NetIQ Advanced Authentication Framework

FIDO U2F Authentication Provider User's Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This FIDO U2F 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 FIDO U2F 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

This document uses the following 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, and buttons are put in bold type, e.g.: the **Logon** window.

Managing FIDO U2F Authenticator

In this chapter:

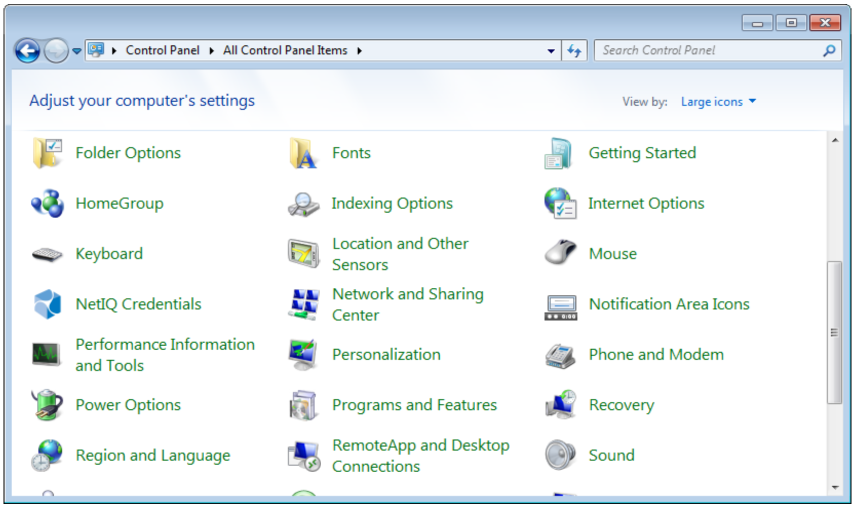
- Microsoft Windows 7/Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003/2003 R2
- Microsoft Windows Server 2012

Microsoft Windows 7/Microsoft Windows Server 2008 R2

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

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

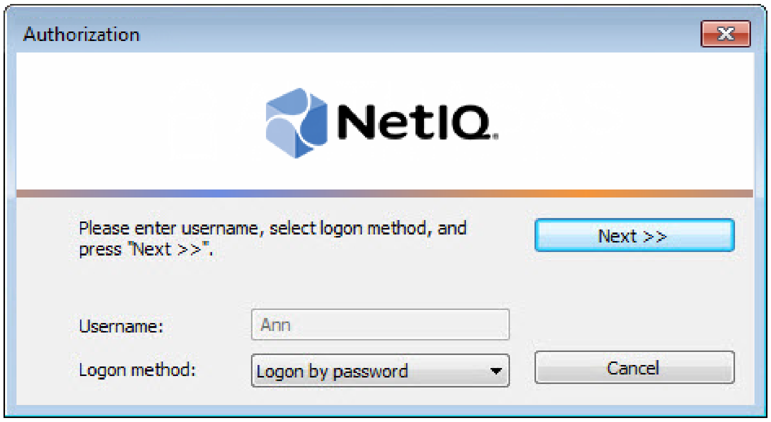
To open the **Authenticators** window from **Control Panel**, in **Control Panel** by categories select **User Accounts > NetIQ Credentials:**



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

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

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).



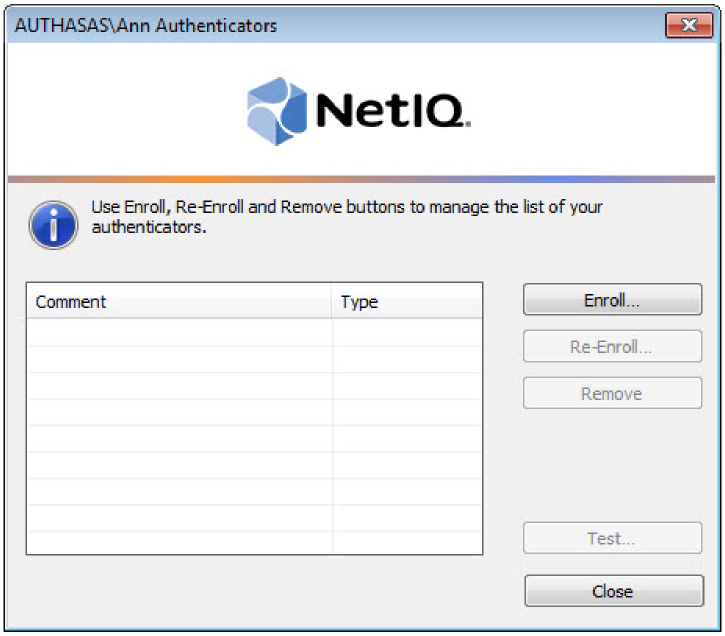
Please enter username, select logon method, and press "Next >>".

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.

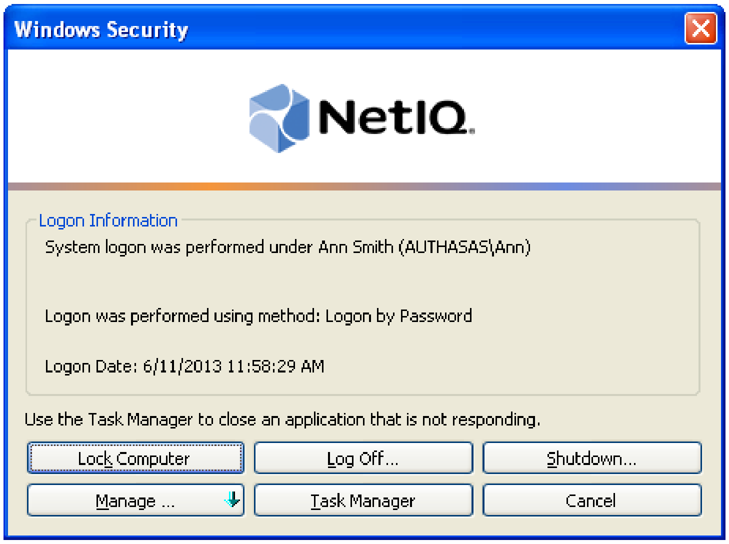
Comment	Type

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.



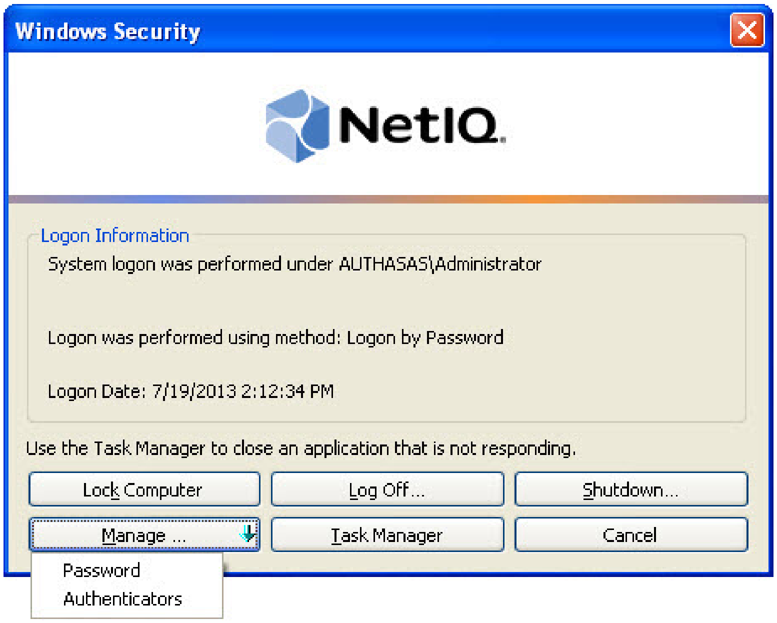
System logon was performed under Ann Smith (AUTHASAS\Ann)

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**.



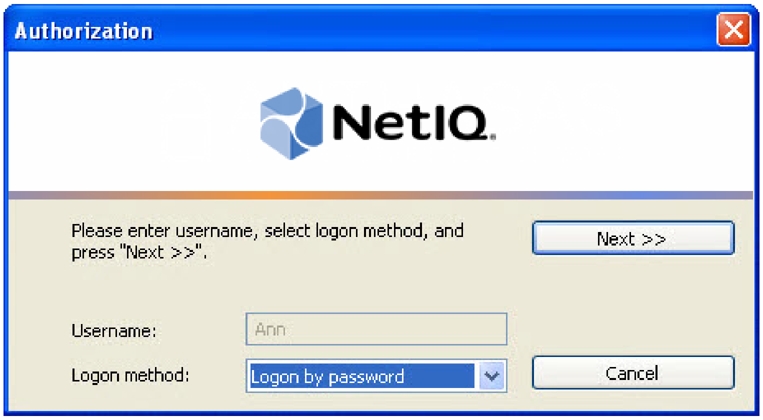
System logon was performed under AUTHASAS\Administrator

Logon was performed using method: Logon by Password

Logon Date: 7/19/2013 2:12:34 PM

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

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



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

Username: Ann

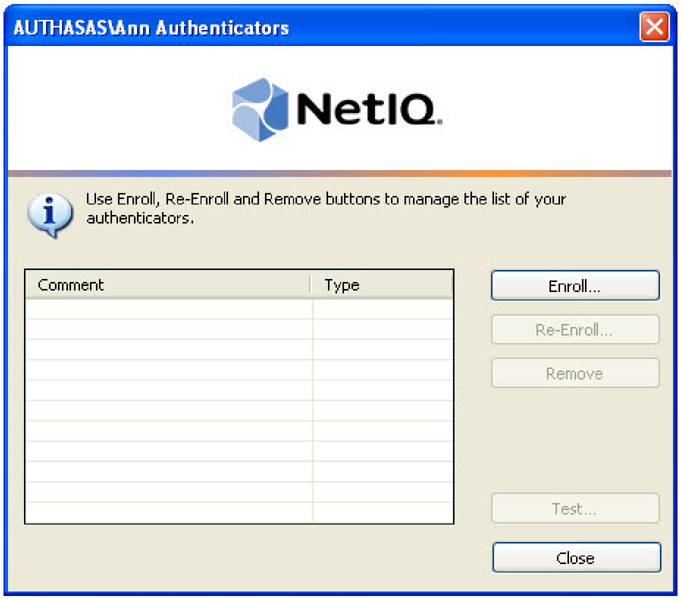
Logon method: Logon by password

- 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.

✱ To be able to test an authenticator, you may use either authenticator or password as logon method.

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



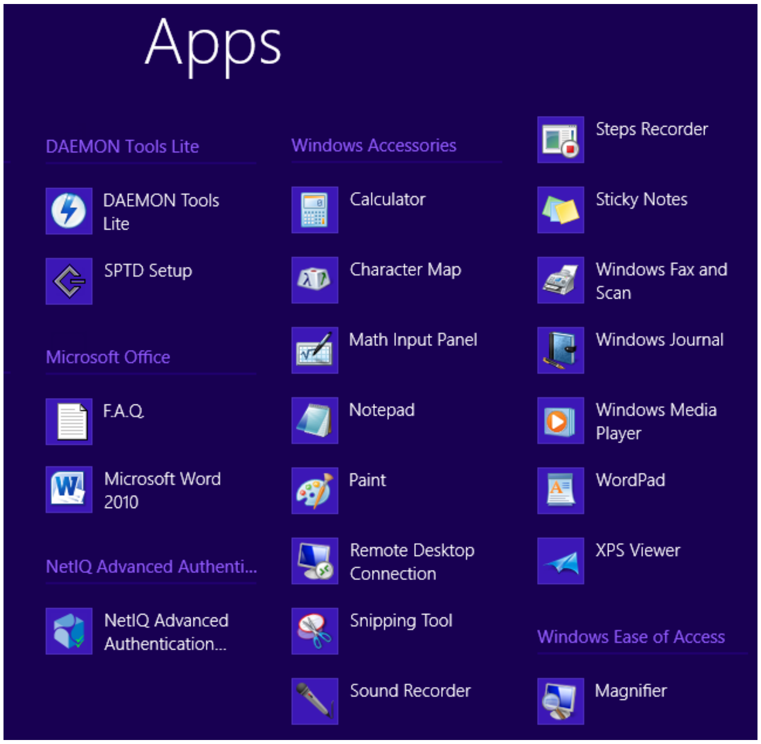
Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

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.

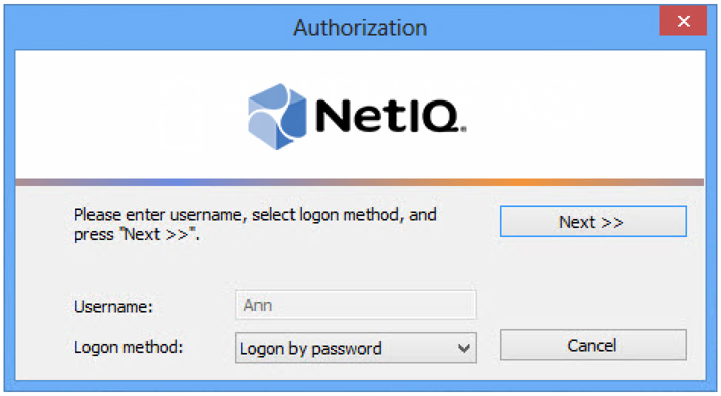
To open the **Authenticators** window, in the **Search** menu select **Apps > NetIQ Advanced Authentication Framework…**.



To open **Authenticators** window, user should 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).



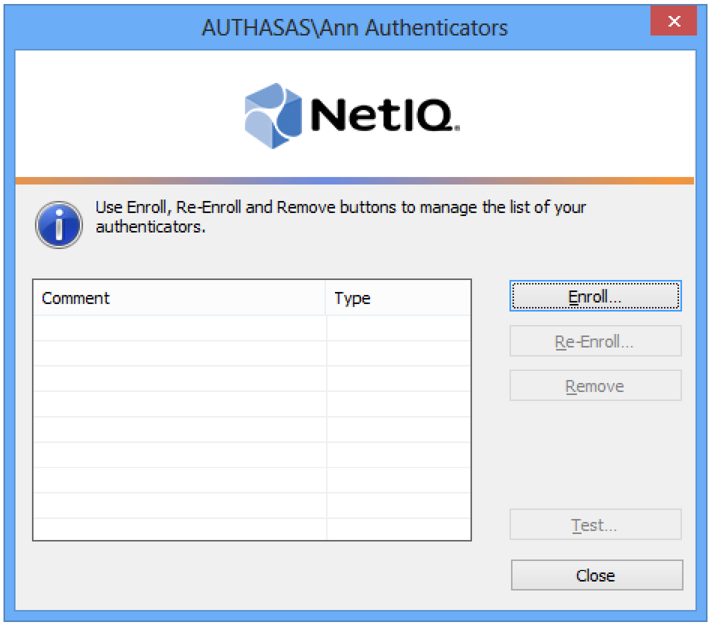
Please enter username, select logon method, and press "Next >>".

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.



AUTHASAS\Ann Authenticators

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

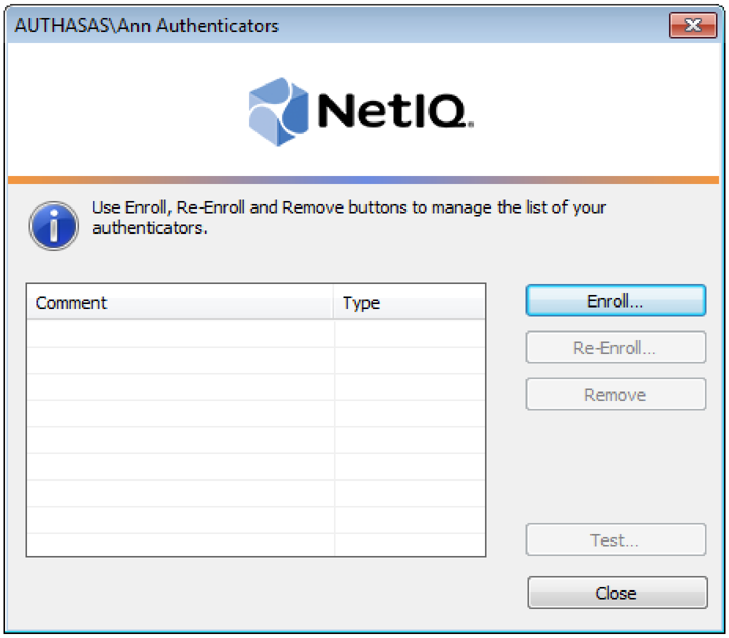
Comment	Type

Enrolling FIDO U2F Authenticator

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 FIDO U2F authenticator:

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

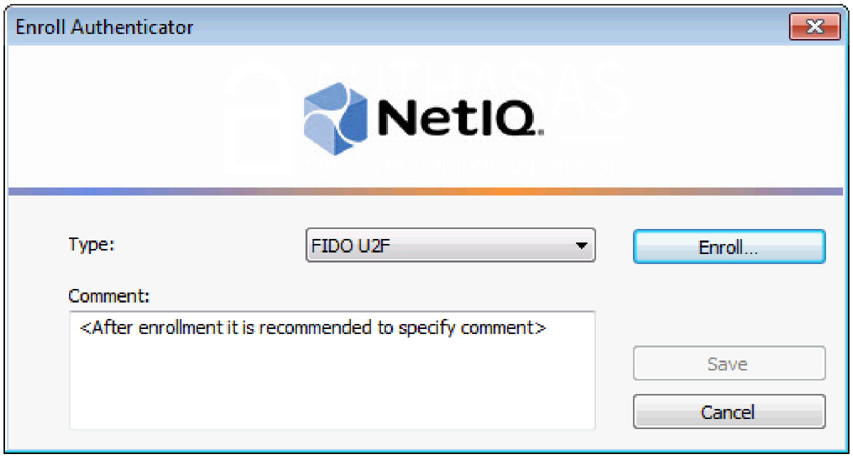


AUTHASAS\Ann Authenticators

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

Comment	Type

2. After the **Enroll Authenticator** window is launched, select **FIDO U2F** from the **Type** drop-down menu and click **Enroll**.

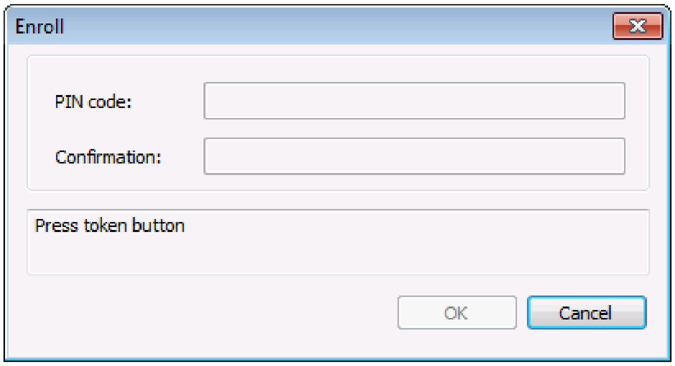


Enroll Authenticator

Type: FIDO U2F

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

3. After the **Enroll** window is launched, insert your token and press its button. Enter your PIN and confirm it.



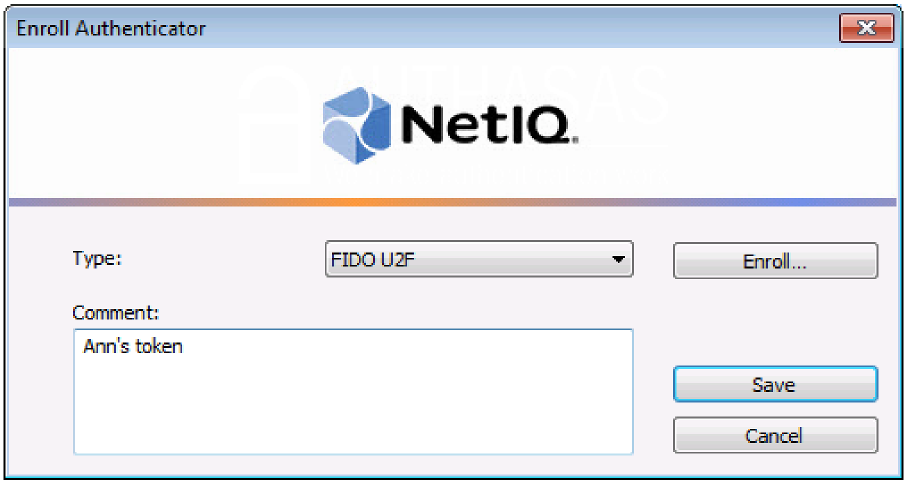
PIN code:

Confirmation:

Press token button

PIN should be entered every time you authenticate with FIDO U2F authentication provider. PIN is not cached for FIDO U2F authentication provider even if the **Enable PIN caching** policy is enabled.

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

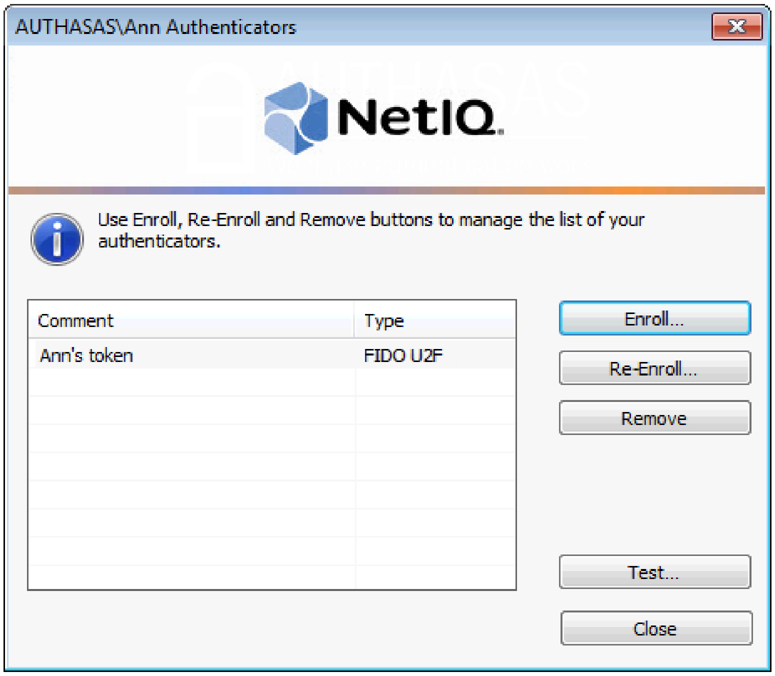


Type: FIDO U2F

Comment: Ann's token

Entering and editing 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.



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

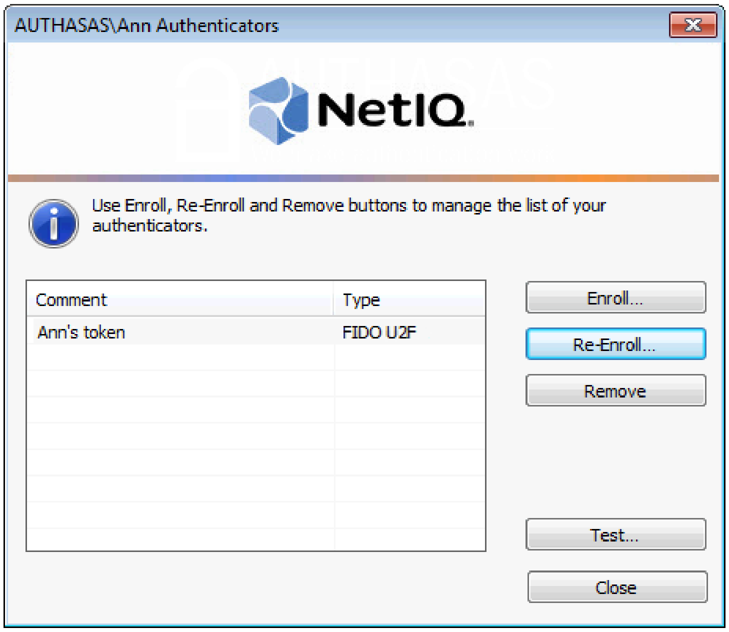
Comment	Type
Ann's token	FIDO U2F

Re-enrolling FIDO U2F 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 FIDO U2F authenticator:

1. Select **FIDO U2F** in the list of authenticators, click **Re-Enroll** in the **Authenticators** window.

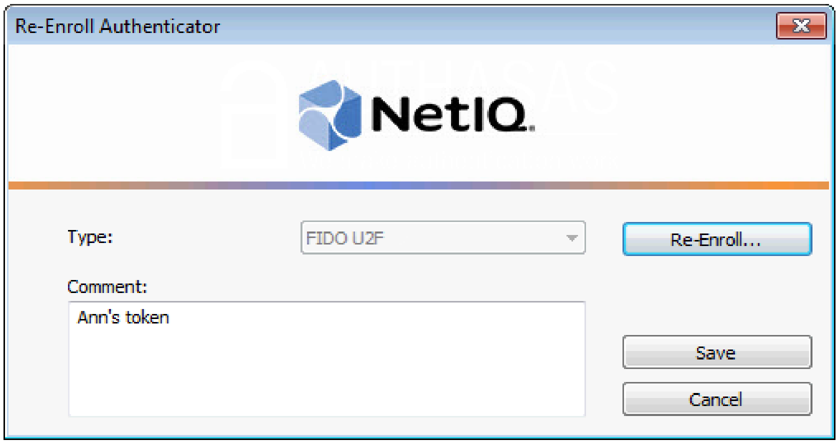


AUTHASAS\Ann Authenticators

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

Comment	Type
Ann's token	FIDO U2F

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



Re-Enroll Authenticator

Type: FIDO U2F

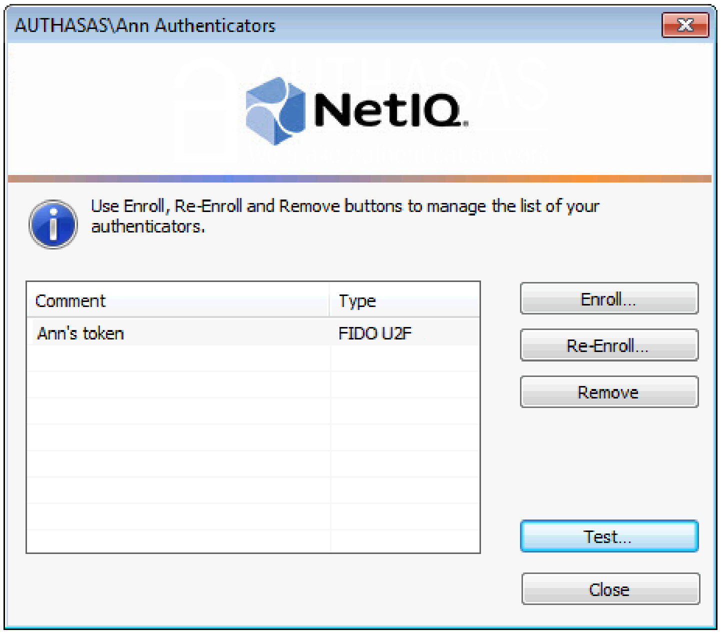
Comment: Ann's token

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

Testing FIDO U2F Authenticator

To test a created FIDO U2F authenticator:

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

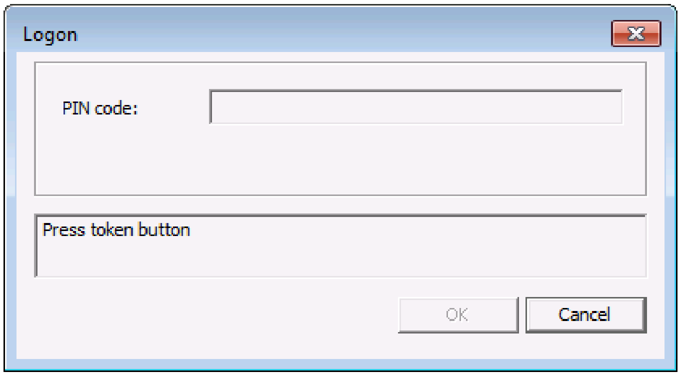


AUTHASAS\Ann Authenticators

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

Comment	Type
Ann's token	FIDO U2F

2. After the **Logon** window is launched, insert your token, press its button and enter your PIN.



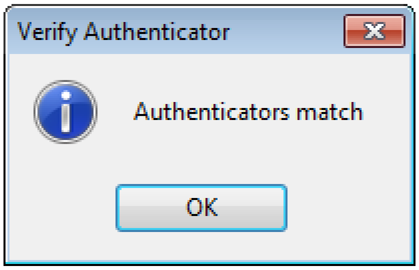
Logon

PIN code:

Press token button

PIN should be entered every time you authenticate with FIDO U2F authentication provider. PIN is not cached for FIDO U2F authentication provider even if the **Enable PIN caching** policy is enabled.

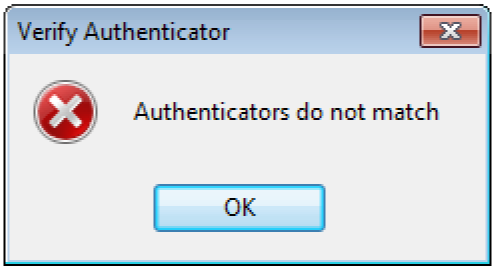
3. When a confirmation message saying: *"Authenticators match"* appears, click **OK**.



Verify Authenticator

Authenticators match

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



Verify Authenticator

Authenticators do not match

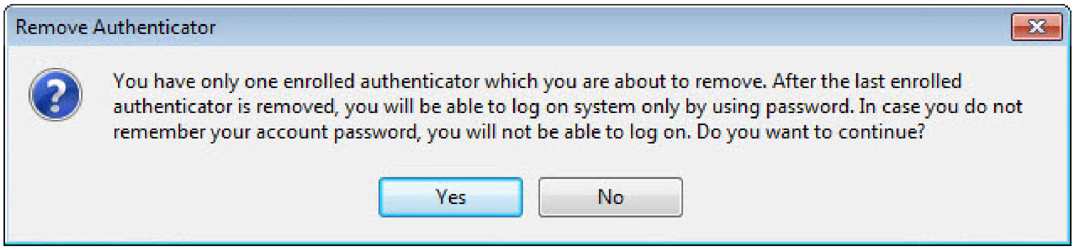
Removing FIDO U2F Authenticator

✱ 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, do not do this just because you do not like your current authenticator. Instead, you can re-enroll it (see Re-enrolling FIDO U2F Authenticator).

⚠ 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

ℹ 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.

ℹ 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**.
6. 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 FIDO U2F authenticator type is absent.
b. The **Enroll** button in the **Authenticators** window is greyed out.

Cause:

a. The FIDO U2F 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.

Index

© *NetIQ*