
Advanced Authentication 6.2

Helpdesk Administration Guide

February 2019

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 © 2019 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 Overview	9
2 Logging in to the Helpdesk Administration Portal	11
3 Managing the Authenticators of Users	13
Bluetooth	14
Enrolling the Bluetooth Authenticator	14
Testing the Bluetooth Authenticator	14
Card	15
Enrolling the Card Authenticator	15
Testing the Card Authenticator	15
Email OTP	16
Enrolling the Email OTP Authenticator	16
Testing the Email OTP Authenticator	16
Emergency Password	17
Enrolling the Emergency Password	17
Testing the Emergency Password Authenticator	17
Facial Recognition	17
Enrolling the Face Authenticator	17
Testing the Face Authenticator	18
FIDO 2.0	18
Enrolling the FIDO 2.0 Authenticator	19
Testing the FIDO 2.0 Authenticator	19
FIDO U2F	19
Enrolling the FIDO U2F Authenticator	19
Testing the FIDO U2F Authenticator	20
Fingerprint	21
Duress Finger	21
Enrolling the Fingerprint Authenticator Using Single Finger Reader	21
Enrolling the Fingerprint Authenticator Using Multi-Finger Reader	22
Assigning a Finger as Duress	22
Testing the Fingerprint Authenticator	23
HOTP	23
Enrolling the HOTP Authenticator	23
Testing the HOTP Authenticator	25
LDAP Password	25
Enrolling the LDAP Password Authenticator	25
Testing the LDAP Password Authenticator	25
Password	26
Enrolling the Password Authenticator	26
Testing the Password Authenticator	26
PKI	26
Enrolling the PKI Authenticator Using PKI Device	27
Enrolling the PKI Authenticator Using Virtual Smartcard	27
Testing the PKI Authenticator	28
RADIUS Client	29

Enrolling the RADIUS Client Authenticator	29
Testing the RADIUS Client Authenticator	29
Security Questions	30
Enrolling the Security Questions Authenticator	30
Testing the Security Questions Authenticator	30
Smartphone	30
Enrolling the Smartphone Authenticator	31
Testing the Smartphone Authenticator	32
SMS OTP	32
Enrolling the SMS OTP Authenticator	33
Testing the SMS OTP Authenticator	33
Swedish BankID	34
Enrolling the Swedish BankID Authenticator	34
Testing the Swedish BankID Authenticator	34
Swisscom Mobile ID	35
Testing the Swisscom Mobile ID Authenticator	35
TOTP	35
Enrolling the TOTP Authenticator	35
Testing the TOTP Authenticator	38
Voice	38
Enrolling the Voice Authenticator	38
Testing the Voice Authenticator	39
Voice OTP	39
Enrolling the Voice OTP Authenticator	39
Testing the Voice OTP Authenticator	39
Web Authentication Method	40
Enrolling the Web Authentication Authenticator	40
Testing the Web Authentication Authenticator	40
Windows Hello	40
Configuring the System Settings for Windows Hello	41
Enrolling the Windows Hello Authenticator	42
Testing the Windows Hello Authenticator	42
4 Sharing Authenticators	43
5 Unlocking Users	45
6 Searching a Card Holder's Information	47
7 Managing Tokens	49
Importing the Token Files	49
Assigning the Tokens to Users	50
CSV File Format to Import the OATH Compliant Tokens	50
8 Managing Endpoints	51
Configuring an Endpoint	51
Creating an Endpoint Manually	52
9 Monitoring a User's Authentication Activity	53

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 reports of various events.

Intended Audience

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

1 Overview

A Helpdesk administrator manages and shares users' authenticators, searches for a card holder's information, assigns tokens to users, and accesses the authentication reports of various events.

The following sections describe the tasks that a helpdesk administrator can perform:

- ◆ [Manage authenticators](#)
- ◆ [Share authenticators](#)
- ◆ [Unlock users](#)
- ◆ [Search for a card holder's information](#)
- ◆ [Manage tokens](#)
- ◆ [Manage endpoints](#)
- ◆ [Monitor a user's authentication activity](#)

2 Logging in to the Helpdesk Administration Portal

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

- 1 Launch the URL `https://<Advanced Authentication Server_ip>/helpdesk` on your browser.
- 2 Specify your **user name**.
- 3 If the administrator has configured the **Google reCAPTCHA** option in the server configuration, you are prompted 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**.
- 6 Specify name of the user that you are managing.
- 7 Click **Next**.
- 8 Specify the credentials of the user (if applicable).
- 9 Select one of the available methods to manage.

You can change the language from the drop-down list on the upper right corner of the Advanced Authentication Helpdesk Administration portal.

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.

3 Managing the Authenticators of Users

An authenticator is a set of encrypted data that contains your authentication information. You can use authenticators to log in to different operating systems such as Linux, Mac OS, and Windows. You can also use these authenticators to log in to VPN and web portals such as Citrix NetScaler, Office 365, Salesforce, and so on. Some of the authenticators such as **SMS**, **Email**, **Voice OTP**, **Swisscom Mobile ID**, **LDAP Password**, and **RADIUS** are enrolled automatically.

You can enroll the authenticators on behalf of the users who require assistance with authentication. After you log in with your credentials the **User to manage** screen is displayed. You must specify the credentials of the user whose authenticators you want to enroll.

For example, Smith is assigned as a Helpdesk administrator. John is an employee who has enrolled authenticators, such as **Card** and **PIN**. John forgets to get his card to the office. John approaches Smith because John is unable to authenticate. Smith logs in to the helpdesk portal, and then on the **User to manage** screen, Smith specifies the username and password of John. This allows Smith to enroll the Card method and authenticate John.

You can enroll the following authenticators on behalf of the users:

- ◆ [“Bluetooth” on page 14](#)
- ◆ [“Card” on page 15](#)
- ◆ [“Email OTP” on page 16](#)
- ◆ [“Emergency Password” on page 17](#)
- ◆ [“Facial Recognition” on page 17](#)
- ◆ [“FIDO 2.0” on page 18](#)
- ◆ [“FIDO U2F” on page 19](#)
- ◆ [“Fingerprint” on page 21](#)
- ◆ [“HOTP” on page 23](#)
- ◆ [“LDAP Password” on page 25](#)
- ◆ [“Password” on page 26](#)
- ◆ [“PKI” on page 26](#)
- ◆ [“RADIUS Client” on page 29](#)
- ◆ [“Security Questions” on page 30](#)
- ◆ [“Smartphone” on page 30](#)
- ◆ [“SMS OTP” on page 32](#)
- ◆ [“Swedish BankID” on page 34](#)
- ◆ [“Swisscom Mobile ID” on page 35](#)
- ◆ [“TOTP” on page 35](#)
- ◆ [“Voice” on page 38](#)
- ◆ [“Voice OTP” on page 39](#)
- ◆ [“Web Authentication Method” on page 40](#)
- ◆ [“Windows Hello” on page 40](#)


Bluetooth

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susane can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

NOTE: To use this method, you must install the Advanced Authentication Device Service. For more information about Device Service, see [Advanced Authentication - Device Service](#) guide.

Enrolling the Bluetooth Authenticator

- 1 Click the Bluetooth  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to the Bluetooth authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Turn on the Bluetooth in your device and ensure that it is discoverable to the other Bluetooth devices.
- 5 Select your Bluetooth enabled device from the list in the **Add Bluetooth authenticator** page.

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

- 6 Click **Save**.

A message Authenticator "Bluetooth" has been added is displayed.

Testing the Bluetooth Authenticator

NOTE: During authentication, ensure that your mobile device is discoverable.

- 1 Click the Bluetooth icon in **Enrolled Authenticators**.
- 2 Click **Test**.

A message `Waiting for the Bluetooth service is displayed`. If the enrolled Bluetooth device is within the range, a message `Authenticator "Bluetooth" passed the test` is displayed.

If the Advanced Authentication Device Service is not installed on the system where you want to authenticate, an error message `Bluetooth service is not available` is displayed. Install the Device Service and try to authenticate again.

Card


The Card method enables you to authenticate using the contactless smart card (with the card serial number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.

TIP: Ensure to install the Advanced Authentication Device Service before you enroll a card. For more information about the Device Service, see the [Advanced Authentication - Device Service](#) guide.

Some card readers are supported only for Microsoft Windows. For more information about the list of supported card readers, see [Supported Card Readers and Cards](#).

Enrolling the Card Authenticator

Before enrolling the Card authenticator, ensure that the card reader is connected to the computer.

- 1 Click the Card  icon in **Add Authenticator**.
A message `Click "Save" to begin` is displayed.
- 2 (Optional) Specify a comment related to the Card authenticator in **Comment**.
- 3 (Optional) Select the preferred category from the **Category**.
- 4 Click **Save**.
A message `Waiting for the card` is displayed.
- 5 Tap a card on the reader.
A message `Authenticator "Card" has been added` is displayed.

Testing the Card Authenticator

- 1 Click the Card icon in **Enrolled Authenticators**.
- 2 Click **Test**.
A message `Waiting for the card` is displayed.
- 3 Tap a card on the reader.
A message `Card has been detected` is displayed for a moment. If the provided card passes the test, a message `Authenticator "Card" passed the test` is displayed. If the card is invalid, a message `Incorrect Card` is displayed.

The following table describes the possible error messages along with the workarounds for the Card authentication.

Table 3-1 Card authenticator - error messages

Error	Possible Cause and Workaround
Card Service unavailable	The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.

Error	Possible Cause and Workaround
Card reader has not been detected	The card reader is not connected properly or reader is not available in the Device Manager. Check the card reader connection settings and then try authenticating again.
Card reader detected	<p>Due to an improper functioning of a system service <code>pcscd</code> in the Mac OS X. To fix this issue, open Terminal application and run the following commands:</p> <pre>kill pcscd</pre> <pre>kill pcscdlite</pre> <p>Then reconnect the reader and try to enroll again.</p>

Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

NOTE: If an email address is not registered in the repository for a user profile, then the Email OTP method is not enrolled automatically. However, you can specify the email address in the **Add Authenticator** section and click **Save** to enroll manually.

Enrolling the Email OTP Authenticator

This authenticator is enrolled automatically and you cannot remove it.



- 1 Click the Email OTP icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to Email OTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify the email address in **Email**.
- 5 Click **Save**.

A message Authenticator "Email OTP" has been added is displayed.

NOTE: An administrator has the privilege to hide the **Email** to prevent users from providing new email address that is not registered in the repository.

Testing the Email OTP Authenticator

- 1 Click the Email OTP icon in **Enrolled Authenticators**.
- 2 Ensure that your email address (specified after the text *The email address to which the OTP is sent to is*) is valid. If the set email address is invalid, update the email address.
- 3 Click **Test**.

A message `OTP password sent, please specify` is displayed.

- 4 Check your email. You must have received an email with the OTP.
- 5 Specify the OTP in **Password**.
- 6 Click **Next**.

A message `Authenticator "Email OTP" passed the test` is displayed. If the provided OTP is invalid, a message `Incorrect OTP password` is displayed.

Emergency Password

If a user forgets or loses a card, you as a helpdesk administrator can enroll a temporary password for the user. This Emergency Password helps the user to authenticate on a temporary basis.

Enrolling the Emergency Password

- 1 Click the Emergency Password icon in the Helpdesk portal.
- 2 (Optional) Specify a comment related to the Emergency Password authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify **Password** and **Confirmation** in the appropriate fields.
- 5 Check the **Start date (UTC)** and **End date (UTC)** when the authenticator is valid. You can change the dates if applicable.
- 6 You can also change the **Maximum logons** value (if applicable).

Testing the Emergency Password Authenticator

- 1 Click the Emergency Password icon in the **Enrolled authenticators** section.
- 2 Click **Test**.
- 3 Specify the Emergency Password in **Password**.
- 4 Click **Next**.


A message `Authenticator Emergency Password passed the test` is displayed.

Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you are successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

Enrolling the Face Authenticator

- 1 Click the Face  icon in **Add Authenticator**.
- 2 Click **Save** to start enrolling the face.

A message `Face Detecting` is displayed.

- 3 The camera captures your face and enrolls for Facial Recognition method.
A message Authenticator "Facial Recognition" has been added is displayed.

NOTE

- ♦ Facial recognition authentication method works with or without the Device Service installed. If the Device Service is not installed, then the browser support is used for capturing the face.
 - ♦ To use the Facial recognition method for OAuth 2.0 and SAML 2.0 integrations, you must have the Advanced Authentication Device Service installed.
-

Testing the Face Authenticator

- 1 Click the Face icon in **Enrolled Authenticators**.
- 2 Click **Test**.
- 3 Present your face in front of the camera.

If your face matches with the enrolled face, the facial authentication is successful and a message Authenticator "Facial Recognition" passed the test is displayed.

The following table describes the possible error messages along with the workaround for the Face authentication.

Table 3-2 Facial Recognition authenticator- error messages

Error	Possible Cause and Workaround
Capture Device cannot be opened	The camera is not connected properly. Check your camera settings and try again.
Mismatch	The enrolled face and presented face does not match. You must present your face again for the authentication.
Timeout	The session has timed out. You must present your face again for the authentication.

FIDO 2.0

The FIDO 2.0 method facilitates you to use any FIDO compliant device either in-built with the system or connected through USB to register and authenticate to the web environment. When you try to authenticate, FIDO compliant device and user gesture, such as tap on token and swipe fingerprint on reader are validated.

NOTE: If the FIDO 2.0 method is enrolled using the Windows Hello in Microsoft Edge 17 or earlier supported browser versions then you must authenticate using the same browser. After upgrading to the latest version of Edge that supports the FIDO 2.0 standards, you must re-enroll the FIDO 2.0 method.

Enrolling the FIDO 2.0 Authenticator



- 1 Click the FIDO 2.0 icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to FIDO 2.0 in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Click **Save**.
A message `Waiting for Web Authentication data is displayed`.
- 5 Connect the device that complies with FIDO standards.
- 6 Perform the action associated to the device.
For example, if you use the FIDO U2F device, connect it to the computer and touch the device when you see a flash.
- 7 Click **Save**.
A message `Authenticator "FIDO 2.0" enrolled is displayed`.

Testing the FIDO 2.0 Authenticator


- 1 Click the FIDO 2.0 icon in **Enrolled Authenticators**.
- 2 Click **Test**.
A message `Waiting for Web Authentication data is displayed`.
- 3 Perform the action associated to the enrolled device.
A message `Authenticator "FIDO 2.0" passed the test is displayed`.

FIDO U2F

The FIDO U2F method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the enrolled token. If the token details match, you are authenticated successfully.

TIP: While you enroll and test the FIDO U2F authentication on any browser except Google Chrome, ensure to install the Advanced Authentication Device Service on the system. The Google Chrome contains a built-in module.

Enrolling the FIDO U2F Authenticator

- 1 Click the U2F  icon in **Add Authenticator**.
A message `Press button "Save" to begin enrolling. is displayed`.
- 2 (Optional) Specify a comment related to U2F in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Click **Save**.

A message `Please touch the flashing U2F device now` is displayed. You may be prompted to allow the site permissions to access your security keys.

- 5 Touch the FIDO U2F button when there is a flash on the device.

A message `Authenticator "U2F" enrolled` is displayed. If there is no flash for more than 10 seconds, reconnect your token and repeat the steps.

NOTE: To use U2F in Google Chrome on Linux, you must perform the following steps:

- 1 Download or create a copy of the file `70-u2f.rules` in the Linux directory: `/etc/udev/rules.d/` from <https://github.com/Yubico/libu2f-host/blob/master/70-u2f.rules>.

If the file is already available, ensure that the content is similar to that specified in <https://github.com/Yubico/libu2f-host/blob/master/70-u2f.rules>.

NOTE: If your version of UDEV is lower than 188, use the rules specified at <https://github.com/Yubico/libu2f-host/blob/master/70-old-u2f.rules>.

- 2 Save the file `70-u2f.rules` and reboot the system.
-

Testing the FIDO U2F Authenticator

- 1 Click the U2F icon in **Enrolled Authenticators**.
- 2 Click **Test**.

A message `Please touch the flashing U2F device now` is displayed. You may be prompted to allow the site permissions to access the security keys in U2F device.

- 3 Touch the FIDO U2F button when there is a flash on the device.

A message `Authenticator "U2F" passed the test` is displayed. If the connected token is invalid, a message `Token is not registered` is displayed.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

Table 3-3 FIDO U2F authenticator - error messages

Error	Possible Cause and Workaround
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	The FIDO U2F service is not installed properly. Install the U2F service and try again.
Timeout. Press "Save" to start again	The session has timed out. Click Save and enroll again.
Enroll failed: Device not attested. Ask your administrator to upload your token attestation certificate	The token does not contain attested certificate. Contact your administrator to add the attestation certificate to your token.
Unexpected error: U2F token error: The visited URL does not match the application ID or it is not in use	The Facets are not configured appropriately. Contact you administration to check the Facets settings.

Fingerprint

The Fingerprint method enables you to authenticate using your fingerprint(s). During enrollment, the fingerprint reader captures the fingerprint. When you try to authenticate on any device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated successfully.

You can enroll fingers for the Fingerprint method using one of the following devices:

- ◆ Single finger reader
- ◆ Multi-finger reader


TIP: Fingerprint(s) enrollment is supported only on Microsoft Windows and Linux RHEL kernel 3.x.x. You must install the Advanced Authentication Device Service.

Linux RHEL supports the fingerprint readers: Green Bit DactyScan84c and Nitgen eNBioScan-C1 for the Fingerprint method enrollment and authentication respectively.

Duress Finger

The Fingerprint method also allows you to assign one of the enrolled fingers as duress. Only under an emergency or a threat, you can authenticate with the duress finger. Use of the duress finger for authentication sends an alert notification to the email address and phone number that the administrator has configured.

Enrolling the Fingerprint Authenticator Using Single Finger Reader

- 1 Click the Fingerprint  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to the Fingerprint authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Select the preferred finger for enrollment and place or swipe the finger on the reader when there is a flash.

NOTE: Number of fingers to be enrolled and the number of scans performed for each finger are mentioned on the **Add Fingerprint authenticator** page.

Red indicators below the fingerprint represents the number of captures that the administrator has configured.

- 5 Repeat **Step 4** to add more fingers for authentication.
- 6 (Conditional) Select one of the enrolled finger as duress from **Assign Duress Finger** list.

NOTE: If you have not enrolled fingers for Fingerprint method, then the **Assign Duress Finger** list will be empty.


- 7 Click **Save**.

A message Authenticator "Fingerprint" has been added is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see [Assigning a Finger as Duress](#).

IMPORTANT: It is recommended to test the authenticator after enrollment. If the test fails, delete the authenticator and enroll it again.

Enrolling the Fingerprint Authenticator Using Multi-Finger Reader

- 1 Click the Fingerprint  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to the Fingerprint authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 (Conditional) Set **Use multi-finger reader for enrollment** to **ON** to use multi-finger reader.

NOTE: An administrator has the privilege to hide the **Use multi-finger reader for enrollment** and force users to enroll with the multi-finger reader.

- 5 Select one of the highlighted fingers combination for enrollment. The fingers combination available are:
 - ◆ Four fingers of the left hand
 - ◆ Four fingers of the right hand
 - ◆ Two thumbs
- 6 Place the fingers on the reader when you see the LEDs of selected fingers flash.
Wait till the reader scans the fingers.
Red indicators below the fingerprint represents the number of captures that the administrator has configured.
- 7 (Conditional) Select one of the enrolled finger as duress from **Assign Duress Finger** list.

NOTE: If you have not enrolled fingers for Fingerprint method, then the **Assign Duress Finger** list will be empty.

- 8 Click **Save**.
A message Authenticator "Fingerprint" has been added is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see [Assigning a Finger as Duress](#).

Assigning a Finger as Duress

- 1 Click the Fingerprint icon in **Enrolled Authenticators**.
- 2 Select the preferred finger as duress from **Assign Duress Finger** list.
The **Assign Duress Finger** list displays the fingers that are enrolled.
- 3 Click **Save**.

Testing the Fingerprint Authenticator

- 1 Click the Fingerprint icon in **Enrolled Authenticators**.
- 2 Click **Test**.
- 3 Place or swipe your finger on the reader.

A message Authenticator "Fingerprint" passed the test is displayed. If the fingerprints are not identical, a message Fingerprint Mismatch is displayed.

The following table describes the possible error message along with the workarounds for the Fingerprint authentication.

Table 3-4 Fingerprint authenticator - error messages

Error	Possible Cause and Workaround
Fingerprint Service unavailable	The Advanced Authentication Device Service is not installed. Ensure to install Advanced Authentication Device Service and try authenticating again.
Fingerprint reader is not connected	The fingerprint reader or vendor specific drivers are not connected properly. Ensure that the fingerprint reader and vendor specific drivers are connected properly to the machine.

HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You must use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If the OTPs are identical, you are authenticated successfully.

Enrolling the HOTP Authenticator


To enroll the HOTP authenticator, you must follow the recommendations of your system administrator. You can enroll HOTP in one of the following ways:

- ♦ [Using YubiKey Hardware token](#)
- ♦ [Using Software token \(DS3 OATH\)](#)
- ♦ [Synchronizing Existing Token with HOTP Counter](#)
- ♦ [Assigning a Token Serial To an Account](#)

NOTE: If a token is already assigned to your account, enrollment is not required.

Using YubiKey Hardware Token


To enroll HOTP using YubiKey hardware token, perform the following steps:

- 1 Click the HOTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to HOTP authenticator in **Comment**.
- 3 Specify the token serial number in **OATH Token Serial**.
- 4 Specify **YubiKeyToken Key ID**.
- 5 Place the cursor in **HOTP 1** and touch the button on YubiKey.
OTP from YubiKey is inserted in **HOTP 1** automatically.
- 6 Repeat **Step 5** in **HOTP 2** and **HOTP3** to insert consequent OTPs.
- 7 Click **Save**.

A message Authenticator "HOTP" has been added is displayed.

Using Software Token


To enroll HOTP using RFC 4226 compliant software token, perform the following steps:

- 1 Click the HOTP  icon in **Add Authenticator**.
- 2 Specify first OTP that generated on the token in **HOTP 1**.
- 3 Specify consequent OTPs from the token in **HOTP 2** and **HOTP 3**.
- 4 Specify 40 characters hexadecimal secret code in **Secret (If you know)**.
- 5 Click **Save**.

A message Authenticator "HOTP" has been added is displayed.


Synchronizing Existing Token with HOTP Counter

If an existing token is assigned to your account, perform the following steps to synchronize the HOTP counter:

- 1 Click the HOTP  icon in **Enrolled Authenticators**.
- 2 Specify first OTP in **HOTP 1** that generated on the token. In case of YubiKey token, connect the hardware token to the system and perform the following steps:
 - 2a Place cursor in **HOTP 1**.
 - 2b Touch button on the token.
- 3 Specify the consequent OTPs from the token in **HOTP 2** and **HOTP 3**. In case of YubiKey token, repeat the steps 2a and 2b.
- 4 Click **Save**.

Assigning a Token Serial To an Account

If the administrator has uploaded the token details on the Advanced Authentication server and you have got the serial number of a token, perform the following steps to assign serial number to your account:

- 1 Click the HOTP  icon in **Enrolled Authenticators**.
- 2 (Optional) Specify a comment related to HOTP authenticator in **Comment**.
- 3 Specify the token's serial number in **OATH Token Serial**.
- 4 Specify the three consequent OTPs in **HOTP 1**, **HOTP 2**, and **HOTP 3** respectively.
- 5 Click **Save**.

Testing the HOTP Authenticator

- 1 Click the HOTP icon in **Enrolled Authenticators**.
- 2 Click **Test**.
- 3 Specify the OTP in **Password**.

If the OTP is valid, a message Authenticator "HOTP" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the HOTP authentication.

Table 3-5 HOTP authenticator - error messages

Error	Possible Cause and Workaround
Incorrect OTP password	If the specified OTP is incorrect or the counter on the token and server are not in sync. Specify a valid OTP and try to authenticate again
Cannot derive the counter. Check your three OTPs.	If one of the specified OTP is incorrect during the enrollment. Try to enroll again with the new OTPs.


LDAP Password

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on an application, the submitted password is compared with the actual password in the corporate directory. If both the passwords are identical, you are authenticated successfully.

Enrolling the LDAP Password Authenticator

This authenticator enrolls automatically and you cannot remove it.

Testing the LDAP Password Authenticator

- 1 Click the LDAP password  icon in **Enrolled Authenticators**.
- 2 Click **Test**.

3 Specify the valid password in **Password**.

4 Click **Next**.

If the password is valid, a message `Authenticator "LDAP password" passed the test` is displayed. If the provided password is invalid, a message `Invalid credentials` is displayed.

Password

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication server. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

Enrolling the Password Authenticator

1 Click the Password `***|` icon in **Add Authenticator**.

2 (Optional) Specify a comment related to Password authenticator in **Comment**.

3 (Optional) Select the preferred category from **Category**.

4 Specify **Password** and **Confirmation**.

NOTE: Ensure that the password contains minimum 5 characters, by default. An administrator has the privilege to change the password length.

5 Click **Save**.

A message `Authenticator "Password" has been added` is displayed.

WARNING: You will not receive any notification about the password expiration. The password expiration value is 42 days, by default. Ensure to sign in to the Self-Service portal and change the password before it expires.

Testing the Password Authenticator

1 Click the Password icon in **Enrolled Authenticators**.

2 Click **Test**.

3 Specify **Password** and **Confirmation**.

4 Click **Next**.

If the test is successful, a message `Authenticator "Password" passed the test` is displayed. If the provided authenticator is invalid, a message `Incorrect password` is displayed.

PKI

The PKI method enables you to authenticate using any one of the following ways:

- ◆ [PKI Device](#)
- ◆ [Virtual Smartcard](#)

PKI Device

PKI device is a hardware device, such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on any device, the certificate in the device is compared with the actual certificate. If the certificates are identical, you are authenticated successfully.


NOTE: You must install the Advanced Authentication Device Service for enrolling the PKI method using PKI device.

Virtual Smartcard

You can also enroll and authenticate the PKI method using a virtual smartcard. Virtual smartcard supports authentication to any web environment and makes use of client SSL certificate to authenticate users. In client certificate authentication, the client browser provides its client certificate to the server to confirm the identity of a user.

A client SSL certificate is a file that contains information, such as digital signature, expiration date, name of user, and name of CA (Certificate Authority). When you try to authenticate on the web environment, authenticity of the client SSL certificate is validated based on the settings that are configured by the administrator.

Enrolling the PKI Authenticator Using PKI Device

- 1 Click the PKI icon  in **Add Authenticator**.
- 2 (Optional) Specify a comment in the **Comment**.
- 3 (Optional) Select the preferred category from the **Category**.
A message `Waiting for the card` is displayed.
- 4 Click **Save**.
- 5 Insert the card in reader or connect the token to the machine.
A message `Use an existing certificate or generate a key pair` is displayed.
- 6 Select a key from **Key**.
If you have connected the token or card reader, the certificate type and expiry date of certificate is populated in **Key** automatically.
- 7 Specify **PIN** code of the device.
- 8 Click **Save**.
A message `Authenticator "PKI" has been added` is displayed.

Enrolling the PKI Authenticator Using Virtual Smartcard

- 1 Try to access the third party website from the browser where your administrator has imported a valid SSL certificate.
The **Certificate** dialog box is displayed.
- 2 Select the preferred client SSL certificate that is issued by the administrator.
You get auto-enrolled to PKI method using virtual smartcard.

NOTE: An administrator has the privilege to disable auto-enrollment of the PKI method using virtual smartcard.

Testing the PKI Authenticator

1 Click the PKI icon in **Enrolled methods**.

2 Click **Test**.

A message `Waiting for card...` is displayed.

3 Insert your card or connect your token to the machine, if you are using a PKI device.

If you are using a virtual smartcard, the client SSL certificate is detected automatically.

4 Specify the PIN of the PKI device in **PIN**.

If the test is successful, a message `Authenticator "PKI" passed the test` is displayed. If the card is invalid, a message `Wrong card` is displayed. If the specified PIN is invalid, a message `Incorrect PIN` is displayed.

The following table describes the possible error message along with the workarounds for the PKI authentication.

Table 3-6 PKI authenticator - error messages

Error	Possible Cause and Workaround
<code>Card reader connected</code>	When a card is not inserted to the reader or the token is not connected to the machine. Insert the card to the reader or connect token to the machine.
<code>Enroll failed: Cannot check revocation status for ...</code>	When the certificate on your device does not contain information about the revocation status location or if the information is inserted, but the Certificate Authority is not available to verify the revocation status.
<code>PKI service is not available</code>	The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.
<code>Key not found. Wrong Card?</code>	You have enrolled the PKI authenticator in the RDP session. Enroll the authenticator again in normal session.
<code>PIN is expired</code>	The PIN assigned to your token has expired. Contact your administrator for the new PIN.
<code>PIN is locked</code>	After certain number of attempts with the incorrect PIN, the PIN is locked. Contact your administrator to reset the PIN.
<code>Token is not present</code>	Token is not connected to the system. Connect the token and try authenticating again.
<code>Token is not recognized</code>	The Device Service is unable to detect the DLL to recognize the token.
<code>Unexpected service status: PLUGIN_NOT_INITED</code>	A vendor module is absent, invalid or not specified. Contact your administrator to check the configuration.

The following table describes the unexpected error codes that are displayed from a PKCS#11 module.

Table 3-7 : Unexpected Error codes

Error Code	Description
CKR_DEVICE_ERROR	The token or USB slot is broken. Try to use a different USB slot.
CKR_DEVICE_MEMORY	There is no space available in the memory of token or there may be some other issue with the memory.
CKR_MECHANISM_INVALID	An invalid mechanism was specified to the cryptographic operation.
CKR_PIN_EXPIRED	Ensure that the card has been initialized or do not use the default PIN and the PIN has 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.

RADIUS Client

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.


For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

Enrolling the RADIUS Client Authenticator

This authenticator is enrolled automatically and you cannot delete it.

By default, a user name from your corporate directory is set. You can change the required user name in **User name** and click **Save**.

Testing the RADIUS Client Authenticator

1. Click the RADIUS Client  icon in **Enrolled Authenticators**.
2. Specify a user name in **User name**.
3. Click **Test**.
4. Specify the password of the RADIUS Client in **Password**.
5. Click **Next**.

A message Authenticator "RADIUS Client" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the RADIUS Client authentication.


Table 3-8 RADIUS Client - error message

Error	Possible Cause and Workaround
Incorrect password	If the specified RADIUS Client password is invalid. Specify a valid password to test the authenticator.
RADIUS server does not reply	If the administrator has not configured RADIUS Client method appropriately. Contact your administrator and report the error message.


Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

Enrolling the Security Questions Authenticator

- 1 Click the Security Questions  icon in **Add Authenticator**.
- 2 (Optional) Specify an optional comment in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify the answers to the security questions that have been set by the administrator.
Ensure that each answer contains at least one character.
- 5 Click **Save**.
A message Authenticator "Security Questions" added is displayed.

Testing the Security Questions Authenticator

1. Click the Security Questions  icon in **Enrolled Authenticators**.
2. Click **Test**.
3. Specify the answers to the security questions.
4. Click **Next**.
A message Authenticator "Security Questions" passed the test is displayed.
If one of the specified answer is invalid, a message Wrong answers is displayed.

Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

Pre-requisite:

To enroll the Smartphone authenticator, you must install the NetIQ Auth application on your smartphone.

For more information about downloading and installing the smartphone app, see [Installing NetIQ Advanced Authentication App](#).

Enrolling the Smartphone Authenticator


You can enroll the Smartphone method in one of the following ways:

- ◆ [Enrolling with a QR code](#)
- ◆ [Enrolling with a link in the email](#)

Enrolling with a QR Code

During the enrollment, you must scan a QR code that creates an authenticator on your mobile app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

To enroll the Smartphone method with a QR code, perform the following steps:

- 1 Click the Smartphone  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to the Smartphone authenticator.
- 3 (Optional) Select the required category from **Category**.
- 4 Click **Save**.
A QR code is displayed.
- 5 Scan the QR code with the Advanced Authentication smartphone app. To do this, perform the following steps:
 - 5a Open the Advanced Authentication smartphone app.
 - 5b Specify a PIN if applicable.
 - 5c Click the + (plus) icon in the **Enrolled Authenticators** screen.
 - 5d The camera of your smartphone is launched.
 - 5e Scan the QR code with the camera.
A message `Authenticator "Smartphone" added` is displayed.
 - 5f Specify your user name and an optional comment in the app.
 - 5g Tap **Save**.
The smartphone authenticator is created.

If you do not enroll the Smartphone authenticator within few minutes, an error message `Enroll failed: Enroll timeout` is displayed. Refresh the browser and try to enroll again.

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

1. Zoom the page to 125-150% and scan the zoomed QR code.
 2. Ensure that nothing overlaps the QR code (mouse cursor, text).
-

Enrolling Through a Link

An administrator will send you the link to your email or via SMS. You must click on the link on your smartphone where the [NetIQ Auth](#) app is installed and you will be redirected to the smartphone app where you can enroll and an authenticator is created.

To enroll the Smartphone method through a link, perform the following steps:

- 1 Check your phone for a new email or SMS. You will receive a link sent by the administrator.
- 2 Click on the link. You will be redirected to the smartphone app.

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

NOTE: In some instances, when you click on the enroll link, you will be redirected to page where the following two links are displayed:

- ◆ Click to enroll.
- ◆ Click to download and install Smartphone authenticator for Android.

If you have the app installed on your phone, use **Click to enroll link**. If you do not have the app then use **Click to download link**.

- 3 Specify a PIN or a Touch ID if applicable.
- 4 Specify your username and password in the **Enroll new authenticator** screen.
- 5 Tap **Sign In**.
- 6 Specify an optional comment in the app.
- 7 Tap **Save**.

The smartphone authenticator is created.

Testing the Smartphone Authenticator

- 1 Click the Smartphone  icon in **Enrolled Authenticators**.

- 2 Click **Test**.

- 3 Open the Advanced Authentication smartphone app.

A push notification is sent to your smartphone.

- 4 Tap **Accept** to accept the authentication request.

A message `Authenticator "Smartphone" passed the test` is displayed.

If you tap **Reject**, the authentication is declined and a message `Auth rejected` is displayed.

If you ignore the authentication request, after few minutes a message `Auth confirmation timeout` is displayed.


SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

NOTE: The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

NOTE: If a phone number is not registered in the repository for a user profile, then the SMS OTP method is not enrolled automatically. However, you can manually enroll the SMS OTP method from the **Add Authenticator** section, by specifying the phone number and clicking **Save**.


Enrolling the SMS OTP Authenticator

- 1 Click the SMS OTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to SMS OTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify the mobile number in **Phone number**.
- 5 Click **Save**.

A message Authenticator "SMS OTP" has been added is displayed.

NOTE: An administrator has the privilege to hide the **Phone number** to prevent users from providing new phone number that is not registered in the repository.

Testing the SMS OTP Authenticator

- 1 Click the SMS OTP  icon in **Enrolled Authenticators**.
Ensure that your mobile phone number is valid.
- 2 Click **Test**.
- 3 You will receive an SMS with an OTP.
- 4 Specify the OTP in **Password**.
- 5 Click **Next**.

A message Authenticator "SMS OTP" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the SMS OTP authentication.

Table 3-9 SMS OTP authenticator - error messages

Error	Possible Cause and Workaround
Incorrect OTP password	The specified OTP is invalid. Specify a valid OTP and try again.
You do not have a phone number. Contact administrator or Helpdesk and register your phone	If your phone number is not registered in the repository. Contact administrator or helpdesk to register phone number.

Swedish BankID

The Swedish BankID method enables you to authenticate using your Swedish Personal Identification Number. To enroll the Swedish BankID authenticator, you must have the BankID app either on your computer or mobile device. When you try to authenticate any device a request is sent to the BankID app, specify the security code to unlock the app. The recorded personal identification number is compared with actual identification number on the BankID app. If the identification numbers match, you are authenticated successfully.

Enrolling the Swedish BankID Authenticator


Before enrolling, ensure that you have the following prerequisites:

- ♦ Social Security Number (SSN)
- ♦ BankID app (either desktop or mobile version).

For more information about the BankID app, see [BankID](#).

NOTE: While you set up the security code for the BankID app, ensure that the code must contain six digits in non-sequential format (for example: 221144).

To enroll the Swedish BankID, perform the following steps:

- 1 Click the BankID  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to BankID authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify the personal identification number in **Personal ID (SSN)**.
- 5 Click **Save**.

A message `Authenticator "BankID" added` is displayed.

Testing the Swedish BankID Authenticator

- 1 Click the BankID icon in **Enrolled Authenticators**.
- 2 Click **Test**.
A message `Start your BankID app` is displayed.
- 3 Open the BankID app.
- 4 Specify **Security Code**.
 - ♦ (Conditional) Click **Identify** on the mobile app.
 - ♦ (Conditional) Click **Verify my identity** on the desktop app.


If the test is successful, a message `Authenticator "BankID" passed the test` is displayed.

Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

This authenticator is enrolled automatically and you cannot remove it.

Testing the Swisscom Mobile ID Authenticator

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

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token, Desktop OTP tool, or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

You can enroll the TOTP authenticator using the Desktop OTP tool. To initiate the tool, use the link that is sent from your administrator. You must click on the link and the Desktop OTP tool is prompted where you can enroll and create an account. While authenticating to any service, you must copy the OTP from the tool and use the OTP to get authenticated.

Enrolling the TOTP Authenticator


To enroll the TOTP authenticator, you must follow the recommendations of your system administrator. You can enroll TOTP method using any one of the following ways:

- ♦ [NetIQ Advanced Authentication App](#)
- ♦ [Google Authenticator App](#)
- ♦ [OATH Compliant Hardware Token](#)
- ♦ [Enrolling TOTP Manually](#)
- ♦ [Desktop OTP Tool](#)

WARNING: The QR code format in the Advanced Authentication and Google Authenticator apps are different. Contact your system administrator to confirm the app recommended for enrollment.

NetIQ Advanced Authentication App

To enroll the TOTP authenticator using Advanced Authentication smartphone app, perform the following steps:

- 1 Click the TOTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to TOTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Open the Advanced Authentication app on your phone.
- 5 Tap **Offline authentication**.
- 6 Tap **+** to add a new authenticator.
- 7 Scan the QR code using the camera on your phone.
- 8 Click **Save** in the **Add TOTP authenticator** page.
A message Authenticator "TOTP" has been added is displayed.
- 9 Tap the new authenticator and specify account name and additional details in **Account** and **Additional info** respectively in the app.
- 10 Click **Save**.


TIP: If you are unable to scan the QR code with Advanced Authentication app, perform the following steps:

1. Zoom the page to 125 - 150%.
2. Scan the zoomed QR code using Google Authenticator app.
Ensure that the mouse cursor is not overlapping the QR code.

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

Google Authenticator App

To enroll the TOTP authenticator using Google Authenticator app, perform the following steps:


- 1 Click the TOTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to the TOTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Open the Google Authenticator app on your phone.
- 5 Tap **BEGIN SETUP** in the app.
- 6 Tap **Scan barcode** to add a new authenticator in the app.
- 7 Scan the QR code using the camera on your phone.
- 8 Click **Save**.

A message Authenticator "TOTP" has been added is displayed.

TIP: If you scan Advanced Authentication app compatible QR code with Google Authenticator app, a message `Invalid barcode` is displayed.


OATH Compliant Hardware Token

To enroll the TOTP authenticator using OATH compliant hardware token, perform the following steps:

- 1 Click the TOTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to TOTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Specify the token's serial number in **OATH Token Serial**.
You can find the serial number behind the token.
- 5 Press the button on the token and specify the one-time password in **OTP**.
- 6 Click **Save**.

A message Authenticator "TOTP" has been added is displayed.

Enrolling TOTP Manually

- 1 Click the TOTP  icon in **Add Authenticator**.
- 2 (Optional) Specify a comment related to TOTP authenticator in **Comment**.
- 3 (Optional) Select the preferred category from **Category**.
- 4 Click + adjacent to **Specify the TOTP secret manually**.
- 5 Specify 40 hexadecimal characters in **Secret**.
- 6 Set **Google Authenticator format of secret (Base32)** to **ON** to display the Google Authenticator app compatible QR code.

By default, **Google Authenticator format of secret (Base32)** is set to **OFF** and Advanced Authentication app compatible QR code is displayed.

NOTE: The administrator has privilege to configure the **Google Authenticator format of secret (Base32)** option in the Administration portal. However, you can override the administrator configured setting.

- 7 Set the preferred value in **Period**. 30 seconds is set by default.
- 8 Click **Save**.

A message Authenticator "TOTP" has been added is displayed.

NOTE: If the administrator has disabled the manual enrollment of TOTP in the Administration portal, then the **Specify the TOTP secret manually** section is not displayed.

Desktop OTP Tool

Before enrolling the TOTP authenticator using the link, ensure that NetIQ Desktop OTP tool is installed on your system.

- 1 Check your registered email or phone for the enrollment link.
- 2 Click on the link.

You are directed to the Desktop OTP tool.

- 3 Specify your LDAP repository or local username, password, and optional comment in the **NetIQ Advanced Authentication OTP Tool** window.
- 4 Click **OK**.
The TOTP authenticator is created in the Desktop OTP tool and enrolled in the Self-Service portal.

Testing the TOTP Authenticator

- 1 Click the TOTP icon in **Enrolled Authenticators**.
- 2 Click **Test**.
- 3 Specify one-time password in **Password**.
- 4 Click **Next**.


If the test is successful, a message `Authenticator "TOTP" passed the test` is displayed. If the one-time password is invalid or the server time is not in sync, a message `Incorrect OTP password` is displayed.

Voice

The Voice method initiates a call to your registered phone number. The phone call requests you to specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are authenticated successfully.

NOTE: If a phone number is not registered in the repository for a user profile, then the Voice method is not enrolled automatically. However, you can specify the phone number in the **Add Authenticator** section and click **Save** to enroll manually.

Enrolling the Voice Authenticator

- 1 Click the Voice  icon in **Add Authenticator**.
- 2 Check whether a valid phone number is specified in **Phone number**.
- 3 (Optional) Specify a comment related to Voice authenticator in **Comment**.
- 4 (Optional) Select the preferred category from **Category**.
- 5 Specify your PIN in **PIN**.

The PIN must contain minimum 3 digits, by default.

- 6 Click **Save**.

A message `Authenticator "Voice" added` is displayed.

NOTE: An administrator has the privilege to hide **Phone number** to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice Authenticator

1 Click the Voice icon in **Enrolled Authenticators**.

2 Click **Test**.

A message `Call has been initiated` is displayed.

3 Answer the call on your phone.

4 Specify your PIN followed by a hash symbol (#) in the dial pad of your mobile phone.

A message `Authenticator "Voice" passed the test` is displayed. If the specified PIN is invalid, a message `Incorrect PIN` is displayed.

WARNING: You will not receive any notification about the PIN expiration. The PIN expiration is set as 42 days, by default. You must sign in to the Self-Service Portal and change the PIN before it expires.


Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short duration. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

NOTE: If a phone number is not registered in the repository for a user profile, then the Voice OTP method is not enrolled automatically. However, you can manually enroll the Voice OTP method from the **Add Authenticator** section, specify the phone number and click **Save**.

Enrolling the Voice OTP Authenticator

This authenticator enrolls automatically and you cannot remove it.

- 1 Click the Voice OTP  icon in **Add Authenticator**.
- 2 Check whether a valid phone number is specified in **Phone number**.
- 3 (Optional) Specify a comment related to voice OTP authenticator in **Comment**.
- 4 (Optional) Select the preferred category from **Category**.
- 5 Receive the call on your phone and listen to the voice OTP.
- 6 Specify the OTP in **Password**.
- 7 Click **Save**.

A message `Authenticator "Voice OTP" added` is displayed.

NOTE: An administrator has the privilege to hide **Phone number** to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice OTP Authenticator

1. Click the Voice OTP  icon in **Enrolled Authenticators**.


2. Click **Test**.
3. Receive the call on your phone and listen to the voice OTP.
4. Specify the OTP in **Password**.
5. Click **Next**.

A message Authenticator "Voice OTP" passed the test is displayed. If the specified OTP is invalid, a message Incorrect answer, try again is displayed.

Web Authentication Method

Advanced Authentication enables you to use authorization on the third-party websites (Identity Providers) to access the Advanced Authentication portals.

Enrolling the Web Authentication Authenticator

- 1 Click the Web Authentication  icon in **Add Authenticator**.
- 2 (Optional) Specify the text related to the authenticator in **Comment**.
- 3 Select the **Identity Provider**.
- 4 (Optional) Specify a hint for the user in **Username hint**.
- 5 Click **Save**.

The enrollment is redirected to the Identity Provider page that you have selected. Specify your credentials.

You will be redirected to the Enrollment page with your enrolled authenticator.

An error Web Authentication failed might be displayed after the authorization on third-party websites during enrollment. Contact your administrator to verify the Web Authentication method settings.

Testing the Web Authentication Authenticator

- 1 Click the Web Authentication  icon in **Enrolled Authenticators**.
- 2 Click **Test**.

You will be automatically authenticated by the enrolled Identity Provider.

Windows Hello

The Windows Hello method facilitates you to use your Windows Hello fingerprint and facial recognition authentication to log in to the Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.

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

This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

Configuring the System Settings for Windows Hello

Before enrolling Windows Hello, you must configure the system settings.

- ◆ [“Configuring Settings for Windows Hello Fingerprint” on page 41](#)
- ◆ [“Configuring Settings for Windows Hello Face Recognition” on page 41](#)

NOTE: You cannot enroll the Windows Hello authentication on an RDP session.

Configuring Settings for Windows Hello Fingerprint

- 1 Click **Start > Settings > Accounts > Sign-in options**.

Under **Windows Hello**, the options for fingerprint is displayed if your computer has a fingerprint reader.

- 2 Click **Set up** under **Fingerprint**.
- 3 Click **Get started**.
- 4 Specify your PIN.

NOTE: If you do not have a PIN, you must create one to set up the fingerprint.

- 5 To enroll fingerprint, scan your finger on the fingerprint reader.

You will have to place your finger multiple times to provide the scanner a good picture of your fingerprints.

- 6 Click **Add Another** if you want to add another fingerprint.

Configuring Settings for Windows Hello Face Recognition

- 1 Click **Start > Settings > Accounts > Sign-in options**.

Under **Windows Hello**, the option for face recognition is displayed if your computer has an external camera.

- 2 Click **Set up** under **Face Recognition**.
- 3 Click **Get started**.
- 4 Specify your PIN.

NOTE: If you do not have a PIN, you must create one to set up the face recognition.

- 5 To enroll the face, present your face to the camera. Follow the on-screen instructions to scan your face.


- 6 Select **Finish** to complete scanning or choose **Improve Recognition** to continue scanning.

NOTE: It is recommended that you select to improve recognition if you change your appearance often. Scanning your face again does not erase the earlier scans. It just helps Windows Hello get better at recognizing you.

For more information about Windows Hello, see the Microsoft Windows website <https://support.microsoft.com/en-in/help/17215/windows-10-what-is-hello>.

NOTE: To enable Windows Hello for all domain-joined Windows 10 workstations and for Windows 10 Enterprise, see <https://community.spiceworks.com/topic/1840001-windows-10-fingerprint-some-settings-are-managed-by-your-organization>.

Enrolling the Windows Hello Authenticator

- 1 Click the Windows Hello  icon.
- 2 (Optional) Specify a **Comment** in **Add Windows Hello authenticator**.
- 3 Select the preferred category from **Category**.

The **Category** option is displayed only if the administrator has set the **Event Categories** option in the Administration portal.

- 4 Specify your username for which Windows Hello is enrolled.

NOTE: If you have enrolled Windows Hello for a local account, you must specify the `<workstationname>\<username>`.

If you want to enroll Windows Hello that is set for a Microsoft account, you can specify `microsoftaccount\user@outlook.com` as the user name. This is helpful if you must login to the Windows operating system using your Microsoft account.

- 5 Click **Save**.

Testing the Windows Hello Authenticator

1. Click the Windows Hello  icon in **Enrolled authenticators**.
2. Click **Test**.
3. Place your finger on the reader or swipe your finger on the swipe sensor for the fingerprint authentication. Present your face for the facial recognition.

An appropriate message is displayed indicating the result of the test.

4 Sharing Authenticators

The **Shared Authenticators** feature allows user A to authenticate to user B's account by using the authenticators of user B (which is shared to A).

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

Bob is the manager of Alice and he is away on a holiday. He has enabled shared authenticator so that Alice can check his emails in his absence. Alice is required to verify an important email that can provide good revenue for the company. Alice can use the shared authenticators feature to access the account of Bob by using her own authenticators.

To share the authenticators of Alice with Bob, perform the following steps:

- 1 Log in to the Helpdesk portal with your Helpdesk administrator credentials.
- 2 In the **User to manage** screen, specify the user name as Bob.
- 3 Click the **Linked Authenticators** tab on the screen.
- 4 Specify the user name whose authenticator can be used as shared authenticator. If you want to use Alice's fingerprint to authenticate to the account of Bob, specify the name as **Alice-Fingerprint**.
- 5 Click **Save**.

Alice will now be able to authenticate to the account of Bob by using her own fingerprint.

NOTE

- ♦ A Full admin can prevent the use of shared authenticators for some events.
 - ♦ The boss Bob must have a chain with the LDAP Password method assigned to the Windows logon, Linux logon, or Mac OS logon event. Bob 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 Alice's fingerprint authenticator is linked to Bob's account, Alice must perform the following steps to get authenticated to Bob's account:

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

5 Unlocking Users

You can unlock the users of the local repository whose accounts are locked because of multiple failed attempts of entering the credentials while logging in.

Perform the following steps to unlock users:

- 1 Log in to the Helpdesk portal.
If any user accounts are locked in the local repository, the **Locked Users** tab is displayed.
- 2 Click the unlock icon against the user whose account you require to unlock.

6 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. You can obtain details, such as name of the card holder, repository information, email address, and mobile number of the user.

To access the Search Card portal, you must assign chains to the **Search card** event in the **Events** section.

IMPORTANT: To use this feature, you must have 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.

7 Managing Tokens

The Tokens Management portal helps you to import a file that contains information about multiple tokens and assign these tokens to users. To access the Tokens Management portal, you must assign chains to the **Tokens Management** event in the **Events** section of the Administration portal.

This chapter contains the following sections:

- ◆ “Importing the Token Files” on page 49
- ◆ “Assigning the Tokens to Users” on page 50
- ◆ “CSV File Format to Import the OATH Compliant Tokens” on page 50

Importing the Token Files

- 1 Log in to the Advanced Authentication Tokens Management portal, (<https://<AdvancedAuthenticationServer>/tokens>).
- 2 Click **Add**.
- 3 Click **Browse**, and then add a **PSKC** or **CSV** file.
- 4 Select the **File type**. The options available are:
 - ◆ **OATH compliant PSKC**: Select this file type if the file is compliant with OATH. For example, HID OATH TOTP compliant tokens.
 - ◆ **OATH csv**: Select this if the format of the file is as mentioned in [CSV File Format to Import the OATH Compliant Tokens](#). You cannot use the YubiKey CSV files.
 - ◆ **Yubico csv**: Select this file type if 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 if **HOTP Length** is set to **6 Digits** and **OATH Token Identifier** is set to **All numeric**.

IMPORTANT: **Moving Factor Seed** must not exceed 100000 characters.

- 5 (Conditional) For **PSKC** files, add the encrypted 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, the administrator need not change the default value of **OTP format** in the **Method Settings Edit** tab. For more information about the OTP format, see [OATH OTP](#).

Assigning the Tokens to Users

When the tokens are imported, you can see the list of tokens. You must assign these tokens to users.

You can assign the tokens in one of the following ways:

- ◆ **Using the Tokens Management portal:** Perform the following steps:
 1. Click **Edit** next to the token.
 2. Select **Owner**.
 3. Click **Save**.
- ◆ **Using Self-Service portal:** You can ask the user to self-enroll a token in the Self-Service portal, and then let the user know an appropriate value from the **Serial** column for the self-enrollment.

CSV File Format to Import the OATH Compliant Tokens

A CSV file, which is imported as an 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 stamp** (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. Ensure to use the Yubico CSV file type. This must be set in the Administration portal (**Advanced Authentication Administration portal > Methods > OATH OTP > OATH Tokens**).

8 Managing Endpoints

Endpoints are automatically added after you install a Windows Client, Linux PAM Client or Mac OS X Client, ADFS MFA plug-in, or Logon Filter and perform a reboot. Additionally, an endpoint is automatically added when you configure an integration with the NetIQ Access Manager (NAM) or z/OS mainframe. RADIUS authentication uses a predefined endpoint.

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.

This chapter contains the following sections:

- ◆ [“Configuring an Endpoint” on page 51](#)

Configuring an Endpoint

- 1 In the **Endpoints** section of the Helpdesk administration portal, click **Edit** against the endpoint you want to edit.

You can rename the endpoint, change its description, or endpoint type.

- 2 Set **Is enabled** to **ON** to enable the endpoint.
- 3 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.

- 4 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 is displayed in the Endpoints page. Also in **Advanced properties**, RAM information is displayed.
- ◆ Advanced Authentication Windows Client 5.6 or later versions, Advanced Authentication Linux PAM Client 6.0 or later versions, Advanced Authentication Mac OS X Client 6.0 or later versions must be installed on the endpoint.

-
- 5 Click **Save**.

Creating an Endpoint Manually

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 **Name** of the endpoint and its **Description**.
- 3 Set **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 Note 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 in 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 the 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*** in the `%ProgramData%\NetIQ\Windows Client\config.properties` file, and then re-start the machine. This recreates the endpoint.

9 Monitoring a User's Authentication Activity

You can monitor the authentication activity of a specific user in the **User report** tab. This report includes all the successful and the failed authentication details of the Advanced Authentication events.

This report allows you to analyze the following details of a specific user:

- ◆ The frequency of login
- ◆ The logged in events
- ◆ The authenticators used for login

To monitor the user report, perform the following steps in the helpdesk portal:

- 1 Specify the name of the user whose authentication report you require to monitor, and then click **Next**.
- 2 Click the **User report** tab.

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

- ◆ **Time**: 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 an X 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.

