



# NetIQ Advanced Authentication Framework

## **OATH Authentication Provider User's Guide**

Version 5.1.0

# Table of Contents

	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
About This Document .....	3
<b>OATH Authenticator Overview</b> .....	<b>4</b>
<b>Managing OATH Authenticator</b> .....	<b>5</b>
Microsoft Windows 7/Microsoft Windows Server 2008 R2 .....	5
Microsoft Windows Server 2012 .....	8
Enrolling OATH Authenticator .....	10
Enrolling OATH TOTP Authenticator with NetIQ Smartphone App .....	12
Enrolling OATH TOTP Compliant Software Tokens .....	14
Enrolling OATH TOTP Compliant Hardware Tokens .....	15
Enrolling OATH HOTP Compliant Hardware Tokens .....	17
Enrolling OATH HOTP Compliant Software Tokens .....	19
Re-enrolling OATH Authenticator .....	20
Testing OATH Authenticator .....	21
Removing OATH Authenticator .....	23
<b>Troubleshooting</b> .....	<b>24</b>
Cannot Enroll Authenticator .....	25
One-Time Password Doesn't Work .....	26
<b>Index</b> .....	<b>27</b>

# Introduction

## About This Document


### Purpose of the Document


This OATH Authentication Provider User's Guide is intended for all user categories and describes how to use the client part of NetIQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to manage OATH type of authentication.


For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ Advanced Authentication Framework – Client User's Guide.


Information on managing other types of authenticators is given in separate guides.

### Document Conventions

 **Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

 **Important notes.** This sign indicates important information you need to know to use the product successfully.

 **Notes.** This sign indicates supplementary information you may need in some cases.

 **Tips.** This sign indicates recommendations.

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

## OATH Authenticator Overview

The **OATH** (open authentication) authentication type takes its name from the Initiative for Open Authentication (OATH), which is a collaborative effort of IT industry leaders aimed at providing reference architecture for universal strong authentication across all users and all devices over all networks.

Open authentication addresses One Time Password (OTP) – based authentication method.

**OTP-based authentication** is intended to act as a bridge between legacy and modern applications. OTP credentials will facilitate integration with applications that rely solely on user passwords. Because end users are already familiar with static passwords, a device-generated password can greatly facilitate the transition to stronger authentication.

In OTP-based authentication method, login is performed using an essentially random password each time. The passwords are generated by a device, most commonly a hardware token associated with the user, and so the password is not based on the user's memory. This greatly increases security.

**TOTP** (Time-based One-time Password Algorithm) is a variant of the OTP authentication, where the one-time password changes at frequent intervals (say, every two minutes). Each one-time password is generated by applying a random-looking cryptographic function to a unique series value. In the time-based case, the value is the current time.

**HOTP** (Hmac-based One-Time Password algorithm) is a variant of OTP authentication, where one-time password is valid for an unknown period of time. HOTP authentication relies on a shared secret and a moving factor. Every time a new OTP is generated, the moving factor will be incremented and as a result generated one-time passwords should be different every time.

# Managing OATH Authenticator

In this chapter:

- [Microsoft Windows 7/Microsoft Windows Server 2008 R2](#)
- [Microsoft Windows Server 2012](#)

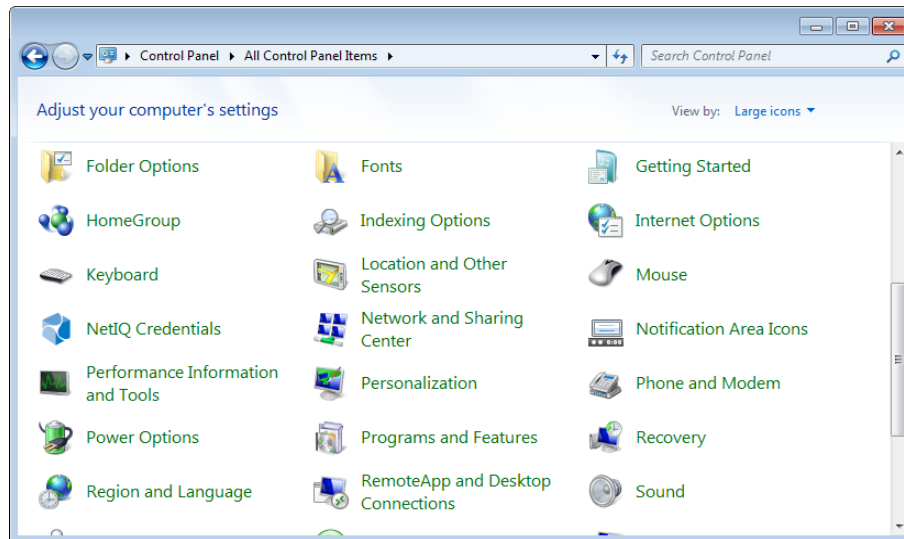
## Microsoft Windows 7/Microsoft Windows Server 2008 R2

Authenticator management options are available in the **Authenticators** window.

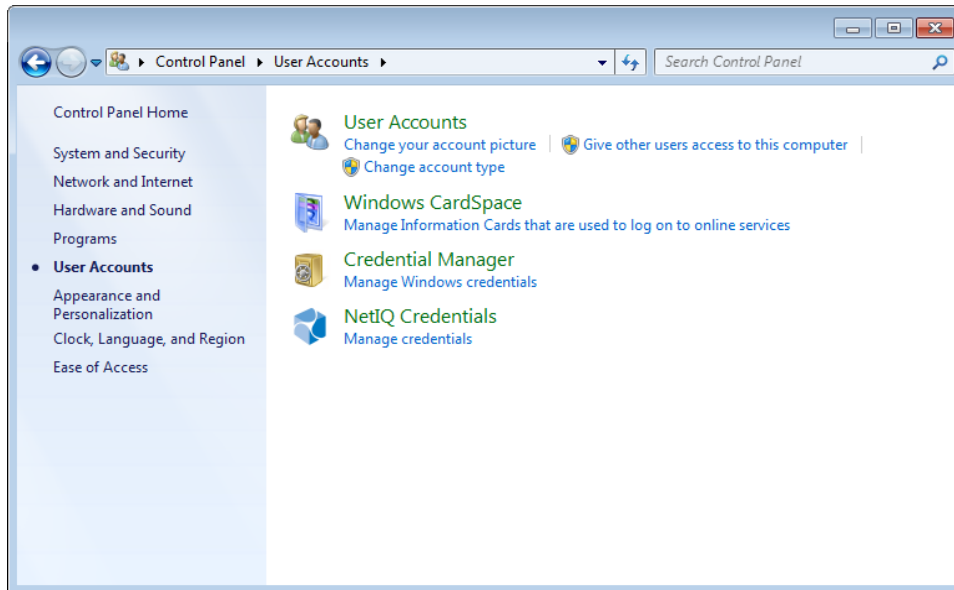
**i** The **Authentication Wizard** window is shown at system start if there are no enrolled authenticators.

To open the **Authenticators** window from **Control Panel**:

- In classic view of **Control Panel** select **NetIQ Credentials** item.



- In **Control Panel** by categories select **User Accounts > NetIQ Credentials**.



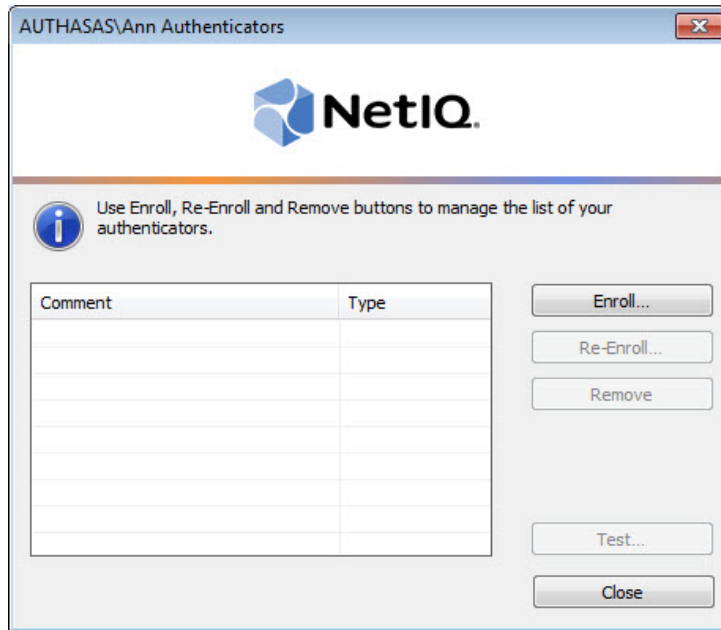
To open **Authenticators** window, user should undertake authorization procedure:

1. In the **Authorization** window, choose authentication method.



2. Get authenticated with the selected method.

3. Once you are authenticated, page for managing authenticators is opened.

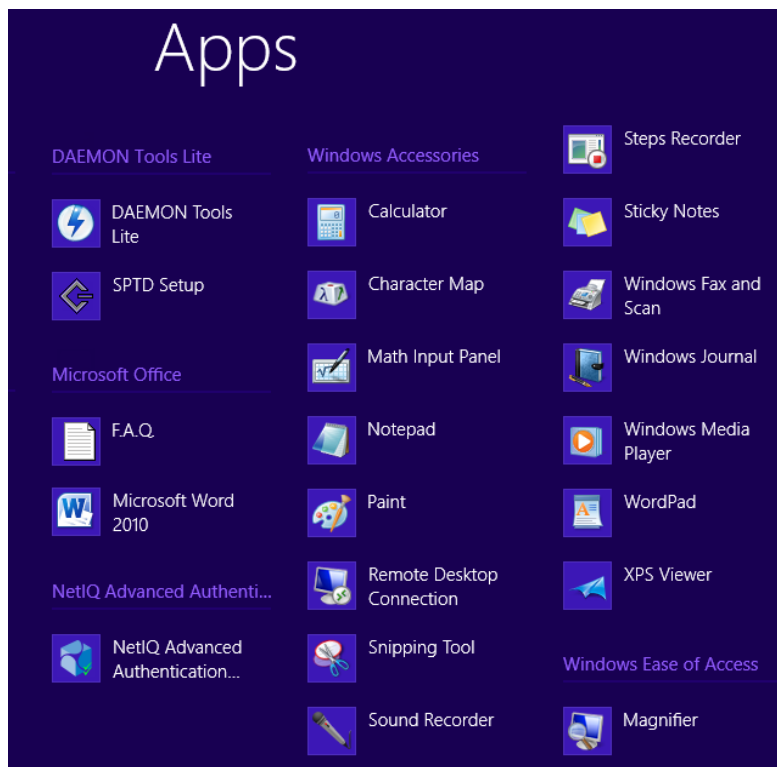


## Microsoft Windows Server 2012

Authenticator management options are available in the **Authenticators** window.

**i** The **Authentication Wizard** window is shown at system start if there are no enrolled authenticators.

To open the **Authenticators**, in the **Search** menu select **Apps > NetIQ Advanced Authentication Framework...**

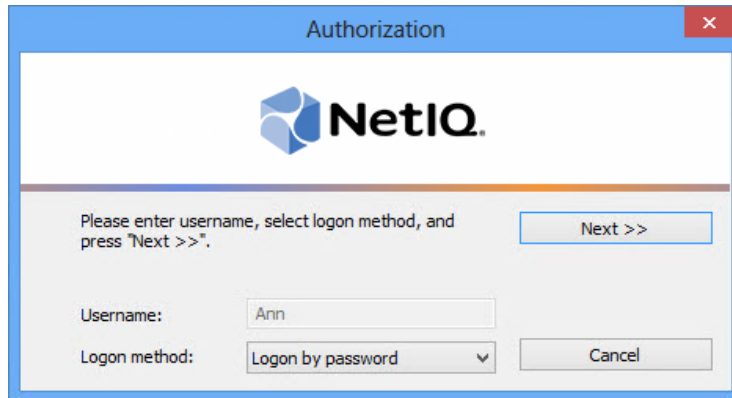


To open **Authenticators** window, user must undertake authorization procedure:

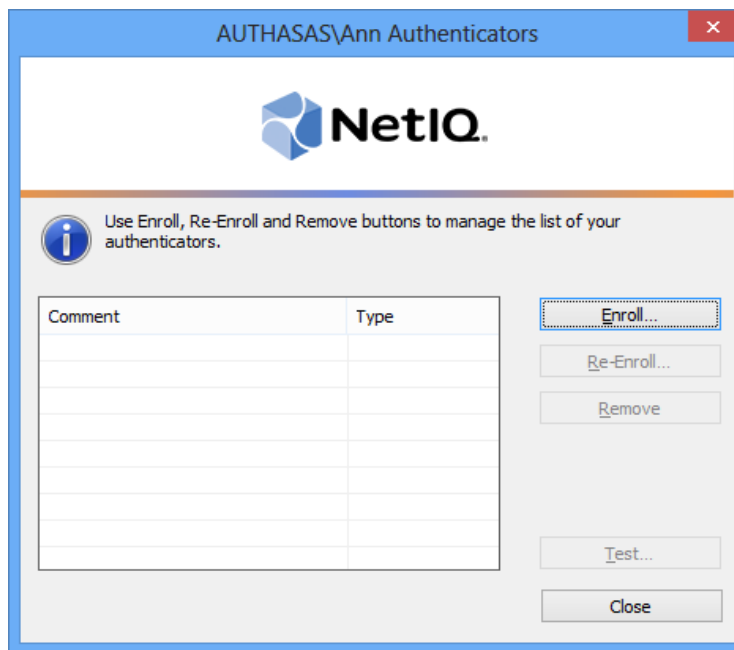
1. In the **Authorization** window, choose authentication method.

**\*** If there are no enrolled authenticators, then the only way to get authorized is **By password**. Otherwise, authentication by password will make enrollment unavailable (i.e. the button **Enroll**, **Re-enroll** and **Remove** will be greyed out).







2. Get authenticated with the selected method.
3. Once you are authenticated page for managing authenticators is opened.



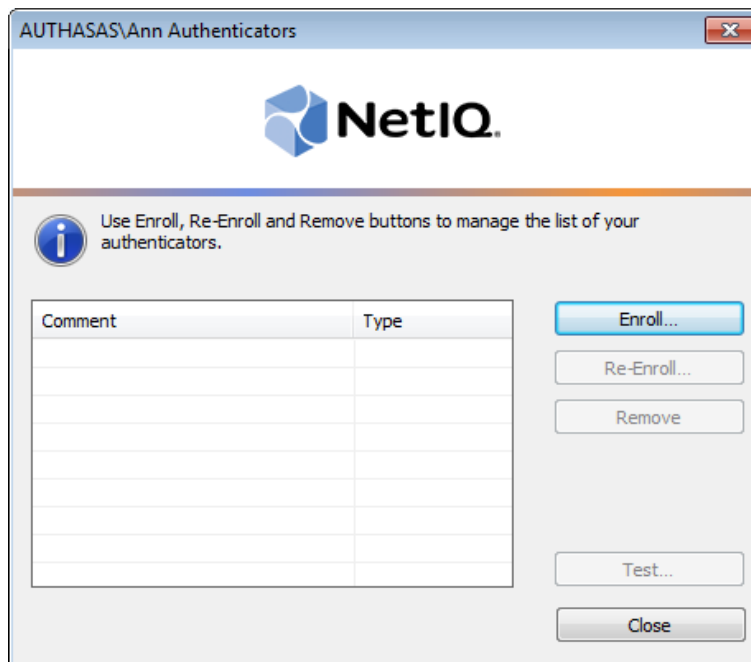
## Enrolling OATH Authenticator

 This operation may be forbidden by NetIQ administrator. In such cases the **Enroll** button in the **Authenticators** window is greyed out.

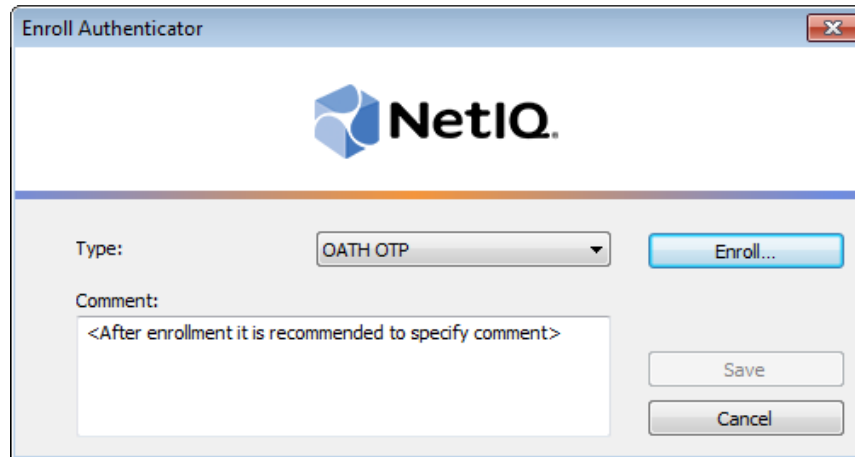
 NetIQ administrator defines the maximum number of authenticators you can have which means you cannot enroll any more authenticators once you have reached the limit.

To enroll an OATH authenticator:

1. Click the **Enroll** button in the **Authenticators** window.




2. When the **Enroll Authenticator** window appears, select **OATH OTP** from the **Type** drop-down menu, click **Enroll**.



3. The **OATH - Enroll** window is launched. Please, select an applicable type of enrollment:

- [Enrolling OATH TOTP Authenticator with NetIQ Smartphone App](#)
- [Enrolling OATH TOTP Compliant Software Tokens](#)
- [Enrolling OATH TOTP Compliant Hardware Tokens](#)
- [Enrolling OATH HOTP Compliant Hardware Tokens](#)
- [Enrolling OATH HOTP Compliant Software Tokens](#)

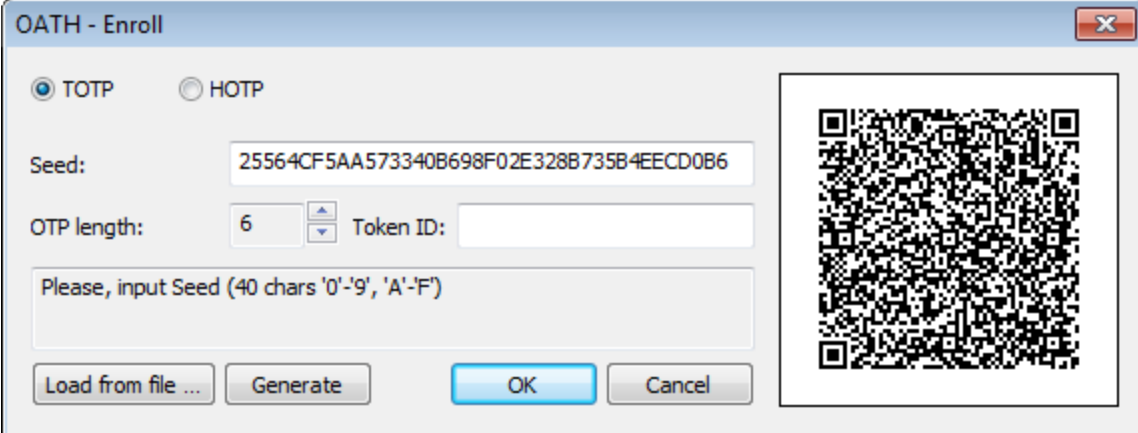
## Enrolling OATH TOTP Authenticator with NetIQ Smartphone App

 Push notifications are not supported for this type of enrollment. It is required to run NetIQ Smartphone app manually and enter the automatically generated OTP to authenticate with the selected authentication provider.


1. Select the **TOTP** authentication type.
2. Click the **Generate** button for automatic seed generation.

 The seed consists of 40 hex-digits.


3. In the **OTP length** box, select the required OTP length. The value should be between 4 and 8.
4. Leave the **Token ID** text field empty.
5. The QR code containing the template data will be launched.



6. Run NetIQ Smartphone app and authorize.
7. Tap the **Scan QR to load config** button to scan the QR code containing the template data.

 The QR code containing the template data can be scanned by using only the NetIQ Smartphone app.

8. Click **OK**.
9. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional. Click **Save**.

 Entering and editing of comments may be forbidden by the system administrator.

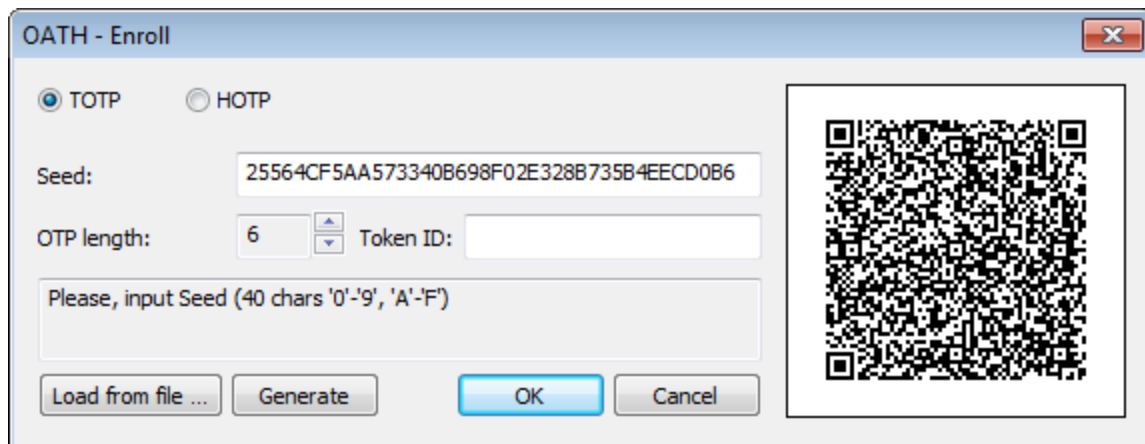
10. A new authenticator is created and visible in the list of authenticators in the **Authenticators** window.

## Enrolling OATH TOTP Compliant Software Tokens

1. Select the **TOTP** authentication type.
2. Enter seed to the **Seed** text field. Select one of the following options:
  - Click the **Generate** button for automatic seed generation. Run any third-party OATH compliant software token and authorize (if applicable). Enter the generated seed to an applicable text field of the token.
  - Generate seed on any third-party OATH compliant software and enter it to the **Seed** text field of the **OATH - Enroll** window.

**i** The seed should consist of 40 hex-digits.

3. In the **OTP length** box, select the required OTP length. The value should be between 4 and 8.
4. Leave the **Token ID** text field empty.



5. Click **OK**.
6. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional. Click **Save**.

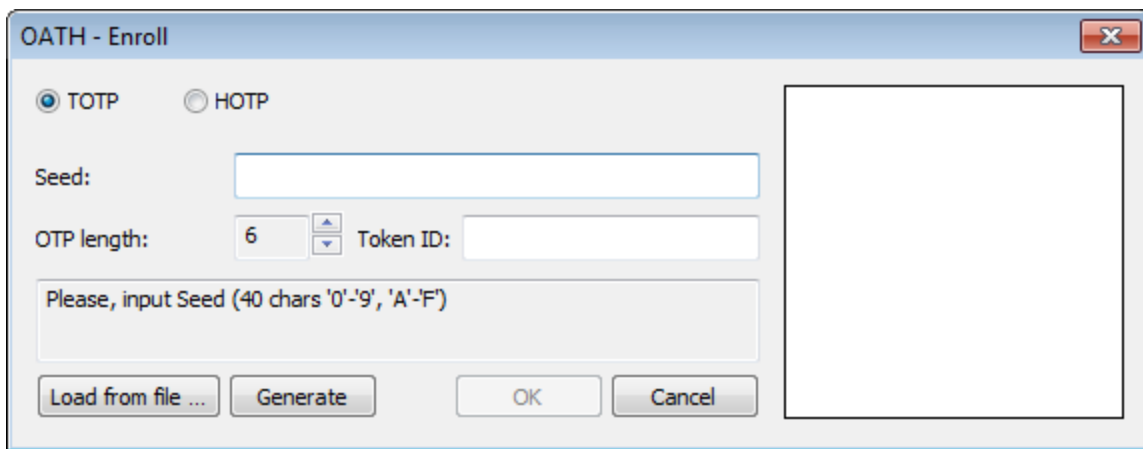
**\*** Entering and editing of comments may be forbidden by the system administrator.

7. A new authenticator is created and visible in the list of authenticators in the **Authenticators** window.

## Enrolling OATH TOTP Compliant Hardware Tokens

- \* This type of enrollment is supported only by ActivIdentity/HID OATH TOTP compliant tokens.
- \* It is easier and more convenient to enroll OATH TOTP compliant hardware tokens using NetIQ Web Enrollment Wizard. Contact NetIQ administrator for assistance.

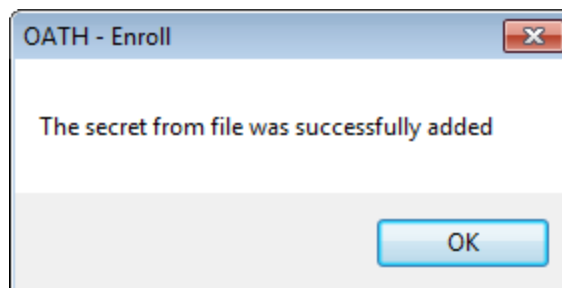
1. Select the **TOTP** authentication type.
2. Click the **Load from file** button in the **OATH - Enroll** window.




3. Select an applicable **.pskc** file.

- \* The **.pskc** file should be unencrypted and contain information only for one token.

4. The secret from file is successfully added. Click **OK**.




5. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional. Click **Save**.

 Entering and editing of comments may be forbidden by the system administrator.


6. A new authenticator is created and visible in the list of authenticators in the **Authenticators** window.




## Enrolling OATH HOTP Compliant Hardware Tokens

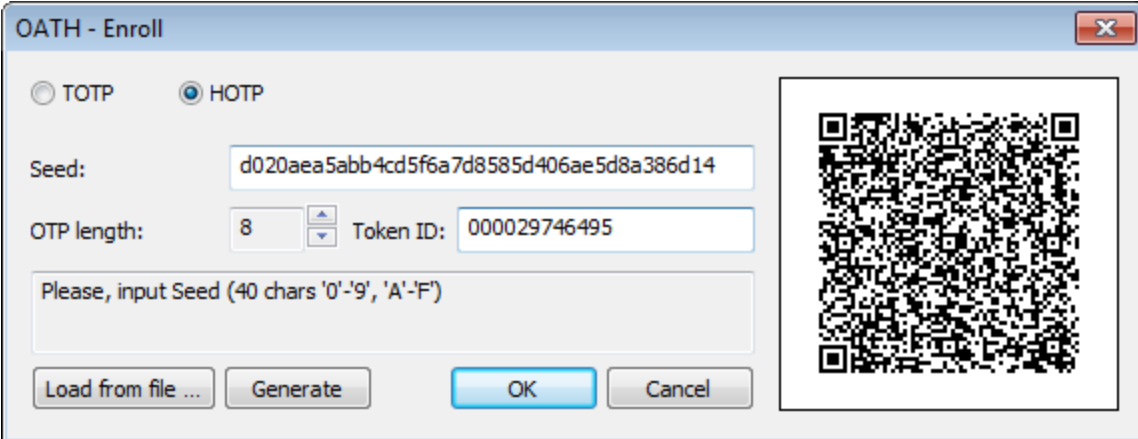
 It is easier and more convenient to enroll OATH HOTP compliant hardware tokens using NetIQ Web Enrollment Wizard. Contact NetIQ administrator for assistance.

1. Select the **HOTP** authentication type.
2. Enter the Secret Key of your token to the **Seed** text field.

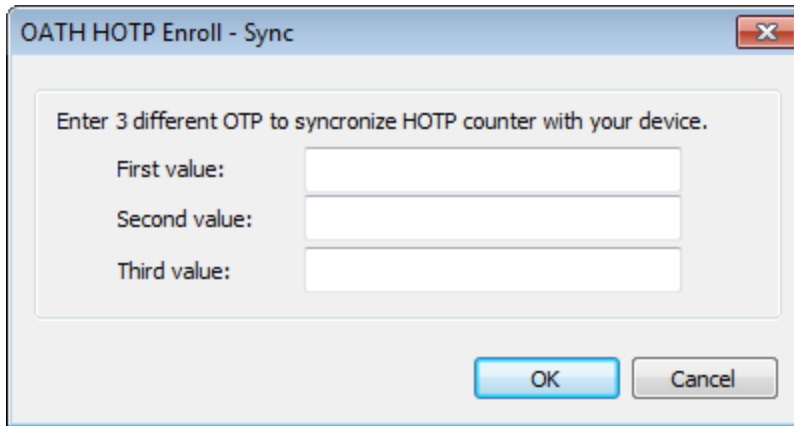
 The seed should consist of 40 hex-digits.

3. In the **OTP length** box, select OTP length according to token's setting.
4. Enter the token ID to the **Token ID** text field.

 To determine the Token ID for YubiKey, it is required to open Notepad and press the YubiKey button 3-4 times. The common beginning for all input values is the Token ID. OTP is the last 6 or 8 digits of the input value.



5. Click **OK**.
6. Enter 3 different OTP to synchronize HOTP counter with your device. Click **OK**.



\* If there is specified the wrong seed or token ID, the following error will be displayed:  
*"Failed to find correct HOTP counter".*

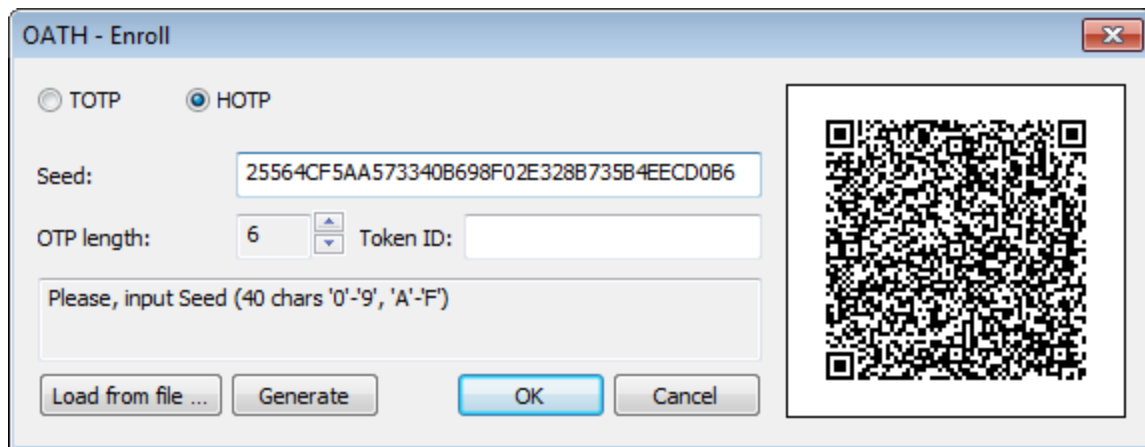
7. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional.  
Click **Save**.

\* Entering and editing of comments may be forbidden by the system administrator.


8. A new authenticator is created and visible in the list of authenticators in the **Authenticators** window.

## Enrolling OATH HOTP Compliant Software Tokens

1. Select the **HOTP** authentication type.
2. Enter seed to the **Seed** text field. Select one of the following options:
  - Click the **Generate** button for automatic seed generation. Run any third-party OATH compliant software token and authorize (if applicable). Enter the generated seed to an applicable text field of the token.
  - Generate seed on any third-party OATH compliant software and enter it to the **Seed** text field of the **OATH - Enroll** window.
3. In the **OTP length** box, select the required OTP length. The value should be between 4 and 8.
4. Leave the **Token ID** text field empty.




5. Click **OK**.
6. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional. Click **Save**.

 Entering and editing of comments may be forbidden by the system administrator.

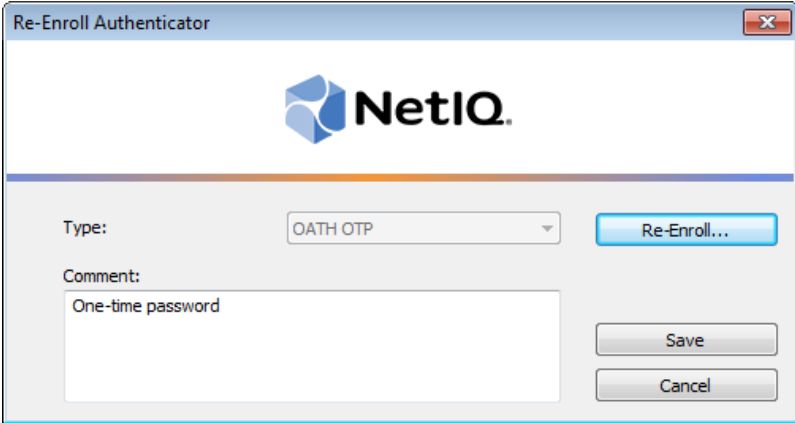
7. A new authenticator is created and visible in the list of authenticators in the **Authenticators** window.

## Re-enrolling OATH Authenticator

 This operation may be forbidden by NetIQ administrator. In such cases the **Re-Enroll** button in the **Authenticators** window is greyed out.

In order to re-enroll a created OATH authenticator:

1. Select **OATH OTP** in the list of authenticators, click **Re-Enroll** in the **Authenticators** window.
2. Click **Re-Enroll** in the **Re-Enroll Authenticator** window.



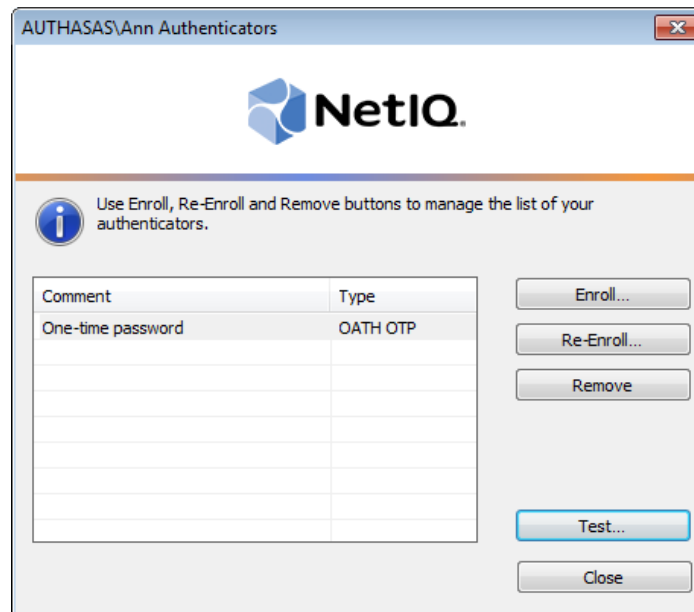
The screenshot shows a dialog box titled "Re-Enroll Authenticator" with the NetIQ logo. It contains a "Type:" dropdown menu with "OATH OTP" selected, a "Re-Enroll..." button, a "Comment:" text area with "One-time password" entered, and "Save" and "Cancel" buttons at the bottom right.

3. Fulfill the steps as during your initial enrollment process.

## Testing OATH Authenticator

To test a created OATH authenticator:

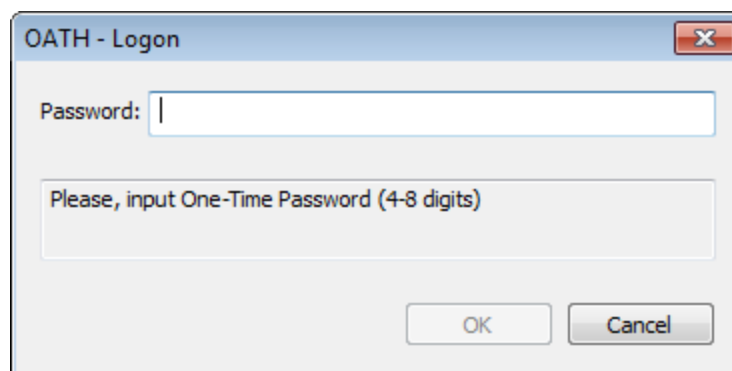
1. Click **Test** in the **Authenticators** window.




**i** Testing can also be performed in the **Enroll authenticator** and **Re-enroll authenticator** windows.

**i** Instead of standard passwords, 6-digits one-time password is used.

2. For TOTP OTP, enter One-Time Password that you receive from NetIQ Smartphone Authenticator. Click **OK**.



For HOTP OTP, enter One-Time Password that is automatically generated by smartphone or hardware token.

 For YubiKey, insert the token into the port and press its button.


3. When a confirmation message saying: "*Authenticators match*" appears, click **OK**.





4. When authenticators do not match an error message appears. Click **OK**.



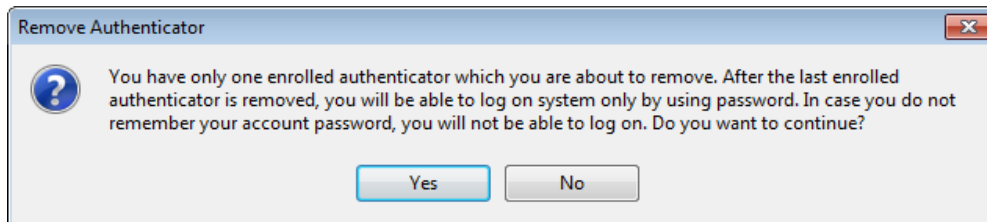
## Removing OATH Authenticator

 This operation may be forbidden by the NetIQ administrator. In such cases the **Remove** button in the **Authenticators** window is greyed out.

 If you are allowed to remove your authenticator, don't do this just because you don't like your current authenticator. Instead, you can re-enroll it.

 Do not remove the only authenticator you have. If you have no authenticators, you can log on with your password only. If a random password was generated for your account and you have removed the only authenticator, you cannot log on in any way.

NetIQ Advanced Authentication Framework™ prevents you from accidentally removing your only authenticator by showing the following dialog:




If you removed the only authenticator and do not know your password, contact the system administrator.

# Troubleshooting

In this chapter:

- [Cannot Enroll Authenticator](#)
- [One-Time Password Doesn't Work](#)

 This chapter provides solutions for known issues. If you encounter any problems that are not listed here, please contact the technical support service.

## Before contacting the support service:

We strongly request that you give a possibly detailed description of your problem to the support technicians and attach logs from the faulty computer. To obtain the logs, use the LogCollector.exe tool (\Tools\LogCollector). Follow the steps below:

1. Copy LogCollector.exe to the local C:\ disk on the faulty computer.

 The tool may not work from a network drive.

2. Run LogCollector.exe.

3. In the dialog that opens, click **Enable all**. As a result, all items in the **Debugged components** section are selected. Close the dialog.

4. Reproduce the steps that caused the problem.

5. Run LogCollector.exe. again and click **Save logs**.

Save the logs to archive.



## Cannot Enroll Authenticator

### Description:

Authenticator is not enrolled because:

- a. The **Type** list in the **Enroll Authenticators** window is empty or OATH authenticator type is absent.
- b. The **Enroll** button in the **Authenticators** window is greyed out.

### Cause:

- a. The OATH authenticator type is not supported (no proper authentication provider is installed).
- b. The operation is forbidden or you have reached the limit on authenticators number.

### Solution:

- a. Contact NetIQ administrator.
- b. No authenticators can be added. For more information, contact NetIQ administrator.

## One-Time Password Doesn't Work

### Description:

The generated one-time password doesn't work.

### Cause:

- a. Group policy is set on the other password generating period.
- b. The password time is out.
- c. Workstation time differs from time of Authenticore Server more than N minutes; N depends on **TOTP checking window** setting.

### Solution:

- a. Check group policy settings and make changes in your mobile device token application.
- b. Try another password.
- c. Synchronize Workstation and Server time.

# Index

---

## A

Authentication 1, 3-5, 8, 23  
Authenticator 3, 5, 8, 12, 14-15, 18-19, 25

## C

Client 3  
Control 5, 12, 14-15, 18-19

## E

Enroll 8, 20-21, 24-25

## G

Generate 12, 14, 19

## H

Hardware 11

## K

Key 17

## L

Logon 3

## M

Microsoft Windows Server 2012 5, 8

## O

OATH 1, 3-5, 10, 12, 14-15, 17, 19-21, 23, 25  
One-time Password 4  
OTP 4, 10, 12, 14, 20

## P

Password 4, 21, 24, 26

## R

Re-enroll 21  
Remove 8, 23

---

**S**

Server 26  
Software 11

**T**

Token 12, 14, 17, 19  
TOTP 4, 11-12, 14-15, 21, 26

**U**

User 5

**W**

Windows 7 5  
Workstation 26