PingFederate®

Google Authenticator Integration Kit

Version 2.1.0

User Guide

Ping Identity®

PingFederate Google Authenticator Integration Kit *User Guide*
Version 2.1.0
May, 2018

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)
Fax: 303.468.2909
Web Site: www.pingidentity.com

Trademarks

Disclaimer

Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **May 23, 2018**.

Contents

Introduction **4**
Intended Audience 4
System Requirements 4
ZIP Manifest 5
Process Overview **6**
Installation and Configuration **7**
Install the Integration Kit 7
Install the Google Authenticator Application 9
Configure PingFederate 9
Complete the Configuration 15
Registering an Account 16

Introduction

This PingFederate Google Authenticator Integration Kit allows an enterprise to leverage its investment in the two-factor authentication service to provide secure single sign-on (SSO) for online services across Internet domains. The included Google Authenticator Adapter provides for two-factor authentication in conjunction with a first-factor PingFederate Adapter.

Note: Two-factor authentication with the Google Authenticator Integration Kit is supported only for PingFederate 8.1.2 and higher.

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of IT infrastructure. Knowledge of networking and user-management configuration is assumed. Some exposure to the PingFederate administrative console may be helpful. Please consult the documentation provided with your server tools if you encounter any difficulties in areas not directly associated with PingFederate or the Google Authenticator Integration Kit.

Additional Resources

Administrators may want to review SSO Integration Kits and Adapters in the PingFederate Administrator's Manual.

Tip: If you encounter any difficulties with configuration or deployment, please try searching the Ping Identity Support Center (www.pingidentity.com/support).

System Requirements

The following prerequisites must be met to implement this Kit:

- PingFederate 8.2.2.0 or higher
- Third-party Google Authenticator Application
- Configured PingFederate Composite Adapter with Google set as second-factor authentication.
- Datastore (a JDBC-compliant database or LDAP directory)

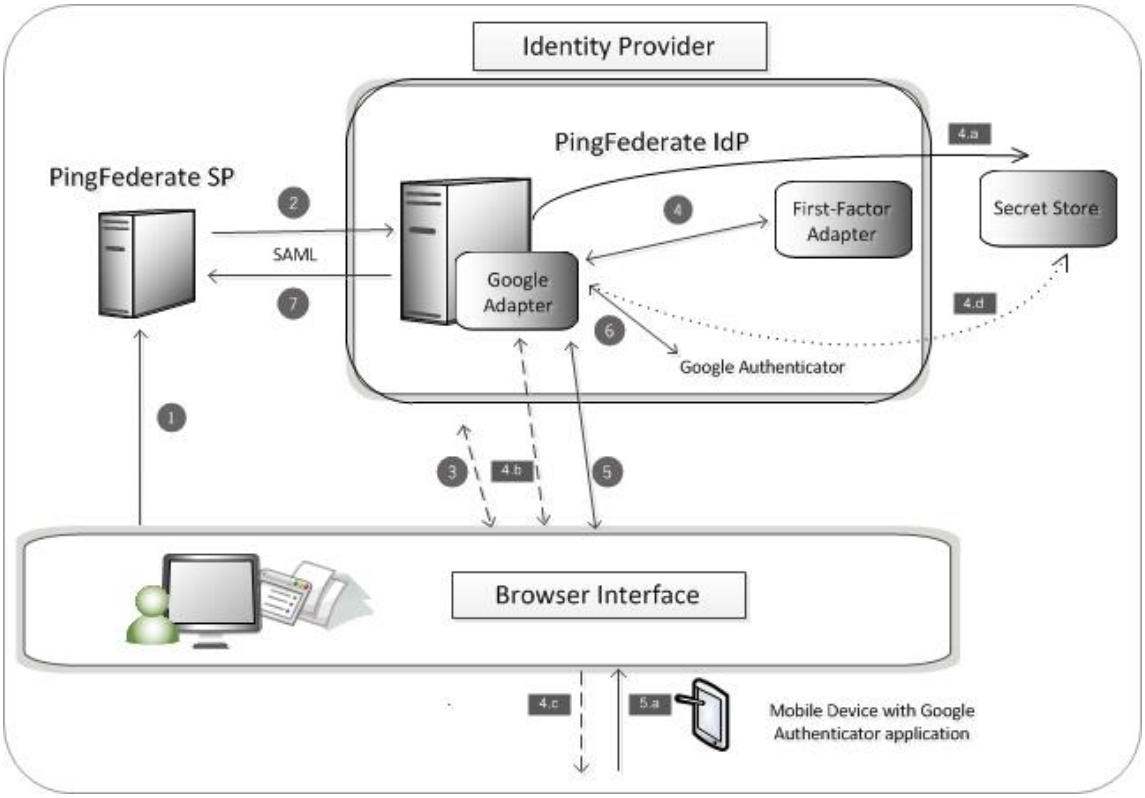
ZIP Manifest

The distribution ZIP file for the Google Authenticator Integration Kit contains the following:

- /docs
    - ReadMeFirst.pdf – contains links to online documentation for PingIdentity products
    - Legal.pdf– copyright and license information
- /dist – contains libraries needed to run the adapter
    - pf-google-authenticator-integration-kit-2.1.0.jar– the Google Authenticator adapter jar file
    - zxing-core-3.3.2.jar – Google ZXing library for Quick Response (QR)-code generation
    - zxing-javase-3.3.2.jar – Google ZXing library for QR-code generation
    - commons-dbutils-1.6.jar – Apache DBUtils library
- /dist/config – contains the config file needed to run the adapter
    - pingfederate-messages.properties – HTML template internationalization properties file fragment – to be added to the existing PingFederate file
- /dist/html – contains files needed to display the adapter
    - html.form.login.googleauthenticator.template.html – User-facing HTML template for login form
    - html.form.register.googleauthenticator.template.html – User-facing HTML template for the optional inline Google Authenticator App registration
    - html.form.timeout.googleauthenticator.template.html – User-facing HTML template for timeout form
- /dist/html/assets/css – contains files used to style the adapter pages
    - main.css – The style sheet used to style the adapter pages
- /dist/html/assets/images – contains image files needed to style the adapter pages
    - background-clouds-large.png – Image file used in the adapter
    - background-clouds-large@2x.png – Image file used in the adapter
    - icon-alert.png – Image file used in the adapter
    - icon-success.png – Image file used in the adapter
    - icon_default.1.png – Image file used in the adapter
    - ping-logo.2x.png – Image file used in the adapter
    - spinner.2x.gif – Image file used in the adapter

Process Overview

The following figure displays an SP-initiated SSO scenario integrating PingFederate into a two-factor authentication scenario using the Google Authenticator Integration Kit:



Processing Steps

1. The user initiates SSO from an SP application through a PingFederate SP server.

   Note: This SP-initiated scenario represents the optimal use case, one in which both the IdP and SP are using PingFederate. However, PingFederate accepts any valid SAML authentication request from an SP. In addition, you can enable IdP-initiated SSO; in this case, the user attempts SSO to an SP application from the IdP site, and the processing sequence would not include the next step.

2. The PingFederate SP Server generates a SAML AuthnRequest to the PingFederate IdP server.
3. If not already logged on at the IdP (via LDAP or IWA), the user is challenged to authenticate.
4. The PingFederate IdP server obtains user-session information via the first-factor adapter (either LDAP or IWA).
   a. The PingFederate IDP server queries the secret store (JDBC or LDAP) for a shared secret associated with the user
   b. (Optional) If configured for in-line registration, and the user has not already registered, the Google Authenticator adapter generates a shared secret and

presents a QR code to the user for registration.

c. (Optional) The user uses the Google Authenticator application to scan the QR code and store the shared secret on their mobile device.

d. (Optional) The shared secret is also stored in the Secret Store.

5. Once the shared secret is present, the Google Authenticator Adapter requests a one-time password (OTP) from the user (a security code provided by the Google Authenticator mobile application).

Note: If the in-line registration process fails or is not configured and the user has no valid shared secret, the authentication will be rejected and the user will be denied access to the resource.

---

e. The user enters the OTP generated by their mobile application in the browser form, which passes the code to the Google Authenticator adapter.

6. The Google Authenticator Adapter uses the username obtained by the first-factor adapter and the OTP to verify the user and the code via the Google Authenticator API.

7. If the validation succeeds, the PingFederate IdP server generates a SAML assertion with the username as the Subject and passes it to the PingFederate SP server.

8. (Not shown) The user is logged on to the SP target application.

Installation and Configuration

This section describes how to:

- Install the Google Authenticator Integration Kit.
- Install a third-party Google Authenticator Application
- Configure PingFederate
- Configure a Composite Adapter
- Register an Account

Install the Integration Kit

1. Stop the PingFederate server if it is running.

   From the integration kit /dist directory, copy the following files into the directory, <PF_install>/server/default/deploy:

   - pf-google-authenticator-integration-kit-2.1.0.jar
   - zxing-core-3.3.2.jar
   - zxing-javase-3.3.2.jar

   From the integration kit /dist directory, copy the following file into the directory, <PF_install>/server/default/lib:

- commons-dbutils-1.6.jar (only deploy if non-existent or a later version exists in PingFederate)

From the integration kit /dist/html directory, copy the following files into the directory, <PF_install>/pingfederate/server/default/conf/template:

- html.form.login.googleauthenticator.template.html
- html.form.register.googleauthenticator.template.html
- html.form.timeout.googleauthenticator.template.html

2. (Optional) This step is only required for PingFederate versions previous to 7.2.

   From the integration kit /dist/html/assets directory, copy the sub directories and its contents into the directory, <PF_install>/server/default/conf/template/assets:

   - /css/*
   - /images/*

3. From the integration kit /dist/config directory, add the contents of the following file:

   pingfederate-message.properties

   into the existing file:

   <PF_install>/pingfederate/server/default/conf/language-packs/pingfederate-messages.properties.

   Note: From the integration kit /dist directory, open the pingfederate-messages.properties file using a text editor and copy the contents of the file into the identical sections of the properties file located at <PF_install>/pingfederate/server/default/conf/language-packs/pingfederate-messages.properties.

   ---

4. Start the PingFederate server.

   For more information, see Starting and Stopping PingFederate in the PingFederate *Administrator's Manual*.

   Note: If PingFederate is deployed in a server-cluster environment, ensure that you repeat this installation on all PingFederate nodes.

   For more information about deploying PingFederate in a cluster and updating configurations, see the PingFederate Server Clustering Guide.

Install the Google Authenticator Application

The Google Authenticator is a general application used to generate One-Time-Passwords (OTP) for enabled accounts. The authenticator needs to receive a secret key for the account through a registration process. The application provides the secret that is encoded in a QR-code, which is scanned by the authenticator. There is also a special OTP uniform resource identifier (URI) for manual entry.

The Google Authenticator supports the TOTP RFC 6238.

Tip: The Google Authenticator is distributed freely for various mobile devices. Search "google authenticator app" to install on your device.

To configure the Google Authenticator Application:

1. Visit the appropriate App Store and install the Google Authenticator Application.
2. Follow the relevant instructions for your device.

Tip: The details and selections in these steps are directly relevant to the Google Authenticator Application. Different authenticator applications are available and can be used interchangeably.

Please note: For iPhone devices that are on iOS 9 and above, there is an issue noted in regards to time sync. Please follow the instructions in any of these articles to manually fix the issue, until a permanent fix has been issued:

http://www.volleythat.com/essays/2015/9/22/did-apple-just-set-millions-of-iphone-clocks-to-the-wrong-time
https://www.reddit.com/r/applehelp/comments/3lau9e/issue_with_time_sync_on_ios_9_iphone_6/
http://www.imobie.com/support/common-ios-9-problems-and-solutions.htm#part13

Configure PingFederate

The Google Authenticator Adapter requires a secret datastore where each user's username and obfuscated secret are stored. The datastore can be a database or an LDAP directory. The datastore must be defined before the Google Authenticator Adapter is configured. The datastore must have a username attribute and a secret attribute for each user. These attributes can be part of an existing user collection or a separate table/tree. The Google Authenticator Adapter must have read access to the datastore for authentication and write access if inline registration is enabled.

Sample Table Schema

Tables and column names are configurable but the data types are fixed with an appropriate length. The following is an example MySQL database table schema:

```
CREATE TABLE `GAUSERS`
(
 `USERNAME` char(255) DEFAULT NULL,
 `SECRET` char(255) DEFAULT NULL,
```

```
 UNIQUE KEY `unique_SECRET` (`SECRET`),
 UNIQUE KEY `unique_USERNAME` (`USERNAME`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1
```

An example Oracle database table schema:

```
CREATE TABLE GAUSERS
(
    USERNAME CHAR(255) DEFAULT NULL,
    SECRET CHAR(255) DEFAULT NULL,
    UNIQUE (USERNAME),
    UNIQUE (SECRET)
);
```

An example MS SQL database table schema:

```
CREATE TABLE GAUSERS
(
    USERNAME CHAR(255) DEFAULT NULL UNIQUE,
    SECRET CHAR(255) DEFAULT NULL UNIQUE,
);
```

Configure the IdP Adapter

Configuring the Google Adapter is one part of the process as the Google Adapter acts as second-factor authentication. A configured first-factor adapter is also needed. Once these two adapters are configured, then a composite adapter configuration is required. See Complete the Configuration for information on how to configure a Composite Adapter.

To configure the IdP Adapter:

1. Log on to the PingFederate administration console and click **Adapters** under IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance Id.

   The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.
4. Select Google Authenticator Adapter as the Type and click **Next**.

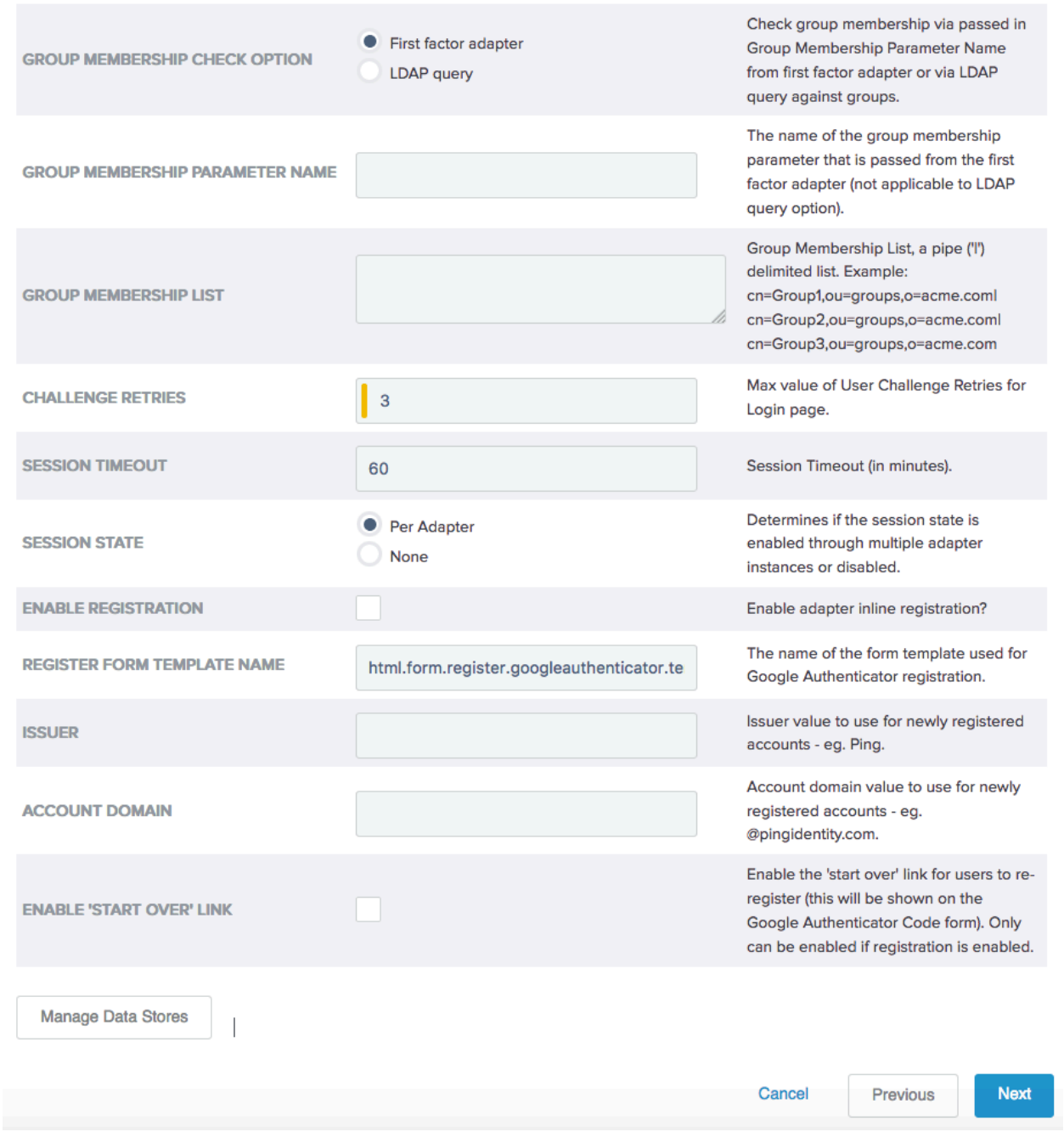
Manage IdP Adapter Instances | Create Adapter Instance

Type | IdP Adapter | Adapter Attributes | Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Google Authenticator configuration

Field Name	Field Value	Description
SECRET DATASTORE	-- Select One --	The Datastore where the user secrets are stored.
SECRET TABLE NAME		The name of the table where user secrets are stored.
USERNAME COLUMN NAME		The name of the column where usernames are stored in the secrets table.
SECRET COLUMN NAME		The name of the column where secrets are stored in the secrets table.
ENABLE USER INSERT	☐	Enable insert of new row in secret table (only applicable for SQL database datastore).
SECRET LDAP DATASTORE	-- Select One --	The LDAP datastore where the user secrets are stored.
LDAP SEARCH BASE		The location in the directory from which the LDAP search begins.
USERNAME SEARCH FILTER		Use ${username) as part of the query. Example (for Active Directory): sAMAccountName=${username).
SECRET ATTRIBUTE		Secret attribute name.
SCOPE OF SEARCH	○ One Level ● Subtree	
LOGIN FORM TEMPLATE NAME	html.form.login.googleauthenticator.te	The name of the form template used for Google Authenticator login.
TIMEOUT FORM TEMPLATE NAME	html.form.timeout.googleauthenticator	The name of the form template used for Google Authenticator timeout.
GROUP MEMBERSHIP MATCH CRITERIA	● Enforce OTP authentication ○ Bypass OTP authentication	Enforce or ByPass OTP authentication for users with matching group membership. Select 'Bypass OTP authentication' if connecting to a SQL database.



5. Click **Manage Data Stores** and make changes as required to the default settings.

   The default Data Store may be modified if necessary or a new Data Store can be added.

6. (Optional) Click **Add New Data Store.**

   For more information, see Managing Data Stores in the PingFederate *Administrator's Manual*.

   f. Select a Data Store Type from the available options.

      - Database

- LDAP
- Custom

g. Click **Next**.

Note: The type of Data Store configuration details and screen options vary depending on Data Store selected.

---

h. Complete the Data Store configuration and click **Done**.

i. On the Summary screen, verify that the information is correct and click **Save**.

7. On the IdP Adapter screen provide entries for each of the fields shown, as indicated in the following table below.

Field	More Information
Secret Datastore	The datastore where the user secrets are stored. Exactly one database or LDAP datastore must be defined, along with the related settings.
Secret Table Name	The table name where users secrets are stored.
Username Column Name	The column name where usernames are stored in the secrets table.
Secret Column Name	The column name where secrets are stored in the secrets table.
Enable User Insert	As part of registration, the adapter can insert a new row in the secret table if there is no existing row for the user. The adapter will only populate the username and secret columns. Only applicable if connecting to a SQL database.
Secret LDAP Datastore	The LDAP datastore where the user secrets are stored. Exactly one database or LDAP directory must be defined, along with the related settings.
LDAP Search Base	The location in the directory from which the LDAP search begins.
Username Search Filter	Use ${username} as part of the query. Example (for Active Directory): sAMAccountName=${username}
Secret Attribute	Secret attribute name.
Scope of Search	Single level or subtree.

Field	More Information
Login Form Template Name	The name of the form template used for Google Authenticator login. The default value is html.form.login.googleauthenticator.template.html. **Note:** This template provides standardized information to the end user. The template can be modified in a text editor to suit your particular informational needs.
Timeout Form Template Name	The name of the form template used for Google Authenticator timeout. The default value is html.form.timeout.googleauthenticator.template.html. **Note:** This template provides standardized information to the end user. The template can be modified in a text editor to suit your particular informational needs.
Group Membership Match Criteria	Enforce or ByPass OTP for users with matching Group Membership. Select 'Bypass OTP authentication' if connecting to a SQL database.
Group Membership Check Option	Check group membership via passed in Group Membership Parameter Name from first factor adapter or via LDAP query against groups.
Group Membership Parameter Name	The name of the group membership parameter that is passed from the first factor adapter (not applicable to LDAP query option).
Group Membership List	Group Membership List, a pipe ('|') delimited list. Example: cn=Group1,ou=groups,o=acme.coml cn=Group2,ou=groups,o=acme.coml cn=Group3,ou=groups,o=acme.com
Challenge Retries	Max value of user challenge retries for Login page. **Note:** The field cannot be left blank.
Session Timeout	Session Timeout (in minutes). Leave blank for indefinite sessions. Session Timeout is ignored if **None** is selected for Session State.
Session State	Determines if the session state is enabled through multiple adapter instances or disabled.
Enable Registration	Enable adapter inline registration. If inline registration is enabled and a user does not have a secret, the adapter generates a new secret and provides a registration page for exchanging it with the Google Authenticator App. If not enabled and user has no secret, the login will fail.

Field	More Information
Register Form Template Name	The name of the form template used for Google Authenticator registration. The default value is html.form.register.googleauthenticator.template.html. **Note:** This template provides standardized information to the end user. The template can be modified in a text editor to suit your particular informational needs.
Issuer	Issuer value to use for newly registered accounts – e.g., Ping.
Account Domain	Account domain value to use for newly registered accounts - eg. @pingidentity.com.
Enable 'Start Over' Link	Enable the 'start over' link for users to re-register (this will be shown on the Google Authenticator Code form). Only can be enabled if registration is enabled.

8. Click **Next**.
9. On the Adapter Attributes screen under Pseudonym, select the checkbox for the username attribute to be used as the expected identifier (username) for account registration.

   (For more information on using the Extended Contract screen, see Extending an Adapter Contract in the PingFederate Administrator's Manual.)

   You may also choose to mask attribute values in PingFederate log files. More information is available on the **Help** page.
10. Click **Next**.
11. On the Summary screen, click **Done**.
12. On the Manage IdP Adapter Instances screen, click **Save**.

Complete the Configuration

To configure the Composite Adapter:

The Google Authenticator Adapter must be configured as the second adapter using the Composite Adapter configuration. The Google Authenticator Adapter expects the single attribute "username" as input.

1. Log on to the PingFederate administration console and click **Adapters** under IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance Id.

   The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

4. Select Composite Adapter as the Type and click **Next**.

For more information, see Composite Adapter Configuration in the PingFederate *Administrator's Manual* for information on how to configure a Composite Adapter.

Note: The Composite Adapter must be configured to provide the expected 'username' attribute.

Registering an Account

To register the account to the Google Authenticator Application:

For users to authenticate via the Google Authentication Adapter, an account must be registered:

Note: During login, the Google Authenticator Adapter presents the user with a page to input the Google Authenticator Code derived from the account registration process. The provided default template can be customized and internationalized.

Registration is the process by which the application and the Authenticator App exchange the user secret. Registration can be done inline via the provided simple registration facility or registration is done externally through another application.

Note: This section describes the process of registration as if inline registration (See the Enable Registration option in the IdP Adapter screen on page 14) is enabled and a user does not have a secret. The adapter generates a new secret and provides a registration page for exchanging it with the Google Authenticator App.

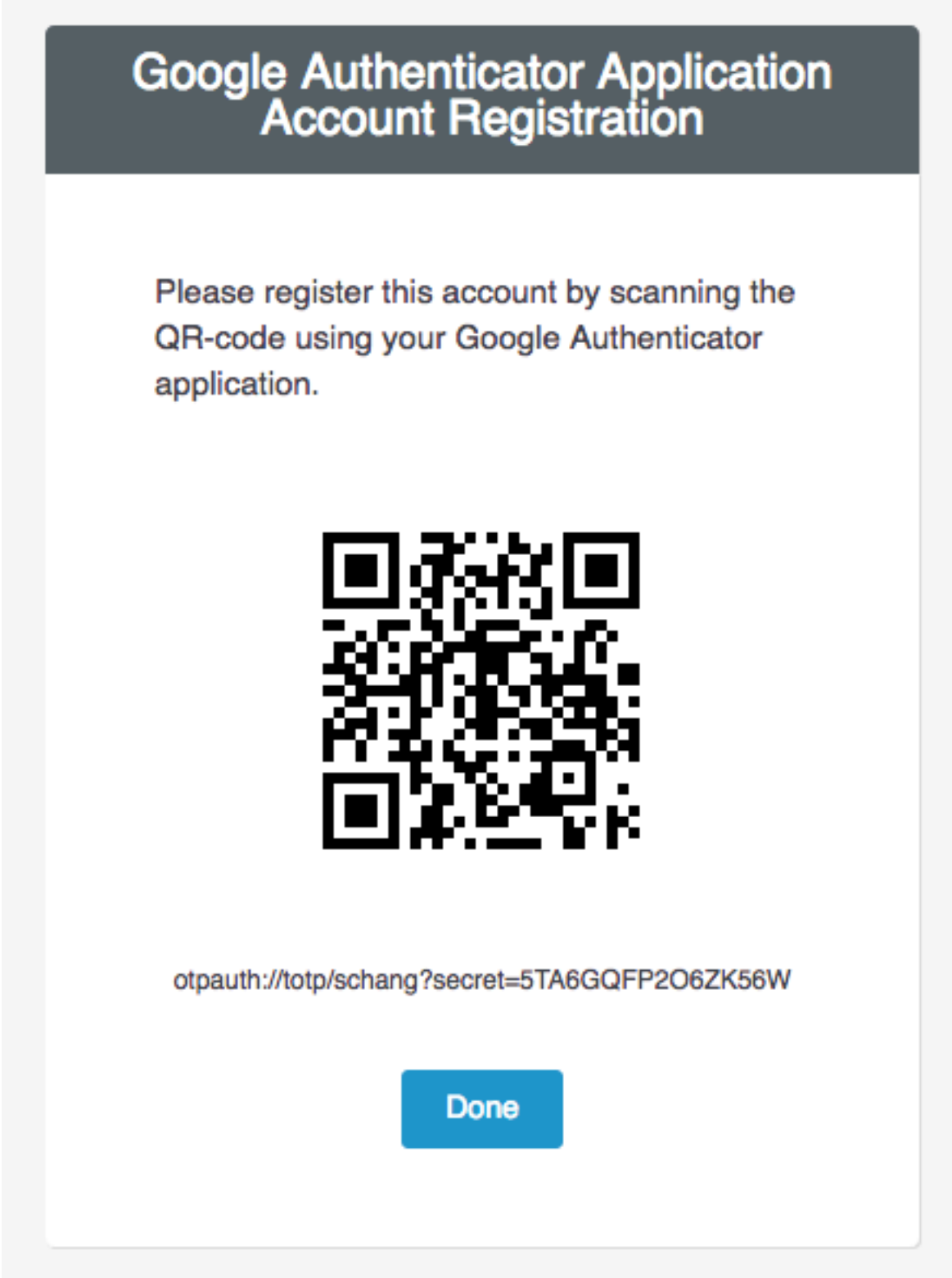
---

1. Login with required credentials (username and password) from the login page served from the first-authentication adapter. Enter the name and password of the user in the Username and Password field.

Note: If you are registering using the generated QR-code, then continue to Step 2. If you are registering using the OTP uniform resource identifier (URI) for manual entry, continue with Step 3.

---

2. (Only for registration using a QR-code) Scan the generated QR-code which contains the encoded secret using the Google Authenticator Application



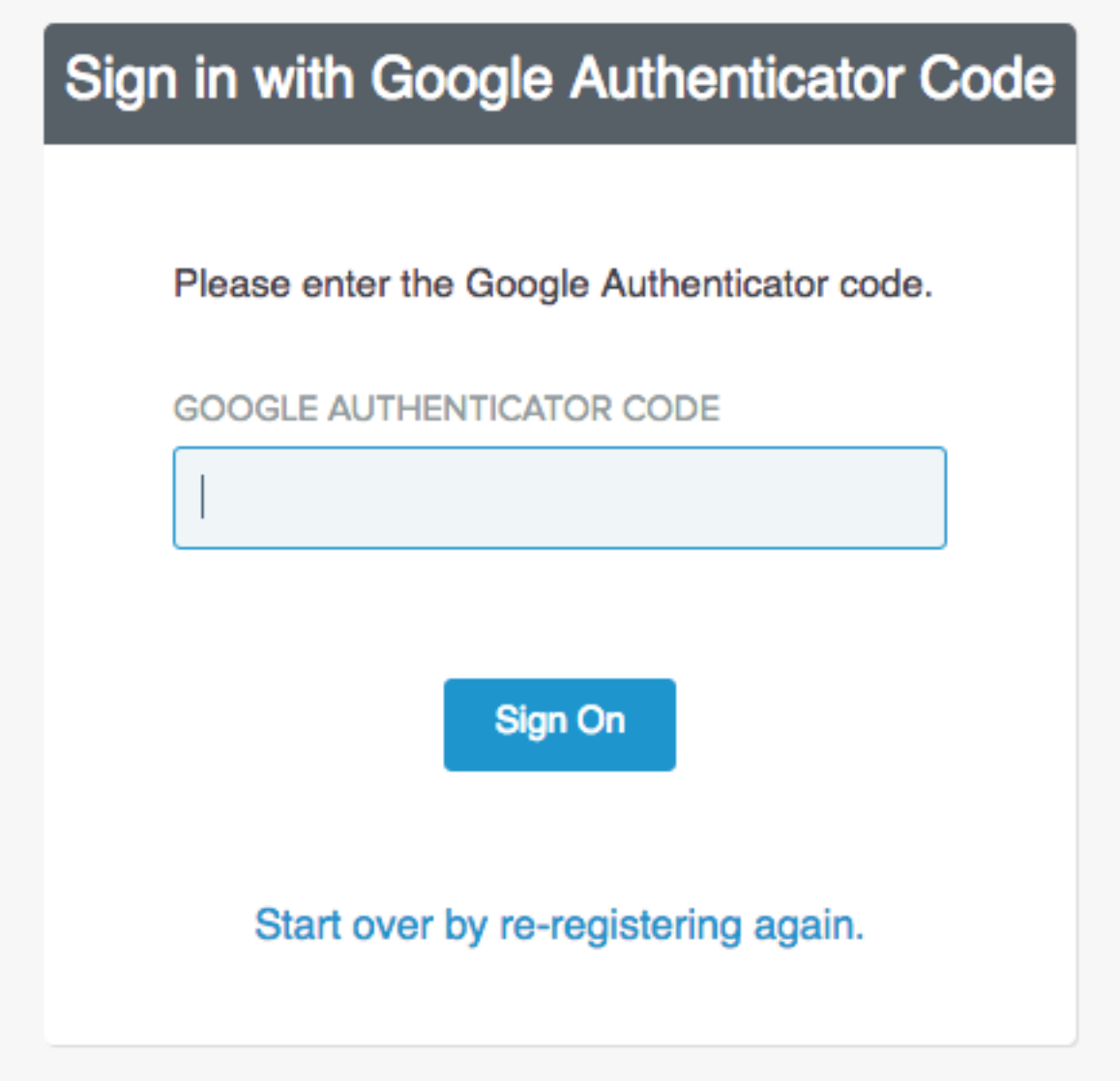
Skip the next step.

3. (Only for registration using the OTP uniform resource identifier (URI)) Copy the generated secret from the special OTP uniform resource identifier (URI) for manual entry and click **Done**.

a. If not done already, launch your Google Authenticator Application.

b. Add the user and generated secret key to the Google Authenticator Application. A One-Time Password (OTP) is generated.

4. Enter the One-Time-Passwords (OTP) in the Google Authenticator code screen and click **Sign On**.



Note: Generated passwords can only be used once and are only available for a limited time frame before use. Please note the remaining time for a generated password before use as the password may expire before use. If that were the case, a new password would need to be generated.