

# Migrate Personal Mobile Profiles from Hybrid Access Gateway to Personal Messaging

Migration Instructions

v1.3 – 24.01.2019

### **Important Notice**

Starting with Hybrid Access Gateway 5.12 the existing functionality to communicate with Personal Mobile profiles will stop working!

Nexus recently introduced the Personal Messaging that needs to be deployed as a separate service on premise to continue with Personal Mobile registration, authentication and signing. Furthermore, a migration of existing Personal Mobile profiles from HAG to Personal Messaging is required.

If you are not using Personal Mobile for authentication or signing you could ignore this document.

### **Important Notice**

This document describes the migration for Hybrid Access Gateway version 5.13.0. If you want to migrate to version 5.12.0 please check Nexus Doc for the corresponding document.

This document and the software described in it are copyrighted

© 2019 Technology Nexus AB. All rights reserved.

All other trademarks and service marks are the property of their respective owners.

Information in this document is subject to change without prior notice.

### Version Notes

Version	Date	Reason for Change	Chapter	Responsible
1.0	29.03.2018	Initial Version		B. Zeuner
1.1	11.04.2018	Added further prerequisites		B. Zeuner
1.2	16.04.2018	Added Important Notice and description for fields that are required to connect to Personal Messaging		B. Zeuner
1.3	24.01.2019	Made changes related to HAG 5.13.1 release		B. Zeuner

## Table of Contents

Table of Contents .....	4
1 Introduction .....	5
2 Install Personal Messaging .....	6
3 Migrate Data from HAG to Nexus Personal Messaging or Nexus GO Messaging .....	7
3.1 Prerequisites .....	7
3.2 Step-by-step instruction.....	7
3.2.1 Export Data from HAG.....	7
3.2.2 Import Data to Personal Messaging.....	7
3.2.3 Import Data to Nexus GO Messaging.....	7
4 Setup Personal Messaging in HAG .....	8
4.1 Prerequisites .....	8
4.2 Step-by-step instruction.....	8
4.2.1 Connect Personal Messaging to HAG.....	8
4.2.2 Add CA certificate.....	9
5 Setup Nexus GO Messaging in HAG .....	10
5.1 Prerequisites .....	10
5.2 Step-by-step instruction.....	10
5.2.1 Connect Nexus GO Messaging to HAG .....	10

## 1 Introduction

Starting with Hybrid Access Gateway 5.12 Nexus will introduce a new way of communicating with Personal Mobile:

The **Nexus Personal Messaging**.

The Personal Messaging is a web-based service for online authentication and signing using Nexus Personal Mobile or Nexus Personal Desktop with smartcards. The Personal Messaging allows for example the same processes, APIs, and workflows to be used for mobile and desktop (smart card, soft token).

In HAG versions before 5.12 the communication between Personal Mobile and HAG was direct. HAG was responsible for doing the provisioning and sending out push notification in case of authentication or signing. With the Personal Messaging this is outsourced to an own service. This brings many advantages. A few of them are mentioned here:

- Personal Messaging allows Personal Mobile profiles with certificates that can be also be used to authenticate to Hybrid Access Gateway
- Personal Mobile profiles could be issued by an external instance such as Nexus PRIME together with Nexus Certificate Manager
- HAG allows authentication with Personal Mobile profiles that were not issued by HAG. All based on certificate trust
- The communication with Personal Mobile could now be built in high availability mode (see <https://doc.nexusgroup.com/display/PUB/High+availability+architecture+for+Personal+Messaging> for more information)

The introduction of the Personal Messaging enables certificates for Personal Mobile profiles to increase the security and enables even more use cases with Personal Mobile. Surely not every customer is in possession of its own Certificate Authority and therefore Hybrid Access Gateway still supports the communication and provisioning of Personal Mobile profiles with raw keys. For this a migration of existing profiles from HAG to Personal Messaging is required.

Nexus offers this new way of communicating in two different flavors:

1. Nexus Personal Messaging
2. Nexus GO Messaging

Customers can choose to install it on-premise. Then it's called **Nexus Personal Messaging**. In addition, Nexus provides a cloud service with the same functionalities that can be used by customers who don't want to install it themselves. In this case, the service is called **Nexus GO Messaging**.

This document describes how to install **Nexus Personal Messaging** on-premise (chapter 2), how to migrate existing Personal Mobile profiles (chapter 3) and how to connect it to the Hybrid Access Gateway (chapter 4). At the end of the document we will describe how to use the cloud service **Nexus GO Messaging** (chapter 5).

*Note: To be able to migrate existing Personal Mobile profiles to Nexus GO Messaging, Hybrid Access Gateway 5.13.0 of above needs to be used.*

## 2 Install Personal Messaging

Please visit [Nexus Doc](#) to find the latest instructions about how to install Nexus Personal Messaging on-premise.

## 3 Migrate Data from HAG to Nexus Personal Messaging or Nexus GO Messaging

### 3.1 Prerequisites

- Personal Messaging is deployed and `server.contextPath=/` and `application.hermod.rest.uribase = /` is set
- Before doing the migration be sure that Hybrid Access Gateway is running in version 5.12 or higher
- Hybrid Access Gateway is up and running

### 3.2 Step-by-step instruction

#### 3.2.1 Export Data from HAG

1. Login to Hybrid Access Gateway administration interface and export personal profiles from HAG:
  1. Go to **Manage System > Database Service**
  2. Click on *Export Personal Mobile Data* link and start export
  3. After export completes, the *backupdata.sql* file is generated and offered for download. This *backupdata.sql* file contains information of existing profiles on HAG. These are the fields that will be exported from the HAG database:
    1. user\_id
    2. message-box-id
    3. access-token
    4. validity time

*Note: Key information (public key) will not be exported to Personal Messaging, HAG will also keep personal profile information along with profile key.*

#### 3.2.2 Import Data to Personal Messaging

1. Connect to the database that Personal Messaging is supposed to use. Any database administration GUI can be used, like for PostgreSQL we can use pgAdmin
2. Execute the SQL statement in downloaded file *backupdata.sql* on Personal Messaging's database. This will populate the database with all Personal Mobile profiles which were present in HAG

#### 3.2.3 Import Data to Nexus GO Messaging

To migrate existing Personal Mobile profiles to the Nexus GO Messaging service please contact Nexus Support.



## 4 Setup Personal Messaging in HAG

### 4.1 Prerequisites

- The migration of Personal Mobile profiles is done

### 4.2 Step-by-step instruction

#### 4.2.1 Connect Personal Messaging to HAG

1. Login to the Hybrid Access Gateway administration interface and go to **Manage System > Policy Service**
2. Click on **Manage Global Policy Service Settings...**
3. Check **Enable Provisioning**
4. Configure Personal Messaging URL, Image API URL, X API Key and Personal Messaging Public URL (refer help page)
5. Save the changes

#### Image: Configuration of Personal Messaging in HAG

##### Provisioning Settings

Enter provisioning settings for use by Personal Mobile, that will apply to all Policy Services. See Online Help page how to configure these and the required callback URL in Personal Messaging.

Enable Provisioning

Personal Messaging URL

Personal Messaging Callback URL

Image API URL

X API Key

*X API key stored*

Personal Messaging Public URL

Attestation Key  No file chosen

*Attestation Key Stored*

Issuer

Initial Messaging TTL  seconds

Self Service Messaging TTL  seconds

Challenge Length

Field Name	Description
Personal Messaging URL	The URL to the Personal Messaging REST Command API which is used for provisioning, authentication and signing. This must be a publicly reachable URL; the following



	<p>configuration assumes that Personal Messaging is set up as a web resource and given a <b>Reserved DNS Mapping</b>, with these publicly accessible paths:</p> <ul style="list-style-type: none"> <li>• <i>personalmessaging/rest/command/</i></li> <li>• <i>personalmessaging/rest/ms</i></li> </ul> <p>The default URL's path component assumes the following Personal Messaging configuration:</p> <ul style="list-style-type: none"> <li>• <i>server.contextPath: /personalmessaging</i></li> <li>• <i>application.personalmessaging.rest.uribase: /rest</i></li> <li>• <i>application.personalmessaging.messageServerLibrary.publicUrl: https://&lt;personalmessaging-public-host&gt;/personalmessaging/rest/ms</i></li> <li>• <i>application.personalmessaging.cors.pathPatterns: '/rest/ms,/rest/ms/**'</i></li> </ul> <p>Set to <i>https://messaging.service.go.nexusgroup.com/command/</i> by default.</p>
Personal Messaging Callback URL	<p>The URL to the Policy Service REST Callback API, Personal Messaging server uses this URL for sending callback response to the Hybrid Access Gateway. This URL needs to be configured in Personal Messaging server as callback URL. The DNS part of URL must be replaced with actual DNS of Access Point service in Hybrid Access Gateway.</p>
Image API URL	<p>The URL to the Distribution Service REST Image API which is used for fetching images to be displayed during authentication when using Personal Mobile. This must be a publicly reachable URL; the default path assumes that Personal Messaging is set up as a web resource and given a <b>Reserved DNS Mapping</b>, with this publicly accessible path:</p> <ul style="list-style-type: none"> <li>• <i>distribution-service/image/v1/rest/image</i></li> </ul> <p>Set to <i>https://&lt;access-point-public-host&gt;/https/distribution-service/image/v1/rest/image</i> by default.</p>
X API Key	<p>X API key is API key of personal messaging server. This value is used to connect to personal messaging server.</p>
Personal Messaging public URL	<p>The public URL of Personal Messaging will be used to redirect poll request of personal app to Personal Messaging server. HAG will send response code 308 along with personal messaging public URL as response of personal poll. Once personal app received this URL, app will start polling to Personal Messaging server. This is only required when upgrading from Hybrid Access Gateway prior to 5.12 version and it has active personal profiles. Below are the examples for Nexus Go Messaging cloud service and on-premise Personal Messaging server:</p> <ul style="list-style-type: none"> <li>• For Nexus GO Messaging: <i>https://messaging.service.go.nexusgroup.com/personalmessaging/rest/ms</i></li> <li>• For Personal Messaging (on-premise): <i>https://&lt;personalmessaging-public-host&gt;/personalmessaging/rest/ms</i></li> </ul> <p>Not set by default.</p>

#### 4.2.2 Add CA certificate

The corresponding CA certificate for Personal Messaging must be uploaded in HAG. To upload CA, go to **Manage System > Certificates > Add Certificate Authority**

## 5 Setup Nexus GO Messaging in HAG

### 5.1 Prerequisites

- The customer has requested an account for Nexus GO Messaging from Nexus Support by providing the callback URL. Together with the account the customer will receive a X API Key

### 5.2 Step-by-step instruction

#### 5.2.1 Connect Nexus GO Messaging to HAG

- Login to the Hybrid Access Gateway administration interface and go to **Manage System > Policy Service**
- Click on **Manage Global Policy Service Settings...**
- Check **Enable Provisioning**
- Configure Personal Messaging URL, Image API URL, X API Key and Personal Messaging Public URL (refer help page)
- Save the changes

**Image: Configuration of Nexus GO Messaging in HAG**

#### Provisioning Settings

Enter provisioning settings for use by Personal Mobile, that will apply to all Policy Services. See Online Help page how to configure these and the required callback URL in Personal Messaging.

Enable Provisioning

Personal Messaging URL

Personal Messaging Callback URL

Image API URL

X API Key

*X API key stored*

Personal Messaging Public URL

Attestation Key  No file chosen

*Attestation Key Stored*

Issuer

Initial Messaging TTL  seconds

Self Service Messaging TTL  seconds

Challenge Length

Field Name	Description
------------	-------------



Personal Messaging URL	<p>The URL to the Nexus GO Messaging REST Command API which is used for provisioning, authentication and signing.</p> <p>Set to <i>https://messagingservice.go.nexusgroup.com/command/</i> by default. This value doesn't need to be changed if Nexus GO Messaging should be used.</p>
Personal Messaging Callback URL	<p>The URL to the Policy Service REST Callback API, Nexus GO Messaging server uses this URL for sending callback response to the Hybrid Access Gateway. This URL needs to be configure in Nexus GO Messaging server as callback URL. The DNS part of URL must be replaced with actual DNS of Access Point service in Hybrid Access Gateway.</p> <p>Customers need to provide this URL to Nexus Support to order an account for Nexus GO messaging.</p>
Image API URL	<p>The URL to the Distribution Service REST Image API which is used for fetching images to be displayed during authentication when using Personal Mobile. This must be a publicly reachable URL; the default path assumes that Nexus GO Messaging is set up as a web resource and given a <b>Reserved DNS Mapping</b>, with this publicly accessible path:</p> <ul style="list-style-type: none"> <li>• <i>distribution-service/image/v1/rest/image</i></li> </ul> <p>Set to <i>https://&lt;access-point-public-host&gt;/https/distribution-service/image/v1/rest/image</i> by default.</p>
X API Key	<p>X API key is API key of Nexus GO Messaging server. This value is used to connect to Nexus GO Messaging server.</p> <p>Customers will receive this value together with the Nexus GO Messaging account.</p>
Personal Messaging public URL	<p>The public URL of Nexus GO Messaging will be used to redirect poll request of personal app to Nexus GO Messaging server. HAG will send response code 308 along with Nexus GO Messaging public URL as response of personal poll. Once personal app received this URL, app will start polling to Nexus GO Messaging server. This is only required when upgrading from Hybrid Access Gateway prior to 5.12 version and it has active personal profiles. Below are the examples for Nexus Go Messaging cloud service and on-premise Nexus GO Messaging server:</p> <ul style="list-style-type: none"> <li>• For Nexus GO Messaging: <i>https://messagingservice.go.nexusgroup.com/personalmessaging/rest/ms</i></li> </ul> <p>Not set by default.</p>