**new_att_logo**

AT&T

User Manual for NPB controller (MVP version)

Version 1.0

Jan 21, 2022

AT&T Labs, Network Operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vendor Contributor** | **Lab Contributor** | **ATS Contributor** | **OPS Contributor** | **TP&E Contributor** |

User Manual for

NPB- Controller (NPBC)

**Contents**

[**Document History** 4](#_Toc94776808)

[Introduction 5](#_Toc94776809)

[**Scenarios of User Interaction** 5](#_Toc94776810)

[1) Fetch Authorization Token 5](#_Toc94776811)

[2) Check if token is valid or not: 6](#_Toc94776812)

[3) Renew the token if validity expired: 6](#_Toc94776813)

[4) Creating IMSI whitelist: 6](#_Toc94776814)

[5) Adding new IMSI to the whitelist: 7](#_Toc94776815)

[6) Check whether added IMSI details were send to Session Manager: 8](#_Toc94776816)

[7) Removing specific IMSI entries from whitelist: 8](#_Toc94776817)

[8) Verifying if specific IMSI already exists in any whitelist: 9](#_Toc94776818)

[9) Removing complete whitelist: 9](#_Toc94776819)

[10) Verify all the IPs allocated for a particular IMSI in a whitelist: 10](#_Toc94776820)

[11) Verify whether IP is allocated or not for a particular IMSI: 10](#_Toc94776821)

[**Alarms from Configuration Manager** 11](#_Toc94776822)

# **Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Issue Date** | **Author(s)** | **Identification of Changes** |
| 1.0 | 21/01/2022 | Wipro | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

This document outlines the different ways of user interaction of the MVP version of NPB-Controller. Most of the user interactions are handled by FilterManagerment Micro service running in CM. There is no GUI support in MVP version. All are CLI interactions based on REST API calls.

Assumptions:

1. System hostname is assumed to be **zrdm60bcsmr01cmr001.eng.mobilephone.net** for the description in this manual. It has to be updated with the actual hostname for query

# **Scenarios of User Interaction**

# Fetch Authorization Token

To access the resource, user needs to be authenticated first through LDAP mechanism. By running the below curl command, we can create the token upon successful authentication. If the authentication details were wrong, then we get the 401 UNAUTHORIZED status.

**Command Syntax-**

**curl -vvv -k -X POST 'https://zrdm60bcsmr01cmr001.eng.mobilephone.net:9080/npbc/auth-server' \**

**--header 'Content-Type: application/json' \**

**--data-raw '{**

**"userName":"sc423s",**

**"password":"S4nt14g0."**

**}'**

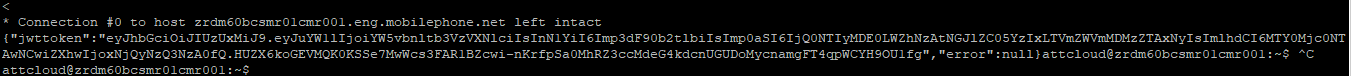
**Result-**

Token is generated successfully which can be used along with subsequent queries.

Token is valid for 45 minutes.

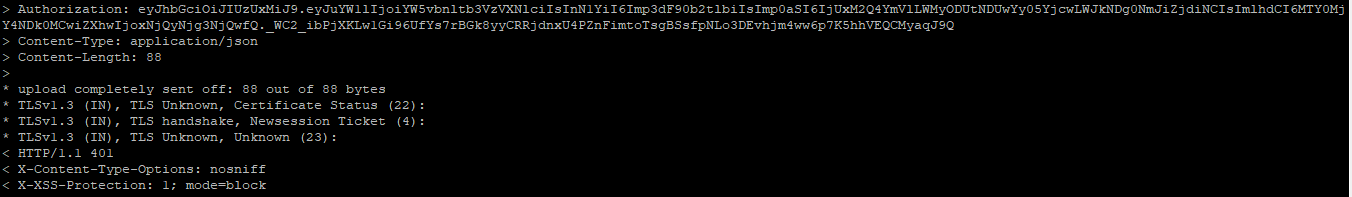
That token can be used in the Authorization header of other API’s.

**Sample Screenshot:**

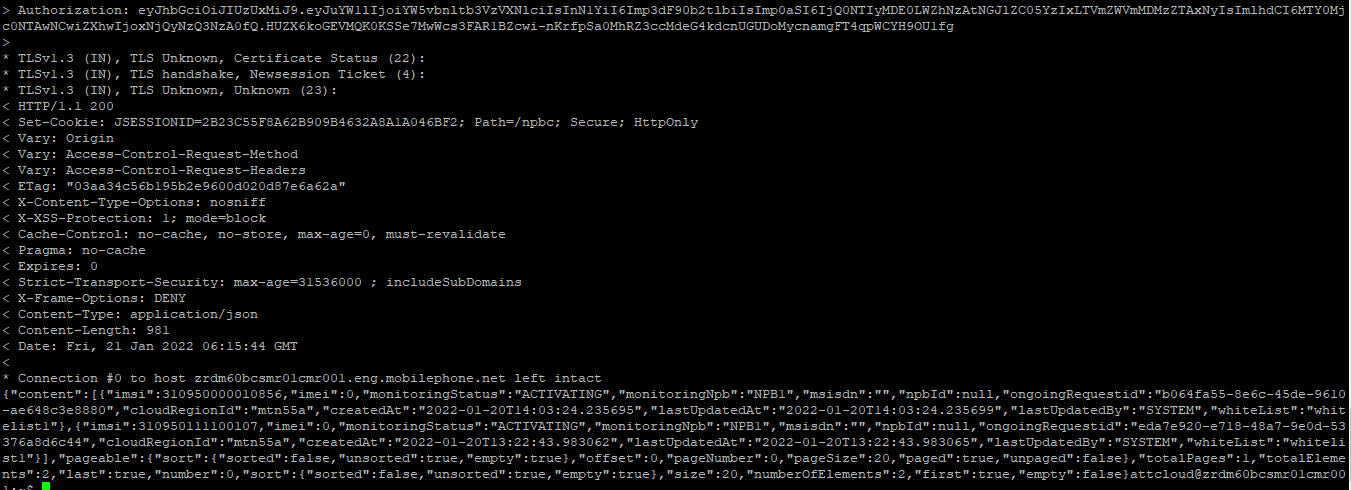


# Check if token is valid or not:

Once a Token is generated, all further API requests have to use this Token only. If the token is invalid or expired, 401 UNAUTHORIZED error status will be returned.



If the token is valid, then API result will be as shown below.



# Renew the token if validity expired:

If the token validity is expired, then step1 process has to be performed for new Token generation.

# Creating IMSI whitelist:

To create the Whitelist, WHITELISTS POST request by using below curl command has to be issued. Place the token, whitelist name and description in the command.

**curl -vvv -k -X POST "https://zrdm60bcsmr01cmr001.eng.mobilephone.net:9080/npbc/config/v1/whitelists" \**

**--header "Authorization: token needs to be placed here" \**

**--header "Content-Type: application/json" \**

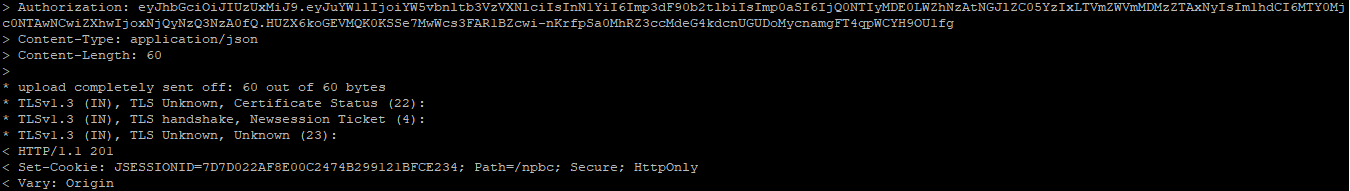
**--data-raw '{**

**"name": "whitelist2",**

**"description" : "testing for imsi"**

**}'**

After running this command, status code 201 indicates Whitelist is added.



# Adding new IMSI to the whitelist:

For adding new IMSI to whitelist, below command has to be used.

In URL place the whitelist name that you want to add the IMSI’s, and in additions section place the iMIS’s that you want to add. Likewise Deletions also

**curl -vvv -k -X PUT "https://zrdm60bcsmr01cmr001.eng.mobilephone.net:9080/npbc/config/v1/whitelists/whitelist1" \**

**--header "Authorization: place the token here" \**

**--header "Content-Type: application/json" \**

**--data-raw '{**

**"identifier": "IMSI",**

**"additions": [**

**{"imsi":"310950000010001"},**

**{"imsi":"310950000010002"}**

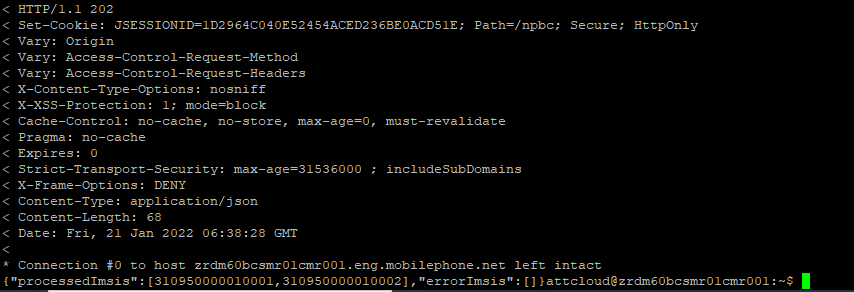
**],**

**"deletions": [**

**]**

**} '**

If it successfully added, then you will get below result. Whatever the iMIS’s are added that will show in **processedImsis** list.



# 6) Check whether added IMSI details were send to Session Manager:

Event Processing Micro service will send added IMSI’s details to the **SESSION MANAGER** using Kafka broadcast message. To ensure this service has sent these details to the SESSION MANAGER or not we can check in below command.

**/home/attcloud/kafka\_2.13-2.7.0/bin/kafka-console-consumer.sh --bootstrap-server localhost:9092 --topic npbcwhitelist --from-beginning**

Here **npbcwhitelist** is the Kafka topic name. This command will print all the broadcast messages received by the topic.

# 7) Removing specific IMSI entries from whitelist:

To remove specific IMSI from whitelist need to run the below curl command and place the whitelist name, token and IMSI’s.

**curl -vvv -k -X PUT "https://zrdm60bcsmr01cmr001.eng.mobilephone.net:9080/npbc/config/v1/whitelists/whitelist1" \**

**--header "Authorization: token needs to be place here " \**

**--header "Content-Type: application/json" \**

**--data-raw '{**

**"identifier": "IMSI",**

**"additions": [**

**],**

**"deletions": [**

**{"imsi":"310950000010001"},**

**{"imsi":"310950000010002"}**

**]**

**} '**

# Verifying if specific IMSI already exists in any whitelist:

To verify the specific IMSI is already exists in any whitelist we need to check the database table details. To connect to the DB follow these commands:

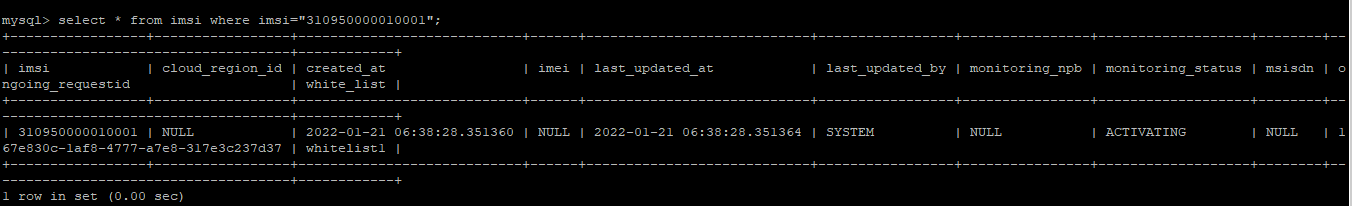
**mysql -u npbc\_configdb -p**

enter the password **Config@123**

**use npbc\_configdb**

after run the select query like **select \* from imsi where imsi=”310950000010001”;**

and check whether it returns the record or not. if the record is there you can check for the white\_list field.

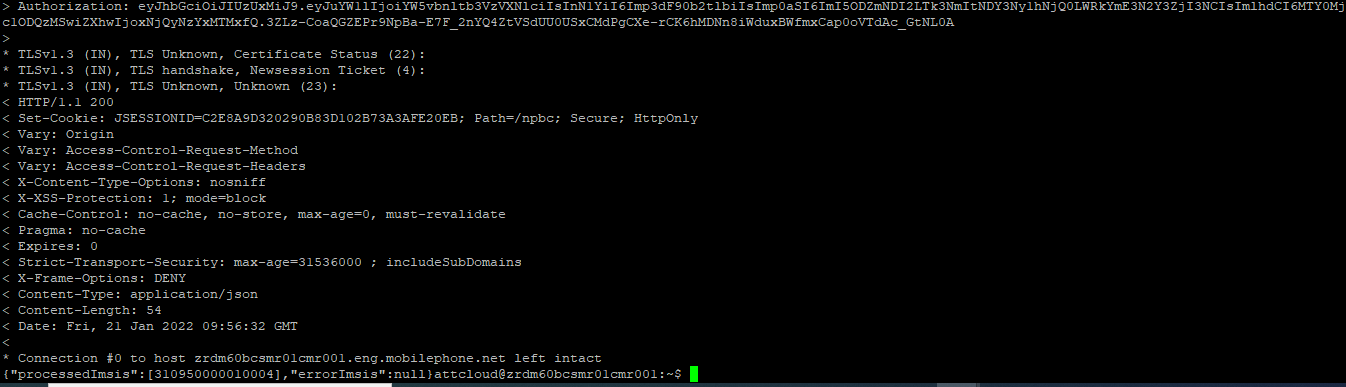


# Removing complete whitelist:

To remove the complete whitelist, we need to call the imsistatusupdate API. It will remove the whitelist and IMSI’s that are related to the whitelist name.

**curl -vvv -k -X PUT "https://zrdm60bcsmr01cmr001.eng.mobilephone.net:9080/npbc/config/v1/imsistatusupdate/whitelist3?status=false" \**

**--header "Authorization: token" \**

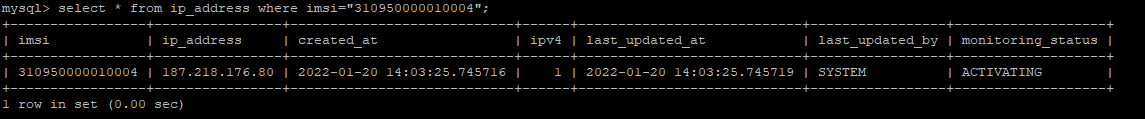


We will get the IMSI’s that are removed in processedImis as shown in image above.

# Verify all the IPs allocated for a particular IMSI in a whitelist:

To check for all the Ips that are allocated for a particular IMSI. We need to run the following sql command. Replace the IMSI.

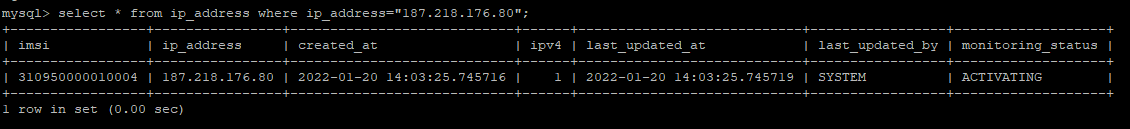
**select \* from ip\_address where imsi="310950000010004";**



# Verify whether IP is allocated or not for a particular IMSI:

To check for whether IP is allocated for a particular IMSI. We need to run the below sql command. Replace the IP address.

**select \* from ip\_address where ip\_address="187.218.176.80";**



# **Alarms from Configuration Manager**

|  |  |  |  |
| --- | --- | --- | --- |
| **Alarm**  **(Part of alarm description)** | **Service reporting the alarm** | **Fault Scenario** | **Syslog Message (Sample)** |
| NPB\_CONFIG\_DB\_DOWN | Filter Mgmt Service | DB is down | Oct 07 14:59:22 zrdm60bcsmr01cmr001 java[103593]:  1633618762 {​​​​ERROR}​​​​​​​​​​​  {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-10-07T14:59:22.593630], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: filtermgmt:: couldn't communicate with DB |
| NPB\_PROGRAMMING\_SERVER\_DOWN | Filter Mgmt Service | NPB Programming Service is down | Oct 07 14:59:22 zrdm60bcsmr01cmr001 java[103593]:  1633618762 {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ERROR}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​  {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-10-07T14:59:22.593630], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: filtermgmt:: failed to communicate with NPB Programming |
| NPB\_CONFIG\_DB\_DOWN | Event Processing Service | DB is down | Oct 07 15:13:32 zrdm60bcsmr01cmr001 java[104782]:  1633619612 {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ERROR}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​  {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-10-07T15:13:32.693110], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: EventProcessingService:: couldn't communicate with DB |
| NPB\_PROGRAMMING\_SERVER\_DOWN | Event Processing Service | NPB Programming Service is down | Oct 07 15:13:32 zrdm60bcsmr01cmr001 java[104782]:  1633619612 {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ERROR}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​  {​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-10-07T15:13:32.693110], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: EventProcessingService:: couldn't communicate with NPB Programming Service |
| NPB\_CONFIG\_DB\_DOWN | NPB Programming Service | DB is down | {​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-11-12T17:49:46.191657700], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: NPB Prog Service:: NPB\_CONFIG\_DB\_DOWN, alarmText: Npb Prog Service:: couldn't communicate with DB |
| NPB\_CONFIG\_PINC\_IF\_DOWN | NPB Programming Service | PINC is down | {​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-11-12T17:49:46.191657700], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL, nature: NON CLEARABLE, alarmDescription: NPB Prog Service::NPB\_CONFIG\_PINC\_IF\_DOWN, alarmText: Npb Prog Service:: couldn't communicate with pinc |
| ​​​​​​​NPB\_FieldSet | NPB Programming Service | Field set not matched | {​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​ timeStamp: [2021-12-14T15:54:29.594475], specificProblems: Field set not matched expecting ipv4 or ipv6,  eventType: Processed FS, probableCause: Wrong Field set is received,  perceivedSeverity: LOW, nature: NON CLEARABLE, alarmDescription: NPB Prog Service::FIELDSET\_NOT\_MATCHED, alarmText: Field set not matched |
| ​​​​​​​Retry | NPB Programming Service | Retry | <1> 255 2021-12-14T16:46:24,837 {​​​​​​​​​FAULT}​​​​​​​​​ timeStamp: [2021-12-14T16:46:24.837281100], specificProblems: Retrying current request, eventType: request is retrying, probableCause: Response is not valid or null, perceivedSeverity: LOW,  nature: NON CLEARABLE, alarmDescription: NPB Prog Service::NPB\_CONFIG\_PINC\_IF\_DOWN, alarmText: received response is null or not valid |
| ​NPB\_CONFIG\_IDAM\_IF\_DOWN | Filter Mgmt Service | IDP is down | {​​​​​​​​​​​​​​​​​​​​​​​​​​​FAULT}​​​​​​​​​​​​​​​​​​​​​​​​​​​ timeStamp: [2021-10-28T12:02:21.943592800], specificProblems: Communications protocol error, eventType:  processing error, probableCause: Communications protocol error, perceivedSeverity: CRITICAL,  nature: NON CLEARABLE, alarmDescription: filtermgmt:: NPB\_CONFIG\_IDAM\_IF\_DOWN,  alarmText: filtermgmt:: failed to communicate with IDP |
| ​​​​​​​ NPB\_CONFIG\_EB\_DOWN | Event Processing Service | Kafka broker is down |  |