NetIQ Advanced Authentication Framework

OATH Authentication Provider User's Guide

Version 5.1.0

Table of Contents

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.

ℹ **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 2003/2003 R2
- Microsoft Windows Server 2012

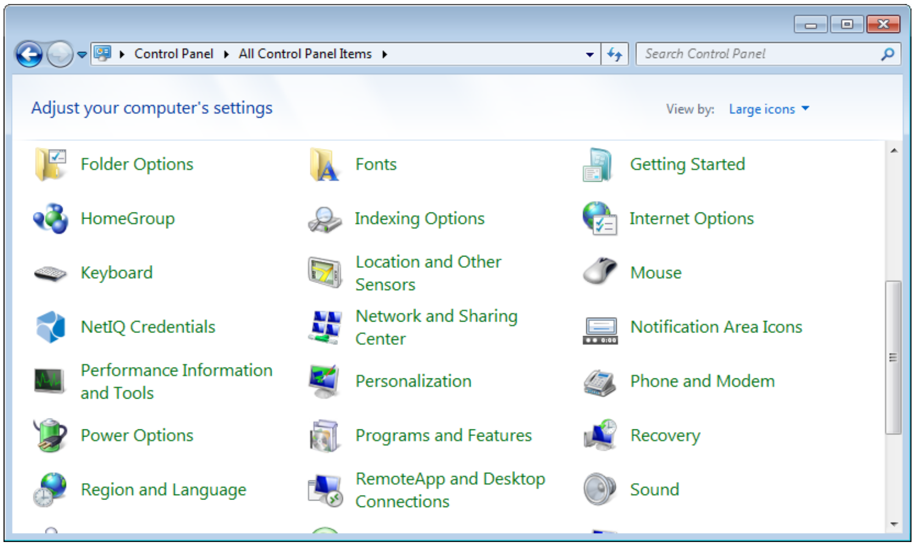
Microsoft Windows 7/Microsoft Windows Server 2008 R2

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

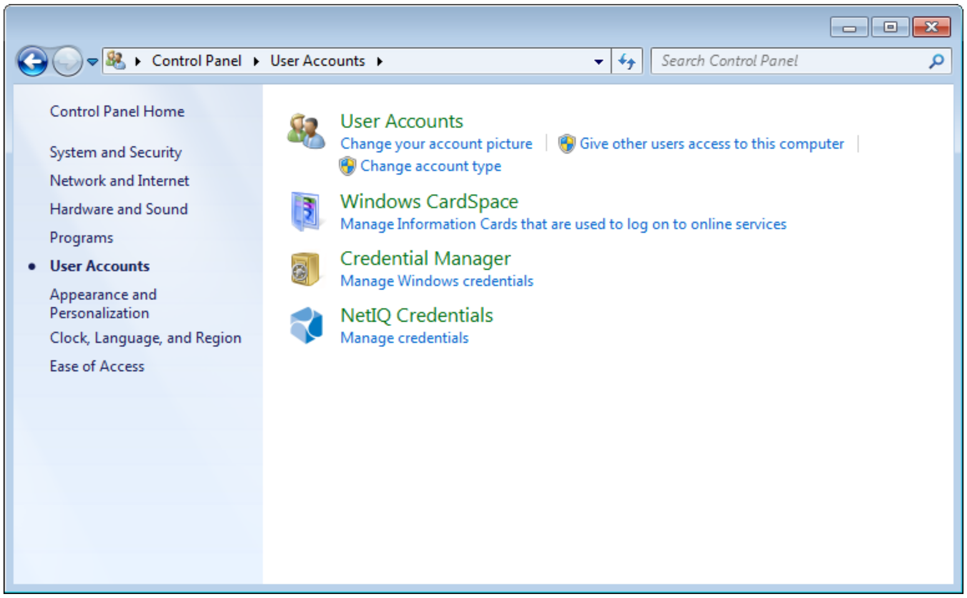
ℹ The **Authentication Wizard** window is shown at system start if there are no enrolled authenticators.

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

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

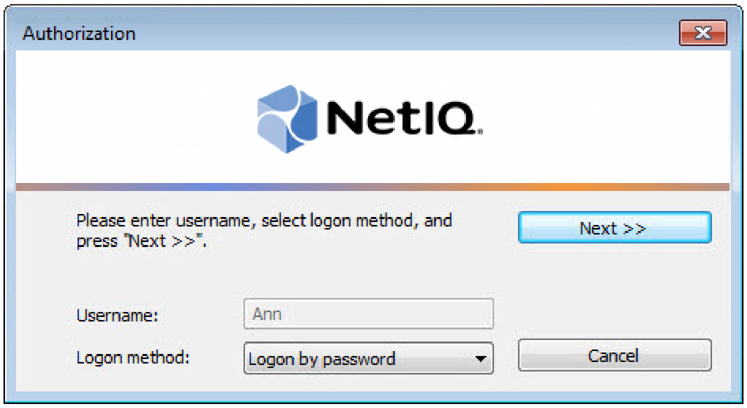


- In **Control Panel** by categories select **User Accounts > NetIQ Credentials**.


Control Panel ▸ User Accounts ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
User Accounts
Change your account picture
Give other users access to this computer
Change account type
Windows CardSpace
Manage Information Cards that are used to log on to online services
Credential Manager
Manage Windows credentials
NetIQ Credentials
Manage credentials

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

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



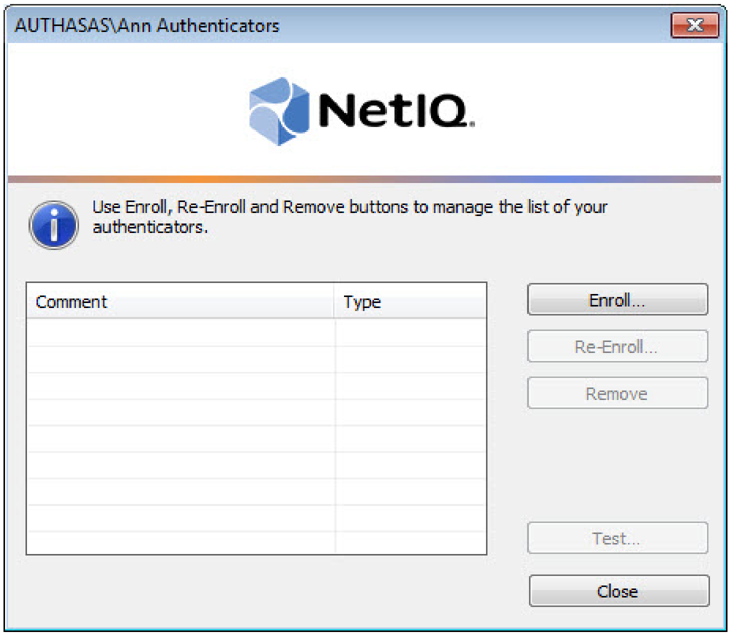
Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Logon by password

2. Get authenticated with the selected method.

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



Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

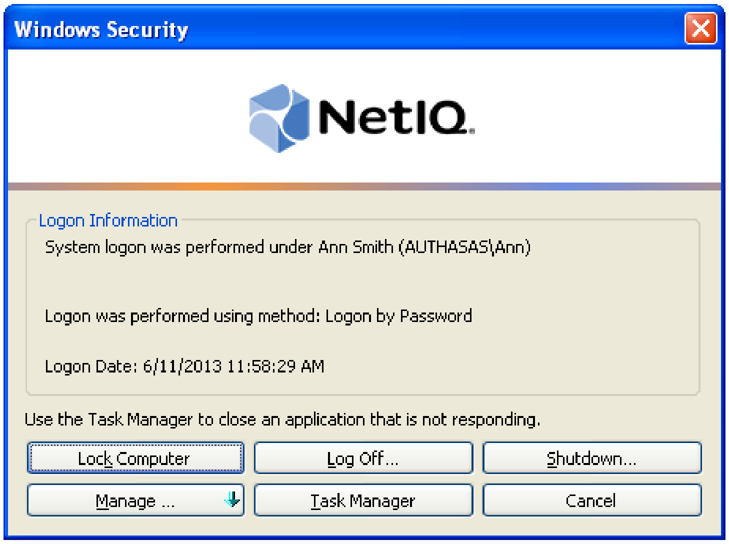
Comment	Type

Microsoft Windows Server 2003/2003 R2

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.



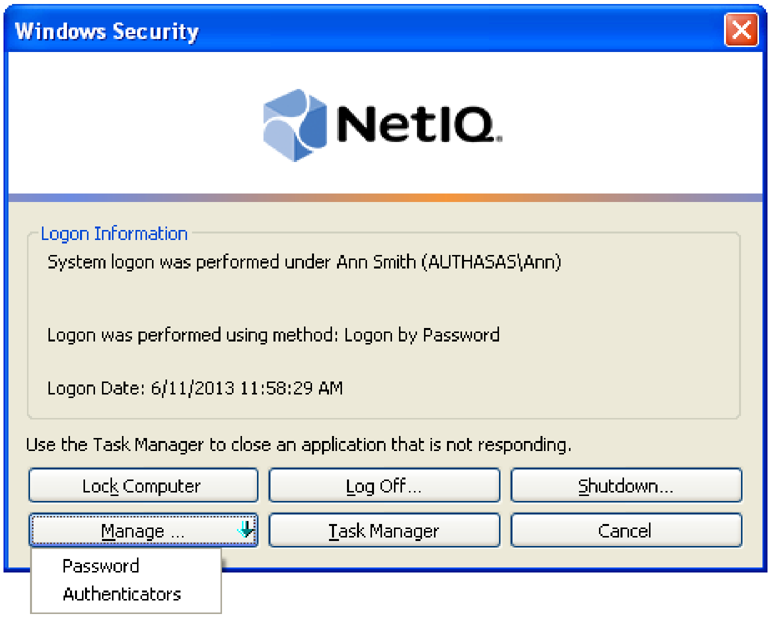
System logon was performed under Ann Smith (AUTHASAS\Ann)

Logon was performed using method: Logon by Password

Logon Date: 6/11/2013 11:58:29 AM

Use the Task Manager to close an application that is not responding.

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



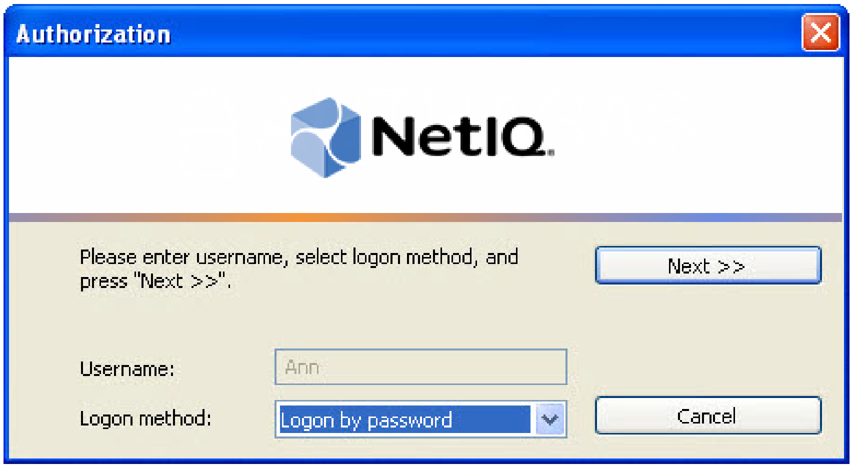
System logon was performed under Ann Smith (AUTHASAS\Ann)

Logon was performed using method: Logon by Password

Logon Date: 6/11/2013 11:58:29 AM

Use the Task Manager to close an application that is not responding.

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



Authorization

Please enter username, select logon method, and press "Next >>".

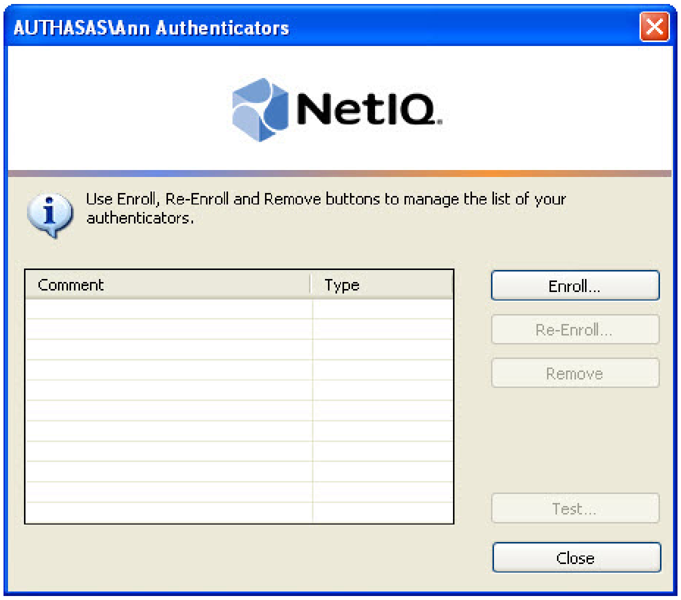
Username: Ann

Logon method: Logon by password

- 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 should use an authenticator as logon method.

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



AUTHASAS\Ann Authenticators

Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

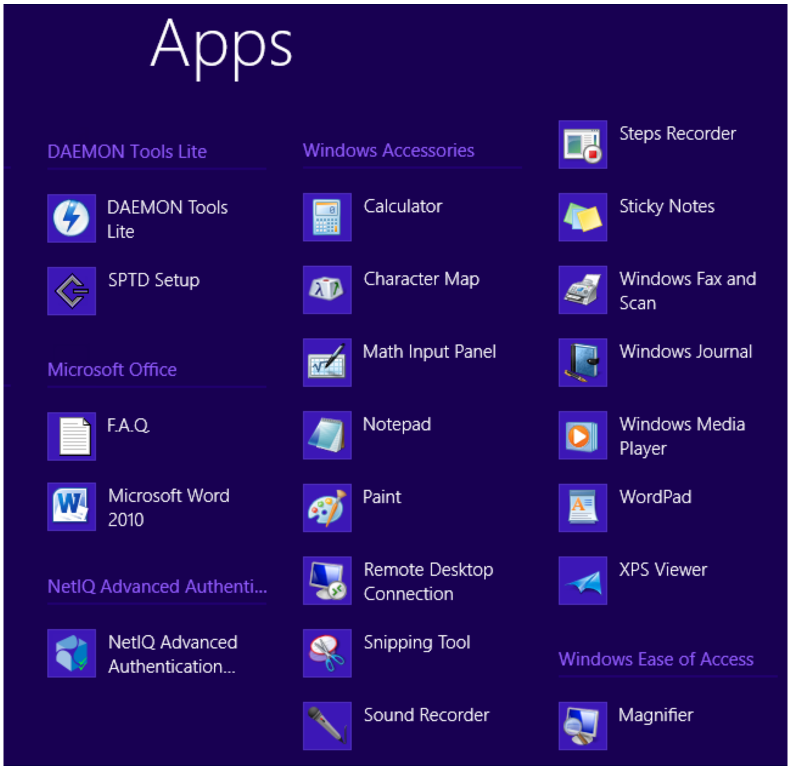
Comment	Type

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.

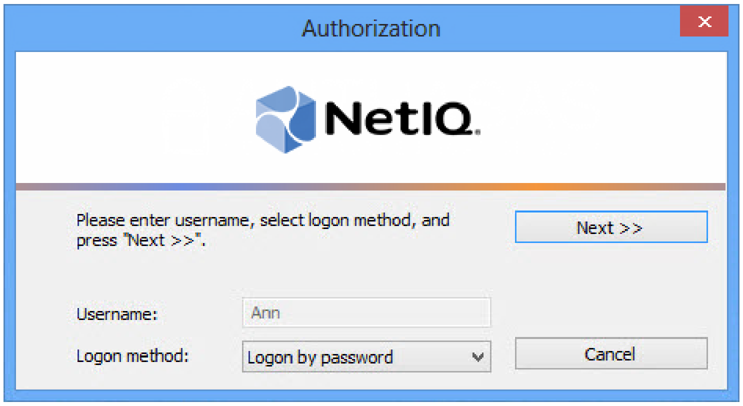
To open the **Authenticators**, in the **Search** menu select **Apps** > **NetIQ Advanced Authentication Framework...**.



To open **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).



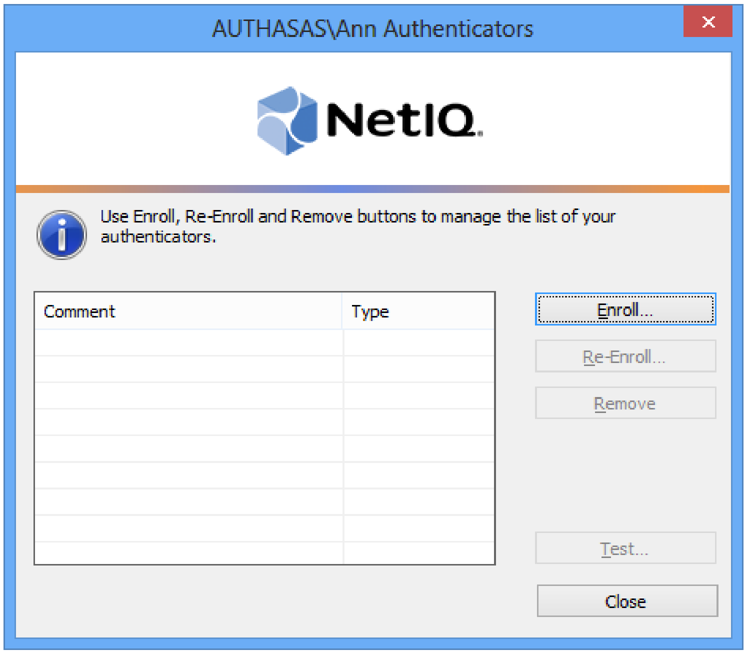
Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Logon by password

2. Get authenticated with the selected method.

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



Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type

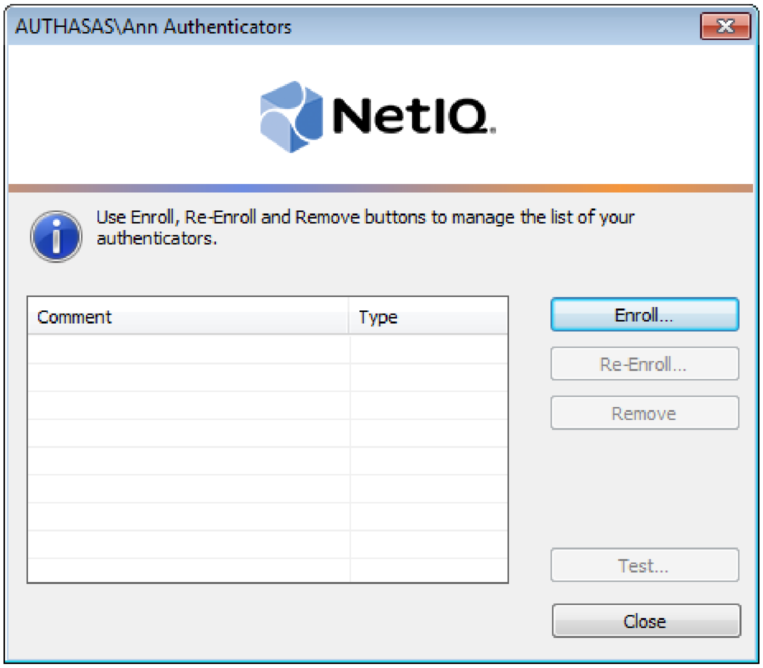
Enrolling OATH Authenticator

✱ 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.

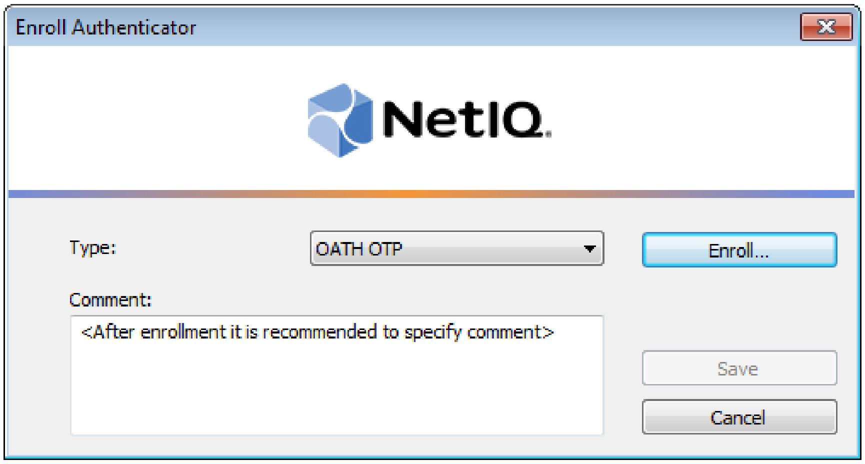
To enroll an OATH authenticator:

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



Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

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



Type: OATH OTP

Comment: <After enrollment it is recommended to specify comment>

3. In the **OATH - Enrolling** window, select the required type of OTP authentication:

- TOTP
- HOTP

TOTP Enrollment

1. Enter seed to the **Seed** text field. Use one of the following methods:

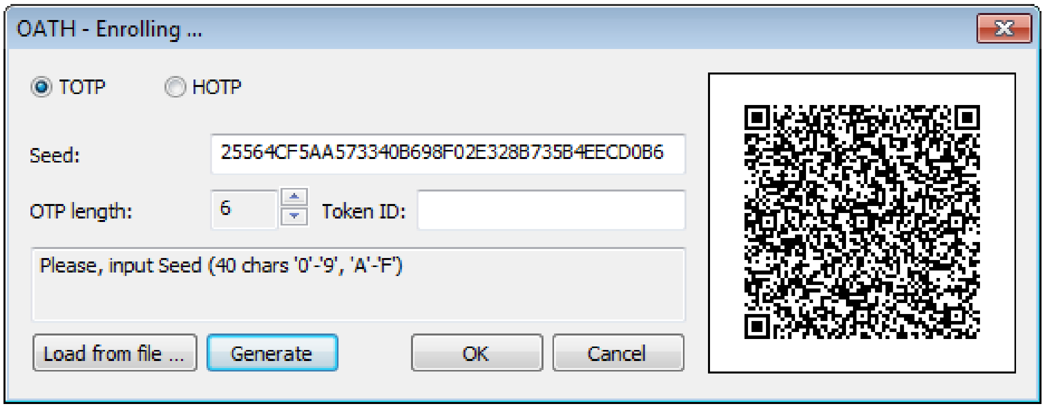
- click the **Generate** button for automatic seed generation;
- type it manually using the stated symbols;
- click the **Load from file** button and select the required **.xml** or **.pskc** file.

ℹ The seed should consist of 40 hex-digits.

2. In the **OTP length** box, select the required OTP length. The value should be between 4 and 8.

3. Leave the **Token ID** text field empty.

4. Scan the QR code containing the template data with NetIQ Smartphone Authenticator. Tap the **Scan QR to load config** button. Click **OK**.


OATH - Enrolling ...

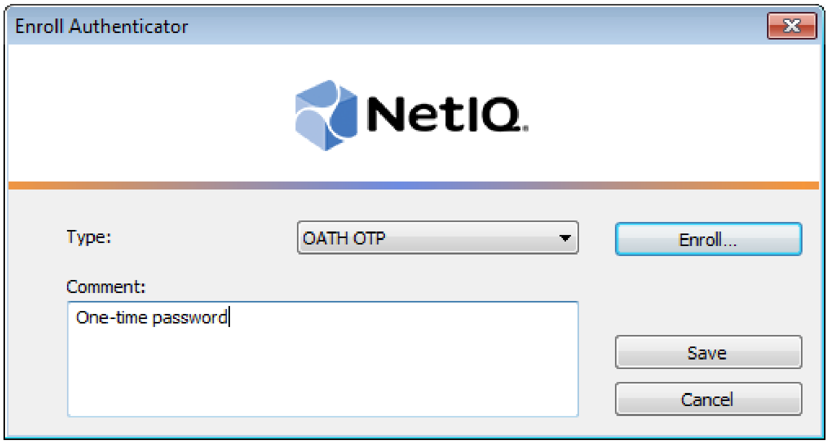
● TOTP ○ HOTP

Seed: 25564CF5AA573340B698F02E328B735B4EECD0B6

OTP length: 6 Token ID:

Please, input Seed (40 chars '0'-'9', 'A'-'F')

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

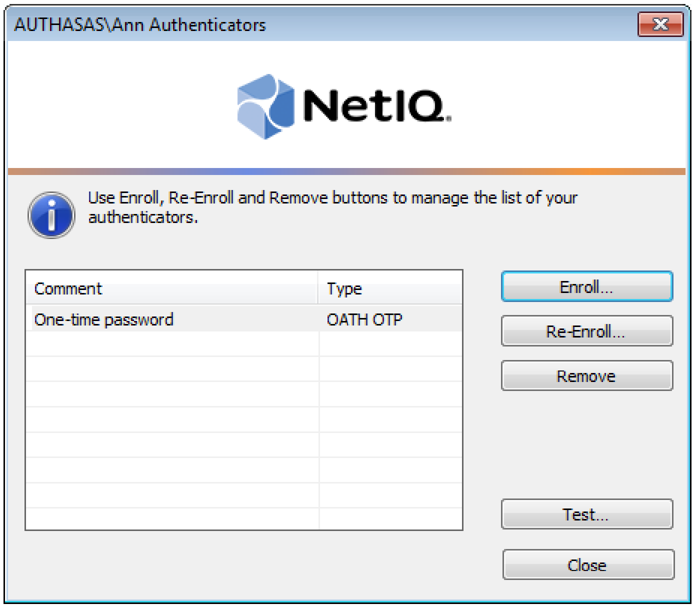

Enroll Authenticator

Type: OATH OTP

Comment: One-time password

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

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


AUTHASAS\Ann Authenticators

Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type
One-time password	OATH OTP

HOTP Enrollment

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

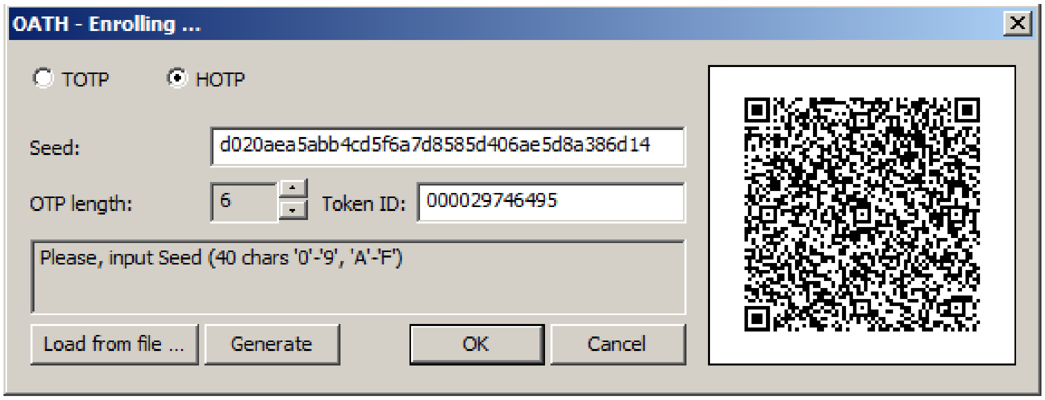
1. Enter the Secret Key of your token to the **Seed** text field.

The seed should consist of 40 hex-digits.

2. In the **OTP length** box, select OTP length according to the token's settings.

3. 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.


OATH - Enrolling ...

○ TOTP ● HOTP

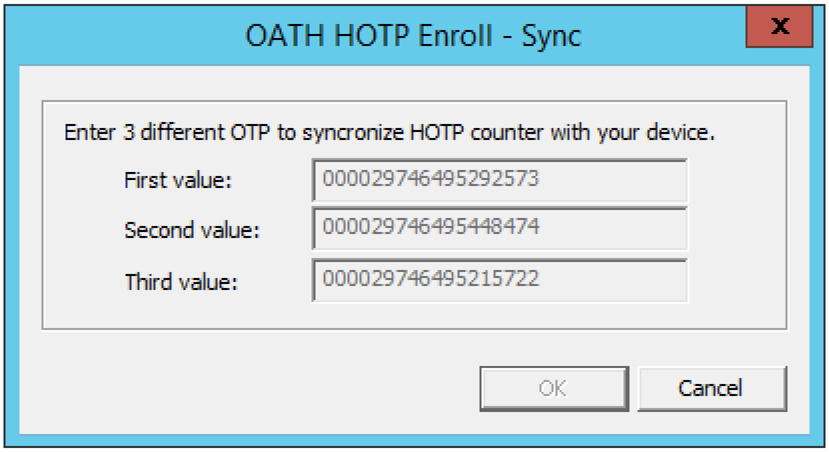
Seed: d020aea5abb4cd5f6a7d8585d406ae5d8a386d14

OTP length: 6 Token ID: 000029746495

Please, input Seed (40 chars '0'-'9', 'A'-'F')

4. Click **OK**.

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


OATH HOTP Enroll - Sync

Enter 3 different OTP to syncronize HOTP counter with your device.

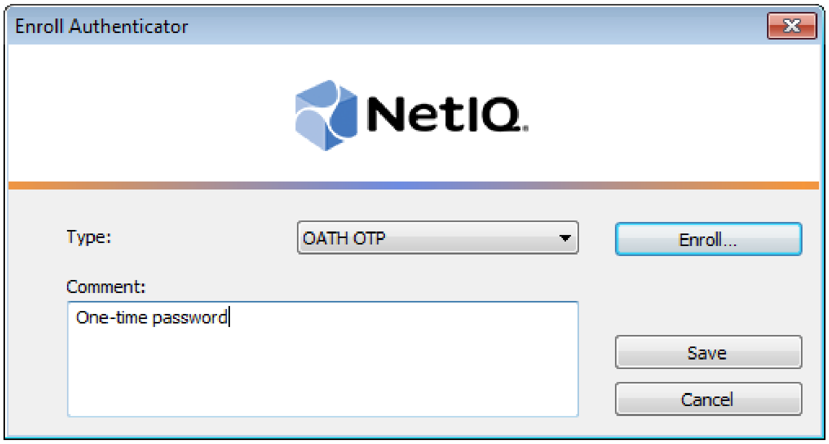
First value: 000029746495292573

Second value: 000029746495448474

Third value: 000029746495215722

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

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

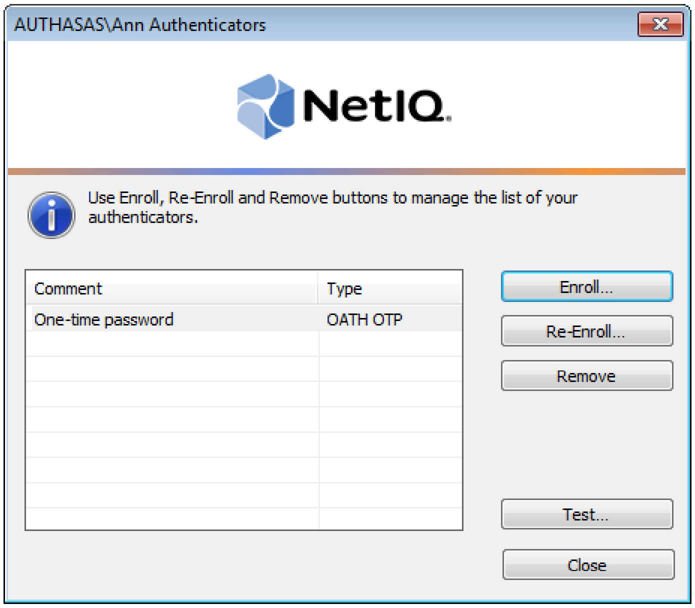

Enroll Authenticator

Type: OATH OTP

Comment: One-time password

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

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


AUTHASAS\Ann Authenticators

Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type
One-time password	OATH OTP

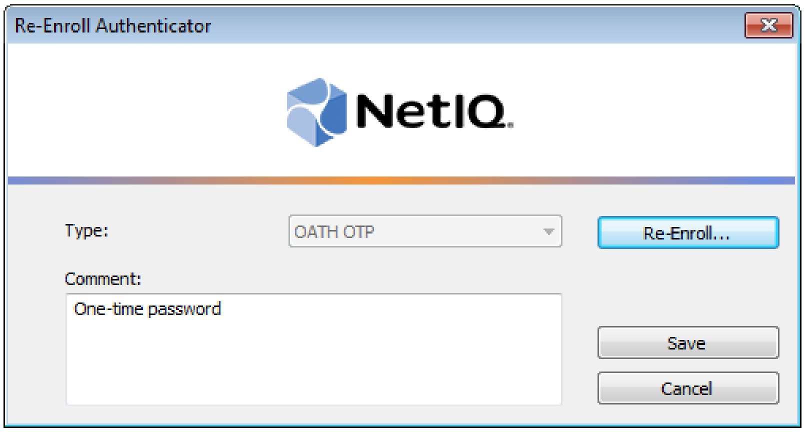
Re-enrolling OATH Authenticator

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.



Type: OATH OTP

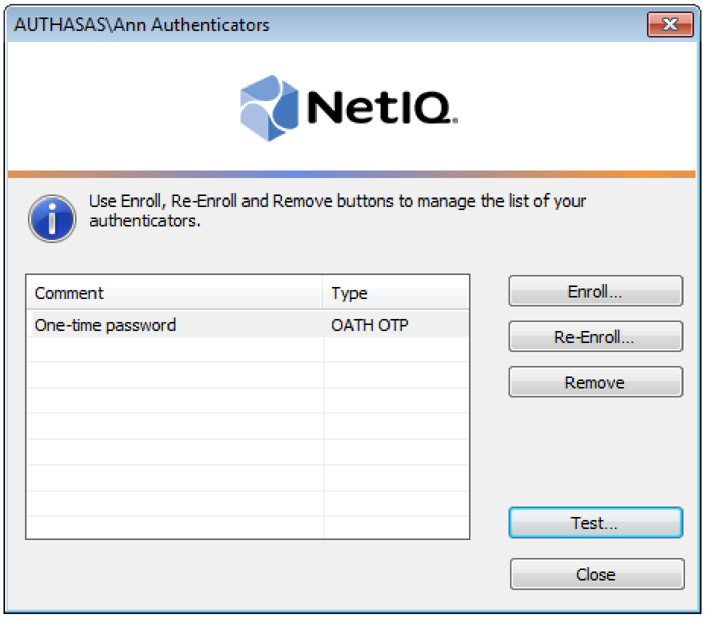
Comment:
One-time password

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.



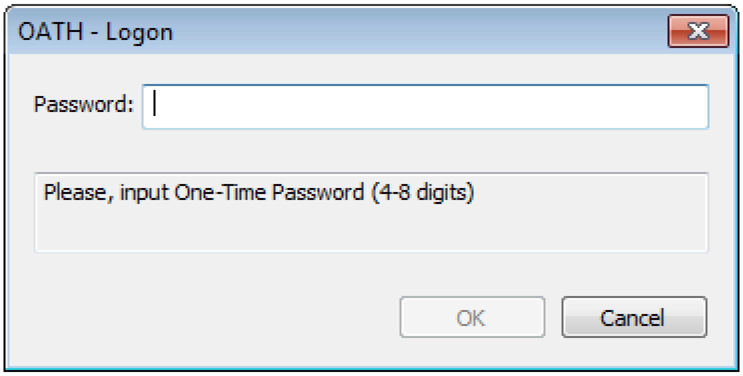
Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type
One-time password	OATH OTP

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

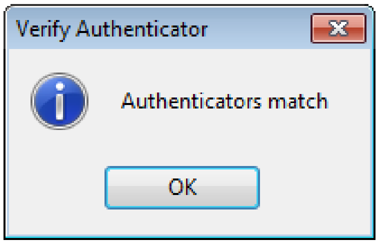


Please, input One-Time Password (4-8 digits)

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

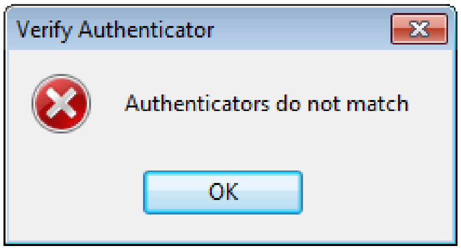
For YubiKey, insert the token into the port and press its button.

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



Authenticators match

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



Authenticators do not match

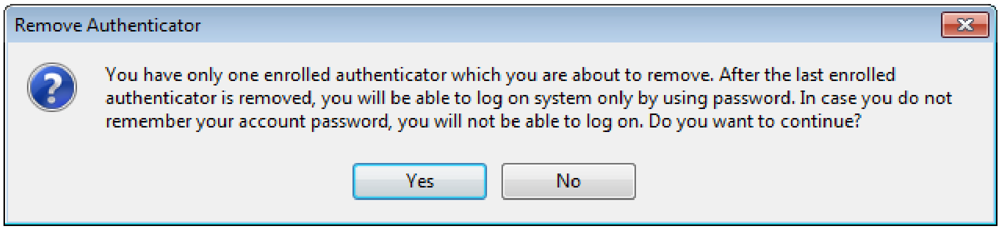
Removing OATH Authenticator

✱ 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:



Remove Authenticator

You have only one enrolled authenticator which you are about to remove. After the last enrolled authenticator is removed, you will be able to log on system only by using password. In case you do not remember your account password, you will not be able to log on. Do you want to continue?

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