



NetIQ Advanced Authentication Framework

OATH Authentication Provider User's Guide for iOS

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
OATH Authenticator Overview	4
Managing NetIQ Smartphone Authenticator	5
First Launch of NetIQ Smartphone Authenticator	6
Next Launches of NetIQ Smartphone Authenticator	9
Re-enrolling Authenticator	13
Troubleshooting	14
One-Time Password Doesn't Work	14
Index	15

Introduction

About This Document


Purpose of the Document


This OATH Authentication Provider User's Guide is intended for all user categories and describes how to use the client part of NetIQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to manage OATH OTP Token. This document is assigned for the description of application's work using iOS for the generation of one-time passwords which will be used for NetIQ Advanced Authentication.


For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ Advanced Authentication Framework – Client User's Guide.


Information on managing other types of authenticators is given in separate guides.

Document Conventions

 **Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

 **Important notes.** This sign indicates important information you need to know to use the product successfully.

 **Notes.** This sign indicates supplementary information you may need in some cases.

 **Tips.** This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, buttons are put in bold type, e.g.: the **Logon** window.

OATH Authenticator Overview

The **OATH** (open authentication) authentication type takes its name from the Initiative for Open Authentication (OATH), which is a collaborative effort of IT industry leaders aimed at providing reference architecture for universal strong authentication across all users and all devices over all networks.

Open authentication addresses One Time Password (OTP) – based authentication method.

OTP-based authentication is intended to act as a bridge between legacy and modern applications. OTP credentials will facilitate integration with applications that rely solely on user passwords. Because end users are already familiar with static passwords, a device-generated password can greatly facilitate the transition to stronger authentication.

In OTP-based authentication method, login is performed using an essentially random password each time. The passwords are generated by a device, most commonly a hardware token associated with the user, and so the password is not based on the user's memory. This greatly increases security.

TOTP (Time-based One-time Password Algorithm) is a variant of the OTP authentication, where the one-time password changes at frequent intervals (say, every two minutes). Each one-time password is generated by applying a random-looking cryptographic function to a unique series value. In the time-based case, the value is the current time.

Managing NetIQ Smartphone Authenticator

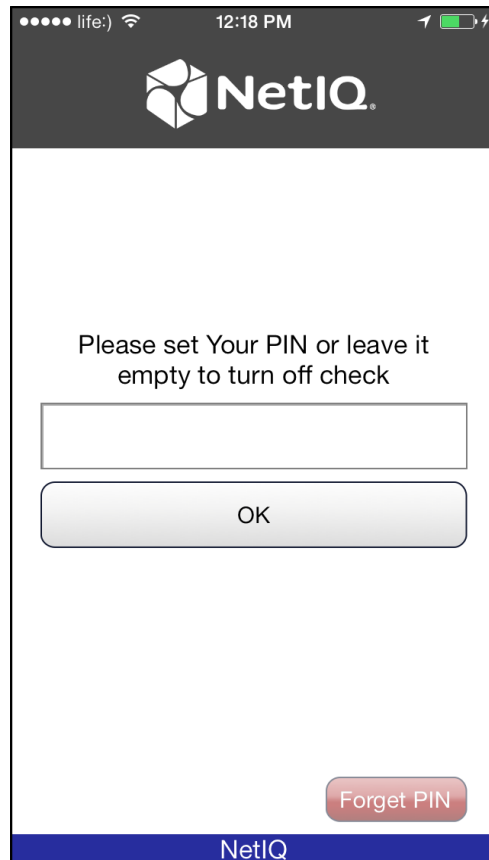
NetIQ Smartphone Authenticator gives you access to the NetIQ system from your phone with the help of a One-Time-Password token. The generated token is valid for that time period that has been set by system administrator (by default the generated token is valid for 30 seconds). NetIQ Smartphone Authenticator is compatible with iPhone, iPod touch and iPad. The application requires iOS 6.1 and later.

In this chapter:

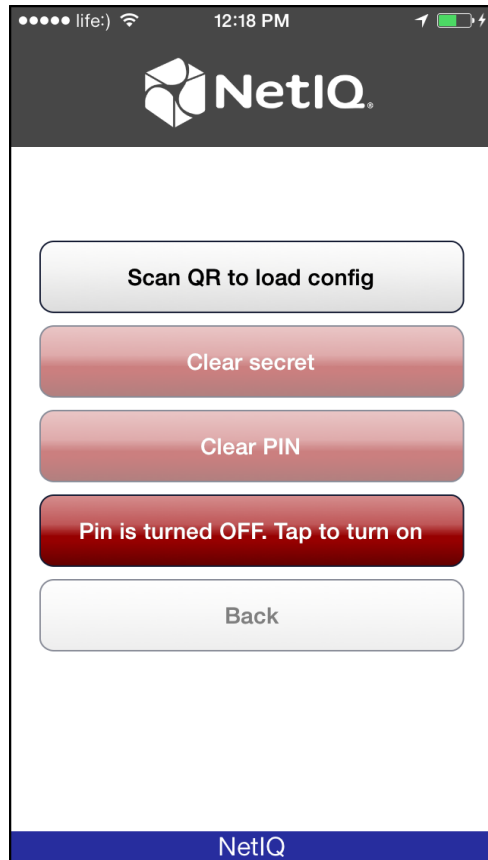
- [First launch of NetIQ Smartphone Authenticator](#)
- [Next launches of NetIQ Smartphone Authenticator](#)
- [Re-enrolling OATH authenticator](#)


First Launch of NetIQ Smartphone Authenticator

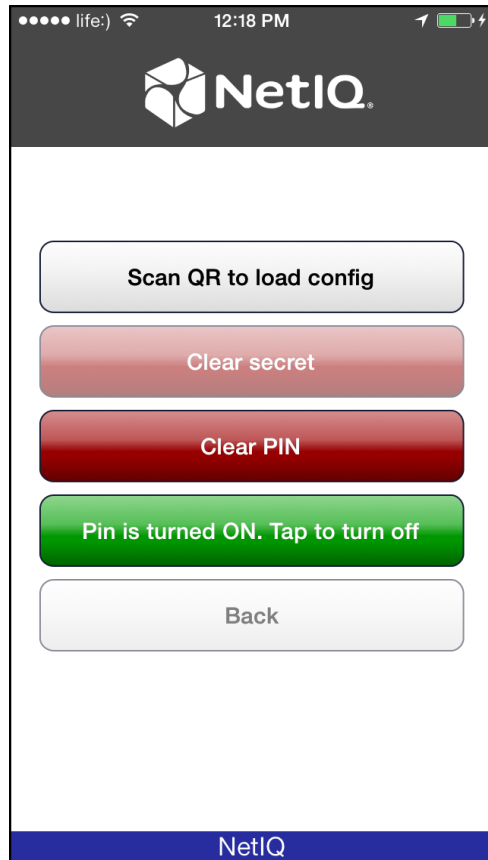
1. Install NetIQ Smartphone Authenticator. You can download it from the Apple Store.
2. Run NetIQ Smartphone Authenticator. The authorization window will be displayed. Tap **OK**.



3. The main menu of NetIQ Smartphone Authenticator will be displayed:



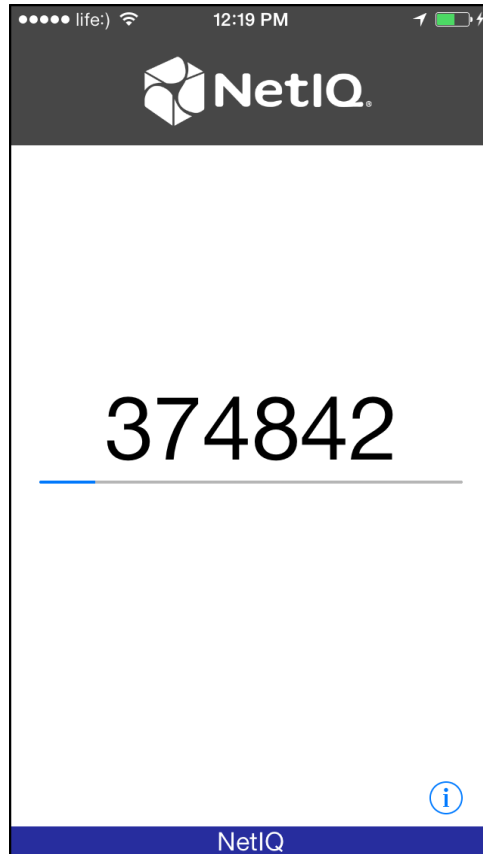
 To turn on the PIN, tap the **PIN is turned off. Tap to turn on** button at the main menu of NetIQ Smartphone Authenticator. Tap the **Clear PIN** button to specify your PIN. Enter your new PIN and tap **OK** to save it.




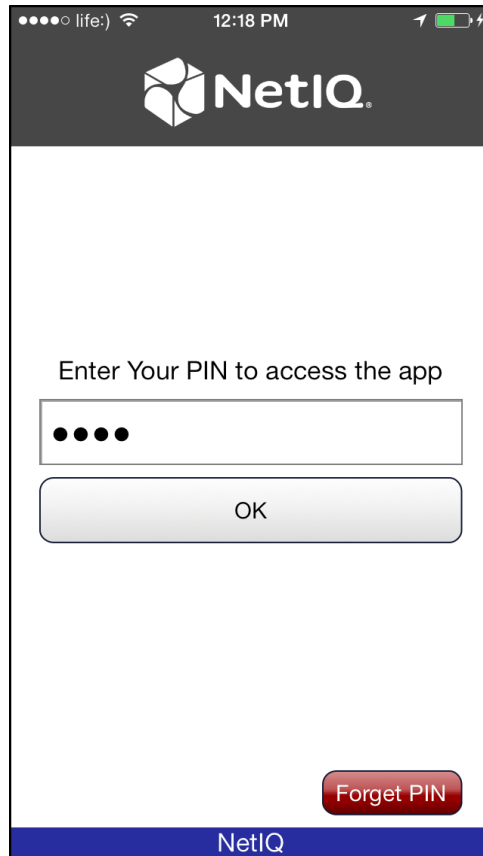
4. Tap the **Scan QR to load config** button to scan the QR code containing the template data.

Next Launches of NetIQ Smartphone Authenticator

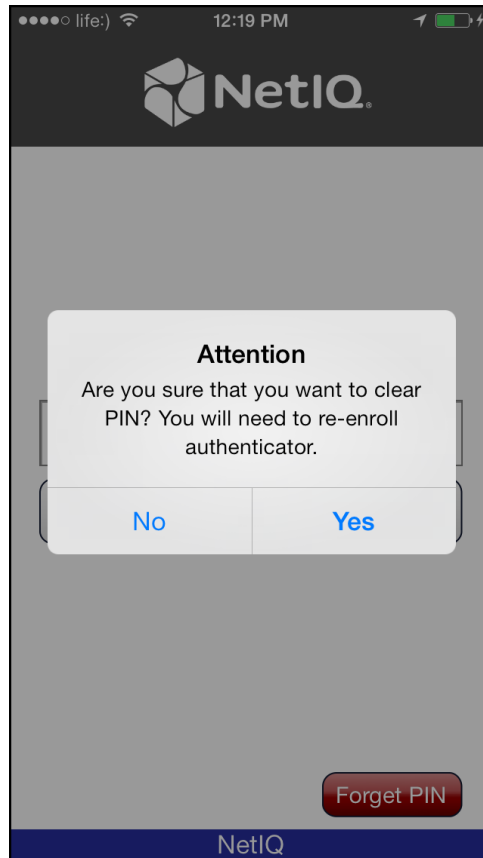
1. Run NetIQ Smartphone Authenticator. The automatically generated OTP will be displayed:



 If you have turned on your PIN, the authorization window will be displayed:

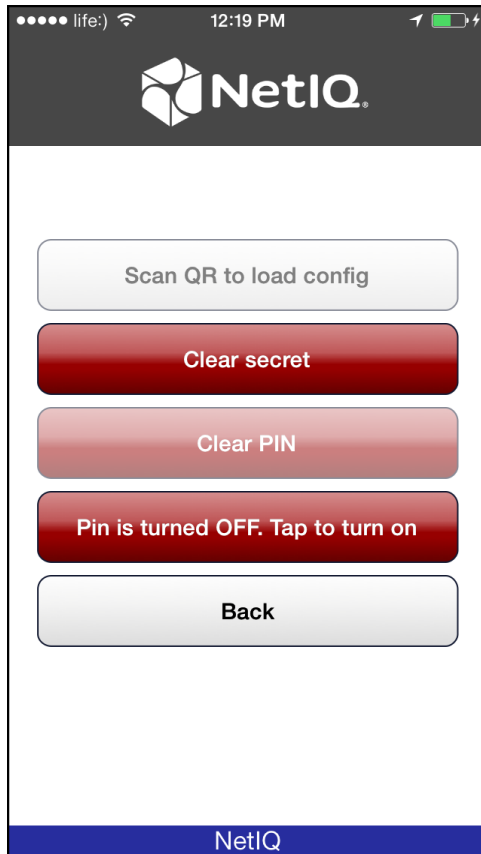


Enter your PIN to access the application and tap **OK**. The automatically generated OTP will be displayed. If you have forgotten your PIN, tap the **Forget PIN** button. The following window will be displayed:



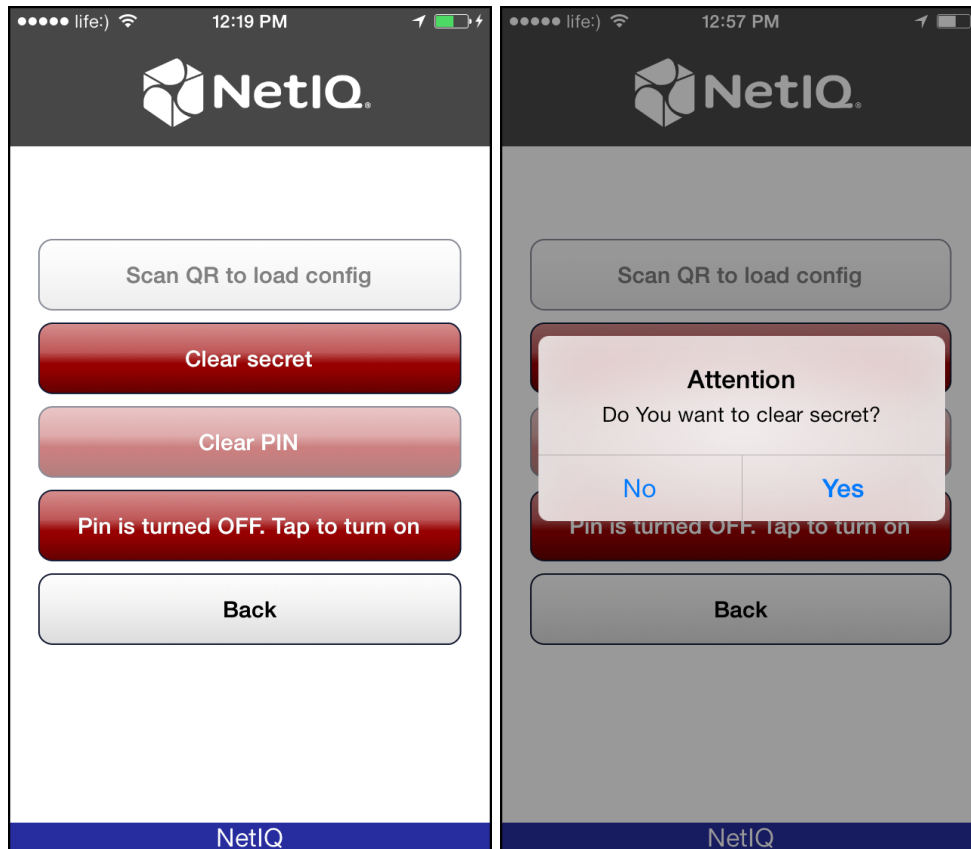
Tap **Yes**, if you want to clear PIN. In this case you will need to re-enroll authenticator. Tap **No**, if you don't want to clear PIN.

2. Tap **Back** to open the main menu of NetIQ Smartphone Authenticator.




Re-enrolling Authenticator

It is possible to enroll authenticator with NetIQ Smartphone Authenticator only one time. To re-enroll authenticator, it is required to clear secret. To do it, tap the **Clear secret** button at the main window of NetIQ Smartphone Authenticator. Tap **Yes** to confirm that you want to clear secret.



When the secret is cleared, the **Scan QR to load config** button will become active. Tap it to scan the QR code containing the template data.

Troubleshooting

 This chapter provides solutions for known issues. If you encounter any problems that are not listed here, please contact the technical support service.

One-Time Password Doesn't Work

Description:

The generated one-time password doesn't work.

Cause:

- a. Group policy is set on the other password generating period.
- b. The password time is out.

Solution:

- a. Check group policy settings.
- b. Try another password.

Index

A

Authentication 1, 3-4
Authenticator 3, 5-6, 9, 13

C

Client 3

L

Logon 3

O

OATH 1, 3-5
One-time Password 4
OTP 3-4, 9

P

Password 4-5, 14
PIN 7, 9

T

TOTP 4