# Sending Notifications

## Overview

In order to send push or SMS notifications to iOS, Android or Windows devices, the MobileFirst Server first needs to be configured with the GCM details for Android, an APNS certificate for iOS or WNS credentials for Windows 8.1 Universal / Windows 10 UWP. Notifications can then be sent to: all devices (broadcast), devices that registered to specific tags, a single Device ID, User Ids, only iOS devices, only Android devices, only Windows devices, or based on the authenticated user.

**Prerequisite**:

- For push notifications, make sure to read the Push Notifications overview (../push-notifications-overview/) tutorial.
- For SMS notifications, make sure to read the SMS Notifications overview (../sms-notifications-overview/) tutorial.

Jump to



## Setting up Notifications

Enabling notifications support involves several configuration steps in both MobileFirst Server and the client application.
Continue reading for the server-side setup, or jump to Client-side setup.

On the server-side, required set-up includes: configuring the needed vendor (APNS, GCM or WNS) and mapping the "push.mobileclient" scope.

### Google Cloud Messaging

Android devices use the Google Cloud Messaging (GCM) service for push notifications.
To setup GCM:

1. Visit Google's Services website (https://developers.google.com/mobile/add?platform=android&cntapi=gcm&cnturl=https:%2F%2Fdevelopers.google.com%2Fcloud-messaging%2Fandroid%2Fclient&cntlbl=Continue%20Adding%20GCM%20Support&%3Fconfigured%3Dtrue).
2. Provide your application name and package name.
3. Select "Cloud Messaging" and click on **Enable Google cloud messaging**.
   - This step generates a **Server API Key** and a **Sender ID**.

> **Note:** Also availbe is the option to generate configuration files. This set-up step is not needed.

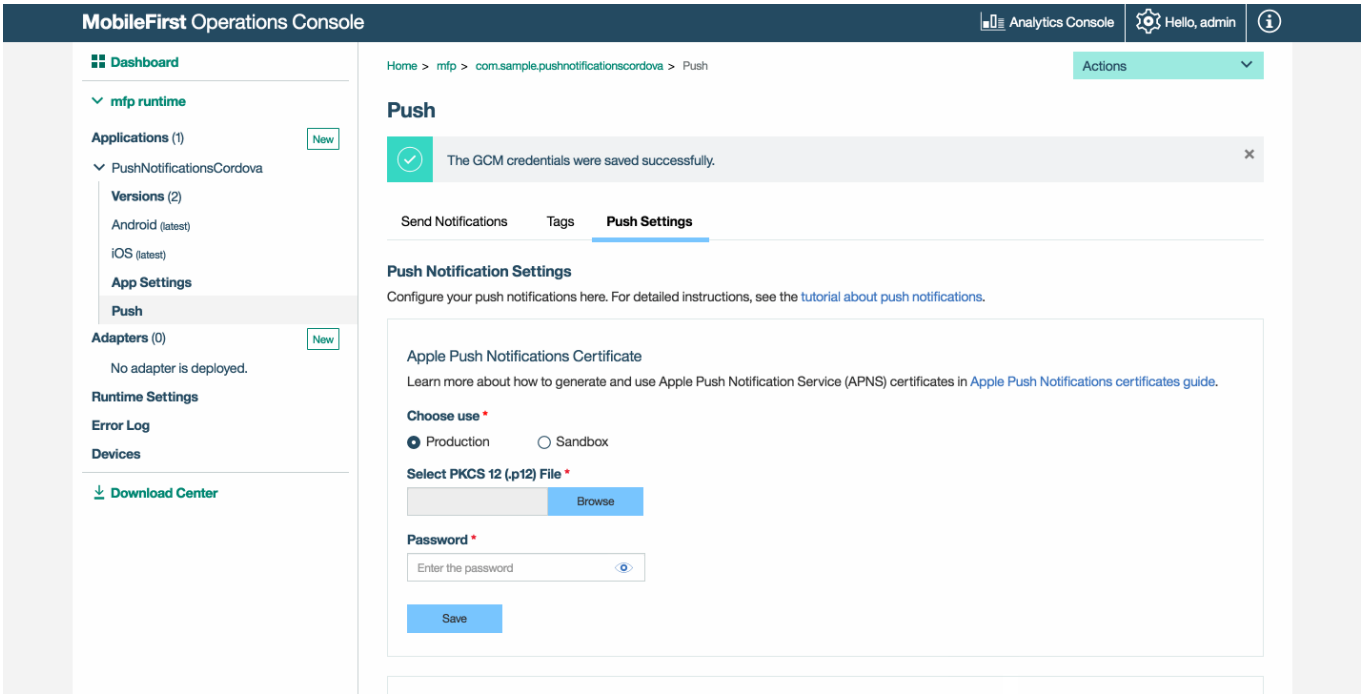
- The generated values are used to identify the application by Google's GCM service in order to send notifications to the device.

4. In the MobileFirst Operations Console → **[your application]** → **Push** → **Push Settings**, add the GCM **Sender ID** and **Server API Key** and click **Save**.

### Notes

If your organization has a firewall that restricts the traffic to or from the Internet, you must go through the following steps:

- Configure the firewall to allow connectivity with GCM in order for your GCM client apps to receive messages.
- The ports to open are 5228, 5229, and 5230. GCM typically uses only 5228, but it sometimes uses 5229 and 5230.
- GCM does not provide specific IP, so you must allow your firewall to accept outgoing connections to all IP addresses contained in the IP blocks listed in Google's ASN of 15169.
- Ensure that your firewall accepts outgoing connections from MobileFirst Server to android.googleapis.com on port 443.



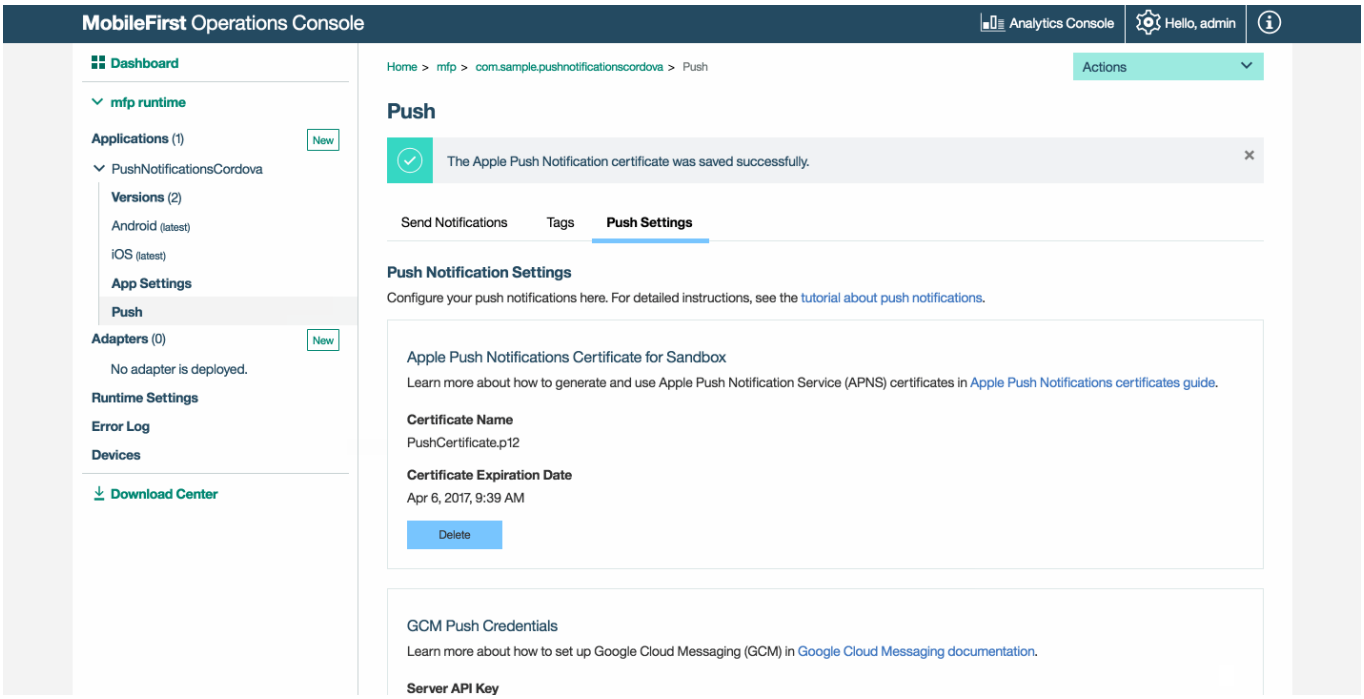

## Apple Push Notifications Service

iOS devices use Apple's Push Notification Service (APNS) for push notifications.
To setup APNS:

1. Generate a push notification certificate (https://www.ibm.com/developerworks/community/blogs/worklight/entry/understanding-and-setting-up-push-notifications-in-development-evnironment?lang=en).
2. In the MobileFirst Operations Console → **[your application]** → **Push** → **Push Settings**, select the certificate type and provide the certificate's file and password. Then, click **Save**.

### Notes

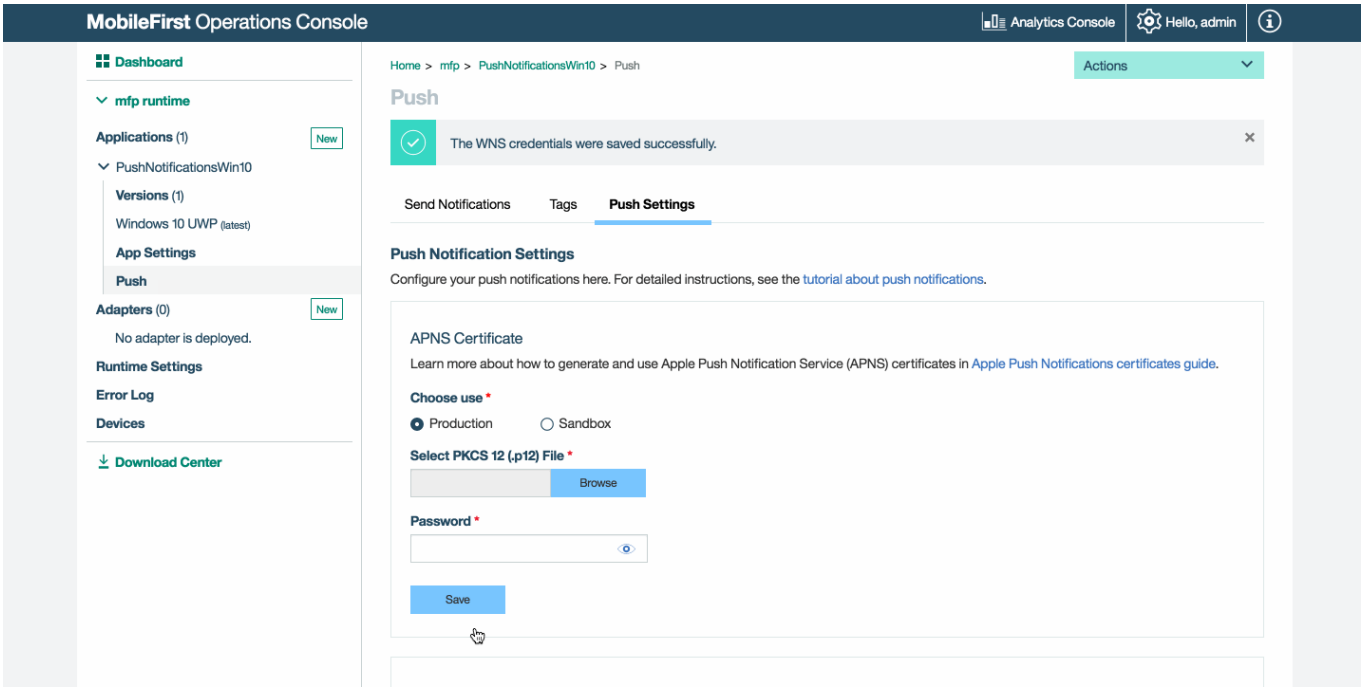
- For push notifications to be sent, the following servers must be accessible from a MobileFirst Server instance:
    - Sandbox servers:
        - gateway.sandbox.push.apple.com:2195
        - feedback.sandbox.push.apple.com:2196
    - Production servers:
        - gateway.push.apple.com:2195
        - Feedback.push.apple.com:2196
        - 1-courier.push.apple.com 5223
- During the development phase, use the apns-certificate-sandbox.p12 sandbox certificate file.
- During the production phase, use the apns-certificate-production.p12 production certificate file.
    - The APNS production certificate can only be tested once the application that utilizes it has been successfully submitted to the Apple App Store.




## Windows Push Notifications Service

Windows devices use the Windows Push Notifications Service (WNS) for push notifications.
To setup WNS:

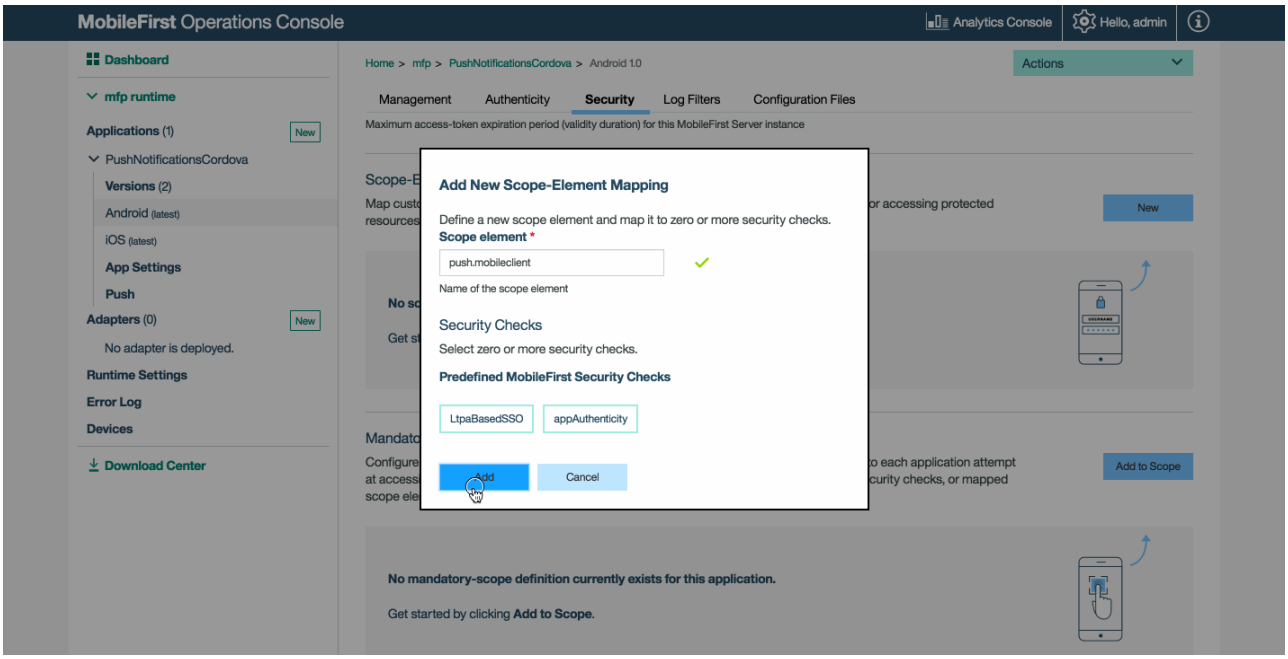
1. Follow the instructions as provided by Microsoft (http://localhost:4000/tutorials/en/foundation/8.0/notifications/sending-push-notifications/#google-cloud-messaging) to generate the **Package Security Identifier (SID)** and **Client secret** values.
2. In the MobileFirst Operations Console → **[your application] → Push → Push Settings**, add these values and click **Save**.




## Scope mapping

Map the **push.mobileclient** scope element to the application.

1. Load the MobileFirst Operations Console and navigate to **[your application] → Security → Map Scope Elements to Security Checks**, click on **Create New**.
2. Write "push.mobileclient" in the **Scope element** field. Then, click **Add**.

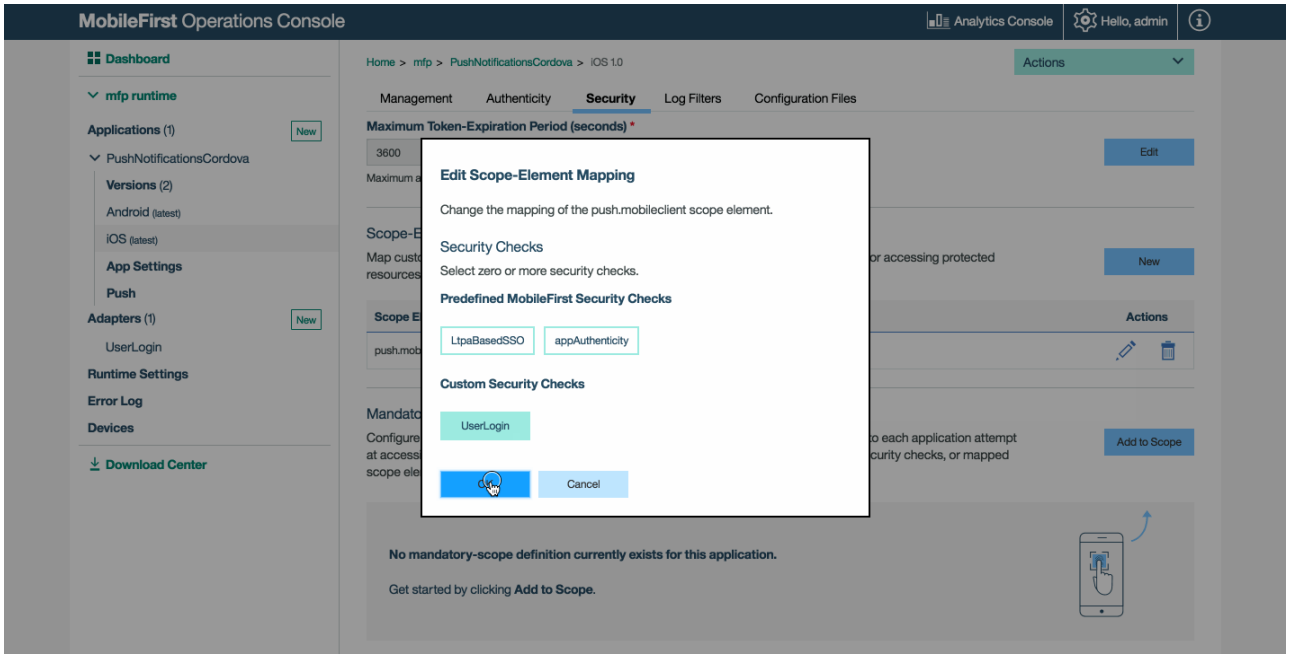



## Authenticated Notifications

Authenticated notifications are notifications that are sent to one or more `userIds`.

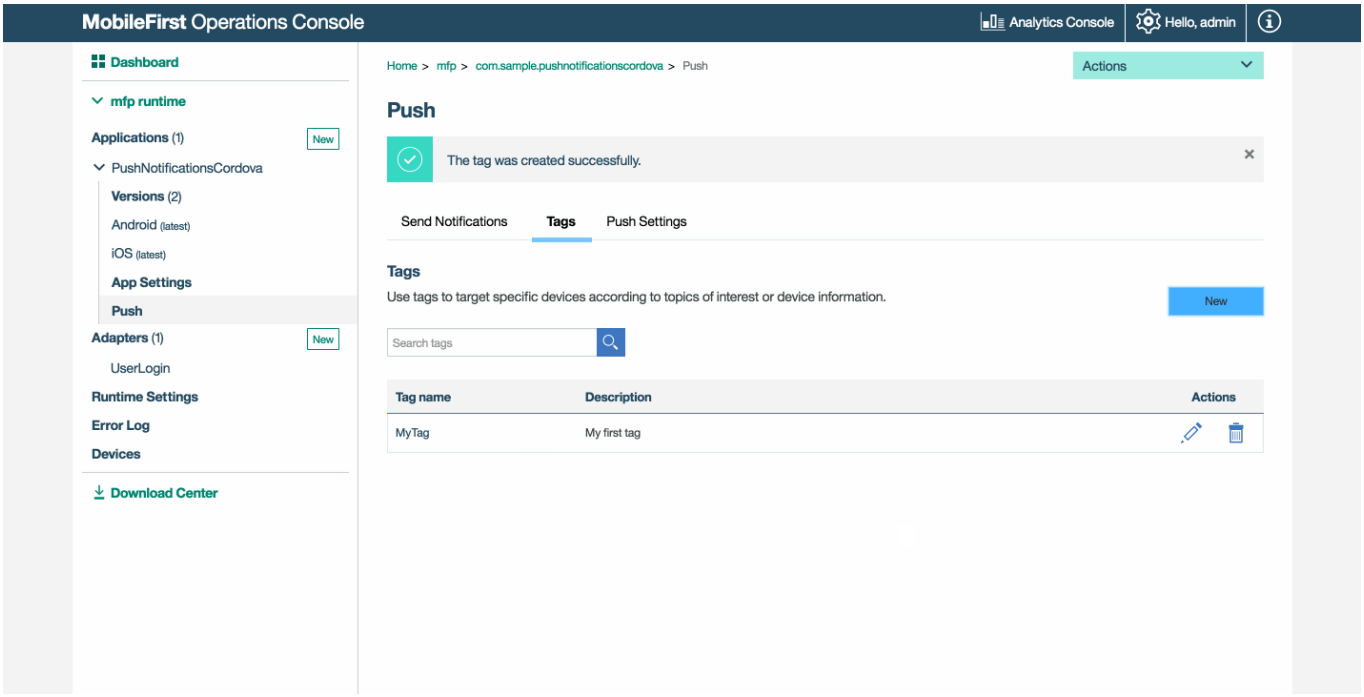
Map the **push.mobileclient** scope element to the security check used for the application.

1. Load the MobileFirst Operations Console and navigate to **[your application] → Security → Map Scope Elements to Security Checks**, click on **Create New** or edit an existing scope mapping entry.
2. Select a security check. Then, click **Add**.




# Defining Tags

In the MobileFirst Operations Console → **[your application]** → **Push** → **Tags**, click **Create New**.
Provide the appropriate `Tag Name` and `Description` and click **Save**.




# Sending Push Notifications

Push notifications can be sent either from the MobileFirst Operations Console or via REST APIs.

- With the MobileFirst Operations Console, two types of notifications can be sent: tag and broadcast.
- With the REST APIs, all forms of notifications can be sent: tag, broadcast and authenticated.

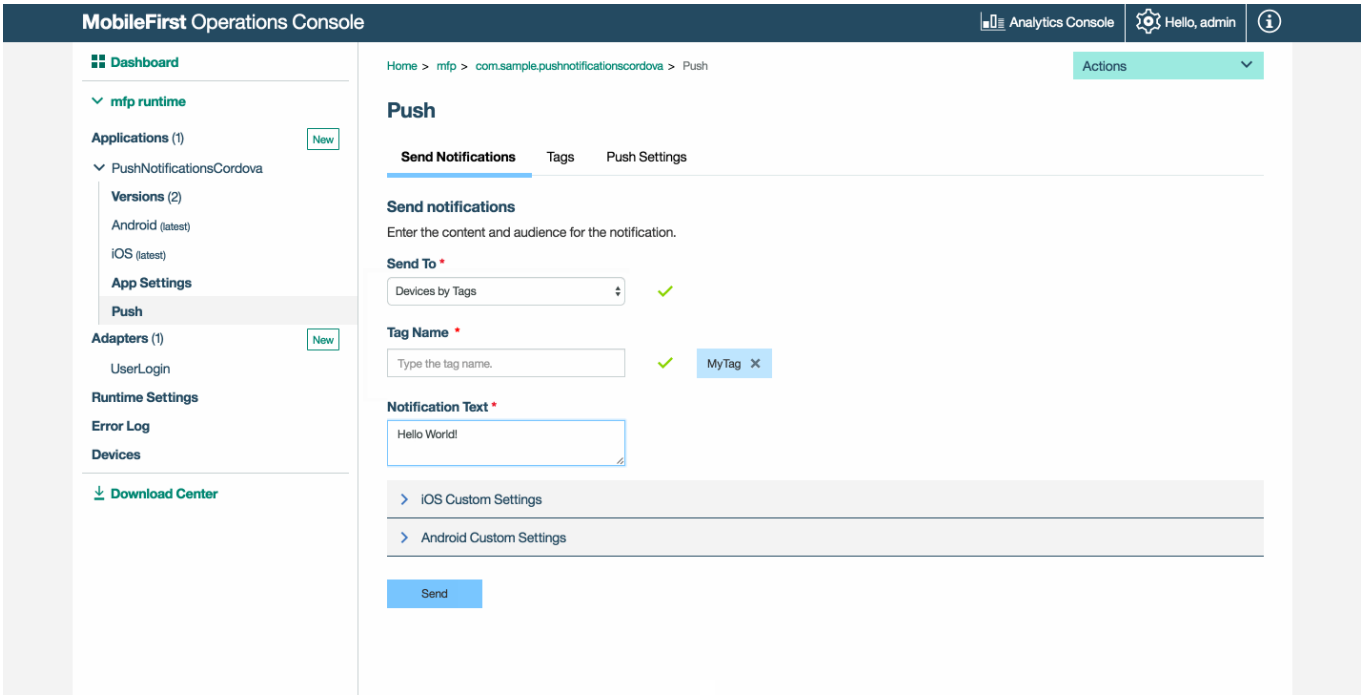
## MobileFirst Operations Console

Notifications can be sent to a single Device ID, a single or several User IDs, only iOS devices or only Android devices, or to devices subscribed to tags.

### Tag notifications

Tag notifications are notification messages that are targeted to all the devices that are subscribed to a particular tag. Tags represent topics of interest to the user and provide the ability to receive notifications according to the chosen interest.

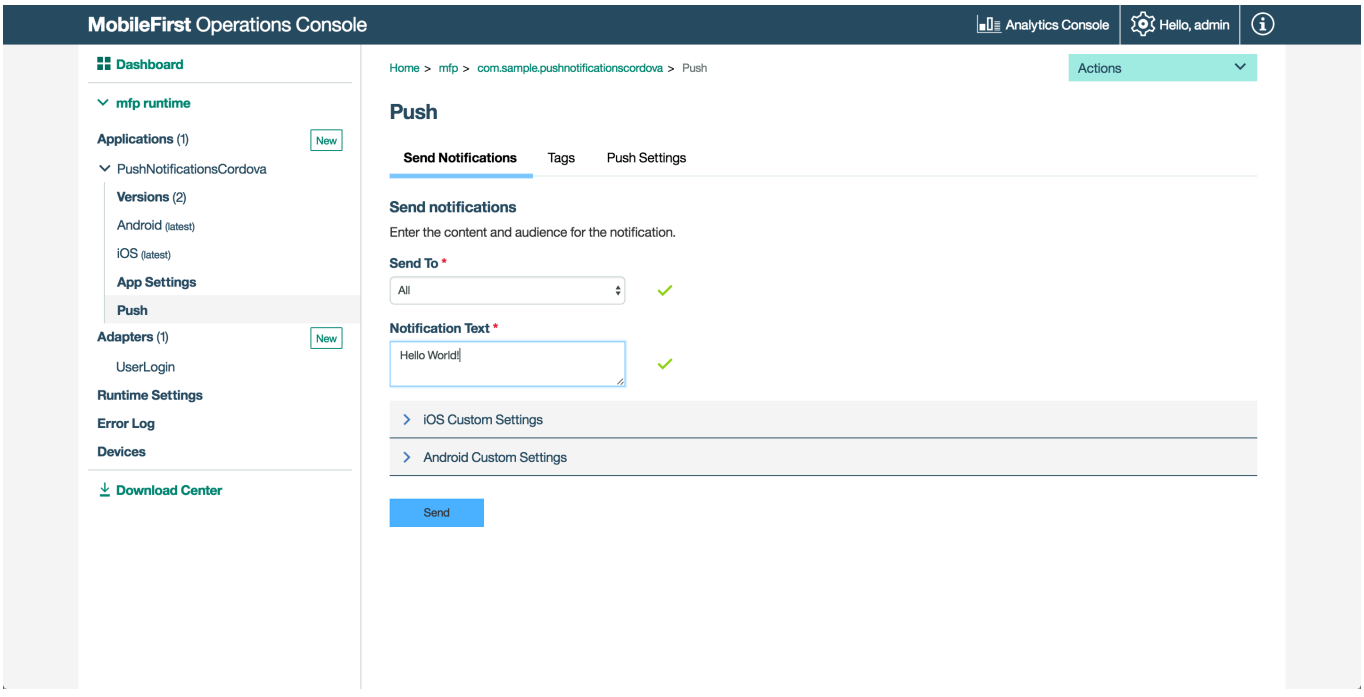
In the MobileFirst Operations Console → **[your application] → Push → Send Push tab**, select **Devices By Tags** from the **Send To** tab and provide the **Notification Text**. Then, click **Send**.




## Broadcast notifications

Broadcast notifications are a form of tag push notifications that are targeted to all subscribed devices. Broadcast notifications are enabled by default for any push-enabled MobileFirst application by a subscription to a reserved `Push.all` tag (auto-created for every device). The `Push.all` tag can be programmatically unsubscribed.

In the MobileFirst Operations Console → **[your application] → Push → Send Push tab**, select **All** from the **Send To** tab and provide the **Notification Text**. Then, click **Send**.




# REST APIs

When using the REST APIs to send notifications, all forms of notifications can be sent: tag & broadcast notifications, and authenticated notifications.

To send a notification, a request is made using POST to the REST endpoint: `imfpush/v1/apps/<application-identifier>/messages`.
Example URL:

```
https://myserver.com:443/imfpush/v1/apps/com.sample.PinCodeSwift/messages
```

> To review all Push Notifications REST APIs, see the "REST API Runtime Services" topic in the user documentation.

## Notification payload

The request can contain the following payload properties:

| Payload Properties | Definition |
|---|---|
| message | The alert message to be sent |
| settings | The settings are the different attributes of the notification. |
| target | Set of targets can be consumer Ids, devices, platforms, or tags. Only one of the targets can be set. |
| deviceIds | An array of the devices represented by the device identifiers. Devices with these ids receive the notification. This is a unicast notification. |
| platforms | An array of device platforms. Devices running on these platforms receive the notification. Supported values are A (Apple/iOS), G (Google/Android) and M (Microsoft/Windows). |
| tagNames | An array of tags specified as tagNames. Devices that are subscribed to these tags receive the notification. Use this type of target for tag based notifications. |
| userIds | An array of users represented by their userIds to send the notification. This is a unicast notification. |
| phoneNumber | The phone number used for registering the device and receiving notifications. This is a unicast notification. |

**Push Notifications Payload JSON Example**

```
{
   "message" : {
   "alert" : "Test message",
  },
  "settings" : {
   "apns" : {
     "badge" : 1,
     "iosActionKey" : "Ok",
     "payload" : "",
     "sound" : "song.mp3",
     "type" : "SILENT",
   },
   "gcm" : {
     "delayWhileIdle" : ,
     "payload" : "",
     "sound" : "song.mp3",
     "timeToLive" : ,
   },
  },
  "target" : {
   "deviceIds" : [ "MyDeviceId1", ... ],
   "platforms" : [ "A,G", ... ],
   "tagNames" : [ "Gold", ... ],
   "userIds" : [ "MyUserId", ... ],
  },
}
```

**SMS Notification Payload JSON Example**

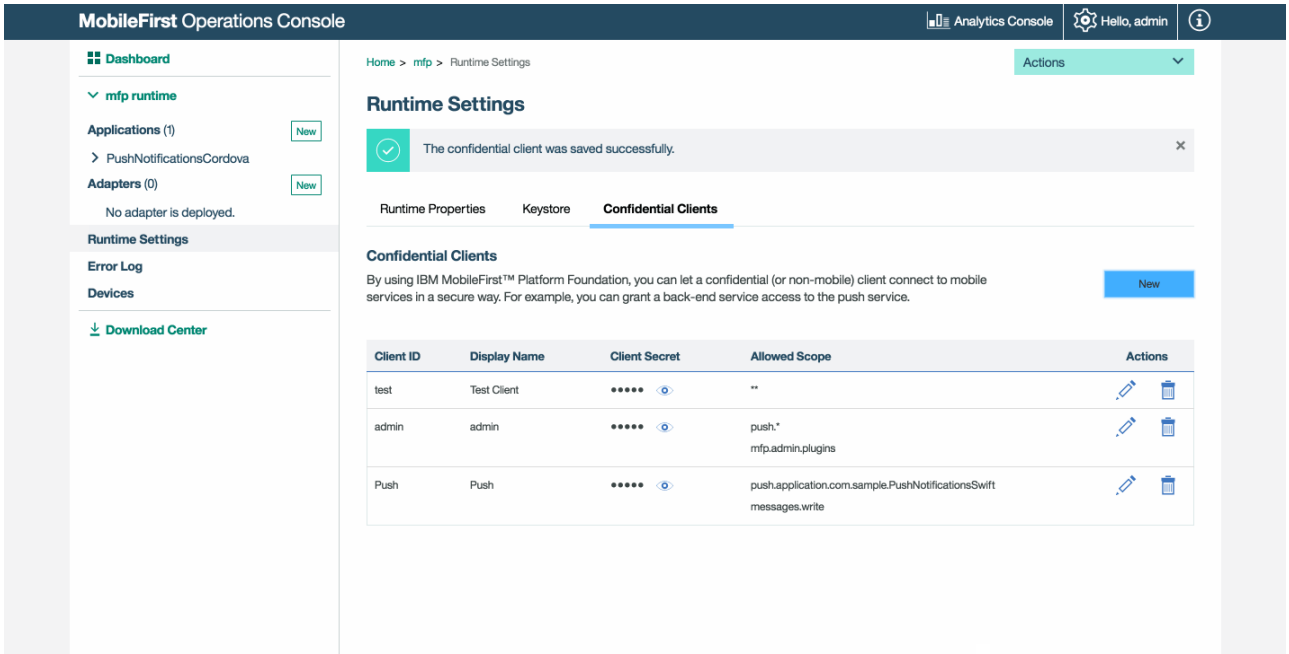
```
{
   "host": "2by0.com",
   "name": "dummy",
   "port": "80",
   "programName": "gateway/add.php",
   "parameters": [{
      "name": "xmlHttp",
      "value": "false",
      "encode": "true"
   }, {
      "name": "httpsEnabled",
      "value": "false",
      "encode": "true"
   }]

}
```

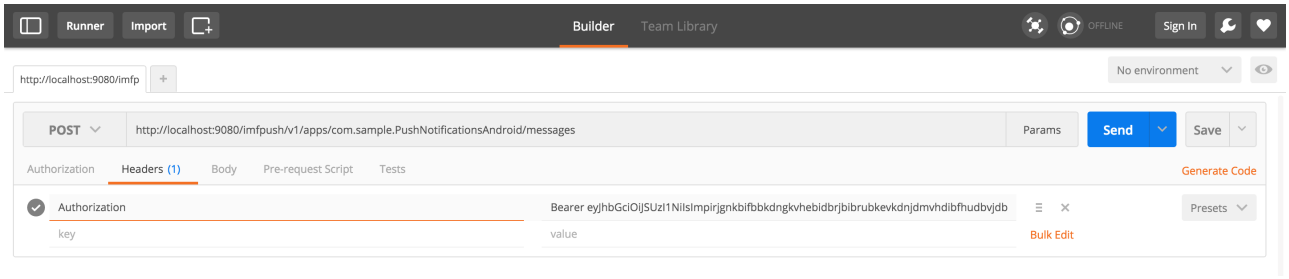
## Sending the notification

The notification can be sent using different tools.
For testing purposes, Postman is used as described below:

1. Configure a Confidential Client (../../authentication-and-security/confidential-clients/).
   Sending a Push Notification via the REST API uses the space-separated scope elements `messages.write` and `push.application.<applicationId>.`

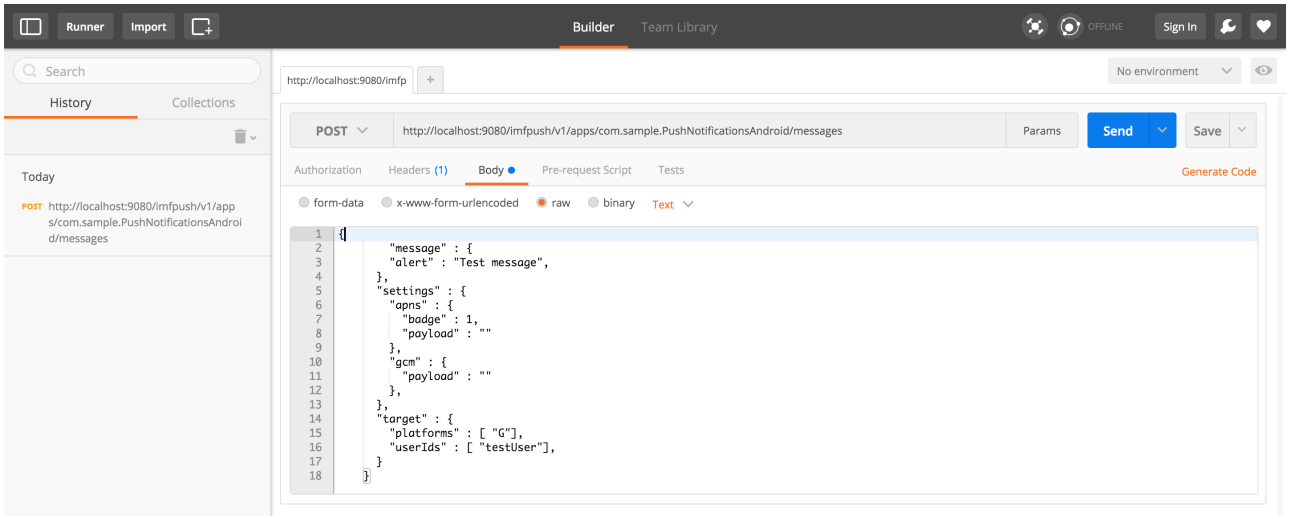



2. Create an access token (../../authentication-and-security/confidential-clients#obtaining-an-access-token).
3. Make a **POST** request to
   **http://localhost:9080/imfpush/v1/apps/com.sample.PushNotificationsAndroid/messages**
   - If using a remote MobileFirst Server, replace the `hostname` and `port` values with your own.
   - Update the application identifier value with your own.
4. Set a Header:
   - **Authorization**: `Bearer eyJhbGciOiJSUzI1NiIsImp ...`
   - Replace the value after "Bearer" with the value of your access token from step (1) above.

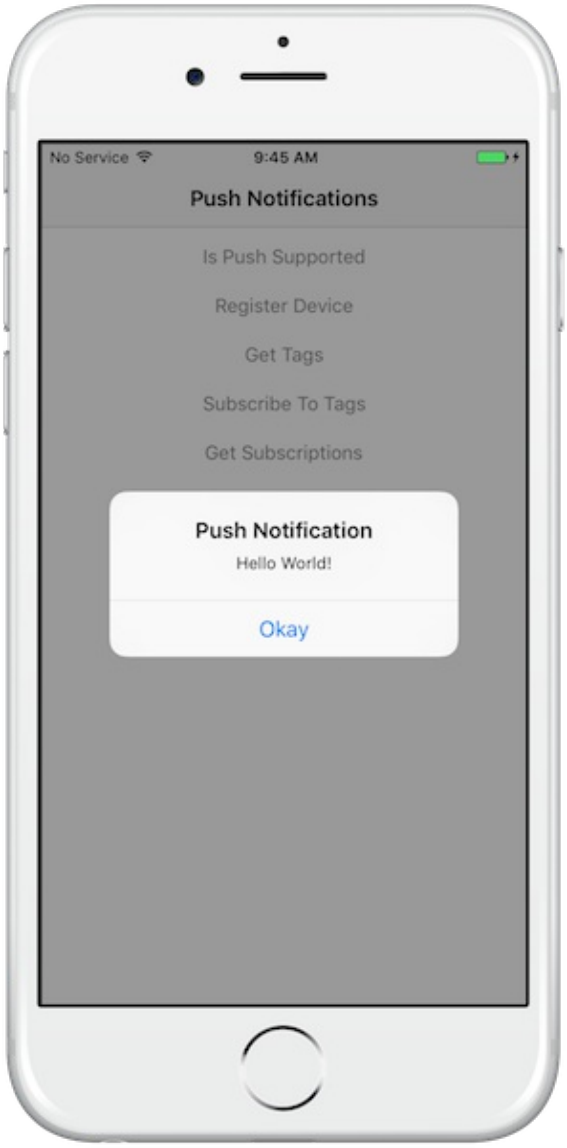



5. Set a Body:
    - Update its properties as described in Notification payload above.
    - For example, by adding the **target** property with the **userIds** attribute, you can send a notification to specific registered users.

```
{
   "message" : {
      "alert" : "Hello World!"
   }
}
```




After clicking on the **Send** button, the device should have now received a notification:




## Customizing Notifications

Before sending the notification message, you can also customize the following notification attributes.

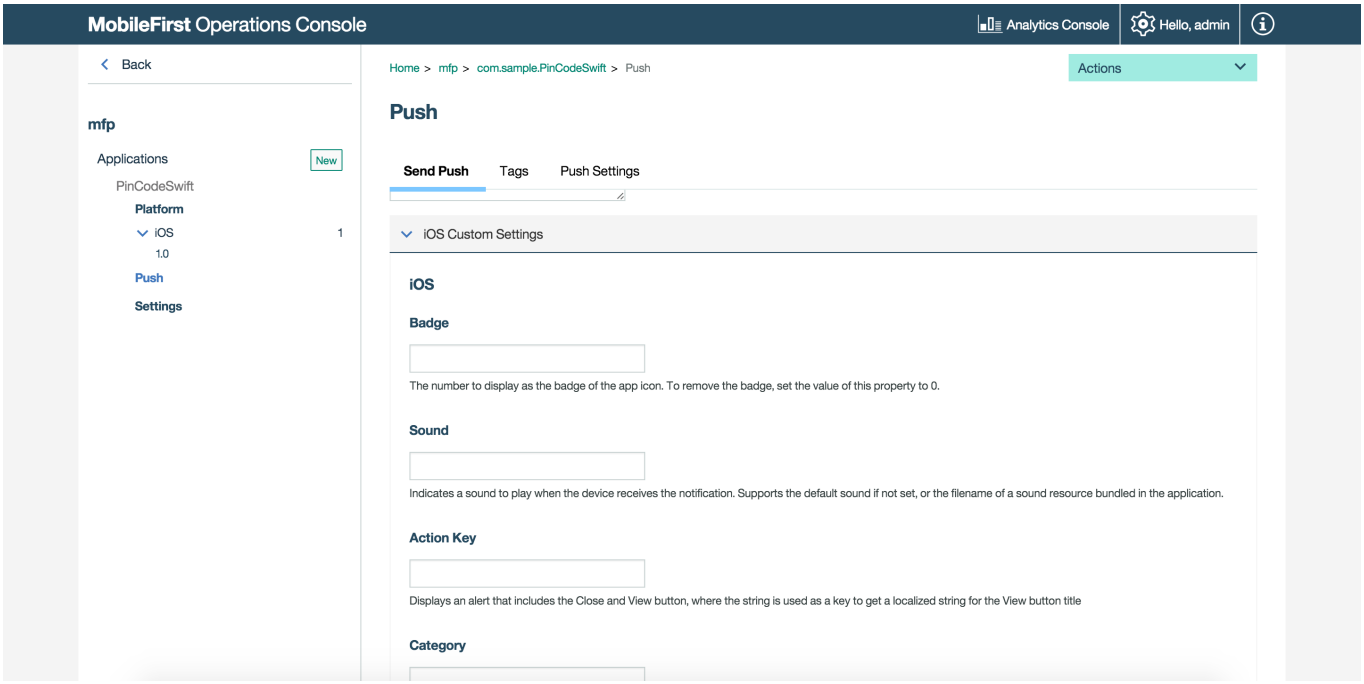
In the MobileFirst Operations Console → **[your application]** → **Push** → **Tags** → **Send Push tab**, expend the **iOS/Android Custom Settings** section to change notification attributes.

## Android

- Notification sound, how long a notification can be stored in the GCM storage, custom payload and more.
- If you want to change the notification title, then add `push_notification_tile` in the Android project's **strings.xml** file.

## iOS

- Notification sound, custom payload, action key title, notification type and badge number.




# Tutorials to follow next

With the server-side now set-up, setup the client-side and handle received notifications.

- Handling push notifications in Cordova applications (../handling-push-notifications-in-cordova)
- Handling push notifications in iOS applications (../handling-push-notifications-in-ios)
- Handling push notifications in Android applications (../handling-push-notifications-in-android)