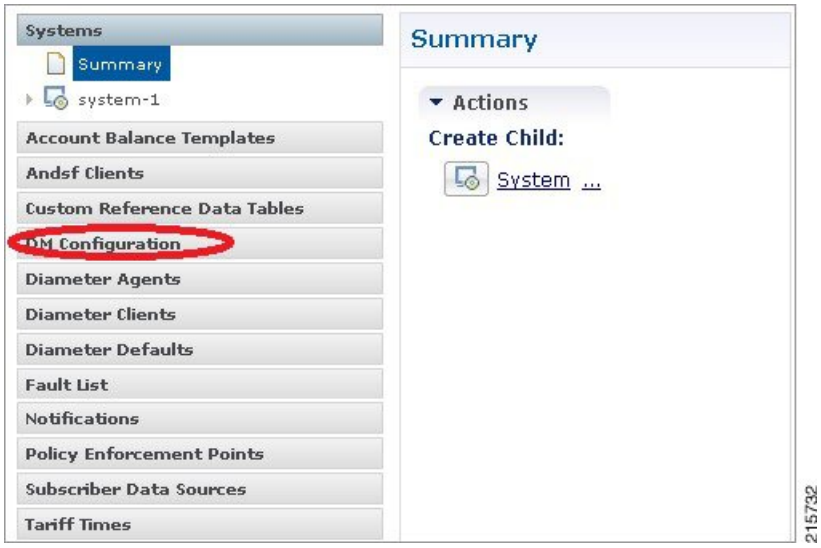
Troubleshooting ANDSF

Policy Builder Scenarios

Not Able to See DM Configuration Tab in Policy Builder after Installation

Figure 1: DM Configuration Tab



Step 1 Execute **list_installed_features.sh** script from Cluster Manager to verify whether the ANDSF feature (**com.broadhop.client.feature.andsf**) is enabled or not.

```
list_installed_features.sh
```

Step 2 In case the above feature (**com.broadhop.client.feature.andsf**) is missing, edit the `/etc/broadhop/pb/features` file from Cluster Manager VM and add the following lines:

com.broadhop.client.feature.andsf

com.broadhop.andsf.service.feature

Step 3 After modifying the feature files, execute the following commands from Cluster Manager:

/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh

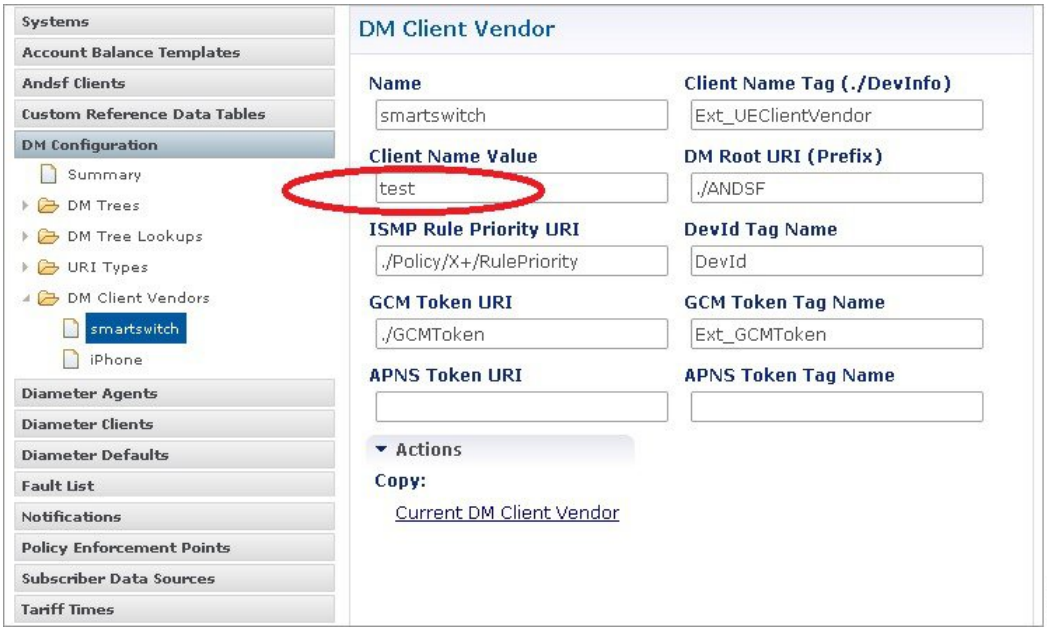
Note If the DM configuration does not show up then do a **restartall.sh** at the end.

Caution Executing `restartall.sh` will cause messages to be dropped.

Diagnostic.sh throws Errors after Restart

Check Client Name Value is not blank as shown in the following figure:

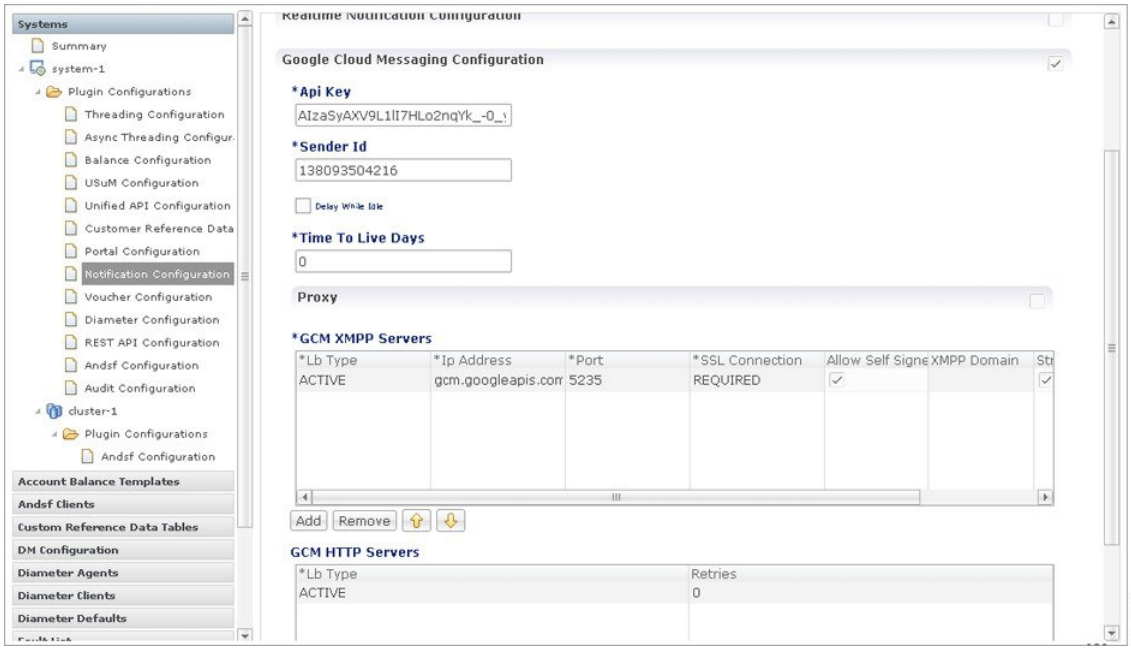
Figure 2: DM Client Vendor



Not Getting GCM Notifications in Logs

Verify the GCM tokens are configured in Policy Builder as shown in the following figure:

Figure 3: Notification Configuration



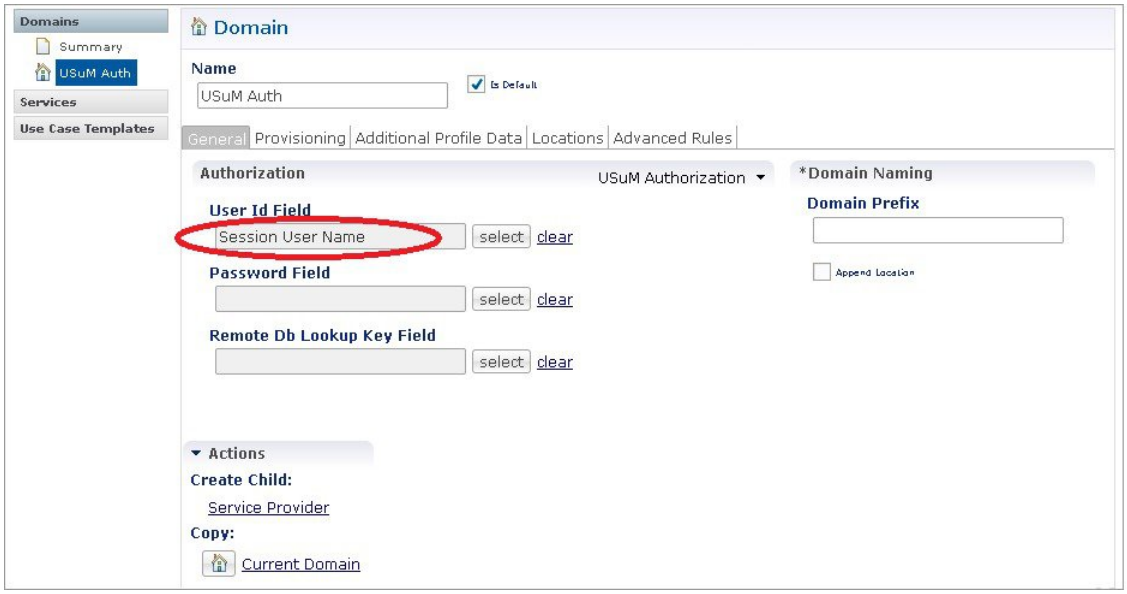
Session is not created for iPhone and Android Users

Step 1 Go to **Services** > **Domains** in Policy Builder.

Step 2 Under **Domains**, select **USum Auth**.

Step 3 On right hand side, in the **General** tab, under **Authorization** tab, check that the **User Id Field** value is set to **Session User Name** for both Android and Apple clients.

Figure 4: USum Auth



Check for service Use Case Templates for GCM, APNS, General, and default Services

Step 1 Go to **Services** tab in Policy Builder and click on **Use Case Templates**.

Step 2 Check that the use case template is there for the service being attached to a particular subscriber.

There should be two use case templates for a general ANDSF service and one more use case template for GCM/APNS notification if you have attached notification service to the subscriber.

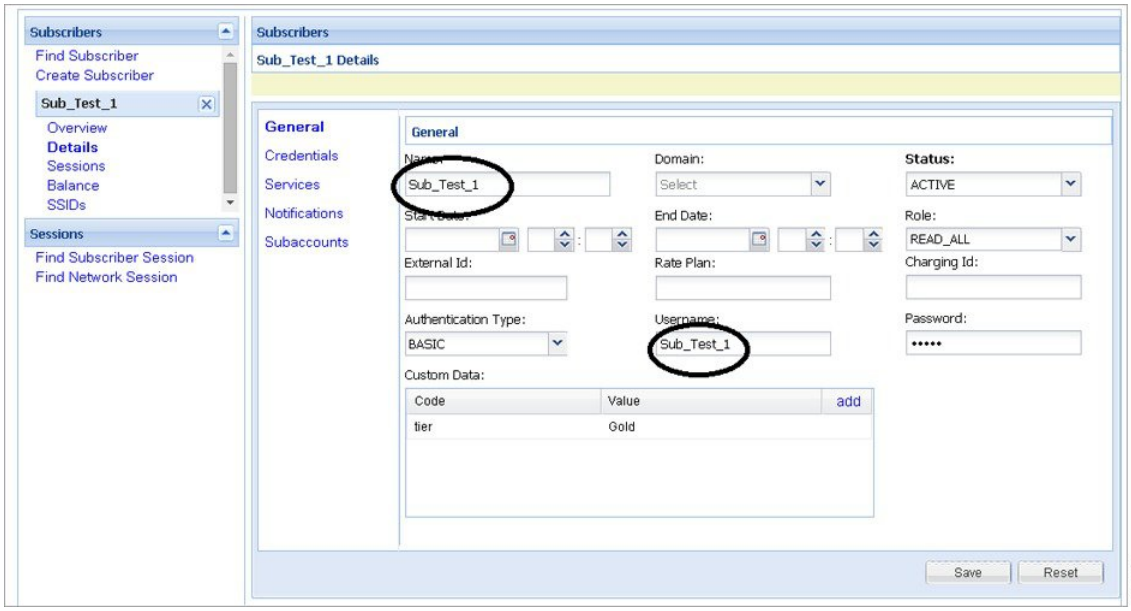
Step 3 If the templates are not there, see the *CPS ANDSF Configuration Guide* to create Use case Templates for the above services.

Control Center Scenarios

Subscriber Session not getting Created and Getting Exception Error (401)

- Make sure username and name should be same and unique.
- In case of Android, username will be IMSI.
- In case of iPhone, username will be MSISDN.

Figure 5: Subscribers



SSID Credentials are Wrongly Passed in Policy

Step 1 Go to Subscriber section in Control Center.

Step 2 Click on **SSID** section.

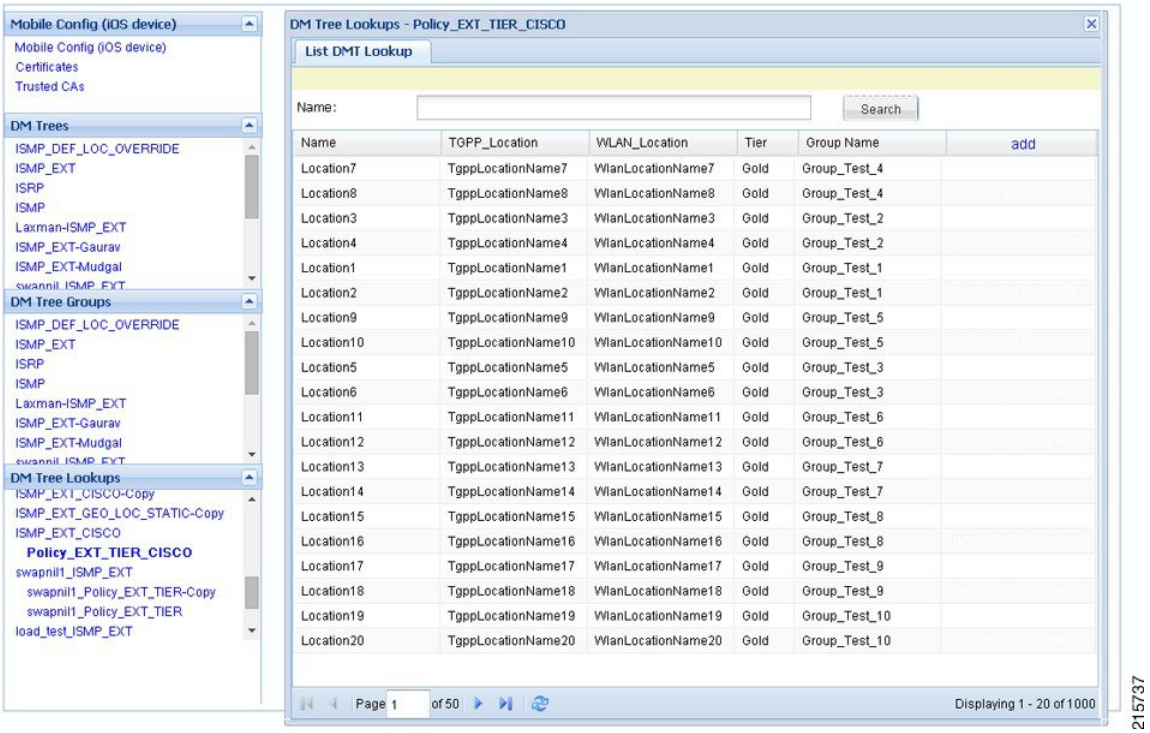
Step 3 Check the subscriber credentials are populated for specific SSIDs.

Step 4 Verify all the above three steps for all the subscribers.

DM Tree Lookups Fail and Exception in consolidated-qns.log

Step 1 Make sure CRD mapping is done properly in DM lookup.

Figure 6: DM Tree Lookups



Step 2 Check the CRD entries in DM tree lookup table.

Step 3 Check whether the CRD tables (for example, check in configuration section) exists and have entries defined in the lookup table.

Data Populated in MongoDB ANDSF Collection, but values are not shown in Control Center

Step 1 Go to all the policy server (QNS) nodes.

Step 2 Edit the following `qns.conf` file at `/etc/broadhop/`.

Step 3 Add the following parameter in the `qns.conf` file.

```
-Dandsf.mongo.thread.maxWaitTime=10000
```

Step 4 Execute `restart.sh` from Cluster Manager VM.

Not able to see the Mobile Configuration Certificate sub screen in Control Center

Step 1 Check if the screen is hidden behind the mobile configuration main screen.

Step 2 Close all the screens and re-open the mobile configuration screen.

If the certificate screen is not visible, you may need to close the Control Center and Mobile Configuration screens and reopen them again to make it visible.

Control Center session timeout frequently and not able to login from another browser

Step 1 Increase the number of sessions limit which will allow to create more sessions.

Step 2 Edit the `qns.conf` file and add the following parameter:

```
-Dcc.user.session.limit=5000
```

Geo-location is not read Properly in Control Center

Step 1 Go to **Configuration** tab in Control Center.

Step 2 Click on the **Geo-location** table and verify the format.

Latitude and Longitude value should be in degrees.

For example:

Longitude: 36.0044

Latitude: -68.9956

Radius: 100

ANDSF Server Scenarios

API Error Codes

The following table provides the information related to API Error Codes:

Table 1: API Error Codes

Error Code	Scenario
400 Bad request	The requested command could not be performed because of malformed syntax in the command. The malformed command may also be returned in the item Element type in the Status. Check SyncML syntax. For more information, refer to *CPS ANDSF Configuration Guide*.
401 Invalid credentials	The requested command failed because of improper authentication or authorization. If the property type of authentication was presented in the original request, then the response code indicates that the requested command has been refused for those credentials. Check **cred data** and **Authentication** type in syncml. For more information, refer to *CPS ANDSF Configuration Guide*.
500 Command failed	The recipient encountered an unexpected condition which prevented it from fulfilling the request. Verify **ssids** are attached to the subscriber and check **qns consolidated** logs in OAM (pcrfclient).
503 Service unavailable	The recipient is currently unable to handle the request due to a temporary overloading or maintenance of the recipient. The implication is that this is a temporary condition, which will be alleviated after some delay Check **qns consolidated** logs in OAM (pcrfclient).

General Errors

Problem Accessing ua/soap Getting Jetty Related Error

This problem occurs when Unified API service is not functioning.

Step 1 Execute **list_installed_features** command to check whether the following features are installed:

PCRF

- `com.broadhop.unifiedapi.interface.feature`
- `com.broadhop.unifiedapi.ws.service.feature`

Policy Builder

- `com.broadhop.client.feature.andsf`
- `com.broadhop.client.feature.unifiedapi`

Step 2 Add the missing features in Policy Builder and PCRF feature file (`/etc/broadhop/pb/features`, `/etc/broadhop/pcrf/features`).

Step 3 Execute the following commands from Cluster Manager.

/var/qps/install/current/scripts/build_all.sh

/var/qps/install/current/scripts/upgrade/reinit.sh

Check if Blank Policy is Retrieved in SyncML Response

This problem occurs whenever a respective policy for the UE request is not found.

Step 1 Make sure lookups defined in Control Center and Policy Builder are properly configured.

Step 2 Map DM configuration templates in Policy Builder with the actual DM configuration in Control Center and also look into subscriber mapped service configuration.

Step 3 Make sure no error object is being created for a non-matching option in Service Configuration. Check if options in Use Case Templates match corresponding Service Options and Service Configuration. They will be marked with a (X) if there is an error.

Step 4 Publish the corrections.

Step 5 After restarting policy server (QNS), run the use case again.

Policy Engine not Returning a Management Response

This problem occurs when a certain process during policy retrieval is failing due to an Exception in some process.

Step 1 Go to Policy Builder.

Step 2 Check that all the configurations are correct as per *CPS ANDSF Configuration Guide*.

Step 3 Check that the Control Center Lookup and associations are properly configured.

Step 4 Check `consolidated-qns.log` in pcrfclient01 VM to debug any relevant exceptions.

Notification Errors

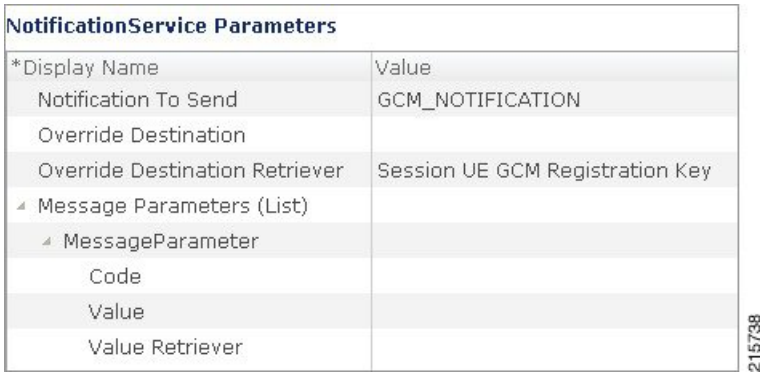
GCM Notification

No GCM Token Found

This generally happens when either UE is not sending the token in Device Info or Server is unable to retrieve this token for notification. Server can only retrieve token and store in the Device session if notification service is properly configured (if not using default configurations).

- Andsf_ISMP_Google_Notification

Figure 7: NotificationService Parameters



In the **Override Destination Retriever**, specify this field which will pick Token from Device Info field, having the following two tags: <GCMToken> for google devices. Make sure these are set in DM Client Vendor Page.

Figure 8: DM Client Vendor

Whenever notification is not received by client, following common error scenarios can occur:

- Couldn't Connect To GCM Server Exception

  This generally happens when Notification Configuration is not configured properly. Ensure load balancer is able to listen on the ports specified by GCM. The feature `com.broadhop.notifications.service.feature` is enabled on Policy Director (lb). Similarly `com.broadhop.notifications.local.feature` should be enabled on Policy Server (qns).

- Policy Builder Configuration
  - Under Notification Configuration check the configuration for GCM Configuration.

- The configuration should not be in error. The correct API key and Sender Id should be present.

- Server Configuration
  - Check there is an active connection established on the port 5235. The firewall is opened for the port.

    ```
    service iptables stop
    ```

    ```
    netstat -apn | grep 5235
    ```
    (Connection should be in established state)
  - Telnet connection is established for the port.

    Ping to **gcm.googleapis.com** should be successful.

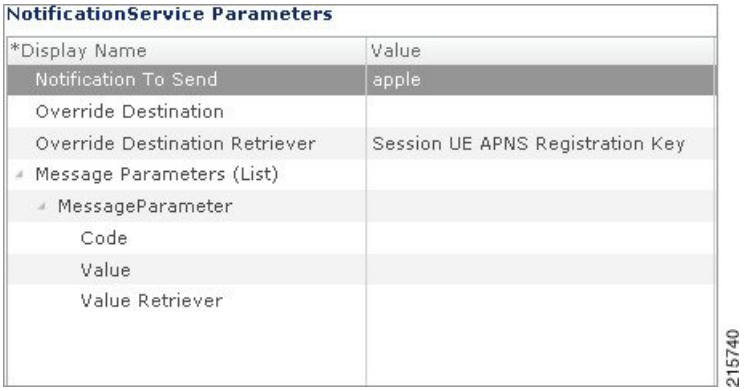
    Ping to **android.googleapis.com** should be successful.
  - A valid xmpp or http connection is established. The same should be visible in policy server (qns) logs on the active policy director (lb). Check Notification is being sent from policy server (qns) and the same is being relayed correctly by the policy director (lb) to the GCM Server.

APNS Notification

- No APNS Token Found

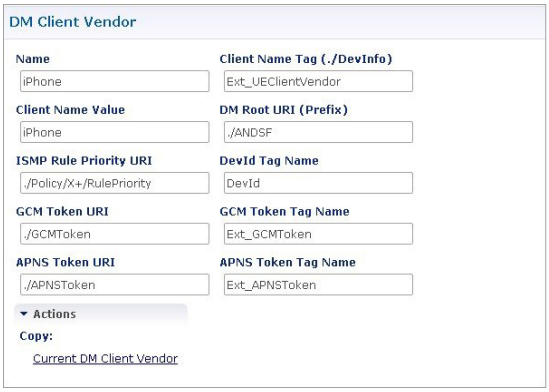
  This generally happens when either UE is not sending the token in Device Info or Server is unable to retrieve this token for notification. Server can only retrieve token and store in the Device session if notification service is properly configured (if not using default configurations)
  - Andsf_ISMP_Apple_Notification

    Figure 9: NotificationService Parameters

    In the **Override Destination Retriever**, specify this field which will pick Token from Device Info field, having the following two tags: <APNSToken> for apple devices. Make sure these are set in DM Client Vendor Page.

Figure 10: DM Client Vendor



Whenever notification is not received by client, following common error scenarios can occur:

- Couldn't Connect To APNS Server Exception

  This generally happens when Notification Configuration is not configured properly. Ensure load balancer is able to listen on the ports specified by APNS. The feature `com.broadhop.notifications.service.feature` is enabled on policy director (lb). Similarly, `com.broadhop.notifications.local.feature` should be enabled on policy server (qns).

- Policy Builder Configuration
  - Check the correct APNS Server is provided with the correct Server Port. The APNS token being sent is valid.
  - A valid Certificate and password is provided.
  - Correct Geo Fence value is configured under the ANDSF Configuration.

- Server Configuration
  - Check there is an active connection established on the port 2195. The firewall is opened for the port.

    `service iptables stop`

    `netstat -apn | grep 2195` (Connection should be in established state)
  - Telnet connection is established for the port.
  - Check if the APNS token is updated with the correct value in the Session Data. This should be a valid APNS Token.
  - Check Notification is being sent from policy server (qns) and the same is being relayed correctly by the policy director (lb) to the APNS Server

Basic Troubleshooting Using ANDSF Logs

Debugging Common Errors using Logging Techniques of ANDSF

The following procedure describes how to enable logs in `logback.xml`.

Step 1 Edit `/etc/broadhop/logback.xml`.

Step 2 Search for the following:

```
<!-- APS Loggers -->
```

Step 3 Change `<logger name="com.broadhop" level="warn"/>` to `<logger name="com.broadhop" level="debug"/>`.

Step 4 (Optional) To enable module specific logging, set the debugging level to debug for the specific module.

For example, `<logger name="com.broadhop.notifications" level="debug"/>` will set the debug level log for notifications module only.

Step 5 Copy this `logback.xml` file to all other policy server (qns) VMs using the following command:

```
copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml
```

Step 6 Capture the trace. Now run the call flow so that the trace is captured in the logs.
Logs will be captured in `/var/log/broadhop`.

Step 7 After you have captured and debugged the logs, roll back the `logback.xml` file.

Debugging Common Call Flow Scenarios for ANDSF using Logging Patterns

Generic Call Flow For Android

Step 1 Enable the logging for broadhop module at debug level as described in Debugging Common Errors using Logging Techniques of ANDSF, on page 13.

Step 2 On pcrfclient01, navigate to /var/log/broadhop.

Step 3 Use the tail command to view the consolidated-engine.log

Step 4 Send Package #1 for the subscriber. Look for the following values:

a) Correct Message and User Info is picked:

```
Message Id: 1

Source: IMEI:User_UseCase_Tier

User Name: User_UseCase_Tier
```

The Correct IMEI and User Name value should be displayed as specified in Control Center.

b) Check if USUSM Authorization was successful. If not, check that the User Name is the same as in Control Center and that Correct Authorization is given in Policy Builder.

```
INFO : (auth) Success USUM_AUTHORIZATION
```

c) Check if DevInfo gets Processed.

```
INFO : (ANSDF) DevInfo processed : vendor SmartSwitch
```

d) If a GCM token is supplied, see if it is read and updated.

```
INFO : (ANSDF) Updating GCM registration key !Vendor: SmartSwitch
```

e) Check the correct Use Case is picked and a valid response is sent to the same Subscriber.

```
INFO : (ANSDF) Sending response for session
imei:User_UseCase_Tier;Session_User_UseCase_Tier

INFO : (use-cases) Use case 'Andsf_ISMP_LOC', status: true, Condition: No Condition Set
```

Step 5 Send Package #3 for the subscriber. The correct policy should to be sent to the user on the basis of the lookups defined in DM Configuration in Control Center.

a) Correct Message and User Info is picked:

```
Message Id: 2

Source: IMEI:User_UseCase_Tier

User Name: User_UseCase_Tier
```

The Correct IMEI and User Name value should be displayed as specified in Control Center.

b) Check that the correct session is picked, as was given in Package #1:

```
Session ID: imei:User_UseCase_Tier;Session_User_UseCase_Tier
```

c) Check that correct TGPP and WLAN Location Values are picked as defined in Control Center under the DM Configuration Tab:

```
INFO : (ANSDF) Processing result cmd: 14

INFO : (ANSDF) Processed URI ./UE_Location/TGPP_Location value: [UseCase_Tier_TGPP]

INFO : (ANSDF) Processed URI ./UE_Location/WLAN_Location value: [UseCase_Tier_WLAN]
```

UseCase_Tier_TGPP is configured in TGPP_Location Table.

UseCase_Tier_WLAN is configured in WLAN_Location Table.

d) Check that the correct lookup is picked as defined in the DM Configuration and correct lookup filters are processed.

```
INFO : (ANSDF) checking state: LOOKUP {90}

INFO : (ANSDF) Processing lookup Policy_EXT_TIER

INFO : (ANSDF) Lookup using ./UE_Location/TGPP_Location value: [UseCase_Tier_TGPP]

INFO : (ANSDF) Lookup using ./UE_Location/WLAN_Location value: [UseCase_Tier_WLAN]

INFO : (ANSDF) Lookup using TIER value: [Gold]
```

e) Correct DM Treee is picked:

```
INFO : (ANSDF) Found subscriber specific node [SSIDTypeWLAN_Location2] in DMT
[UseCase_SSID_Tier]
```

UseCase_SSID_Tier is the Tree that is configured for the Lookups defined above in Control Center DM Configuration.

f) A valid response command is sent to the client:

```
INFO : (ANDSF) Adding Replace [response=2,7] for
imei:User_UseCase_Tier;Session_User_UseCase_Tier, msg=2
```

g) A valid Syncml response is sent:

```
INFO : (ANSDF) Sending response for session
imei:User_UseCase_Tier;Session_User_UseCase_Tier
```

Generic Call Flow For Apple

Step 1 Enable the logging for broadhop module at debug level as described in Debugging Common Errors using Logging Techniques of ANDSF, on page 13.

Step 2 On pcrfclient01, navigate to `/var/log/broadhop`.

Step 3 Use the **tail** command to view the consolidated-engine.log.

Step 4 Send Package #1 for the subscriber. Look for the following values:

a) Correct Message and User Info is picked:

```
Source: UUID:User_UseCase_IOS_1

User Name: User_UseCase_IOS

UUID: User_UseCase_IOS_1
```

The Correct UUID and User Name value should be displayed as specified in Control Center.

b) Correct Services are attached to the subscriber:

```
SERVICES: Andsf_ISMP_Apple_Notification Andsf_ISMP_GEO_LOC_STATIC
```

c) Check if USUSM Authorization was successful. If not, check that the User Name is the same as in Control Center and that Correct Authorization is given in Policy Builder.

```
INFO : (auth) Success USUM_AUTHORIZATION
```

d) Check the correct Use Case is picked and a valid response is sent to the same Subscriber.

```
INFO : (use-cases) Use case 'Andsf_ISMP_Apple_Notification', status: false, Condition:
("DM Device MO"=false)

INFO : (use-cases) Use case 'Andsf_ISMP_GEO_LOC_STATIC', status: true, Condition: No
Condition Set
```

Step 5 Send Package #3 for the subscriber. The correct policy should to be sent to the user on the basis of the lookups defined in DM Configuration in Control Center.

a) Correct Message and User Info is picked:

```
Message Id: 2

Source: UUID:User_UseCase_IOS_1

User Name: User_UseCase_IOS

UUID: User_UseCase_IOS_1
```

Correct UUID and User Name value should be displayed as specified in Control Center.

b) Correct Session is picked as was given in Package #1:

```
Session ID: uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1
```

c) Check the DevInfo gets Processed:

```
INFO : (ANSDF) Pre-fetch URI ./DevInfo cmd: 4

INFO : (ANSDF) DevInfo processed : vendor iPhone DevId: 12345 DevType: NA
```

d) If an APNS token is supplied, see if it is read and updated.

```
INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: iPhone, Client: NA, DevId: 12345,
GCMToken: null
```

e) Check that correct Geo Location Values are picked as defined in Control Center under the DM Configuration Tab:

```
INFO : (ANSDF) Processed URI ./UE_Location/Geo_Location value: [geo_1]
```

geo_1 is configured in Geo_Location Table.

f) Check that the correct lookup is picked as defined in the DM Configuration and correct lookup filters are processed:

```
INFO : (ANSDF) checking state: LOOKUP {90}

INFO : (ANSDF) Processing lookup Policy_EXT_GEO_LOC_STATIC

INFO : (ANSDF) Lookup using ./UE_Location/Geo_Location value: [geo_1]
```

g) A valid response command is sent to the client:

```
INFO : (ANDSF) Adding Replace [response=2,6] for
uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1, msg=2
```

h) A valid Syncml response is sent:

```
INFO : (ANSDF) Sending response for session
uuid:User_UseCase_IOS_1;Session_User_UseCase_IOS_1
```

GCM Notification

Step 1 Check that the GCM Token is defined and updated in the Logs for the subscriber:

```
UUID: Sub_Test_1

User Name: User_UseCase_GCM_1

INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: SmartSwitch, Client: NA, DevId:
User_UseCase_Tier, GCMToken:
APA91bGbvmHGxpePBt_HkV3Rqw7SW01GyaiqoYdvJv1SPPtQDrO62RGEK-tbk5-bQ5VOCgj4fHM98LzEQPLw6uR4
XlSqu-FW7lqwApCTf-ssjIo1_1oFmyd-VDpcyvN0PIkkGeW0wDNilcjyLmX92bfpusD6RUuIx_1m88maJJzSQPiM
fdq3rTA

INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 2 On Subscriber Version Update, check that the Notification is being sent:

```
POLICY RESULT SUCCESS:

session action = None
```

```
domainId = ANDSF

subscriberId = 00300000e4b0fb825589222c

SERVICES: NOTIF_GCM Andsf_ISMP_Tier

TRIGGER: com.broadhop.spr.impl.messages.RefreshSPRProfile Key:
pk:userId:User_UseCase_GCM_1

DEBUG MSGS:

  INFO : (core) Lock obtained on key: pk:userId:User_UseCase_GCM_1

  INFO : (core) Successful load by key: pk:userId:User_UseCase_GCM_1

  INFO : (ANSDF) Sending PUSH on subscriber-version update

  INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:44 IST 2015
```

Step 3 On the Load Balancer, check qns-1.log:

```
Received GCM Notification request : Request:

template name: GCM_NOTIFICATION

collapse key: COLL_KEY_1

time to live: 1


DEBUG c.b.n.gcm.GcmMessageManager.? - Standard parameters used for sending GCM notification
: timeToLive(days) : 5, delayWhileIdle : false, collapseKey : COLL_K****,
apiKeyAIzaSyAXV9L1lI7HLo2n********************, senderId1380935*****

DEBUG c.b.n.gcm.GcmMessageManager.? - GCM message to be sent : Test Message

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Listener Received: <message><gcm xmlns="goog

DEBUG c.b.notifications.gcm.GcmXmppServer.? - XMPP packate recieved : {"registration_id":

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Collector Received: <message><gcm
xmlns="google:mobile:data"

DEBUG c.b.notifications.gcm.GcmXmppServer.? - CCS ACK received !!

DEBUG c.b.n.i.a.SendGcmNotificationRequest.? - GCM Notification request processing got
completed !!
```

APNS Notification

Step 1 Check that the APNS Token is defined and updated in the Logs for the subscriber:

```
UUID: Sub_Test_1

User Name: User_UseCase_IOS_8

INFO : (ANSDF) Reusing GCM/APNS token !!Vendor: SmartSwitch, Client: NA, DevId: 12345

INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 2 On Subscriber Version Update, check that the Notification is being sent:

```
POLICY RESULT SUCCESS:

session action = None

domainId = ANDSF

subscriberId = 00500000e4b0fb8255892f94

SERVICES: ISMP_Apple_Notification

TRIGGER: com.broadhop.spr.impl.messages.RefreshSPRProfile Key:
pk:userId:User_UseCase_IOS_08

DEBUG MSGS:

  INFO : (core) Lock obtained on key: pk:userId:User_UseCase_IOS_08

  INFO : (core) Successful load by key: pk:userId:User_UseCase_IOS_08

  INFO : (ANSDF) Sending PUSH on subscriber-version update

  INFO : (ANSDF) Setting next evaluation time Tue Jun 23 14:54:43 IST 2015
```

Step 3 On the Load Balancer, check qns-1.log:

```
DEBUG c.b.n.impl.NotificationsManager.? - sendApplePushNotification: Device Token being
pushed to is: 67349132e3631b7a5642d2dae5991359042120c9ca0c30236bcc0bcaed1741c7.

DEBUG c.n.apns.internal.ApnsConnectionImpl.? - Made a new connection to APNS

DEBUG c.n.apns.internal.ApnsConnectionImpl.? - Message
"com.notnoop.apns.ApnsNotification@ecdaaeef"
```

Notification for Revalidation Timer

Step 1 Check that the value for revalidation timer (as defined in Policy Builder) is set in the logs:

```
INFO : (ANSDF) Setting next evaluation time Tue Jun 23 13:05:09 IST 2015
```

Step 2 Check that a revalidation Timer Push Notification is sent after the timer has expired. Check that correct Use Case and Trigger are used:

```
qns02 [2015-06-23 13:03:05,317] ================================================

  POLICY RESULT SUCCESS:

    session action = None

    domainId = ANDSF

    subscriberId = 00153c00e4b0c35e558901c0

    SERVICES: Andsf_ISMP_Tier

    TRIGGER: com.broadhop.cache.TimerExpired request:

  key: null:userId:User_UseCase_Tier
```

```
  DEBUG MSGS:

    INFO : (ANSDF) Sending PUSH for re-validation timer expiry

    INFO : (ANSDF) Setting next evaluation time Tue Jun 23 13:13:05 IST 2015

    INFO : (use-cases) Use case 'Andsf_ISMP_LOC', status: true, Condition: No Condition Set

==========================================================================
```

Step 3 On the Load Balancer, check qns-1.log:

```
Received GCM Notification request : Request:

template name: GCM_NOTIFICATION

collapse key: COLL_KEY_1

time to live: 1


DEBUG c.b.n.gcm.GcmMessageManager.? - Standard parameters used for sending GCM notification
: timeToLive(days) : 5, delayWhileIdle : false, collapseKey : COLL_K****,
apiKeyAIzaSyAXV9L1lI7HLo2n******************, senderId1380935*****

DEBUG c.b.n.gcm.GcmMessageManager.? - GCM message to be sent : Test Message

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Listener Received: <message><gcm xmlns="goog

DEBUG c.b.notifications.gcm.GcmXmppServer.? - XMPP packate recieved : {"registration_id":

DEBUG c.b.notifications.gcm.GcmXmppServer.? - Collector Received: <message><gcm
xmlns="google:mobile:data"

DEBUG c.b.notifications.gcm.GcmXmppServer.? - CCS ACK received !!

DEBUG c.b.n.i.a.SendGcmNotificationRequest.? - GCM Notification request processing got
completed !!
```