User Guide

Advanced Authentication - Smartphone Applications

Version 5.6

Legal Notices

Contents

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.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

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. You can also email 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.

About this Book

The Smartphone Applications User Guide has been designed to guide users about how to download the application for the different platforms. The guide also guides users about how to enroll and authenticate the smartphone in the Advanced Authentication environment.

Intended Audience

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

1 System Requirements

Before installing, ensure the following system requirements are met depending on the Smartphone you have:

- Apple iOS 9/ 10 is installed for iphone.
- Google Android 4.4.4/ 5.1/ 6.0/ 7.0, 3 megapixel camera with the autofocus function is supported on an Android Smartphone.
  - The Android phone must have a fingerprint scanner to use fingerprint sensor to access the application. The minimum version is Android 6 and later. The Android device must support Google Fingerprint Authentication API. For example, Samsung Galaxy Note 4 on Android 6 does not support Google Fingerprint Authentication API and fingerprint does not work in the application. Fingerprint is mostly supported for Android devices that were released after 2015.
- Windows Phone 10/ 10 Anniversary update, 3 megapixel camera with the autofocus function is supported on a Windows phone.

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.Users must have the updated smartphone apps with geo-fencing support to use the functionality.

2 Installing the Smartphone Application

Perform the following steps for a new installation of the Smartphone application.

1. You can download smartphone application from iTunes or Google Play. Click one of the following links to download the application in iTunes or Google Play.
    - Smarpthone Authenticator for iOS
    - Smartphone Authenticator for Android
    - Smartphone Authenticator for Windows Phone
2. After you install the application, click one of the following links to choose your platform to explore the technical materials for using the app:
    - Using the Smartphone Application on iOS
    - Using the Smartphone Application on Android
    - Using the app on Windows Phone

3 Using the Smartphone Application on iOS

Launching the Application

Perform the following steps to launch the application after installing it:

1. Click to run the Advanced Authentication application.
2. Accept the license agreement.

   A message `Enter your PIN` is displayed.
3. Specify a PIN to access the application and tap **OK.**

   A message `Advanced Authentication Would Like to Send You Notifications` is displayed.

   Tap **Allow** to enable the push notification.It is recommended to enable the push notification.

   The **Enrolled Authenticators** screen is displayed.
4. You can enroll the authenticators for authentication. For more information about how to enroll authenticators, see "Enrolling on the Smartphone Application".

   The menu icon ≡ on the left panel helps you to navigate to the different tabs of the application.
5. Click the menu icon ≡ and then select any of the following tabs based on the requirement:
   - **Enrolled Authenticators**: This page displays the authenticators that you have enrolled.
   - **Authentication requests**: This page displays any requests that are sent as push notifications for authentication.
   - **Request History**: This page displays all the requests that you have accepted or declined. You can view the status of authentication requests and if there are any suspicious requests, you can report them to the administrator.
   - **Settings**: This page allows to configure settings for PIN and Touch_id (fingerprint recognition).
   - **About**: This page displays information about the current version of the application.
6. Tap **Save**.

Configuring Security Settings for the Application

After you install the application or upgrade from previous versions, you must set up a PIN for the application.

It is recommended to enable **PIN** and **Fingerprint** options for maintaining security and user's convenience respectively.

NOTE: You cannot edit the **PIN** and **Fingerprint** settings if the settings have been enforced on the server by the Advanced Authentication administrator.

To configure security settings, perform the following steps:

1. Click **Settings**. The **MANAGE PIN** screen is displayed.
2. Turn **Pin** to **ON** to enable the PIN protection for your application.
3. You can also switch **Touch Id** to **ON** to enable fingerprint authentication. The fingerprint you set for the phone is used as a Touch Id for the smartphone application.

   NOTE: **Touch Id** is disabled if you disable the **Pin** setting.

   The maximum attempts to enter an incorrect Pin is ten after which the data on your application is wiped out.

   ---
4. Tap **Change Pin** to change the pin and specify the old and new pin.

Enrolling on the Smartphone Application

To enroll an authenticator on your smartphone, perform the following steps:

1. Initialize enrollment by using any of the following:
   - Advanced Authentication Self-Service portal (Smartphone or TOTP method)
   - Advanced Authentication Web Enrollment Wizard (Smartphone or OATH OTP authenticator)
   - Advanced Authentication Client - Enrollment Wizard

   After you initiate an enrollment, a QR code is displayed on laptop or computer screen.
2. Tap the **+** icon on the top-right of the **Enrolled Authenticators** screen.

   A message `Advanced Authentication Would like to Access the Camera` is displayed.
3. Click **OK**.
4. Use the camera of your smartphone to capture the QR code.

   The screen closes automatically when a green square appears over the QR code indicating that a compliant QR code is captured.

   TIP: 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.

   ---
5. Specify **Account** and **Additional info** for the authenticator.
6. Tap **Save** on the top of the screen to save the authenticator. The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen.

7. After you enroll an authenticator, you can edit or delete it on your smartphone. To do this, in the **Enrolled Authenticators** screen long press the authenticator and swipe to the left. A menu is displayed with the **Edit** and **Delete** buttons.

NOTE: If you delete an authenticator on the Enrollment site, the authenticator on your smartphone remains unaffected and vice versa.

Authenticating with the Smartphone Application

After you enroll an authenticator, you can authenticate on an application with your Smartphone.

To authenticate on an application, ensure that your smartphone has an internet connection and then perform the following steps:

1. Initialize the authentication on the endpoint.

   A push notification `Authentication required!` is displayed if your smartphone is locked or the smartphone application is closed.
2. The application prompts to provide a **Touch ID** or specify the **PIN** that you provided for the application.

   Accept or **Reject** buttons are displayed as push notifications in the **Authentication Requests** screen.
3. Tap **Accept** to accept the authentication request.

   A message `Accepted` is displayed if you accept the authentication request or `Rejected` if you reject the authentication request.

Authenticating Offline Or with the TOTP Method

If your smartphone does not have an internet connection or you have enrolled the TOTP method (not Smartphone), then perform the following steps to authenticate:

1. Tap the menu icon ☰ and tap **Enrolled Authenticators**.

   The authenticators are displayed in the **Enrolled Authenticators** screen.
2. You can specify the OTP displayed for the authenticator for authenticating on the application.

TIP: If the authentication fails, ensure that the time on your smartphone is synchronized.

4

Using the Smartphone Application on Android

NOTE: You must disable the **Allow mock locations** option in **Developer options** of smartphone settings.

Launching the Application

Perform the following steps to launch the application after installing it:

1. Click to run the Advanced Authentication application.
2. Accept the license agreement.

   A message `Enter your PIN` is displayed.
3. Specify a **PIN** to access the application then tap **OK.**

   A message `Advanced Authentication Would Like to Send You Notifications` is displayed.

   Tap **Allow** to enable the push notification. It is recommended to enable the push notification.

   The **Enrolled Authenticators** screen is displayed.
4. You can enroll the authenticators for authentication. For more information about how to enroll authenticators, see "Enrolling on the Smartphone Application".

   The menu icon ≡ on the left panel helps you to navigate to the different tabs of the application.
5. Click the menu icon ≡ and then select any of the following tabs based on the requirement:
   - **Enrolled Authenticators**: This page displays the authenticators that you have enrolled.
   - **Authentication requests**: This page displays any requests that are sent as push notifications for authentication.
   - **Request History**: This page displays all the requests that you have accepted or declined. You can view the status of authentication requests and if there are any suspicious requests, you can report them to the administrator.
   - **Settings**: This page allows to configure settings for PIN and Fingerprint (fingerprint recognition).
   - **About**: The page displays information about the current version of the application.
6. Tap **Save**.

Configuring Security Settings for the App

After you install the application or upgrade from previous versions, you must set up a PIN for the application.

It is recommended to enable **PIN** and **Fingerprint** options for maintaining security and user's convenience respectively.

NOTE: You cannot edit the **PIN** and **Fingerprint** settings if the settings have been enforced on the server by the Advanced Authentication administrator.

To configure security settings, perform the following steps:

1. Click **Settings**.
2. Turn **PIN** to **ON** to enable the PIN protection for your application.
3. You can also switch **Fingerprint** option to **ON** to enable fingerprint authentication. The fingerprint you set for the phone is used as a touch sensor for the smartphone application.

   NOTE: Fingerprint is disabled if you disable the **PIN** setting.

   The maximum attempts to enter an incorrect Pin is ten after which the data on your application is wiped out.

   ---

4. Tap **Change PIN** to change the pin and specify the old and new pin.

Enrolling on the Smartphone Application

To enroll an authenticator on your smartphone, perform the following steps:

1. Initialize enrollment by using any of the following:
   - Advanced Authentication Self-Service portal (Smartphone or TOTP method)
   - Advanced Authentication Web Enrollment Wizard (Smartphone or OATH OTP authenticator)
   - Advanced Authentication Client - Enrollment Wizard

   After you initiate an enrollment, a QR code is displayed on laptop or computer screen.
2. Tap the **+** icon on the lower-right of the **Enrolled Authenticators** screen.

   A message `Advanced Authentication Would like to Access the Camera` is displayed.
3. Click **OK**.
4. Use the camera of your smartphone to capture the QR code.

   The screen closes automatically when a green square appears over the QR code indicating that a compliant QR code is captured.

   TIP: 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.

   ---

5. Specify **Account** and **Additional info** for the authenticator.
6. Tap **Save**. The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen.
7. After you enroll an authenticator, you can edit or delete it on your smartphone.

To do this, in the **Enrolled Authenticators** screen long press the authenticator and swipe to the left. A menu is displayed with the **Edit** and **Delete** buttons.

NOTE: If you delete an authenticator on the Enrollment site, the authenticator on your smartphone remains unaffected and vice versa.

Authenticating with the Smartphone Application

After you enroll an authenticator, you can authenticate on an application with your Smartphone.

To authenticate on an application, ensure that your smartphone has an internet connection and then perform the following steps:

1. Initialize the authentication on the endpoint.

   A push notification `Authentication required!` is displayed if your smartphone is locked or the smartphone application is closed.

2. The application prompts to provide a **Touch sensor** or specify the **PIN** that you provided for the application.

   Accept or **Reject** buttons are displayed as push notifications in the **Authentication Requests** screen.

3. Tap **Accept** to accept the authentication request.

   A message `Accepted` is displayed if you accept the authentication request or `Rejected` if you reject the authentication request.

Authenticating Offline Or with the TOTP Method

If your smartphone does not have an internet connection or you have enrolled the TOTP method (not Smartphone), then perform the following steps to authenticate:

1. Tap the menu icon ☰ and tap **Enrolled Authenticators**.

   The authenticators are displayed in the **Enrolled Authenticators** screen.

2. Specify the OTP displayed for the authenticator for authenticating on the application.

TIP: If the authentication fails, ensure that the time on your smartphone is synchronized.

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

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.

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.

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.

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.

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.

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.

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 you 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.

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 theAdvanced Authentication Web Enrollment Wizard, because itshows 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 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.

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.