NetIQ Advanced Authentication Framework

Security Officer Guide

Version 5.2.0

Table of Contents

Introduction

About This Document

Purpose of the Document

NetIQ Advanced Authentication Framework User Documentation is intended for security officers and describes how to manage users' authenticators.

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.

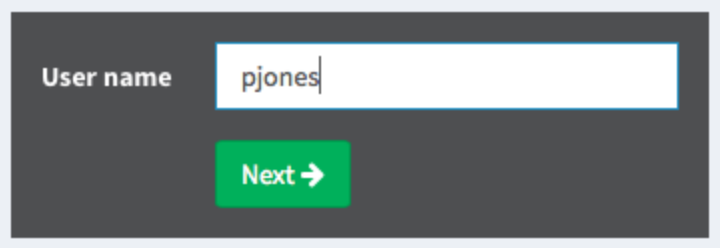
- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

Authenticators Management

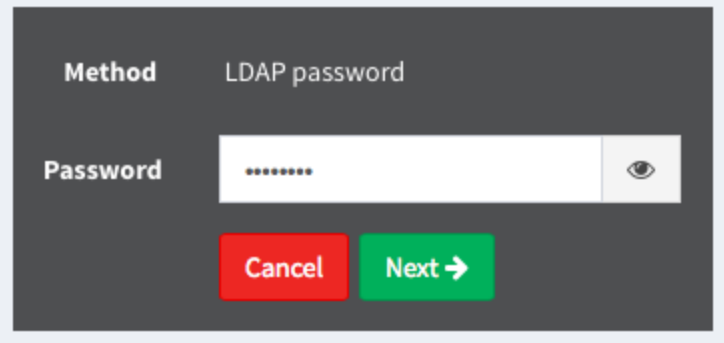
To use the NetIQ Advanced Authentication Framework a user needs to have at least one enrolled ***authenticator***. Authenticator is a set of encrypted data, which contains your authentication data and which you can use to perform log on to Windows, MacOS, remote resources (if applicable) or NetIQ Access Manager etc. Some of the authenticators (like **SMS**, **Email** and **RADIUS**) are enrolling automatically and if user needs to use only one or some of them, he/she can skip the enrollment stage.

The enrollment can be performed on the NetIQ Advanced Authentication Framework Helpdesk Portal. Ask your system administrator to provide you the URL.

1. Open the URL in your browser and you will see the **User name** prompt.

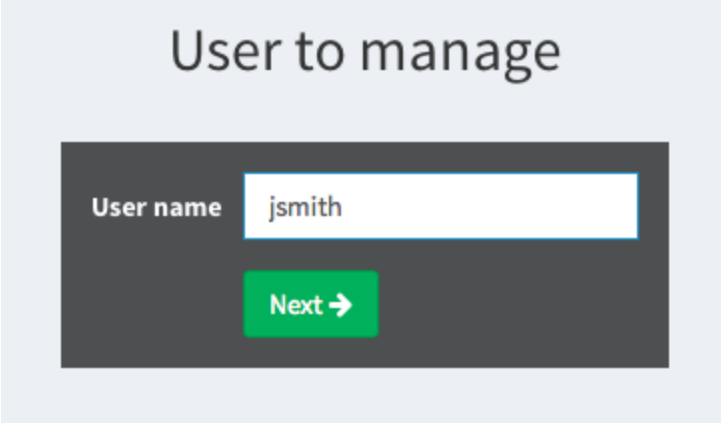


2. Enter your user name and click **Next** button.

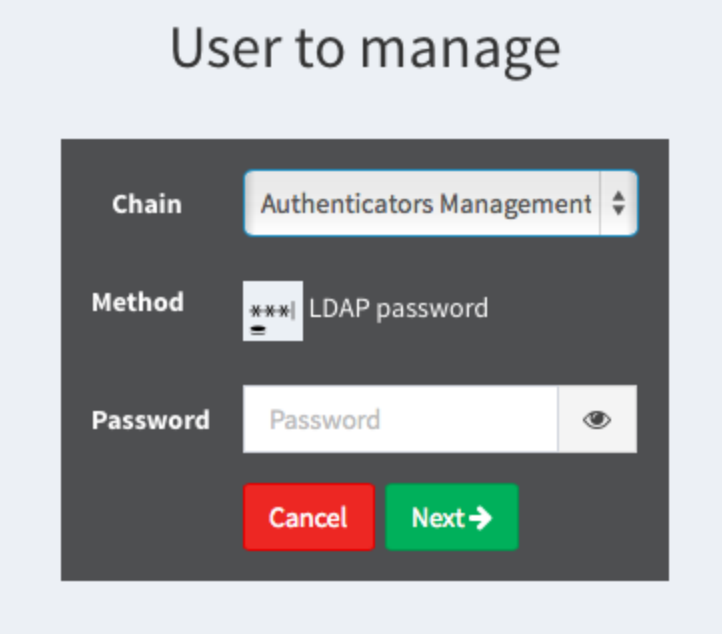


3. Enter your password and click **Next** button. If the provided information is correct you will get access to the Helpdesk Portal.

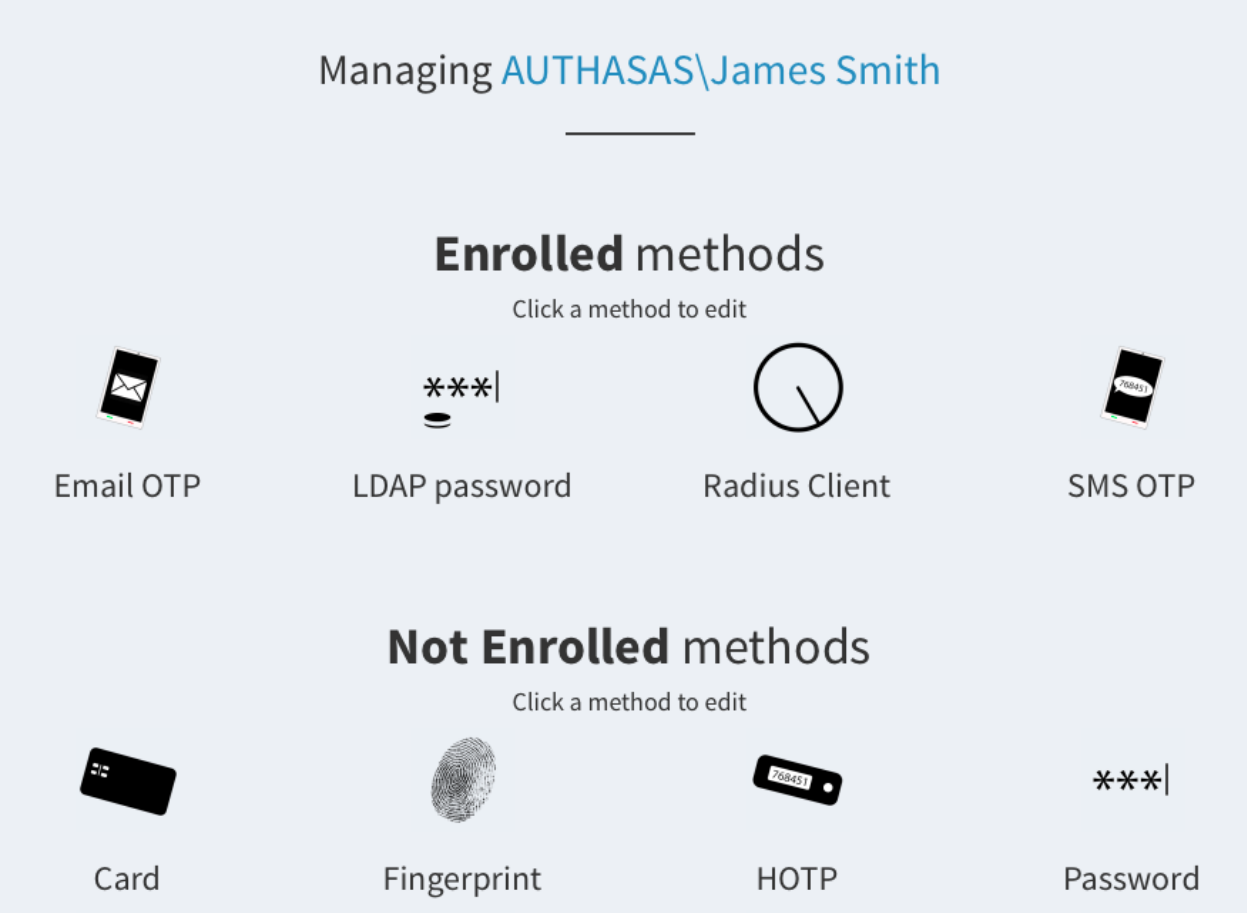
4. Enter name of user which you need to manage. Click **Next**.



5. Enter user credentials (if applicable) to get access for user management.



6. Select one of the available methods to manage.



Methods which enroll automatically:

1. Email OTP
2. LDAP password
3. Radius Client
4. SMS OTP

Not Enrolled methods:

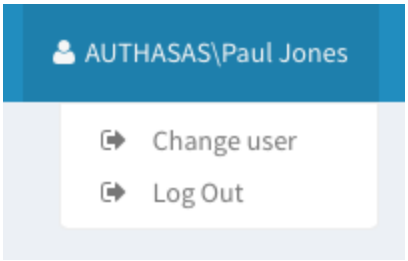
1. Card
2. Emergency Password
3. Fingerprint
4. HOTP
5. Password
6. Security Questions
7. Smartphone
8. TOTP
9. U2F
10. Voice Call

After enrollment a method will be moved to the **Enrolled methods** section.

To change a managed user click a user name in caption **Managing <username>** and then click **OK**.

An alternative way is to click your user name in top right corner and then click **Change user**.

From the same menu you can log out from the Helpdesk Portal. To do it click **Log Out**.



Card

At the moment the Card enrollment is supported only on Microsoft Windows. The NetIQ Smartcard Service component must be installed.

To enroll a card click the Card icon.

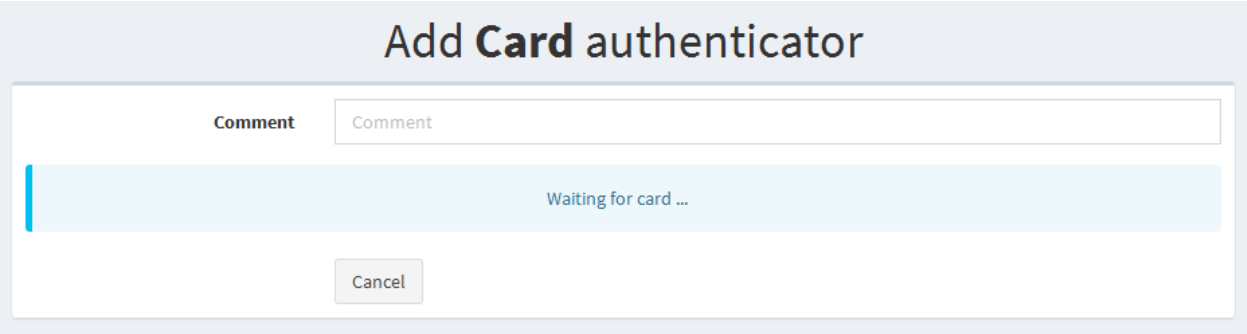
Then follow the steps below:

1. You see a message **Press button "Save" to begin**.

2. You may enter a comment in **Comment** field. It should be a text like *my white card*.

3. Ensure that your card reader is connected to the machine.

4. Click **Save** button. You will see a message **Waiting for card...**



5. Tap a card on the reader. For a second you will see a message **Card has been detected**, then the Card enrollment page will be closed and you will see a message **Authenticator "Card" enrolled**.

If you see a message **Card Service unavailable** ensure that you have the NetIQ Smartcard Service installed.

If you see a message **Card reader not detected** ensure that you have a card reader properly connected to the machine and the reader is available in Device Manager.

To test the authenticator follow the next steps:

1. Click the Card icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message **Waiting for card...**
3. Tap a card on the reader. For a second you will see a message **Card has been detected**, then the Card enrollment page will be closed and you will see a message **Authenticator "Card" passed the test**. If the provided card is invalid you will see a message **Wrong smartcard**.

Email OTP

The Email OTP authentication method sends an email to your email address with a one-time password (OTP). You can use this OTP to authenticate withing a certain time frame.

This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

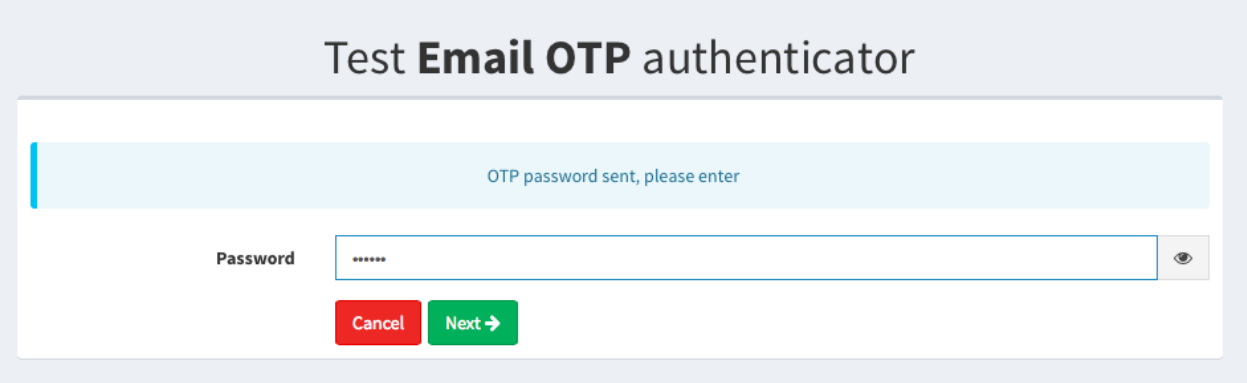
1. Click the Email OTP icon in the **Enrolled methods** section.

2. Ensure that your email address (specified after the text **The email address your One-Time Password is sent to is:**) is valid. Contact your system administrator to change the email address if it's invalid.

3. Click **Test** button. In few seconds you will see a message **OTP password sent, please enter**.

4. Check your email. You should get an email message with one-time password.

5. Enter the OTP to the **Password** field.



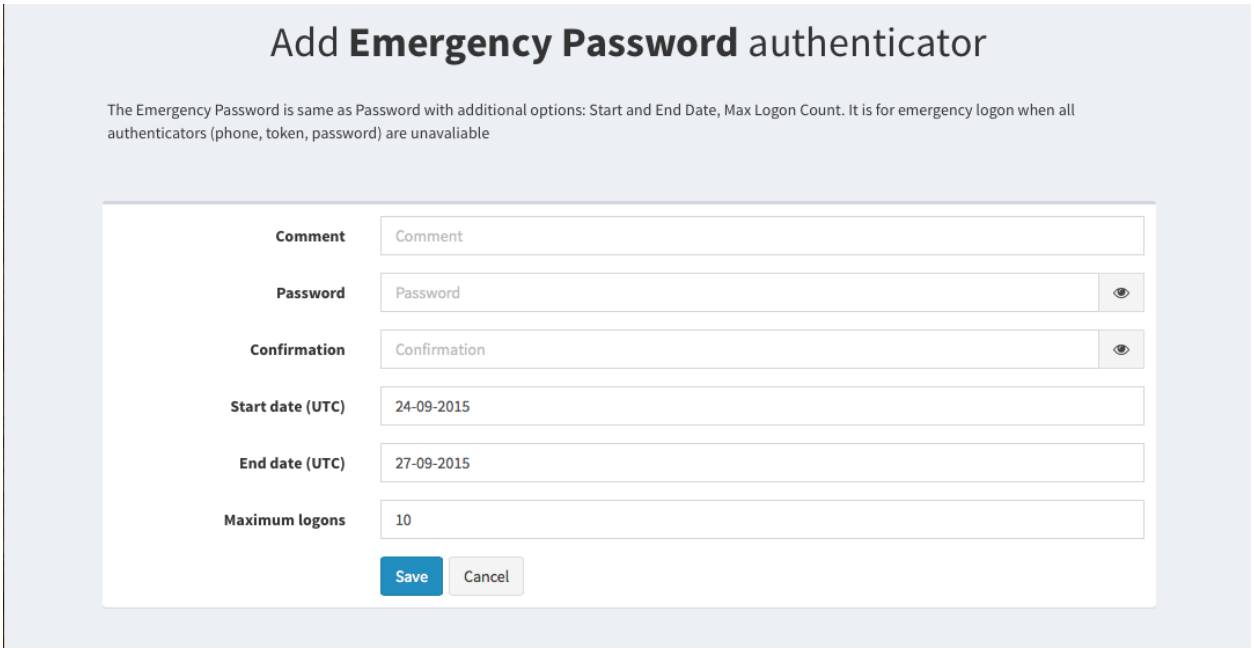
6. Click **Next**. You will see a message **Authenticator "Email OTP" passed the test**. If the provided authenticator is invalid you will see a message **Wrong answer, try again**.

Emergency Password

The Emergency Password is a temporary password which can be enrolled for the users who forgot smartphone or lost a card. Enrollment of the Emergency Password authenticator by users is forbidden intentionally by security reason.

To enroll an emergency password authenticator click the Emergency Password icon in the Helpdesk Portal. Then follow the steps below:

1. You may enter a comment in Comment field. It should be a text like *lost a card*.
2. Specify **Password** and enter its **Confirmation** in the appropriate fields.
3. Check the **Start date (UTC)** and **End date (UTC)** when the authenticator is valid. You may change the dates if applicable.
4. You may also change the **Maximum logons** value (if applicable).



To test the enrolled authenticator follow the steps below:

1. Click the Emergency Password icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter the emergency password to the **Password** field.
4. Click **Next**. You will see a message **Authenticator "Emergency Password" passed the test**. If the provided authenticator is invalid you will see a message **Wrong password**.

Fingerprint

At the moment the Fingerprint enrollment is supported only on Microsoft Windows. The NetIQ WBF Capture Service component must be installed.

To enroll a card click the Fingerprint icon.

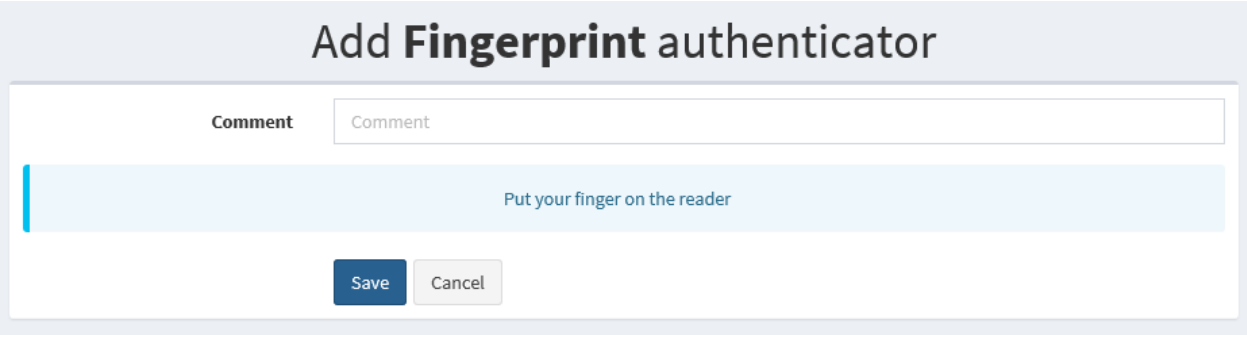
Then follow the steps below:

1. You see a message **Press button "Save" and put your finger on the reader**.

2. You may enter a comment in **Comment** field. It should be a text like *left index finger*.

3. Ensure that your fingerprint reader is connected to the machine.

4. Click **Save** button. You will see a message **Put your finger on the reader**.



5. Put your finger in case of touch sensor or swipe your finger in case of swipe sensor. You will see a message **Authenticator "Fingerprint" added**.

It's strongly recommended to test the authenticator after enrollment. If you are not able to get a successful test, please delete the authenticator and enroll it again.

If you see a message **Fingerprint Service unavailable** ensure that you have the NetIQ Smartcard Service installed.

If you see a message **Enroll failed: Fingerprint reader is not connected** ensure that a fingerprint reader is properly connected to the machine and the reader is available in Device Manager.

To test the authenticator follow the next steps:

1. Click the Fingerprint icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message **Put your finger on the reader**
3. Put your finger in case of touch sensor or swipe your finger in case of swipe sensor. You will see a message **Authenticator "Fingerprint" passed the test**. If the provided fingerprint is invalid you will see a message **Mismatch**.

HOTP

HOTP is a counter-based one-time password. This method uses a counter that is in sync with your HOTP token and the server.

To enroll the HOTP authenticator you should follow recommendations of your system administrator. The following cases are possible:

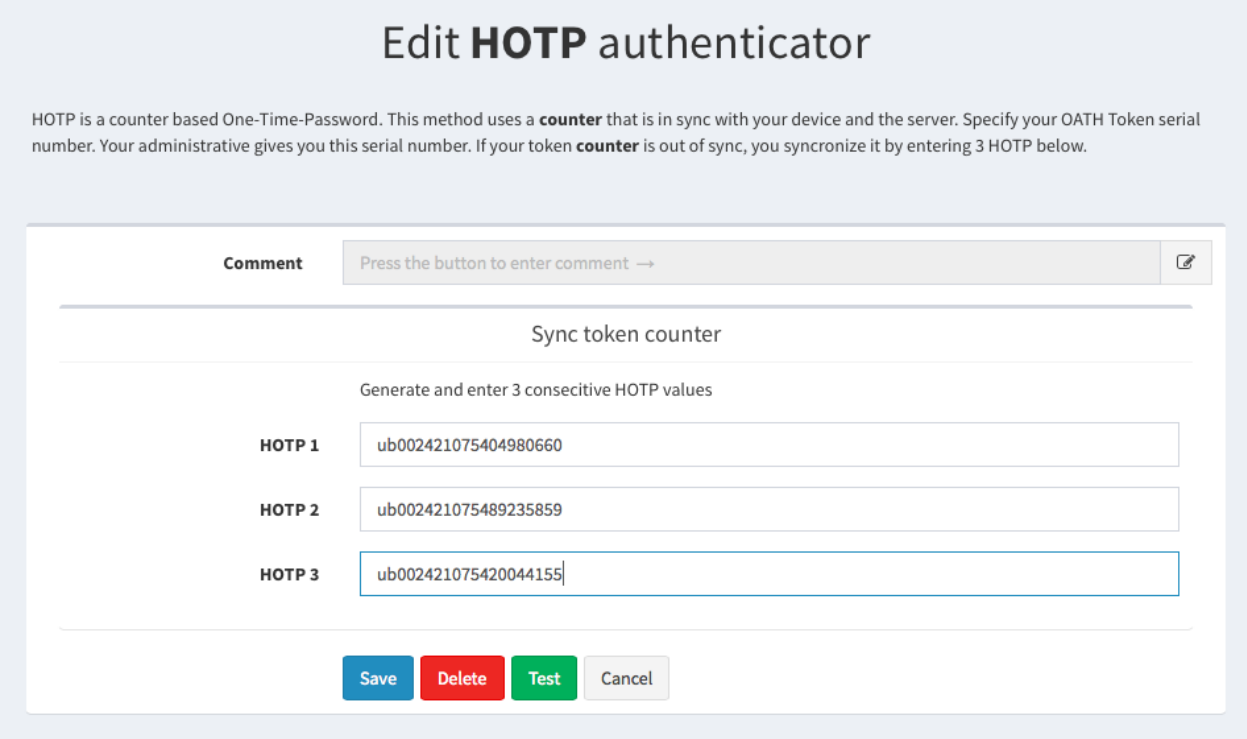
A. A new token is already assigned to your account and enrollment is not needed.
B. A used token is assigned to your account and the HOTP counter synchronization is required.
C. You get an information about serial number of your token and need to assign it to your account.
D. You want to enroll the authenticator manually.

To enroll a HOTP authenticator click the HOTP icon.

B. A used token is assigned to your account and the HOTP counter synchronization is required.

To perform the HOTP counter synchronization follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. Enter an OTP from your token, or in case of an OATH HOTP compliant YubiKey token usage connect your token to the workstation, set cursor to the **HOTP 1** field and press the token's button.
3. Repeat the actions described in point 3 for the **HOTP 2** and **HOTP 3** fields.

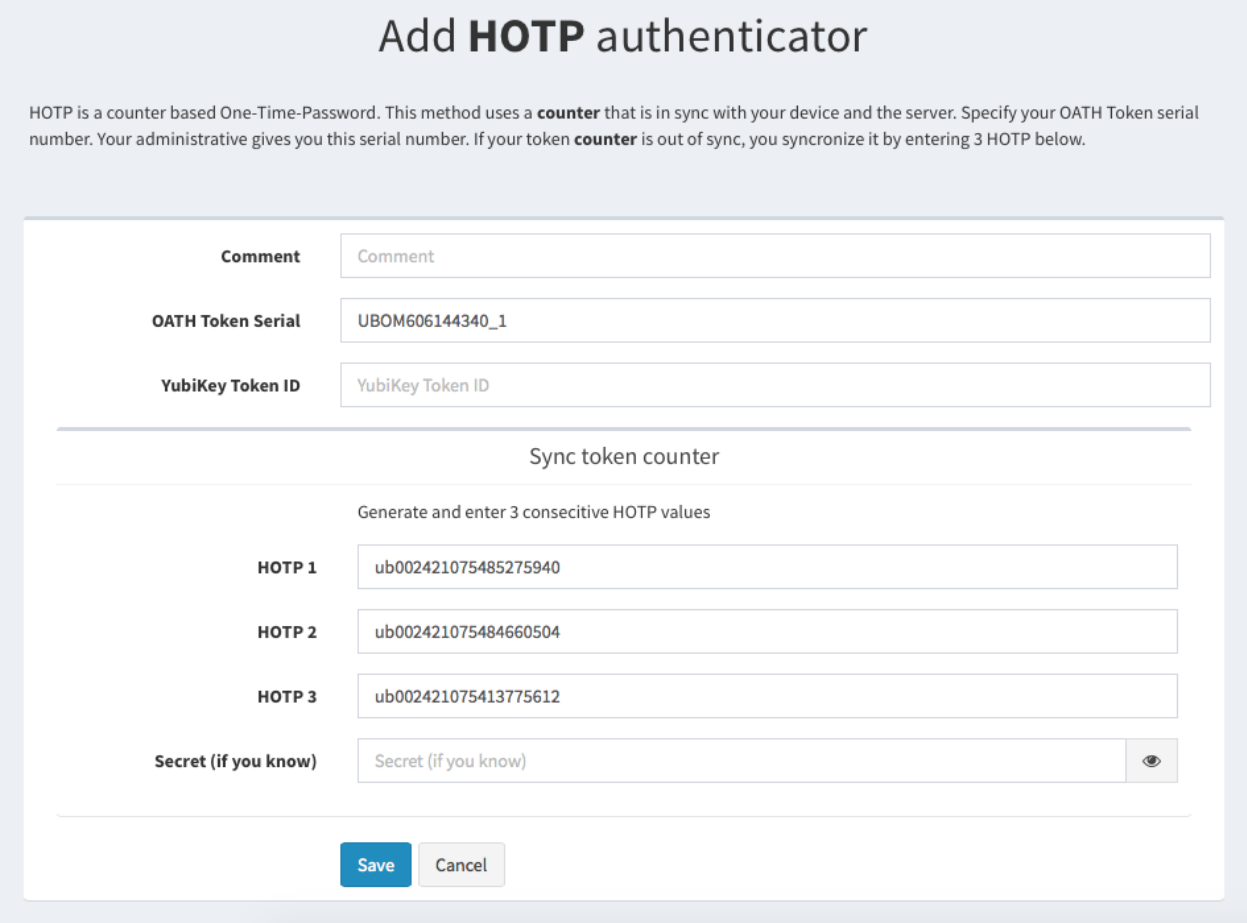


4. Click **Save** button.

C. You get an information about serial number of your token and need to assign it to your account.

To assign an existing token for your account follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. You can specify an optional comment in **Comment** field.
3. Enter the token's serial number provided by your system administrator to the **OATH Token Serial** field.
4. Enter three consecutive one-time passwords to the **HOTP 1**, **HOTP 2**, **HOTP 3** fields.

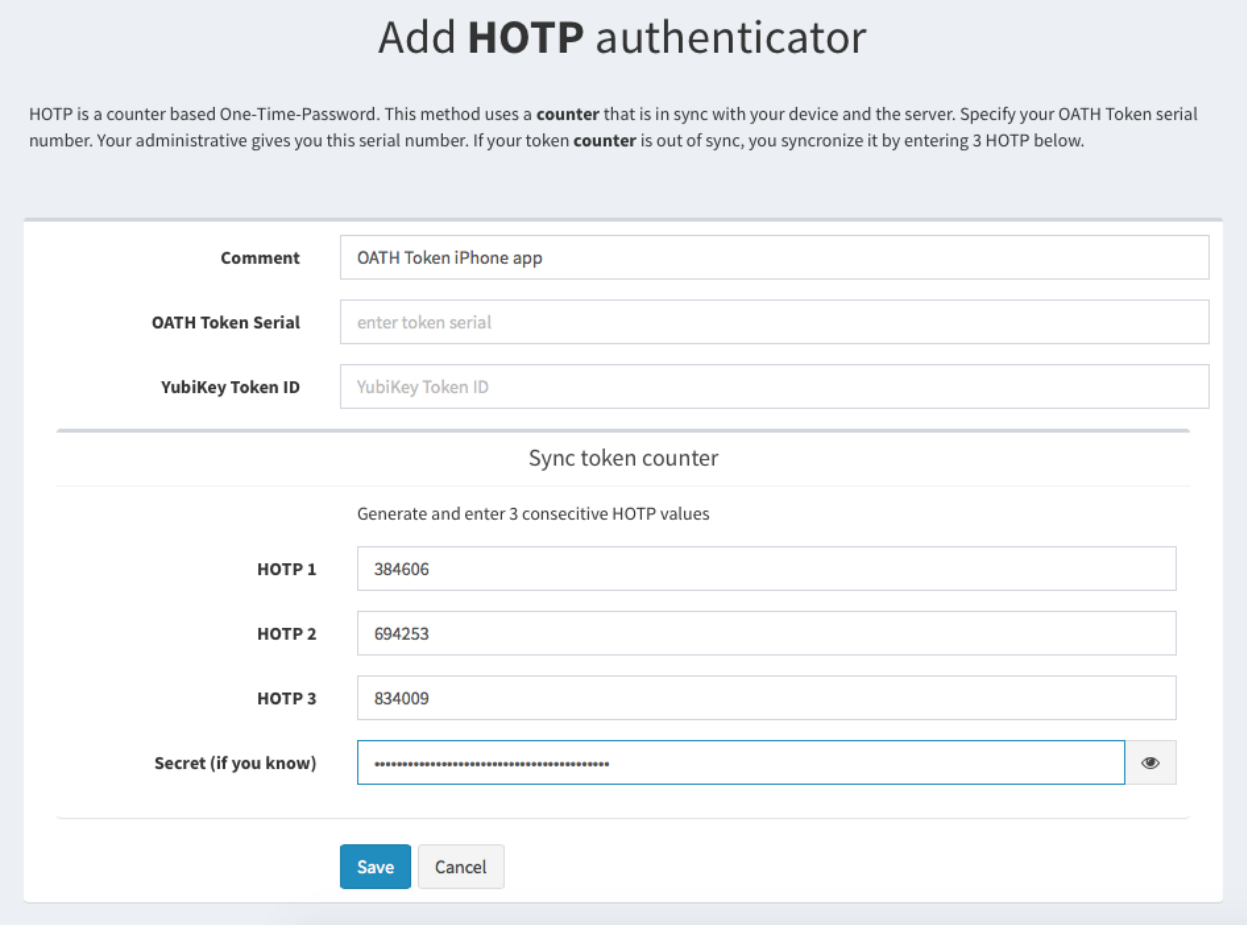


5. Click **Save** button.

D. You want to enroll the authenticator manually.

To enroll a new authenticator manually follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. You can specify an optional comment in **Comment** field.
3. Enter three consecutive one-time passwords to the **HOTP 1**, **HOTP 2**, **HOTP 3** fields.
4. Enter 40 hexadecimal characters secret code to the **Secret (if you know)** field.



5. Click **Save** button.

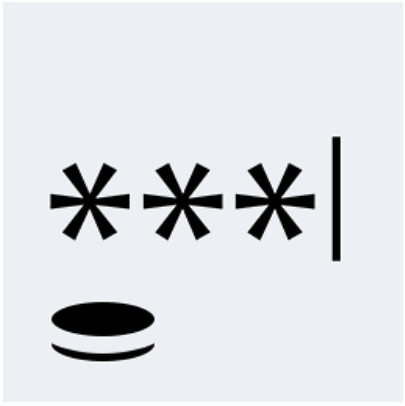
LDAP Password

The LDAP password is a password of your corporate account.

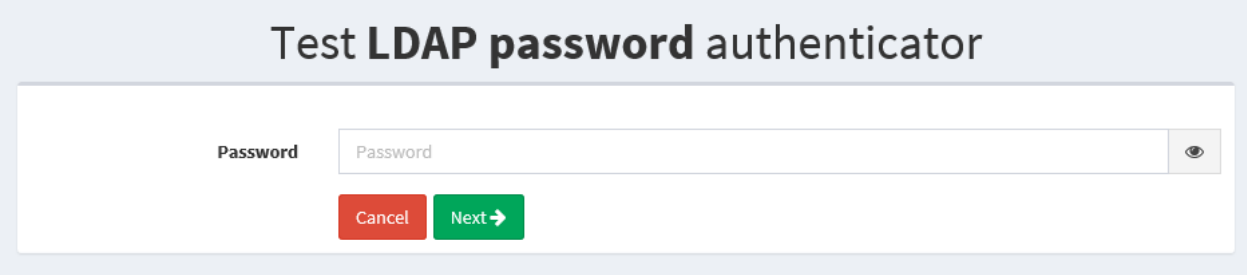
This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

1. Click the LDAP password icon in the **Enrolled methods** section.



2. Click **Test** button.



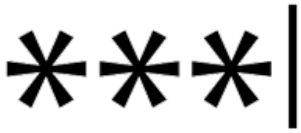
3. Enter your password to the **Password** field.

4. Click **Next**. You will see a message **Authenticator "LDAP password" passed the test**. If the provided authenticator is invalid you will see a message **Invalid credentials**.

Password

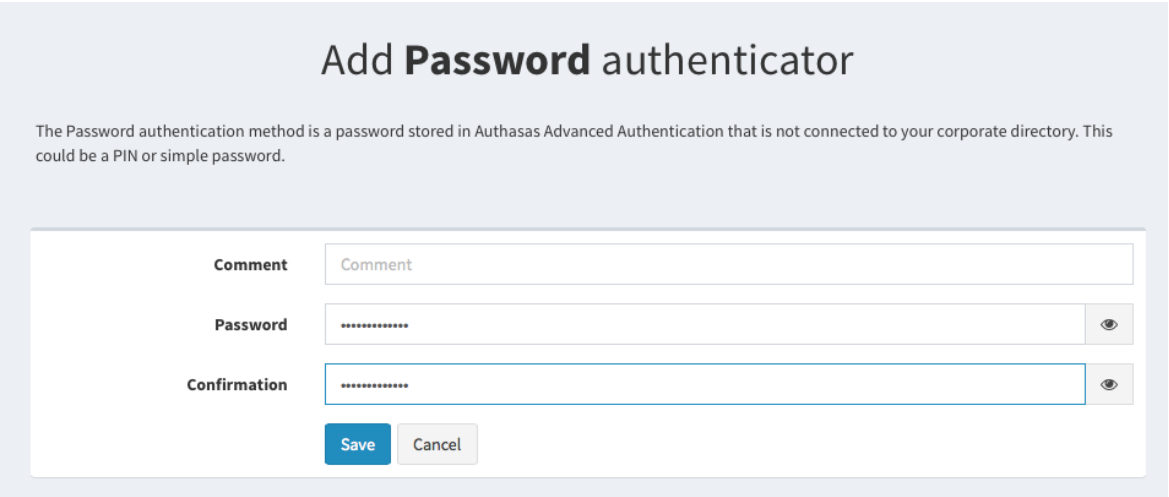
The Password authenticator is a password stored in the NetIQ Advanced Authentication Framework appliance, that is not connected to your corporate directory. This could be a PIN or simple password.

To enroll a password click the Password icon.



Then follow the steps below:

1. You can specify an optional comment in **Comment** field.
2. Enter a **Password** and its **Confirmation** in the appropriate fields. The password must be not less 5 characters (by default, it may be changed by your system administrator).



3. Click **Save** button. You will see a message **Authenticator "Password" added**.

To test the authenticator follow the next steps:

1. Click the Password icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter your password.
4. Click **Next**. You will see a message **Authenticator "Password" passed the test**. If the provided authenticator is invalid you will see a message **Wrong password**.

 You will not get notification about the password expiration. It's required to sign in to the Self-Service Portal and change the password each 42 days.

Radius Client

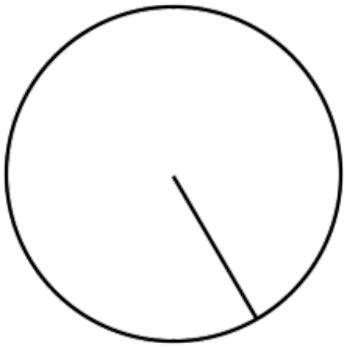
The Radius Client authentication method forwards your authentication request to a third-party Radius Server.

This authenticator enrolls automatically and it's not possible to remove it.

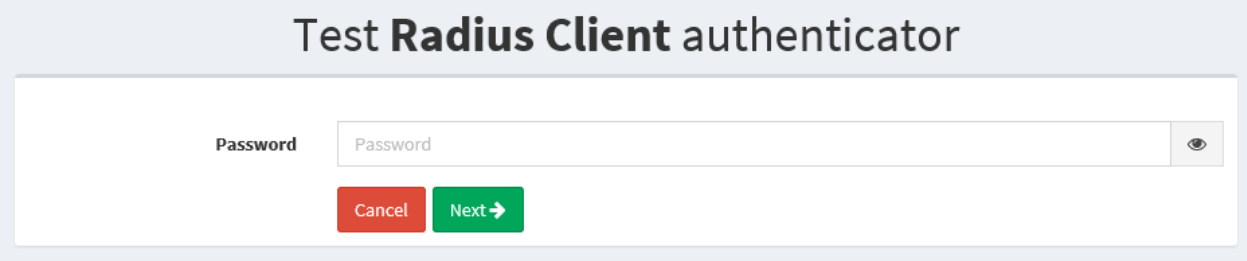
By default a user name from your corporate directory is used. To change it specify a required name in the **User name** field. Then click **Save** button.

To test the enrolled authenticator follow the steps below:

1. Click the Radius Client icon in the **Enrolled methods** section.



2. Click **Test** button.



3. Enter Radius password to the **Password** field.

4. Click **Next**. You will see a message **Authenticator "Radius Client" passed the test**.

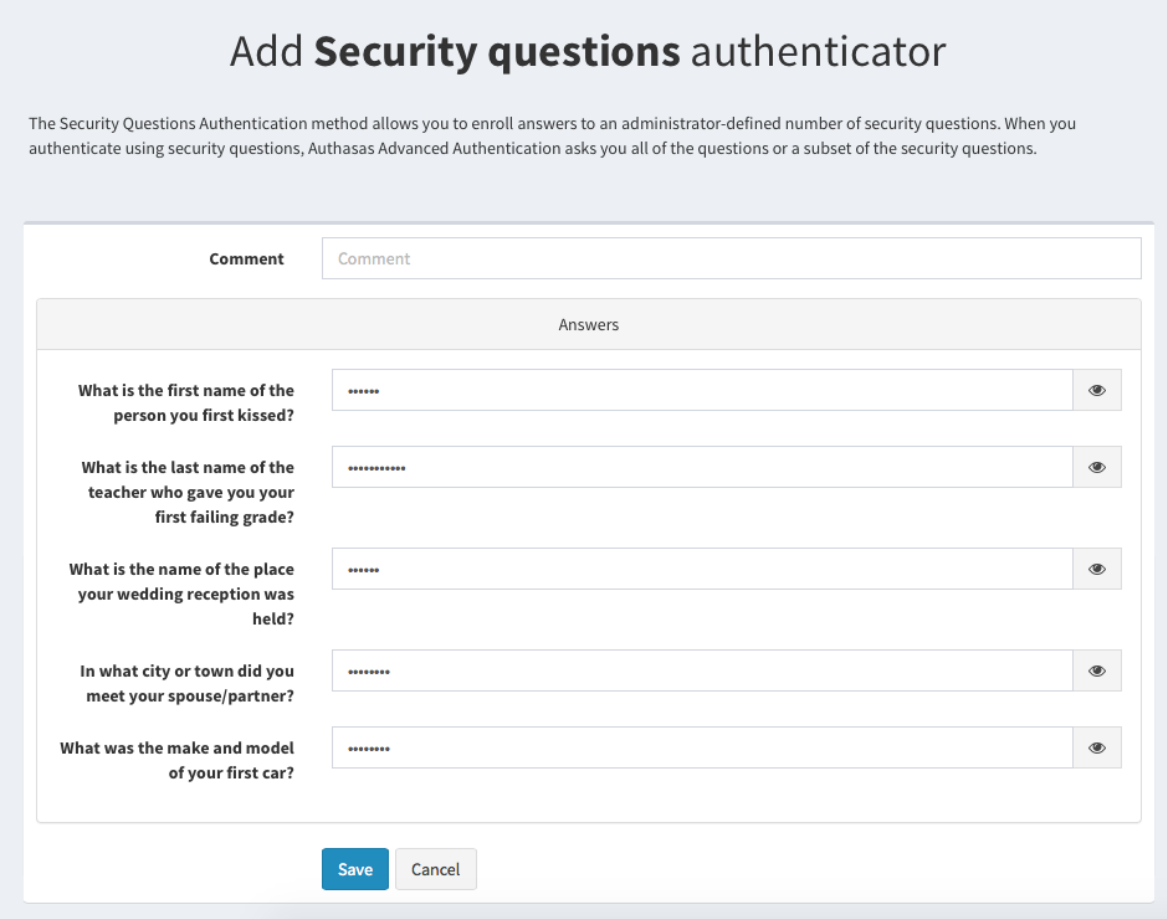
Security Questions

The Security Questions authenticator allows you to enroll answers to an administrator-defined number of security questions. When you authenticate using security questions, NetIQ Advanced Authentication Framework asks you all of the security questions or a subset of the security questions.

To enroll an authenticator click the Security Questions icon.

Then follow the steps below:

1. You can specify an optional comment in **Comment** field.
2. Enter answers to the security questions. Each answer must contain not less 1 character (by default, it may be changed by your system administrator).



3. Click **Save** button. You will see a message **Authenticator "Security Questions" added**.

To test the authenticator follow the next steps:

1. Click the Security Questions icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter answers to the security questions.
4. Click **Next**. You will see a message **Authenticator "Security Questions" passed the test**. If at least one of the provided answers is invalid you will see a message **Wrong answers**.

Smartphone

To enroll the Smartphone authenticator it's required to use the NetIQ Advanced Authentication smartphone app (Apple iOS app, Google Android app).

To enroll a smartphone authenticator click the Smartphone icon.

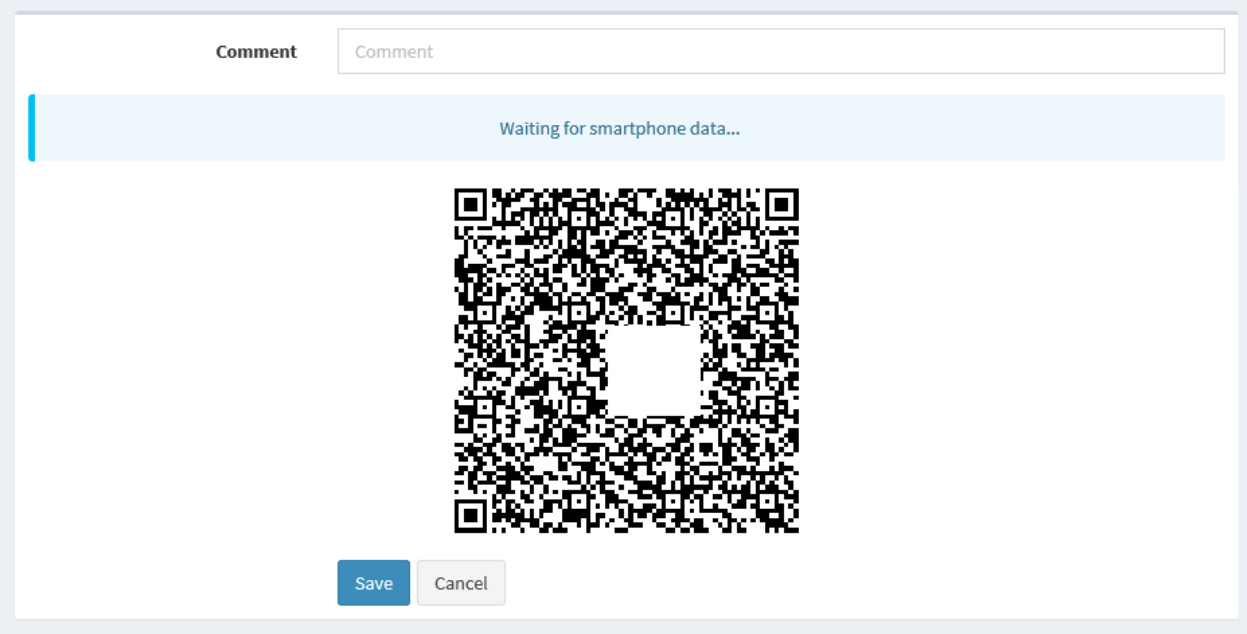
Then follow the steps below:

1. You see a message **Press button "Save" to start smartphone enrolling**.

2. You may enter a comment in **Comment** field. It should be a text like *my iPhone*.

3. Click **Save** button. You will see a QR code.

4. Move a cursor out of the QR code and open the NetIQ Advanced Authentication smartphone app.



5. Tap **Offline authentication** button in the app.

6. Tap **+** button to add a new authenticator in the app.

7. Use camera of your smartphone to scan the QR code.

8. You will see a message **Authenticator "Smartphone" added**.

9. Enter your username and an optional comment in the smartphone app.

10. Save the authenticator on your smartphone.

You may get the error **Enroll failed: Enroll timeout** if you didn't enroll the authenticator during few minutes. In this case refresh the browser page and initialize enrollment again.

If you are not able to scan the QR code with NetIQ Advanced Authentication app, try to do the following:

a. try to scan the zoomed QR code by making a zoom of the page to 125-150%.
b. ensure that nothing overlaps the QR code (mouse cursor, text).

To test the authenticator follow the next steps:

1. Click the Smartphone icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message **Waiting for smartphone data...**

3. Open the NetIQ Advanced Authentication smartphone app. You will get an authentication request message.
4. Tap **Accept** button to accept the authentication request. You will see the message **Authenticator "Smartphone" passed the test**. If you tap the **Reject** button, the authentication will be declined and you will see the message **Auth rejected**. If you ignored the authentication request, in a couple of minutes you will get a message **Auth confirmation timeout**.

SMS OTP

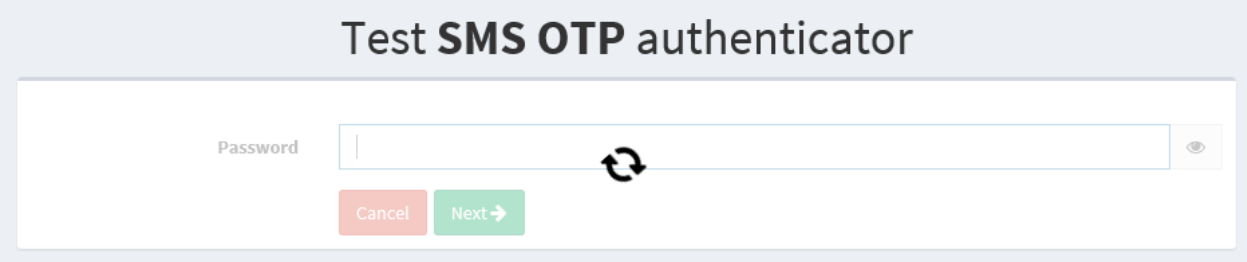
The SMS OTP authentication method uses your mobile phone number from your account attribute. The authenticator sends an SMS message to your mobile phone. The message contains One-Time Password (OTP). You can use this OTP to authenticate withing a certain time frame.

This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

1. Click the SMS OTP icon in the **Enrolled methods** section.

2. Ensure that your mobile phone number (specified after the text **The mobile number where an SMS OTP is sent:**) is valid. Contact your system administrator to change the mobile number if it's invalid.



3. Click **Test** button. In few seconds you will see a message **OTP password sent, please enter**.

4. Check your SMS. You should get an SMS message with one-time password.

5. Enter the OTP to the **Password** field.

6. Click **Next**. You will see a message **Authenticator "SMS OTP" passed the test**. If the provided authenticator is invalid you will see a message **Wrong answer, try again**.

TOTP

TOTP is a time-based one-time password. This method uses a predefined time step, which is equal to 30 seconds by default. It means that each 30 seconds a new one-time password will be generated.

To enroll the TOTP authenticator you should follow recommendations of your system administrator. TOTP method supports different cases of usage:

A. Using NetIQ Advanced Authentication smartphone app (Apple iOS ap, Google Android app).
B. Using Google Authenticator app.
C. Using OATH TOTP compliant hardware token.
D. Using OATH TOTP compliant software token.

⚠ Format of QR codes for the NetIQ Advanced Authentication and Google Authenticator apps are different, so you need to ask your system administrator which of the apps you should use.

To enroll a TOTP authenticator click the TOTP icon.

A. Using NetIQ Advanced Authentication smartphone app

In you want to enroll an authenticator using NetIQ Advanced Authentication smartphone app follow the next steps:

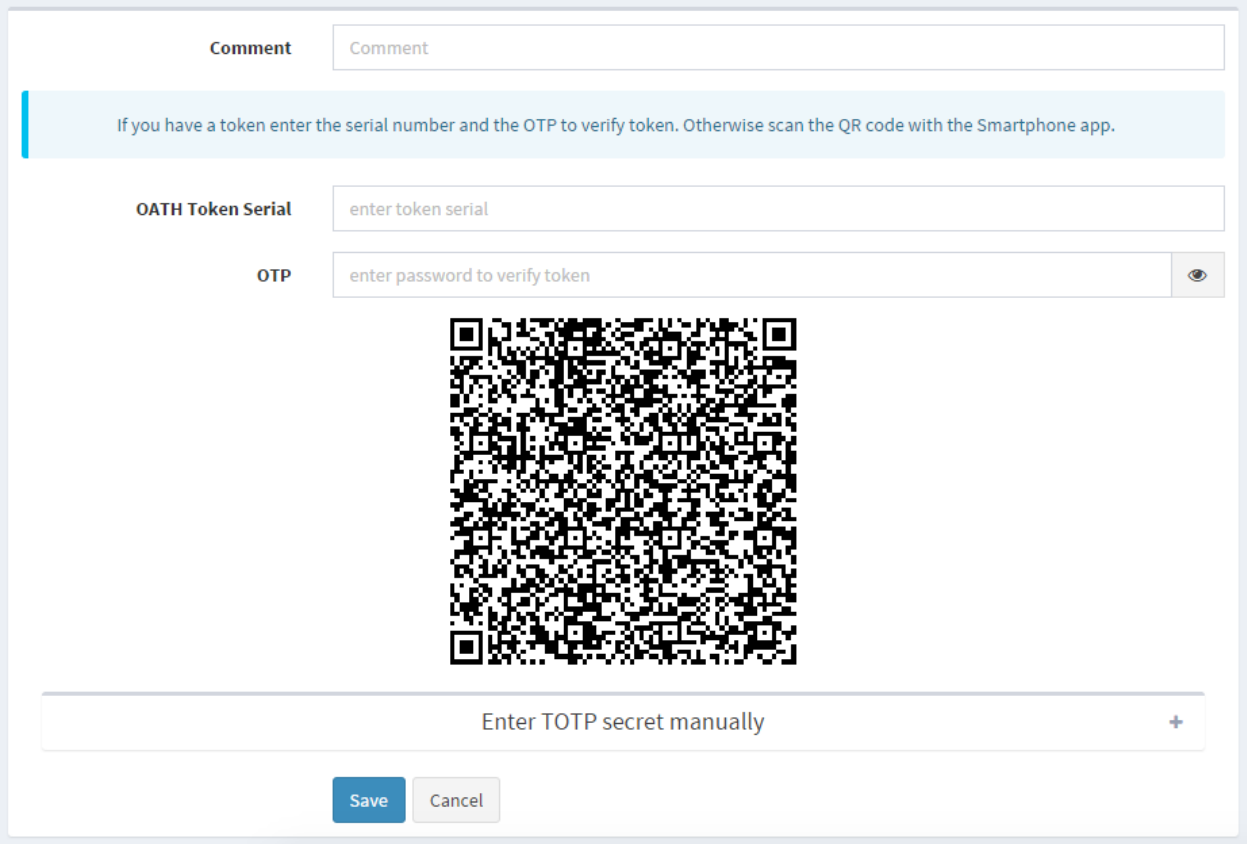
1. You may enter a comment in **Comment** field. It should be a text like *my iPhone*.

2. Move a cursor out of the QR code and open the NetIQ Advanced Authentication smartphone app.

3. Tap **Offline authentication** button in the app.

4. Tap **+** button to add a new authenticator in the app.

5. Use camera of your smartphone to scan the QR code.



6. Click **Save** button.

7. You will see a message **Authenticator "TOTP" added**.

8. Enter your username and an optional comment in the smartphone app.

9. Save the authenticator on your smartphone.

If you are not able to scan the QR code with NetIQ Advanced Authentication app, try to do the following:

a. try to scan the zoomed QR code by making a zoom of the page to 125-150%.
b. ensure that nothing overlaps the QR code (mouse cursor, text).
c. try to scan it using the Google Authenticator app.

If it doesn't work, contact your system administrator.

B. Using Google Authenticator app

Follow the steps below to enroll an autheticator using the Google Authenticator app:

1. You may enter a comment in **Comment** field. It should be a text like *my iPhone*.
2. Move a cursor out of the QR code and open the Google Authenticator app.
3. Tap **BEGIN SETUP** text in the app.
4. Tap **Scan barcode** button to add a new authenticator in the app.
5. Use camera of your smartphone to scan the QR code.
6. Click **Save** button.
7. You will see a message **Authenticator "TOTP" added**.

 You may get the *Invalid barcode* error. It means that probably the QR code is compatible with NetIQ Advanced Authentication app.

C. Using OATH TOTP compliant hardware token

To enroll OATH TOTP compliant hardware token follow the steps below:

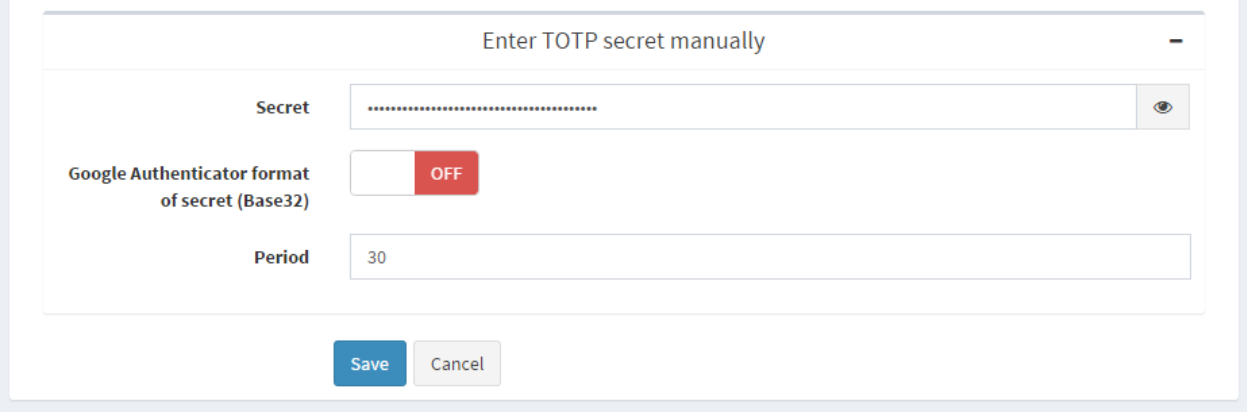
1. You may enter a comment in **Comment** field. It should be a text like *HID token*.
2. Enter your token's serial number to the **OATH Token Serial** field. You may get the information on back side of your token.
3. Press the token's button and enter the OTP to the **OTP** field.
4. Click **Save** button.
5. You will see a message **Authenticator "TOTP" added**.

D. Using OATH TOTP compliant software token

To enroll OATH TOTP compliant software token follow the steps below:

1. You may enter a comment in **Comment** field. It should be a text like *A phone app*.

2. Expand the **Enter TOTP secret manually**.



3. Enter 40 hexadecimal characters in **Secret** field.

4. Check the **Google Authenticator format of secret (Base32)** option if you use the Google Authenticator app.

5. Change the **Period** value if required (30 seconds by default).

6. Click **Save** button.

7. You will see a message **Authenticator "TOTP" added**.

U2F

The FIDO U2F enrollment is supported on Microsoft Windows and Apple MacOS. The NetIQ FIDO U2F Service component must be installed for enrollment if you don't use the Google Chrome browser. It contains a built-in module.

To enroll a FIDO U2F authenticator click the U2F icon.

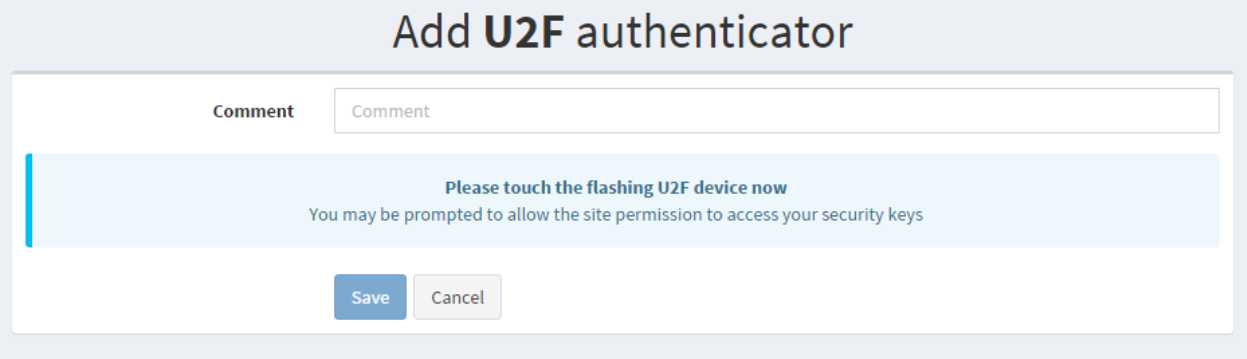
Then follow the steps below:

1. You see a message **Press button "Save" to begin enrolling**.

2. You may enter a comment in **Comment** field. It should be a text like *YubiKey token*.

3. Ensure that your FIDO U2F token is properly connected to the machine.

4. Click **Save** button. You will see a message **Please touch the flashing U2F device now. You may be prompted to allow the site permissions to access your security keys**



5. Look at the FIDO U2F token. If it's flashing, press a FIDO U2F button. You will see a message **Authenticator "U2F" enrolled**. If it doesn't flash wait 10 seconds, if it still doesn't flash then reconnect your token and repeat the steps.

 If you see a message **Cannot reach local FIDO U2F Service. Ask your admin to enable it. You may use Google Chrome browser, it has a built-in U2F support** ensure that you have the NetIQ FIDO U2F Service installed.

 If you see a message **Timeout. Press "Save" to start again** click **Save** again.

To test the authenticator follow the next steps:

1. Click the U2F icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message **Please touch the flashing U2F device now. You may be prompted to allow the site permissions to access your security keys**
3. Press a FIDO U2F button. You will see a message **Authenticator "U2F" passed the test**. If the provided card is invalid you will see a message **Token is not registered**.

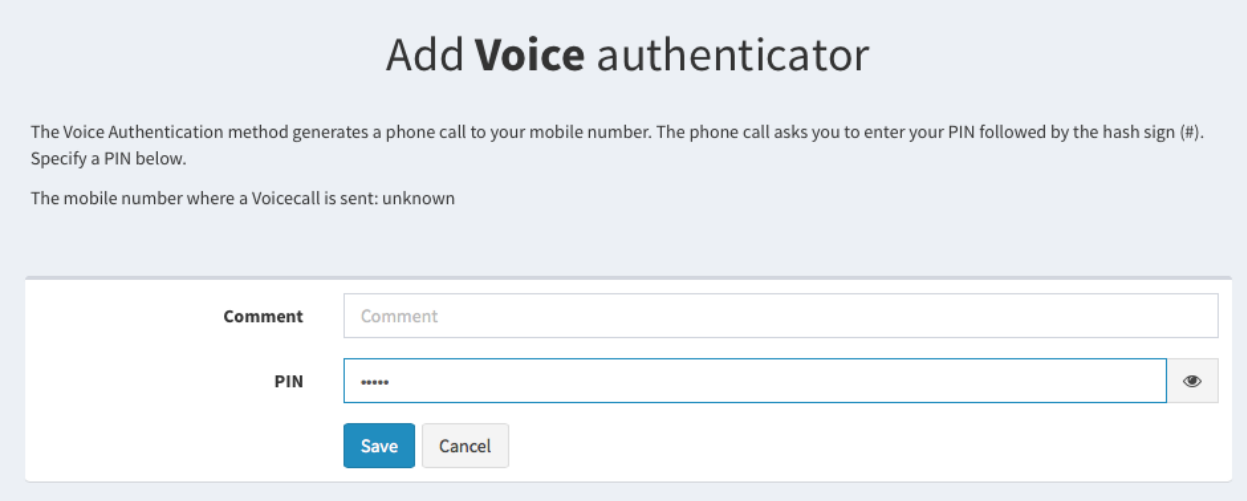
Voice Call

The Voice Call authenticator initiates a phone call to your mobile number. The phone call asks you to enter your PIN. You need to specify the PIN during enrollment.

To enroll a Voice Call authenticator click the Voice icon.

Then follow the steps below:

1. Ensure that a valid phone number is set in the field **The mobile number where a Voicecall is sent:**.
2. You can specify an optional comment in **Comment** field.
3. Specify a **PIN**. By default it must contain at least 3 digits.



4. Click **Save** button. You will see a message **Authenticator "Voice" added**.

 You may get the error **Enroll failed: User has no phone number. Please contact administrators/helpdesk and register your phone**. In this case contact your system administrator and ask to add your phone number for your account.

To test the authenticator follow the next steps:

1. Click the Voice icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Take up the phone and listen to the answerphone.
4. Enter your PIN and tap hash sign (#).
5. You will see a message **Authenticator "Voice" passed the test**. If the provided PIN is invalid you will see a message **Wrong PIN**.

 You will not get notification about the PIN expiration. It's required to sign in to the Self-Service Portal and change the PIN each 42 days.

Index