Enterprise Integration Platform

***Anypoint platform setup details and questionnaires***

Table of Contents

[1. Purpose 3](#_Toc71759724)

[2. Business Group 3](#_Toc71759725)

[**Steps to Create Business Groups:** 3](#_Toc71759726)

[3. Environments 5](#_Toc71759727)

[**Steps to Create Environments:** 6](#_Toc71759728)

[4. Virtual Private Cloud 7](#_Toc71759729)

[**Name** 7](#_Toc71759730)

[**Region** 8](#_Toc71759731)

[**CIDR Block** 8](#_Toc71759732)

[**How to Decide on the Size of CIDR Block:** 8](#_Toc71759733)

[**Firewall Rules** 10](#_Toc71759734)

[5. Dedicated Load Balancer 11](#_Toc71759735)

[**Steps to Create Dedicated Load Balancer:** 12](#_Toc71759736)

[6. Virtual Private Network 14](#_Toc71759737)

[**Anypoint VPN IPSec Tunneling** 14](#_Toc71759738)

[**Routing Type**: 15](#_Toc71759739)

[**Tunnel Configuration:** 16](#_Toc71759740)

[**Limitations** 16](#_Toc71759741)

[**Recommendations** 17](#_Toc71759742)

Introduction

# Purpose

This document sets the context and provides guidelines to gather detail requirements to setup Anypoint platform and CloudHub.

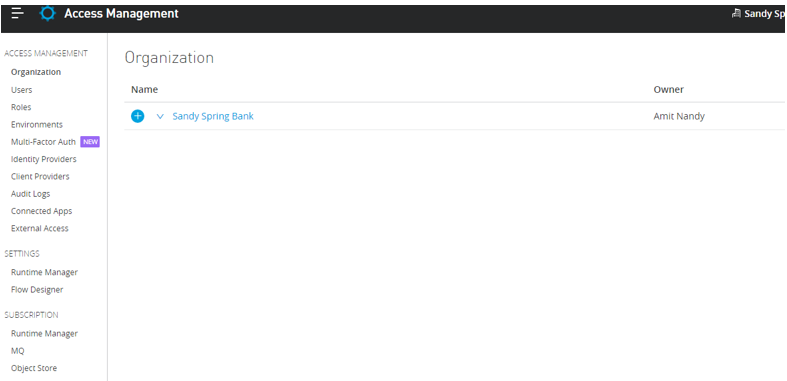
# Business Group

Business groups are self-contained resource groups that contain MuleSoft Anypoint Platform resources such as applications and APIs. Business groups provide a way to separate and control access to MuleSoft Anypoint Platform resources because users have access only to the business groups in which they have a role.

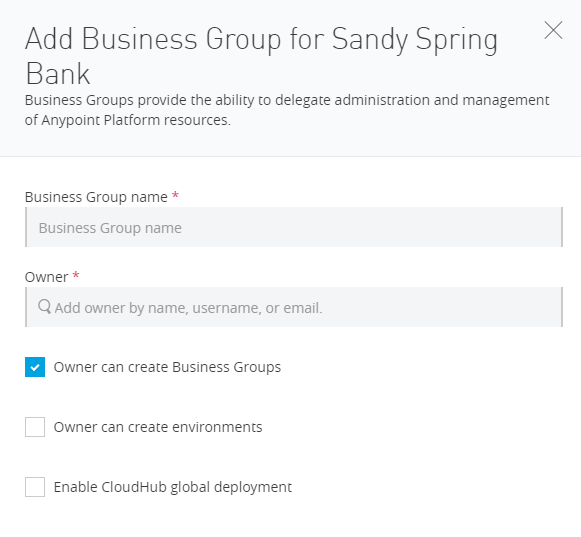
***Recommendation:*** My recommendation is to create vpc under master org. We can have Business Group as “**Digital Banking**”

## **Steps to Create Business Groups:**

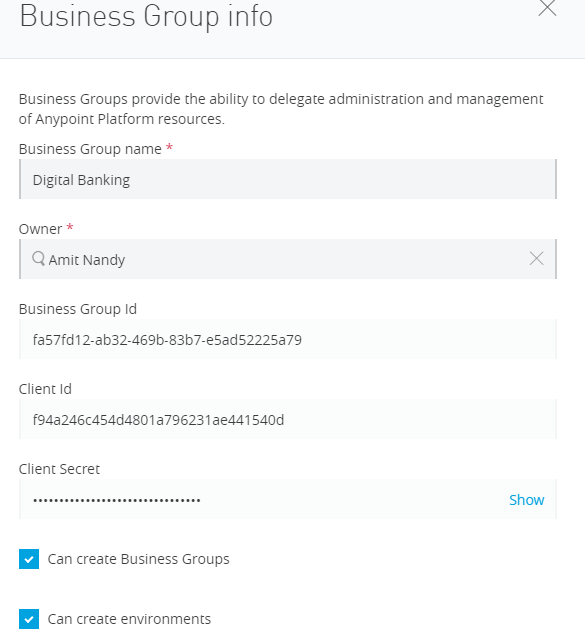
* Login to Anypoint Platform as an admin user.
* Click on Access Management
* Click on Organizations.



* Click on “**+**” under organization.



* Enter Business Group Name, Owner Name and tick checkbox “Owner can create environments”. Leave all others as default.



# Environments

MuleSoft gives you an opportunity to create multiple environments within a VPC.

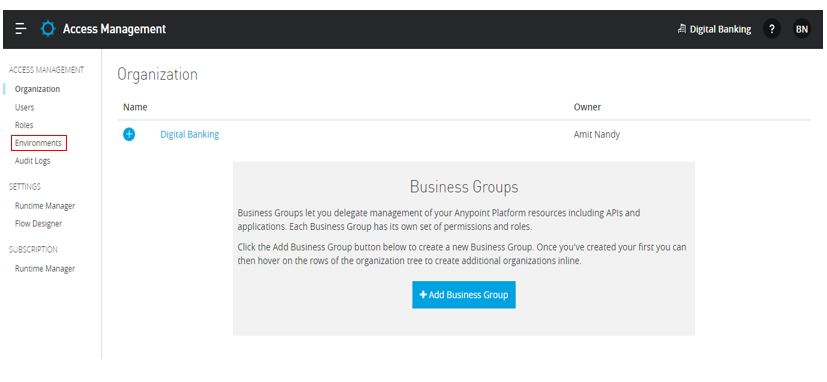
Environments get associated with one VPC and only one. What’s we need to understand here is that we can have multiple environments in the same VPC, but each environment can be associated to only one VPC. One environment cannot be part of two VPCs

Please list the environment names which you want to have in your non-prod and prod vpc.

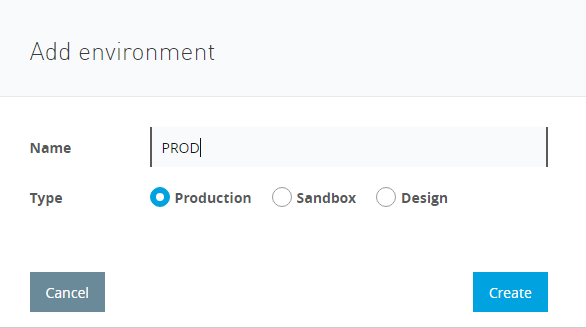
|  |  |  |  |
| --- | --- | --- | --- |
| VPC | Examples | Names | Recommendation |
| Non-Prod | DEV, QA |  | DEV, SIT, UAT |
| PROD | PROD |  | PROD |

## **Steps to Create Environments:**

* Login to Anypoint platform as an admin user.
* On right top corner select master organization (Sandy Spring Bank).
* Under business group select “Digital Banking”.
* Click on Access Management.
* Click Environments on left menu.



* Click on Add Environment Button.
* Enter “PROD” in Name text box.
* select production radio button and click on create.



* Repeat the same steps for non-prod environment (SIT and UAT).
* Select sandbox radio button and click create.

# Virtual Private Cloud

A [VPC in Anypoint](https://www.mulesoft.com/platform/services/vpc-virtual-private-cloud) is a virtual, private, and isolated network segment that we can create within the MuleSoft infrastructure to host our CloudHub workers. Each Mule VPC:

* Will get a dedicated range of private IP addresses for our workers.
* Will have its own firewall to secure access to the workers within it.
* Will span across all the availability zones of the AWS region where the VPC is created.

To setup the VPC we need the below information.

## **Name**

The name to identify your Anypoint VPC. Also, it should be

* Be unique within the organization.
* Between 3 - 42 characters long.
* Contain only lowercase letters, numbers, and dashes
* You cannot change the name of a VPC after you create it. To change the name, delete and recreate the VPC.

***Example***: ssb.nonprod-vpc, ssb-prod-vpc

## **Region**

The region to which the Anypoint VPC is bound, The recommended region to use might vary depending on how you connect to your Anypoint VPC.

* If you are using a VPN tunnel, you might want to choose the CloudHub region closest to your data center.
* However, if you are peering with your private AWS VPC, you need to create your Anypoint VPC in the same AWS region.

## **CIDR Block**

The size of the Anypoint VPC in Classless Inter-Domain Routing (**CIDR**) notation.

* 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.
* This setting is configurable only during this initial creation of an Anypoint VPC. Once the Anypoint VPC instance is created, you cannot resize it or edit your selected CIDR block.

## **How to Decide on the Size of CIDR Block:**

To calculate the proper sizing for your Anypoint VPC, you first need to understand that the number of dedicated IP addresses is not the same as the number of deployed workers.

For each worker deployed to CloudHub, the following IP assignation takes place:

* At least two IP addresses per worker to perform at zero-downtime.
* For better fault tolerance, the VPC subnet may be divided into up to four Availability Zones.
* A few IP addresses are reserved for infrastructure.
* 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.
* No of environment you are going to have in non-prod.

**Note:**  Due to this structure, the smallest network subnet block you can assign for your Anypoint VPC is /24 and the largest /16.

So, you are planned to have 100 in each environment (please envision for future scalability) APIs in the VPC, then calculations should be as below.

* 100 \* 2 (no of non-prod environment) = 200
* 200 \* 2 (zero downtime) = 400
* 400 \* 4 (no of Availability Zones) = 1600
* 1600 + 20% (for infrastructure) = 1920

So, we should assign at least 1920 private IPs, which is almost 10 times the maximum number of expected apps to deploy in VPC.

|  |  |  |
| --- | --- | --- |
| CIDR | Total IPs | Usable IPs |
| /24 | 256 | 254 |
| /23 | 512 | 510 |
| /22 | 1024 | 1022 |
| /21 | 2048 | 2046 |
| /20 | 4096 | 4094 |
| /19 | 8192 | 8190 |
| /18 | 16,384 | 16,382 |
| /17 | 32,768 | 32,766 |
| /16 | 65,536 | 65,534 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Year | 2021 | 2022 | 2023 | 2024 |
| No of Environment |  |  |  |  |
| No Of application |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VPC Name | Region | CIDR Block | # of IPs | Environments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

***Recommendations:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VPC Name | Region | CIDR Block | # of IPs | Environments |
| ssb-non-prod-vpc | Us-east (N. Virginia) | /19 | 8192 | DEV, SIT, UAT |
| ssb-prod-vpc | Us-east (N. Virginia) | /20 | 4096 | PROD |

## **Firewall Rules**

By default, all inbound traffic is blocked, and you need to configure firewall rules to allow traffic to your worker.

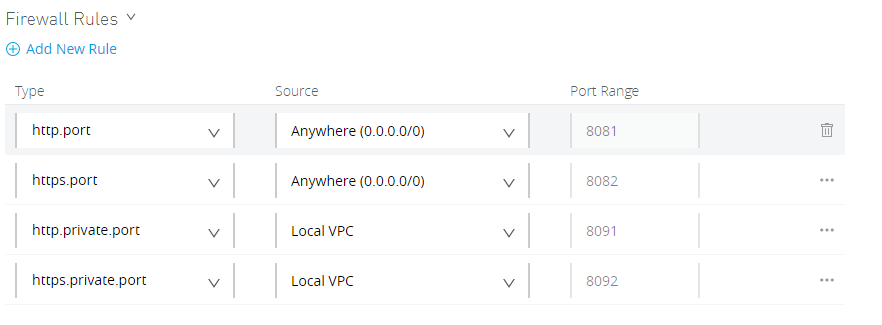
When you create an Anypoint VPC, four firewall rules are created by default:

* Two rules to allow inbound connections from within your local Anypoint VPC through ports 8091 and 8092:

This firewall rules allow traffic from within the Anypoint VPC to reach your workers through 8091 and 8092. These are the only ports used by your CloudHub-dedicated load balancer to proxy all external communications to your workers

* Anywhere (0.0.0.0/0) rules allow traffic from any host to reach your workers through ports 8081 and 8082. CloudHub’s shared load balancer uses these ports to proxy external requests to your workers.

You can remove these rules if you don’t want your internal workers to be reached by the publicly accessible load balancer



# Dedicated Load Balancer

CloudHub Dedicated load balancers enable you to:

* Handle load balancing among the different CloudHub workers that run your application.
* Define SSL configurations to provide custom certificates and optionally enforce two-way SSL client authentication.
* Configure proxy rules that map your applications to custom domains.

This enables you to host your applications under a single domain.

As you can associate multiple environments with the same Anypoint VPC, you can use the same dedicated load balancer for your different environments.

**Name:**Must be unique across all DLBs defined in Anypoint Platform (by all MuleSoft customers). You cannot rename once created, so delete it and create it with a new name. The domain name for your LB will be as **<lb-name>.lb.anypointdns.net**

**Target VPC:**Select target VPC for which this LB should be created

**Timeout in Seconds:**Specify the amount of time the DLB waits for a Mule application response. 300 milliseconds are the default value.

**Whitelisted CIDR's:**The IP addresses you specify here are the only IP addresses that can access the load balancer. The default value is 0.0.0.0/0

***Recommendation:***

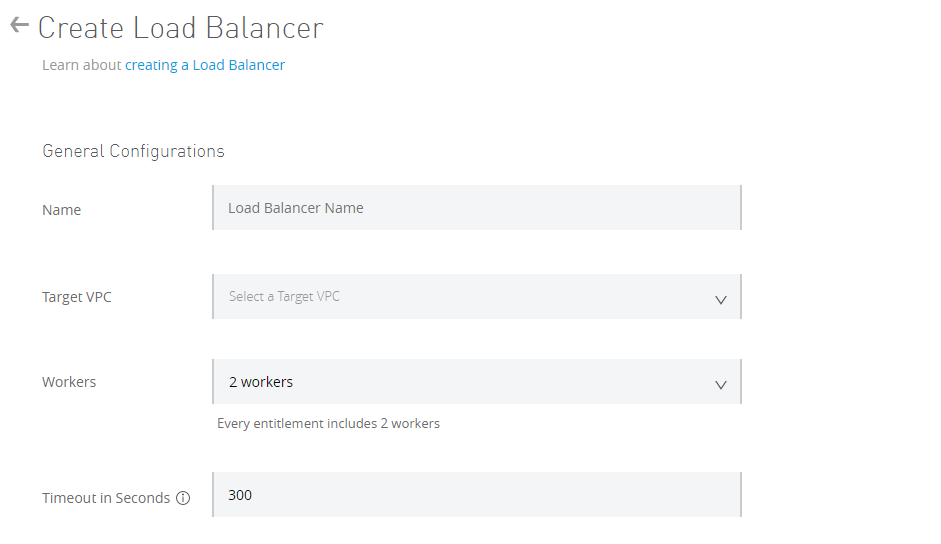
|  |  |  |
| --- | --- | --- |
| DLB Name | DLB URLs | Certificate Names |
| nonprod-sandyspringbank | nonprod-sandyspringbank.lb.anypointdns.net | 1-way-SSL (internal):  <<placeholder of certificate name>>  2-way-SSL (internal): <<placeholder of certificate name>> |
| prod-sandyspringbank | prod-sandyspringbank.lb.anypointdns.net | 1-way-SSL (internal): <<placeholder of certificate name>>  2-way-SSL (internal): <<placeholder of certificate name>> |

**DNS Name**: Recommendation

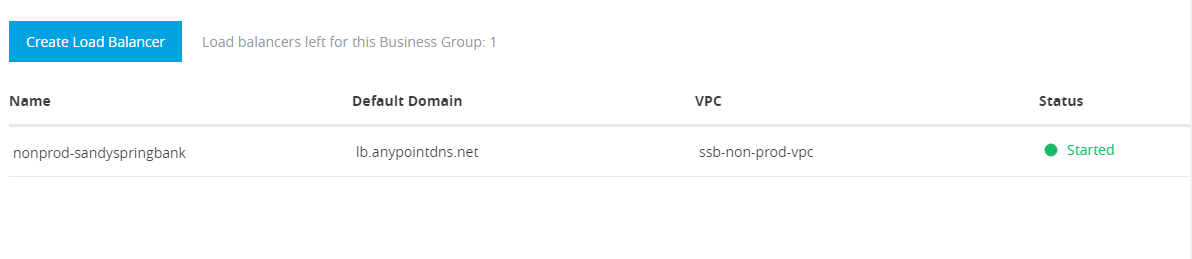
* **Non-prod:** api-np.sandyspringbank.com
* **Prod:** api.sandyspringbank.com

## **Steps to Create Dedicated Load Balancer:**

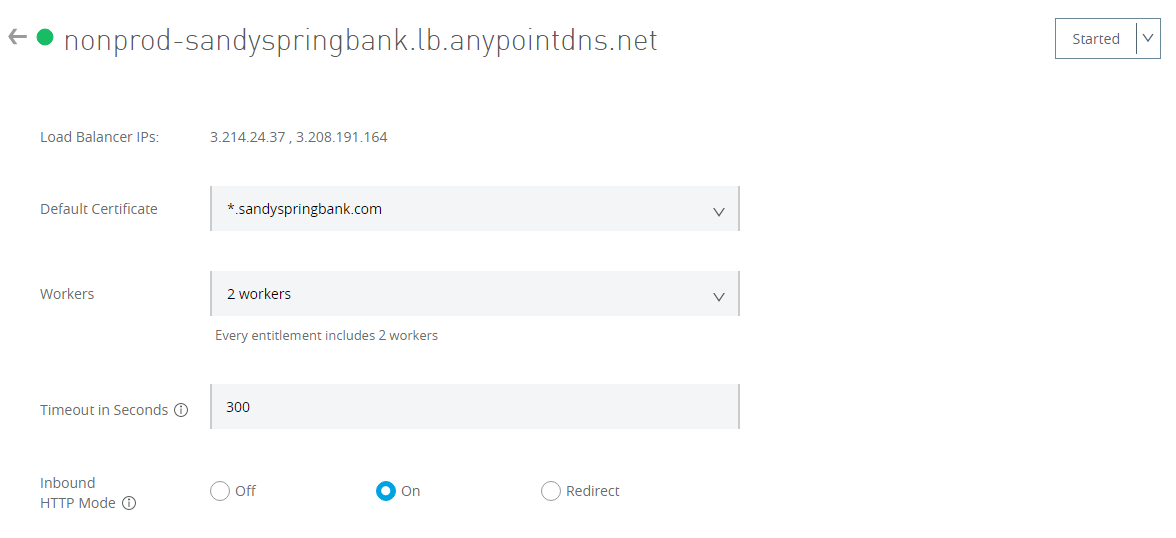
* Login to Anypoint platform as an admin user.
* Click on Runtime Manager.
* Click on Load Balancers and click create load balancer.
* Enter Name as “nonprod-sandyspringbank”.
* Select target VPC as ssb-non-prod-vpc.



* Click Add Certificates.
* Choose public key and private key from your stored location. It only supports .PEM file.
* Click on save certificate.
* Click on Create Load Balancer.
* Load Balancer will start configuring and once done the status shows Started.



* Click on newly created load balancer and you can see all the configuration as below.



# Virtual Private Network

Anypoint VPN is to create a secure connection between your MuleSoft Virtual Private Cloud (VPC) and your on-premises network. You can create multiple site-to-site VPNs if required.

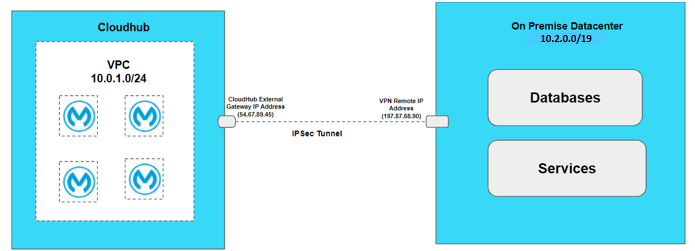
Anypoint VPN supports site-to-site Internet Protocol security (IPsec) connections. A physical or software appliance, called a VPN endpoint, is the terminator on your side of the connection. The MuleSoft side of the connection is an implementation of a virtual private gateway (VGW).

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

A single VPN provides increased availability for your MuleSoft VPC. Routine maintenance can briefly disable one of the two tunnels of your VPN connection. During this time, your VPN connection automatically fails over to the second tunnel, so access is not interrupted. For this reason, both tunnels must be configured on your endpoint.

## **Anypoint VPN IPSec Tunneling**

VPN IPSec tunnel is a set of protocols or standards to establish a connection with an on-premise datacenter. IPSec tunnel is applied at the IP layer and it allows us to connect the entire network instead of a single device.



**Note:**IP Addresses used in the above pictures are just examples

**Name:**Name of VPN. Example “**ssb-datacenter-vpn**”

**VPC:**Select the VPC for which you want to create a VPN.

**Remote IP Address:**The public IP address of your VPN endpoint. This must be a single, static IP address of the VPN device on customer data center.

## **Routing Type**:

* **Static:**As the name suggests, it will use static routes. You need to specify the routes (subnet) in your network that are accessible through the Anypoint VPN.
  + **CIDR:**  enter a subnet to make accessible through the VPN, for example, 10.2.0.0/19.
  + You can add more subnets, a maximum of 95 route table entries are allowed per VPC.
* **BGP (dynamic routing): Border Gateway Protocol (BGP)**is a protocol for dynamic routing which will re-calculate routes after every network change. For dynamic routing, we need to define the below.
  + **Remote ASN (Autonomous System Number):** Enter the ASN corresponding to your data center. You can use an existing ASN assigned to your network or a private ASN (64512–65534) that is not already assigned to your network. The default value is 65001.
  + **Local ASN (Autonomous System Number):** Assign an ASN for the MuleSoft side. Use a private ASN (64512–65534) that is not already assigned to your network. The default value is 64512.

***Recommendation:*** *Choose the Border Gateway Protocol (BGP) type if your device supports it.*

## **Tunnel Configuration:**

* **Automatic:**No other inputs are required. This option automatically configures the tunnel settings for your Anypoint VPN. The tunnel settings are visible after VPN creation.
* **Custom:**If you need a custom configuration for a tunnel.
  + In the **PSK** (Pre-Shared key) field for each tunnel and point-to-point CIDR, enter a value between 8-64 characters that does not begin with zero (0). The CIDR block must be unique across all VPN connections.
* Once the VPN is created, we can download the VPN configuration, which can be then shared with network administrator to configure on data center VPN device

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

*Recommendation: Automatic*

**Note:** SSB VPN endpoint must initiate traffic to establish and maintain the connection because the Anypoint VPN endpoint acts only as a responder.

## **Limitations**

Anypoint VPN does not support these features and configurations:

* Network Address Translation (NAT)
* IPv6
* IKEv2 with policy-based VPNs
* Advertising a default route (0.0.0.0/0) over BGP or static routing

## **Recommendations**

* Adjust the maximum segment size of TCP packets entering the VPN tunnel.

VPN headers require additional space, which reduces the amount of space available for data.

To limit the impact of this behavior, configure your endpoint with TCP MSS Adjustment: 1387 bytes.

* Reset the DF flag on packets.

Packets might carry a Don’t Fragment (DF) flag, indicating that the packet must not be fragmented. Some VPN devices can override the DF flag and fragment packets unconditionally when required. If available, enable the setting Clear Don’t Fragment (DF) Bit