



NetIQ Advanced Authentication Framework - Smartphone Applications

User Guide

Version 3.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
System Requirements	4
Install Smartphone Application	5
Usage of the app on iOS	6
First Launch	7
Enrollment	11
Further Launches	14
Smartphone Authentication	16
TOTP and Offline Authentication	19
Manage Authenticators	20
Forgotten PIN	23
Usage of the app on Android	25
First Launch	26
Enrollment	29
Further Launches	32
Smartphone Authentication	34
TOTP and Offline Authentication	37
Manage Authenticators	38
Forgotten PIN	41
Troubleshooting	43
Enrollment can't be performed	43
Authentication using NetIQ Smartphone Authenticator Fails	45
One-Time Password Doesn't Work	46
Index	47

Introduction

About This Document

Purpose of the Document

This Smartphone Applications User Guide is intended for users and describes where to download the application for your platform and how to enroll and authenticate using your smartphone in environment with NetIQ Advanced Authentication Framework deployed.

Document Conventions

This document uses the following 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, and buttons are put in bold type, e.g.: the **Logon** window.

System Requirements

The following operating systems are supported:

- Apple iOS 8/ 9
- Google Android 4.2/ 4.3/ 4.4/ 5.1/ 6.0, 3 megapixel camera with the autofocus function.
- Windows Phone 8.1/ 10, 3 megapixel camera with the autofocus function.

Install Smartphone Application

Use one of the links to download the application in iTunes or Google Play:

[Authasas Smarpthone Authenticator for iOS](#)

[Authasas Smartphone Authenticator for Android](#)

Choose your platform to explore the technical materials regarding usage of the app:

- [Apple iOS](#)
- [Google Android](#)

Usage of the app on iOS

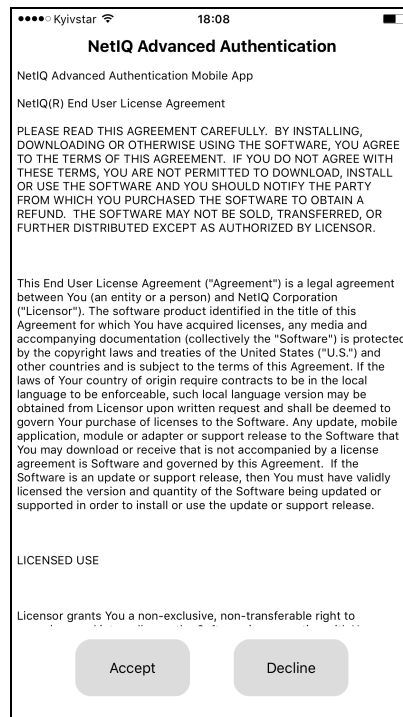
Select a chapter from the list:

- [First launch](#)
- [Enrollment](#)
- [Further launches](#)
- [Smartphone Authentication](#)
- [TOTP and Offline Authentication](#)
- [Manage Authenticators](#)
- [Forgotten PIN](#)

First Launch

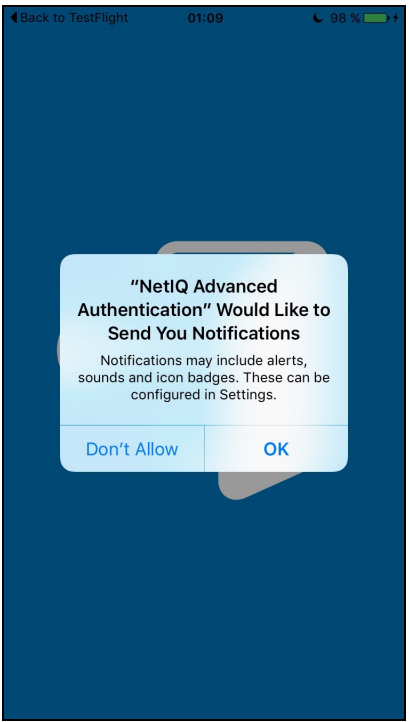


1. Use the  icon to run the NetIQ Advanced Authentication application.
2. You will see a license agreement. Please read carefully and tap **Accept** if you accept the license agreement.

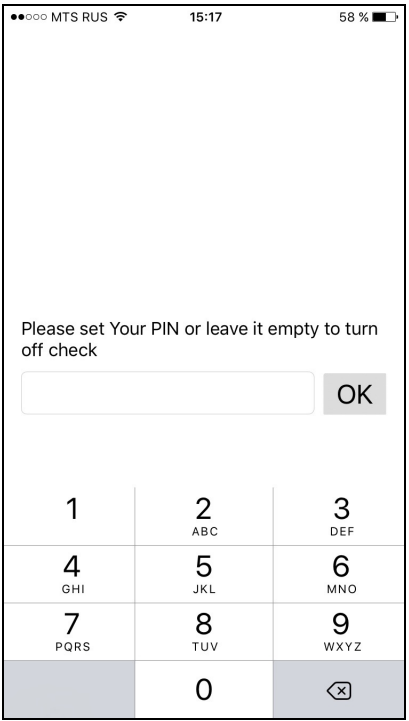


3. You will get a system message "*NetIQ Advanced Authentication*" *Would Like to Send You Notifications*.

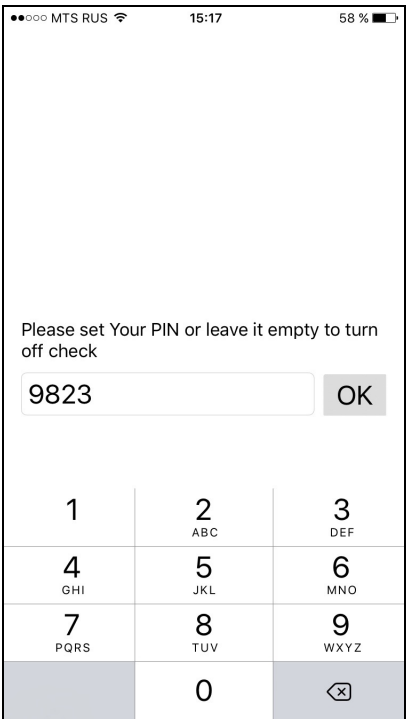
It's recommended to have the push notification enabled. Tap **OK** to enable the push notification.



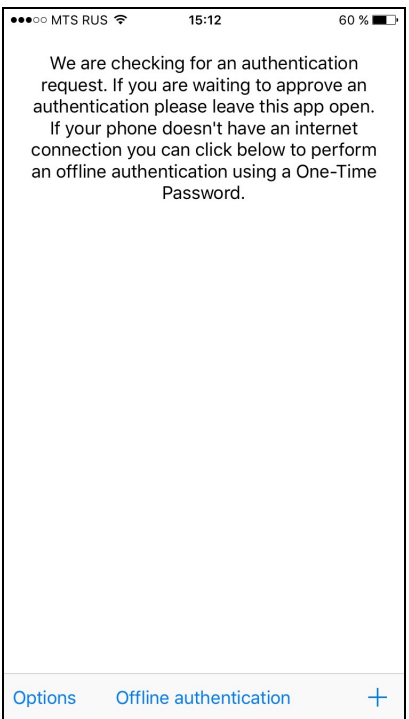
4. You will see a message *Please set Your PIN or leave it empty to turn off check.*



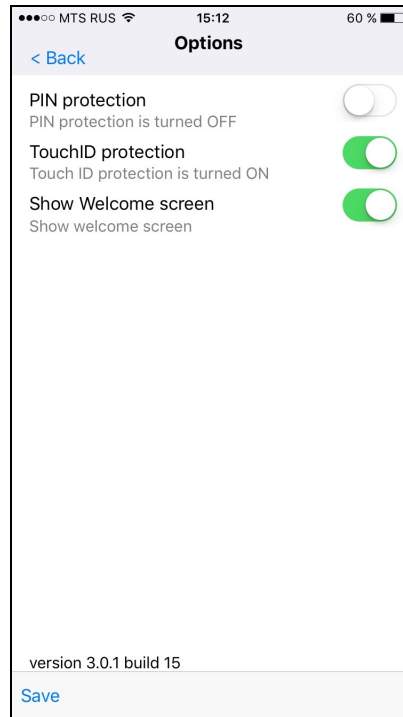
It's recommended to specify a PIN code to secure access to the app. Specify a PIN code or leave the PIN field empty and tap **OK**.



5. You will see the Welcome screen.



6. If your device supports Touch ID, tap **Options** in the bottom menu. Enable the **TouchID protection** option. Tap **Save** in the bottom menu to save the settings.

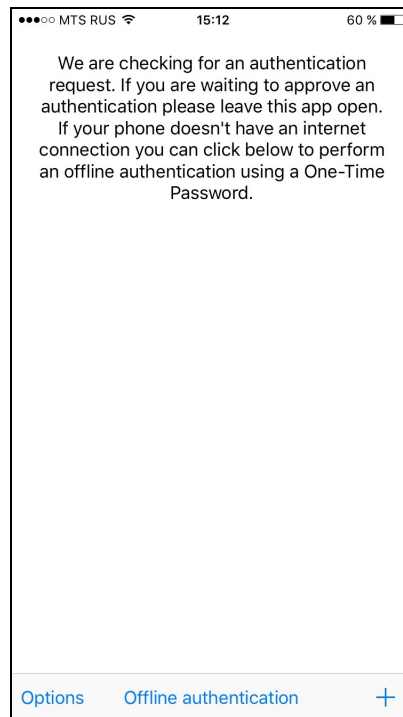


7. If you are going to enroll a TOTP authenticator (not Smartphone), you can disable the Welcome screen for ease of use. To do it disable the **Show Welcome screen** option in the **Options**. Then tap **Save**.

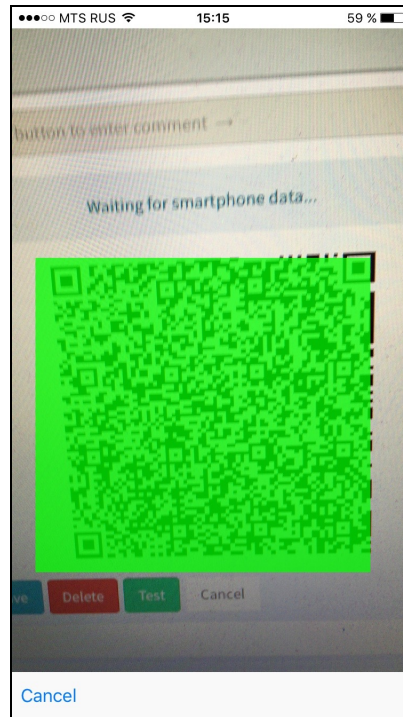
Enrollment

Before starting enrollment on the smartphone app, initialize enrollment in NetIQ Advanced Authentication Self-Service Portal (Smartphone or TOTP method) or NetIQ Web Enrollment Wizard (Smartphone or OATH OTP authenticator) or NetIQ Client - Enrollment Wizard.

1. When you see a QR code on the screen, tap + button in the bottom menu of the Welcome screen.



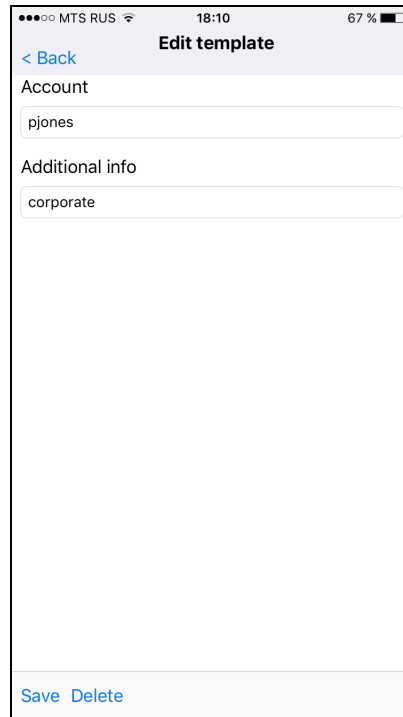
2. Use camera of your device to capture the shown QR code.



The screen will be closed automatically when a compliant QR code is captured.

i If you see a red square over the QR code you are likely trying to scan a non-compliant QR code. Contact your system administrator.

3. You may enter the **Account** and **Additional information** for the authenticator.

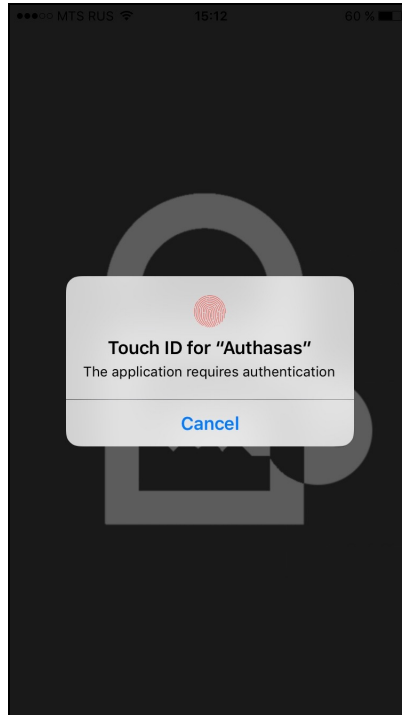


4. Tap blank space to hide the onscreen keyboard. Then tap **Save** in bottom of the screen to save the authenticator. You will be switched back to the Welcome screen.

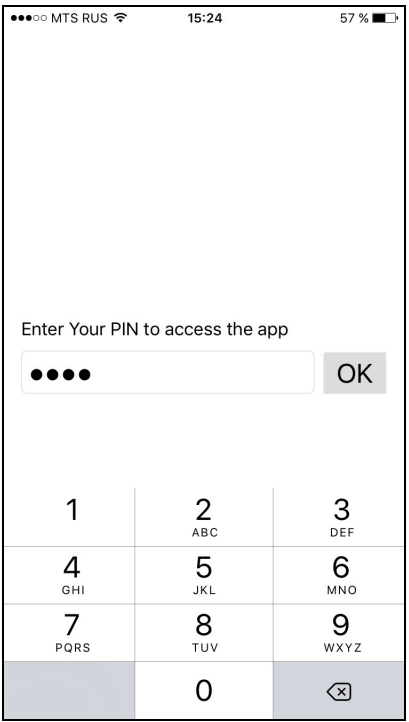
Further Launches



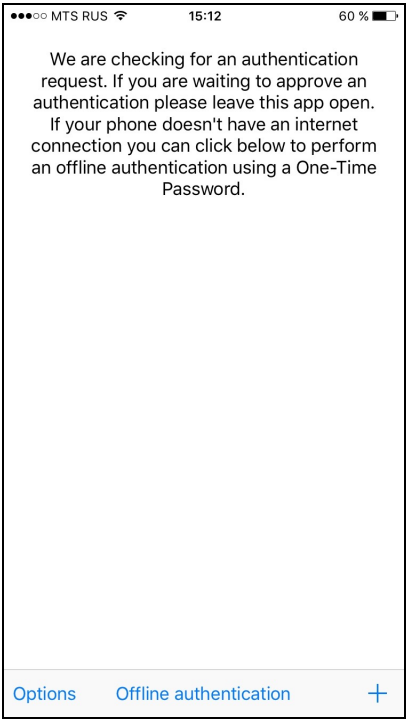
1. Use the icon to run the NetIQ Advanced Authentication application.
2. You will either get a Touch ID request and you will need to provide your fingerprint.



Or you will need to enter a PIN code (if applicable) and then tap **OK**.



You will see the Welcome screen if you have successfully authenticated to use the app.



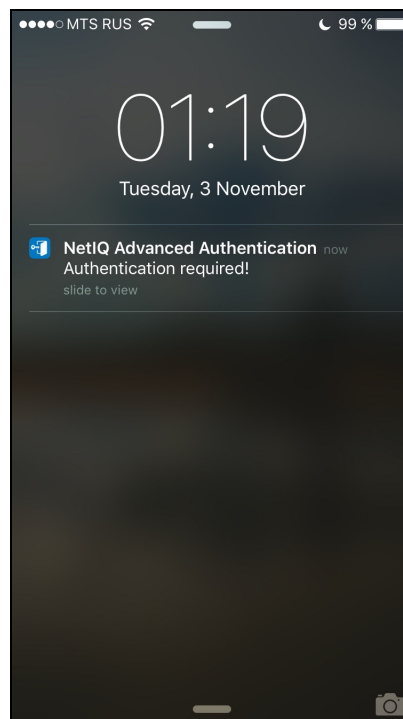
Smartphone Authentication

To authenticate using the smartphone application (if your device has an internet connection), initialize the authentication on your endpoint.

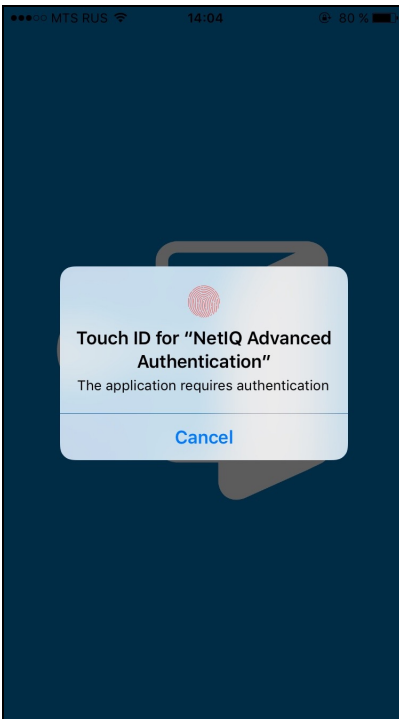
? If push notification wasn't received within several seconds, run the application manually and authorize in it. Temporary troubles with push notifications may be related to Apple push services.

? Push notifications are not supported if you have a TOTP authenticator enrolled. [Check the following article.](#)

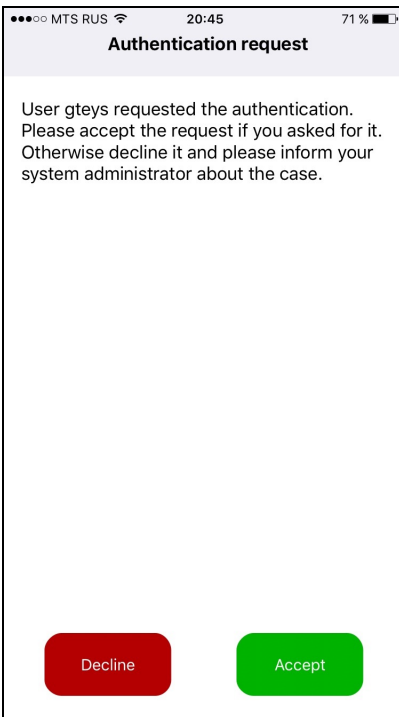
1. You will be notified with a push notification *Authentication required!*, if your device is locked or the smartphone application is closed.



2. Slide the notification, authorize in the app (Touch ID or PIN protection, if applicable).



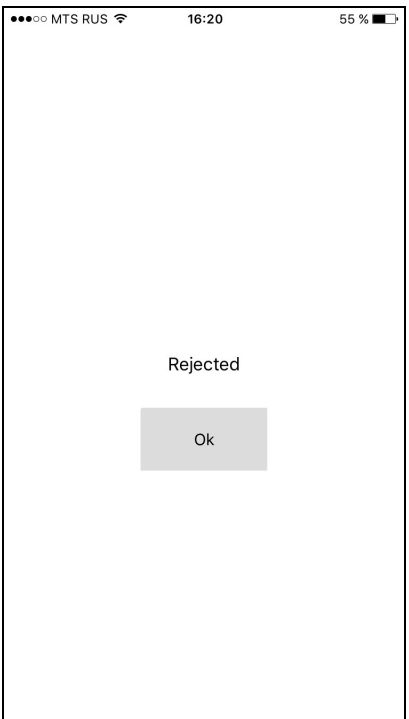
3. Tap **Accept** button to accept the authentication request. If you didn't request the authentication tap **Decline** to reject the authentication request.



You will see the message *Accepted* if you accepted the authentication request.



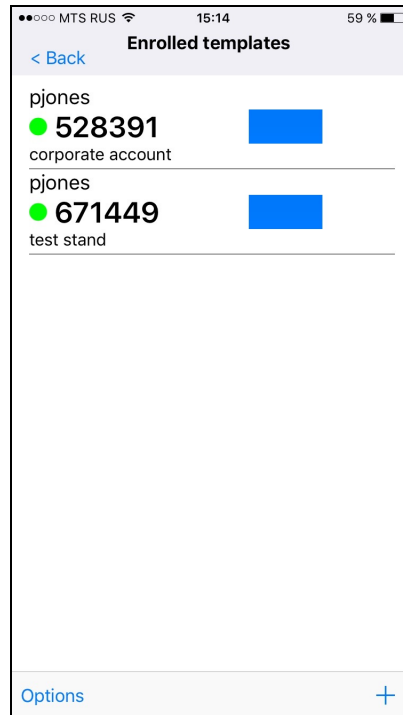
Or you will see the message *Rejected* if you rejected the authentication request.



TOTP and Offline Authentication

If your device doesn't have an internet connection or you have the TOTP method (not Smartphone) enrolled follow the instruction to perform authentication.

1. On the Welcome screen tap **Offline authentication** button. You will see a list of enrolled authenticators.



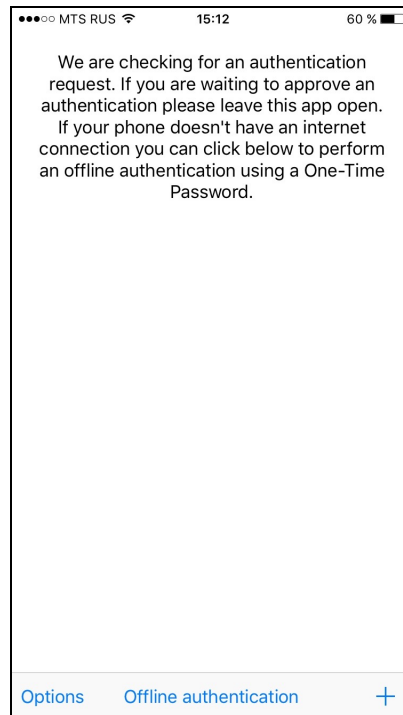
2. Use a shown one-time password value to authenticate.

 If you are not able to authenticate ensure that a time on your device is synchronized.

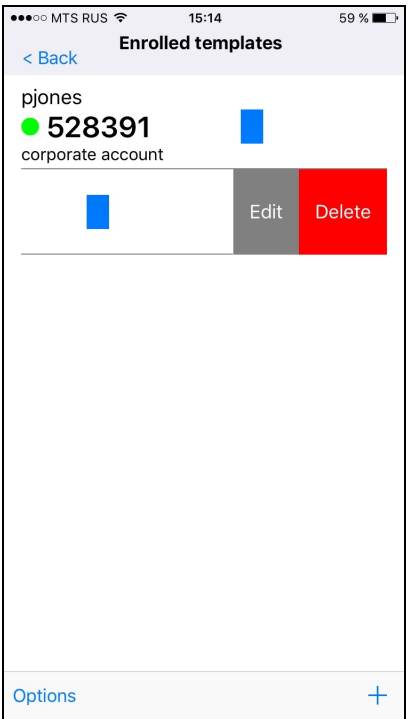
Manage Authenticators

To manage the existing authenticators follow the instruction:

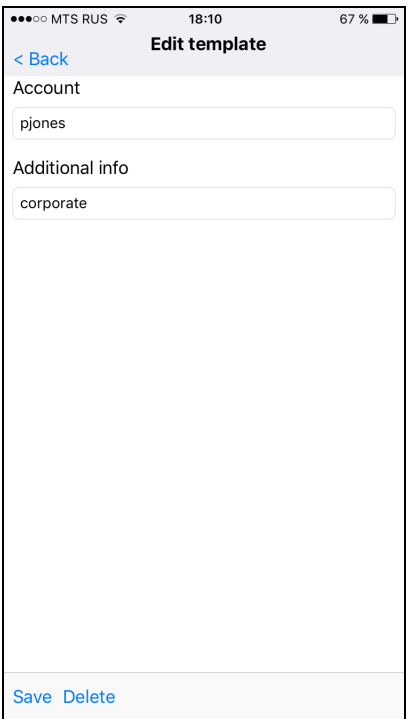
1. On the Welcome screen tap **Offline authentication** button.



2. Slide an authenticator which you want to edit or delete to left. You will see the **Edit** and **Delete** buttons.

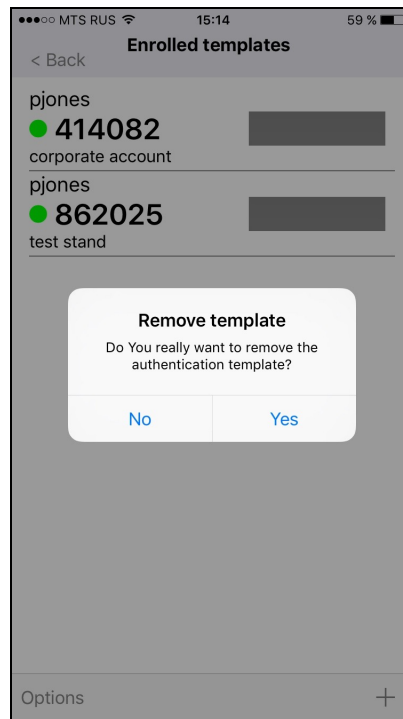


3. Tap **Edit** button if you want to edit information on the enrolled authenticator. Make required changes in the **Account** and **Additional info** fields.



Tap blank space to hide the onscreen keyboard. Then tap **Save** to save the changes.

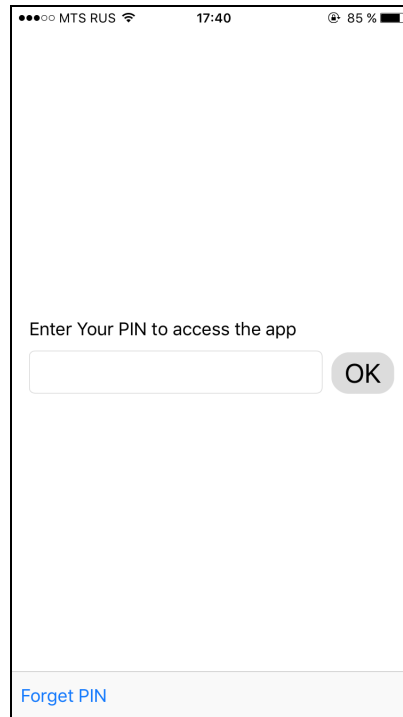
4. Tap **Delete** to remove the enrolled authenticator. You will need to confirm the action by tapping **Yes**.



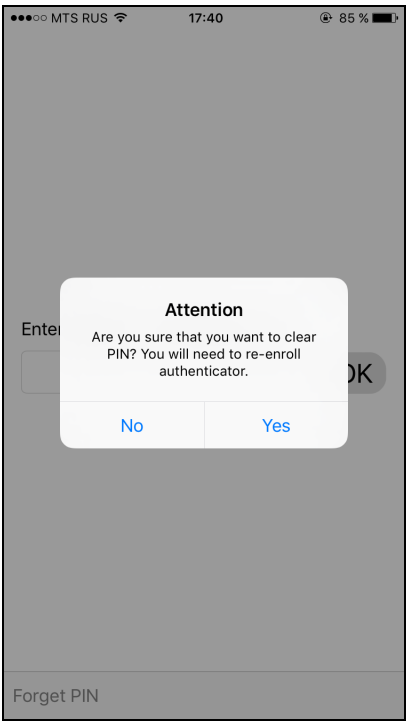
Forgotten PIN

In case of forgotten PIN you will have to reset and re-enroll the existing authenticators.

1. Tap blank space on the PIN request screen to hide the onscreen keyboard (if you see it).
2. Click the menu button to access the menu.



3. Click **Yes** if you agree to reset the enrolled authenticators.



Usage of the app on Android

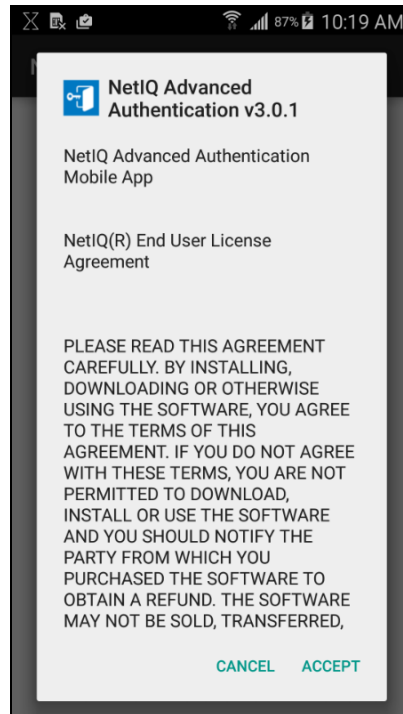
Select a chapter from the list:

- [First launch](#)
- [Enrollment](#)
- [Further launches](#)
- [Smartphone Authentication](#)
- [TOTP and Offline Authentication](#)
- [Manage Authenticators](#)
- [Forgotten PIN](#)

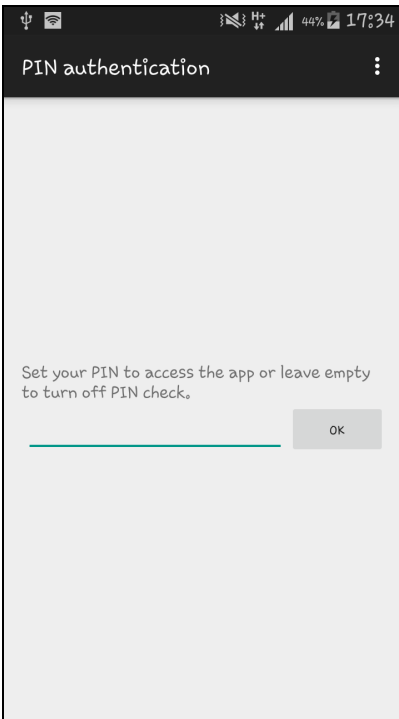
First Launch



1. Use the  icon to run the NetIQ Advanced Authentication application.
2. You will see a license agreement. Please read carefully and tap **ACCEPT** if you accept the license agreement.

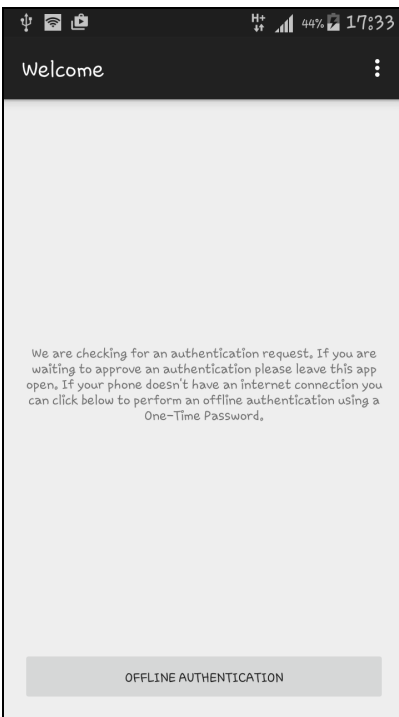


3. Set a PIN to access the app or leave it empty to turn off the PIN check.

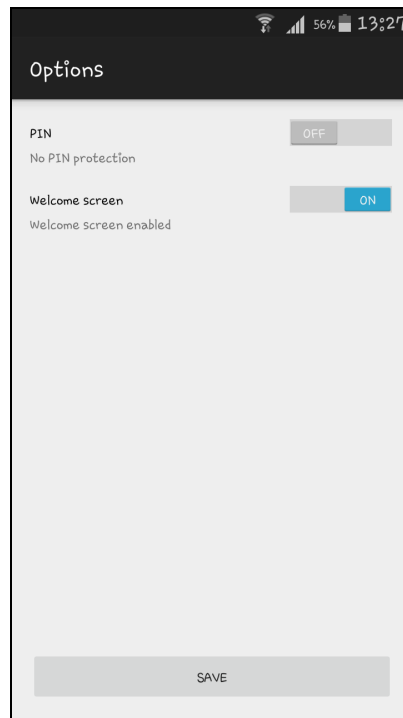


It's recommended to specify a PIN code to secure access to the app. Specify a PIN code or leave the PIN field empty and tap **OK**.

4. You will see the Welcome screen.



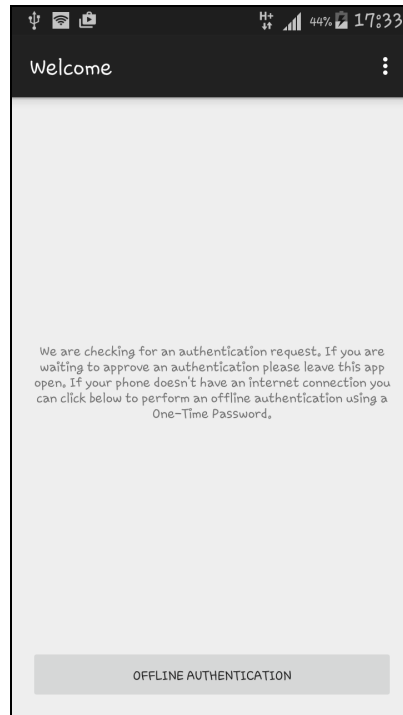
5. If you are going to enroll a TOTP authenticator (not Smartphone), you can disable the Welcome screen for ease of use. To do it tap the menu button, select **Options**. In the opened settings disable the Welcome screen. Then tap **Save**.



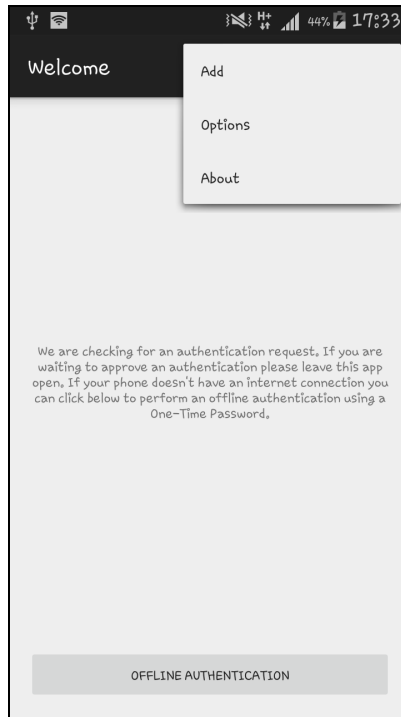
Enrollment

Before starting enrollment on the smartphone app, initialize enrollment in NetIQ Advanced Authentication Self-Service Portal (Smartphone or TOTP method) or NetIQ Web Enrollment Wizard (Smartphone or OATH OTP authenticator) or NetIQ Client - Enrollment Wizard.

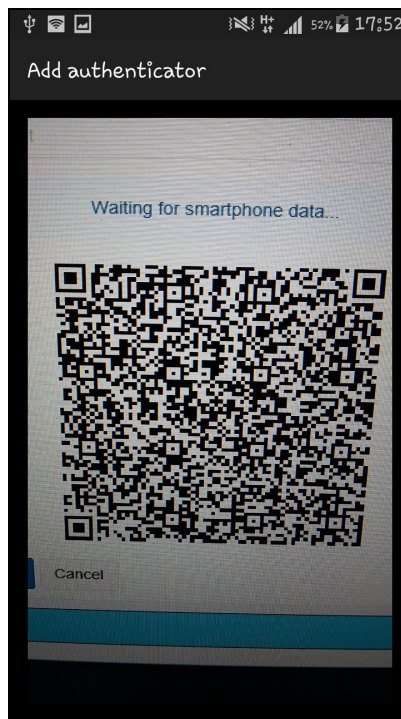
1. When you see a QR code on the screen, tap top right menu button of the Welcome screen.



2. Tap **Add** button.



3. Use camera of your device to capture the shown QR code.



The screen will be closed automatically when a compliant QR code is captured.

 If you see a red square over the QR code you are likely trying to scan a non-compliant QR code. Contact your system administrator.

4. You may enter the **Account** and **Additional information** for the authenticator.

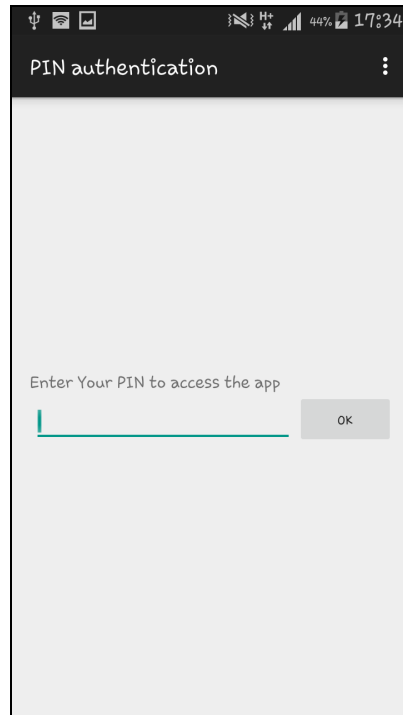


4. Tap **Save** to save the authenticator. You will be switched back to the Welcome screen.

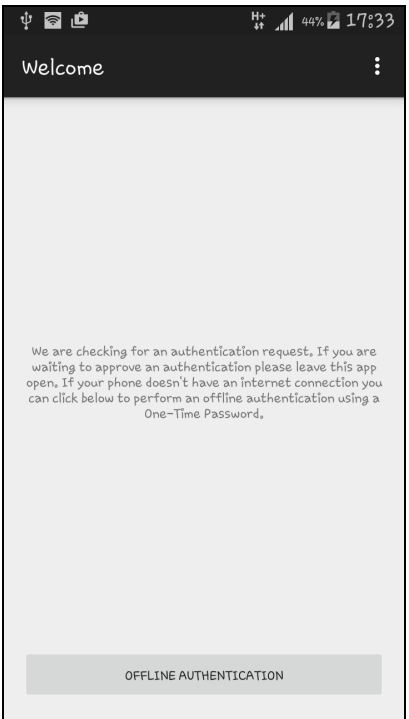
Further Launches



1. Use the  icon to run the NetIQ Advanced Authentication application.
2. You will need to enter a PIN code (if applicable) and then tap **OK**.



You will see the Welcome screen if you have successfully authenticated to use the app.



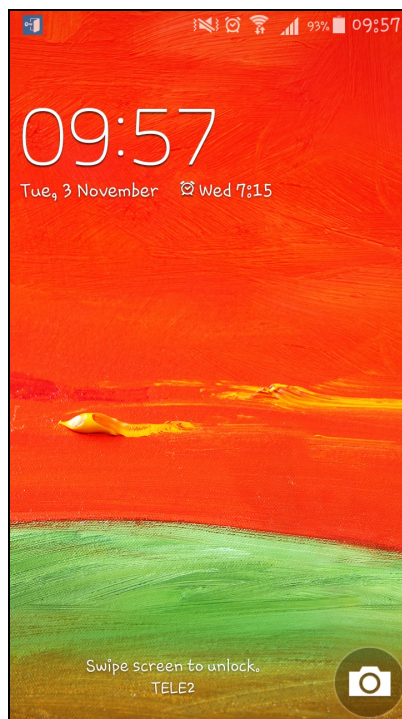
Smartphone Authentication

To authenticate using the smartphone application (if your device has an internet connection), initialize the authentication on your endpoint.

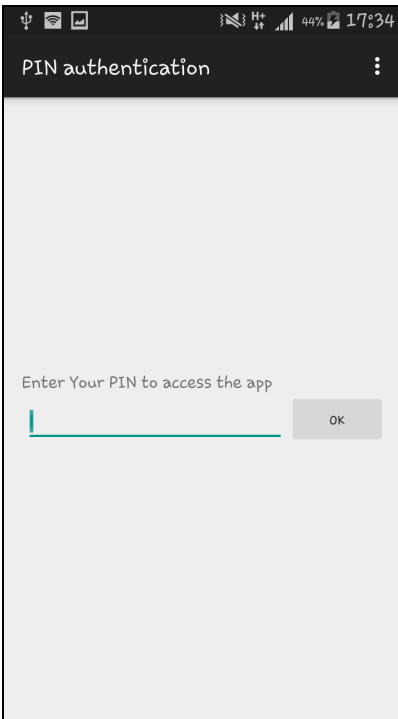
? If push notification wasn't received within several seconds, run the application manually and authorize in it. Temporary troubles with push notifications may be related to Google push services.

? Push notifications are not supported if you have a TOTP authenticator enrolled. [Check the following article.](#)

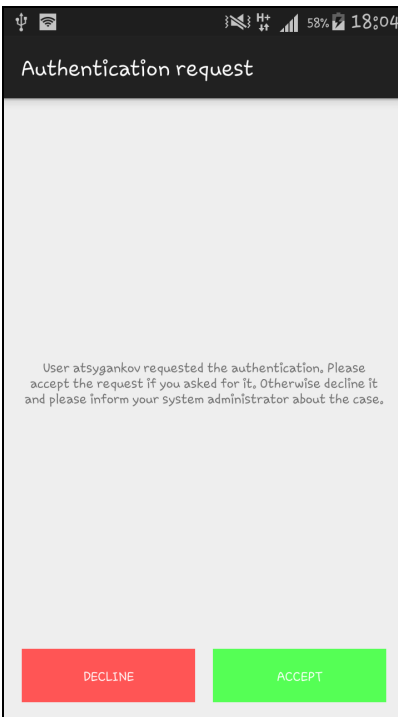
1. You will be notified with a push notification *Authentication required!*, if your device is locked or the smartphone application is closed.



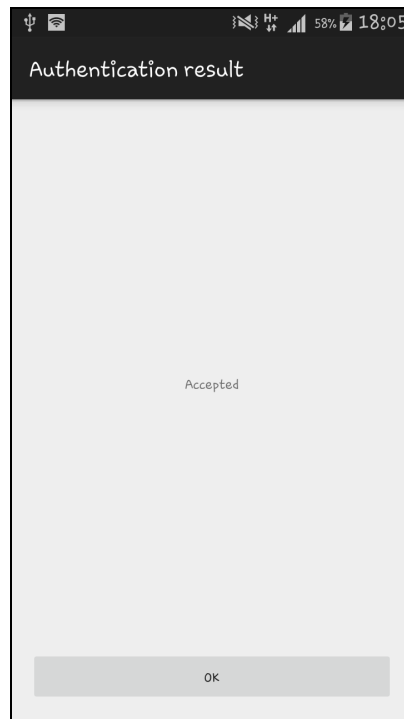
2. Unlock the device and authorize in the app.



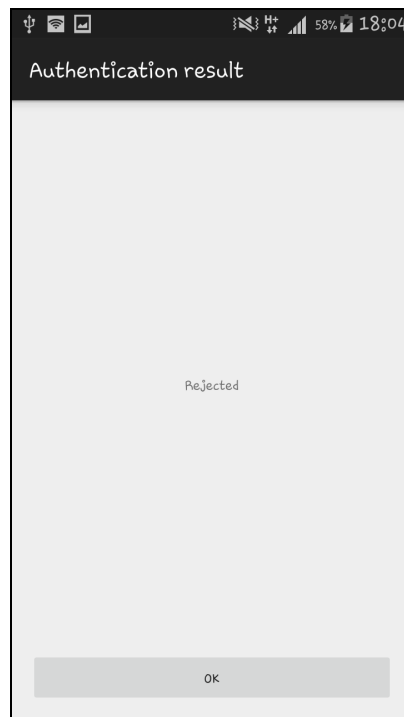
3. Tap **ACCEPT** button to accept the authentication request. If you didn't request the authentication tap **DECLINE** to reject the authentication request.



You will see the message *Accepted* if you accepted the authentication request.



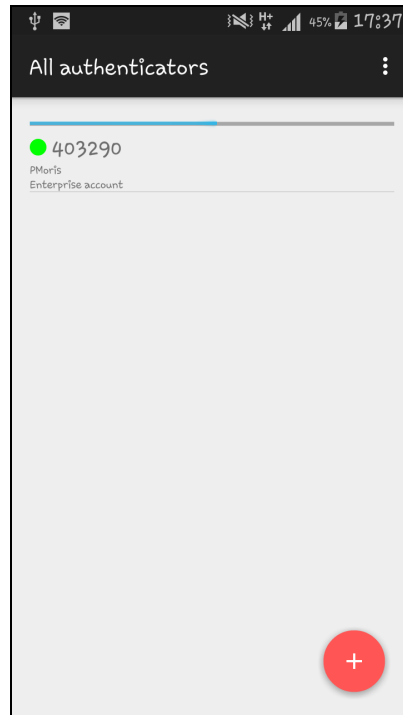
Or you will see the message *Rejected* if you rejected the authentication request.



TOTP and Offline Authentication

If your device doesn't have an internet connection or you have the TOTP method (not Smartphone) enrolled follow the instruction to perform authentication.

1. On the Welcome screen tap **Offline authentication** button. You will see a list of enrolled authenticators.



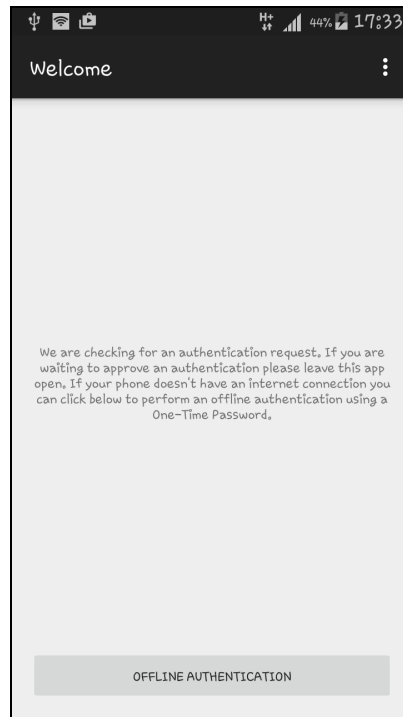
2. Use a shown one-time password value to authenticate.

 If you are not able to authenticate ensure that a time on your device is synchronized.

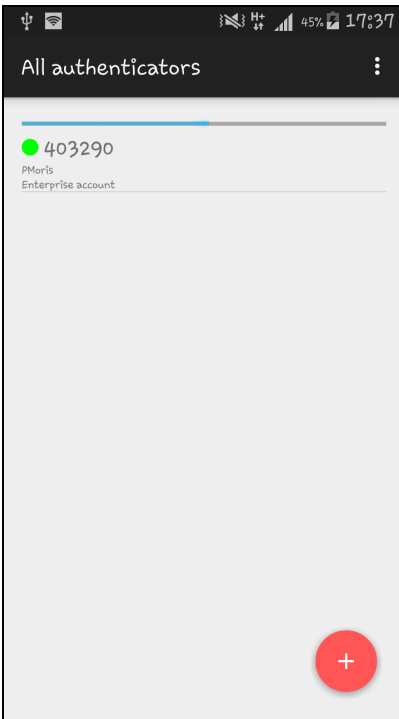
Manage Authenticators

To manage the existing authenticators follow the instruction:

1. On the Welcome screen tap **OFFLINE AUTHENTICATION** button.

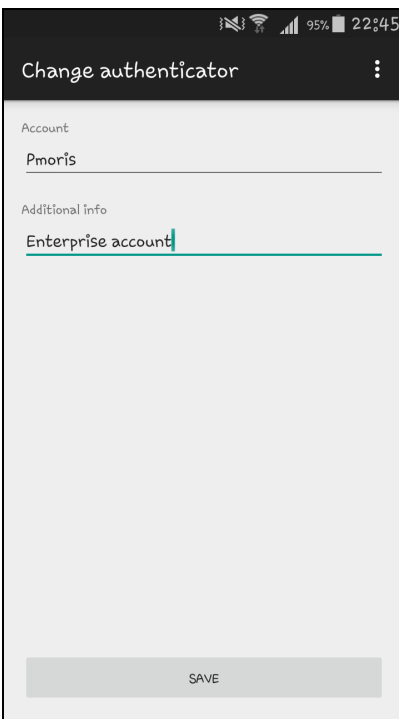


2. Tap an authenticator which you want to edit or delete.

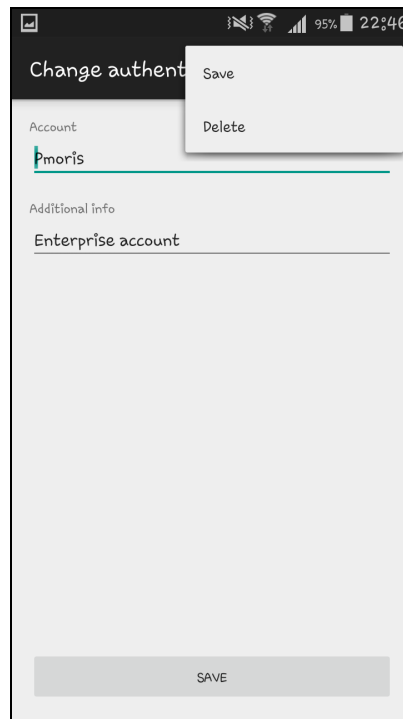


You will see the **Change authenticator** screen.

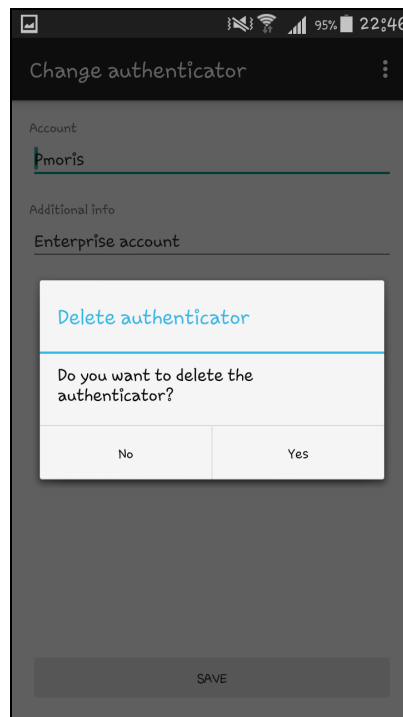
3. If you want to change Account or Additional info make the changes and then tap **Save**.



4. If you want to remove the authenticator, tap menu button and then tap **Delete** to remove the enrolled authenticator.



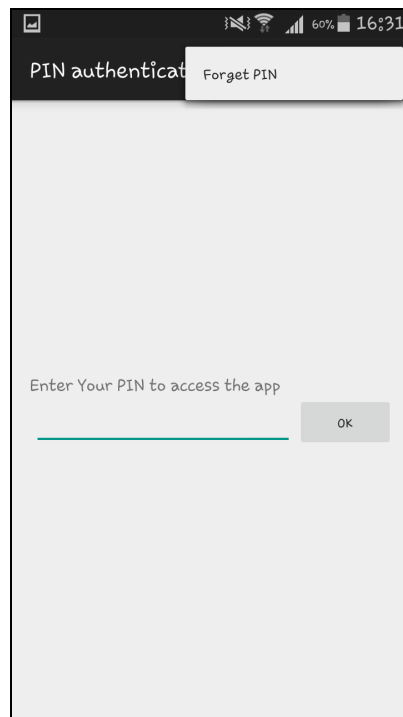
You will need to confirm the action by tapping **Yes**.



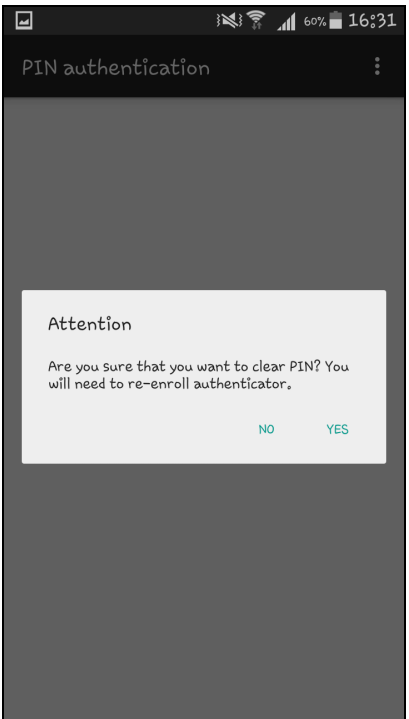
Forgotten PIN

In case of forgotten PIN you will have to reset and re-enroll the existing authenticators.

1. Click the menu button to access the menu.



2. Click **YES** if you agree to reset the enrolled authenticators.



Troubleshooting

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

Enrollment can't be performed

Description:

Can't scan a QR code.

Issues:

I). My smartphone can't scan a QR code.

II). I get the following message after when a QR code is scanned:

Android app: *Please ask your admin if the error will be repeated: Device add error*

iOS app: *Error: JSONEmptyField, message: The field AddDeviceResult is an empty string*

Windows Phone app: *Can't load the authenticator: Salt is null or empty*

Causes:

I). The app supports only NetIQ Advanced Authentication compliant QR codes. The other QR codes can't be scanned with the NetIQ smartphone app.

II) Incorrect configuration.

Solution:

I)

1. Ensure that you are trying to scan a QR code

1.1. In NetIQ Advanced Authentication Self-Service Portal for **Smartphone** or **TOTP** method. In case of TOTP method usage probably the Google Authenticator format of QR code is enabled. Contact your system administrator to check this.

1.2. In NetIQ Advanced Authentication Web Enrollment Wizard for **Smartphone** or **OATH OTP** method (when TOTP mode is selected).

1.3. Using Smartphone or OATH OTP method within a first logon on workstation or later in Authenticators Management. A QR code which is shown in **OATH - Enroll** window may be too small (depending on screen resolution). It's recommended to perform the enrollment through

the NetIQ Advanced Authentication Web Enrollment Wizard, because it shows the larger QR codes and the Web Enrollment Wizard improves the user's experience in OATH OTP authenticator enrollment.

II) Administrator should verify correctness of Smartphone method configuration. This may be related to a conflict on IP address/port.

Recommendations:

I)

- a. Ensure that mouse cursor doesn't overlap the QR code.
- b. If you are enrolling the authenticator in browser try to zoom in the page with the QR code to 125-150%. It may be required for screens with high resolution.
- c. Try to enroll on another monitor (brightness, contrast, glossy surface may affect).
- d. Check on the smartphone that the QR code is in focus. Some Android devices has no autofocus feature and may have problems with scanning the QR codes.
- e. Try to use another smartphone.

II) Contact your system administrator.

Authentication using NetIQ Smartphone Authenticator Fails

Description:

Authentication using with NetIQ Smartphone Authenticator fails.

Causes:

1. There is no Internet connection on the Server with Smartphone authentication dispatcher.
2. The authentication timeout.

Solution:

1. You can login with OTP that is automatically generated by NetIQ Smartphone Authenticator.
2. Request the authentication again. Do not wait for push notification. Open the app manually and accept the authentication request.

One-Time Password Doesn't Work

Description:

The generated one-time password doesn't work.

Cause:

- a. There is a significant time drift between your smartphone and server.
- b. Authenticator is invalid or used not correctly.

Solution:

- a. Ensure that a time on your smartphone is synced with a time server. Ensure that you have a valid time zone specified on your smartphone.
- b. Contact your system administrator.

Index

A

Account 12, 21, 31, 39
Administrator 44
Application 5
Authentication 1, 3, 6-7, 11, 14, 16, 25-26, 29, 32, 34, 43, 45
Authenticator 3, 5, 43, 45-46

C

Client 11, 29

D

Delete 20, 40
Device 43

E

Edit 20
Error 43

L

Logon 3

M

Manage 6, 20, 25, 38

O

OATH 11, 29, 43
OTP 43, 45

P

Password 46
PIN 6, 8, 14, 16, 23, 25-26, 32, 41

S

Server 45
System 4

T

TOTP 6, 10-11, 16, 19, 25, 28-29, 34, 37, 43

U

User 1, 3

W

Windows 4, 43