Advanced Authentication 6.3

Smartphone App Guide

December 2019

Legal Notices

Contents

About this Book 5

1 Installing NetIQ Advanced Authentication App 7

Prerequisites . . . 7
Installation Procedure . . . 7

2 Using the NetIQ Advanced Authentication App on iOS 9

Launching the NetIQ Advanced Authentication App . . . 9
Configuring Security Settings for the App . . . 10
Enrolling an Authenticator on the App . . . 10
Enrolling with a QR Code . . . 11
Enrolling with a Link . . . 11
Authenticating with the NetIQ Advanced Authentication App . . . 12
Authenticating Smartphone Offline Or with TOTP Method . . . 12

3 Using the NetIQ Advanced Authentication App on Android 15

Launching the NetIQ Advanced Authentication App . . . 15
Configuring Security Settings for the App . . . 16
Enrolling an Authenticator on the App . . . 16
Enrolling with a QR Code . . . 17
Enrolling with a Link . . . 17
Authenticating with the NetIQ Advanced Authentication App . . . 18
Authenticating Smartphone Offline Or with the TOTP Method . . . 18

4 Troubleshooting 21

Users Are Unable to Enroll the Smartphone Authenticator . . . 21
Issue While Enrolling the Smartphone Authenticator in Android App . . . 22
Authentication Using the Smartphone Authenticator Fails . . . 22
Issue with One-Time Password . . . 22

About this Book

The NetIQ Advanced Authentication Smartphone App Guide has been designed to guide users about how to download the app for the different smartphone platforms. The guide also instructs 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 Installing NetIQ Advanced Authentication App

This chapter guides you through the process of installing the NetIQ Advanced Authentication App and requirements for installation.

- "Prerequisites" on page 7
- "Installation Procedure" on page 7

Prerequisites

To install the NetIQ Advanced Authentication app, the device must meet some requirements based on the smartphone you have. For system requirements of NetIQ Advanced Authentication app, see Smartphone Applications Requirement.

NOTE: If the fingerprint scanner is not available in your smartphone, then you can use PIN to access the app.

NOTE: If an Advanced Authentication administrator enables the geo-fencing feature, then access to the location must be allowed for the NetIQ Advanced Authentication app in the smartphone.

Installation Procedure

1 Download the NetIQ Advanced Authentication app on your smartphone in one of the following ways:

- Navigate to Google Play store or App store and search for the NetIQ Advanced Authentication app.
- Scan one of the following QR code corresponding to the platform in your smartphone to navigate to the respective app download page in the store:
  - **QR code for Android**

- **QR code for iOS**

2 Perform one of the following actions to install the app based on the platform in your smartphone:

   - **Android**: Tap **Install**.
   - **iOS**: Tap **Get**.

   After you install the app, click one of the following links to use the app based on the platform of your smartphone:

   - Using the NetIQ Advanced Authentication App on iOS
   - Using the NetIQ Advanced Authentication App on Android

2 Using the NetIQ Advanced Authentication App on iOS

You can authenticate with the NetIQ Advanced Authentication app on your iOS phone. You must enroll the authenticator on the Advanced Authentication Self Service portal using the app. To enroll and authenticate using the app on your iOS phone, perform the following tasks:

- "Launching the NetIQ Advanced Authentication App" on page 9
- "Configuring Security Settings for the App" on page 10
- "Enrolling an Authenticator on the App" on page 10
- "Authenticating with the NetIQ Advanced Authentication App" on page 12
- "Authenticating Smartphone Offline Or with TOTP Method" on page 12

Launching the NetIQ Advanced Authentication App

1. Tap  to run the NetIQ Advanced Authentication app.
2. Accept the license agreement.

   A message `New PIN` is displayed.
3. Specify a PIN to access the app and tap **OK.**

   A message `"NetIQ Auth" Would Like to Send You Notifications` is displayed.
4. Tap **Allow** to enable the push notification.

   It is recommended to enable the push notification.

   You can enroll the authenticators for authentication in the **Enrolled Authenticators** screen. For more information about how to enroll authenticators, see "Enrolling an Authenticator on the App".

   The menu icon  on the left panel helps you to navigate to the different tabs of the app.
5. Tap the menu icon  and select any of the following tabs based on the requirement:
   - **Enrolled Authenticators**: This screen displays the authenticators that you have enrolled.
   - **Authentication requests**: This screen displays the requests that are sent as push notifications for authentication.
   - **Request History**: This screen 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 screen allows you to configure settings for PIN and Fingerprint (fingerprint recognition).
   - **About**: This screen displays information about the current version of the application.

NOTE: You need to reinstall the NetIQ application and re enroll the authenticator if you restore your phone from iCloud.

Configuring Security Settings for the App

After installing the app, you must set up a PIN for the app.

It is recommended to enable the **Pin** and **Touch ID** options for maintaining the security and user's convenience respectively.

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

To configure the security settings on the app, perform the following steps:

1. Tap **Settings**.
2. Set **Touch ID** to **ON** to enable fingerprint authentication. The fingerprint you set for the phone is used as a touch sensor for your app.

   NOTE

   - Touch ID is disabled if you disable the **Pin** setting.
   - The maximum attempts to specify an incorrect PIN is 10 after that the data on your app is erased.
   - If you provide an incorrect Touch ID for 3 to 4 attempts, the **Touch sensor** pop-up is not displayed and only the **Enter PIN** screen is displayed. Also, **Touch ID** is set to **OFF** and **Pin** remains **ON**.
3. Set **Pin** to **ON** to enable the PIN protection for your app.
4. Tap **Change Pin** to change the PIN of the app.

   Specify your current PIN, then specify and confirm the new PIN.

Enrolling an Authenticator on the App

1. You can enroll the Smartphone authenticator in one of the following ways:
   - Enrolling with a QR code
   - Enrolling with a Link
2. After you enroll an authenticator, you can edit or delete it on your smartphone.

   To do this, tap on the preferred authenticator in the **Enrolled Authenticators** screen. The **Edit template** screen is displayed, update the details and tap **Save** to update the authenticator. You can tap **Delete** to remove the authenticator.

   NOTE: If you delete an authenticator from the Self-Service portal, the authenticator on your app is deleted. However, if you delete an authenticator on your app, the authenticator on the Self-Service portal remains unaffected.

Enrolling with a QR Code

1 Initialize enrollment using the Advanced Authentication Self-Service portal (Smartphone or TOTP method).

For more information, see Enrolling the Smartphone Authenticator.

After you initiate an enrollment, a QR code is displayed on your laptop or computer screen.

2 Open the NetIQ Advanced Authentication app on your smartphone.

3 Tap the + icon on the upper-right of the **Enrolled Authenticators** screen.

A message `Advanced Authentication Would like to Access the Camera` is displayed.

4 Tap **OK**.

5 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.

---

6 Specify **Account** and **Additional info** for the authenticator.

The content in the **Account** field can be any information. For example, a comment **VPN** if the authenticator is related to a VPN authentication. The information in the **Account** field is displayed below the enrolled authenticator.

Additional info can be any notes related to the authenticator.

7 Tap **Save**.

The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen of your smartphone app.

Enrolling with a Link

1 Check your phone for a new email or SMS.

You will receive a link from the administrator.

2 Tap on the link. You will be redirected to the NetIQ Advanced Authentication app.

If you have not installed the smartphone app, you will be redirected to the AppStore from where you can install the app.

3 Specify a PIN or a Touch ID if applicable.

4 Specify your username and password in the **Enroll new authenticator** screen.

5 Tap **Sign In**.

6 Specify an optional comment in the app.

7 Tap **Save**.

The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen of your smartphone app.

Authenticating with the NetIQ Advanced Authentication App

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

1 Initialize the authentication on the endpoint.

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

2 Perform one of the following based on the settings enforced by the administrator:

2a Tap the notification in the mobile notification bar on your smartphone.

The NetIQ Advanced Authentication app opens and prompts to provide a **Touch ID** or specify the **Pin** that you registered for the app.

A push notification with **Accept** or **Reject** buttons are displayed in the **Authentication Requests** screen.

On the lock screen, swipe to the left and then tap the **View** button to see the buttons.

NOTE: An administrator has the privilege to display the action buttons **Accept** and **Reject** with the notification in the mobile notification bar. This allows you to take action directly from the notification without opening the app.

2b Open the NetIQ Advanced Authentication app.

The app prompts to provide a **Touch ID** or specify the **Pin** that you registered for the app. A push notification with **Accept** or **Reject** buttons are displayed 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 Smartphone Offline Or with TOTP Method

If your smartphone does not have an internet connection to receive the push notifications or if you have enrolled the TOTP method, perform the following steps to authenticate using the OTP:

1 Initialize the authentication on the endpoint.

2 Open the NetIQ Advanced Authentication app.

3 Tap the menu icon  in the app and tap **Enrolled Authenticators**.

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

4 Perform one of the following based on the authenticator for authenticating on the app:

- Specify the OTP displayed for the Smartphone authenticator.

- Specify the OTP displayed for the TOTP authenticator.

The following table describes the color of the dots beside the OTP and what it indicate:

Color	What it indicates
Grey	The gray color indicates it is TOTP authentication.
Green	The green color indicates it is Smartphone authentication, and the Advanced Authentication cluster in which you enrolled the authenticator is available.
Red	The red color indicates it is Smartphone authentication, and the Advanced Authentication cluster in which you enrolled the authenticator is unavailable.

NOTE: You can also tap the TOTP to copy to the clipboard.

You get authenticated to the endpoint if the OTP is valid.

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

3 Using the NetIQ Advanced Authentication App on Android

You can authenticate with the NetIQ Advanced Authentication app on your Android phone. You must enroll the authenticator on the Advanced Authentication Self Service portal using the app. To enroll and authenticate using the app on your Android phone, perform the following tasks:

- "Launching the NetIQ Advanced Authentication App" on page 15
- "Configuring Security Settings for the App" on page 16
- "Enrolling an Authenticator on the App" on page 16
- "Authenticating with the NetIQ Advanced Authentication App" on page 18
- "Authenticating Smartphone Offline Or with the TOTP Method" on page 18

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

Launching the NetIQ Advanced Authentication App

1 Tap  to run the NetIQ Advanced Authentication app.

2 Accept the license agreement.

A message `New PIN` is displayed.

3 Specify a **PIN** to access the app, then tap **OK.**

You can enroll the authenticators for authentication in the **Enrolled Authenticators** screen. For more information about how to enroll authenticators, see Enrolling an Authenticator on the App.

The menu icon  on the left panel helps you to navigate to the different tabs of the app.

4 Tap the menu icon  and select any of the following tabs based on the requirement:

- **Enrolled Authenticators**: This screen displays the authenticators that you have enrolled.
- **Authentication requests**: This screen displays the requests that are sent as push notifications for authentication.
- **Request History**: This screen 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 screen allows you to configure settings for PIN and Fingerprint (fingerprint recognition).
- **About**: The screen displays information about the current version of the app.

Configuring Security Settings for the App

After installing the app, you must set up a PIN for the app.

It is recommended to enable the **PIN** and **Fingerprint** options for maintaining the 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 the security settings in the app, perform the following steps:

1. Tap **Settings**.
2. Set **PIN** to **ON** to enable the PIN protection for your app.
3. Set **Fingerprint** to **ON** to enable fingerprint authentication. The fingerprint you set for the phone is used as a touch sensor for your app.

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

   The maximum attempts to specify an incorrect PIN is 10 after that the data on your app is erased.

   ---

4. Tap **Change PIN** to change the PIN of the app.

   Specify your current PIN, then specify and confirm the new PIN.
5. Tap **Change permissions** to manage permissions for the camera and location of your smartphone.

   Tap **OK** to continue.

   Tap **App permissions** and enable the **Camera** and **Location** as per your requirement.

Enrolling an Authenticator on the App

1. You can enroll the Smartphone authenticator in one of the following ways:
   - Enrolling with a QR Code
   - Enrolling with a Link
2. After you enroll an authenticator, you can edit or delete it on your smartphone.

   To do this, tap on the preferred authenticator in the **Enrolled Authenticators** screen. The **Change Authenticator** screen is displayed, update the details and tap **Save** to update the authenticator.

   You can tap the delete icon to remove the authenticator.

   NOTE: If you delete an authenticator from the Self-Service portal, the authenticator on your app is deleted. However, if you delete an authenticator on your app, the authenticator on the Self-Service portal remains unaffected.

Enrolling with a QR Code

1 Initialize enrollment using the Advanced Authentication Self-Service portal (Smartphone or TOTP method).

For more information, see Enrolling the Smartphone Authenticator.

After you initiate an enrollment, a QR code is displayed on your laptop or computer screen.

2 Open the NetIQ Advanced Authentication app on your smartphone.

3 Tap the + icon on the lower-right of the **Enrolled Authenticators** screen.

A message `Advanced Authentication Would like to Access the Camera` is displayed.

4 Tap **OK**.

5 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.

---

6 Specify **Account** and **Additional info** for the authenticator.

The content in the **Account** field can be any information. For example, a comment **VPN** if the authenticator is related to a VPN authentication. The information in the **Account** field is displayed below the enrolled authenticator.

Additional info can be any notes related to the authenticator.

7 Tap **Save**.

The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen of your app.

Enrolling with a Link

1 Check your phone for a new email or SMS.

You will be receiving a link from the administrator.

2 Tap on the link. You will be redirected to the NetIQ Advanced Authentication app.

If you have not installed the app, you will be redirected to the Google Play store from where you can install the app.

3 Specify a PIN or touch the fingerprint sensor if applicable.

4 Specify your username and password in the **Enroll new authenticator** screen.

5 Tap **Sign In**.

6 Specify an optional comment in the app.

7 Tap **Save**.

The authenticator that you enrolled is displayed in the **Enrolled Authenticators** screen of your app.

Authenticating with the NetIQ Advanced Authentication App

After you enroll an authenticator, you can authenticate on an app with your smartphone.

1 Initialize the authentication on the endpoint.

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

2 Perform one of the following based on the settings enforced by the administrator:

2a Tap the notification in the mobile notification bar on your smartphone.

The **Accept** or **Reject** buttons are displayed.

On the lock screen, swipe down to view the buttons. However, if the app is closed or not available in the tray then buttons are not displayed.

NOTE: An administrator has the privilege to display the action buttons **Accept** and **Reject** with the notification in the mobile notification bar. This allows you to take action directly from the notification without opening the app.

NOTE: After enrolling the Smartphone method, for the first authentication the actions buttons are not displayed with the notification in the notification bar. Therefore, you must launch the NetIQ Authentication app to accept or reject the request.

2b Open the NetIQ Advanced Authentication app.

The app prompts to provide a **Touch sensor** or specify the **PIN** that you registered for the app.

A push notification with **Accept** or **Reject** buttons are displayed 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 Smartphone Offline Or with the TOTP Method

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

1 Initialize the authentication on the endpoint.

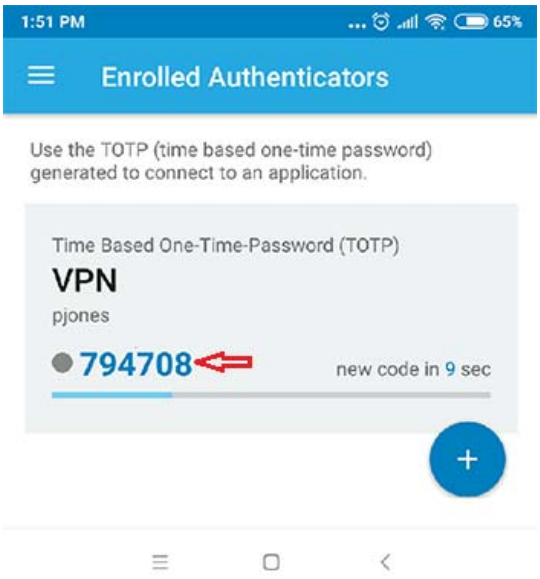
2 Open the NetIQ Advanced Authentication app.

3 Tap the menu icon  and tap **Enrolled Authenticators**.

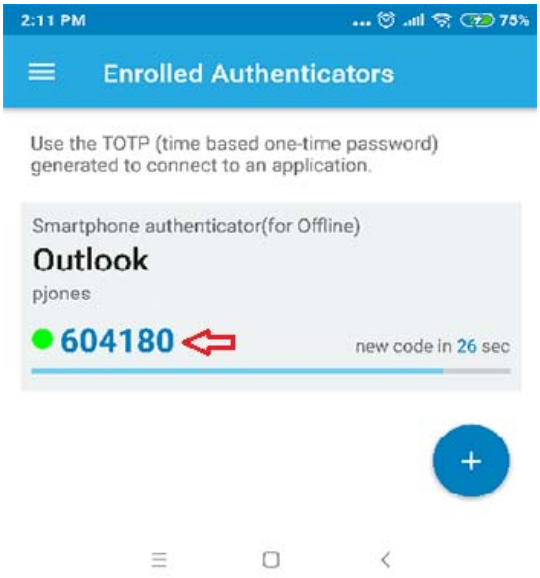
The authenticators are displayed in the **Enrolled Authenticators** screen.

4 Perform one of the following based on the authenticator for authenticating on the app:

- Specify the OTP displayed for the Smartphone authenticator.



- Specify the OTP displayed for the TOTP authenticator.



You get authenticated to the endpoint if the OTP is valid.

The following table describes the color of the dots beside the OTP and what it indicate:

Color	What it indicates
Grey	The gray color indicates it is TOTP authentication.
Green	The green color indicates it is Smartphone authentication, and the Advanced Authentication cluster in which you enrolled the authenticator is available.
Red	The red color indicates it is Smartphone authentication, and the Advanced Authentication cluster in which you enrolled the authenticator is unavailable.

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

4 Troubleshooting

This chapter contains the following sections:

- "Users Are Unable to Enroll the Smartphone Authenticator" on page 21
- "Issue While Enrolling the Smartphone Authenticator in Android App" on page 22
- "Authentication Using the Smartphone Authenticator Fails" on page 22
- "Issue with One-Time Password" on page 22

Users Are Unable to Enroll the Smartphone Authenticator

Issue: When users try to enroll the Smartphone authenticator using a QR code, the smartphone is unable to scan the QR code or the following error message is displayed based on the platform of the smartphone:

- **Android app**: `Please ask your admin if the error will be repeated: Device add error`
- **iOS app**: `JSONEmptyField, message: The field AddDeviceResult is an empty string`

Reason:

- If you are scanning a QR code that is not compatible with the Google Authenticator or NetIQ Auth apps. The other QR codes cannot be scanned using the NetIQ Advanced Authentication app.
- If an administrator has not configured the smartphone authenticator appropriately.

Workaround: Perform one of the following:

- Log in to the Advanced Authentication Self-Service portal and scan the QR code that complies with the Google Authenticator or NetIQ Auth apps.
- Contact your administrator and request to validate the configurations of Smartphone authenticator.

Recommendation: It is recommended to consider the following points while you are scanning the QR code:

- The mouse cursor is not overlapping with the QR code.
- While using the screen with high resolution, zoom-in the web page with the QR code to 125-150 %. The screen with more brightness, contrast, or glossy surface might affect enrollment.
- Focus your smartphone on the QR code appropriately. Some Android devices do not have auto-focus feature. This might cause issues while scanning the QR code or try to use another smartphone.

Issue While Enrolling the Smartphone Authenticator in Android App

Issue: When users try to enroll the Smartphone authenticator using the Android app, an error message `java.security.cert.CertPathValidatorException: Trust anchor for certification path not found` is displayed.

Reason: This issue is due to the self-signed certificate that the administrator has uploaded in the **Server Options** of the Administration portal. The certificate either does not contain all the required certificates or it does not contain information in the following order:

```
-----BEGIN PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: intermediate.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

Workaround: Contact your administrator and request to validate the configuration of the Smartphone authenticator. This issue may be related to a conflict in the IP address or port.

You can access the Advanced Authentication server URL in the browser of your Android smartphone to validate the certificate. If the certificate is invalid, a warning message is displayed stating that the connection is not trusted.

Authentication Using the Smartphone Authenticator Fails

Issue: When you try to authenticate using the Smartphone authenticator, the authentication fails.

Reason: This issue occurs if there is no Internet connection on the server that processes the smartphone authentication requests or when the authentication times-out.

Workaround: Perform one of the following:

- Navigate to the **Enrolled Authenticators** screen and use the One-Time Password (OTP) that is generated for an authenticator to authenticate without any push notification.
- Initiate the authentication again. Do not wait for the push notification. Instead open the app and tap **Accept** to accept the authentication request.

Issue with One-Time Password

Issue: When users try to authenticate with a one-time password, the authentication fails.

Reason: This issue occurs when the time on your smartphone and the server are not synchronized or while using OTP of an invalid authenticator.

Workaround: Perform one of the following:

- Synchronize the time on your smartphone with the time on the server. Select a valid time zone on your smartphone.
- Contact your system administrator.