

---

# User Guide

## Advanced Authentication - Smartphone Applications

Version 5.4

## Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

**Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.**

---

# Contents

<b>About NetIQ Corporation</b>	<b>5</b>
<b>About this Book</b>	<b>7</b>
<b>1 System Requirements</b>	<b>9</b>
<b>2 Installing Smartphone Application</b>	<b>11</b>
<b>3 Using the app on iOS</b>	<b>13</b>
3.1 First Launch . . . . .	13
3.2 Enrollment . . . . .	13
3.3 Further Launches . . . . .	14
3.4 Smartphone Authentication . . . . .	14
3.5 TOTP and Offline Authentication . . . . .	14
3.5.1 TOTP and Offline Authentication . . . . .	14
3.6 Manage Authenticators . . . . .	15
3.7 Forgotten PIN . . . . .	15
<b>4 Using the app on Android</b>	<b>17</b>
4.1 First Launch . . . . .	17
4.2 Enrollment . . . . .	17
4.3 Further Launches . . . . .	18
4.4 Smartphone Authentication . . . . .	18
4.5 TOTP and Offline Authentication . . . . .	18
4.6 Manage Authenticators . . . . .	19
4.7 History . . . . .	19
<b>5 Using the App on Windows Phone</b>	<b>21</b>
5.1 First Launch . . . . .	21
5.2 Enrollment . . . . .	22
5.3 Further Launches . . . . .	22
5.4 Smartphone Authentication . . . . .	22
5.5 TOTP and Offline Authentication . . . . .	23
5.6 Manage Authenticators . . . . .	23
5.7 Forgotten PIN . . . . .	23
<b>6 Troubleshooting</b>	<b>25</b>
6.1 Enrollment can't be performed . . . . .	25
6.2 Authentication using Advanced Authentication Smartphone Authenticator Fails . . . . .	26
6.3 One-Time Password Doesn't Work . . . . .	26



---

# About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

## Our Viewpoint

### **Adapting to change and managing complexity and risk are nothing new**

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

### **Enabling critical business services, better and faster**

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

## Our Philosophy

### **Selling intelligent solutions, not just software**

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

### **Driving your success is our passion**

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

## Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

## Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>North and South America:</b>	1-713-418-5555
<b>Europe, Middle East, and Africa:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at [www.netiq.com/documentation](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

## Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit [community.netiq.com](http://community.netiq.com).

---

# About this Book

The Smartphone Applications User Guide has been designed for all users and describes where to download the application for your platform and how to enroll and authenticate your smartphone in the Advanced Authentication environment.

## Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.



---

# 1 System Requirements

The following operating systems are supported:

- ♦ Apple iOS 8/ 9/ 10
- ♦ Google Android 4.2/ 4.3/ 4.4/ 5.1/ 6.0/ 7.0, 3 megapixel camera with the autofocus function.
- ♦ Windows Phone 8.1/ 10/ 10 Anniversary update, 3 megapixel camera with the autofocus function.

---

**NOTE:** If an Advanced Authentication administrator enables the geo-fencing feature, then access to the location must be enabled for the NetIQ Advanced Authentication app on the smartphone. The users must have the updated smartphone apps with Geo-fencing support to use the functionality.

---



---

# 2 Installing Smartphone Application

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

- ♦ [Smartphone Authenticator for iOS](#)
- ♦ [Smartphone Authenticator for Android](#)

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

- ♦ [Using the app on iOS](#)
- ♦ [Using the app on Android](#)
- ♦ [Using the App on Windows Phone](#)



---

# 3 Using the app on iOS

- ◆ [First Launch](#)
- ◆ [Enrollment](#)
- ◆ [Further Launches](#)
- ◆ [Smartphone Authentication](#)
- ◆ [TOTP and Offline Authentication](#)
- ◆ [Manage Authenticators](#)
- ◆ [Forgotten PIN](#)

## 3.1 First Launch

1. Click the  icon to run the Advanced Authentication application.
2. Accept the license agreement.
3. A message `Please set Your PIN` is displayed. Specify a PIN to access the app and tap **OK**.
4. A message `Advanced Authentication Would Like to Send You Notifications` is displayed.  
It is recommended to enable the push notification. Tap **OK** to enable the push notification.  
A Welcome screen is displayed.
5. If you want to enroll a TOTP authenticator (other than Smartphone), you can hide the Welcome screen by disabling the **Show Welcome screen** option in **Options**. Tap **Save**.

## 3.2 Enrollment

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

---

**TIP:** 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.

## 3.3 Further Launches

1. Use the  icon to run the 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.

## 3.4 Smartphone Authentication

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

---

**TIP:** 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 [TOTP and Offline Authentication](#).

---

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.

## 3.5 TOTP and Offline Authentication

### 3.5.1 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.

---

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

---

## 3.6 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**.

## 3.7 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. Tap **Forget PIN**.
3. Tap **Yes** if you agree to reset the enrolled authenticators.



---

# 4 Using the app on Android

Select a chapter from the list:

- ◆ [First Launch](#)
- ◆ [Enrollment](#)
- ◆ [Further Launches](#)
- ◆ [Smartphone Authentication](#)
- ◆ [TOTP and Offline Authentication](#)
- ◆ [Manage Authenticators](#)
- ◆ [History](#)

---

**NOTE:** [Allow mock locations](#) option in [Developer options](#) of smartphone settings must be disabled.

---

## 4.1 First Launch

1. Use the  icon to run the 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.
4. You will see the Welcome screen.

## 4.2 Enrollment

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

1. When you see a QR code on the screen, tap + button.
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.

---

**TIP:** 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 **Save** to save the authenticator. You will be switched back to the Enrolled Authenticators screen.

## 4.3 Further Launches

1. Use the  icon to run the Advanced Authentication application.
2. You will need to enter the PIN code.

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

---

**NOTE:** All the information will be erased after 10 continuous attempts to authenticate with wrong pin. You will have to re-enroll all the authenticators after the wipe.

---

## 4.4 Smartphone Authentication

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

---

**TIP:** 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 [TOTP and Offline Authentication](#).

---

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.

---

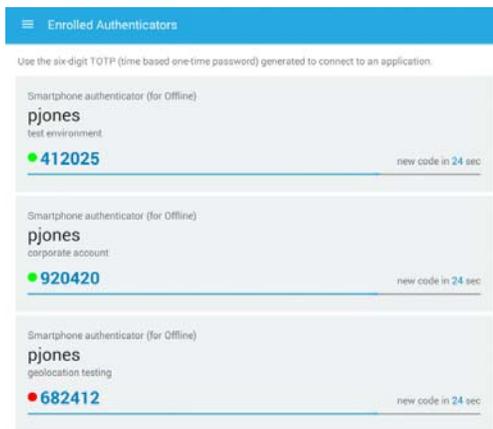
**NOTE:** **ACCEPT** and **REJECT** buttons are disabled (grayed out) when the server requests for the authenticator's location and until the location is available.

---

## 4.5 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 menu button and then tap **Enrolled Authenticators** button. You will see a list of enrolled authenticators.



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

---

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

---

---

**NOTE:** Offline logon is not possible when Geo-fencing feature is enabled. In such case you will see the message `TOTP login is disabled` on the endpoint side.

---

## 4.6 Manage Authenticators

To manage the existing authenticators follow the instruction:

1. On the Welcome screen tap menu button and then tap **Enrolled Authenticators** 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 **Delete** button.  
You will need to confirm the action by tapping **Yes**.

## 4.7 History

You can view the history of authentication requests. The status of the authentication requests can be viewed and if there are any suspicious requests, you can report them to the administrator.

1. Tap the menu button to access the menu.
2. Tap Request History.



---

# 5 Using the App on Windows Phone

This section contains the following sub sections:

- ◆ [First Launch](#)
- ◆ [Enrollment](#)
- ◆ [Further Launches](#)
- ◆ [Smartphone Authentication](#)
- ◆ [TOTP and Offline Authentication](#)
- ◆ [Manage Authenticators](#)
- ◆ [Forgotten PIN](#)

## 5.1 First Launch

1. Tap the smartphone  icon to run the Advanced Authentication application. A message `Enter new PIN or leave it empty` is displayed.
2. Specify a PIN code in the text box or leave the PIN text box blank and tap **OK**. The **Authentication Check** screen is displayed.

---

**NOTE:** It is recommended to specify a PIN code for secure access to the app.

---

3. You can disable the **Authentication Check** screen if you want to enroll a TOTP authenticator (other than smartphone).

To disable the screen:

- a. Tap on the Properties icon and select options. The **Options** screen is displayed.
  - b. Slide the **Welcome screen** switch to the left. The option is now grayed out.
4. Tap **Save** to save the settings.

---

**NOTE:** You can enable or disable the **Use location service** option in the Windows phone app. However, it is not recommended to disable the option as Advanced Authentication server may require geo location check for successful authentication.

---

## 5.2 Enrollment

Before you start an enrollment on the smartphone app, you need to enroll yourself in the Advanced Authentication Self-Service Portal (Smartphone or TOTP method) or Web Enrollment Wizard (Smartphone or OATH OTP authenticator) or Client - Enrollment Wizard.

To enroll on the smartphone app, perform the following steps:

1. After you start the enrollment, a QR code is displayed on the screen. Tap the plus  icon in the lower part of the **Welcome screen**. The application directs the screen to the camera of your phone.
2. Place the camera of the phone in a direction to capture the QR code on the screen. A green square is displayed over the QR code. The screen is automatically closed when a compliant QR code is captured.

---

**NOTE:** If you see a red square over the QR code, you are trying to scan a non-compliant QR code. Contact your system administrator for further assistance.

---

3. After the QR code is successfully scanned, the **Change authenticator** screen is displayed. Enter a relevant name for your account in the **Account name** text box and information about your account in the **Additional info** text box.
4. Tap on the Save  icon to save the authenticator settings. The authenticator settings are saved and the screen navigates back to the Welcome screen.

## 5.3 Further Launches

1. Tap the smartphone authenticator  icon to run the Advanced Authentication application.
2. Enter a PIN (if you have specified) to access the app and tap **OK**. The Welcome screen is displayed.

## 5.4 Smartphone Authentication

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

---

**NOTE:** If you did not receive a push notification within several seconds, run the application manually and authorize on it. Temporary troubles with push notifications may be related to Microsoft push services.

Push notifications are not supported if you have a TOTP authenticator enrolled. See [TOTP and Offline Authentication](#) for more information.

---

1. A push notification **Authentication required!**, is sent to your device if your device is locked or the smartphone application is closed.
2. Unlock the smartphone and authorize in the app with the PIN (if applicable).
3. The screen displays the **Accept** and **Reject** buttons. Tap **Accept** to accept the authentication request or **Decline** to decline the request.

An Accepted or Rejected message is displayed on the smartphone based on the selection.

## 5.5 TOTP and Offline Authentication

If there is no internet connection on your device or the TOTP method (other than smartphone) is enrolled, perform the following steps to perform authentication.

1. On the **Welcome screen** tap **Offline authentication**. A list of enrolled authenticators are displayed along with the One Time Passwords (OTP).
2. Use an appropriate OTP from the list to authenticate.

---

**NOTE:** If you are not able to authenticate, ensure that the time on your device is synchronized.

---

## 5.6 Manage Authenticators

You can edit or delete the existing authenticators on your smartphone.

1. On the Welcome screen tap **Offline authentication**.
2. Tap on the authenticator that you want to edit or delete. The **Change Authenticator** screen is displayed.
3. If you want to edit the authenticator, make the changes in the **Account name** and the **Additional info** text boxes and tap the save  icon to save the changes.
4. Alternatively, if you want to delete the authenticator, tap the delete icon. A confirmation message is displayed for the deletion. Tap **OK** to delete the authenticator.

## 5.7 Forgotten PIN

If you have forgotten your PIN, you will have to reset and re-enroll the existing authenticators.

1. Tap anywhere on the blank screen around the **Enter your PIN to access the app** text box to hide the keyboard and display **Forget PIN** button.
2. Tap on the **Forget PIN** button. A message is displayed to confirm whether you want to clear the PIN and re-enroll the authenticators.
3. Tap **OK** to reset the enrolled authenticators.



---

# 6 Troubleshooting

---

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

---

## 6.1 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 Advanced Authentication compliant QR codes. The other QR codes can't be scanned with the Advanced Authentication smartphone app.

II) Incorrect configuration.

### Solution:

I)

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

1.1. In 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 Advanced Authentication Web Enrollment Wizard for 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 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.

## **6.2 Authentication using Advanced Authentication Smartphone Authenticator Fails**

### **Description:**

Authentication using with Advanced Authentication 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 Advanced Authentication Smartphone Authenticator.
2. Request the authentication again. Do not wait for push notification. Open the app manually and accept the authentication request.

## **6.3 One-Time Password Doesn't Work**

### **Description:**

The generated one-time password doesn't work.

### **Cause:**

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

### **Solution:**

1. 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.
2. Contact your system administrator.