NetIQ Advanced Authentication Framework

User 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 all user categories and describes how to enroll authenticators and use the assigned authentication chains for different endpoints (Windows Client, MacOS Client, NetIQ Access Manager Advanced Authentication plugin).

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.

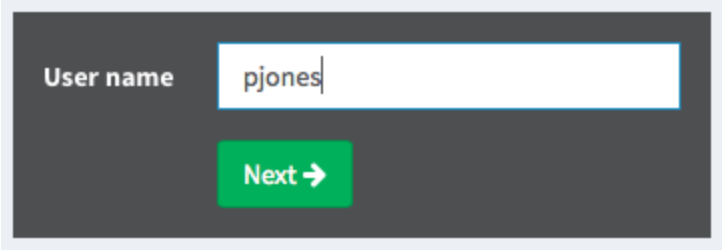
- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

Authenticators Management

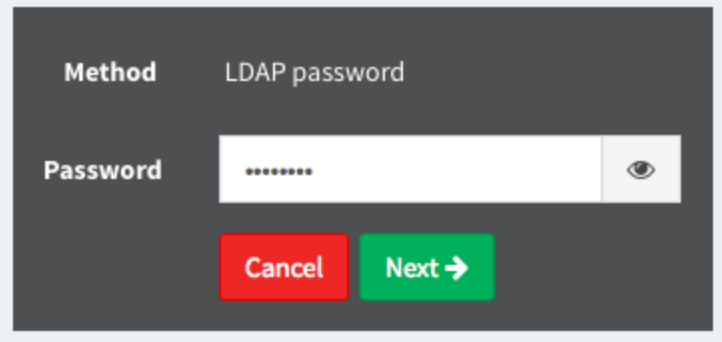
To use the NetIQ Advanced Authentication Framework you need to have at least one enrolled ***authenticator***. Authenticator is a set of encrypted data, which contains your authentication data and which you can use to perform log on to Windows, MacOS, remote resources (if applicable) or NetIQ Access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

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

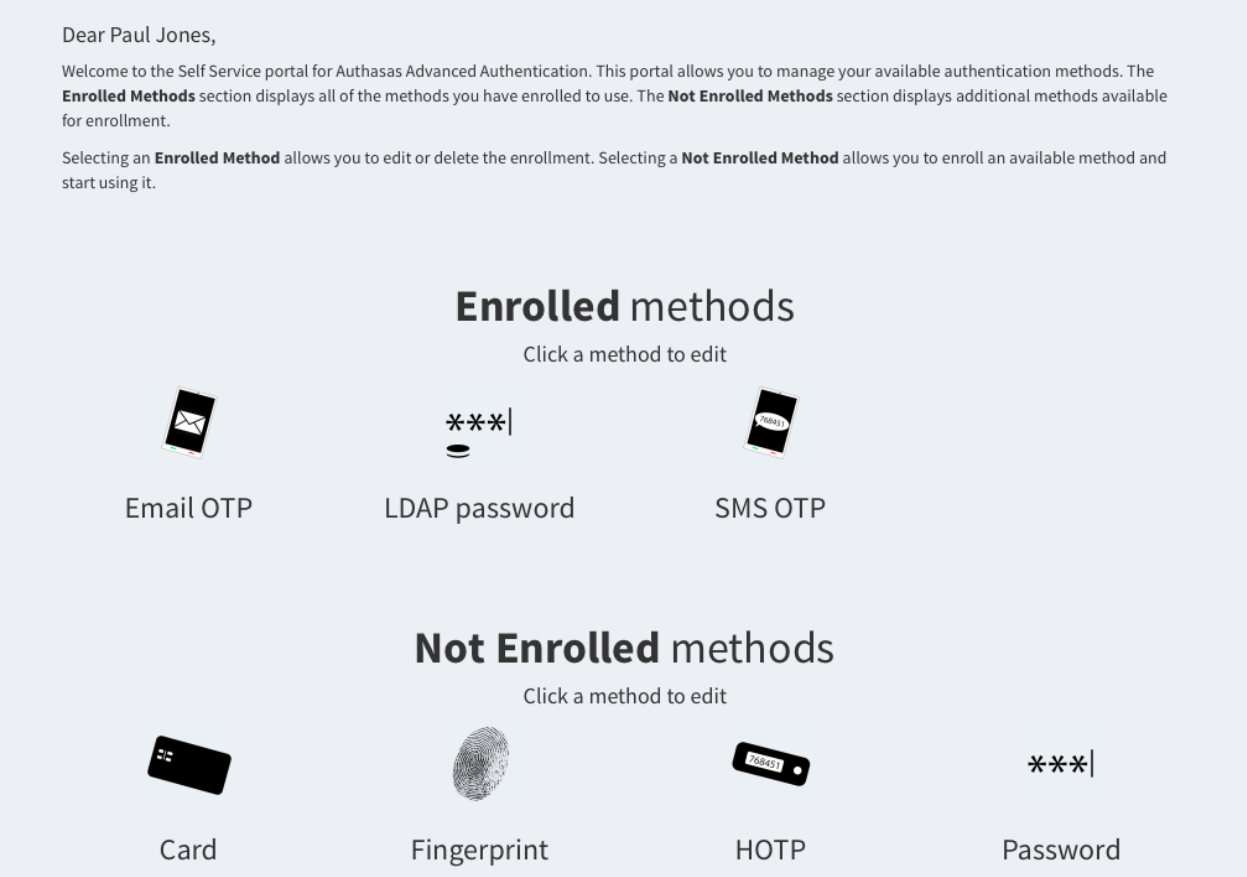
1. Open the URL in your browser and you will see the **User name** prompt.



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 Self-Service Portal.



A set of **Not Enrolled methods** may vary. Contact your system administrator if you don't see a method which you need to enroll.

4. Select a method to enroll.

Methods which enroll automatically:

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

Methods which enroll by security officer only:

1. Emergency Password

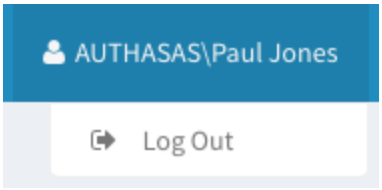
Not Enrolled methods:

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

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

To re-enroll an existing authenticator click the enrolled method, change settings (if applicable) and click **Save**. To delete an existing authenticator click **Delete**.

To log out from the Self-Service Portal click your user name in top right corner and then 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.

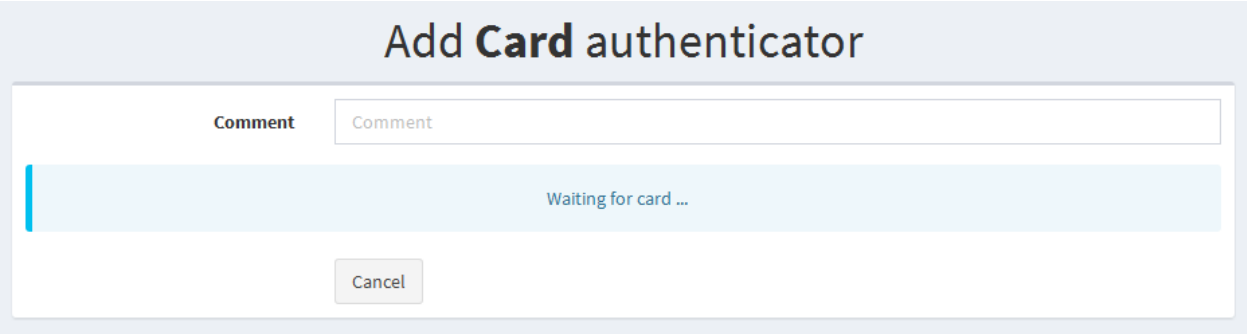
Then follow the steps below:

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:

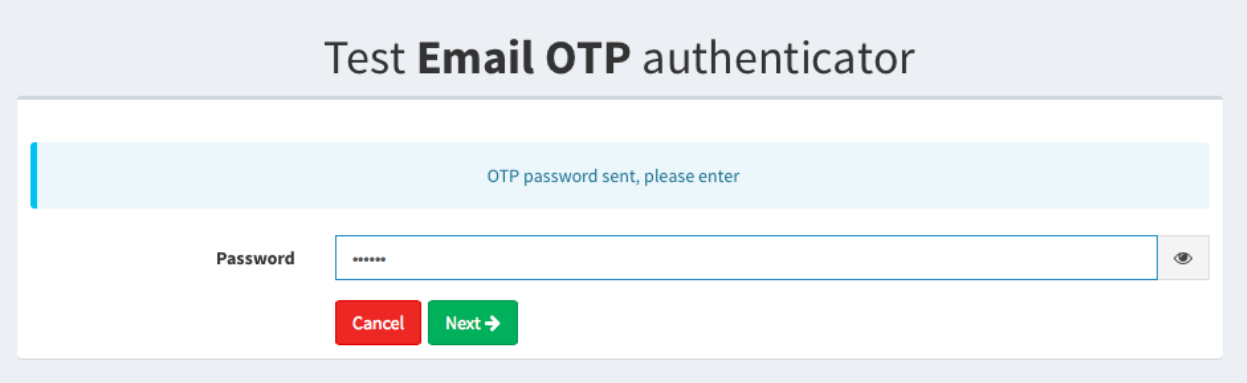
1. Click the Email OTP icon in the **Enrolled methods** section.

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**.

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.

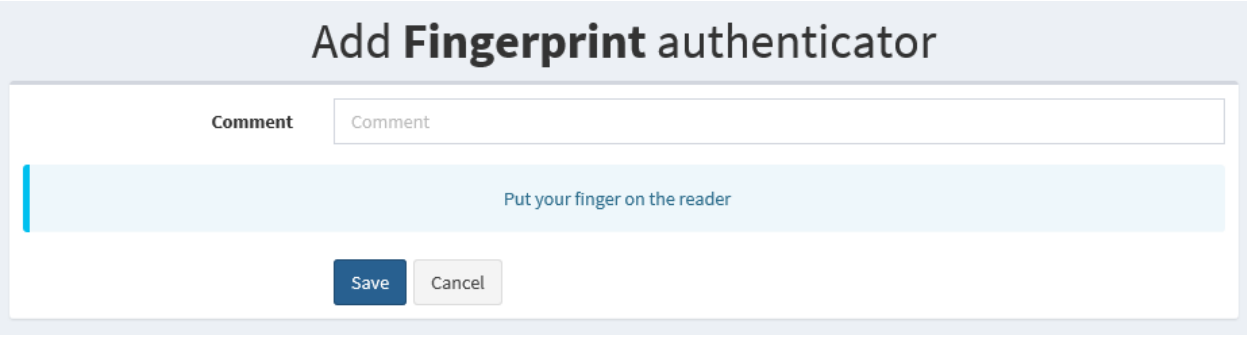
Then follow the steps below:

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:

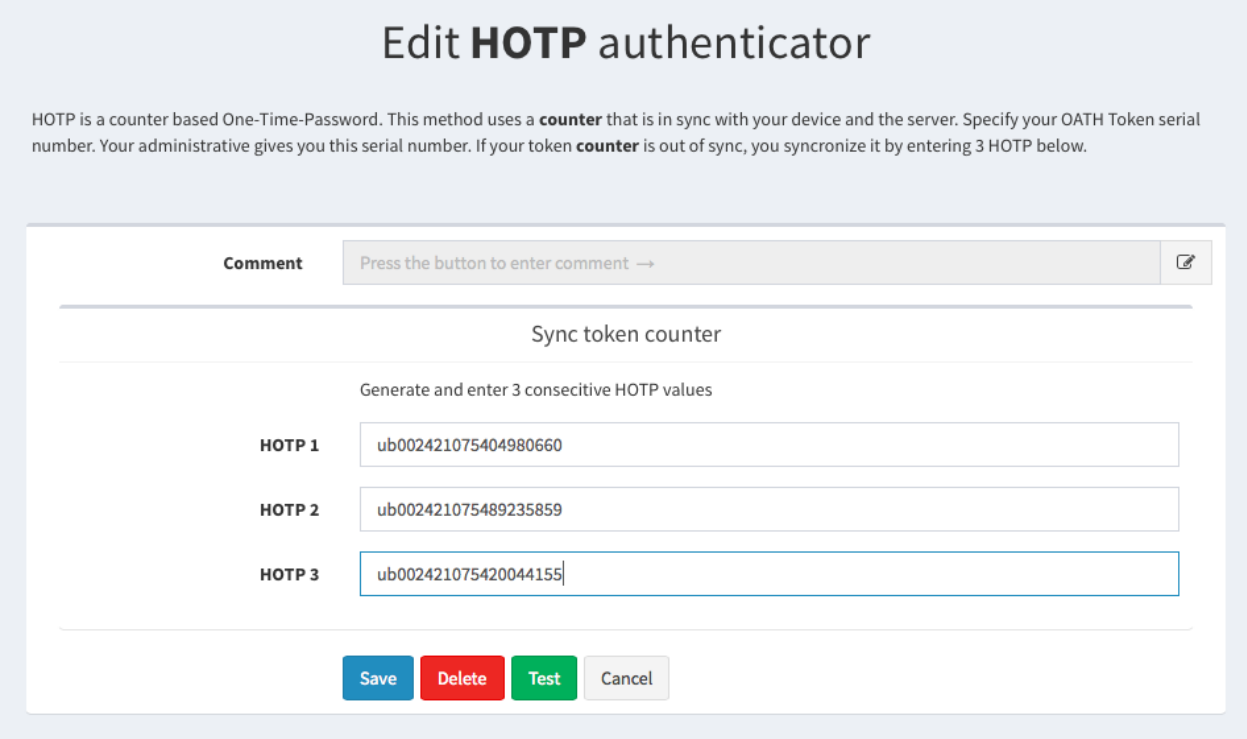
A. A new token is already assigned to your account and enrollment is not needed.
B. A used token is assigned to your account and the HOTP counter synchronization is required.
C. You get an information about serial number of your token and need to assign it to your account.
D. You want to enroll the authenticator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

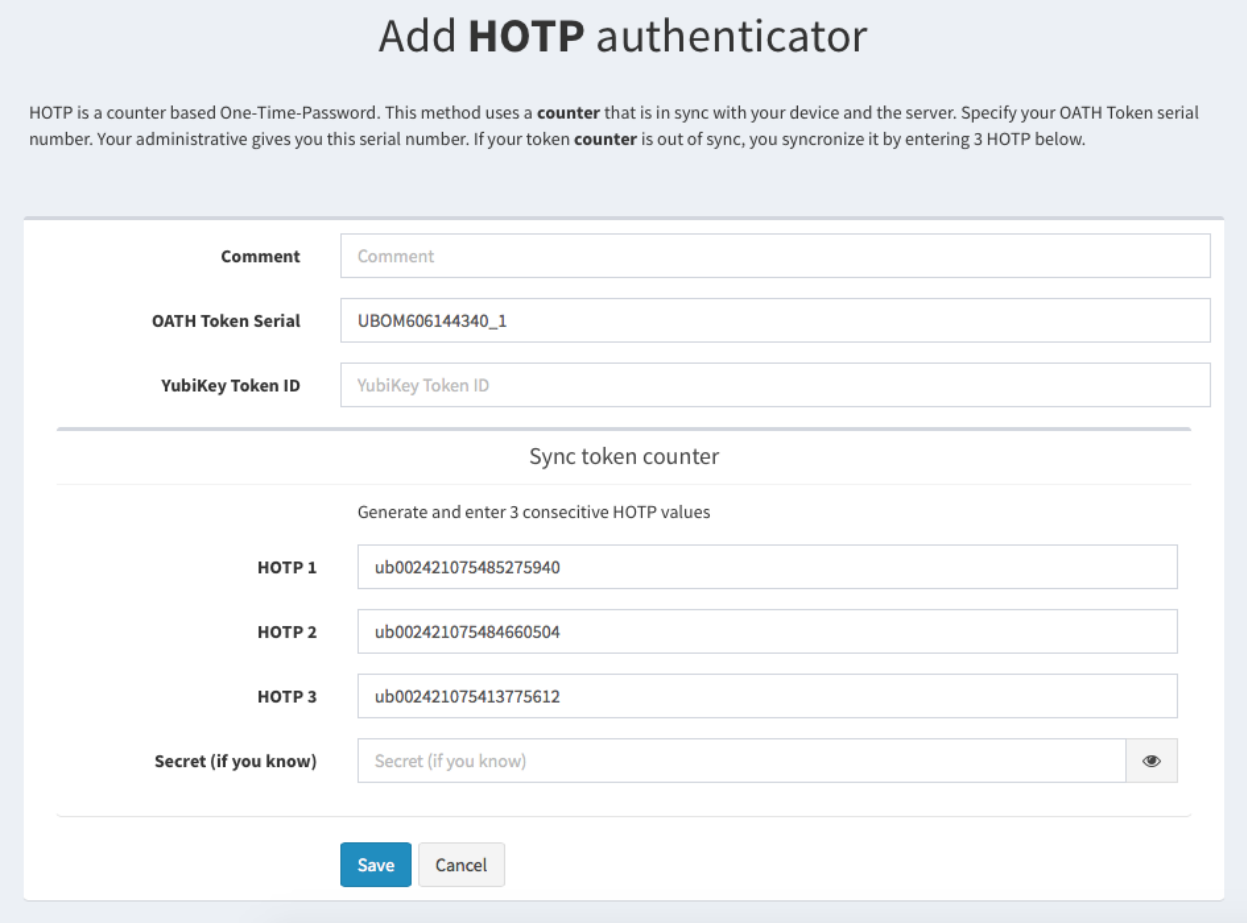


4. Click **Save** button.

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.

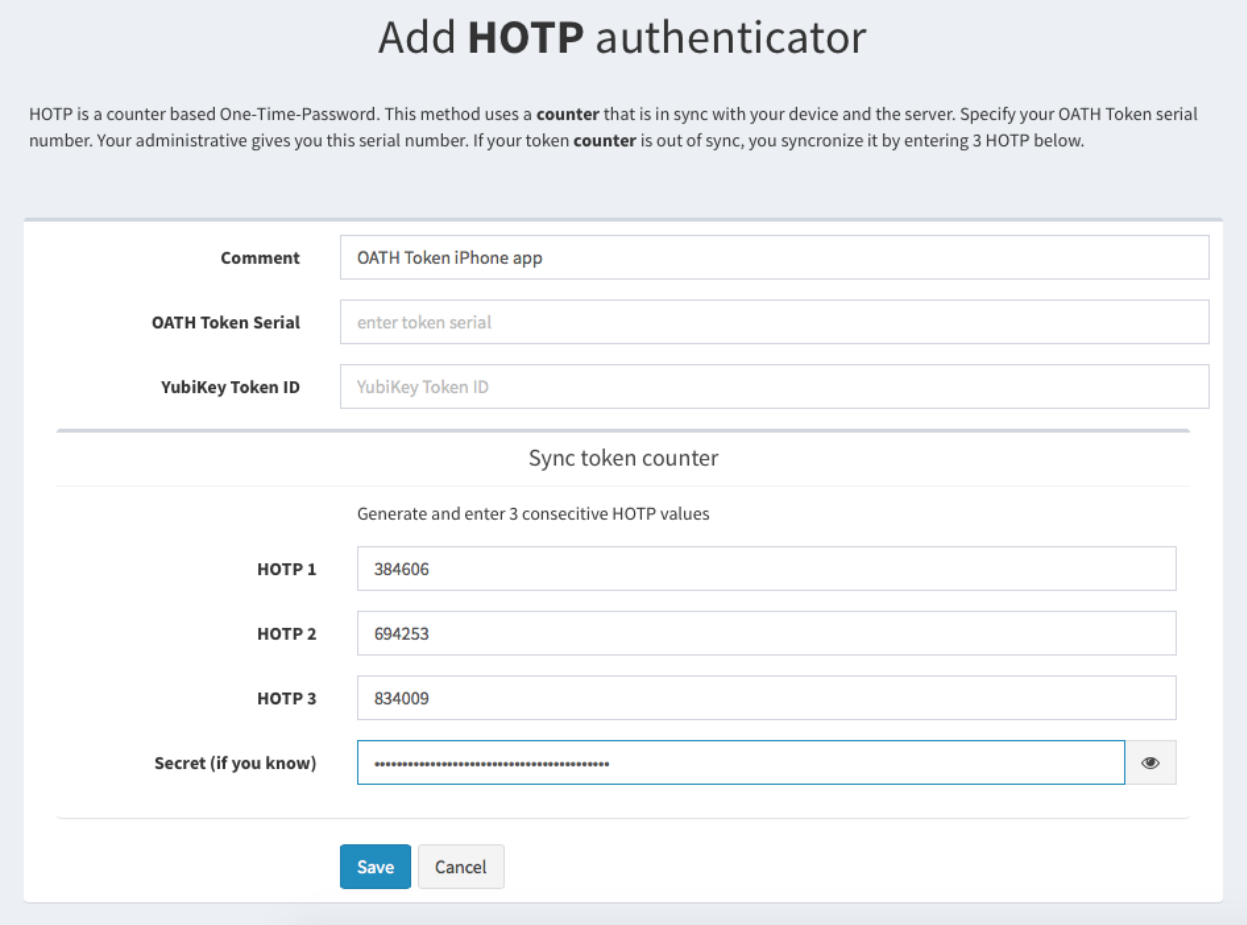


5. Click **Save** button.

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.

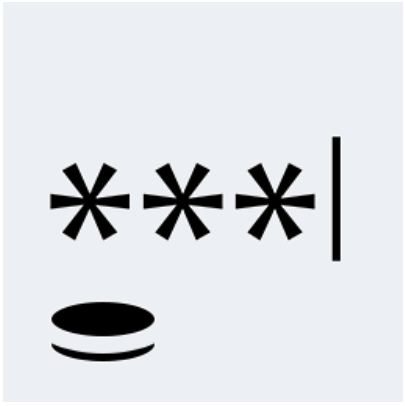
LDAP Password

The LDAP password is a password of your corporate account.

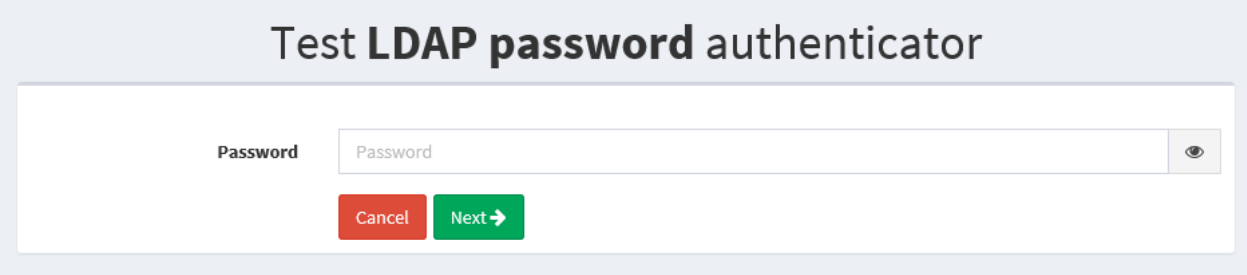
This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

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



2. Click **Test** button.



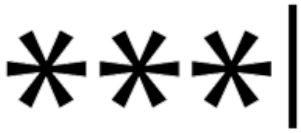
3. Enter your password to the **Password** field.

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

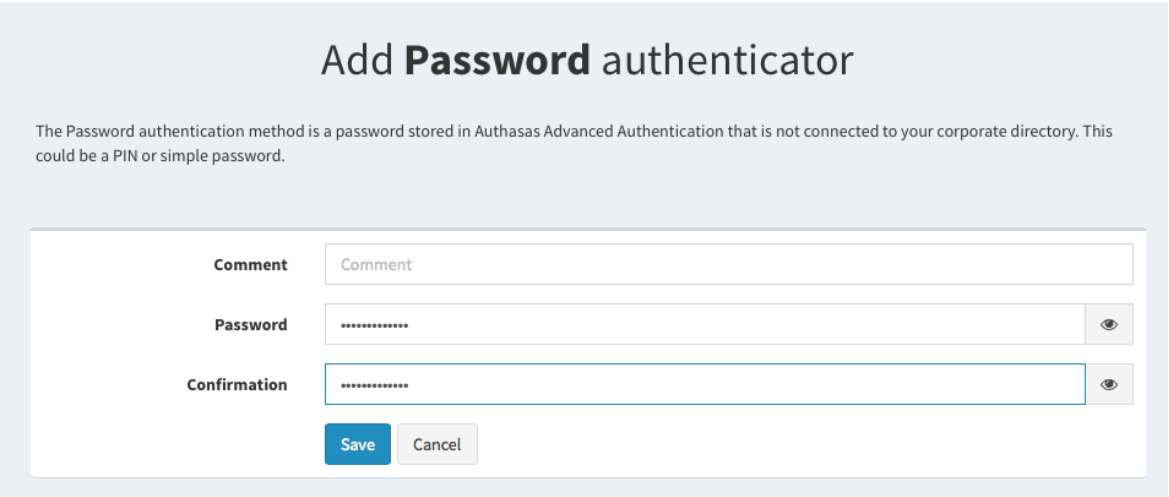
The Password authenticator is a password stored in the NetIQ Advanced Authentication Framework appliance, that is not connected to your corporate directory. This could be a PIN or simple password.

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

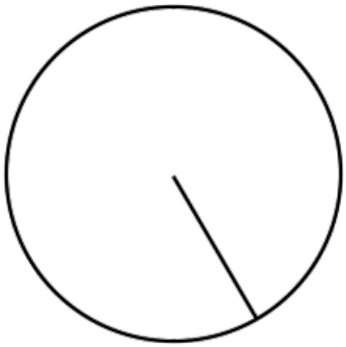
The Radius Client authentication method forwards your authentication request to a third-party Radius Server.

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

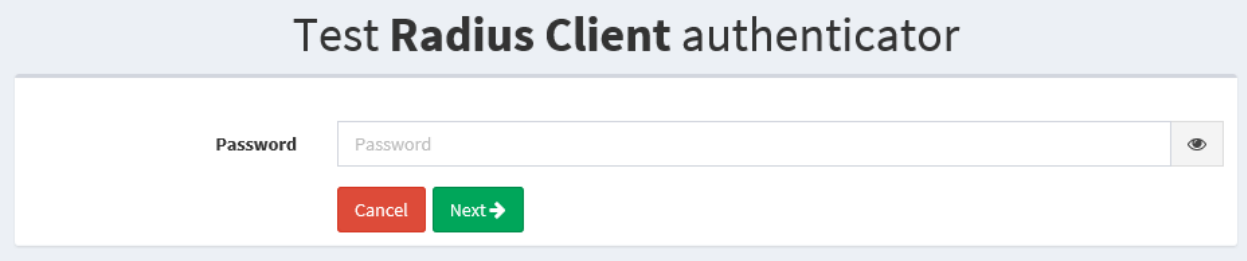
By default a user name from your corporate directory is used. To change it specify a required name in the **User name** field. Then click **Save** button.

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**.

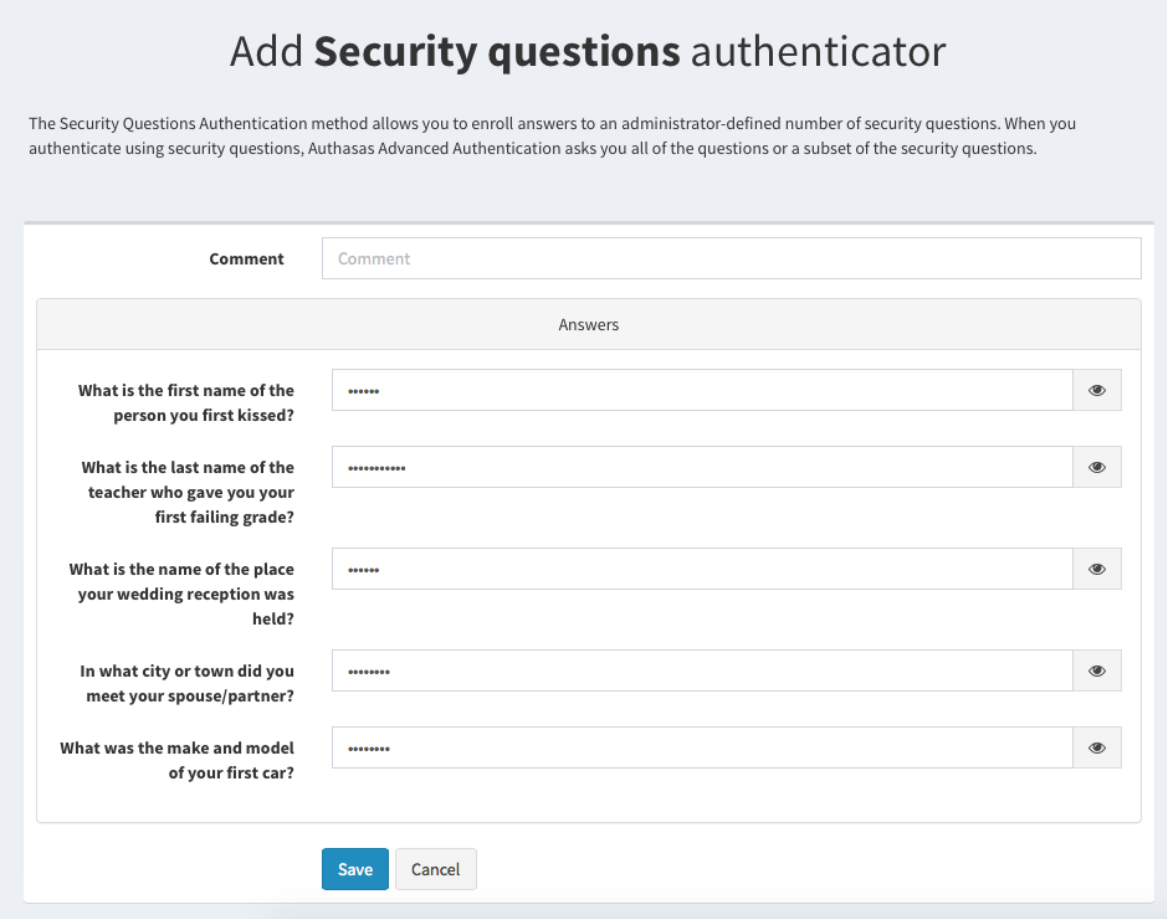
Security Questions

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.

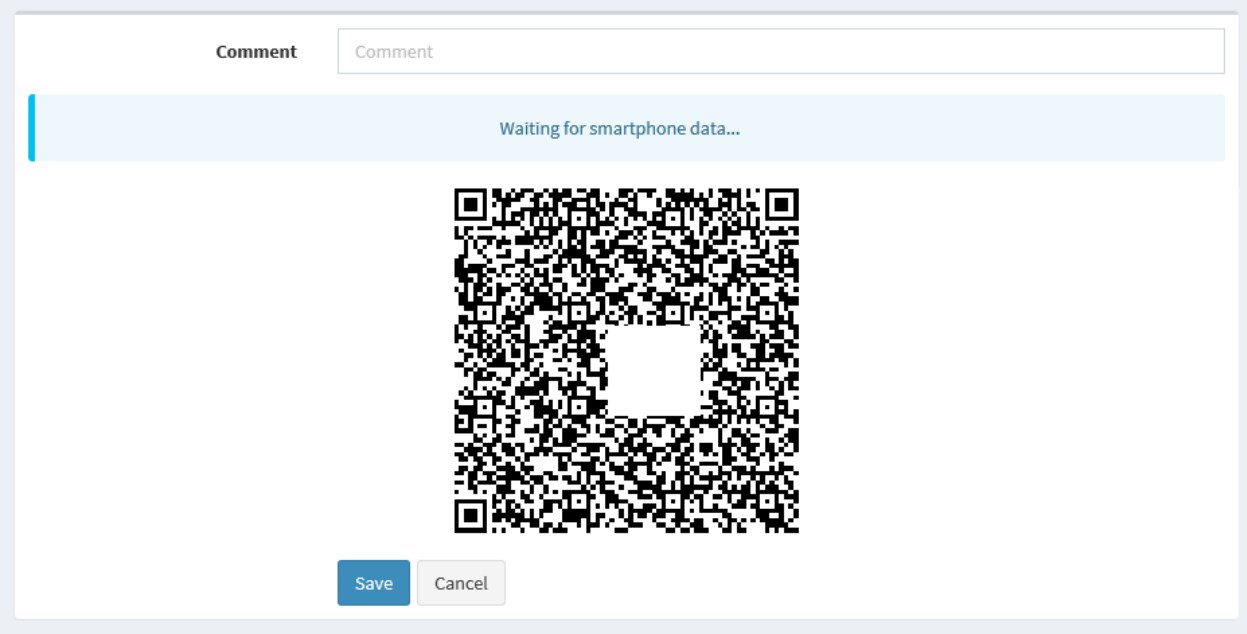
Then follow the steps below:

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

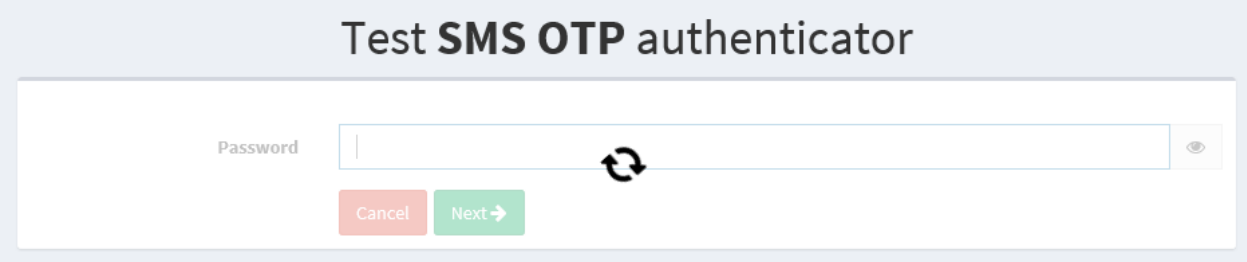
The SMS OTP authentication method uses your mobile phone number from your account attribute. The authenticator sends an SMS message to your mobile phone. The message contains One-Time Password (OTP). You can use this OTP to authenticate withing a certain time frame.

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:

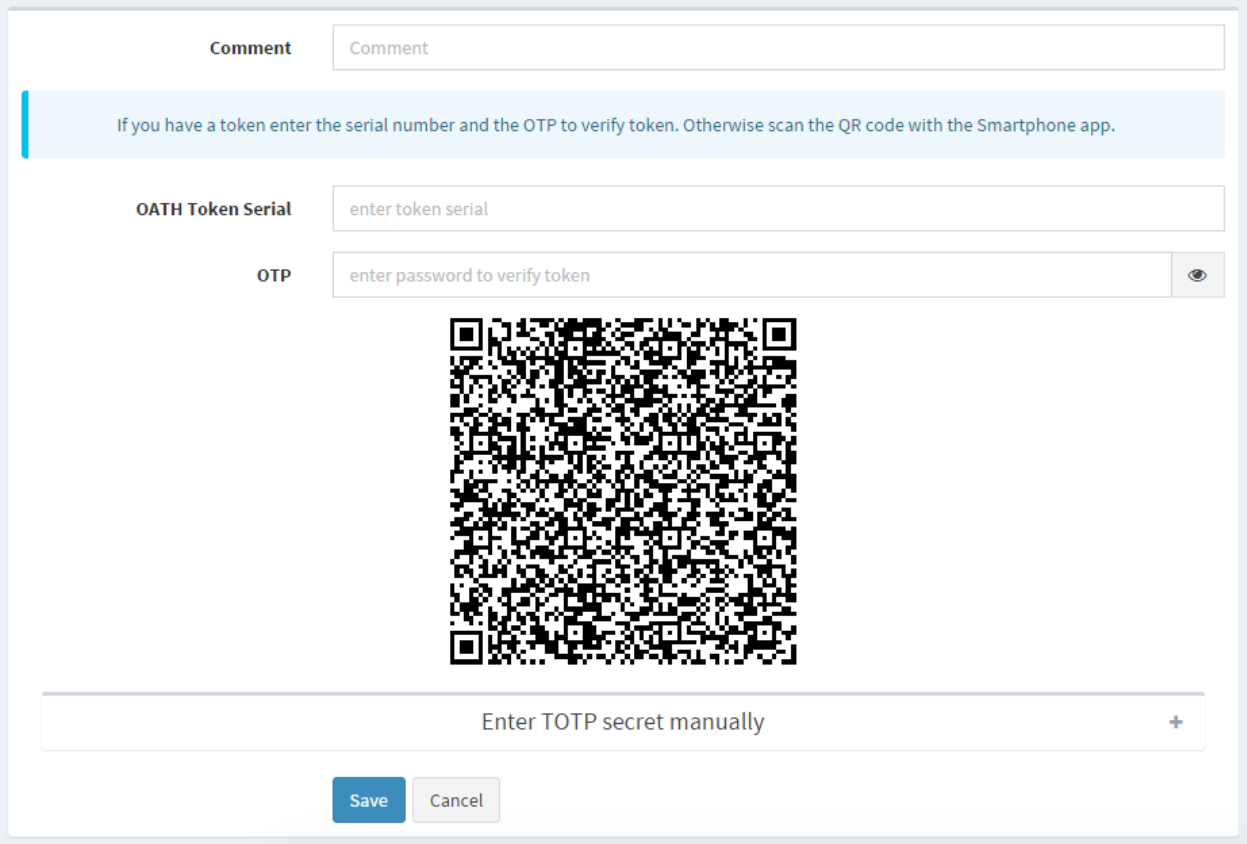
1. You may enter a comment in **Comment** field. It should be a text like *my iPhone*.

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:

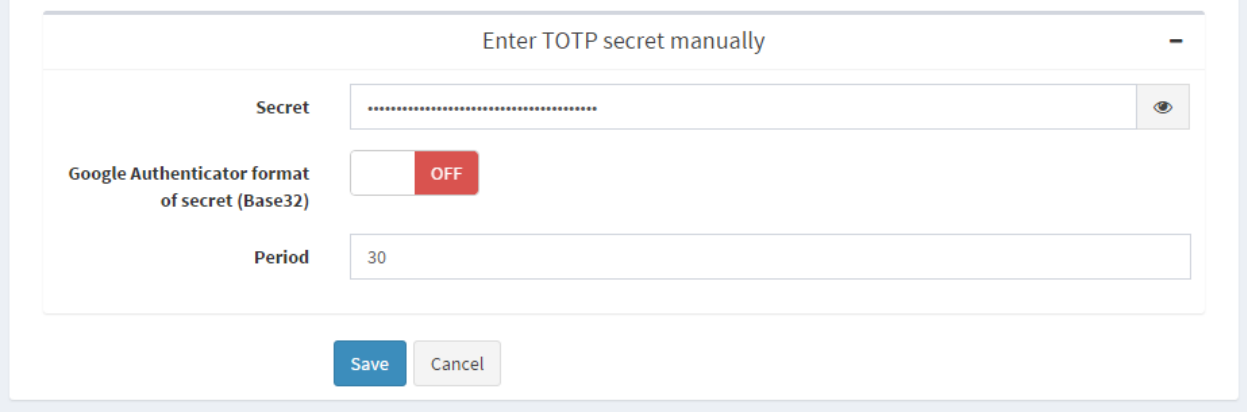
1. You may enter a comment in **Comment** field. It should be a text like *HID token*.
2. Enter your token's serial number to the **OATH Token Serial** field. You may get the information on back side of your token.
3. Press the token's button and enter the OTP to the **OTP** field.
4. Click **Save**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

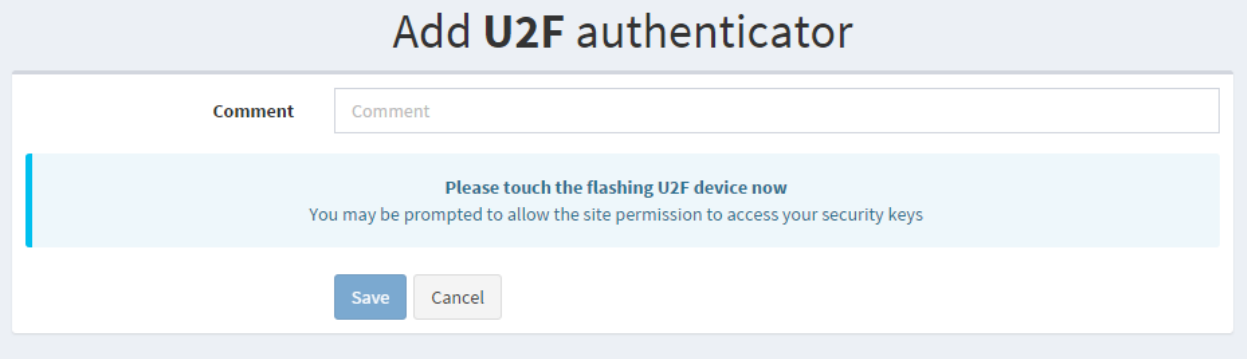
Then follow the steps below:

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**.

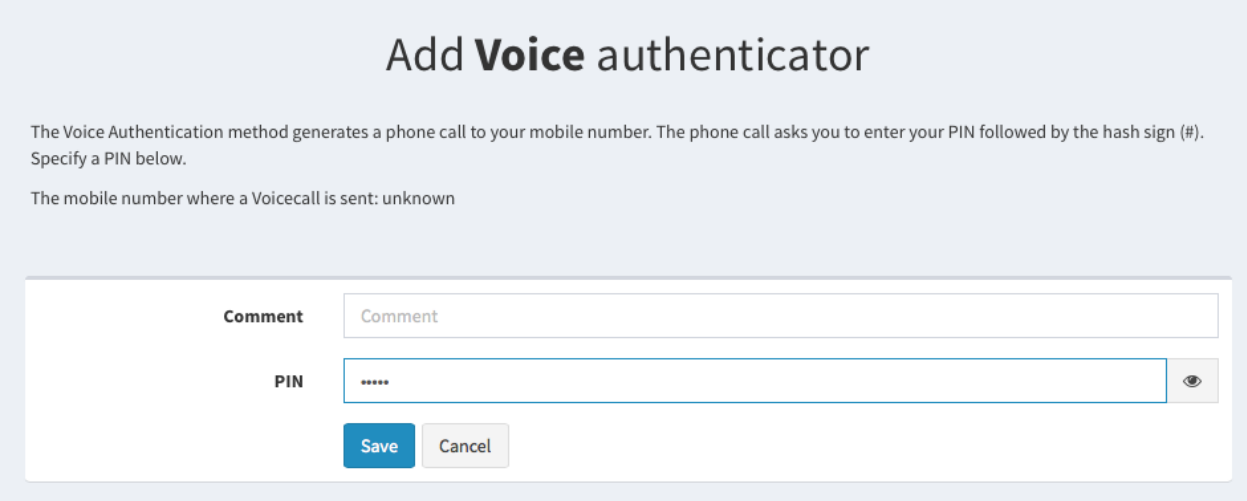
Voice Call

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.

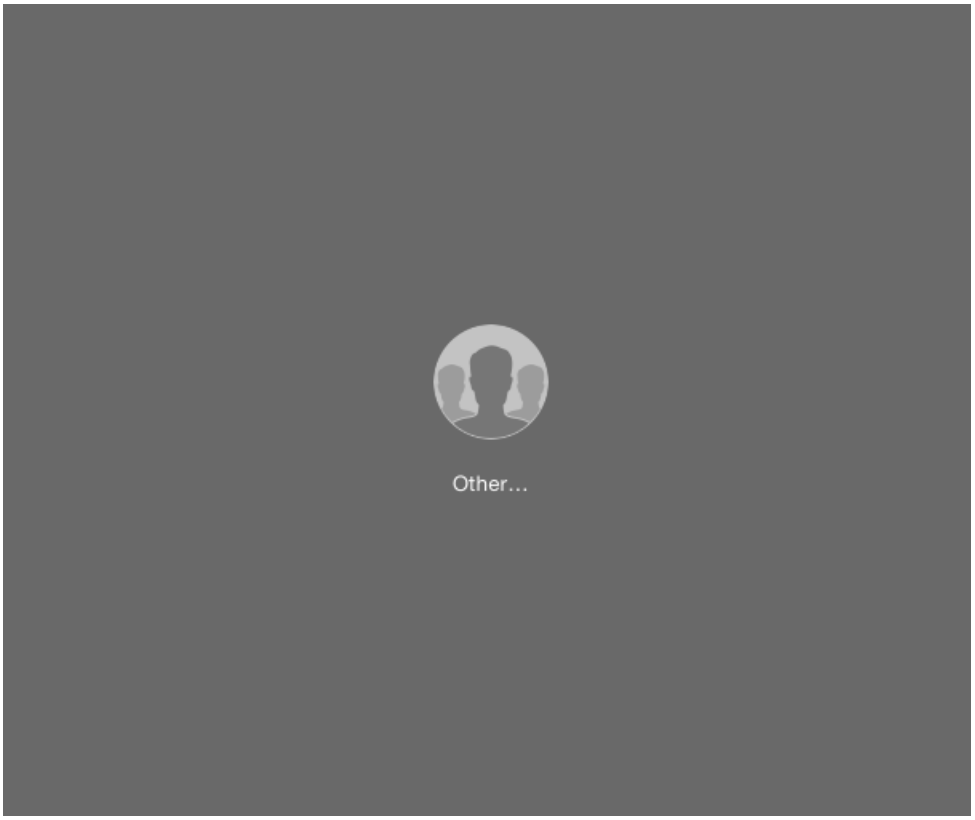
To test the authenticator follow the next steps:

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.

Log On to Mac

To perform a first log on to Mac using the NetIQ Advanced Authentication Framework on the user selection screen click **Other...** button.

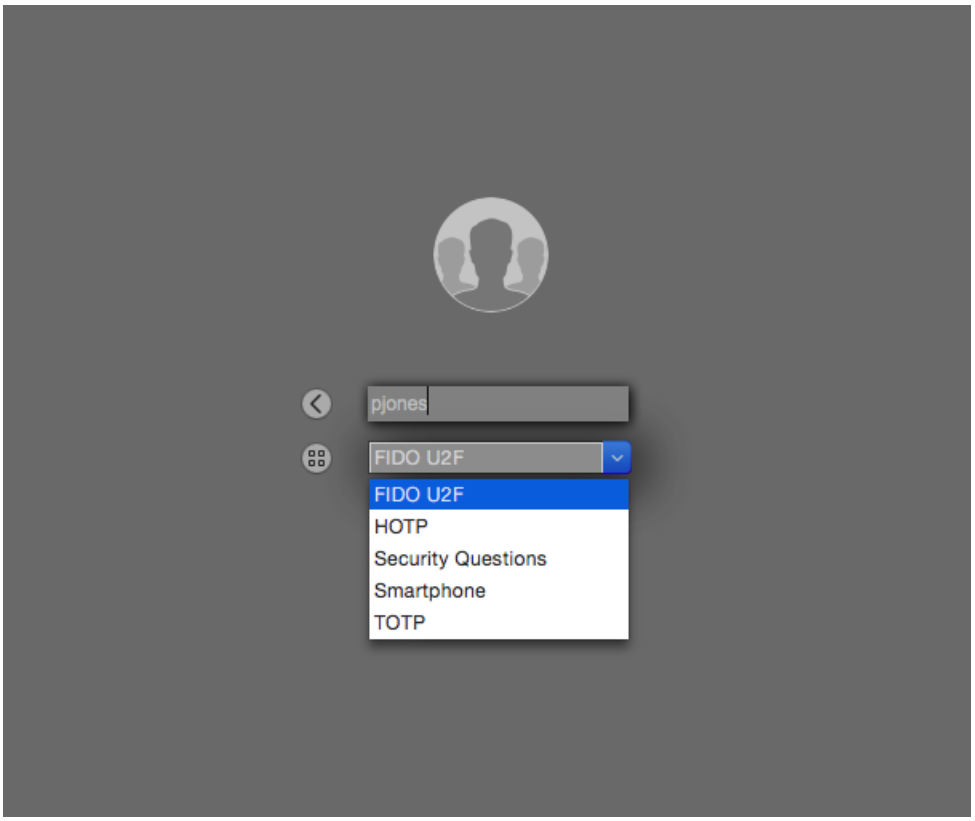


You will see the NetIQ Advanced Authentication Framework log in menu:

Enter your user name in the **Enter user name** field. You may be able to enter the user name without your domain name or with it. E.g. **pjones** or **company\pjones**.

Depending on assigned authentication chains you will be prompted to provide different authentication data. The authentication chain is a set of one or some authentication methods.

You are able to select an authentication chain from the list of available chains using the list button. If you click it you will see a dropdown menu in which a last used chain is selected.



Click down arrow of the dropdown menu to select another chain.

The following links will help you to get information on how to authenticate using a specific method of assigned authentication chain:

1. Email OTP
2. Emergency Password
3. HOTP
4. LDAP Password
5. Password
6. RADIUS
7. Security Questions
8. Smartphone
9. SMS
10. TOTP
11. U2F
12. Voice Call

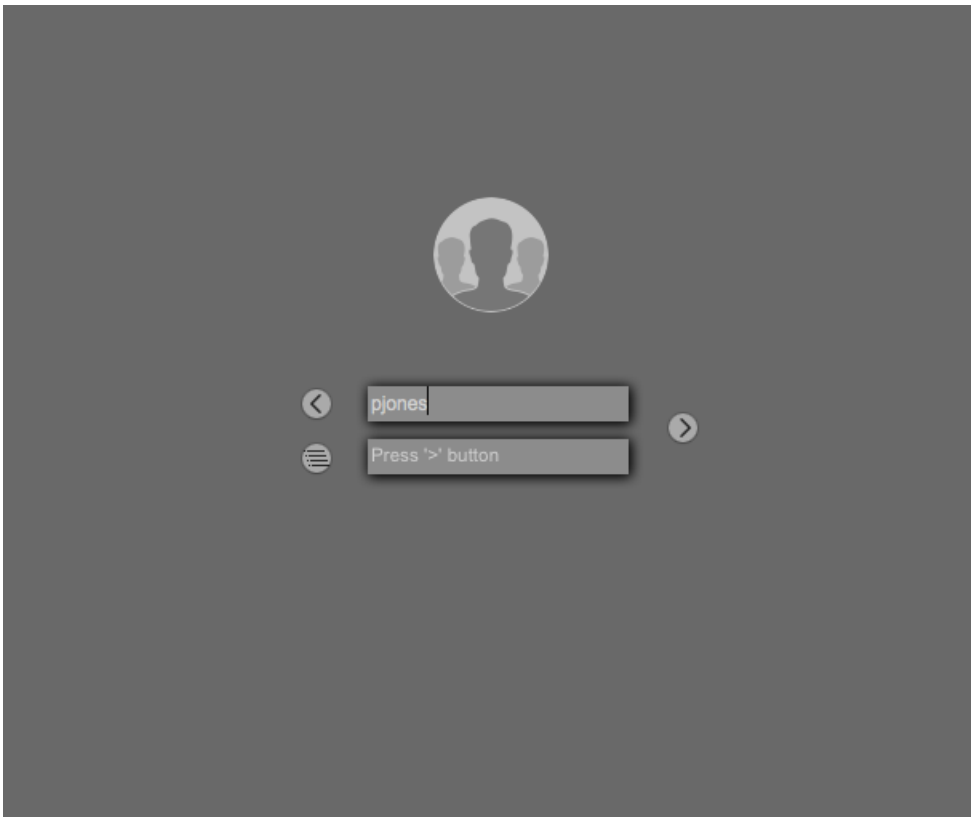
From the log on screen you can click back arrow button to switch back to the user selection screen.

Email

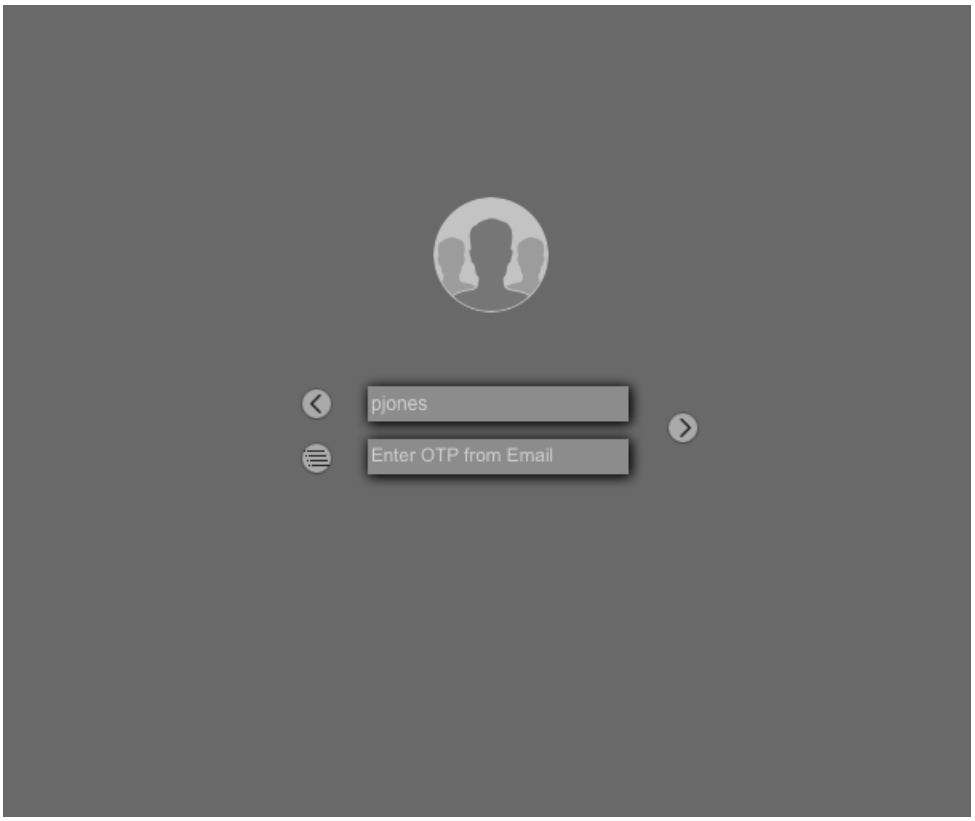
To perform authentication by Email method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Click **>** button to send you an automatic email message.

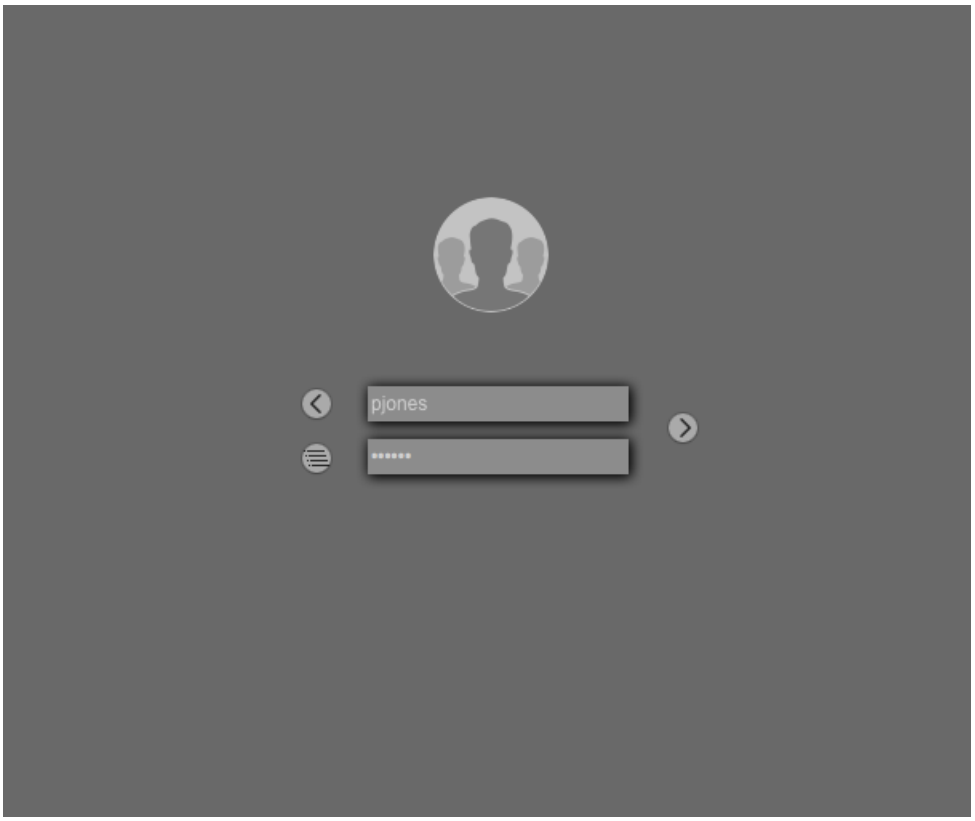


In few seconds the message **Press '>' button** will be changed to **Enter OTP from Email**.



3. Set focus to the field and check your email. You should get an email message with one-time password (E.g. *User Paul Jones from pjones-macbook-air.local login to MacOS logon: OTP: 381441*).

4. Enter the OTP from Email to the field.



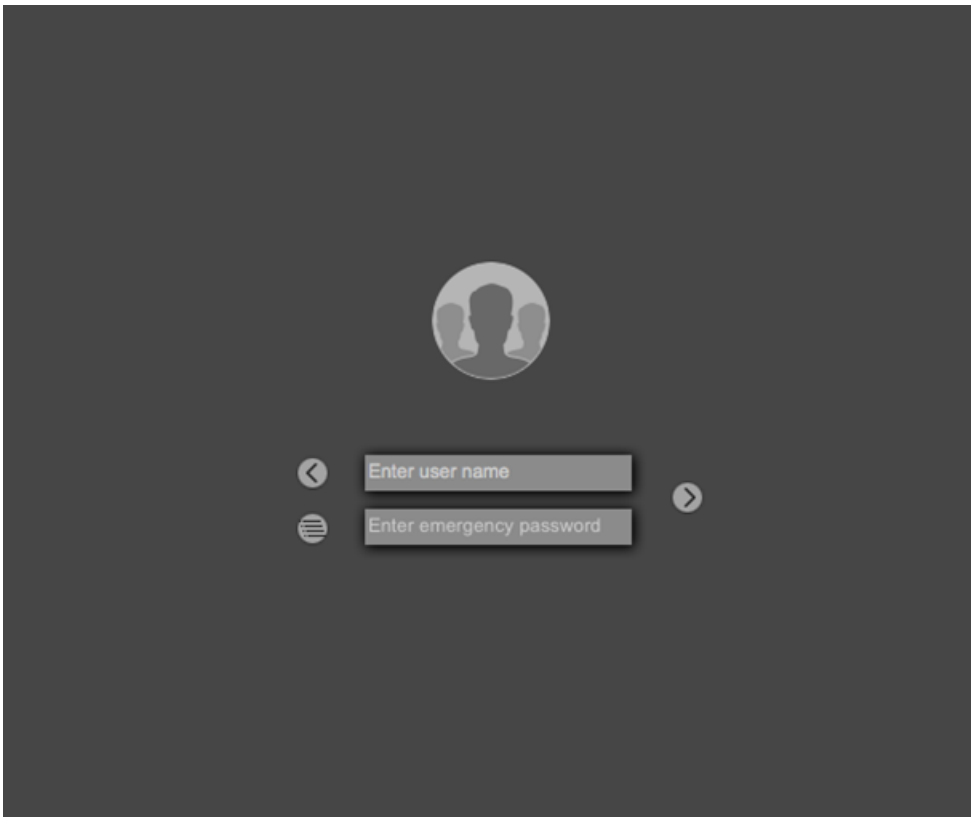
5. Click **>** button.

Emergency Password

To perform authentication by Emergency Password follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Enter emergency password** field and enter your emergency password.



3. Click **>** button.

FIDO U2F

To perform authentication by FIDO U2F method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Click ">" button.

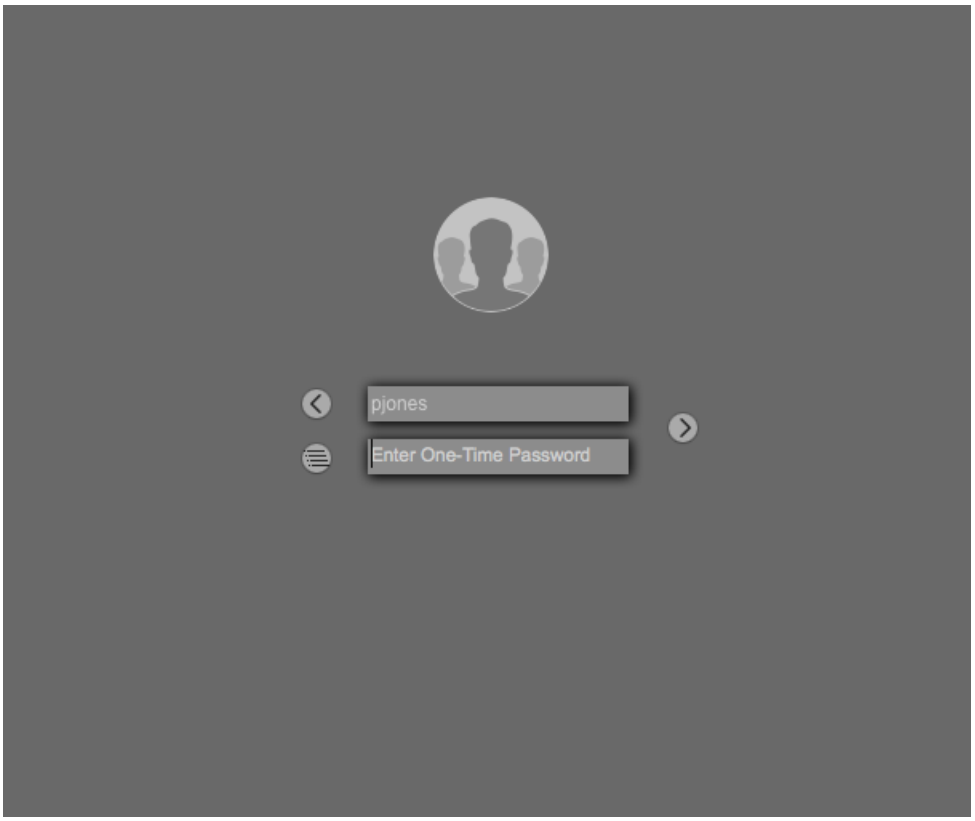
3. When you see the message **Touch the token** look at the FIDO U2F token. If it's flashing, press a FIDO U2F button. If it doesn't flash wait 10-15 seconds, if it still doesn't flash then reconnect your token and repeat the steps.

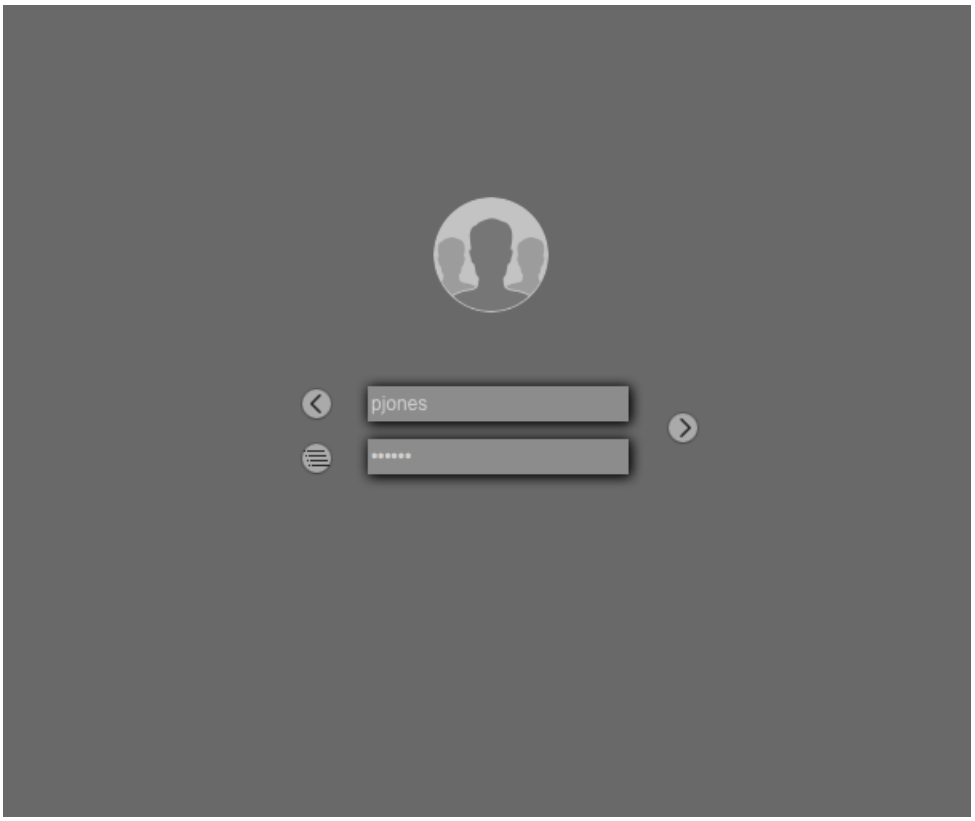
HOTP

To perform authentication by HOTP method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Enter One-Time Password** field and enter your HOTP manually or if you use a hardware USB token click the token's button





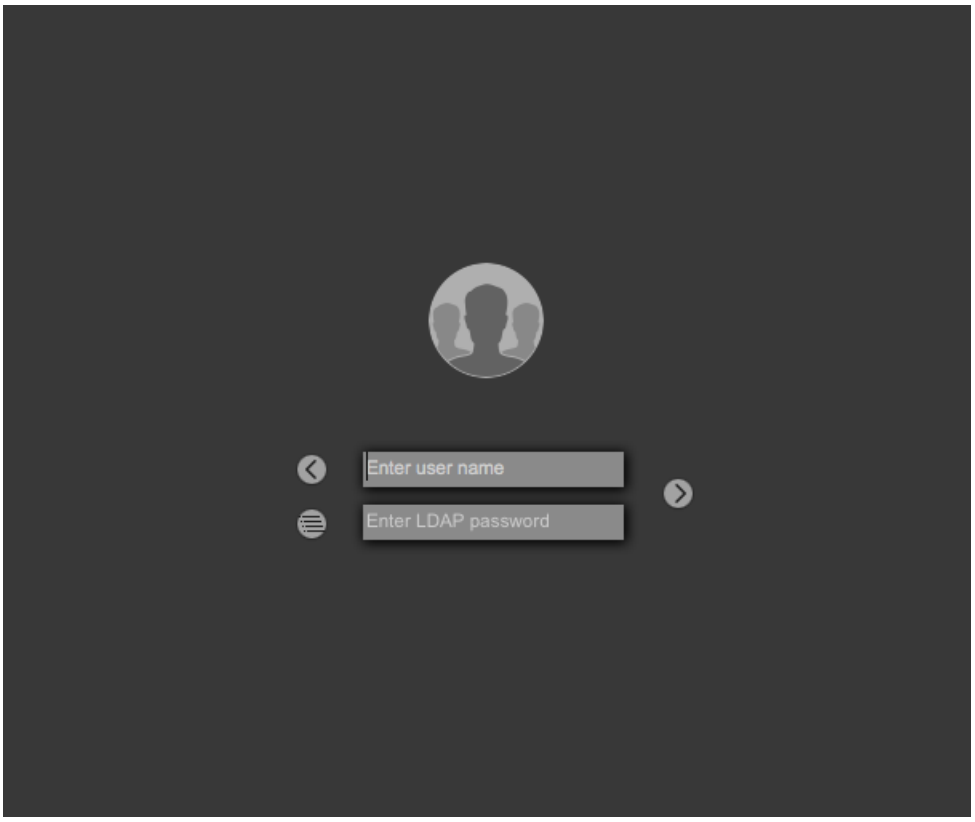
3. Click **>** button.

LDAP Password

To perform authentication by LDAP password follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Enter LDAP password** field and enter password to your corporate account.



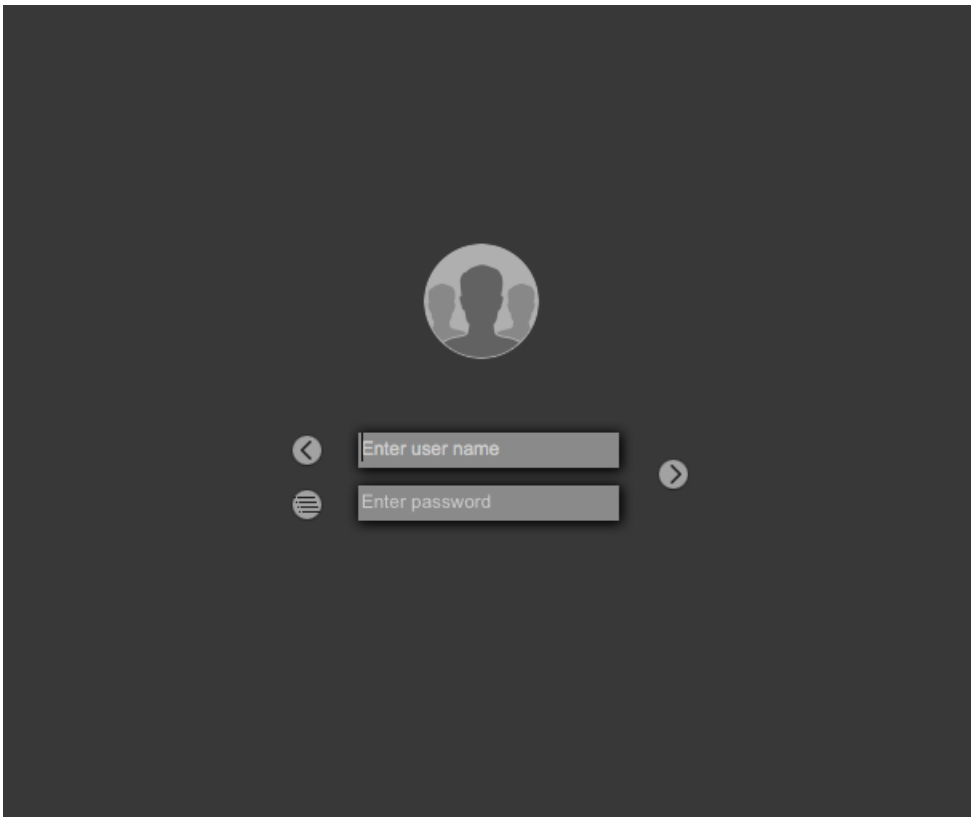
3. Click **>** button.

Password

To perform authentication by Password follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Enter password** field and enter password to your NetIQ Advanced Authentication Frameworkaccount.



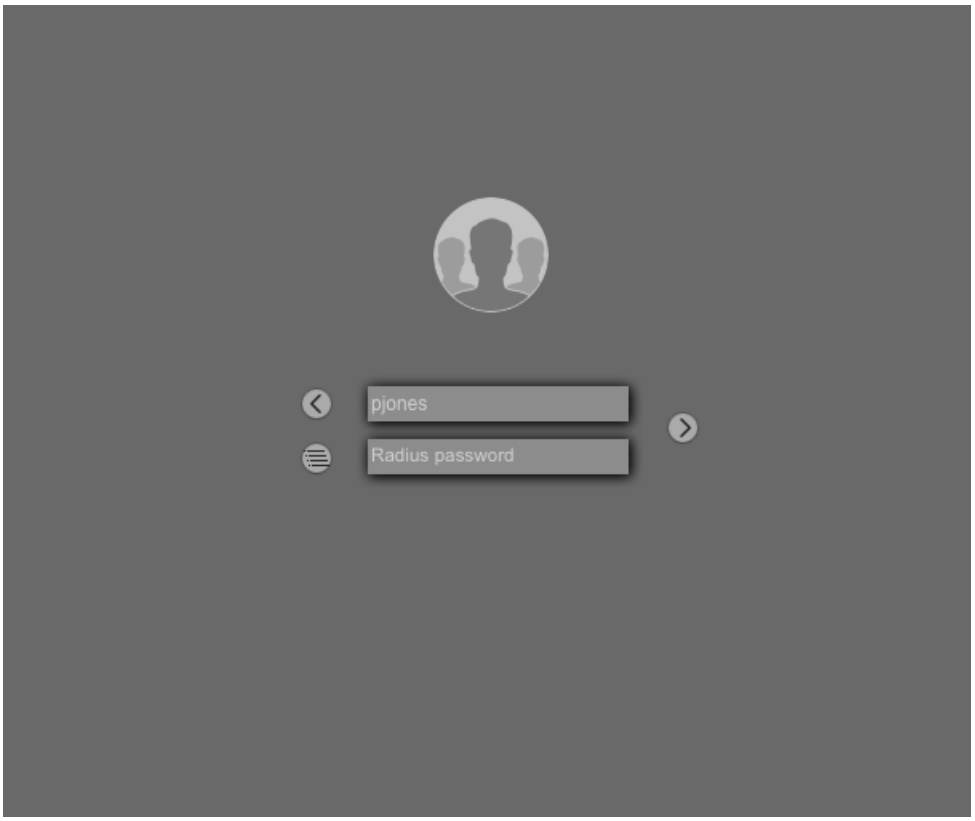
3. Click **>** button.

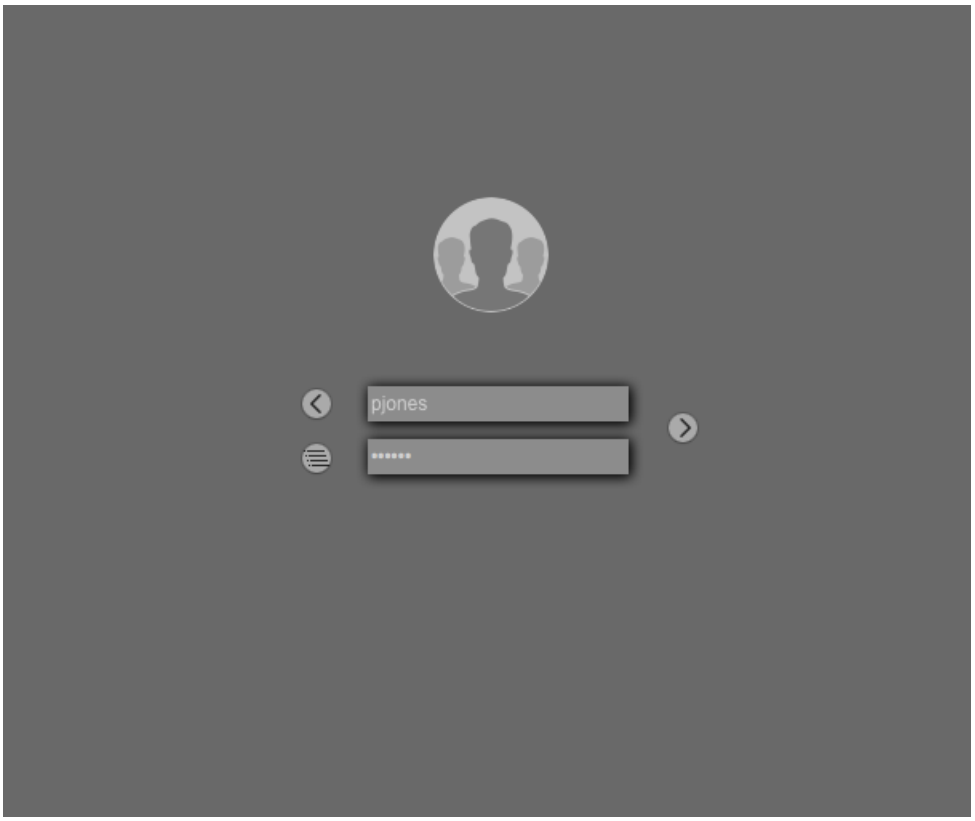
RADIUS

To perform authentication by RADIUS method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Radius password** field and enter your RADIUS password.





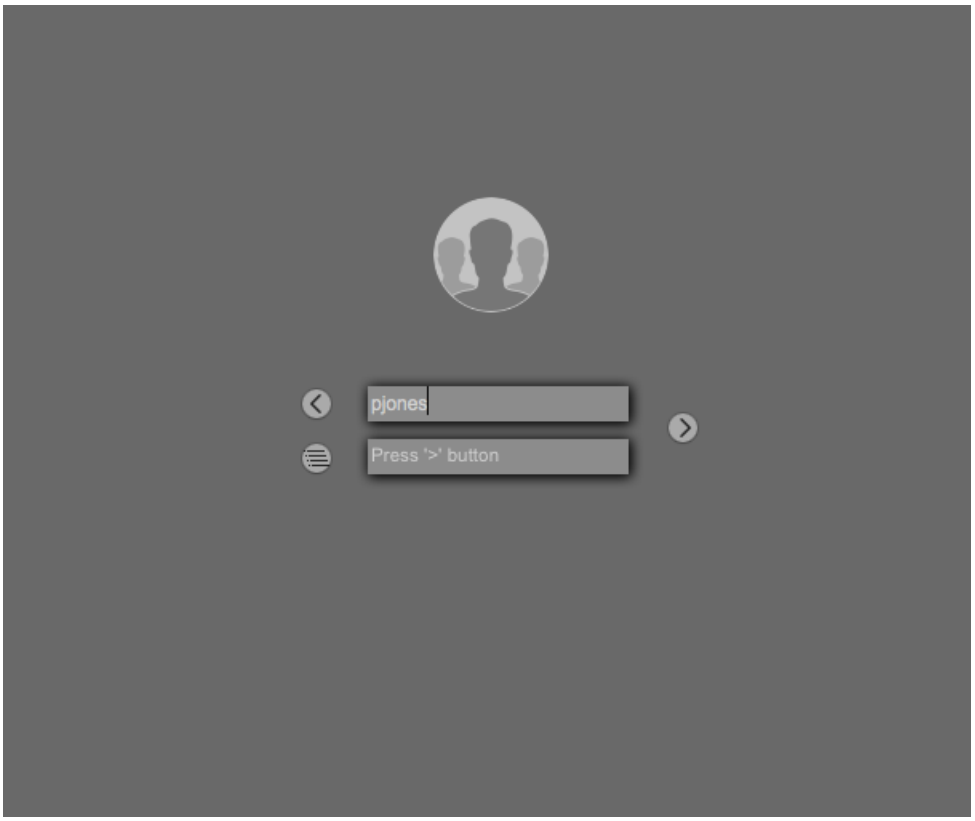
3. Click **>** button.

Security Questions

To perform authentication by Security Questions method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Click **>** button.



3. Set focus to the question field and enter your security answer.

4. Click **>** button.

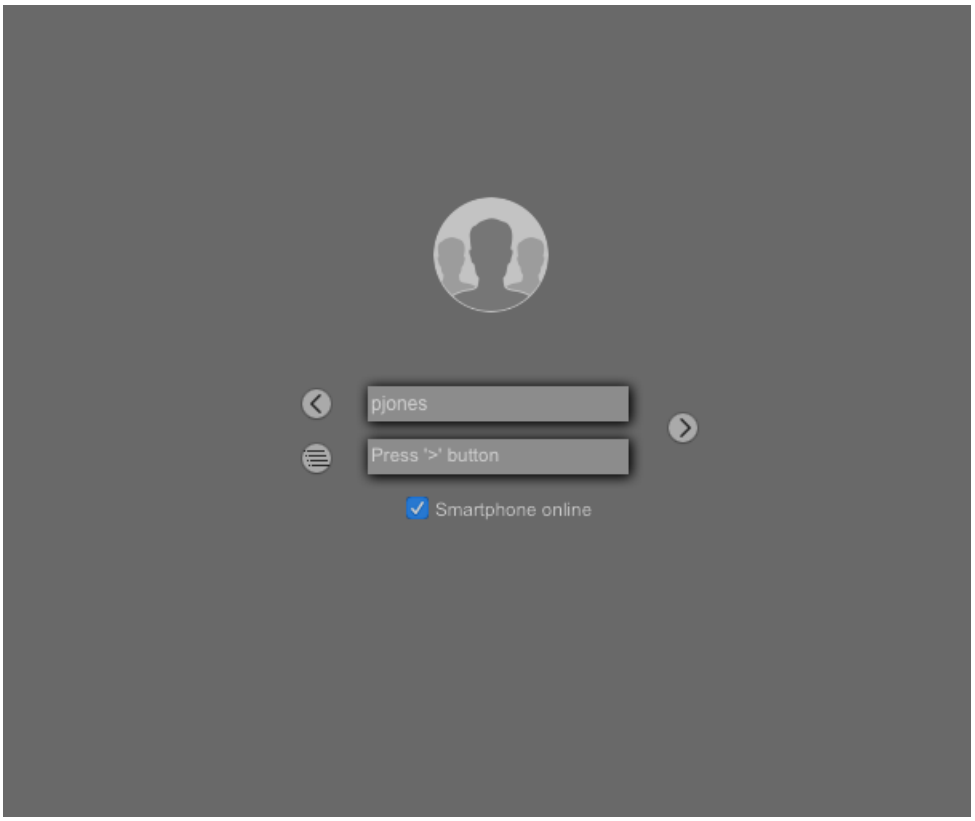
5. Repeat steps 3-4 for all the required security questions.

Smartphone

To perform authentication by Smartphone method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. If your smartphone has an internet connection leave the **Smartphone online** option checked.



2.1. Click **>** button to send an authentication request to your smartphone.

2.2. Open the NetIQ Advanced Authentication smartphone app. You will get an authentication request.

2.3. Tap **Accept**.

3. If your smartphone doesn't have an internet connection uncheck the **Smartphone online** option.

3.1 Open the NetIQ Advanced Authentication smartphone app.

3.2. Tap **Offline authentication** to get a one-time password

3.3. Enter the one-time password in **Enter One-Time Password** field.

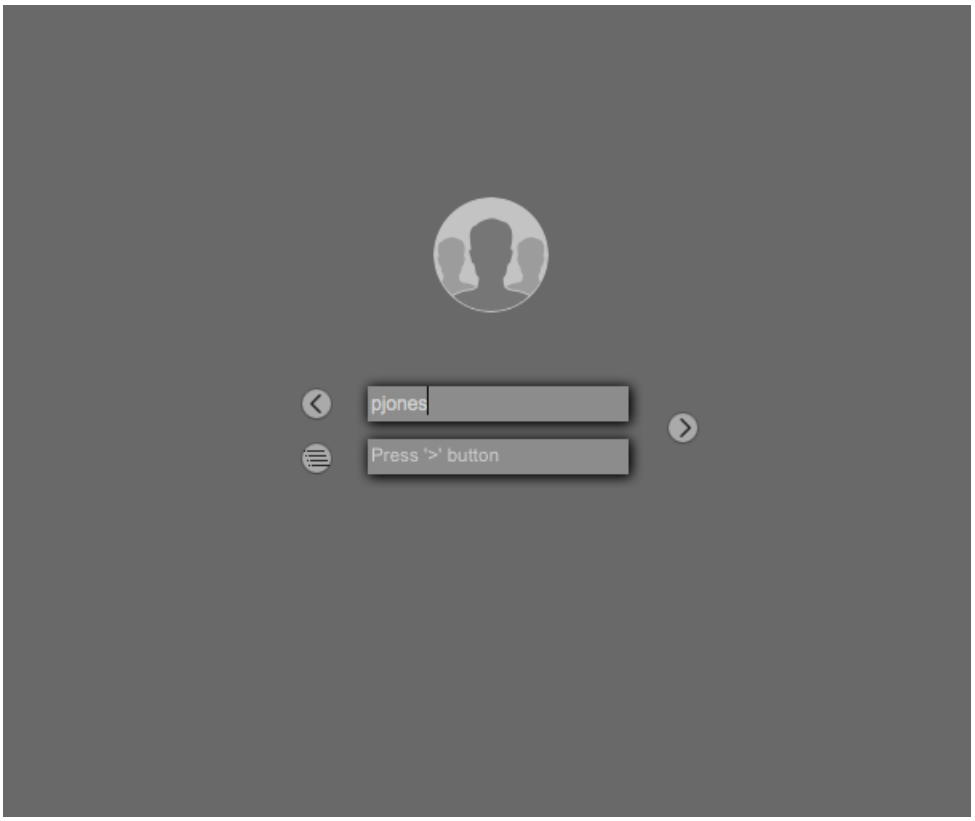
3.4. Click **>** button.

SMS

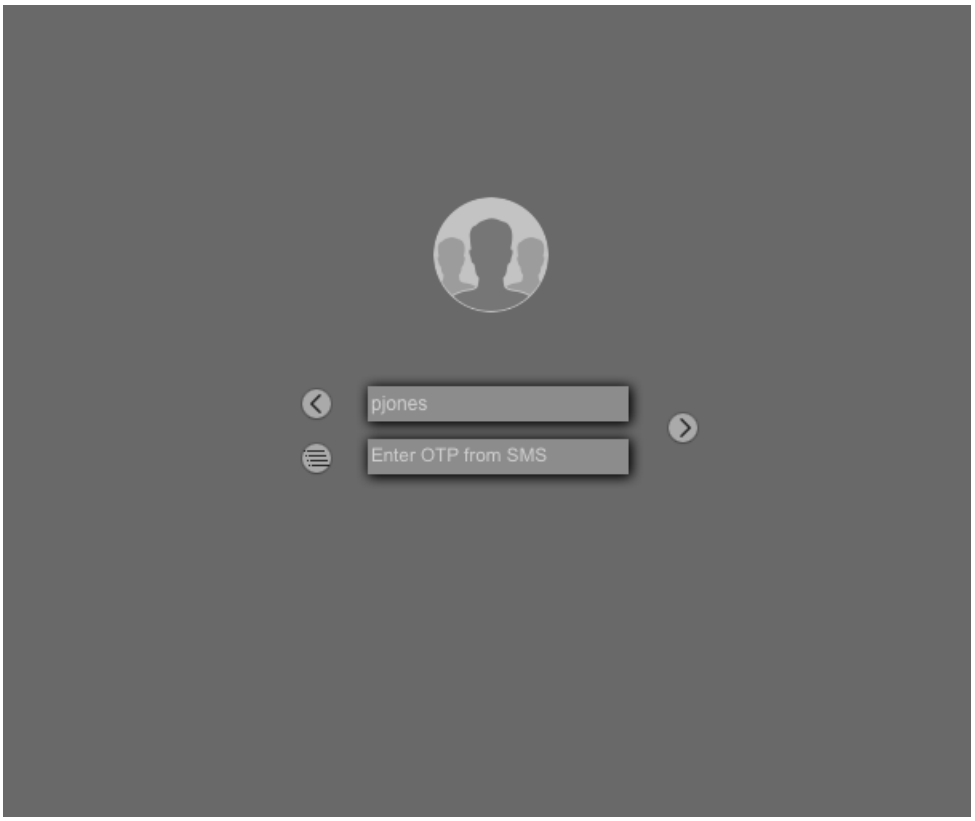
To perform authentication by SMS method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Click ">" button to send you an SMS message.

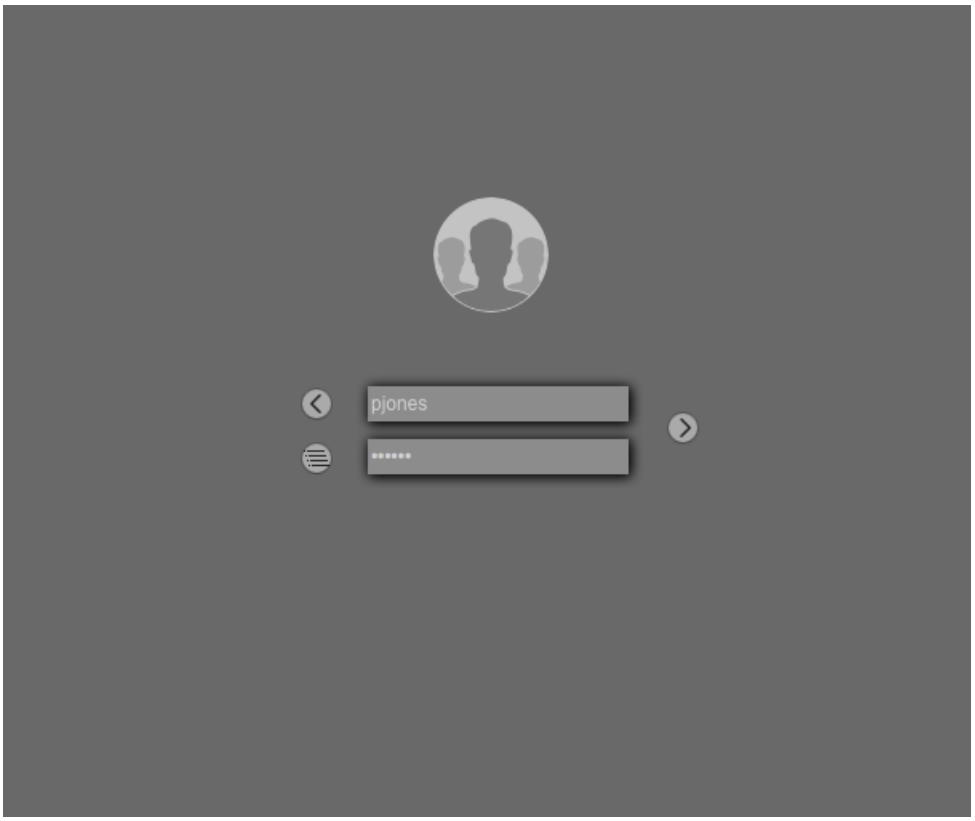


In few seconds the message **Press '>' button** will be changed to **Enter OTP from SMS**.



3. Set focus to the field and check your phone. You should get an SMS message with one-time password.

4. Enter the OTP from SMS to the field.



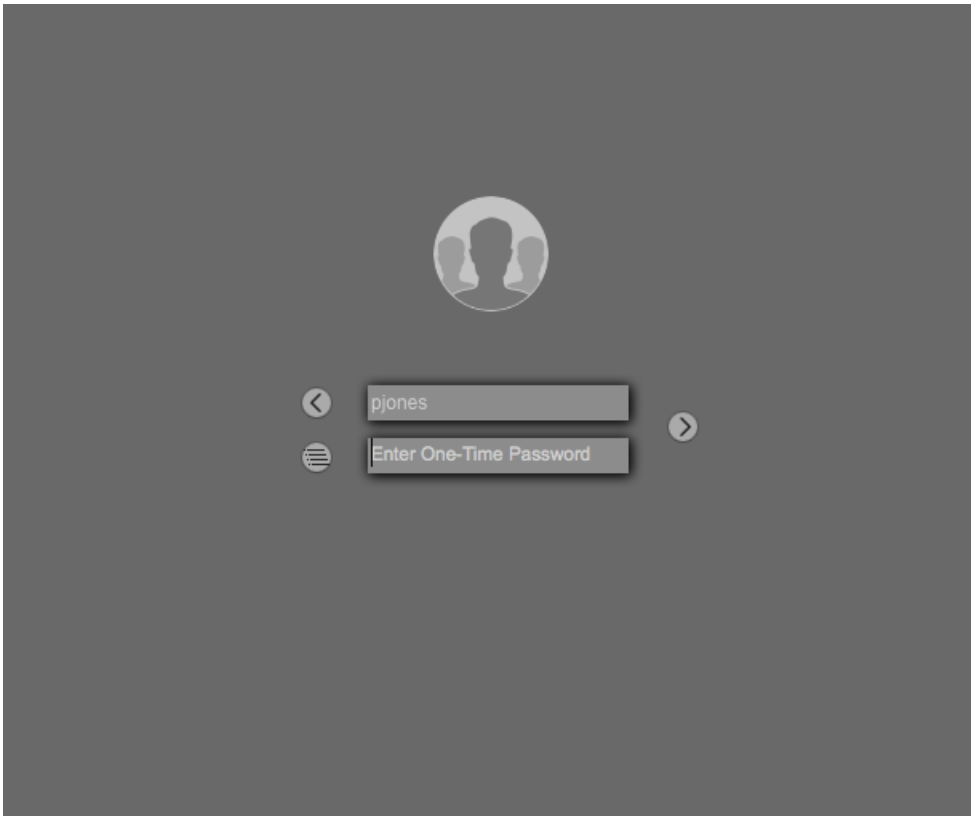
5. Click ">" button.

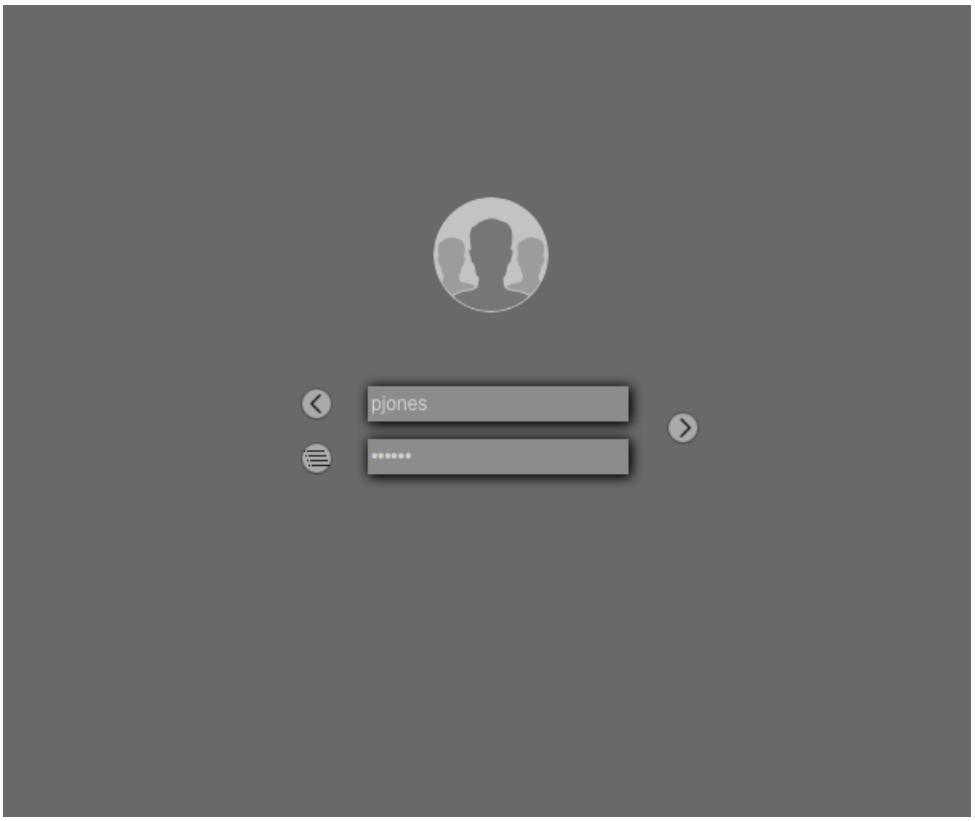
TOTP

To perform authentication by TOTP method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Enter One-Time Password** field and enter TOTP from your hardware or software token.





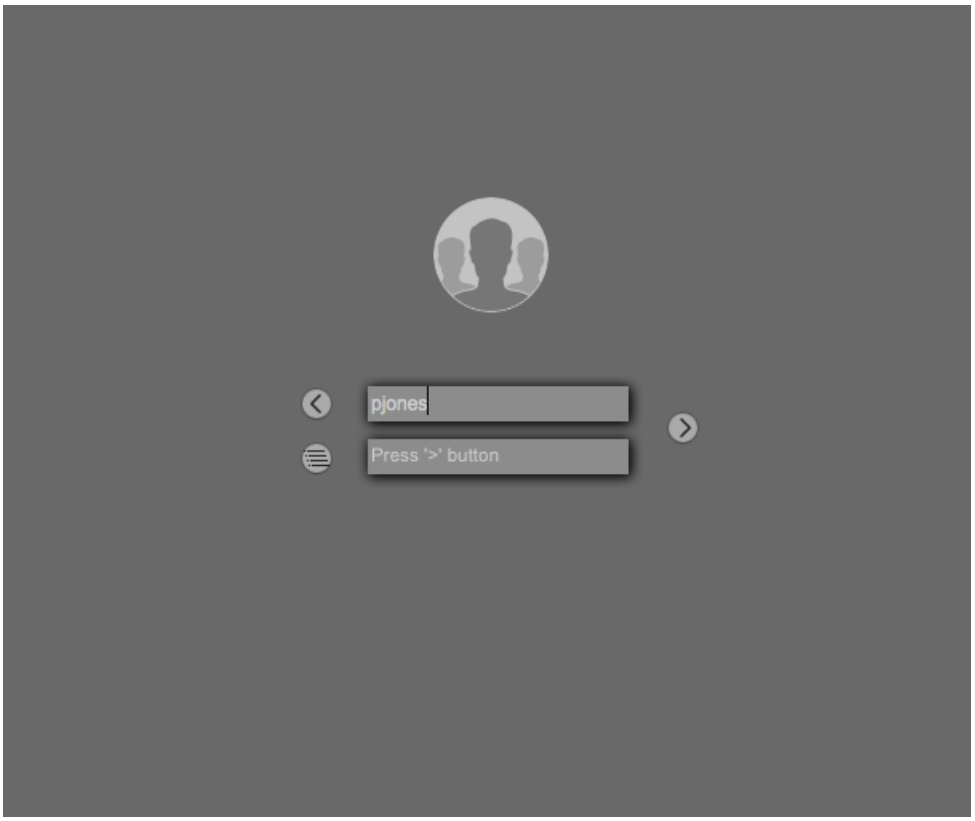
3. Click **>** button.

Voice Call

To perform authentication by Voice Call method follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Click ">" button and wait for a call.



3. Take a call, listen to the answerphone, then enter your PIN code. After it enter hash sign (#).

Log On to Windows

To perform a first log on to Windows using the NetIQ Advanced Authentication Framework on the user selection screen click **Other user**.

You will see the NetIQ Advanced Authentication Framework Other user log in screen. To perform the log on follow the steps below:

1. Click **Sign-in options** to expand a list of available chains.
2. Click a required authentication chain.
3. Enter user name in the **User name** field.
4. Press **Enter** or click **->** button
5. Authenticate using the required authentication method(s).

The following links will help you to get information on how to authenticate using a specific method of assigned authentication chain:

1. Card
2. Email OTP
3. Emergency Password
4. Fingerprint
5. HOTP
6. LDAP Password
7. Password
8. RADIUS
9. Security Questions
10. Smartphone
11. SMS
12. TOTP
13. U2F
14. Voice Call

From the log on screen you can click back arrow button to switch back to the user selection screen.

Card

To perform authentication by Card method follow the steps below:

1. Ensure that the card reader connected to your machine.

2. Tap your card on the reader or insert a smart card to the reader.

The Card method supports 1:N feature. It means that you don't need to enter a user name, it will be detected automatically by Advanced Authentication Framework. It's possible to authenticate when you just bring a card to the reader on a screen where you see the message *Press CTRL+ALT+DEL to log on*.

If you get the error **Wrong smartcard** you are likely trying to use a wrong card. Repeat with another card if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error **Please connect a reader**, ensure that the reader is properly connected. Try to connect it to a different USB slot.

If you get the error **<Your user name> has no authenticator for Smartcard**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

 If you leave a card on the reader during log on, after log on it's possible to lock the operating system automatically when you take off the card from the reader (if it's configured by your system administrator). Then you may put a card to the reader to unlock the operating system.

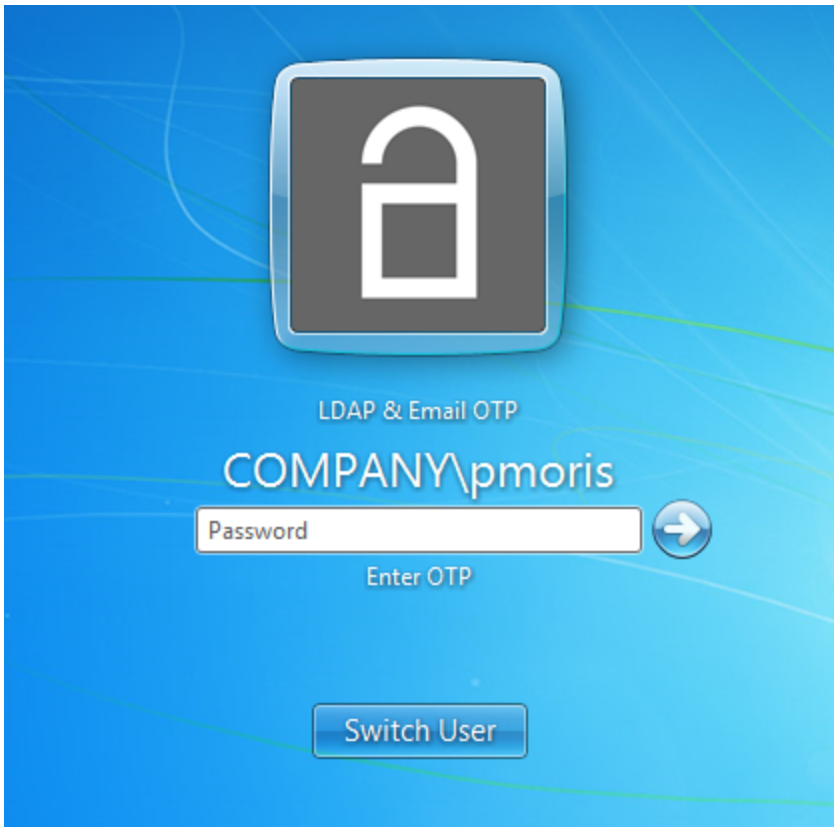
 Tap a card to lock/unlock OS is not supported in 5.2.

Email

To perform authentication by Email method follow the steps below:

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

2. Enter the OTP from Email to the field.



3. Click **>** button.

If you get the error **Wrong answer**, please check if the entered OTP is correct. You may get the error if you try to enter the OTP after some minutes because of the OTP expiration. Retry the attempt.

If you get the error **Can't send OTP. User has not an email**, please ask your system administrator to add your email address to the account properties.

Emergency Password

To perform authentication by Emergency Password follow the steps below:

1. Set focus to the **Password** field and enter your emergency password.

3. Click **Next** button.

If you get the error **Wrong password** you are likely trying to use a wrong emergency password.

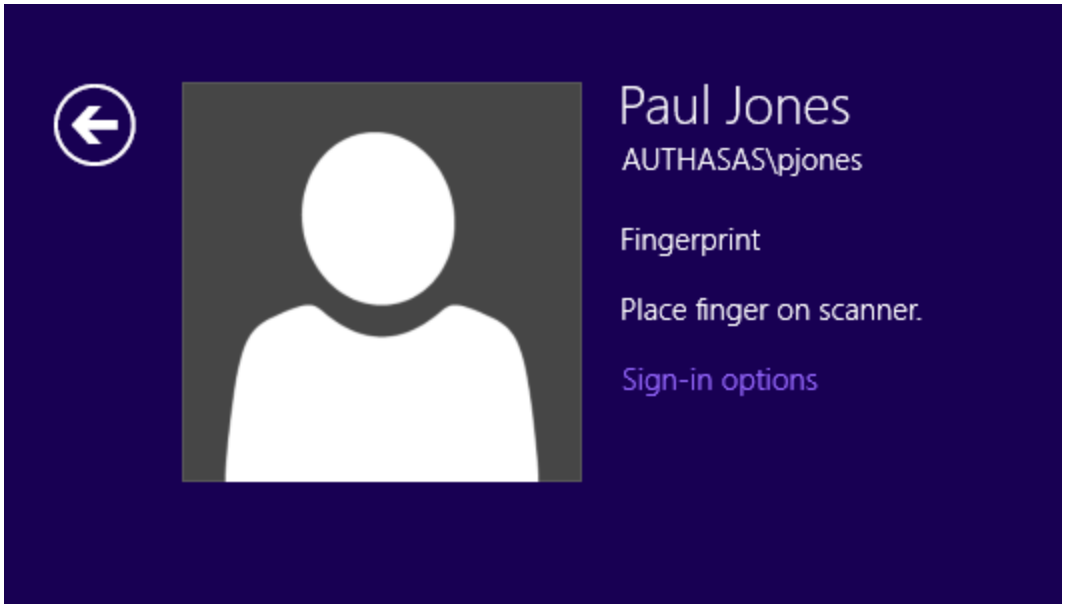
If you get the error **<Your user name> has no authenticator for Emergency Password**, you need to contact your security officer.

Fingerprint

To perform authentication by Fingerprint method follow the steps below:

1. Ensure that a fingerprint reader connected to your machine.

2. Put you finger on the reader in case of touch sensor or swipe your finger in case of swipe sensor.



If you get the error **Please connect a scanner**, ensure that the reader is properly connected. Try to connect it to a different USB slot.

If you get the error **<Your user name> has no authenticator for Fingerprint**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

FIDO U2F

To perform authentication by FIDO U2F method follow the steps below:

1. Ensure that the FIDO U2F token is connected to the workstation.

2. Press the token's button.

If you get the error **Wrong token. Try another one**, you are likely trying to use a wrong token. Repeat with another token if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error **U2F token is not connected**, check that the token is properly connected to the workstation.

If you get the error **<Your user name> has no authenticator for U2F**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

HOTP

To perform authentication by HOTP method follow the steps below:

1. Enter your HOTP manually or if you use a hardware USB token click the token's button.

3. Click **>** button.

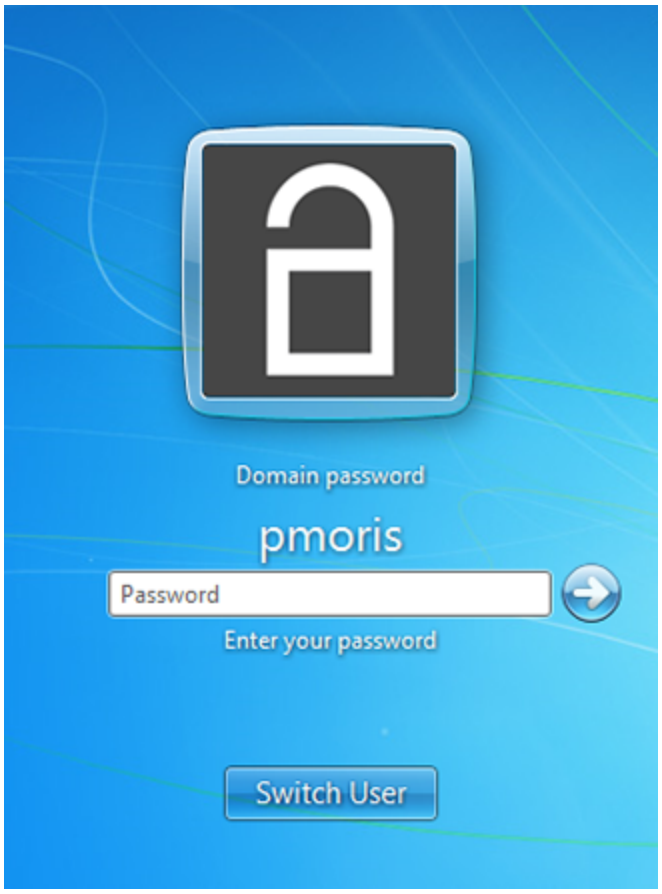
If you get the error **Wrong answer** you are likely trying to use a wrong OTP.

If you get the error **<Your user name> has no authenticator for HOTP**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

LDAP Password

To perform authentication by LDAP password follow the steps below:

1. Enter your domain password.



3. Click **>** button.

If you get the error **Invalid credentials**, you are trying to use a wrong domain password.

Password

To perform authentication by Password follow the steps below:

1. Enter password to your NetIQ Advanced Authentication Frameworkaccount.

3. Click **Next** button.

If you get the error **Wrong password** you are likely trying to use a wrong password.

If you get the error **<Your user name> has no authenticator for Password**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

RADIUS

To perform authentication by RADIUS method follow the steps below:

1. Enter your RADIUS password.

3. Click **>** button.

If you get the error **Wrong answer** you are trying to use a wrong RADIUS password.

Security Questions

To perform authentication by Security Questions method follow the steps below:

1. Enter your answer to the specified security question.

2. Click **>** button.

3. Repeat steps 1-3 for all the required security questions.

If you get the error **Wrong answer** you have entered a wrong answer.

If you get the error **<Your user name> has no authenticator for Security Questions**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Smartphone

To perform authentication by Smartphone method follow the steps below:

1. If your smartphone has an internet connection open the NetIQ Advanced Authenticationsmartphone app and accept the authentication request.

2. If your smartphone doesn't have an internet connection click **->** button.

2.1. Open the NetIQ Advanced Authentication smartphone app.

2.2. Enter the one-time password from the smartphone app.

2.3. Click **>** button.

If you get the error **<Your user name> has no authenticator for smartphone**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

SMS

To perform authentication by SMS method follow the steps below:

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

2. Enter the OTP from SMS to the field.

5. Click ">" button.

If you get the error **Can't send OTP. User has not a mobile phone**, please ask your system administrator to add your mobile phone number to the account properties.

TOTP

To perform authentication by TOTP method follow the steps below:

1. Enter TOTP from your hardware or software token.

3. Click **>** button.

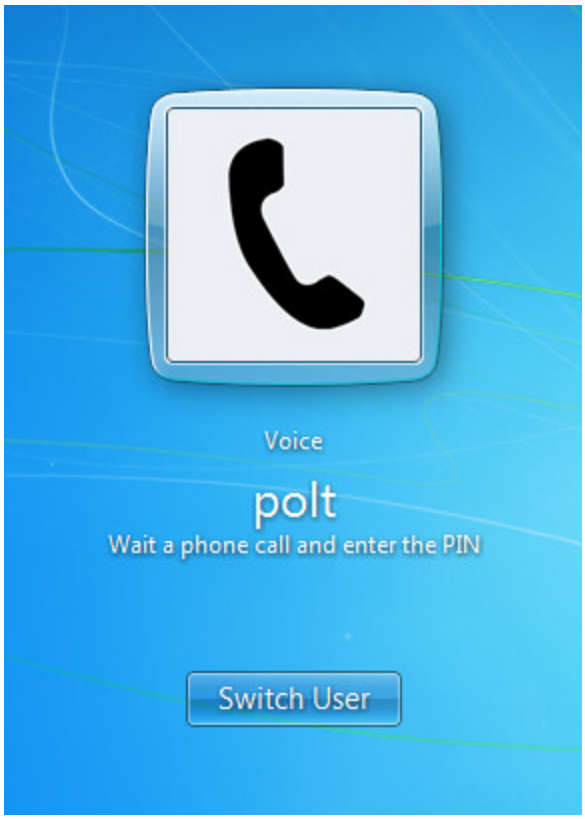
If you get the error **Wrong answer** you are likely trying to use a wrong OTP.

If you get the error **<Your user name> has no authenticator for TOTP**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Voice Call

To perform authentication by Voice Call method follow the steps below:

1. Take a call, listen to the answerphone, then enter your PIN code. After it enter hash sign (#).



Log On to NetIQ Access Manager

To perform a log on to NetIQ Access Manager using the NetIQ Advanced Authentication Framework select an appropriate card (if applicable).

The following links will help you to get information on how to authenticate using a specific method of assigned authentication chain:

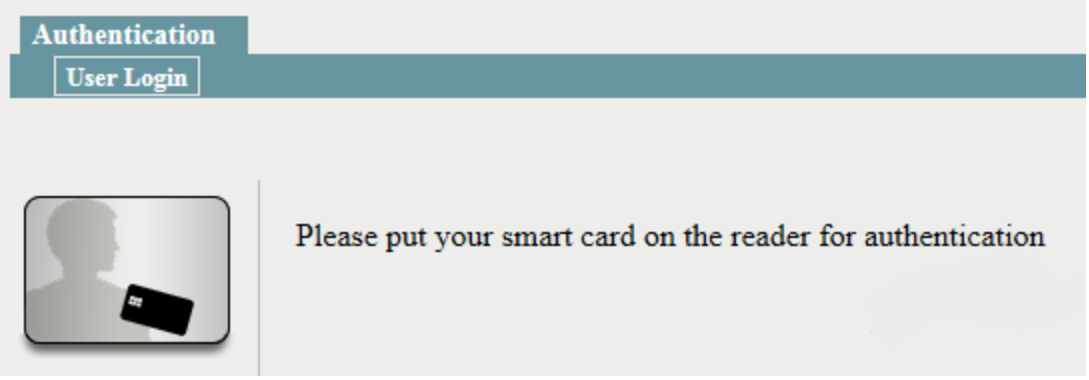
1. Card
2. Email OTP
3. Emergency Password
4. HOTP
5. Password
6. RADIUS
7. Security Questions
8. Smartphone
9. SMS
10. TOTP
11. U2F
12. Voice Call

Card

To perform authentication by Card method follow the steps below:

1. Ensure that the card reader connected to your machine.

2. Tap your card on the reader or insert a smart card to the reader.



If you get the error **Authorization by smartcard failed** you are likely trying to use a wrong card. Repeat with another card if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error **The smartcard reader is not connected, please connect the smartcard reader and try again**, ensure that the reader is properly connected. Try to connect it to a different USB slot, the click **try again**.

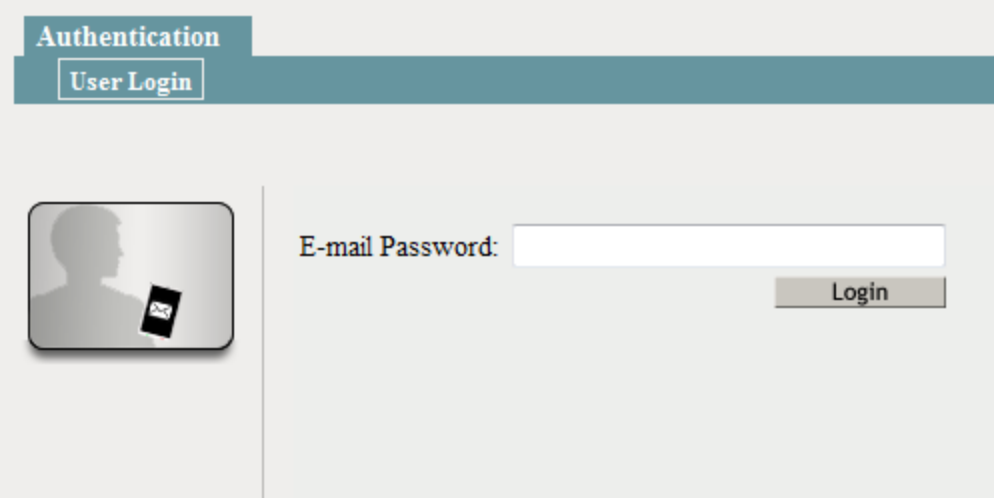
If you get the error **<Your user name> has no authenticator for Smartcard**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Email

To perform authentication by Email method follow the steps below:

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

2. Enter the OTP from Email to the **Email Password** field.



3. Click **Login** button.

If you get the error **This cannot be OTP password**, please check if the entered OTP is correct. You may get the error if you try to enter the OTP after some minutes because of the OTP expiration. Retry the attempt.

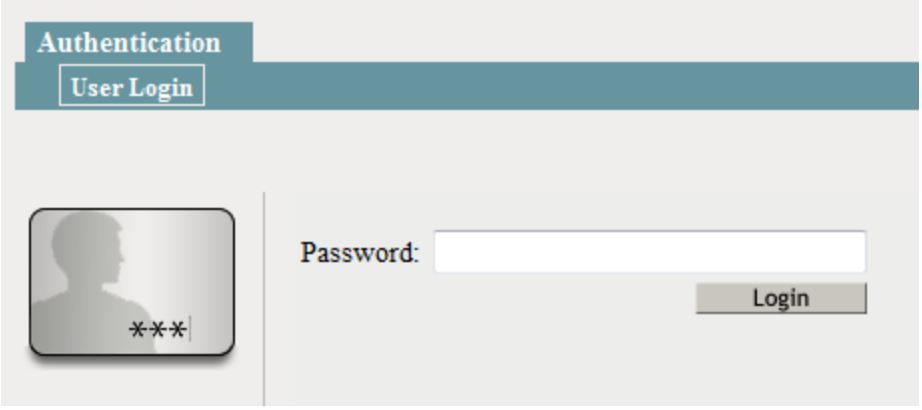
If you get the error **Can't send OTP. User has not an email**, please ask your system administrator to add your email address to the account properties.

Emergency Password

To perform authentication by Emergency Password follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Password** field and enter your emergency password.



3. Click **Login** button.

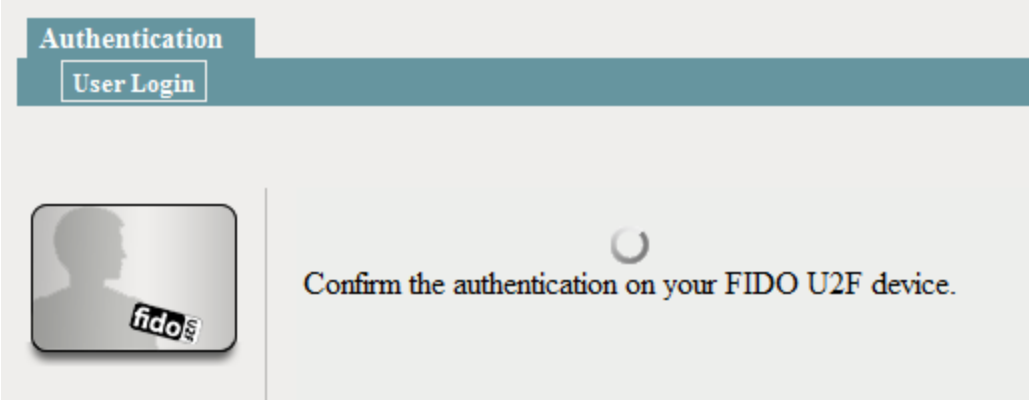
If you get the error **Login failed, please try again** you are likely trying to use a wrong emergency password.

FIDO U2F

To perform authentication by FIDO U2F method follow the steps below:

1. Ensure that the FIDO U2F token is connected to the workstation.

2. Press the token's button.



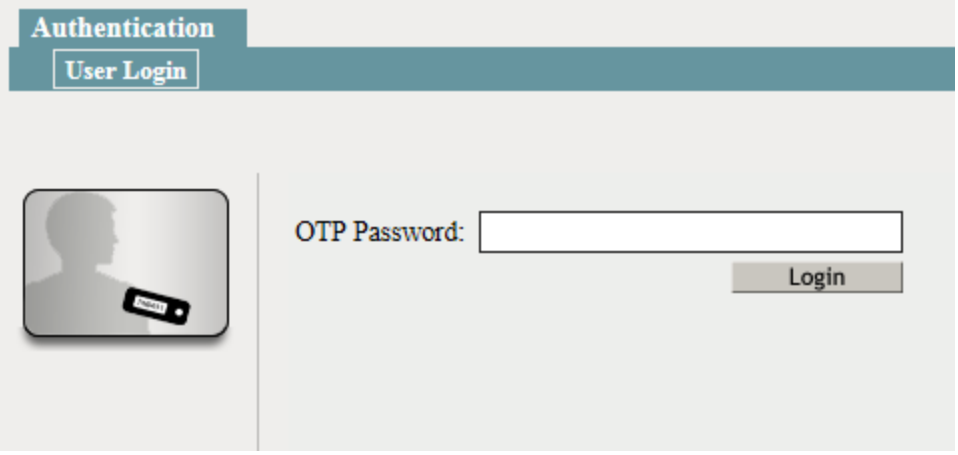
If you get the error **Authorization by Fido U2F failed**, you are likely trying to use a wrong token. Repeat with another token if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error **<Your user name> has no authenticator for U2F**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

HOTP

To perform authentication by HOTP method follow the steps below:

1. Enter your HOTP manually to the **OTP Password** field or if you use a hardware USB token set focus to the field and click the token's button.



3. Click **Login** button.

If you get the error **Authorization by OTP failed. The counter-based password was wrong** you are likely trying to use a wrong OTP.

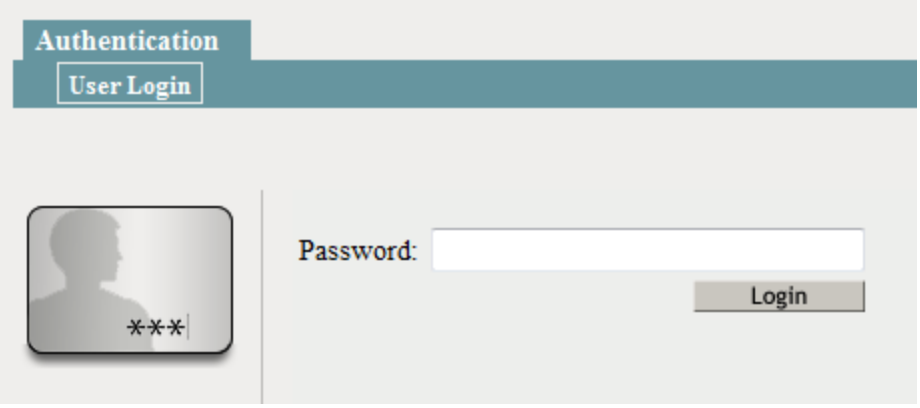
If you get the error **<Your user name> has no authenticator for HOTP**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Password

To perform authentication by Password follow the steps below:

1. Ensure that your user name is entered (if applicable).

2. Set focus to the **Password** field and enter your password.



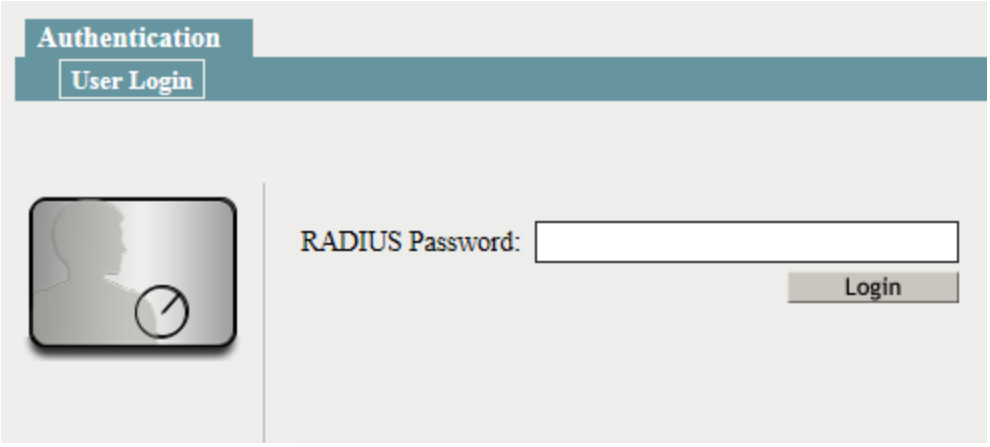
3. Click **Login** button.

If you get the error **Login failed, please try again** you are likely trying to use a wrong password.

RADIUS

To perform authentication by RADIUS method follow the steps below:

1. Enter your RADIUS password.



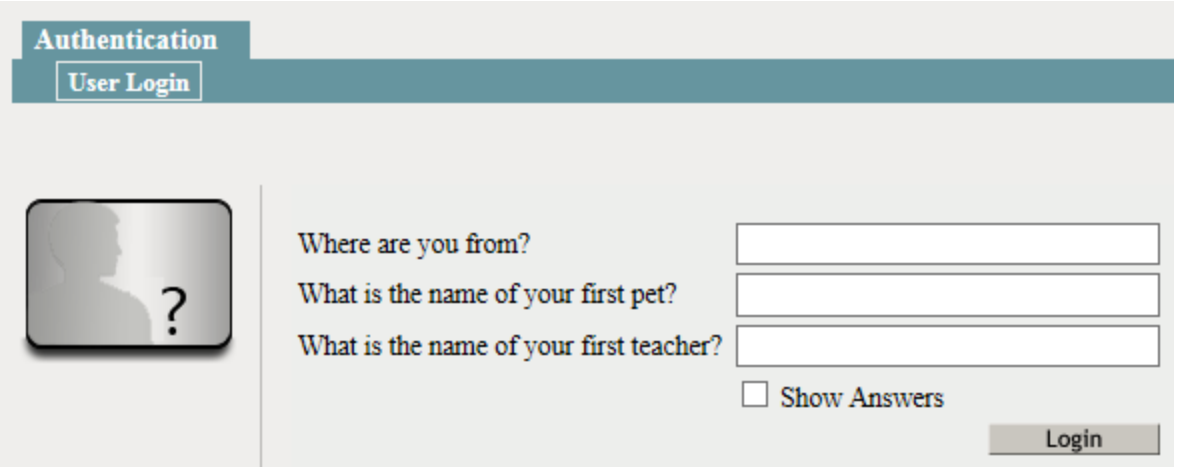
3. Click **Login** button.

If you get the error **Authorization by RADIUS failed** you are trying to use a wrong RADIUS password.

Security Questions

To perform authentication by Security Questions method follow the steps below:

1. Enter your answers to the security question.



2. Click **Login** button.

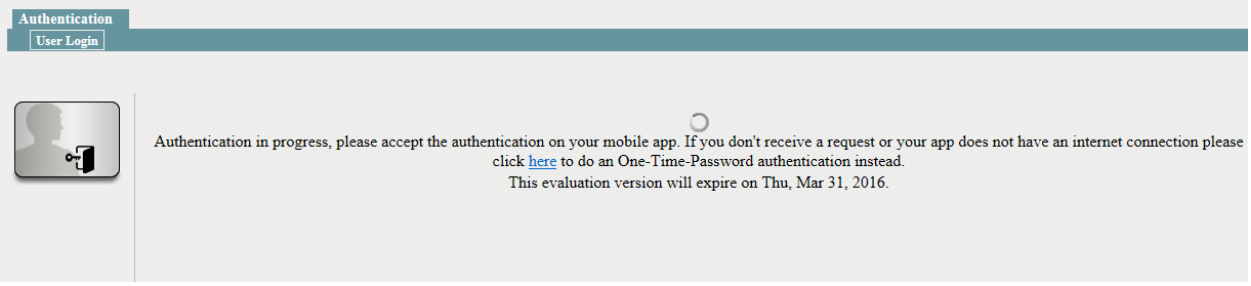
If you get the error **Authorization by Security Question failed. The answers was wrong** you have entered the wrong answers.

If you get the error **<Your user name> has no authenticator for Security Questions**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Smartphone

To perform authentication by Smartphone method follow the steps below:

1. If your smartphone has an internet connection open the NetIQ Advanced Authenticationsmartphone app and accept the authentication request.



2. If your smartphone doesn't have an internet connection click **here** in the text.

2.1. Open the NetIQ Advanced Authentication smartphone app.

2.2. Enter the one-time password from the smartphone app to the **Smartphone OTP** field.

2.3. Click **Login** button.

If you get the error **Authorization by smartphone failed. The password was wrong** you have entered a wrong Smartphone OTP or rejected the authentication or authentication has been rejected by timeout.

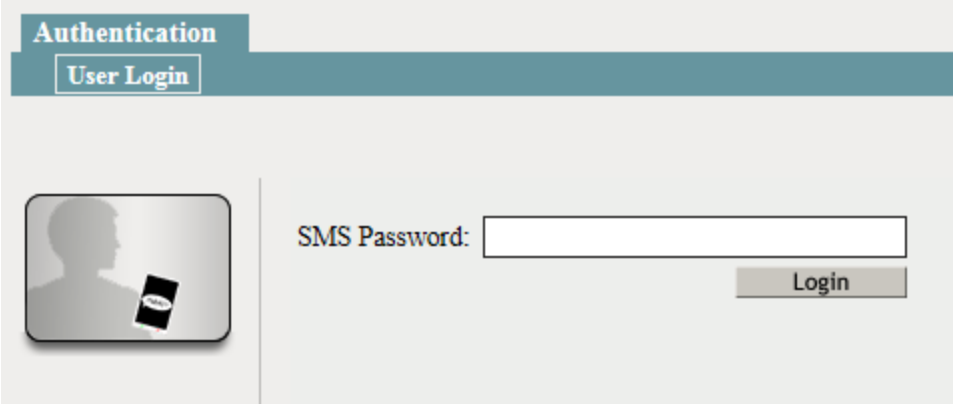
If you get the error **<Your user name> has no authenticator for smartphone**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

SMS

To perform authentication by SMS method follow the steps below:

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

2. Enter the OTP from SMS to the **SMS Password** field.



5. Click "Login" button.

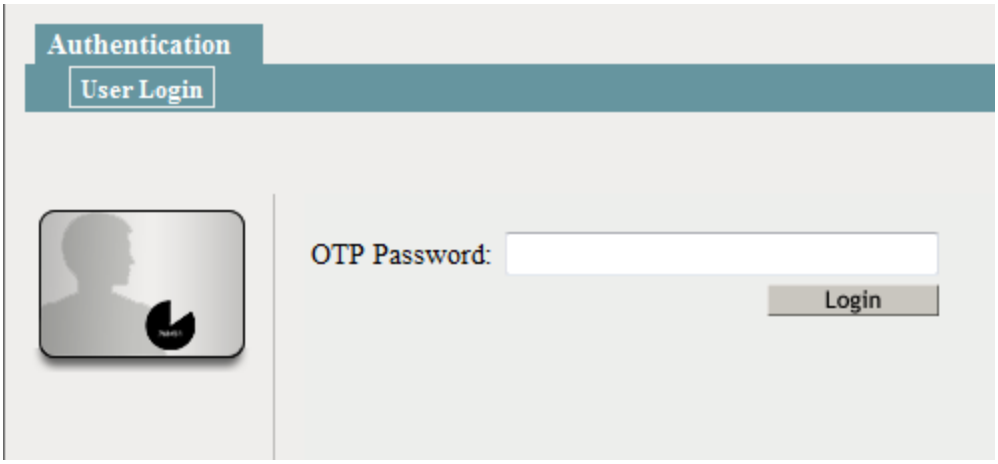
If you get the error **Authorization by sms failed. The password was wrong** you have entered the wrong OTP.

If you get the error **Can't send OTP. User has not a mobile phone**, please ask your system administrator to add your mobile phone number to the account properties.

TOTP

To perform authentication by TOTP method follow the steps below:

1. Enter TOTP from your hardware or software token.



3. Click **Login** button.

If you get the error **Authorization by OTP failed. The time-based password was wrong** you are likely trying to use a wrong OTP.

If you get the error **<Your user name> has no authenticator for TOTP**, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

Voice Call

To perform authentication by Voice Call method follow the steps below:

Take a call, listen to the answerphone, then enter your PIN code. After it enter hash sign (#).

Index