How to Implement Pledge with McAfee OTP 3.X & 4.X
Table of Contents

TERMINOLOGY

1 Pledge Overview
   Pledge Profile Service
   Pledge Enrollment
   Pledge Client

2 Network Requirements for Pledge
   Enrollment Process Description

2 Pledge Profile Service
   2.1 Create Pledge Profile Service user account and Customer account
   2.2 Pledge Profile Service Customer account

3 Configure McAfee OTP Enrollment
   3.1 McAfee OTP version 4.X
      Configure OATH Key database for Enrollment
      Configure OATH Key database Client
      Configure OTP database for Enrollment authentication
      Configure Enrollment authentication client
      Enable McAfee One Time Password Enrollment
      Start McAfee One Time Password Embedded HTTP Server
      Pledge Enrollment interface
   3.2 McAfee OTP version 3.X
      Configure Pledge Enrollment Database
      Configure Pledge Enrollment Client
      Enable Pledge Enrollment
      Pledge Enrollment interface

4 Test McAfee One Time Password Enrollment
# Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pledge</strong></td>
<td>Pledge is a McAfee software token infrastructure following the HOTP (RFC 4226) OATH standard.</td>
</tr>
<tr>
<td><strong>Pledge Profile Service (PPS)</strong></td>
<td>A McAfee web service to design and customize a Pledge profile, PPS is responding to User enrollment request.</td>
</tr>
<tr>
<td><strong>Pledge Enrollment (PE), Enrollment and Pledge Enrollment Module</strong></td>
<td>PE is the McAfee OTP v3.X web application dedicated to automate Profile delivery to Users. From McAfee OTP v4.0, it is replaced with a similar application called Enrollment where the Pledge module is only one OTP method out of many (SMS, email, HW Tokens).</td>
</tr>
<tr>
<td><strong>Pledge User Profile</strong></td>
<td>A Pledge User Profile is made of a PPS Theme and Template that are combined with an OATH key and a Pledge profile ID.</td>
</tr>
<tr>
<td><strong>Pledge ID</strong></td>
<td>A Pledge ID is created by Pledge Profile Service, it is representing a Pledge User Profile and when used with a Pledge Client it will download a unique User profile.</td>
</tr>
<tr>
<td><strong>Pledge Profile</strong></td>
<td>A Pledge profile is designed following a corporation's branding and security standard. It is a template for all Pledge User Profiles downloaded onto Pledge Clients. The graphic portion of a Profile is called a Theme and the Configuration portion is called a Template.</td>
</tr>
<tr>
<td><strong>Pledge Client</strong></td>
<td>Pledge Client application is available as a Cellular or Desktop version. When a User profile has been downloaded it becomes a Software Token that generates one-time passwords based on the OATH algorithm.</td>
</tr>
<tr>
<td><strong>PPS User account</strong></td>
<td>A User account must be created prior to create a Customer Account. Email address is used as login name and a otp will be sent to email address to secure login.</td>
</tr>
<tr>
<td><strong>PPS Customer account</strong></td>
<td>Customer account is the PPS placeholder where customers can upload pictures to create one or more Theme as well as one or more Template.</td>
</tr>
<tr>
<td><strong>OATH</strong></td>
<td>Open Authentication (OATH) is an open standard designed to offer strong authentication with multiple vendors.</td>
</tr>
<tr>
<td><strong>OTP / otp</strong></td>
<td>McAfee One Time Password Server / one time password</td>
</tr>
<tr>
<td><strong>Pledge Enrollment Database</strong></td>
<td>An LDAP or SQL database used to store Pledge Users OATH key.</td>
</tr>
<tr>
<td><strong>Native Client</strong></td>
<td>A McAfee OTP Client object that is representing an application using McAfee APIs to communicate with OTP, the Enrollment application for example.</td>
</tr>
</tbody>
</table>
1 Pledge Overview

Pledge turns devices into security tokens and is available for most cellulares and Desktop Operating Systems. The Pledge Software Token comes with a complete infrastructure for automation of OATH key enrollment and profile customization. Instead of using a hardware security token when logging in, you simply use your preferred device.

This guide describes how to implement Pledge together with McAfee OTP.

The Pledge system infrastructure consists of three components:

- Pledge Profile Service
- Pledge Enrollment / McAfee OTP
- Pledge Client

Basic Pledge implementation process is as follows:

The process begins with the creation of a Pledge Profile Service user account and a customer account, then follows the configuration of McAfee OTP Enrollment and ends with the download of a User profile and its verification.

1. Create Pledge Profile Service user account.
2. Create Pledge Profile Service customer account.
3. Configure McAfee One Time Password Enrollment service.
4. Verify configuration.

Pledge Profile Service

Pledge Profile Service (PPS) is the Web Service environment where administrators can configure and customize their Pledge Themes and Templates. A designer tool is available to associate logos, pictures and colors as well as configure PIN-code settings, OATH key type and contact information such as text and service desk URL for example.

Pledge Profile Service is an Internet web service provided by McAfee.

Pledge Enrollment

Pledge Enrollment (PE) is the McAfee OTP v3.X web application dedicated to automate the delivery of Pledge User Profiles to User devices.

From McAfee OTP v4.0, it is replaced with a similar application, called Enrollment, where the Pledge module is only one OTP method to enroll with among others (SMS, email, HW Tokens).

Both PE and the Pledge module automates the delivery of User Profiles to end-user devices.

There are two ways to enroll for Pledge, end-users can enroll themselves or Pledge administrators will do it for them.

When a User enrolls for Pledge:

- PE verifies User credentials and sends a request to PPS
- PPS generates an OATH key as well as an ID
- PPS sends the Pledge OATH key & ID to PE
- PE is presents ID & QR code to User at the same time it copies the Pledge OATH key into Pledge User attribute
- User enter ID on device and User profile is downloaded

**When a User is enrolled for Pledge by an Administrator:**
When an Administrator is enrolling a User, it is the Administrator who’s shown the Pledge ID & QR code. Administrators have different options to forward this information to User or complete the enrollment process themselves when they have the User device.
A Group object must be created in User Store with one or more administrative users prior to configure this option.

**Pledge Client**
The Pledge Client application can generate one-time passwords based on the OATH algorithm when a Pledge User profile has been downloaded. It can be installed on most cellular devices and Desktop Operating systems. The Pledge Client supports multiple Pledge profiles which make it possible to authenticate to systems from different organizations, Internet Services, Corporations or ISP solutions.
The Pledge client for cellars is available from Apple App store, Google play and Windows phone store. The Desktop version can be downloaded from the McAfee download site with a McAfee OTP grant number.

**Network Requirements for Pledge**
Pledge Clients must have access to pledge-api.nordedge.com on port 443
Pledge Enrollment must have access to pledge-api.nordedge.com on port 443
To access Pledge Profile Service Administrator workstation must have access to pledge.nordedge.com on port 443
Enrollment Process Description

1. User is enrolling for a Pledge Profile via Enrollment Web Page
2. OTP is verifying User credentials
3. PE is sending a web service request to PPS
4. At this point PPS is:
   - Generating an OATH key corresponding to Template configuration (HOTP, TOTP, OCRA)
   - Packaging the Theme and Template together
   - Generating a unique Profile ID
   - Combining all the above into an XML message available from PPS for as long as configured by Administrator
   - Responding to PE with OATH key and Pledge User Profile ID.
5. PE is sending OATH key information to OTP.
6. OTP is storing data in selected location (LDAP User attribute, SQL, .)
7. PE web page is presenting the Pledge ID & QR code to end-user or administrator.
8. Pledge Client application must be launched on device, select the plus symbol, enter Pledge ID, Pledge Client is contacting PPS and requesting corresponding Pledge User Profile.
9. Pledge Profile Service is responding with XML message, flags the Pledge ID as downloaded and destroy the stored OATH key.

The Pledge Software Token is now ready to generate one-time passwords.
2 Pledge Profile Service

2.1 Create Pledge Profile Service user account and Customer account

The first step is to create a user account (this account may also be used to manage other PPS Customer account) then a Customer account.

- Launch an Internet Browser and enter URL: https://pledge.nordicedge.com

Note: Nordic Edge is now a part of McAfee, a wholly owned subsidiary of Intel Corporation.

- Click “Create user account”.

- Enter your email address.
- Enter a password.
- Click Next.
- Open email used when creating the PPS user account.

Pledge Profile Service email verification

There are two alternatives to verify your email address and activate your Pledge Profile Service user account.

1. Enter the following verification code on the User Registration page in the Verification code field:
   m7dkknjgouz7dpn017p3m2kmrea8m118n9p65b5mb2sn7rfzn2ehsta2nb99uf

2. Click on the following link to activate your Pledge Profile Service user account:
   

   Note: This will open a new browser tab or window to complete the User Registration

   - Copy the Verification code or click on the link. In this example we copy the Verification code.
   - Paste the Verification code.
   - Click Next.
● Read the license agreement and when done select I Agree.
● Click Next.

The User Registration is now completed.
● Click Next and proceed with Customer account creation.
- Enter company or organization.
- Click Next.

- Store the Customer ID and Customer password in a safe place, it will be used later to configure PE.
- Click Next.
Customer Account Registration

These are the customer credentials, store them in a safe place.

These credentials must be used to configure the McAfee One Time Password Enrollment web application, which is found in OTP Configurator - Misc - Enrollment - Pledge.

Customer ID: 48a9xxxxxxxxxxxxx: c-1bc4e106152
Customer password: LOE=xxxxxxxxxxx: CHNra

Next  Cancel
The Customer Account Registration is now completed.
Click Done.

2.2 Pledge Profile Service Customer account

Using Pledge Profile Service User Interface, you can create and customize a corporate theme and template with your company branding, for example logo, icon, button, background color and text color.
You can also choose the OATH type (HOTP, TOTP, OCRA) as well as set the PIN code length and the length of time User profiles will be available for download.
Consult the McAfee OTP Product guide for details.

By default a Pledge Customer Account is configured to use HOTP and is assigned the default McAfee Pledge Theme and Template.
In this guide we will use the default.
Notes:
Changes made in Pledge Profile Service will not take effect until users enroll for a Pledge Profile.
Make sure settings like PIN code protection and support information are configured before end-users begins to enroll for Pledge Profiles.

3 Configure McAfee OTP Enrollment

In this guide, McAfee OTP is installed on a Windows Active Directory Domain Server with Host Address 127.0.0.1 and LDAPS port 636 is used to connect to Active Directory.
To be able to use port 636 with a Microsoft Windows Server it must be configured for LDAPS.
You can enable LDAP over SSL (LDAPS) by installing a properly formatted certificate from either a Microsoft certification authority (CA) or a non-Microsoft CA according to the Microsoft guidelines:
http://support.microsoft.com/kb/321051

The OTP Server Database used by the Pledge enrollment web application to store Pledge OATH keys can be any LDAP or SQL database. Both the user objects and OATH keys are often stored in the same database but it is possible to use an LDAP User Store to authenticate Users and an SQL database to store their Pledge OATH keys, for example.
3.1 McAfee OTP version 4.X

McAfee OTP enrollment application is no longer dedicated to Pledge Enrollment, there are three enrollment modules that Administrators can configure, Pledge Enrollment, SMS/email Enrollment, HW OATH Tokens Enrollment.

In this guide we will focus on the Pledge Enrollment module and the prerequisites for McAfee OTP 4.X are as follows:
- Two Database objects must be created (LDAP or SQL), one to authenticate Users (Not OATH type) and one to store their OATH keys (OATH type).
- Two Client objects must be created, one for the Enrollment application and one for the Pledge Enrollment module.

The Database to authenticate Users must be assigned to the Client for Enrollment application and the database to store OATH keys must be assigned to the Pledge Enrollment Client.

Basic Enrollment setup for Pledge is as follows:
1. Create and configure an OTP Database to store Pledge OATH keys. In this example it is an LDAP database called OATH Key database.
2. Create and configure an OTP Database to authenticate users. In this example it is an LDAP database called Enrollment authentication.
3. Create and configure a Native OTP Client associated with the OATH Key database.
4. Create and configure a Native OTP Client associated with the authentication database.
5. Configure Enrollment and the Pledge module using Clients from Steps 3 & 4 and with PPS credentials.
6. Start Enrollment web application.

Configure OATH Key database for Enrollment
This Database is used to store Pledge OATH keys.
- Start McAfee OTP with C:\Program Files\McAfee\OTP\otpserver.exe
  Always right click and use “Run as administrator” when starting otpserver.exe on Windows Servers.
- Click on Configuration button
- Click Databases and then LDAP Database button.
Host Settings
User object chosen as Admin DN must have write permissions to selected OATH-key attribute selected to store and update their Pledge OATH keys.

- Choose a Display name for the database. In this example “OATH Key database”.
- Select Uses OATH and HOTP/TOTP.
- Enter Active Directory server IP address, in this example 127.0.0.1.
- Use Port number 636.
- Enter Admin DN, do NOT use a User Principal Name (UPN).
- Enter Admin DN password.
- Click on Test Connection. You should get a message saying “LDAP connection success”.
LDAP Search Setting

The BASE DN is the search base from where McAfee OTP will start its search for user objects in Active Directory domain.

- Click the button with three dots on the right side of the Base DN field to browse Active Directory.
- Click the Container from where to start searching for user objects and click OK.
Search Filter
The Search filter must correspond to LDAP directory type you are using. In this example Microsoft Active Directory.

- Click “Samples” button.
- Select Microsoft Active Directory, click OK and Yes.

OATH Key attribute
OATH Key field must correspond to an Active Directory user object attribute which is not currently in use in the Active Directory domain. This attribute must be a String type, have a minimum length of 60 characters and be multi valued if multiple Profiles is enabled for Users. In this guide the Active Directory attribute “carLicense” is used.

Note: When McAfee One Time Password is configured to encrypt OATH Keys the attribute length must be unlimited.

- Use the browse button and select attribute.
- Click OK.
- Click Save.
The OATH Key database configuration should be similar to:

Configure OATH Key database Client

McAfee OTP Pledge Enrollment requires a Native OTP Client associated with User Database configured to store the Pledge OATH Keys.

Note: Pledge Enrollment uses TCP port 3100

- In the left pane click "Clients" and then in the right pane click "New Native Client".
- Enter a Display Name. In this example “OATH Key database client”.
- Enter 127.0.0.1 as the Client IP address.
- Enter “OATH Keys database client” as Client name detection (A value MUST be set).
- Choose the “OATH Key database” configured earlier as the User Database.
- Click Save.

Configure OTP database for Enrollment authentication
Used by Enrollment application to authenticate Users and Administrators.

- In left pane, click on Databases and then on LDAP Database button.

**Host Settings**

- Choose a Display name for the database. In this example “Enrollment authentication”.
- Enter IP address to Active Directory server. In this example 127.0.0.1.
- Use default Port number 636.
- Enter Admin DN, do not use User Principal Name (UPN).
- Enter Admin DN password.
- Click Test Connection. You should get a message saying “LDAP connection success”.
LDAP Search Settings

- Click on the button with three dots on the right side of the Base DN field to browse Active Directory.
- Click on the Container from where to search for user objects and click OK.

Search Filter

The Search filter must correspond to LDAP type you are using, in this example Microsoft Active Directory.

- Click “Samples” button.
- Choose Microsoft Active Directory, click OK and Yes.
- Save Config.
The Enrollment authentication database configuration should be similar to:

Configure Enrollment authentication client

McAfee OTP Enrollment requires an OTP Client that is associated with User Database where user objects exists.

Note: Pledge Enrollment uses TCP port 3100

- In the left pane click "Clients" and then in the right pane click "New Native Client".
● Enter a Display Name. In this example “Enrollment authentication client”.
● Enter 127.0.0.1 as the Client IP address.
● Enter “Enrollment authentication client” as Client name detection (A value MUST be set).
● Choose database “Enrollment authentication” configured earlier.
● Click Save and then close OTP Configurator.

Enable McAfee One Time Password Enrollment

To enable Pledge Enrollment and configure it to use the OTP Clients created previously as well as PPS credentials from Customer account created earlier.

Note: Verify that firewalls allows connection to PPS address pledge-api.nordicedge.com via TCP port 443.

● In the left pane, expand Misc and select Enrollment.
- Enable Enrollment.
- Select “Enrollment authentication client” as Authentication client.
- Optional: Require OTP authentication, will secure login to Pledge Enrollment with a one-time password.
- Optional: Administrator Role settings, to configure the group object that will have the Administrative right to Enroll Users, Group object must already exist in User Store and have at least one user as a member.

- “Attribute name:” must be the name of the user object attribute that is used to store group membership, i.e. memberOf with Active Directory.
- “Group name:” must be the Group Object name created for this administrative task.

- Click on Pledge enrollment.
- Select Enable Pledge enrollment.
- Enter your Pledge Profile Service Customer ID.
- Enter your Pledge Profile Customer password.
- Select OATH Key database Client.
- Click Done.
- Click Save Config.
- Optional: Profile download notification, this is to configure a Delivery method that Pledge Enrollment Administrators can use to send Profile ID and QR Code to User, for example via SMS:

- Click Done.

Notes:
- Pledge Customer ID and password were created in Step 2.1, when password was lost you can login to Pledge Profile Service with your User account and create a new password for your Customer account.
- The Profile Template ID is optional, when nothing is specified the Default Template will be used.
Start McAfee One Time Password Embedded HTTP Server

- In the left pane, expand Misc and click on Embedded HTTP Server.
- Click Enable Embedded HTTP Server.
- Click Save.
- Restart OTP Server or click on Start HTTP Server.

Note: When using the Standalone Configurator or the RemoteConfigurator, the Start HTTP Service button is not visible, restart McAfee OTP after closing OTP Configurator.

Pledge Enrollment interface

McAfee OTP Enrollment web application is accessible via an Internet browser:
https://<OTPServerIP>:8080/Enroll
3.2 McAfee OTP version 3.X

Basically the following must be done to configure Pledge Enrollment with McAfee OTP 3.X:
- Create a Pledge Enrollment Database with corresponding settings for Pledge OATH key storage
- Create a Pledge Enrollment Client for the Pledge Enrollment
- Start Pledge Enrollment

Configure Pledge Enrollment Database

The OTP Server Database is used by the Pledge enrollment web application to store Pledge OATH keys. This database can be any LDAP or SQL database and in this guide Microsoft Active Directory (Active Directory) is used.

Start McAfee OTP with C:\Program Files\McAfee\OTP\otpserver.exe
Always right click and use “Run as administrator” when starting otpserver.exe on Windows Servers.
Click on the Configuration button.

- Click on Databases and then on LDAP Database button.
OTP Server is installed on Windows Active Directory Domain Server in this scenario. Localhost IP-address 127.0.0.1 is used as Host address as well as standard LDAP port 636 to connect to AD.

Notes: Username chosen as Admin DN must have write permissions to the Users OATH-key attribute to store their Pledge OATH keys.

Also, to use the Locked Account feature from OTP Server, Admin DN user must have write permissions to modify the selected attribute.

- Choose a Display name for the database. In this example “Pledge Enrollment Database”
- Select “Uses HOTP or TOTP (OATH)”.
- Enter IP address from Active Directory server (In this example 127.0.0.1)
- Port number, use default 636
- Enter Admin DN (Do not use User Principal Name)
- Enter Admin DN password
- Click on Test Connection (You should get a message saying “LDAP connection success”)

**LDAP Search Settings**

The BASE DN is the search base where OTP Server will look for user objects in Active Directory domain.

- Click on the button with three dots on the right side of the Base DN field to browse Active Directory
- Click on Container where user objects are existing and click OK.
Search Filter

Configure the search filter specifically for the directory type, for example Microsoft Active Directory.

- Click on “Sample Button”.
- Choose Microsoft Active Directory, click OK and Yes.

OATH Key attribute

OATH Key field must correspond to an AD user object attribute which is not currently in use in target AD domain. This attribute must be a String type, have a minimum length of 60 characters (unencrypted) and be multi valued for multiple profiles support.
In this guide the attribute "carLicense" is used.

- Use the browse button and select attribute

- Click OK

The Pledge Enrollment database configuration should be similar to:
Configure Pledge Enrollment Client

The Pledge Enrollment service requires OTP Server to be configured with a corresponding Native OTP Server Client.

Note: Pledge Enrollment uses TCP port 3100 (Enrollment service <==> OTP Server)

- In the left pane click “Clients” and then in the right pane click “New Native Client”
- Enter a Display Name for your Pledge Enrollment Client. In this example “Pledge Enrollment Client”
- Enter 127.0.0.1 as the IP address
- Choose the “Pledge Enrollment Database” configured earlier as the User Database
- Click on Advanced button

- Enable name detection
- Enter Client Name, for example “PledgeEnrollment”.
The Pledge Enrollment Client configuration should be similar to:

Enable Pledge Enrollment

Enable Pledge Enrollment and configure it to use the Pledge Enrollment database created previously as well as Pledge Profile Service credentials from Customer account created earlier.

Note: Verify that firewalls allows McAfee OTP to connect to Pledge Profile Service address pledge-api.nordicedge.com via TCP port 443.

- In the left pane, expand Misc and select Pledge Enrollment.
- Select the OATH database, in this example “Pledge Enrollment Database”.
- Enter the Pledge Profile Service Customer ID in the field “Pledge web services username”.
- Enter the Pledge Profile Customer password in the field “Pledge web services password”.
- Enter the Client Name Detection name, in this example “PledgeEnrollment”.
- Click Save Config.

Note: Use the function “Allow user to enroll multiple profiles” when users are allowed to use Pledge Profiles on more than one device.
- In the left pane, select Embedded HTTP Server.
- Click on Enable Embedded HTTP Server.
- Click on Save.
- Restart OTP Server or click on Start HTTP Service.

**Note:** Select Enable SSL to protect Pledge Enrollment service with SSL.
Pledge Enrollment interface
McAfee OTP Pledge Enrollment web application is accessible via an Internet browser:
Self-enrollment: https://<OTPServerIP>:8080/PledgeEnrollment/enroll.jsp
Admin-enrollment: https://<OTPServerIP>:8080/PledgeEnrollment/supportenroll.jsp

4 Test McAfee One Time Password Enrollment
This step requires a McAfee Pledge Software Token client application to be installed on a device.
Download the application from your vendor app store, for example App store, Google Play or Microsoft Store.
Install McAfee Pledge on your device:
  ● Go to App store, Google Play or Microsoft Store.
  ● Search for “Pledge”.
  ● Download and install the Pledge Client application.

User Enrollment
  ● Start a Internet browser and go to https://<OTPServerIP>:8080/Enroll
  ● Enter username and password
Click on OTP method you want to enroll to, in this scenario McAfee Pledge.

At that point you will get a Pledge ID and a QR code. You can use either the Pledge ID or use the camera function to scan the QR code. In this example we use the Pledge ID.

On the device where you have installed McAfee Pledge Software Token Client application:
- Start Pledge application.
- Click on the plus (+) symbol.
- Enter Pledge Profile ID, in this case 53846255.
- Optional, enter PIN code to protect the Pledge Profile. This is a personal code which must be kept secret.
- Click on Generate one-time password.
- Enter PIN code (optional)
- When asked, enter the one-time password that you generated.
Click on Next.

The enrollment process is completed.
Administrator Enrollment

- Start a Internet browser and go to https://<OTPServerIP>:8080/Enroll
- Enter Administrator username and password (Must be member of Pledge Enrollment Administrator Role)

- Click the Pledge Admin module
- Click Enroll User

- Enter username and Click Enroll
At this point Administrator have several options to complete user enrollment:

- Tell User its Profile ID and guide User through procedure to add a profile on a Pledge device
- Click on Profile ID button and scan the QR code with User device

**Activate profile**

Download the user’s Pledge Profile by entering the profile ID in your Pledge application or by scanning the QR-code.

<table>
<thead>
<tr>
<th>Profile ID</th>
<th>QR-code</th>
</tr>
</thead>
<tbody>
<tr>
<td>63032665</td>
<td><img src="qr_code.png" alt="QR Code" /></td>
</tr>
</tbody>
</table>

- Click Send Activation link to forward link to User with delivery method configured with Profile Download Notification from the Pledge Enrollment module settings.

- Click Send

**Note:** When Profile download Notification was configured with SMS delivery method the “Destination” field is populated with User cellular number and when SMTP was configured it is an email address.

**Send activation link**

Send Pledge activation link to end user

Destination: 555-0100

Then User clicks on link received via SMS and the Pledge Client from the cellular phone will download corresponding Pledge Profile.