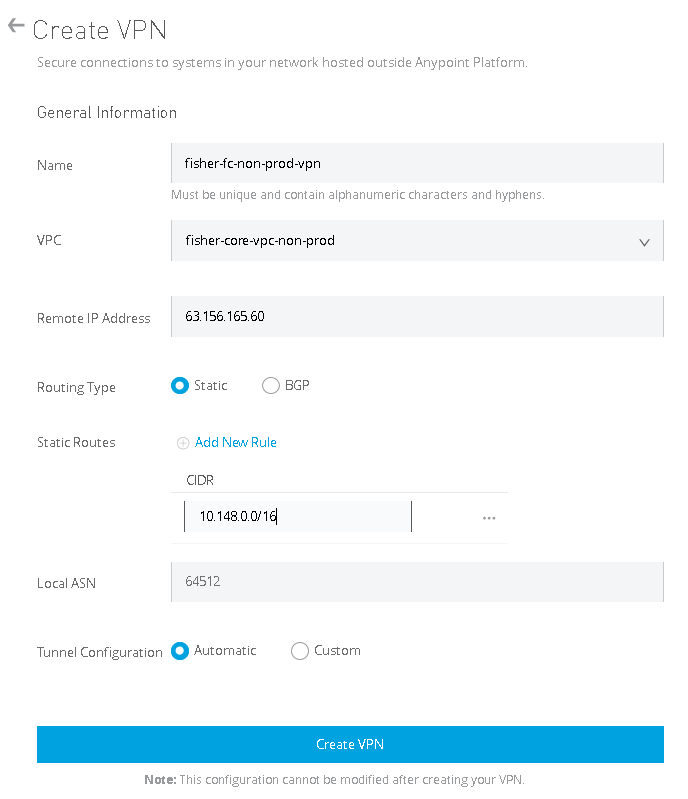
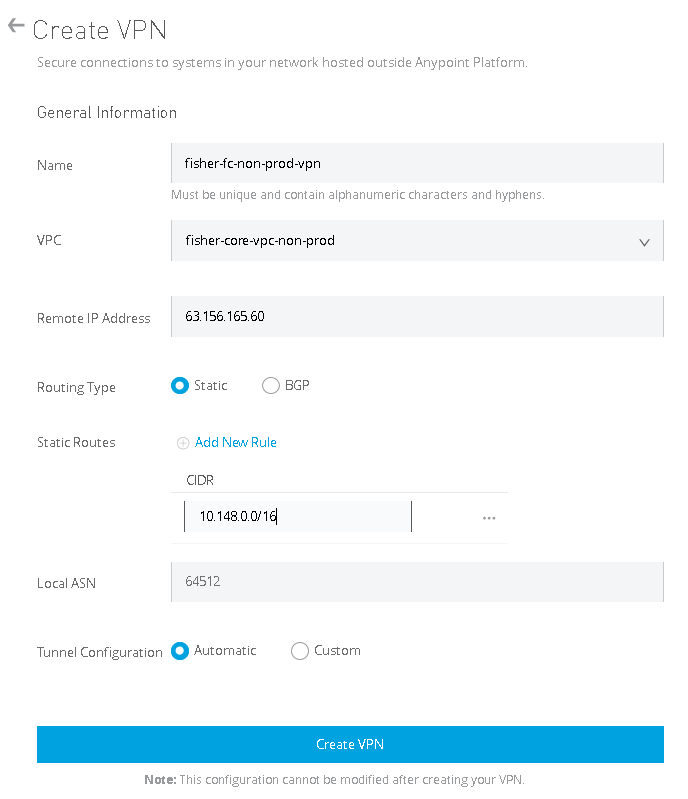
## 4.2 VPN (IPsec Tunnel) diagram

## 4.3 Checklist for Creating an Anypoint VPN

* Remote IP address: The public IP address of your VPN endpoint
  + This must be a single, static IP address
* Static Routes (CIDR): The subnets in your network to make accessible through the VPN
  + This information is required only if you are using static routing
* Remote and Local ASN: The Autonomous System Number specifies the collection of routing prefixes
  + You must configure both a remote and local ASN
  + This is required only if you are using dynamic routing
* Pre-shared Key (PSK): The shared secret for the VPN tunnels
  + These values are auto-generated if you select Automatic Tunnel Configuration
* Point-to-Point CIDR: Private IP range for the VPN tunnel interfaces
  + These values are auto-generated if you select Automatic Tunnel Configuration

## 4.4 Steps to setup Anypoint VPN

* Sign into Anypoint Platform and select Runtime Manager
* Select the environment where you want to create an Anypoint VPN
* From the menu on the left, click VPNs, and then click Create VPN
* Enter or select the following information for your Anypoint VPN:
  + **Name**: Enter a name for your Anypoint VPN
  + **VPC**: From the drop-down list, select the Virtual Private Cloud for the Anypoint VPN connection
  + **Remote IP Address**: Enter the public IP address of your VPN endpoint (customer gateway public IP)
  + **Routing Type**: You can select either BGP (dynamic) or Static.
    - Choose the Border Gateway Protocol (BGP) type if your device supports it
  + **Tunnel Configuration:**
    - **Automatic:** 
      * This option automatically configures the tunnel settings for Anypoint VPN.
        + The tunnel settings are visible after VPN creation
    - **Custom:**
      * We need to provide PSK (Pre-shared Key: The shared secret for the VPN tunnels) & Point-to-Point CIDR (the Private IP range for the VPN tunnel interfaces)
    - **Click “Create VPN”**

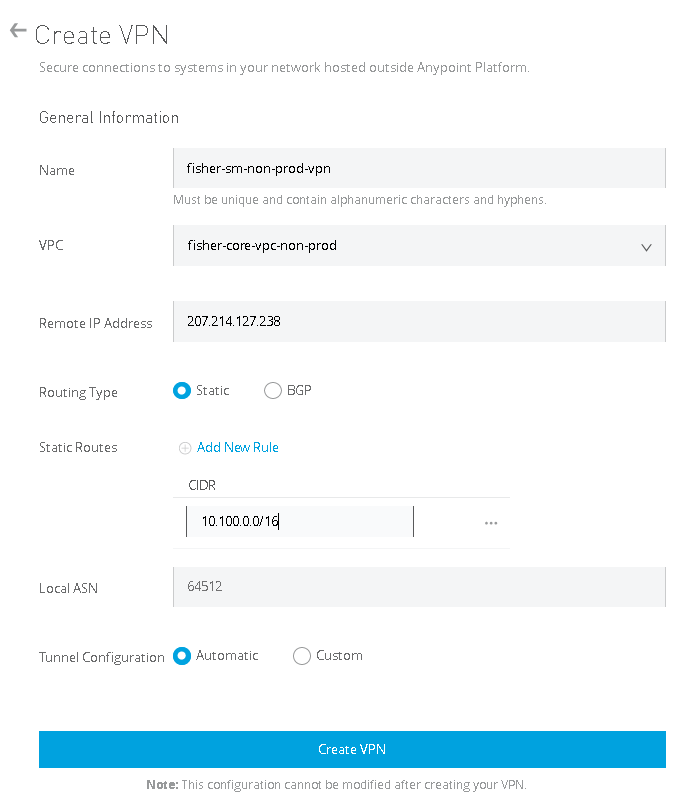


**Fig**: Non-Prod(1) VPN Configuration

* The status of the VPN will change to “Pending” with Tunnel 1 and Tunnel 2 both in “Pending” state
  + This indicates that the VPN is being configured on the CloudHub side
  + This is the expected status while the infrastructure is created

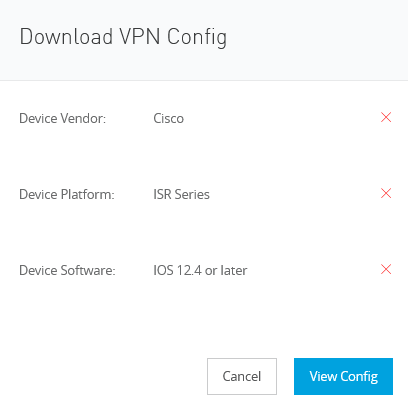
***After the status changes to AVAILABLE, continue with the next steps.***

*Note: You cannot modify tunnel settings after you create the Anypoint VPN connection. To change the settings for an existing connection, you must delete the Anypoint VPN connection and create a new one.*

****

**Fig**: Non-Prod(2) VPN Configuration

* Download the configuration file from your Anypoint VPN
* You have an option to select the configuration file based on your device type, either Cisco or a generic
  + Your Customer Gateway device vendor determines the option you select here
    - If it’s a Cisco device, select Cisco, or select generic for all other types of customer gateways



* Configure your VPN endpoint: Share the VPN configuration file with your VPN endpoint administrator

## 

## 4.5 How to generate interesting traffic for Anypoint VPN (verify vpc-vpn connectivity)?

* Download ***“Net Tools API 2.2.0”*** application from the following github [link](https://github.com/mulesoft-labs/net-tools-api/releases/download/2.2.0/net-tools-v2.2.0.jar)
* Deploy the application to each VPC where you wish to the verify connectivity
* After deployment of the application is done in cloudhub, it can be accessed by the web-browser and the connectivity of different destination IP addresses can easily be tested

***Note****: Find the tutorials on using* ***“Net Tools API 2.2.0”*** *application in the following* [*link*](https://help.mulesoft.com/s/article/How-To-Use-Network-Tools-Application?r=5&ui-force-components-controllers-recordGlobalValueProvider.RecordGvp.getRecord=1)

# 5. Dedicated Load Balancer (DLB)

## 5.1 Overview

The Dedicated Load Balancer, sits inside the Client’s VPC, routes external HTTP and HTTPS traffic to multiple Mule applications deployed to CloudHub workers in a Virtual Private Cloud (VPC).

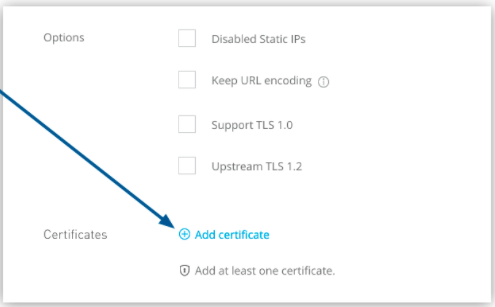
**Note:** Unlike DLB, “***Shared Load Balancer (SLB)***” does not allow an user to configure a custom SSL certificate or proxy rules. There is one SLB clustered instance in each CloudHub region that serves all the CloudHub customers in that AWS region.

## 5.2 Benefits

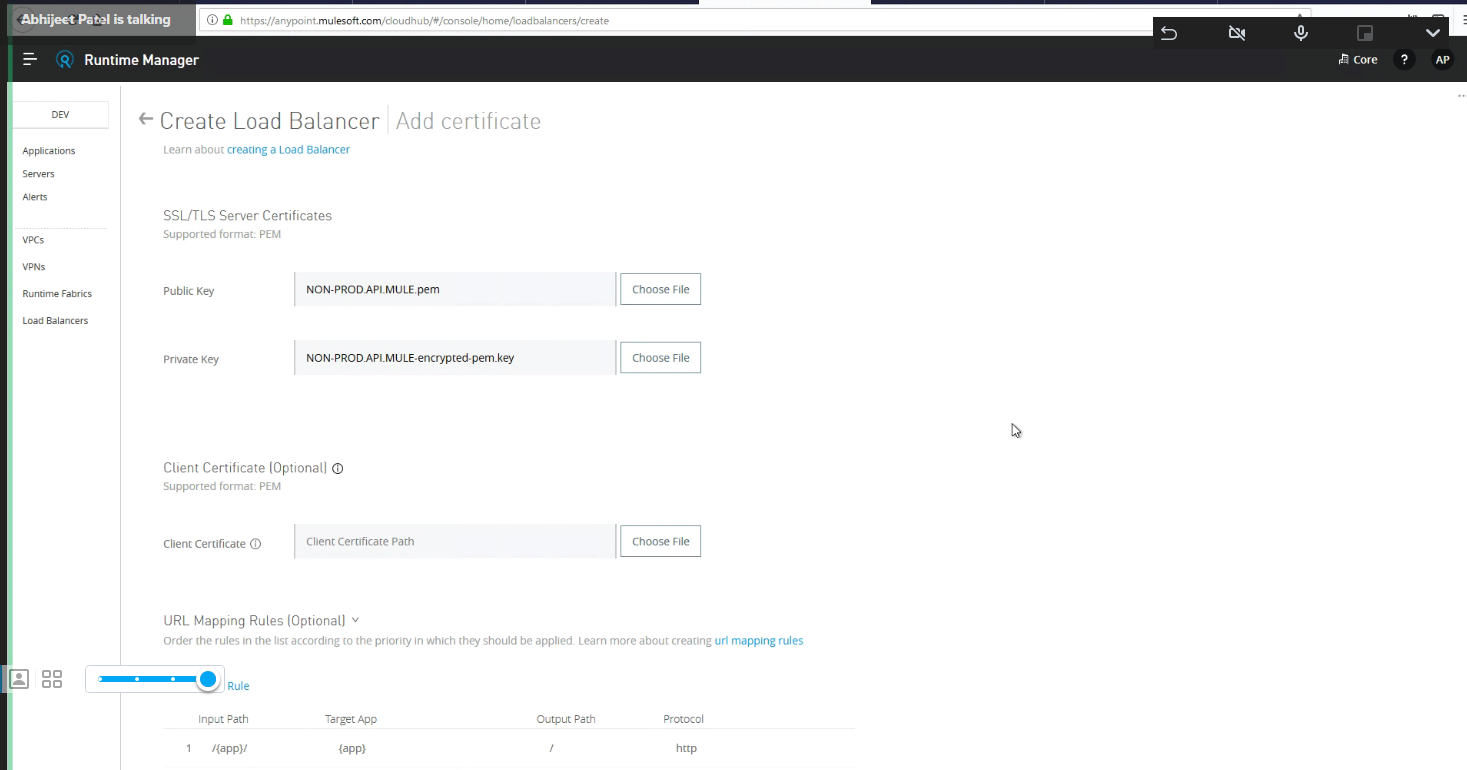
* Allows custom TLS certificates (including 2-Way TLS Authentication)
* Define proxy rules and route requests to the appropriate REST resource
* Use a custom/vanity domain which is registered on a DNS server
* Allows IP Whitelist/Blacklist
* VPCs and DLBs can safely connect CloudHub environments with internal networks
* It can handle Mule event payloads up to 200 MB

## 5.3 Steps to setup Load Balancer

* After entering Runtime manager inside Anypoint platform, click on “Create Load Balancer”
* Enter a name for your load balancer
* Select a target Anypoint VPC from the drop-down list
* Specify the amount of time the DLB waits for a response from the Mule application in the Timeout in Seconds field (The default value is 300 seconds)
* Add any whitelisted classless inter-domain routing (CIDR) as required
* Select the inbound HTTP mode for the load balancer
* Assigning your custom domain (CNAME mapping needs to be done at the DNS server)
* Add a certificate:
  + Click Add certificate



* + On the “***Add certificate page***”, select Choose File to upload both public key and private key files
  + You can enable two-way SSL by uploading client certificates



**Fig:** Adding certificates to Non-Prod DLB

* Define routing rules
  + We can define different routing rules
  + In the URL Mapping Rules section, we can adjust the routing mechanism

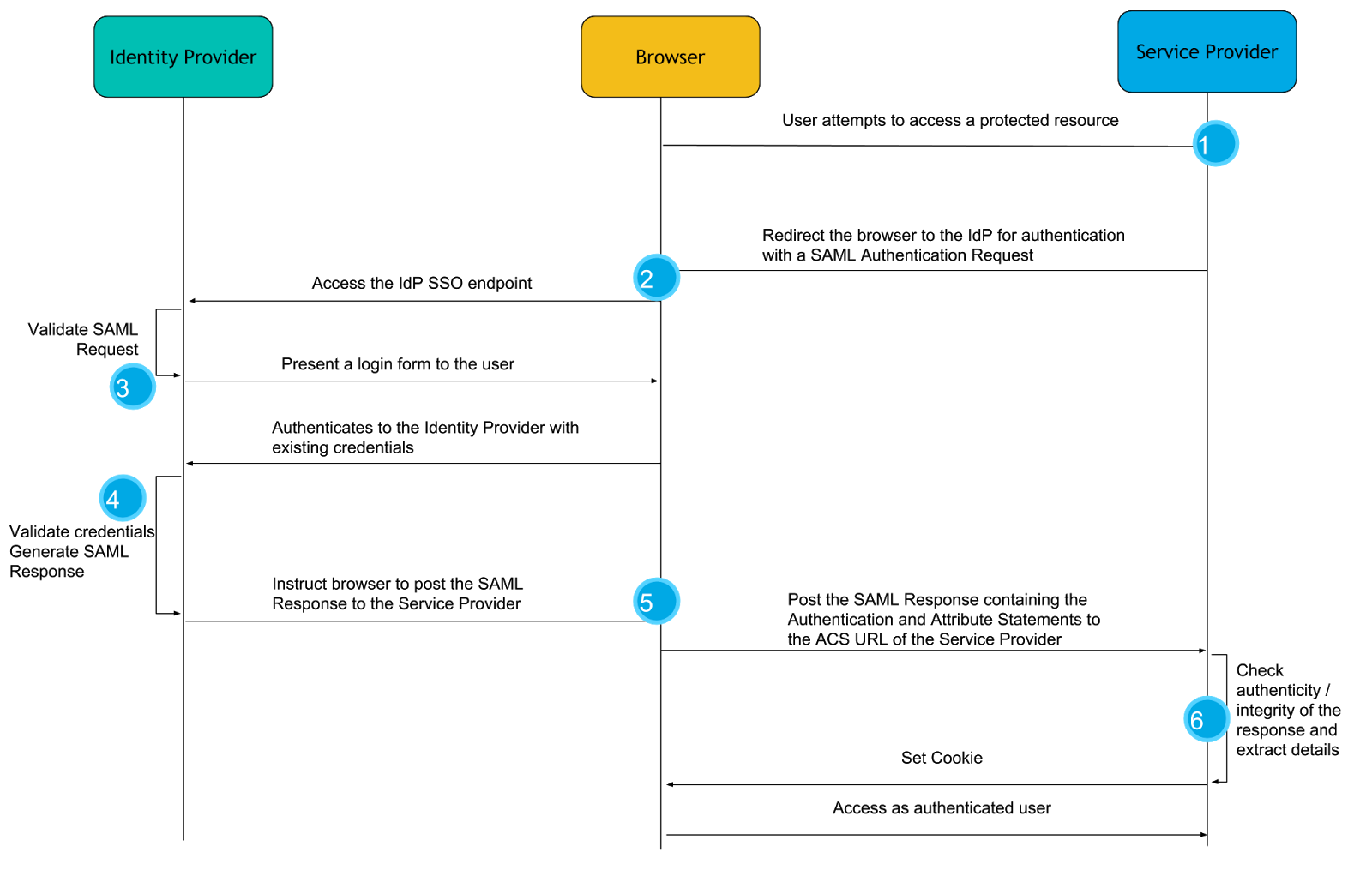
# 6. Okta Integration

## 6.1 Overview

The goal is to configure the Anypoint Platform to use Okta as an Identity Provider using Security Assertion Markup Language (SAML). SAML is an open standard that permits identity providers to pass authorization credentials to service providers. Basically, SAML allows you to log into different websites with only one set of credentials. The idea is that it’s less complicated to manage one login per user than it is to administer multiple logins for different applications throughout the Fisher.

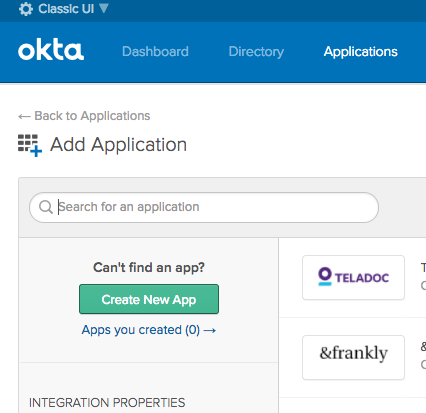
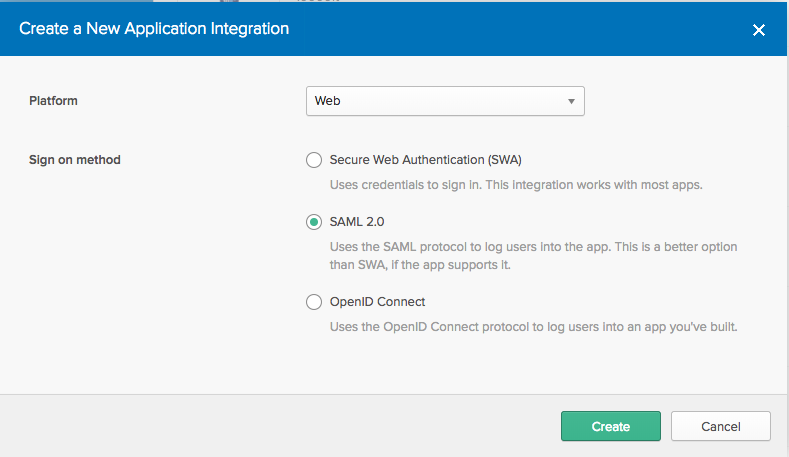
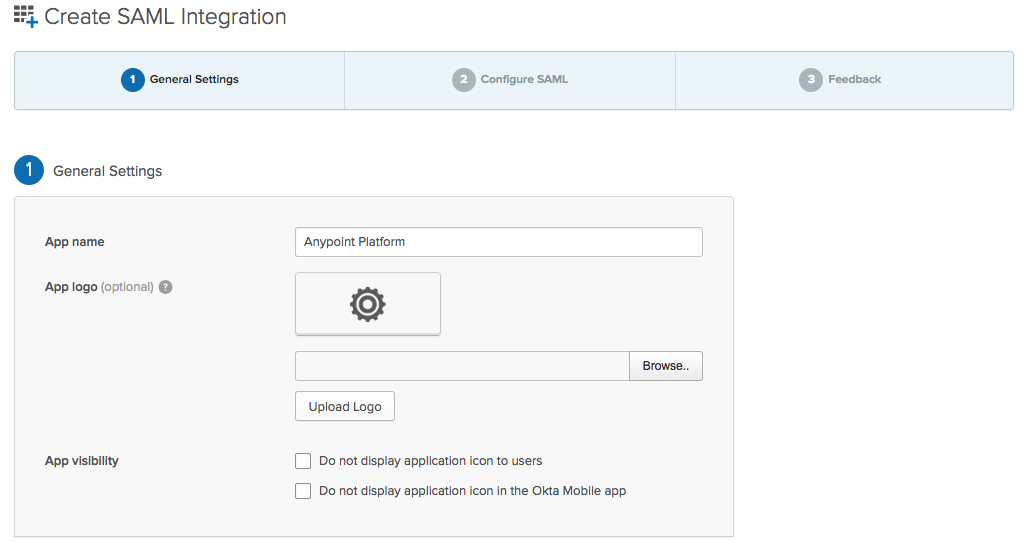
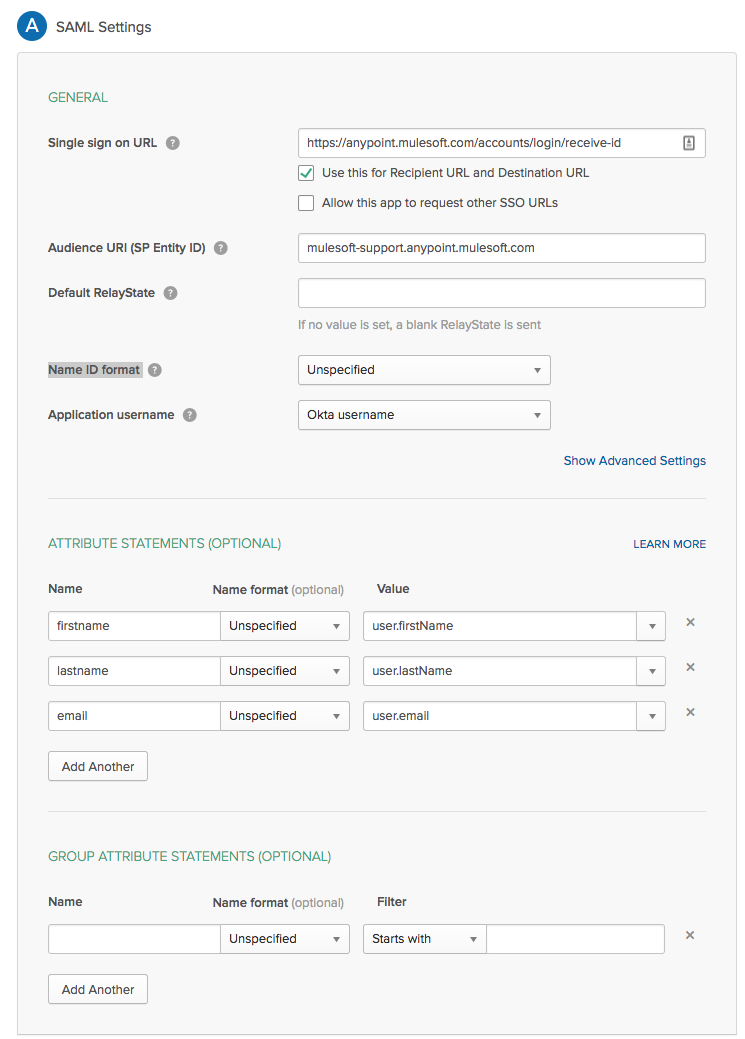
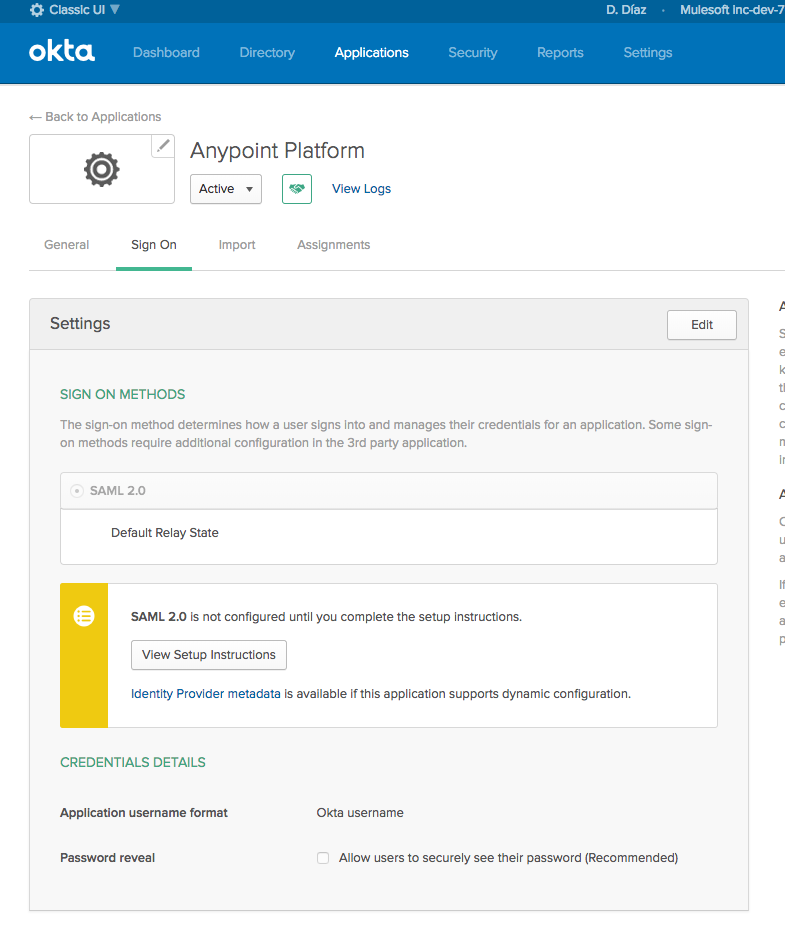
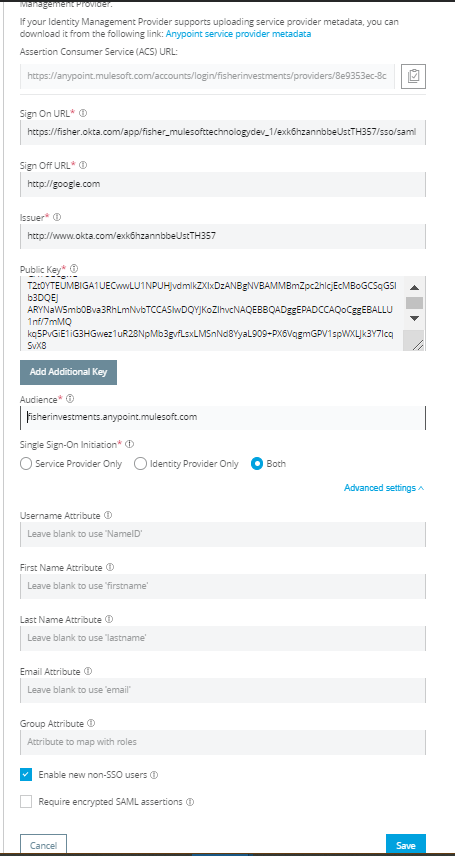
In order to standardize communication between the identity and service providers, SAML uses Extensible Markup Language (XML). This links the user’s identity authentication to the authorization to use a service.

SAML interaction diagram:



## 6.2 Steps to Set Up Okta Integration

Okta Configuration

* **Step 1:** 
  + Make sure to select Classic UI on the top left
  + Head over to Okta UI -> Applications -> Create New App
  + 
* **Step 2:** 
  + Select SAML 2.0 for the New Application Integration
  + 
* **Step 3:** 
  + Under General Settings give it a name and a logo (optional)
  + 
* **Step 4:** 
  + Under Configure SAML enter the following settings:
    - Single sign on URL: https://anypoint.mulesoft.com/accounts/login/receive-id
    - Audience URI (SP Entity ID): {organisation}.anypoint.mulesoft.com
    - Name ID format: Unspecified
    - Application username: Okta username
* **Step 5:** 
  + For Attribute Statements enter the following information:
    - Attribute name: firstname
    - Attribute format: Unspecified
    - Attribute value: user.firstName
    - Attribute name: lastname
    - Attribute format: Unspecified
    - Attribute value: user.lastName
    - Attribute name: email
    - Attribute format: Unspecified
    - Attribute value: user.email
  + 
* **Step 5:** 
  + Hit Next until you're returned to the main Application page.
* **Step 6:** 
  + Out of the main Application page, click on the View Setup Instructions inside the Settings box.
  + 
* **Step 7:** 
  + With this information, you will set up the Anypoint platform.
  + Complete the required following fields on the Platform:
    - Sign On URL:
      * This is the URL you'll be redirected to for IdP sign-on.
      * https://fisher.okta.com/app/fisher\_mulesofttechnologydev\_1/exk6hzannbbeUstTH357/sso/saml
    - Sign Off URL:
      * URL to send the Single Log-Out request to, so users both sign out of the Anypoint Platform and have their SAML user’s status set to signed out.
      * For example: http://orgname.okta.com/app/{AppName}/{AppID}/slo/saml
    - Issuer:
      * Should match the issuer of the SAML assertion.
      * http://www.okta.com/exk6hzannbbeUstTH357
    - Public Key:
      * Public key provided by the identity provider, used to sign the SAML assertion (x.509 Certificate).
    - Audience:
      * The exact same arbitrary string value defined in Step 8.
      * fisherinvestments.anypoint.mulesoft.com
    - Single Sign-On Initiation: Both
    - Enable new non-SSO users: Checked
      * **Note**: for Single Sign-On Initiation and Enable new non-SSO users, once the SailPoint integration is completed, the value for Single Sign-On should be set to “Service Provider Only”; and Enable new non-SSO users should be unchecked.
  + 
* **Step 8:**
  + Assign user to your application in Okta
    - Click on Assignment tab> click assign> select user
  + Then test if SSO is working
    - Go to the "My Apps" button on the top right and click your application. It should log you in
* **Notes:**
  + If you wish to take advantage of using groups, MuleSoft supports sending user group information through the SAML assertion to assign users to corresponding Roles in MuleSoft.
  + To take advantage of this functionality, users that you add to your MuleSoft application must belong to a group.