SIGNiX Technical Document

PUSH NOTIFICATION GUIDE

V3.6
November 2020

SIGNiX

Contents

Introduction 2
Prerequisites for Implementing Notifications 3
Subscribing to Notifications 4
Request and Response Formats 5
Actions 6
Notification Failure and Retries 7
Notification Service Management 7
Setting Up Your Server 8
Push Notification Implementation Process 9
Unsuccessful Notification Testing Checklist 10
Client Responsibilities for Continued Notifications 11
References 11

Introduction

Push notifications allow SIGNiX customers to track significant events in their transactions as they happen.

In order to receive push notifications, SIGNiX customers must set up a server to accept them. The server must be configured to take requests from SIGNiX through the Internet and must offer the RESTful interface described in the sections below.
When this server receives a notification from SIGNiX, it may do whatever is required to react to the event. However, please note the following important requirement:

All push notifications must be responded to as quickly as possible, typically in no more than a few hundred milliseconds. If it is necessary to do any follow-up processing, such as downloading completed documents after receiving a complete notification, please do it *after* responding to the notifications.

Prerequisites for Implementing Notifications

- All prerequisites for B2B API Integration
- Dev Resource familiar with Server setup and URL/web pages
- A URL that SIGNiX push notifications can be sent to with an active server page that uses software to process the request and generate a response
- Server that can respond to / acknowledge push notification in timely fashion
- Server that can communicate using TLS1.2
- Your server for receiving production push notifications must support HTTPS (http is only allowable in Signix's Test environment). The server certificate must come from a widely trusted commercial certification authority. Allow at least one of the following cipher suites for SIGNiX to connect to your Server:

Cipher Suite
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Cipher Suite
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5

Subscribing to Notifications

To subscribe or unsubscribe to events, contact your SIGNiX technical representative and provide a Base URL for receiving event notifications, as described below.

If there are certain Push Notifications that you would prefer to not receive, let your SIGNiX Rep know. SIGNiX can block any/all PNs from going out for the entire account. Note that this is not available on a per transaction basis.

If you have password requirements to meet, please discuss with your SIGNiX Rep.

If you will be using a new notification receiving server, you will also need to provide its public Static IP address so we can whitelist it in our firewall. You will want to use **Port 80 for http** and **Port 443 for https** (note that Production ONLY allows for https). Any variation from those common default Ports, please let us know right away to determine best course of action.

Request and Response Formats

Your notification receiving server must offer a single-entry point for receiving notifications. SIGNiX PN requests will include your Base URL with appendage of: ? + action + the appropriate request parameters for the event.

Notification information is encoded into the following request parameters:

- **action** - The type of event that occurred. See below for valid values.
- **id** - Signix Document Set ID for the transaction in which the event occurred. Example: "id":"1494353ca93: -7d01: -6f6de9aa:2x3f39"
- **extid –** Client Transaction ID for the transaction in which the event occurred. Let your SIGNiX Rep know if you cannot receive the Transaction ID as it can be turned off.
  Example: "extid":"00012345"
- **pid** - The ordinal ID of the party that caused the event. Included only for events relating to a party. Format is Pnn. Example: "pid": "P01"
- **refid** – The RefId of the party that caused the event. Included only for events relating to a party and where the <RefID> was included in the SubmitDocument for that party. Let SIGNiX Rep know if you cannot receive the RefID as it can be turned off. If you have both pid and refid, best practice is to digest refid and ignore pid.
  Example: "refid": "Signer1"
- **ts** - The time the event occurred. Reported in "yyyy-MM-dd'T'HH:mm:ss" format default of Eastern time zone. Let your SIGNiX Rep know if you need a different time zone.
  Example: "ts":"2014-10-24T15:44:19"

There is no message content in the requests. All the information supplied by the notification is in the URL.

!! IMPORTANT !!

When you have successfully received a push notification, return HTTP status code 200 OK. In addition to the 200 OK code, please include text of "OK" as content in the response. The response should have no content other than "OK".

Any other status code will indicate some type of failure. There are no exceptions to this rule, and integrations will be rejected if this process is not followed.

Actions

The following event types will be reported. Note that these are case-sensitive:

Send

Cause: Transaction was submitted / activated / started / resumed

Example: https://customer.com/landingpage?action=send&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&ts=2014-10-27T04:57:52

partyComplete

Cause: Party completed all their required actions.

Example: https://customer.com/landingpage?action=partyComplete&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&pid=P01&refid=Signer1&ts=2014-10-27T04:57:52

complete

Cause: Transaction completed.

Example: https://customer.com/landingpage?action=complete&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&ts=2014-10-27T04:57:52

suspend

Cause: Transaction suspended because <SuspendOnStart> = yes, Signer failed authentication, or Submitter is modifying the Transaction.

Example: https://customer.com/landingpage?action=suspend&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&ts=2014-10-27T04:57:52

cancel

Cause: Transaction cancelled because Signer Opted Out & chose "Cancel" or Submitter cancelled it.

Example: https://customer.com/landingpage?action=cancel&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&ts=2014-10-27T04:57:52

expire

Cause: Transaction expired.
Example: https://customer.com/landingpage?action=expire&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&ts=2014-10-27T04:57:52

partyOptedOut

Cause: Party has opted out of the Transaction and chose a reason that cancels that Transaction.
Example: https://customer.com/landingpage?action=partyOptedOut&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&pid=P01&refid=Seller&ts=2014-10-27T04:57:52

partyNotificationFailed

Cause: A Party's email bounced.
Example: https://customer.com/landingpage?action=partyNotificationFailed&id=1495076a37d:-6cb8:-4f127ef3:2x3f39&extid=00012345&pid=P01&refid=Seller&ts=2014-10-27T04:57:52

Notification Failure and Retries

If SIGNiX fails to receive an "OK" response within a short timeout period, it will consider the request as failed. Failed requests are queued for re-sending. Every few minutes, SIGNiX will retry the request at the head of the resend queue. If it succeeds, the next queued request will be retried and so on. If there is another failure, retrying stops until the beginning of the next retry period. Please note that until we receive an "OK" response on the PN we retry, all of your other PNs going to same URL will be queued behind the first one. Until that PN succeeds, all of your PNs will essentially be blocked. This does not affect other Clients' PNs as their PNs will be thrown in front of the failing PNs since they'll be pointing to different URLs. We reserve the right to stop doing retries after 3 or more attempts.

Notification Service Management

Push Notifications are designed to rapidly deliver small messages to inform your workflow. Please note and accommodate the following behaviors in your implementation. SIGNiX monitors for system misuse and reserves the right to suspend or terminate service if specified behaviors are not followed.

1. Respond to all push notifications within a few hundred milliseconds.

2. SIGNiX will make a good faith attempt to send push notifications as events occur in real time.

3. If the initial send attempt fails, SIGNiX will attempt to resend a notification 5 minutes later. Note that this delay may cause you to receive the notification out of order if another subscribed event occurs for that transaction before the resend.

4. SIGNiX may attempt to make more than one resend attempt at its discretion. Each attempt is at least 5 minutes after the previous attempt. Attempts may stop after the 3rd failed/rejected PN.

5. SIGNiX will timeout (fail) a send attempt after no less than 5 seconds and no more than 30 seconds (exact timing modifiable at SIGNiX's discretion) if it does not receive the correct acknowledgement as described above from your server. SIGNiX expects a sent request to be immediately acknowledged, and we strongly recommend handling notification response asynchronously from other processing.

6. Occasional failures are somewhat common and are handled as in note 2 as we could be sending many thousands or millions of notifications per day. Substantive outages such as all notifications failing must be handled more critically. In these cases, SIGNiX may reasonably choose to temporarily disable notifications until your system has recovered its ability to receive. The client may request regeneration or resend and SIGNiX may be able to accommodate that request but we do not offer a response time guarantee and we may respond to these requests on a case by case, customized basis.

7. Since occasional failures are common, and are retried automatically, SIGNiX does not notify clients of occasional push failures. We will only notify you in the case of a substantial failure event, such as all or most of your pushes failing. Such outage notifications will occur through normal support communication channels.

8. SIGNiX will need to know the IP address or range of IP addresses for your notification receiving URLs so that they can be whitelisted in our firewall.

9. In the future, we may choose to include content in the notification message. SIGNiX recommends that you write your notification processing code so that content in the message does not cause regression issues.

10. Current push notifications focus on transactions. In the future, SIGNiX may make notifications available for additional events.

Setting Up Your Server

You may implement your notification receiving server using any technology you choose, however, SIGNiX may only be able to help troubleshoot with a RESTEasy setup. Most of our users have had success using a receiving server, written in Java, for the JBoss Application Server with RESTEasy framework. Here are some items that might help you in getting setup:

You can read more about and see examples for how to use Resteasy:
http://resteasy.jboss.org/

Access RESTEasy JAX-RS User Guide:
http://docs.jboss.org/resteasy/docs/3.0.17.Final/userguide/html_single/index.html

As you set up, few things to keep in mind:

- ✓ Push Notifications uses GET method
- ✓ In Webtest, SIGNiX accepts both **HTTP (Port 80)** and **HTTPS (Port 443)** Base URL
- ✓ In Production, SIGNiX only accepts **HTTPS (Port 443)** Base URL
- ✓ Static IP Addresses are currently required. If that is not possible, SIGNiX can clear your domain name instead.
- ✓ In Production and Webtest, SIGNiX is currently using TLS1.2
- ✓ URLs are case-sensitive and the PN entered at SIGNiX must match your URL exactly. When providing SIGNiX with the Base URL, make sure to check that it is an exact duplicate
- ✓ Your URL must have a landing page/active server page after the Domain as SIGNiX needs a target page when sending the URL. For example,
  Your URL: https://ABCCompany.hfc.comcastbusiness.com

  Then, include the landing/target page name such as "landingpage", "landingpage.aspx", "Index.jsp", etc.

  And provide SIGNiX a full Base URL. Here are some examples:

  https://ABCCompany.hfc.comcastbusiness.com/index.aspx

  https://ABCCompany.hfc.comcastbusiness.com/PushNotifications

  https://ABCCompany.hfc.comcastbusiness.com/PushNotifications/index.aspx

  https://ABCCompany.hfc.comcastbusiness.com/PushNotifications.aspx

  https://ABCCompany.hfc.comcastbusiness.com/PushNotifications.jsp

Push Notification Implementation Process

1. Code your push notification receiving server and set it up on a test platform. Provide the URL of the server to SIGNiX, and also provide the public IP addresses of the server or servers associated with these URLs. ***Make sure your firewall will allow incoming requests from the Internet from the SIGNiX test platform. The SIGNiX test platform is at IP address 52.34.103.46 (webtest.signix.biz).***
2. Submit test transactions to the SIGNiX test platform, and check that you receive and properly manage each push notification. Let SIGNiX know of testing status and results.
3. SIGNiX will confirm that each push notification is accepted in under 1 second.
4. Once ALL push notifications have been successfully tested and your Integration has gone through our Go-Live Review process, you may deploy your software to your production platform. Provide SIGNiX with the production Base URLs and the IP addresses of the corresponding production servers. ***Make sure your firewall will allow incoming requests from the Internet from the SIGNiX production platform. The SIGNiX production platform is at IP address 50.56.20.60 (www.signix.net).***

5. Submit a few test transactions to the SIGNiX production platform and check that the results match the results from the test system. Let SIGNiX know of testing status and results.
6. SIGNiX will confirm that each push notification is accepted in under 1 second.

In order to ensure that push notifications come from SIGNiX, it is recommended that receivers of push notifications filter incoming requests by origin IP address, or implement a supported type of client authentication on push notification requests, as described in "Authenticating SIGNiX as an HTTP/HTTPS Client".

Unsuccessful Notification Testing Checklist

If you are not receiving push notifications from SIGNiX, please go down the checklist with your team and confirm you have all of the following confirmed before contacting your SIGNiX Rep. SIGNiX will then provide you with any errors spotted in your test transaction, when possible, and provide resolution suggestions when possible. Client and SIGNiX will work together to resolve any PN issue but Client is required to follow each suggestion and provide feedback in a timely fashion as well as provide the appropriate dev resources to help resolve when necessary.

- ✓ Your server is Live
- ✓ URL provided to SIGNiX matches actual URL
  - No spelling errors
  - No spaces and no additional or missing text/characters
  - Capitalization is correct for each letter
- ✓ You provided SIGNiX all of the IP addresses associated with your server for Webtest/Production
- ✓ Your IP address is not dynamic (could have updated to an unknown address for SIGNiX)
- ✓ It is true that Client has had no Server or Domain Name updates/changes
- ✓ You cleared/whitelisted SIGNiX's IP address for Webtest/Production
- ✓ You have at least 1 of SIGNiX's cipher suites
- ✓ The URL leads to an active server page that can process SIGNiX notifications.
- ✓ Your server knows and can digest the full PN Request sent by SIGNiX – including any variation per event in the appended transaction info
- ✓ Your URL is set up for ASPX or HTML but not Both
- ✓ Your URL's Header is set to application/JSON
- ✓ Your Server is configured to RESTful interface
- ✓ Your Server is configured to handle 'GET' requests
- ✓ It is true that you do not have an 'Idle Time-Out' set to 0 on your Server
- ✓ You are using Port 80 for 'http' or Port 443 for 'https'
- ✓ It is true that you did not apply a Password/Permission without letting SIGNiX know
- ✓ Check that your SSL certs are set up correctly on your server (i.e. all intermediate certificates are present, etc.). Check your site via an SSL testing page such as: https://www.ssllabs.com/ssltest/index.html
- ✓ You have SIGNiX's Root Cert in your Trust Store
  - Go to https://webtest.signix.biz.
  - Click on the padlock in the address bar
  - Click on "details" (different depending on browser)

- Look for "view certificate" button
- Click on "certification path" and then select root and/or intermediate cert(s)
- Click "view certificate" and then find "copy to file"

✓ If all of the above have been answered 'YES', contact your SIGNiX Rep and be prepared to share the following:

- Your Server's Root Certs

Client Responsibilities for Continued Notifications

Let your SIGNiX Rep know if you plan on doing any of the following after successful push notification setup. Please note that SIGNiX will attempt to honor any request asap but advance notice is required in order to meet your timelines. We cannot guarantee a fast turn-around and your integration might be affected with push notifications not being received and your flow breaking because of it.

✓ Updates to SSL Server Certificates
✓ Receiving server IP address changes

References

Clients are provided the following docs/files and latest versions are available on SIGNiX's Development site:

https://www.signix.com/devcommunity

☐ "SIGNiX Interface Guide" - Interface Specifications (aka "**B2BSpec/** SIGNiX B2B SDK")

☐ Within **"PushNotificationTools"** zip File**:**

PDFs:
- ✓ **"SIGNiX Push Notification Guide"** – *All you need to know to get ready to accept PNs*
- ✓ **"SIGNiX Authenticated as HTTP Client" -** *Provides information on security around PNs.*

Files:
- ✓ **Response.java -** *Will help you with creating response to SIGNiX's PN*