
Helpdesk Administration Guide

Advanced Authentication

Version 6.1

Legal Notice

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

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 Getting Started with the Helpdesk Portal	9
Assigning a Helpdesk Administrator	9
Logging In to the Helpdesk Administration Portal	9
2 Managing the Authenticators	11
BankID	12
Bluetooth	13
Card	13
Email OTP	14
Emergency Password	15
Facial Recognition	15
Fingerprint	16
HOTP	17
LDAP Password	18
Password (PIN)	18
PKI	18
Radius Client	19
Security Questions	20
Smartphone	20
SMS OTP	22
TOTP	22
U2F	24
Voice	25
Swisscom Mobile ID Method	26
Voice OTP	26
3 Unlocking the Locked Users	29
4 Sharing Authenticators	31
5 Searching a Card Holder's Information	33
6 Managing Tokens	35
CSV File Format To Import OATH Compliant Tokens	36
7 Managing Endpoints	37
8 Monitoring User Authentications Activity	39

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

About this Book

This Helpdesk Administrator guide is designed for Helpdesk administrators and describes how to manage and share users' authenticators, search card holder's information, assign tokens to users, and access report of various events.

Intended Audience

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

1 Getting Started with the Helpdesk Portal

A Helpdesk administrator is privileged to manage the Helpdesk portal. The Helpdesk portal provides capabilities to ensure a good customer experience. This includes assisting in re-enrolling the authenticators, assigning tokens wherever required, and assigning specific user roles.

Users can contact the Helpdesk administrator when they face issues with the authenticators. The Helpdesk administrator will either re-enroll the authenticator on the user's behalf or will create a new authenticator.

Example

Bob has enrolled a password authenticator for authentication with Advanced Authentication.

However, Bob has forgotten or lost his password and is unable to log in to any of the applications that require this authentication. Bob then reaches the Helpdesk administrator who logs in to the Helpdesk portal to create an emergency password and gives it to Bob for temporary usage.

Assigning a Helpdesk Administrator

A full administrator can assign a user as an Helpdesk administrator in the **Repositories > Local > Edit > Global Roles > ENROLL ADMINS** of the Administration portal.

For more information, see “[Local Repository](#)” in the [Advanced Authentication - Administration](#) guide.

Logging In to the Helpdesk Administration Portal

To log in to the Advanced Authentication Helpdesk Administration portal, perform the following steps:

1. Open the URL in your browser and you will see the **User name** prompt.
2. Specify your **user name**.
3. If the administrator has configured the **Google reCAPTCHA** option in the server configurations, you will be asked to go through the reCAPTCHA to prove that you are a human and not a robot. A series of images are displayed based on a specific criteria and you must select the appropriate images.
4. Click **Next**.
5. Specify your password and click **Next**. If the provided information is correct you will get access to the Helpdesk Portal.
6. Specify name of the user which you need to manage.
7. If the administrator has configured the **Google reCAPTCHA** option in the server configurations, you will be asked to go through the reCAPTCHA to prove that you are a human and not a robot. A series of images are displayed based on a specific criteria and you must select the appropriate images.
8. Click **Next**.
9. Specify user credentials (if applicable) to get access for user management.
10. You can change the language from the drop-down list on the upper right corner of the Advanced Authentication Helpdesk Administration portal main page.

The supported languages are: Arabic, Canadian French, Chinese Simplified, Chinese Traditional, Danish, Dutch, English, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, Hebrew, and Swedish.

11. Select the authenticators to manage the authenticators of a user.

2 Managing the Authenticators

To use the Advanced Authentication 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 Advanced Authentication Access Manager etc. Some of the authenticators such as **SMS**, **Email**, **Voice OTP**, **LDAP Password**, **Swisscom Mobile ID** and **RADIUS** enroll automatically for default category and other categories added. If user needs to use only one or some of them, he/she can skip the enrollment stage.

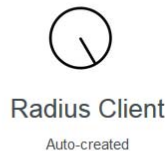
The enrollment can be performed on the Advanced Authentication Helpdesk Portal. Ask your system administrator to provide you the URL.

Dear paul jones,

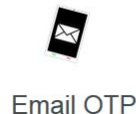
Welcome to the self-service portal for NetIQ Advanced Authentication. This portal allows you to manage your available authentication methods. The **Enrolled authenticators** section displays all of the methods that you have enrolled to use. The **Add authenticator** section displays additional methods available for enrollment.

Selecting an enrolled method allows you to edit or delete the enrollment. Selecting a not enrolled method allows you to enroll in available method and start using it.

Enrolled authenticators



Add authenticator



Methods which enroll automatically:

1. [Email OTP](#)
2. [LDAP Password](#)
3. [Radius Client](#)
4. [SMS OTP](#)
5. [Voice OTP](#)

Not Enrolled methods:

1. [BankID](#)
2. [Bluetooth](#)
3. [Card](#)

4. [Emergency Password](#)
5. [Facial Recognition](#)
6. [Fingerprint](#)
7. [HOTP](#)
8. [Password \(PIN\)](#)
9. [PKI](#)
10. [Security Questions](#)
11. [Smartphone](#)
12. [TOTP](#)
13. [U2F](#)
14. [Voice](#)
15. [Swisscom Mobile ID Method](#)

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

BankID

In BankID method, you are authenticated through your personal identification number. To enroll the BankID authenticator, you must have BankID app either on your computer or mobile device. When you try to authenticate on the endpoint (like laptop or web application) a request is sent to the BankID app, where you specify the security code. Based on the security code, the recorded personal identification number is compared with actual identification number on the BankID app. If the identification numbers match, you will be successfully authenticated.

Prerequisite

Ensure that you have the following:

- ♦ Social Security Number (SSN)
- ♦ BankID app (either desktop or mobile version). For more information, refer [BankID](#).

To enroll a Bank ID, perform the following steps:



1. Click the Bank ID **BankID** icon.
2. Specify the optional comment in **Comment**.
3. Specify the personal identification number in **Personal ID (SSN)**.
4. Click **Save**.

A message Authenticator "BankID" added is displayed.

To test the authenticator, perform the following steps:

1. Click the Bank ID icon in the **Enrolled authenticators** section.
2. Click **Test**.

A message `Start your BankID app` is displayed.

3. Open the BankID app.
4. Specify **Security Code**.
 - a. Click **Identify** on the mobile app.
 - b. Click **Verify my identity** on the desktop app.

If the personal identification number on app matches with the enrolled number, a message `Authenticator "BankID" passed the test` is displayed.

Bluetooth

The Bluetooth authentication method allows to authenticate using your Bluetooth enabled mobile device.

NOTE: To use the **Bluetooth** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see [Advanced Authentication - Device Service guide](#).

To enroll the Bluetooth method perform the following steps:



1. Click the Bluetooth icon.
2. Specify a comment in **Comment** field, if required.
3. Select the required category from the **Category** list, if applicable.
4. Turn on the Bluetooth in your mobile device and also ensure that it is discoverable to other Bluetooth devices.
5. Select your Bluetooth enabled mobile device from the list.

NOTE: If your mobile device is not listed, click **Refresh list** to reload the devices.


6. Click **Save**.

To test the authenticator perform the following steps:

1. Click the Bluetooth icon in the **Enrolled authenticators** section.
2. Click **Test**. A message `Waiting for Bluetooth service` is displayed and then a message is displayed indicating the result of the test.

Card

NOTE: You must install Advanced Authentication Device Service before you enroll a card. Some card readers are supported only for Microsoft Windows. Contact your administrator for more information.

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. Select the required category from the **Category** list.
4. Ensure that your card reader is connected to the machine.
5. Click **Save** button. You will see a message `Waiting for card...`
6. 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.`

TIP: If you see a message `Card Service unavailable` ensure that you have the Advanced Authentication 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. Try to reconnect the reader.

You may get the message `Card reader detected on Mac OS X`. It is related to an improper work of a system service `pcscd`. To fix the issue, run Terminal and run the following commands:

```
kill pcscd
```

```
kill pcscdlite
```

Then reconnect the reader and re-initiate the enrollment.

To test the authenticator follow the next steps:

1. Click the Card icon in the **Enrolled authenticators** 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.

NOTE: If there is no email in the account profile for the user in the repository, then the Email OTP method is not enrolled automatically. However, you can manually enroll the Email OTP method from the **Add authenticators** section, by entering the email address and then clicking **Save**.

To test the enrolled authenticator follow the steps below:

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

2. Ensure that your email address (specified after the text **The email address your One-Time Password is sent to is:**) is valid. Change the email address if it is 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. Select the required category from the **Category** list.
3. Specify **Password** and enter its **Confirmation** in the appropriate fields.
4. Check the **Start date (UTC)** and **End date (UTC)** when the authenticator is valid. You may change the dates if applicable.
5. 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 authenticators** 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.**

Facial Recognition

The Facial Recognition method allows you to get automatically authenticated by presenting your face. The image of the face is captured by a web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you will be successfully authenticated.

To enroll a face, perform the following steps:

- 1 Click the Face  icon.
- 2 Click **Save** to start enrolling the face.
A message **Face Detecting** is displayed.
- 3 Your face will be captured by the camera and enrolled.

NOTE: Facial recognition method works with or without the Device Service installed. If Device Service is not installed, then the browser support is used for capturing the face.

To test the authenticator perform the following steps:

- 1 Click the Face icon in the **Enrolled authenticators** section.
- 2 Click **Test**.
- 3 Place your face in front of the camera.


If your face matches with the enrolled face, the facial authentication is successful.

You may get the following errors for this method:

- ♦ If the integrated camera is not connected properly, an error message `Capture Device cannot be opened` is displayed. Check your camera settings and try again.
- ♦ If there is a mismatch in the faces, an error message `Mismatch` is displayed. You must present your face again for the authentication.
- ♦ If the session has timed out, an error message `Timeout` is displayed. You must present your face again for the authentication.

Fingerprint

TIP: Fingerprint enrollment is supported only on Microsoft Windows. You must install Advanced Authentication Device Service.

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. Select the required category from the **Category** list.
4. Ensure that your fingerprint reader is connected to the machine.
5. Click **Save** button. You will see a message **Put your finger on the reader**.
6. 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**.

IMPORTANT: 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.

TIP: If you see a message `Fingerprint Service unavailable` ensure that you have the Advanced Authentication Smartcard Service installed.

TIP: 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 authenticators** 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:

1. A new token is already assigned to your account and enrollment is not needed.
2. A used token is assigned to your account and the HOTP counter synchronization is required.
3. You get an information about serial number of your token and need to assign it to your account.
4. 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 authenticators** 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 authenticators** 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 authenticators** 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 authenticators** 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 (PIN)

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

To enroll a password (PIN) click the Password (PIN)  icon.

Then follow the steps below:

1. You can specify an optional comment in **Comment** field.
2. Select the required category from the **Category** list.
3. Enter a **Password (PIN)** and its **Confirmation** in the appropriate fields. The password (PIN) must be not less 5 characters (by default, it may be changed by your system administrator).
4. Click **Save** button. You will see a message Authenticator "Password (PIN)" added.

To test the authenticator follow the next steps:


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

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

PKI

NOTE: You must install Advanced Authentication Device Service for the PKI method enrollment.

To enroll a PKI method, perform the following steps:

1. Click the PKI icon .
2. Click **Save** to begin the enrollment.
3. Enter a comment in **Comment**. For example, `black crypto stick`.
4. Select the required category from the **Category** list.
5. A message `Waiting for card...` is displayed. Present your card or plug in your crypto stick to the machine.
6. A message `Use an existing certificate or generate a key pair` is displayed. Select a key from **Key** or leave the **Generate a key pair** option as blank.
7. Enter the PIN code of the device in **PIN**.
8. Click **Save**. The message `Authenticator "PKI" enrolled` is displayed.

NOTE: If an error `Card reader connected` is displayed, ensure that a card is presented on the reader/ crypto stick is connected.

If an error `Enroll failed: Cannot check revocation status for ...` is displayed, then the certificate on your device has no information about where to find the revocation status, or the information is presented but the Certificate Authority is not available to check the revocation status.

If an error `Card service unavailable` is displayed, restart your machine.

If an error `Key not found. Wrong Card?` is displayed, you might have enrolled the PKI authenticator in RDP session. Re-enroll the authenticator in normal session.

The following unexpected error codes (the errors are from a PKCS#11 module) could be displayed:

- ♦ `CKR_DEVICE_ERROR`: The token or USB slot is broken. Try to use a different USB slot.
- ♦ `CKR_DEVICE_MEMORY`: No space left on token or other problems with the token's memory.
- ♦ `CKR_MECHANISM_INVALID`: An invalid mechanism was specified to the cryptographic operation.
- ♦ `CKR_PIN_EXPIRED`: Ensure that the card has been initialized, or you do not use the default PIN and the PIN has not expired.
- ♦ `CKR_PIN_LOCKED`: The user PIN is locked.
- ♦ `CKR_TOKEN_NOT_RECOGNIZED`: The token has not been recognized.
- ♦ `OPERATION FAILED`: Contact your system administrator to analyze the debug logs.

To test the authenticator, perform the following steps:

1. Click the PKI icon in the **Enrolled authenticators** section.
2. Click **Test**. A message `Waiting for card...` is displayed.
3. Present your card or connect your crypto stick to the machine.
4. Enter PIN code of the device in **PIN**. A message `Authenticator "PKI" passed the test` is displayed. If the authenticator is invalid, a message `Wrong card` is displayed.

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 authenticators** 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, Advanced Authentication 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. Select the required category from the **Category** list.
3. Enter answers to the security questions. Each answer must contain not less 1 character (by default, it may be changed by your system administrator).
4. 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 authenticators** 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

TIP: To enroll the Smartphone authenticator it's required to use the Advanced Authentication smartphone app ([Apple iOS app \(https://itunes.apple.com/us/app/netiq-advanced-authentication/id843545585\)](https://itunes.apple.com/us/app/netiq-advanced-authentication/id843545585), [Google Android app \(https://play.google.com/store/apps/details?id=com.netiq.oathtoken\)](https://play.google.com/store/apps/details?id=com.netiq.oathtoken)).




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. Select the required category from the **Category** list.
4. Click **Save** button. You will see a QR code.
5. Move a cursor out of the QR code and open the Advanced Authentication smartphone app.



6. Tap **Offline authentication** button in the app.
7. Tap **+** button to add a new authenticator in the app.
8. Use camera of your smartphone to scan the QR code.
9. You will see a message Authenticator "Smartphone" added.
10. Enter your username and an optional comment in the smartphone app.
11. Save the authenticator on your smartphone.

TIP: 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.

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

1. try to scan the zoomed QR code by making a zoom of the page to 125-150%.
2. 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 authenticators** section.
2. Click **Test** button. You will see a message `Waiting for smartphone data...`

3. Open the 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.

NOTE: If there is no phone number in the account profile for the user in the repository, then the SMS OTP method is not enrolled automatically. However, you can manually enroll the SMS OTP method from the **Add authenticators** section, by entering the phone number and then clicking **Save**.

To test the enrolled authenticator follow the steps below:

1. Click the SMS OTP  icon in the **Enrolled authenticators** section.
2. Ensure that your mobile phone number (specified after the text **The mobile number where an SMS OTP is sent:**) is valid. Change the mobile number if it is 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 and hence for every 30 seconds a new one-time password is generated.

To enroll the TOTP authenticator, follow the recommendations of your system administrator.

TOTP method supports the following types of usage:

- ♦ Advanced Authentication smartphone app (**Apple iOS ap** (<https://itunes.apple.com/us/app/netiq-advanced-authentication/id843545585>), **Google Android app** (<https://play.google.com/store/apps/details?id=com.netiq.oathtoken>)).
- ♦ Google Authenticator app.
- ♦ OATH TOTP compliant hardware token.
- ♦ OATH TOTP compliant software token.

WARNING: The format of the QR codes for Advanced Authentication and Google Authenticator apps are different. Contact your system administrator to know which apps you must use.

To enroll a TOTP authenticator, perform the following steps:

- 1 Click the TOTP  icon.

Then perform the following tasks based on the required preferences:

A. Using Advanced Authentication smartphone app

- 2 Specify a comment in **Comment**. For example, my iPhone.
- 3 Select the required category from **Category**.
- 4 Move the cursor out of the QR code and open the Advanced Authentication smartphone app.
- 5 Tap **Offline authentication** in the app.
- 6 Tap **+** to add a new authenticator in the app.
- 7 Use the camera of your smartphone to scan the QR code.
- 8 Click **Save**.

A message Authenticator "TOTP" added is displayed.

- 9 Specify your username and an optional comment in the smartphone app.
- 10 Save the authenticator on your smartphone.

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

1. Scan the zoomed QR code by zooming the page to 125-150%.
2. Ensure that nothing overlaps the QR code (mouse cursor, text).
3. Try to scan the QR code using the Google Authenticator app.

If you are unable to scan the QR code, contact your system administrator.

B. Using Google Authenticator app

- 1 Specify a comment in **Comment**. For example, my iPhone.
- 2 Select the required category from **Category**.
- 3 Move the cursor out of the QR code and open the Google Authenticator app.
- 4 Tap **BEGIN SETUP** in the app.
- 5 Tap **Scan barcode** to add a new authenticator in the app.
- 6 Use the camera of your smartphone to scan the QR code.
- 7 Click **Save**.

A message Authenticator "TOTP" added is displayed.

TIP: If an error `Invalid barcode` is displayed, then it could be that the QR code is compatible with Advanced Authentication app.

C. Using OATH TOTP compliant hardware token

- 1 Specify a comment in **Comment**. For example, HID token.
- 2 Select the required category from **Category**.

- 3 Specify your token's serial number in **OATH Token Serial**. The token's serial number is displayed on the back of your token.
- 4 Press the token's button and specify the OTP in **OTP**.
- 5 Click **Save**.

A message Authenticator "TOTP" added is displayed.

D. Using OATH TOTP compliant software token

- 1 Specify a comment in **Comment**. For example, A phone app.
- 2 Select the required category from **Category**.
- 3 Specify the **Enter TOTP secret manually**.
- 4 Specify the 40 hexadecimal characters in **Secret**.
- 5 Select the **Google Authenticator format of secret (Base32)** option if you are using the Google Authenticator app.
- 6 Change the value of **Period** value if required (30 seconds by default).
- 7 Click **Save**.

A message Authenticator "TOTP" added is displayed.

To test the enrolled authenticator, perform the following steps:

- 1 Click the TOTP  icon in the **Enrolled authenticators** section.
- 2 Click **Test**.

Then perform the following tasks based on the required preferences:

A. Using Advanced Authentication smartphone app

- 3 Open the NetIQ Auth app.
- 4 Open the **Enrolled Authenticators** section to view Time Based One-Time Password.
- 5 Specify the TOTP in **Password**.
- 6 Click **Next**.

B. Using Google Authenticator app

- 7 Open the Google Authenticator app.
- 8 Specify the One-time password in **Password**.
- 9 Click **Next**.

C. Using Google Authenticator app

- 10 Specify the One-time password shown on your hardware token in **Password**.
- 11 Click **Next**.

D. Using Google Authenticator app

- 12 Specify the One-time password shown on your hardware token in **Password**.
- 13 Click **Next**.

U2F

TIP: You must install Advanced Authentication Device Service for all browsers except Google Chrome. 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. Select the required category from the **Category** list.
4. Ensure that your FIDO U2F token is properly connected to the machine.
5. 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.
6. 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.

TIP: 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 Advanced Authentication FIDO U2F Service installed.

If a message Enroll failed: Device not attested. Ask your administrator to upload your token attestation certificate is displayed, contact your administrator to add your token attestation certificate.

TIP: 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 authenticators** 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

The Voice 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 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. Select the required category from the **Category** list.
4. Specify a **PIN**. By default it must contain at least 3 digits.
5. Click **Save** button. You will see a message Authenticator "Voice" added.

TIP: 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 authenticators** 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`.

WARNING: 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.

Swisscom Mobile ID Method

The Swisscom Mobile ID authentication method uses your mobile phone number from your account attribute. The authenticator sends an authentication request to your mobile phone. You need to accept it.

This authenticator enrolls automatically and it is not possible to remove it.

To test the Swisscom Mobile ID authenticator, click the Swisscom Mobile ID  icon in the **Enrolled authenticators** section and perform the following steps:

1. Click **Test**. A message is displayed indicating that the you must accept the request on the mobile phone.
2. Accept the request. A message `Authenticator "Swisscom Mobile ID" passed the test` is displayed.


Voice OTP

The Voice OTP authenticator initiates a phone call to your mobile number. You will receive the voice OTP in the phone call.

This authenticator enrolls automatically and it is not possible to remove it.

NOTE: If there is no phone number in the account profile for the user in the repository, then the Voice OTP method is not enrolled automatically. However, you can manually enroll the Voice OTP method from the **Add authenticators** section, by entering the phone number and then clicking **Save**.

To test the enrolled authenticator perform the following steps:

1. Click the Voice OTP  icon in the **Enrolled authenticators** section.
2. Click **Test**.

3. Receive the call on your phone and listen to the voice OTP.
4. Enter the One-Time Password in the **Password** field.
5. Click **Next**. A message Authenticator "Voice OTP" passed the test is displayed. If the provided authenticator is invalid you will see a message Wrong answer, try again.

3 Unlocking the Locked Users

You can unlock users of the local repository who are locked because of multiple attempts to login with their passwords.

- 1 Login to the Helpdesk portal.
- 2 If any users are locked in the local repository, the **Locked Users** tab is displayed.
- 3 Click the unlock icon against the user whom you want to unlock.

4 Sharing Authenticators

You can allow users to authenticate to another user's account by using their own authenticators. For example, if the share authenticator option is enabled, the secretary's account can be shared with the account of boss and the secretary will be able to authenticate to the account of boss by using her own authenticators.

The authenticators that can be shared are: TOTP, HOTP, Password, Fingerprint, Card, and FIDO U2F.

To share the authenticators of a user with another user, perform the following steps:

- 1 Login and specify the name of the user to whom you want to share the authenticators to.
- 2 Click the **Linked Authenticators** tab on the screen.
- 3 Specify the user name whose authenticator you want to use. For example, if you want to use secretary's fingerprint to authenticate to the account of boss, specify the name as Secretary-Fingerprint.
- 4 Click **Save**.

Secretary will now be able to authenticate to the account of boss by authenticating with her own fingerprint.

NOTE

- ♦ An administrator can disallow the use of shared authenticator to login to some events.
 - ♦ The boss must have a chain with the LDAP Password method assigned to the Windows logon, Linux logon, or Mac OS logon event. Boss must authenticate at least once to have the LDAP Password cached on the workstation (for Windows, Linux, or Mac OS Clients).
-

How to Use Shared Authenticators

After the authenticator of the secretary is shared with the account of the boss, the secretary must perform the following steps to get authenticated:

1. Secretary specifies the username of boss.
2. Secretary uses her authenticator to authenticate to the account of boss.

5 Searching a Card Holder's Information

With the Search Card portal, you can get a card holder's contact information by tapping the card on the card reader. Information such as name of the card holder, repository information, email address, and mobile number of the user can be obtained.

You must assign chains to the **Search card** event in the **Events** section.

IMPORTANT: To use this feature, you must have the Device Service installed on the computer.

To get the user information from the card, perform the following steps:

1. Log in to the Advanced Authentication Search Card portal (`https://<AdvancedAuthenticationServer>/search-card`).
2. Tap a card on the card reader. The card holder's user name, repository information, email address, and mobile number are displayed.

NOTE: If the card was not enrolled before, a message `No user was found for this card` is displayed.

6 Managing Tokens

With Managing Tokens you can import a file that contains information about multiple tokens and assign the tokens to users.

You must assign chains to the Tokens Management event in the **Events** section to access Tokens Management portal.

To import token files, perform the following steps:

- 1 Log in to the Advanced Authentication Tokens Management portal (<https://<AdvancedAuthenticationServer>/tokens>).
 - 2 Click **Add**.
 - 3 Click **Browse** and add a PSKC or CSV file.
 - 4 Select the **File type**. The options available are:
 - ♦ **OATH compliant PSKC**: This file type must be compliant with OATH. For example, HID OATH TOTP compliant tokens.
 - ♦ **OATH csv**: This file type must contain the format as described in [CSV File Format To Import OATH Compliant Tokens](#). You cannot use the YubiKey CSV files.
 - ♦ **Yubico csv**: In this file type, you must use one of the supported **Log configuration output** (see [YubiKey Personalization Tool > Settings tab > Logging Settings](#)) formats with comma as a delimiter.
 - ♦ Traditional format: In this file type, **OATH Token Identifier** must be enabled.
 - ♦ Yubico format: This file type is supported only for **HOTP Length** set to **6 Digits** and **OATH Token Identifier** set to **All numeric**.
-
- IMPORTANT:** **Moving Factor Seed** must not exceed 100000.
-
- 5 Add the encrypted PSKC files. For this, select **Password** or **Pre-shared key** in **PSKC file encryption type** and provide the information.
 - 6 Click **Upload** to import tokens from the file.

NOTE: Advanced Authentication receives an **OTP format** from the imported tokens file and stores the information in the enrolled authenticator. Therefore, Advanced Authentication Administrator need not change the default value of **OTP format** on the **Method Settings Edit** tab. For more information on the OTP format, see [OATH OTP](#).

When the tokens are imported, you can see the list of tokens. You can use the **Search by token or owner** to search for a preferred token. You can also browse the tokens list to find the required token manually. You must assign these tokens to the users. The token is assigned in the following ways:

- ♦ You can do the following:
 1. Click **Edit** next to the token.

2. Select **Owner**.
 3. Click **Save**.
- ♦ A user can self-enroll a token in the Self-Service portal. Administrator must let the user know an appropriate value from the **Serial** column for the self-enrollment.

CSV File Format To Import OATH Compliant Tokens

A CSV file, which is imported as OATH csv file in the **Administration portal > Methods > OATH OTP > OATH Tokens** tab, must contain fields with the following parameters:

- ♦ Token's serial number
- ♦ Token's seed
- ♦ (Optional) Type of the token: TOTP or HOTP (by default HOTP)
- ♦ (Optional) OTP length (default value is 6 digits)
- ♦ (Optional) Time step (default value is 30 seconds)

Comma is a delimiter.

The following is an example of a CSV file:

```
Token001, 15d2fa517d3c6b791bd4cc2044c241429307001f
Token002, 8c557fc050721037fd31e1d3345b5d3263263e0f, totp, 8
Token003, 658208efea5ac49d5331ba781e66f2c808cccc8e, hotp, 6
Token004, 89f0dfe1c90379da6a11aaca2fc1070f606efe36, totp, 6, 60
```

IMPORTANT: For the YubiKey tokens, you must use the traditional format of the CSV (check **YubiKey Personalization Tool > Settings tab > Logging Settings**) with comma as a delimiter. Use Yubico csv file type (**Advanced Authentication Administration portal > Methods > OATH OTP > OATH Tokens**).

7 Managing Endpoints

Endpoints are devices where the Advanced Authentication server authenticates. An endpoint can be a Windows workstation for Windows Client endpoint, or Advanced Authentication Access Manager appliance for the NAM endpoint and so on.

The endpoints are automatically added when you install a plug-in such as NAM or install Windows Client. The RADIUS endpoint, an OSP endpoint that is used for WebAuth authentication, and Endpoint41 and Endpoint42 are the predefined endpoints.

NOTE: Endpoint41 and Endpoint42 are created for the integration with legacy NAM and NCA plug-ins, which are used in NAM 4.2 and earlier versions with Advanced Authentication 5.1.

The NAM and NCA plug-ins work with the hard coded endpoint ID and secret. In Advanced Authentication 5.2 and later, you must register the endpoints. This breaks the backward compatibility with old plug-ins. These two legacy endpoints allow to keep the old plug-ins working.

To configure an endpoint for Advanced Authentication, perform the following steps:

- 1 In the **Endpoints** section, click **Edit** against the endpoint you want to edit.
- 2 You can rename the endpoint, change its description or endpoint type.
- 3 Set **Is enabled** to **ON** to enable the endpoint.
- 4 Set **Is trusted** to **ON** if the endpoint is trusted. In some integrations such as Migration Tool, Password Filter, NAM, and NCA you must enable the **Is trusted** option for their endpoints.
- 5 Specify an **Endpoint Owner** if you have configured a specific chain to be used by the Endpoint owner only. This is a user account that must be able to use a different **chain** than the other users for authentication.

The Endpoint Owner feature is supported for Windows Client, Mac OS Client, and Linux PAM Client only.

NOTE: Additional information such as **Operating System**, **Software** version, **Last session** time and **Device** information are displayed. Also in **Advanced properties**, RAM information is displayed.

Advanced Authentication Windows Client 5.6 or newer, Advanced Authentication Linux PAM Client 6.0 or newer, Advanced Authentication Mac OS X Client 6.0 or newer must be installed on the endpoint.

- 6 Click **Save**.

You can create an endpoint manually. This endpoint can be used for the third-party applications that do not create endpoints.

To create an endpoint manually, perform the following steps:

- 1 In the **Endpoints** section, click **Add**.
- 2 On the **Add endpoint** page, specify a **Name** of the endpoint and its **Description**.
- 3 Set the **Type** to **Other**.
- 4 Set **Is enabled** to **ON**.

- 5 Set **Is trusted** to **ON** if the endpoint is trusted.
- 6 Leave **Endpoint Owner** blank.
- 7 Click **Save**. The **New Endpoint secret** window is displayed.
- 8 Take down the values specified in **Endpoint ID** and **Endpoint Secret** and place them in a secure place in your application.

NOTE: You will not be able to get the **Endpoint ID** and **Endpoint Secret** later on the appliance.

- 9 Click **OK**.

NOTE: **Tenancy settings** are not supported for Endpoints.

IMPORTANT: You must ensure not to remove an endpoint that has at least one component running on it such as Windows Client, Logon Filter, RD Gateway plug-in, or ADFS plug-in. Endpoint is removed automatically when you uninstall Windows Client. However you must remove the endpoint manually when you uninstall Logon Filter, RD Gateway plug-in or ADFS plug-in.

If you remove an endpoint accidentally, ensure to remove the records with prefix **endpoint*** from the `%ProgramData%\NetIQ\Windows Client\config.properties` file and re-start the machine. This recreates the endpoint.

8

Monitoring User Authentications Activity

You can monitor the authentication activity of a preferred user from the repository in the User report. This includes both the successful and failed authentication details of the various events of Advanced Authentication. This report enables you to examine how often a user logged in, different events to which a user has logged in and authenticators used for login.

To monitor the authentication logs of a user, perform the following steps:

- 1 Specify the preferred user name to monitor the authentication report in the Helpdesk portal and click **Next**.
- 2 Click the **User report** tab.

The **User report** includes the following information about each authentication activity of the user:

- ♦ **Time**: The time when the user initiated the login.
- ♦ **Tenant**: Name of the tenant to which the user is associated.
- ♦ **Server**: IP address of the Advanced Authentication server that processed the authentication.
- ♦ **User name**: Name of the user.
- ♦ **Event name**: Name of the event to which the user tried to log in.
- ♦ **Chain name**: Name of the chain used for authentication.
- ♦ **Method name**: Name of the method used for authentication.
- ♦ **Result**: Authentication result. A check mark indicates successful authentication and a cross mark indicates failed authentication.
- ♦ **Reason**: A comment about the cause of failed authentication. The **Reason** is empty for a particular login activity if the authentication is successful.

