Mobile Login Requests (Push Notifications) Registration Method for 2-Factor Authentication
Introduction

Use this guide to configure and register mobile devices to use Push Notifications as a 2-Factor Authentication registration method.

SecureAuth IdP supports two (2) types of Push options for 2-Factor Authentication: Push Notification (alert) and Push-to-Accept.

The **Push Notification** alert message is sent directly to a mobile device and includes a one-time passcode (OTP) to use during the 2-Factor Authentication workflow. **Push-to-Accept** sends a login request to a mobile device that prompts the end-user to Accept or Deny access.

To use either of these Push options, the Push Notifications functionality must be enabled in all realms designated to offer the option, and end-users must register their mobile device(s) to receive the notifications before utilizing the registration method during login.

When end-user Push Notification requests are submitted, SecureAuth IdP builds a tunnel using Apple APN and Google GCM services to distribute custom messages to registered mobile devices.
Prerequisites

1. Download the SecureAuth IdP Mobile OTP App from the Google Play Store or Apple App Store

<table>
<thead>
<tr>
<th>Device</th>
<th>Download URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td><a href="https://itunes.apple.com/us/app/secureauth-otp/id615536686">https://itunes.apple.com/us/app/secureauth-otp/id615536686</a></td>
</tr>
</tbody>
</table>

NOTE: See SecureAuth Compatibility Guide for a list of supported, compatible mobile devices

2. Configure the **SecureAuth App Enrollment Realm** where end users can register their device(s) for Push Notification

3. Create a **New Realm** or access existing realm(s) in the SecureAuth IdP Web Admin to which the Push Notification will be applied (Realm A in the SecureAuth IdP Configuration Steps)

(OPTIONAL) 4. Create a **New Realm** or access an existing realm in the SecureAuth IdP Web Admin that is configured for the **Account Management** page (help desk) to enable administrator Push Notification enrolled device(s) revocation (Realm B in the SecureAuth IdP Configuration Steps)

(OPTIONAL) 5. Create a **New Realm** or access an existing realm in the SecureAuth IdP Web Admin that is configured for the **Self-service Account Update** (end user self service) to enable end user Push Notification enrolled device(s) self-revocation (Realm C in the SecureAuth IdP Configuration Steps)

6. Configure the following tabs in the Web Admin before configuring Push Notifications (and Account Management Page and Self-service Account Update):
   - **Overview** – the description of the realm and SMTP connections must be defined
   - **Data** – an enterprise directory must be integrated with SecureAuth IdP
   - **Workflow** – the way in which users will access the target must be defined
   - **Registration Methods** – other 2-Factor Authentication methods that will be used to access the target (if any) must be defined
   - **Post Authentication** – the target resource or post authentication action must be defined (see Realm B and Realm C for specific Post Authentication configurations for Account Management Page and Self-service Account Update)
   - **Logs** – the logs that will be enabled or disabled for this realm must be defined

SecureAuth IdP Configuration Steps

Realm A

Data
<table>
<thead>
<tr>
<th>Property</th>
<th>Source</th>
<th>Field</th>
<th>Data Format</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Default Provider</td>
<td>memberOf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td>Default Provider</td>
<td>givenName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td>Default Provider</td>
<td>sn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone 1</td>
<td>Default Provider</td>
<td>telephoneNumber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone 2</td>
<td>Default Provider</td>
<td>mobile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone 3</td>
<td>Default Provider</td>
<td>homePhone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone 4</td>
<td>Default Provider</td>
<td>pager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Default Provider</td>
<td>audio</td>
<td>Plain Binary</td>
<td></td>
</tr>
<tr>
<td>Push Notification Tokens</td>
<td>Default Provider</td>
<td>jpegPhoto</td>
<td>Plain Binary</td>
<td></td>
</tr>
<tr>
<td>OATH Tokens</td>
<td>Default Provider</td>
<td>postalAddress</td>
<td>Plain Binary</td>
<td></td>
</tr>
<tr>
<td>Access Histories</td>
<td>Default Provider</td>
<td>photo</td>
<td>Plain Binary</td>
<td></td>
</tr>
</tbody>
</table>
In the Membership Connection Settings section, map a directory field to the Push Notification Tokens Property.

In typical AD deployments, the Data Format is Plain Binary and the jpegPhoto directory field is utilized.

1. Check Writable

The Push Notification Tokens Property can be stored as Plain Binary or in JSON format, and has distinct requirements for the LDAP directory attribute mapped to the Property based on the Data Format selection.

For Plain Binary, these requirements must be met for the directory field that contains the Push Notification Token:

- **Length**: 4096 minimum
- **Data Type**: Octet string (bytes)
- **Multi-valued**

For JSON, these requirements must be met for the directory field that contains the Push Notification Token:

- **Length**: 4096 minimum
- **Data Type**: DirectoryString
- **Multi-valued**

Click Save once the configurations have been completed and before leaving the Data page to avoid losing changes.

NOTE: For SQL, ASP.net, and Oracle data stores, only the Plain Binary Data Format is supported (configured in the Data tab); and for ODBC data stores, Push is not supported.
3. In the **Registration Configuration** section, under **Mobile Login Requests (Push Notifications)**, select **Passcode (OTP), Accept / Deny, or Passcode (OTP) + Accept / Deny** from the **Request Type** dropdown
   - **Passcode (OTP):** Enable Push Notifications to enrolled mobile devices
   - **Accept / Deny:** Enable Push-to-Accept requests to enrolled mobile devices
   - **Passcode (OTP) + Accept / Deny:** Enable Push Notifications and Push-to-Accept requests to enrolled mobile devices (both options appear on client-side login page)

4. If **Accept / Deny** or **Passcode (OTP) + Accept / Deny** is selected in step 3, then set the **Login Request Timeout** to determine the number of minutes during which the Push-to-Accept request is valid

5. If **Accept / Deny** or **Passcode (OTP) + Accept / Deny** is selected in step 3, then set the **Company Name**, which appears on the Push-to-Accept request

6. If **Accept / Deny** or **Passcode (OTP) + Accept / Deny** is selected in step 3, then set the **Application Name** to a descriptive name / phrase, which appears on the Push-to-Accept request

7. Set the **Device Max Count** to -1 if there is no limit to the number of devices that can be enrolled for Push Notifications
   
   To establish a limit, set the maximum number of devices that can be enrolled for Push Notifications

8. If a max count is set, select **Allow to replace** from the **When exceeding max count** dropdown if end users can replace existing enrolled devices with newer ones

9. If a max count is set and **Allow to replace** is selected in step 8, then select **Created Time** from the **Replace in order by** dropdown to replace the oldest enrolled device with the newest one
   
   Select **Last Access Time** to replace the least recently used enrolled device with the newest one
Realm B

These are optional configuration steps to enable administrator (help desk) revocation of Push Notification enrolled device(s).

This realm must be set up for the Account Management page post authentication action.

Refer to Account Management (Help Desk) Page Configuration Guide for more information.

Data

1. Follow steps 1-2 in the Data configuration steps of Realm A.

   The directory attribute used for Push Notification Tokens (e.g. jpegPhoto) must be the same across all SecureAuth IdP realms utilizing Push Notifications / Push-to-Accept Login Requests to ensure consistency.

Post Authentication

2. In the Post Authentication section, select Account Management from the Authenticated User Redirect dropdown.

   Click Save once the configurations have been completed and before leaving the Post Authentication page to avoid losing changes.

Identity Management

3. Click Configure help desk page to enable or disable help desk functions.

   Help Desk
<table>
<thead>
<tr>
<th>SecureAuth Field</th>
<th>Display Type</th>
<th>Datastore Fieldname</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name:</td>
<td>Show Enabled</td>
<td>givenName</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name:</td>
<td>Show Enabled</td>
<td>sn</td>
<td>Last Name</td>
</tr>
<tr>
<td>Phone 1:</td>
<td>Show Enabled</td>
<td>telephoneNumber</td>
<td>Phone 1</td>
</tr>
<tr>
<td>Phone 2:</td>
<td>Show Enabled</td>
<td>mobile</td>
<td>Phone 2</td>
</tr>
<tr>
<td>Phone 3:</td>
<td>Show Enabled</td>
<td>homePhone</td>
<td>Phone 3</td>
</tr>
<tr>
<td>Phone 4:</td>
<td>Show Enabled</td>
<td>pager</td>
<td>Phone 4</td>
</tr>
<tr>
<td>Email 1:</td>
<td>Show Enabled</td>
<td>mail</td>
<td>Email 1</td>
</tr>
<tr>
<td>Email 2:</td>
<td>Show Enabled</td>
<td>WWWHomePage</td>
<td>Email 2</td>
</tr>
<tr>
<td>Email 3:</td>
<td>Show Enabled</td>
<td>physicalDeliveryOfficeName</td>
<td>Email 3</td>
</tr>
<tr>
<td>Email 4:</td>
<td>Show Enabled</td>
<td>facsimileTelephoneNumber</td>
<td>Email 4</td>
</tr>
<tr>
<td>OATH Seed:</td>
<td>Hide</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>Digital Fingerprints:</td>
<td>Show Enabled</td>
<td>audio</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>jpegPhoto</td>
<td></td>
</tr>
<tr>
<td>Push Notification Devices:</td>
<td>Show Enabled</td>
<td></td>
<td>Push notification devices (uncheck to remove)</td>
</tr>
<tr>
<td>OATH OTP Devices:</td>
<td>Hide</td>
<td>postalAddress</td>
<td></td>
</tr>
<tr>
<td>Password Reset:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlock User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable/Disable User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Select **Show Enabled** from the **Push Notification Devices** dropdown to show this function on the help desk page and enable administrative revocation of enrolled devices.

Digital Fingerprints (Uncheck to revoke)
- Windows 7 - Chrome 46.0.2490: 11/23/2015 10:45:20 AM

Push notification devices (uncheck to remove)

Update Reset

Data was updated successfully.

!! Click **Save** once the configurations have been completed and before leaving the **Help Desk** page to avoid losing changes.

---

**Realm C**

These are *optional* configuration steps to enable end user self-service revocation of Push Notification enrolled device(s)

This realm must be set up for the **Self-service Account Update** post authentication action

Refer to [Self-service Account Update page configuration](#) for more information

---

**Data**

1. Follow steps 1-2 in the **Data** configuration steps of **Realm A**

   The directory attribute used for Push Notification Tokens (e.g. **jpegPhoto**) *must be the same* across all SecureAuth ldP realms utilizing Push Notifications / Push-to-Accept Login Requests to ensure consistency.
2. Select **Self Service Account Update** from the **Authenticated User Redirect** dropdown in the **Post Authentication** tab in the Web Admin.

⚠️ Click **Save** once the configurations have been completed and before leaving the **Post Authentication** page to avoid losing changes.

3. Click **Configure self service page** to enable or disable self-service functions.
<table>
<thead>
<tr>
<th>SecureAuth Field</th>
<th>Display Type</th>
<th>Datastore Fieldname</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name:</td>
<td>Show Enabled</td>
<td>givenName</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name:</td>
<td>Show Enabled</td>
<td>sn</td>
<td>Last Name</td>
</tr>
<tr>
<td>Phone 1:</td>
<td>Show Enabled</td>
<td>telephoneNumber</td>
<td>Phone 1</td>
</tr>
<tr>
<td>Phone 2:</td>
<td>Show Enabled</td>
<td>mobile</td>
<td>Phone 2</td>
</tr>
<tr>
<td>Phone 3:</td>
<td>Show Enabled</td>
<td>homePhone</td>
<td>Phone 3</td>
</tr>
<tr>
<td>Phone 4:</td>
<td>Show Enabled</td>
<td>pager</td>
<td>Phone 4</td>
</tr>
<tr>
<td>Email 1:</td>
<td>Show Enabled</td>
<td>mail</td>
<td>Email 1</td>
</tr>
<tr>
<td>Email 2:</td>
<td>Show Enabled</td>
<td>WWW-HomePage</td>
<td>Email 2</td>
</tr>
<tr>
<td>Email 3:</td>
<td>Show Enabled</td>
<td>physicalDeliveryOfficeName</td>
<td>Email 3</td>
</tr>
<tr>
<td>Email 4:</td>
<td>Show Enabled</td>
<td>facsimileTelephoneNumber</td>
<td>Email 4</td>
</tr>
<tr>
<td>OATH Seed:</td>
<td>Hide</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>Digital Fingerprints:</td>
<td>Show Enabled</td>
<td>audio</td>
<td>Digital Fingerprints (Unclear)</td>
</tr>
<tr>
<td>Push Notification Devices:</td>
<td>Show Enabled</td>
<td>jpegPhoto</td>
<td>Push notification devices (uncheck to remove)</td>
</tr>
<tr>
<td>OATH OTP Devices:</td>
<td>Hide</td>
<td>postalAddress</td>
<td></td>
</tr>
<tr>
<td>Password React:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlock User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable/Disable User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete User:</td>
<td>Hide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Select **Show Enabled** from the **Push Notification Devices** dropdown to show this function on the help desk page and enable self-revocation of enrolled devices.

**Digital Fingerprints (Uncheck to revoke)**
- **Windows 7 - Chrome 46.0.2490:** 11/23/2015 10:45:20 AM

**Push notification devices (uncheck to remove)**
- **iPod touch:** 11/24/2015 10:14:46 AM; 11/25/2015 9:09:12 AM

[Buttons: Update, Reset]

- **Data was updated successfully.**

---

**End-user Experience**

End-users must enroll their mobile devices (**Authenticate App**) in the **SecureAuth App Enrollment Realm** to use Push Notification and / or Push-to-Accept as Multi-Factor Authentication methods.

**NOTE:** Workflows for Authenticate App versions 5.0 and 4.x differ due to architectural changes in the app. Refer to the sample images for the version of the app installed – **v5.0** or **v4.x** – for the specified type of Push Notification.
In **SecureAuth IdP v9.0.2+**, when the end-user is presented the page of Multi-Factor Authentication methods from which to choose, the Multi-Factor Authentication method that was last selected and used in a successful login attempt persists as the default method for the next login in each device / browser.

**Passcode (OTP) Request Type (Push Notification)**

1. When logging on a SecureAuth IdP realm in which the Passcode (OTP) Push Notification login request type is enabled, the **Push Notification** choice appears in the Multi-Factor Authentication methods list.

2. Select **Send passcode** and click **Submit**.

3. A passcode Push Notification is delivered to the app on the enrolled device, displayed on the home screen, with the OTP.
SecureAuth now
Your one time password is 1039,
Ota.
slide to view
Accept / Deny Request Type (Push-to-Accept)

1. When logging on a SecureAuth IdP realm in which the Accept / Deny Push Notification login request type is enabled, the **Push-to-Accept** choice appears in the Multi-Factor Authentication methods list.

2. Select **Send login request** and click **Submit**.

3. A Push-to-Accept request is delivered to the enrolled app on the device, ready for the end-user's approval or denial response on the app.

If the end-user does not respond to the request within the configured time period:

- “The request has expired” message appears on the app.
- “The login request is no longer valid” message appears on the realm page along with the link “Please click here to use an alternate verification method.”
Push-to-Accept Images Example (v5.0)

When the notification is sent to the app...

If the app is closed

4a. Swipe down on the login request notification

5a. Tap Accept to obtain secure access to the realm

If the app is open

4b. Tap Accept to obtain secure access to the realm
Login request. Tap to see request in app.
Login request. Tap to see request in app.

Accept

Deny
Login request from:

SecureAuth Corporation

SecureAuthApp

j smith

192.162.2.73

Approve this request

Deny this request
4. Tap (or swipe) to access the **Accept** and **Deny** options on the next screen.

5. Tap **Accept** to obtain secure access to the realm.

6. The application alerts the end-user that the Multi-Factor Authentication method has been accepted.

The expiration message appears if an **Accept** or **Deny** action is not taken within the configured time period.
SecureAuth now
Login request. Tap to see request in app.
slide to view
SA QA
User SelfService

Admin55
11:00:08 at 11/24/2015
Login Request

Accepted!
The request has expired