NetIQ Advanced Authentication Framework

OATH Authentication Provider User's Guide

Version 5.1.0

© *NetIQ*

Table of Contents

1

Table of Contents **2**

Introduction **3**

About This Document 3

OATH Authenticator Overview **4**

Managing OATH Authenticator **5**

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 5

Microsoft Windows XP/Microsoft Windows Server 2003 7

Microsoft Windows 8/Microsoft Windows Server 2012 10

Enrolling OATH Authenticator 12

Re-enrolling OATH Authenticator 15

Testing OATH Authenticator 17

Removing OATH Authenticator 19

Troubleshooting **20**

Cannot Enroll Authenticator 21

One-Time Password Doesn't Work 22

Index **23**

© NetIQ

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.

© *NetIQ*

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.

© NetIQ

Managing OATH Authenticator

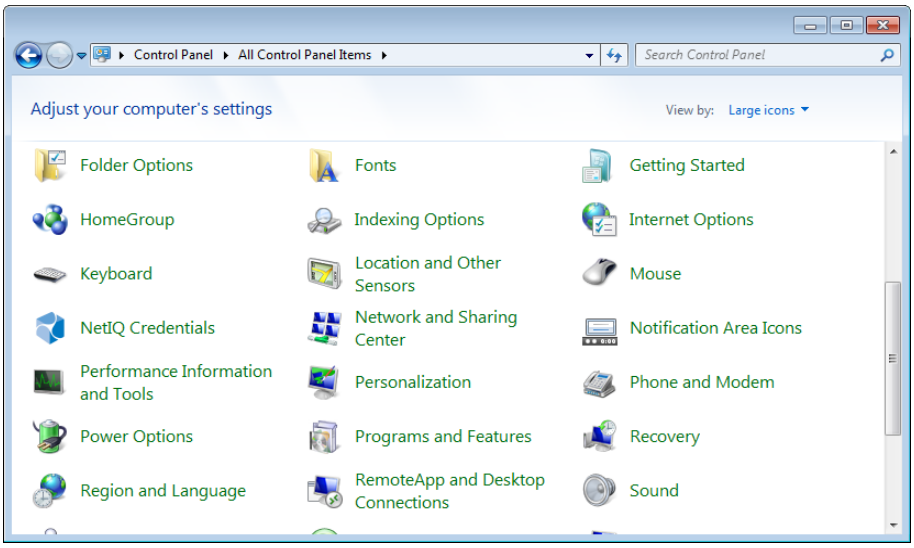
Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

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

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

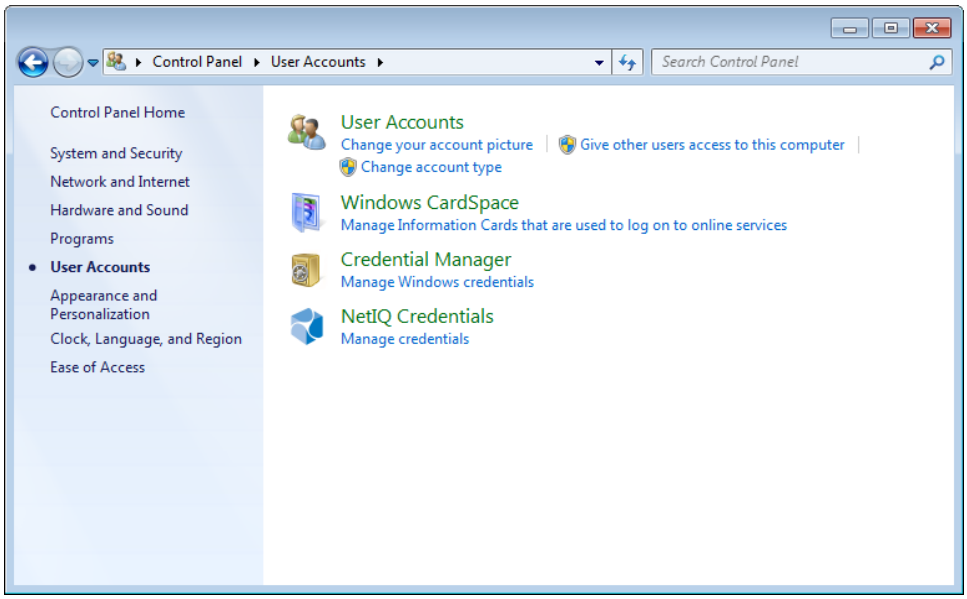
To open the **Authenticator**s window from **Control Panel**:

• In classic view of control panel select NetIQ Credentials item.



• In control panel by categories select **User Accounts** > **NetIQ Credentials**.

© *NetIQ*

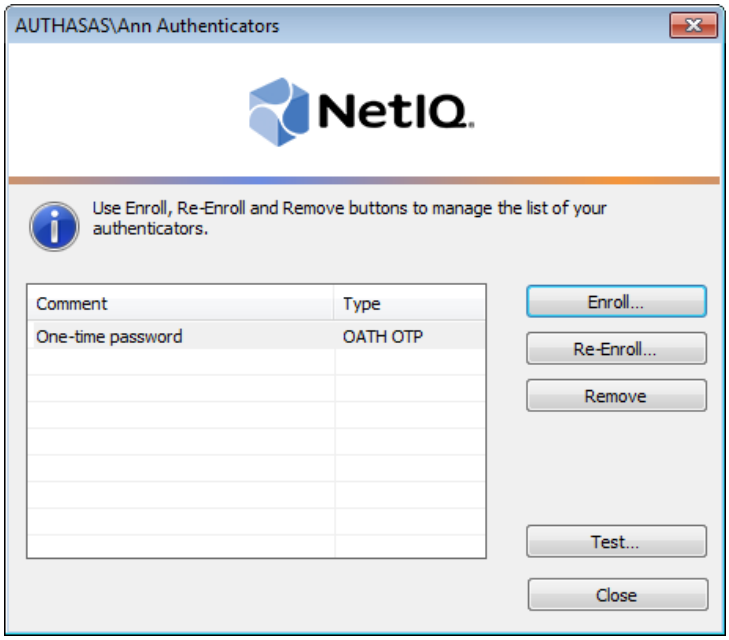


To open **Manage Authenticators** window, user must undertake authorization procedure:

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.



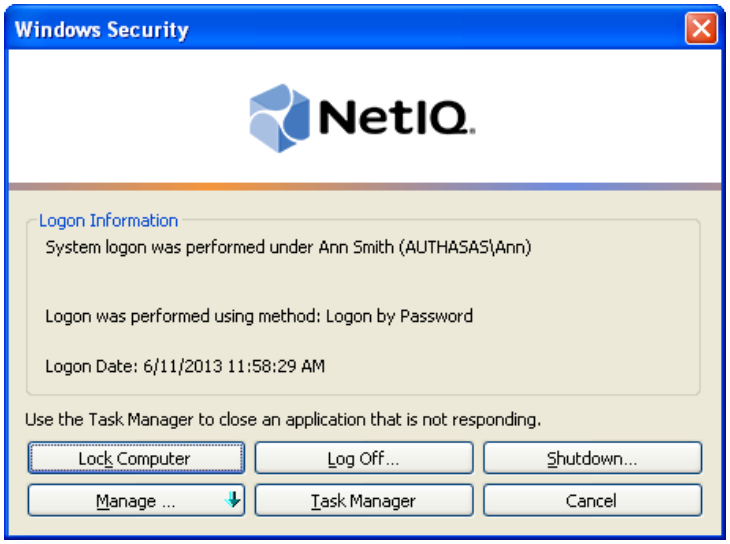
© NetIQ

Microsoft Windows XP/Microsoft Windows Server 2003

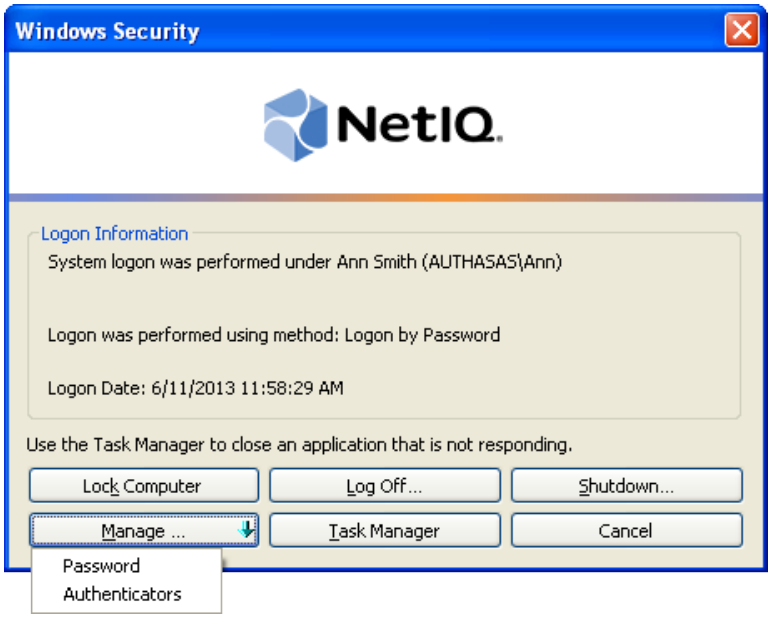
Authenticator management options are available in the **Authenticators** window.

To open the **Authenticators** window:

1. From your desktop, press **[Ctrl]+[Alt]+[Del]**. The **Windows Security** window is displayed.

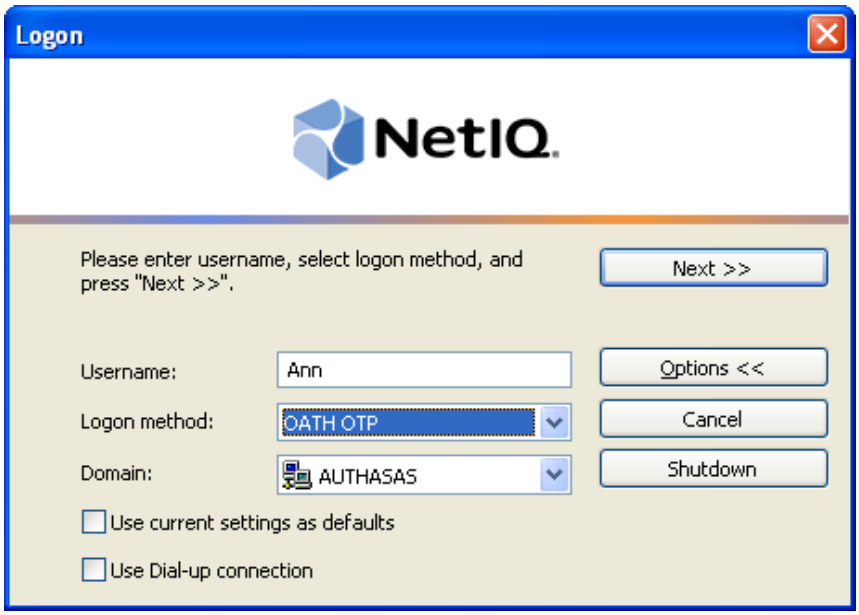


2. Click **Manage** and select **Authenticators**.



© NetIQ

3. The **Authorization** window is displayed.



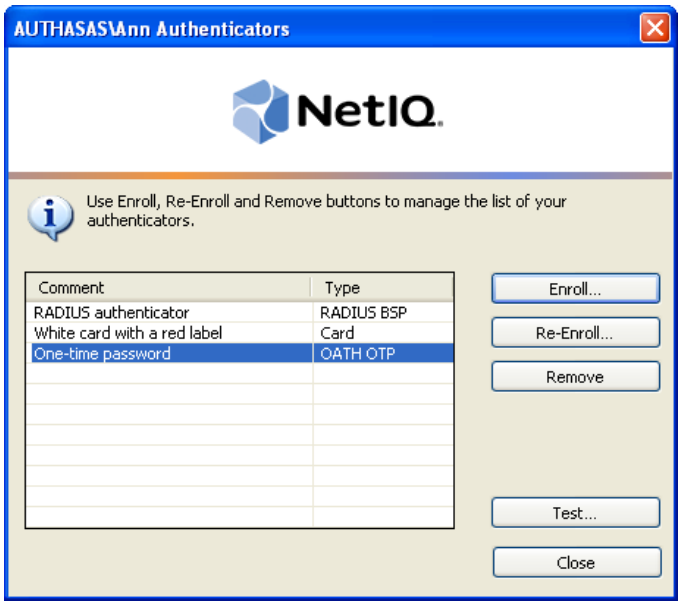
• From the **Logon method** list, select a logon method (an authenticator type or **Logon by password**).

• Click **Next**.

To be able to add, re-enroll or remove an authenticator, you must use an authenticator as logon method.

After successful authentication the **Authenticators** window is displayed.

© *NetIQ*


AUTHASAS\Ann Authenticators
NetIQ
Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.
Comment
Type
RADIUS authenticator
RADIUS BSP
White card with a red label
Card
One-time password
OATH OTP
Enroll...
Re-Enroll...
Remove
Test...
Close

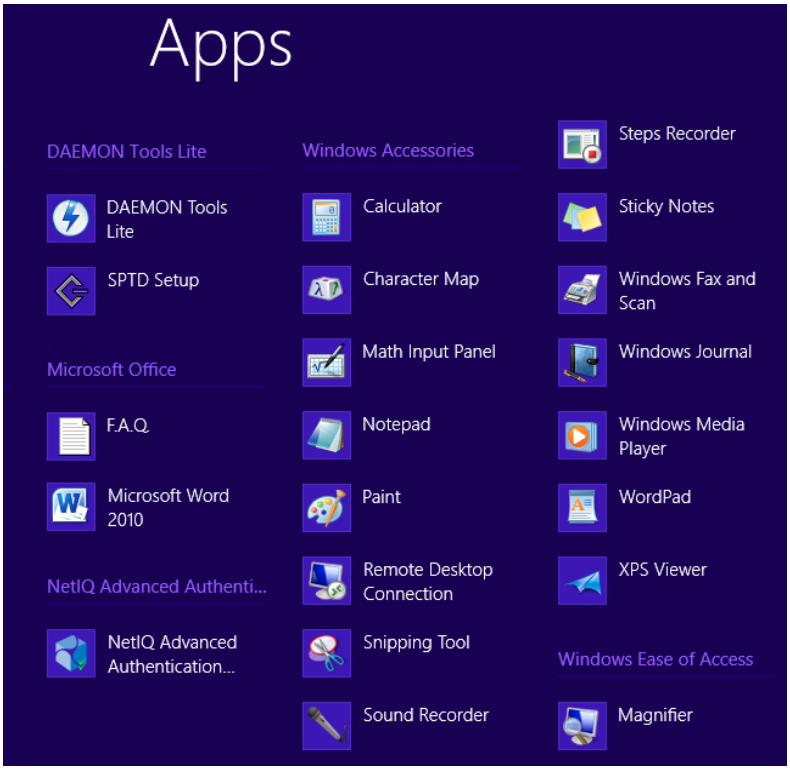
© NetIQ

Microsoft Windows 8/Microsoft Windows Server 2012

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

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...**.

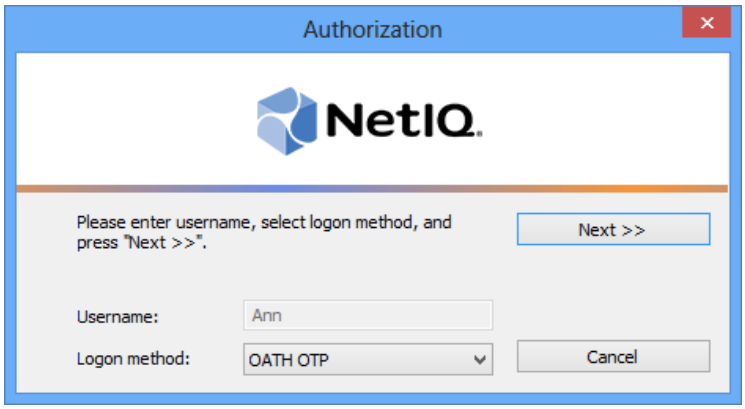


To open **Manage Authenticator**s window, user must undertake authorization procedure:

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

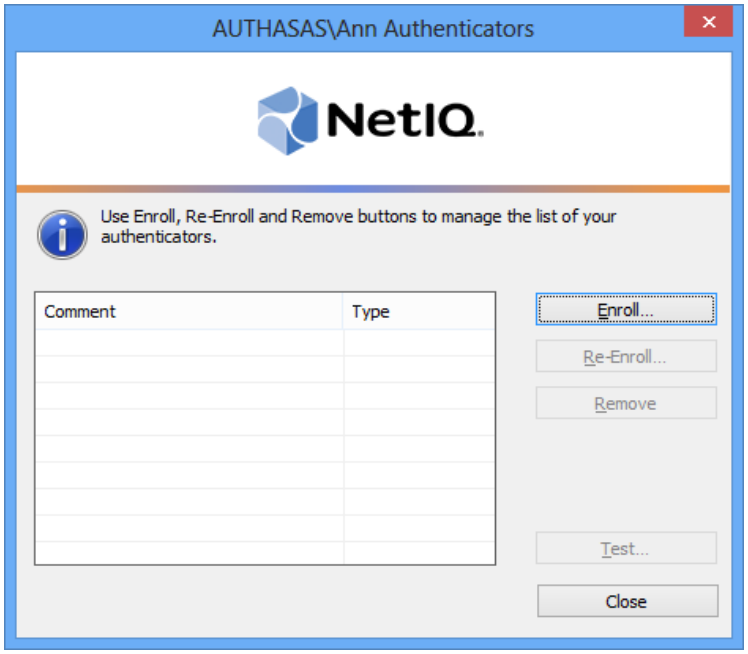
If there are no enrolled authenticators, then the only way to get authorized is **By password**. Otherwise, authentication by password will make enrollment unavailable (i.e. the button **Enroll, Re-enroll** and **Remove** will be greyed out).

© *NetIQ*



2. Get authenticated with the selected method.

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



© NetIQ

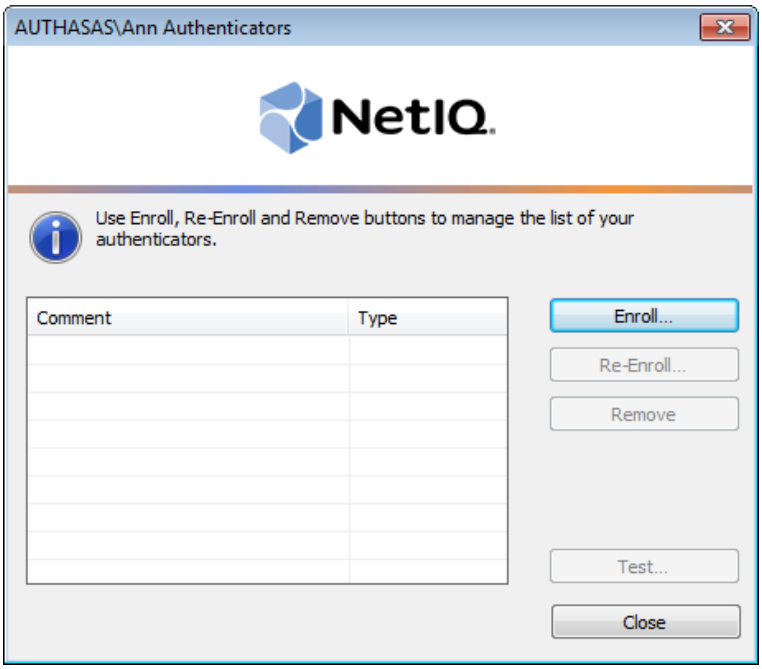
Enrolling OATH Authenticator

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 canhave which means you cannot enroll any more authenticators once you have reachedthe limit.

To enroll an OATH authenticator

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



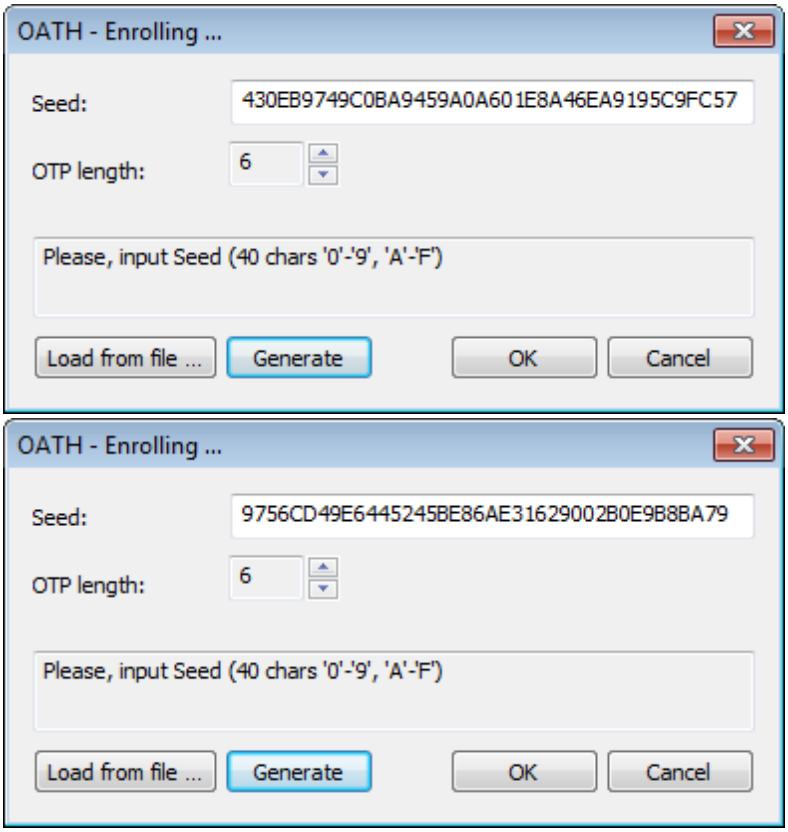
2. When the **Enroll Authenticator** window appears, select **OATH OTP** from the **Type** drop-down menu, click **Enroll...**.

© *NetIQ*

3. In the **Enrolling** window, press the **Generate** button for automatic seed generation, or type it manually using the stated symbols. Add a new token on your mobile device using this seed. Press **OK**.

You can use free mobile device token applicationsfor generating passwords:

• for iOS;
• for Android.

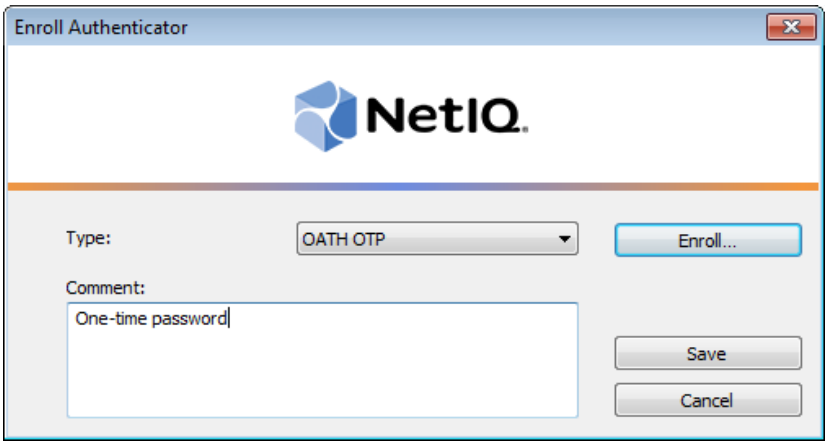


© *NetIQ*

The seed should consist of 40 hex-digits.

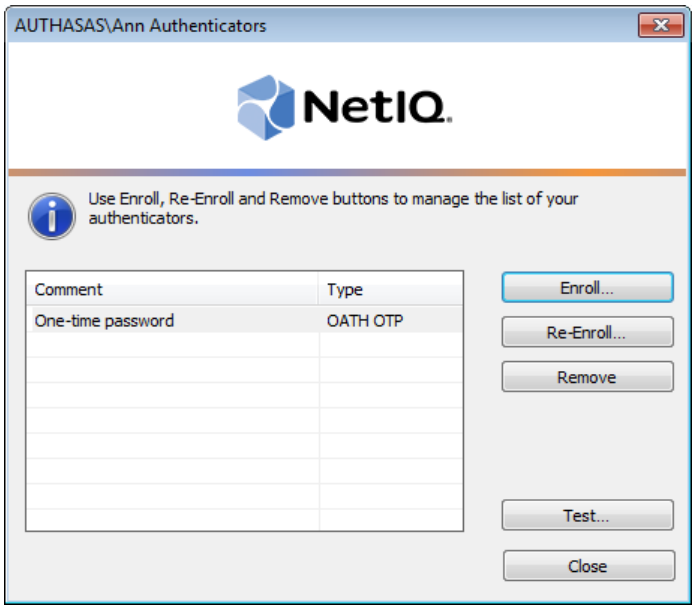
When the PIN Required Policy is enabled, the user should input OTP together with a PIN code in one field. If domain password is used instead of PIN, then the user should input OTP together with a domain password in one field.

4. 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.

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



© NetIQ

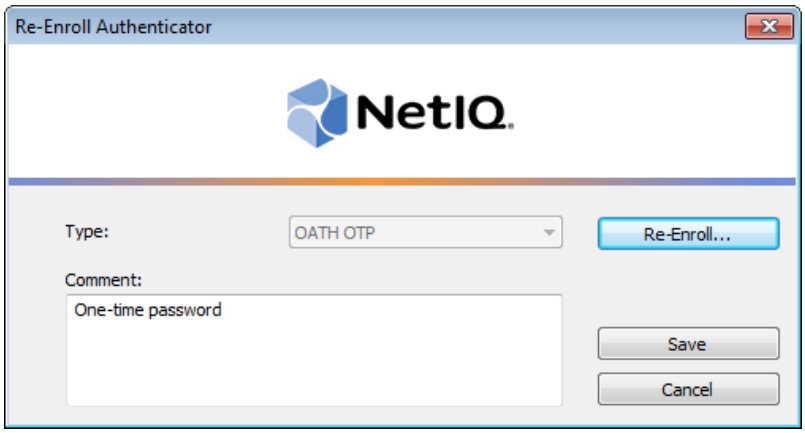
Re-enrolling OATH Authenticator

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

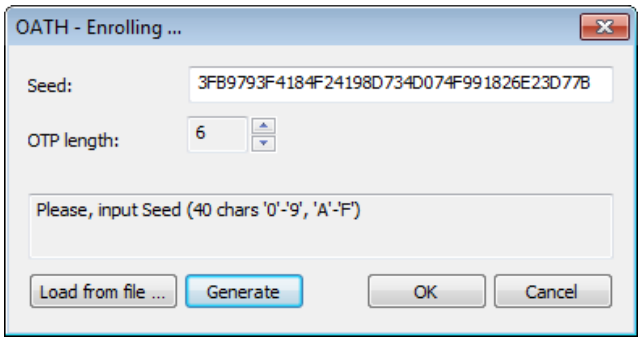
In order to re-enroll a created OATH authenticator

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

2. Click **Re-Enroll...** in the **Re-Enroll Authenticators** window.

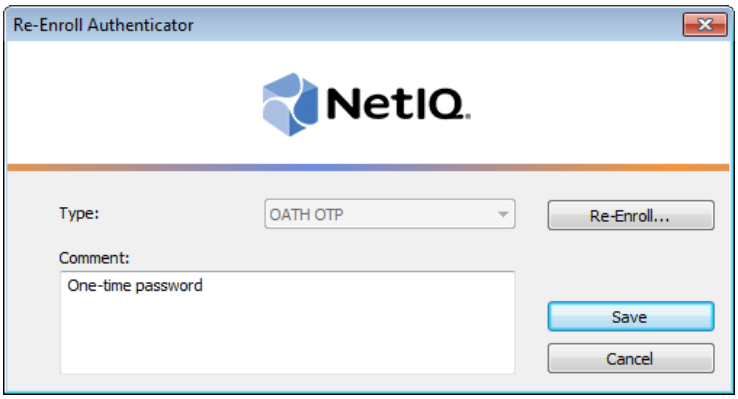


3. Generate or enter the new seed. Click **OK**.



4. Click **Save** in the **Re-Enroll Authenticator** window.

© NetIQ

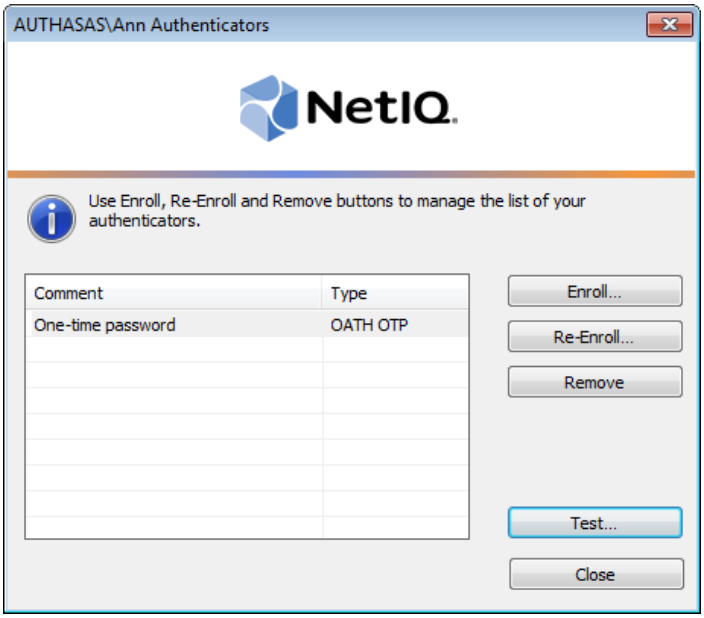

Re-Enroll Authenticator
NetIQ
Type:
OATH OTP
Re-Enroll...
Comment:
One-time password
Save
Cancel

© NetIQ

Testing OATH Authenticator

To test a created OATH authenticator

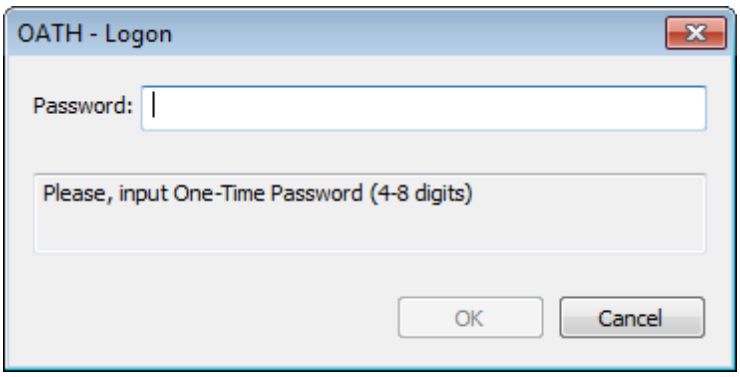
1. Click **Test...** in the **Authenticators** window.



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

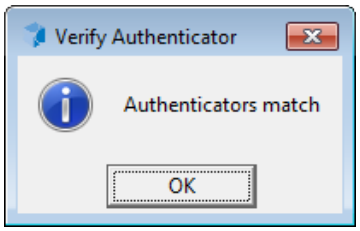
Instead of standard passwords, 6-digits one-time password is used.

2. In the **Verifying** window enter **Password** that you receive from Mobile device token application, click **OK**.



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

© *NetIQ*



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

© *NetIQ*

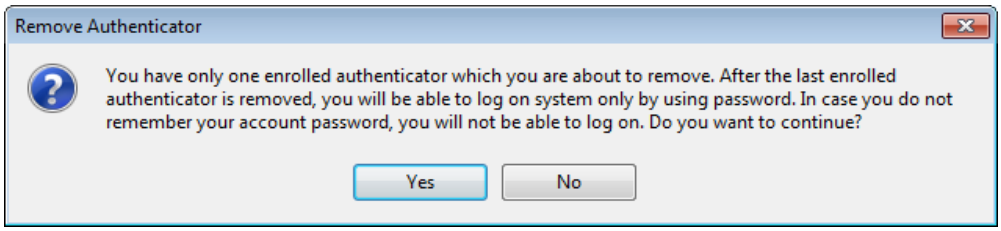
Removing OATH Authenticator

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.

© NetIQ

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.

© NetIQ

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.

© *NetIQ*

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.

© *NetIQ*

Index

A

Authentication 1, 3-5, 10, 19
Authenticator 3-5, 7, 10, 21

C

Client 3
Control 5, 14

E

Enroll 10, 15, 17, 20-21

G

Generate 13, 15

L

Logon 3, 8

M

Manage 6-7, 10

O

OATH 1, 3-5, 12, 15, 17, 19, 21
One-time Password 4
OTP 4, 12, 15

P

Password 4, 17, 20, 22
PIN 14

R

Re-enroll 17
Remove 10, 19

S

Server 22

T

TOTP 4, 22

© *NetIQ*

U

User 5

W

Windows 7
Windows 8 10
Windows Vista 5
Windows XP 7
Workstation 22

© *NetIQ*