

Troubleshoot APNS "400 bad request" Errors

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components used](#)

[Background information](#)

[Troubleshoot](#)

[Solution](#)

[Verify](#)

Introduction

This document describes how to troubleshoot APNS "400 bad request" errors; a known issue documented in the Cisco bug ID [CSCvi01660](#).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- **Apple Push Notifications** configuration.
- **Apple Push Notifications** functionality.

Components used

This document is not restricted to specific hardware and software versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background information

When your cluster is enabled for Push Notifications, Cisco Unified Communications Manager and the IM and Presence Service use either the Apple, or Google cloud's Push Notification service to send push notifications to compatible Cisco Jabber or Webex clients that run on iOS or Android devices. Push Notifications let your system communicate with the client, even after it has entered into background mode (also known as suspended mode). Without Push Notifications, the system is possibly unable to send calls or messages to clients that have entered into background mode.

To authenticate with the Cisco Cloud your Cisco Communications Manager Server generates a token as a part of the onboarding process, If you receive a "400 bad request" message, then your machine access token to the Push Notifications service has expired and you need to update the access token manually according to the documentation:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_push-notifications-deployment-guide/cucm_b_push-notifications-deployment-guide_chapter_01.html?bookSearch=true

Troubleshoot

Set the next logs to debug and collect it with the Real Time Monitoring Tool:

Cisco Unified Communications Manager :

Cisco Push Notification Service

Cisco Management Agent Service

Cisco Unified Communications Manager IM and Presence:

Cisco XCP Config Manager

Cisco XCP Router

On the Cisco Push Notification Service logs, you can see that the CUCM receives multiple 400 responses while fetching the token which makes APNS fail, hence the counters do not increase:

```
2024-07-16 15:09:50,514 DEBUG [Timer-144] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:19:51,007 DEBUG [Timer-145] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:29:51,605 DEBUG [Timer-146] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:39:52,096 DEBUG [Timer-147] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:49:52,565 DEBUG [Timer-148] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400 2024-07-16 15:59:53,032 DEBUG [Timer-149] ccmpns.CCMPNServer (CCMPNServer.java:306) - fetchAndStoreAccessToken() Response received : 400
```

You can see an invalid response on the Cisco XCP Router logs around the time in which the call is made:

```
2024-07-16 17:21:43,464 DEBUG [Timer-1382] xmlframework.XCPConfigMgr - FetchAndStoreAccessToken: Calling createAccessToken() with granttype:refresh_token, refreshToken:MTc2YzFhN2YtMDA1Ny00MTVILWJGZmMjcwYTU3MjY1NGI1NzItZmE0, accessTokenURL proxyUsernamenull 2024-07-16 17:21:43,468 INFO [Timer-1382] utilities.CloudOnboarding - TRACKING ID::::::FOS_e8e8ee93-818f-4fe5-8a23-6b08a879b91b 2024-07-16 17:21:43,790 ERROR [Timer-1382] utilities.TomcatTrustManager - checkServerTrusted:entered 2024-07-16 17:21:43,791 ERROR [Timer-1382] utilities.TomcatTrustManager - checkServerTrusted:entered 2 2024-07-16 17:21:43,958 DEBUG [Timer-1382] xmlframework.XCPConfigMgr - XCPConfigMgr:Inside responseStatus() 2024-07-16 17:21:43,958 ERROR [Timer-1382] xmlframework.XCPConfigMgr - 400 Bad Request: invalid_request, unsupported_grant_type, invalid_client, invalid_refresh_token, tokenlimit_reached 2019-07-16 17:21:43,958 DEBUG [Timer-1382] xmlframework.XCPConfigMgr - XCPConfigMgr:FetchAndStoreAccessToken: Inside Finally Block
```

This is a known Cisco bug ID [CSCvi01660](#).

Solution

Build a laboratory system and update the Refresh Token from the laboratory to the production system.

Once you have deployed the laboratory system, perform the next steps:

Step 1:

On your Call Manager publisher open a CLI session and run the command “run sql select * from machineaccountdetails” and save all the output in a .txt file:

```
admin:run sql select * from machineaccountdetails
pkid                                refreshtoken
      accesstokenurl                pushmsurl
      alarmurl
=====
=====
e40c24c0-cd4c-4256                 OGYyZGI2MWMtNjUwYy00Y2FiLThh
efreshToken https://idbroker.webex.com/idb/oauth2/v1/access_token https://push.webex.com/fos/api/v1/metrics https://fos-a.webex.com/fos/api/v1/alarm
```

Once all the output is saved, pay special attention to your Call Manager pkid, for example, our laboratory environment is “e40c24c0-cd4c-4256”.

Also, run the command “run sql select * from machineaccountdetails” in your laboratory environment and save all the output in a .txt file.

Pay special attention to the refreshtoken in your laboratory environment as this is the valid token that we use to replace the invalid token in your production environment. In our laboratory environment is something like "OGYyZGI2MWMtNjUwYy00Y2FiLThh".

Step 2:

We need to replace your current non-working refresh token with the valid laboratory token.

After you have saved your production pkid, run this sql query in your production Call Manager Publisher:

```
run sql update machineaccountdetails set refreshtoken='here goes the valid refresh token of your laboratory environment' where pkid='here goes your production pkid'.
```

The previous sql query changes your non-working token with the working one from your laboratory environment.

Step 3:

After you have updated the machineaccountdetails with the lab refresh token, please restart these services:

Cisco Unified Communications Manager ::

- Cisco Management Agent Service (CMAS)
- Cisco Push Notification Service (CCMPNS)
- Tomcat

Cisco Unified Communications Manager IM and Presence:

- XCP Config manager
- XCP Router
- Tomcat

These services must be restarted after hours to avoid any service impact.

Verify

Now run again “run sql select * from machineaccountdetails” on all nodes including the IMPs and verify now that you have my refresh token.