

# CiscoDNA – Bluecat Gateway Integration Guideline

## 1. Setup Bluecat Gateway.

Please refer the following document:

**bluecat\_gateway\_installation\_guide\_18.10.2.pdf**

Login **vpn.bluecatlabs.net** VPN and download cisco\_dna.tar.gz:

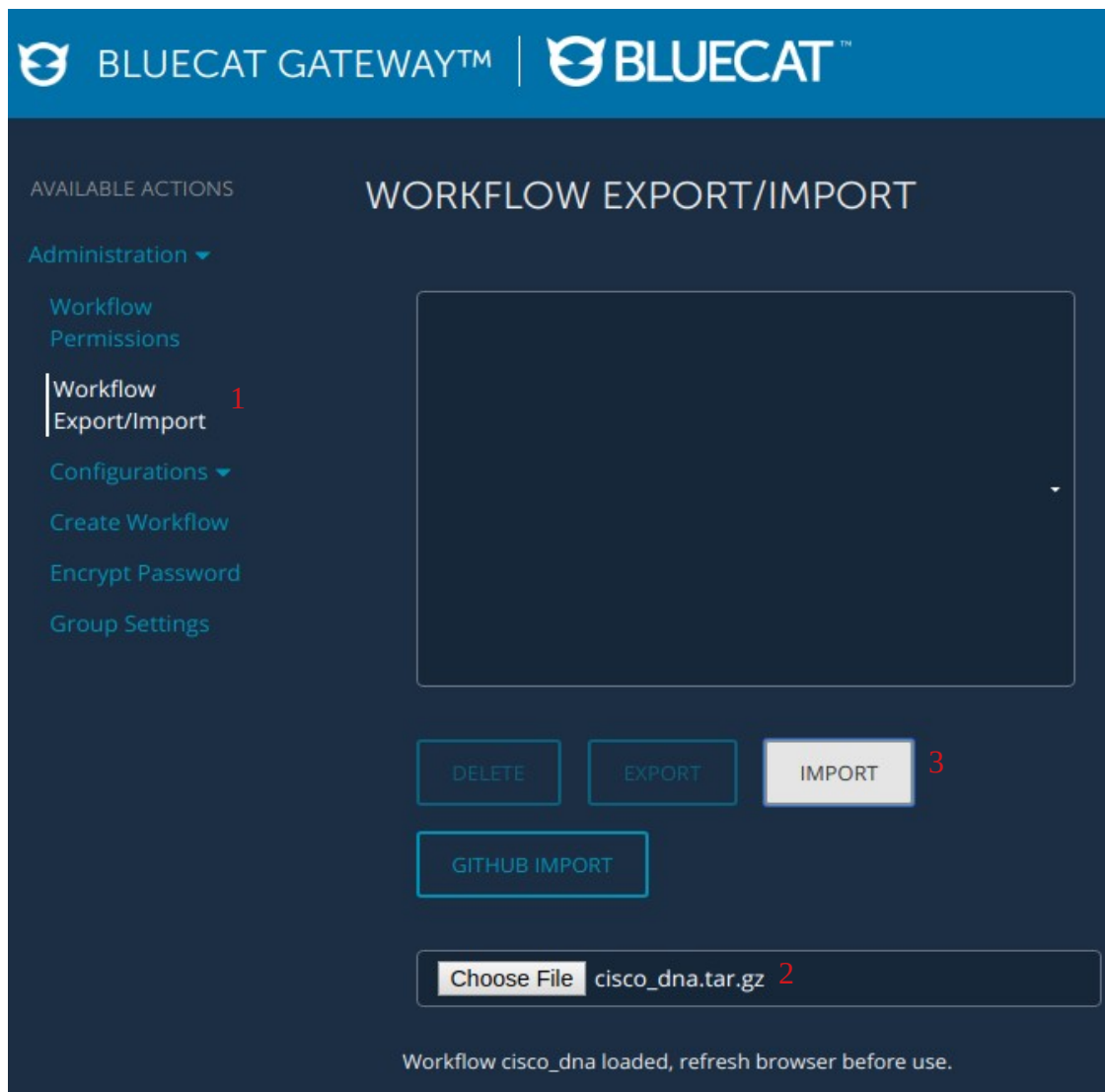
[http://10.245.0.162:8081/repository/bluecatnw/com/bluecatnw/cisco\\_dna/cisco\\_dna.tar.gz](http://10.245.0.162:8081/repository/bluecatnw/com/bluecatnw/cisco_dna/cisco_dna.tar.gz)

Precondition: the container must be installed lib contains in ipam\requirements.txt first. Below is command to install lib for container.

```
# sudo docker exec bluecat_gateway pip install netaddr --user
```

```
# sudo docker container restart bluecat_gateway
```

- Access bluecat-gateway address and login.
- Select Administration\Workflow Export/Import item
- Click browse file and choose cisco\_dna.tar.gz
- Click Import button.
- Restart bluecat\_gateway container



- f. Re-login gateway and select Administration\Workflow Permissions item
- g. Select ipam, then select ipam\_page, select all in New Group Name field, click ADD.

BLUECAT GATEWAY™

BLUECAT™

AVAILABLE ACTIONS

Administration ▾

Workflow Permissions 4

Workflow Export/Import

Configurations ▾

Create Workflow

Encrypt Password

Group Settings

WORKFLOW PERMISSIONS

Workflows:

Administration

admin

create\_workflow

encrypt\_password

Administration/Configurations

configs

cisco\_dna

ipam 5

Type: api

ipam\_page 6

Page title: Cisco\_DNA\_IPAM\_Interface

Description: Gateway workflow to be IPAM interface to integrate with Cisco DNA Centre

Endpoint: ipam/ipam\_endpoint

Group Name/UDF value:

all

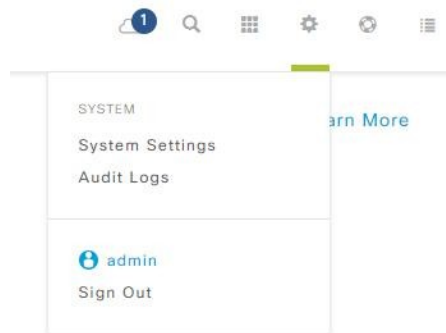
all 7

ADD 8

DELETE

Changes saved.

2. Setup CiscoDNA integrates BlueCat gateway
  - a. Access Cisco DNA Center address and login
  - b. Go to System Settings



- c. Select Settings tab and click IP Address Manager  
Select GENERIC provider and click to View select box to load view.

System 360 Software Updates **Settings** Data Platform Users Backup & Restore

Search

Authentication and Policy Servers

Certificate

Cisco Credentials

Debugging Logs

Device Controllability

Device EULA Acceptance

Integration Settings

Integrity Verification

**IP Address Manager**

Network Resync Interval

PKI Certificate Management

Proxy Certificate

Proxy Config

SFTP

SNMP Properties

Telemetry Collection

Trustpool

vManage Properties

### IP Address Manager

Use this form to set your IPAM server settings.

Server Name\* ?

your\_server\_name

Server Url\* ?

https:// or http:// <gateway\_address>

Username\* ?

nquochthai

Password\* ?

Provider\*

GENERIC

View\*

nquochthai

Apply Delete

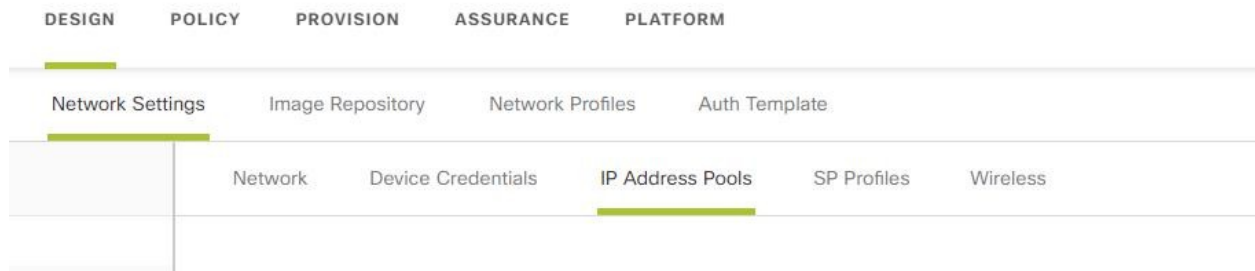
### 3. Using CiscoDNA UI.

#### a. Create pool.

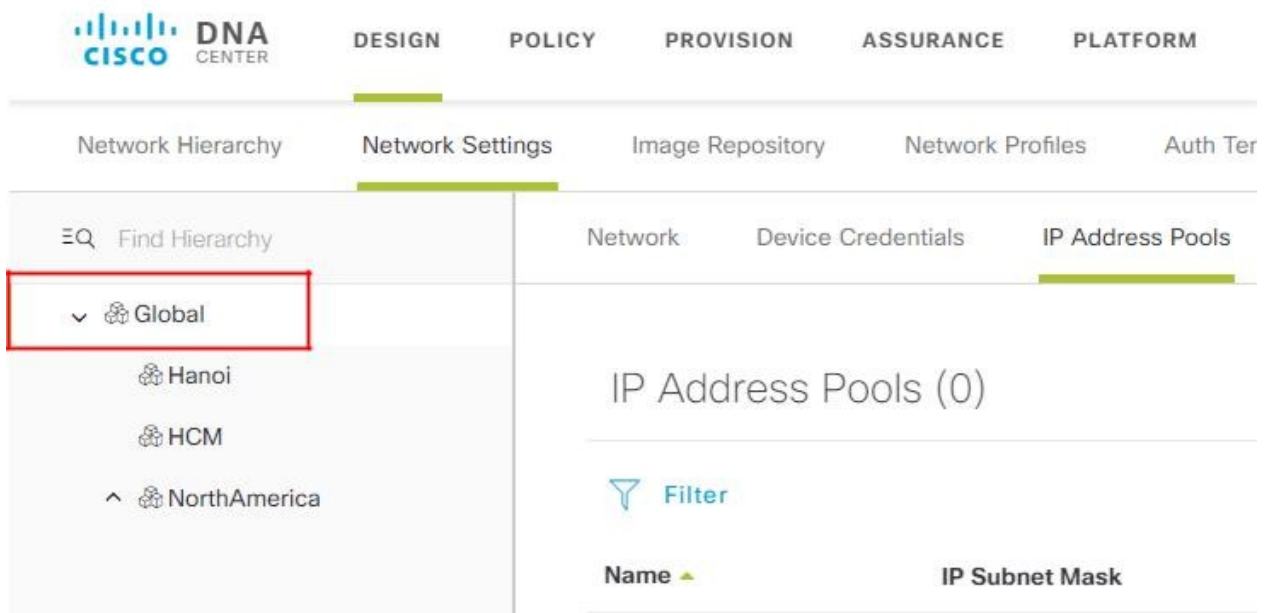
There are two ways to create pool.

# Using Import function to import existing pool in BAM

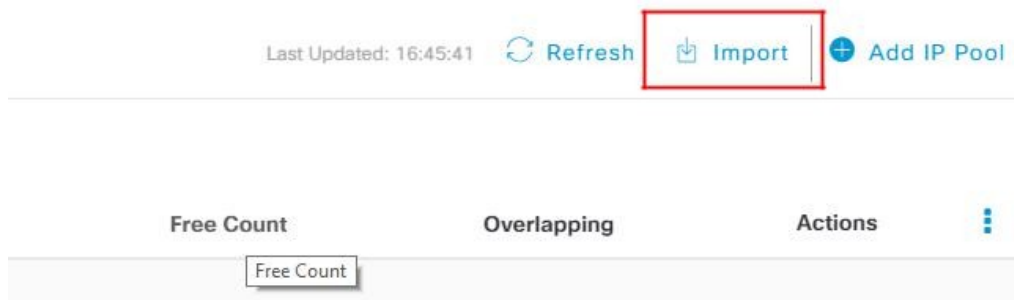
- Go to Design\Network Settings\IP Address Pools tab.



- Select Global node.



- Click Import icon.



- Import IP Pools window opened
- Input Cidr and click Retrieve button.
- Select pools that want to import then click Import

Import IP Pools

×

---

CIDR

16.0.0.0/8

Retrieve

*Note: Enter a CIDR and click on Retrieve to get the list of IP Pools available to import from GENERIC.*

☐

Select All

---

☒

16.0.0.0/20

---

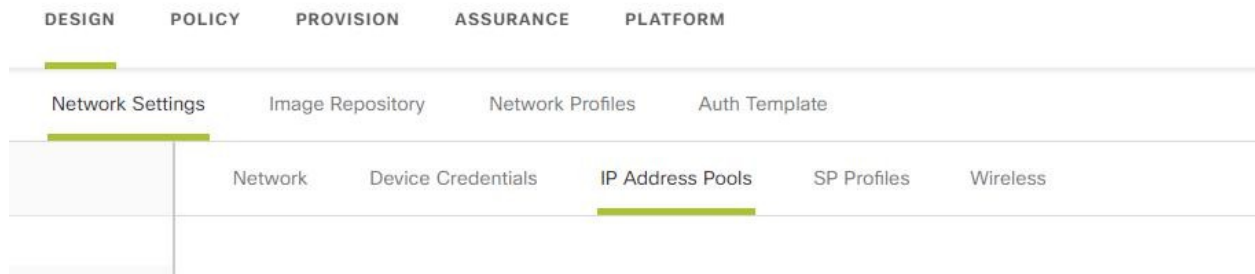
Showing 1 of 1

Cancel

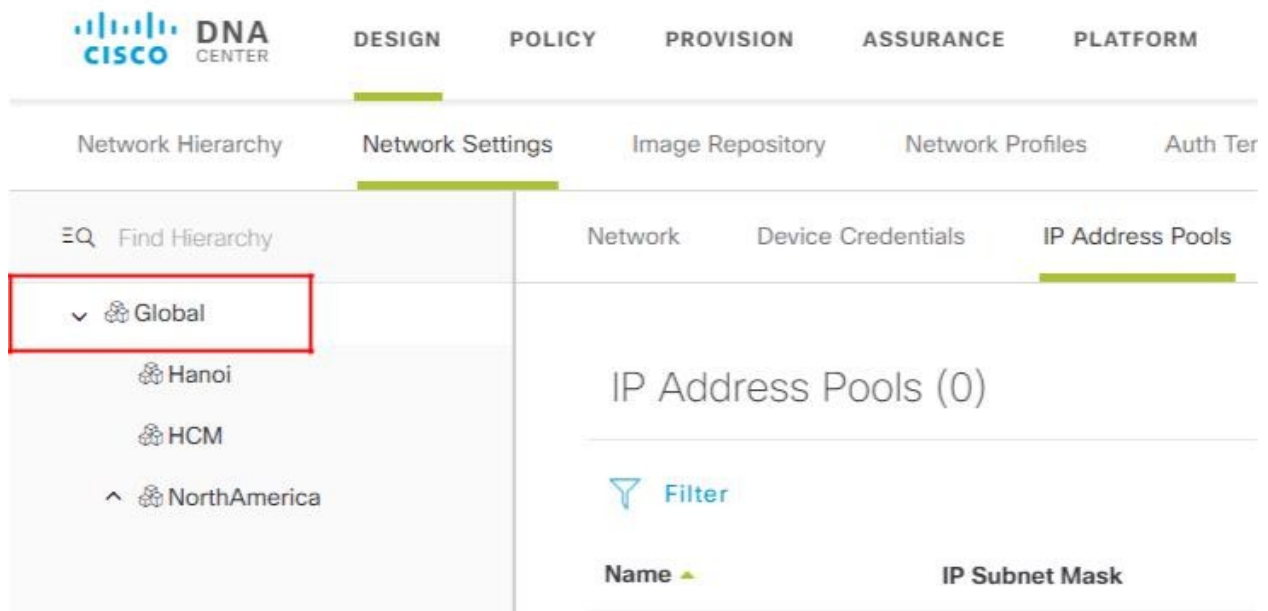
Import

# Using Add IP Pool function to create new pool

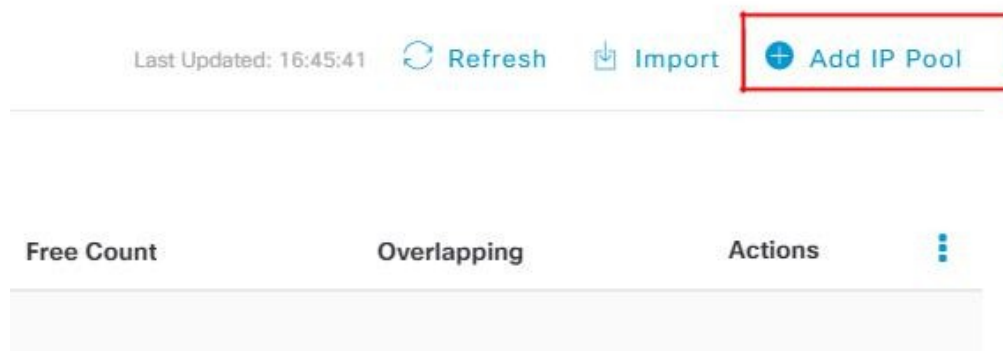
- Go to Design\Network Settings\IP Address Pools tab.



- Select Global node



- Click Add IP Pool icon



- Input IP Pool Name, IP Subnet, CIDR Prefix, Gateway IP Address.
- Select DHCP server, DNS server if any.
- Click Save button.

Add IP Pool

×

IP Pool Name \*

create\_pool\_testing

IP Subnet \*

10.0.0.0

CIDR Prefix

/8 (255.0.0.0) ▼

Gateway IP Address \*

10.0.0.1|

DHCP Server(s) ▼

DNS Server(s) ▼

☐ Overlapping

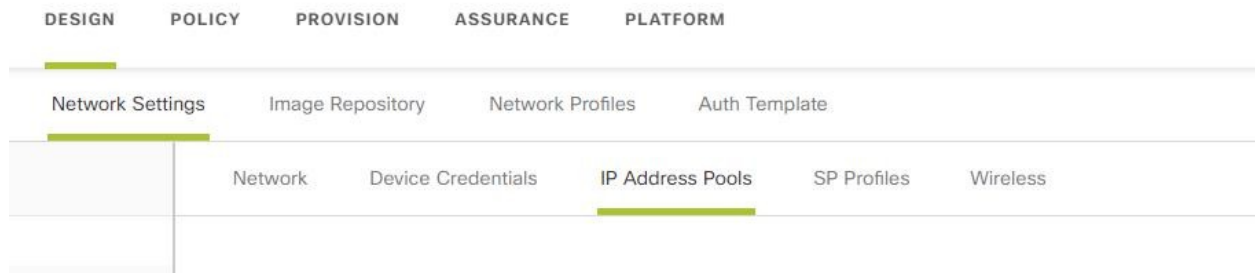
Cancel

Save

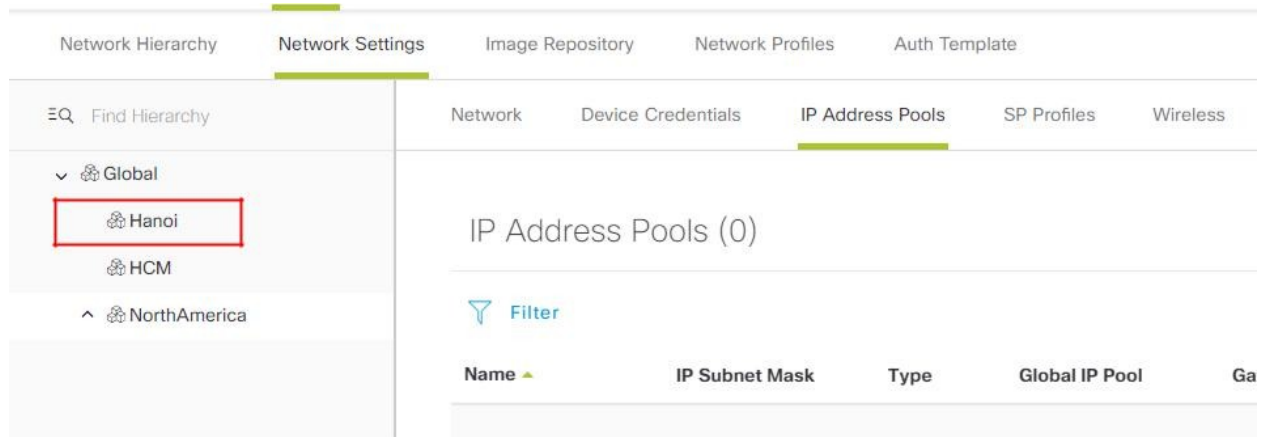
b. Create Sub-pool

Precondition: Global pool had been created.

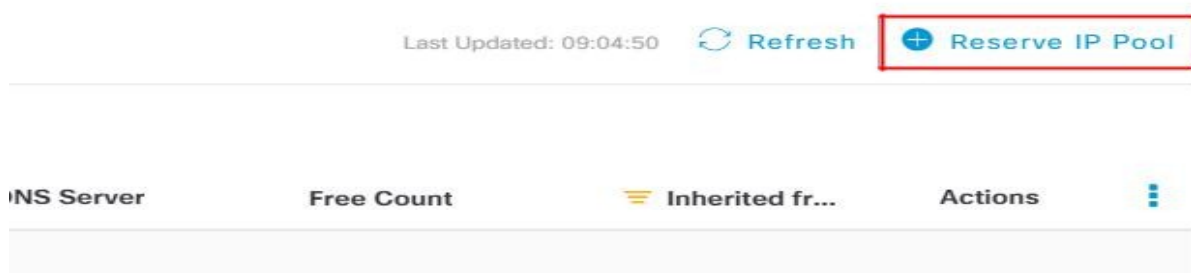
- Go to Design\Network Settings\IP Address Pools tab.



- Select sub node under Global. If not then create.



- Click Reserve IP Pool icon





- Input IP Pool Name
- Select Type is Generic
- Select Global IP Pool
- Input IP Subnet, CIDR Prefix
- Input Gateway if any.
- Select DHCP server, DNS server if any.
- Click Reserve button.

Reserve IP Pool

IP Pool Name \*

sub\_pool

Type

Generic

Global IP Pool \*

16.0.0.0\_20 (16.0.0.0/20)

CIDR Notation / No. of IP Addresses \*

16.0.0.0

/24 (255.255.255.0)

OR

No. of IP Addresses

Gateway IP Address

16.0.0.2

DHCP Server(s)

DNS Server(s)

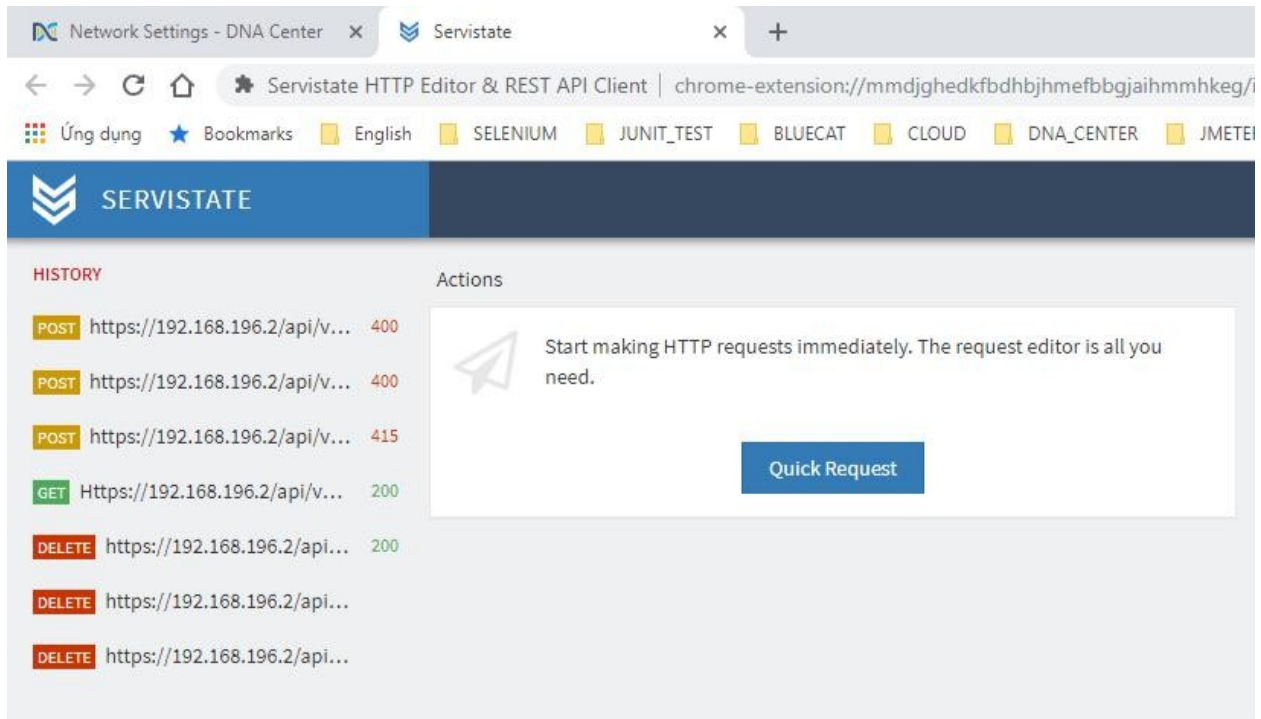
☐ Overlapping

Cancel

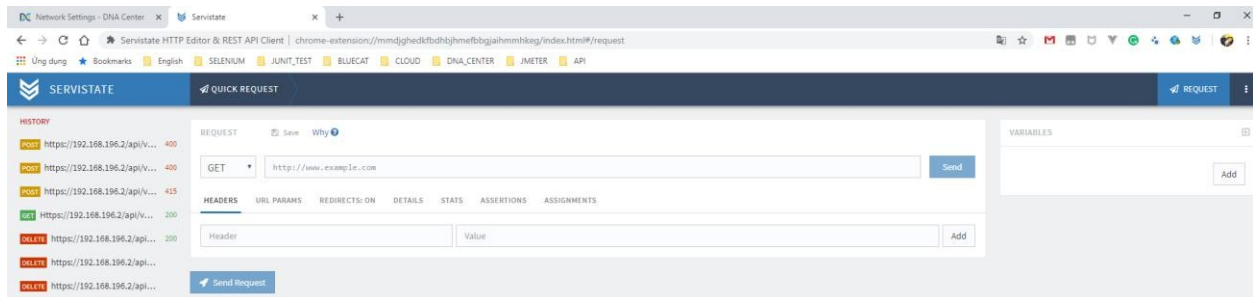
Reserve

### c. Assign IP Address

- Precondition: Client plugin was installed. The suggested plugin is Servistate HTTP Editor and REST API Client
- Login to DNAC and open plugin in another tab



- Click Quick Request button to open GUI



- Get pool\_id by send Get quest like below:  
[https://<DNAC address>/api/v2/ippool?ipPoolName=<pool\\_name>](https://<DNAC address>/api/v2/ippool?ipPoolName=<pool_name>)

The screenshot displays the Servistate HTTP Editor & REST API Client interface. The top section shows a 'QUICK REQUEST' tab with a 'GET' method and the URL 'https://192.168.196.2/api/v2/ippool?ipPoolName=17.0.0.0\_10'. Below this, the 'HEADERS' tab is active, showing a table with 'Header' and 'Value' columns. A 'Send Request' button is visible. The 'RESPONSE' section shows a status of '200 OK' with a body size of 463 B and a response time of 203 ms. The 'BODY' tab is active, displaying the response in 'FORMATTED' view. The JSON response is as follows:

```
1 {
2   "response": [
3     {
4       "ipPoolName": "17.0.0.0_10",
5       "dhcpServerIps": [],
6       "gateways": [],
7       "createTime": 1547810774723,
8       "lastUpdateTime": 1547810791329,
9       "totalIpAddressCount": 4194304,
10      "usedIpAddressCount": 1048576,
11      "parentUuid": "root",
12      "owner": "ipam",
13      "shared": true,
14      "overlapping": false,
15      "configureExternalDhcp": false,
16      "usedPercentage": 0,
17      "clientOptions": {},
18      "dnsServerIps": [],
19      "context": [],
20      "ipv6": false,
21      "id": "6fb77d93-d25a-4cca-8538-1861723735ba",
22      "ipPoolId": "17.0.0.0/10"
23    }
24  ],
25  "version": "1.0"
26 }
```

The 'id' field in the response is highlighted with a red box.

- Send Post request:

<https://<DNAC address> /api/v1/maintenance/assignip/<poolid>>

Below is the payload:

```
{  
  "owner": "DNAC",  
  "numberOfAddresses": 2  
}
```

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** `https://103.166.196.2/api/v1/maintenance/assignip/1001001-0730-4000-0000-000000000000`
- Headers:** One header is defined: `Content-Type: application/json`.
- Form Data:** The payload is shown in JSON format:

```
{  
  "owner": "DNAC",  
  "numberOfAddresses": 2  
}
```
- Buttons:** "Send" and "Send Request" buttons are visible.

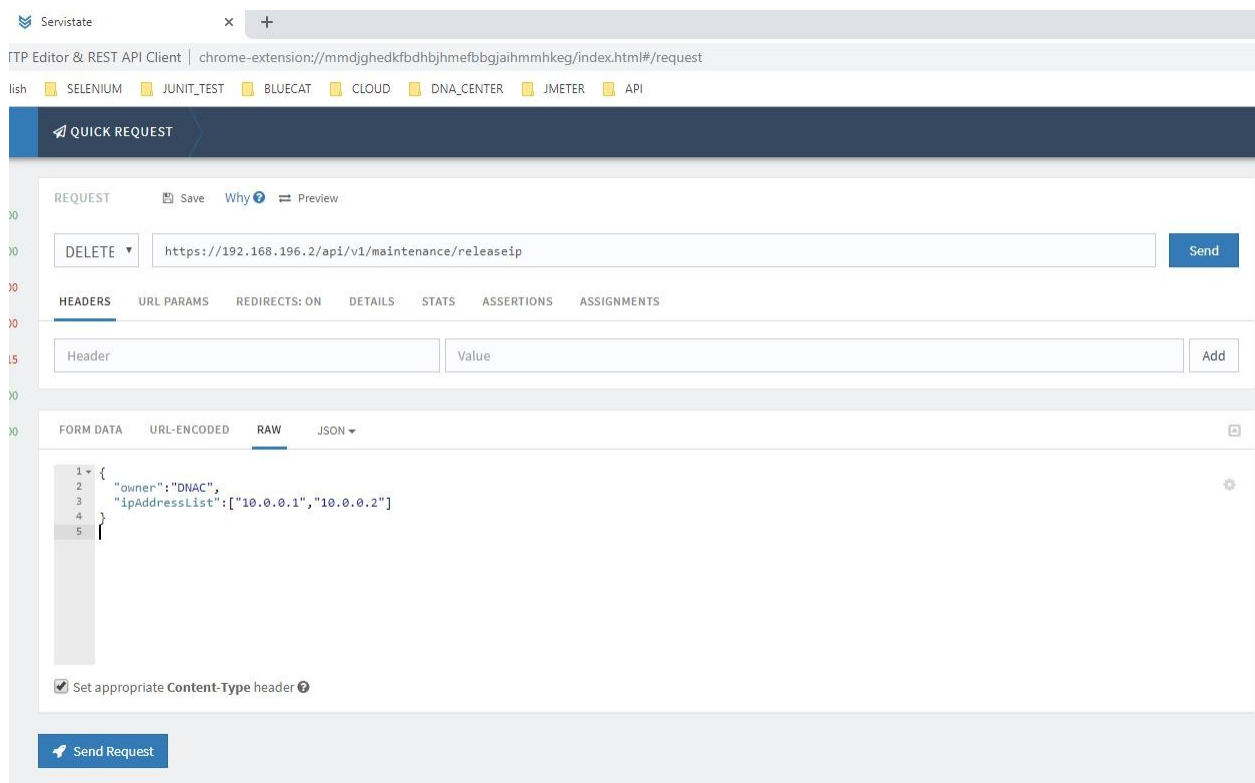
#### d. Release IP Address

- Precondition: Rest Client plugin was installed
- Open Rest Client
- Send Delete request

<https://<DNAC address>/api/v1/maintenance/releaseip>

Below is the payload

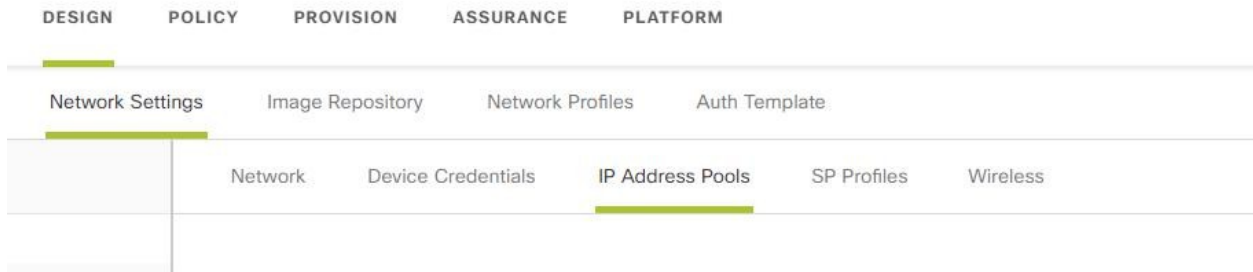
```
{  
  "owner": "DNAC",  
  "ipAddressList": [ "10.0.0.0 ", "10.0.0.01"]  
}
```



e. Release Sub-pool

Precondition: All IP addresses under sub-pool must be released first

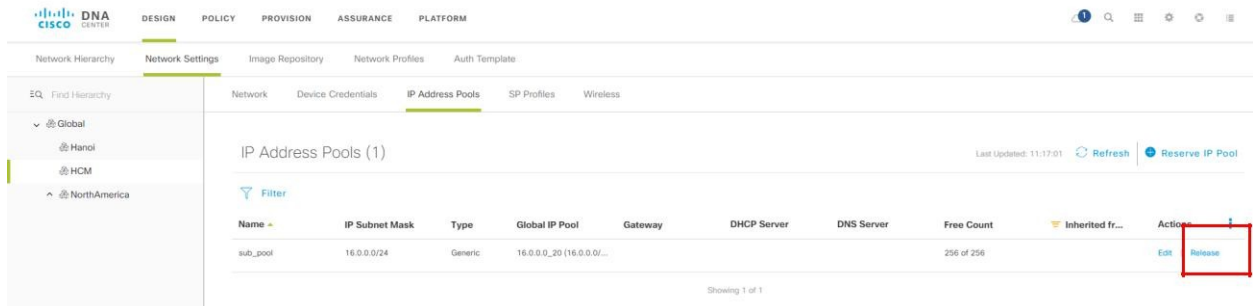
- Go to Design\Network Settings\IP Address Pools tab.



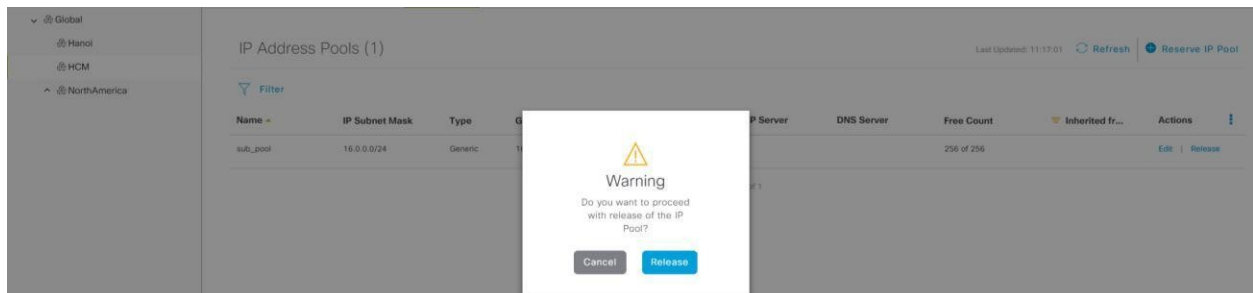
- Select sub node under Global.



- Click Release icon on row contains sub-pool want to be released



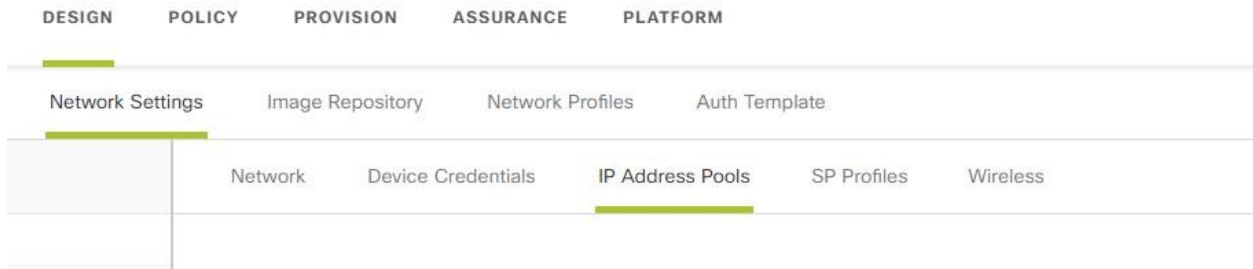
- Click Release button on Confirm popup.



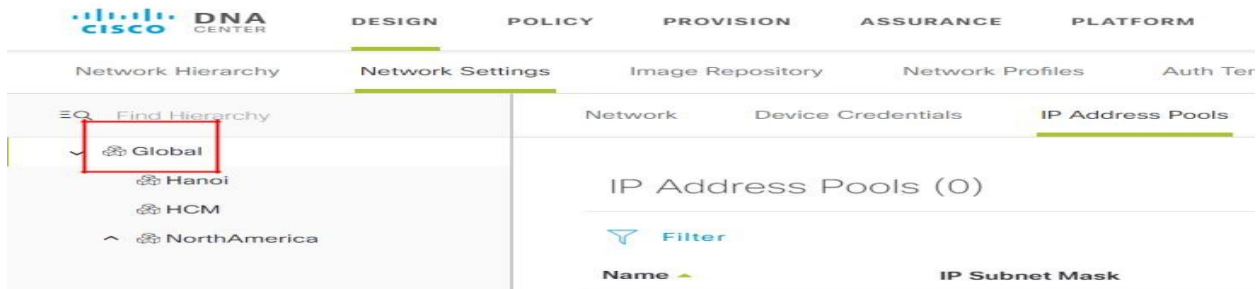
## f. Release Pool

Precondition: All sub-pool under Global must be released first.

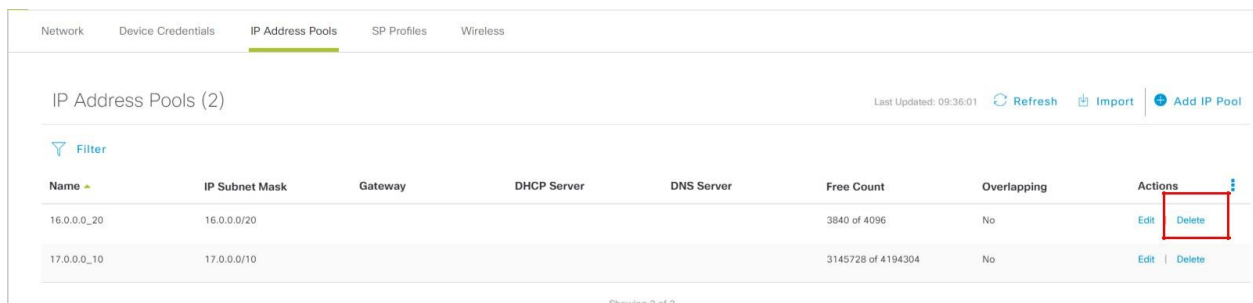
- Go to Design\Network Settings\IP Address Pools tab.



- Select Global.



- Click Delete icon on row contains pool to be deleted



- Click Delete button on Confirm popup.

