



NetIQ Advanced Authentication Framework

FIDO U2F Authentication Provider User's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Managing FIDO U2F Authenticator	4
Microsoft Windows 7/Microsoft Windows Server 2008 R2	4
Microsoft Windows Server 2012	6
Enrolling FIDO U2F Authenticator	8
Re-enrolling FIDO U2F Authenticator	11
Testing FIDO U2F Authenticator	13
Removing FIDO U2F Authenticator	15
Troubleshooting	16
Cannot Enroll Authenticator	17
Index	18

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.

 **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:

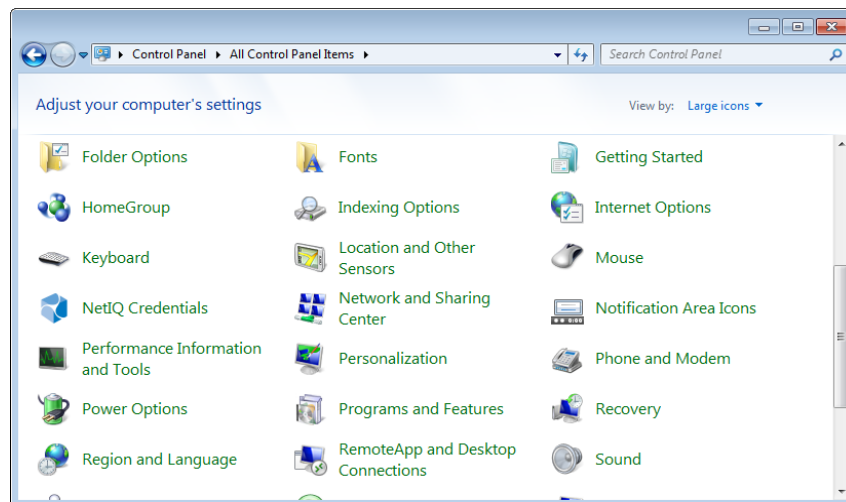
- [Microsoft Windows 7/Microsoft Windows Server 2008 R2](#)
- [Microsoft Windows Server 2012](#)

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 **Control Panel** by categories select **User Accounts > NetIQ Credentials**:



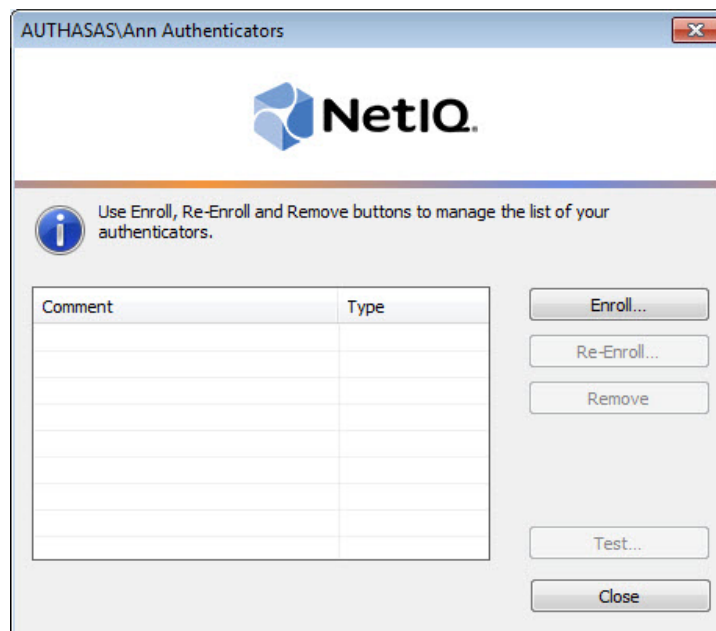
To open **Authenticators** window, user should undertake authorization procedure:

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).



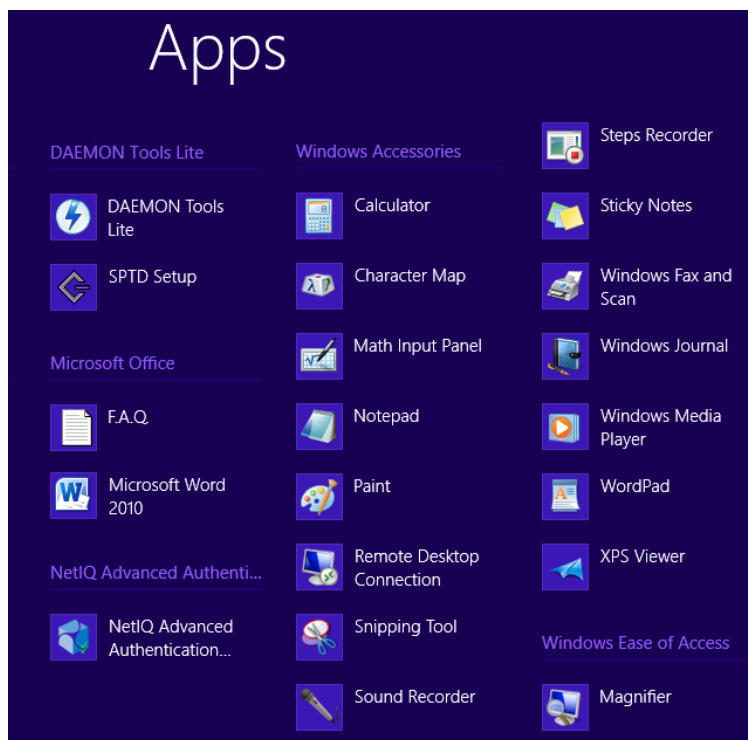
2. Get authenticated with the selected method.
3. Once you are authenticated, page for managing authenticators is opened.



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


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

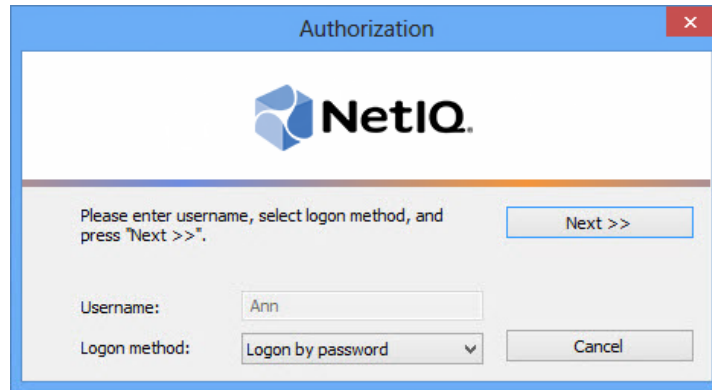
To open the **Authenticators** window, in the **Search** menu select **Apps > NetIQ Advanced Authentication Framework...**



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

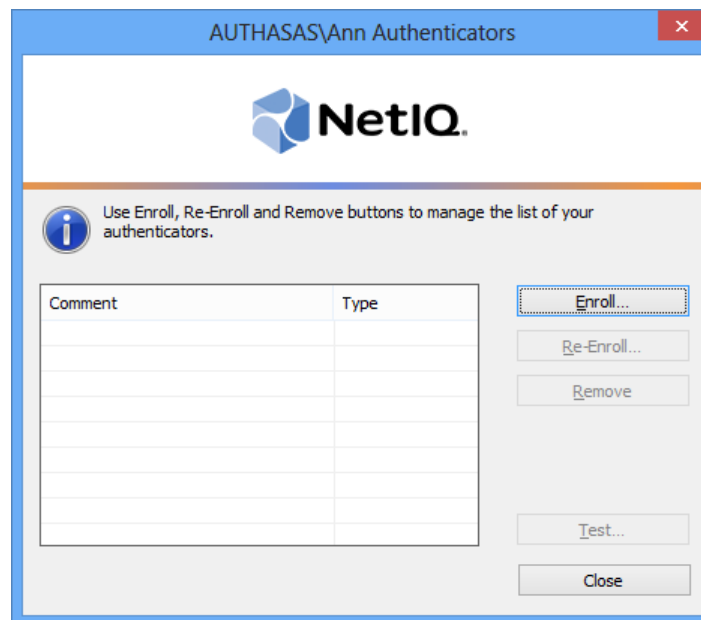
1. In the **Authorization** window, choose authentication method.

 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).




2. Get authenticated with the selected method.

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

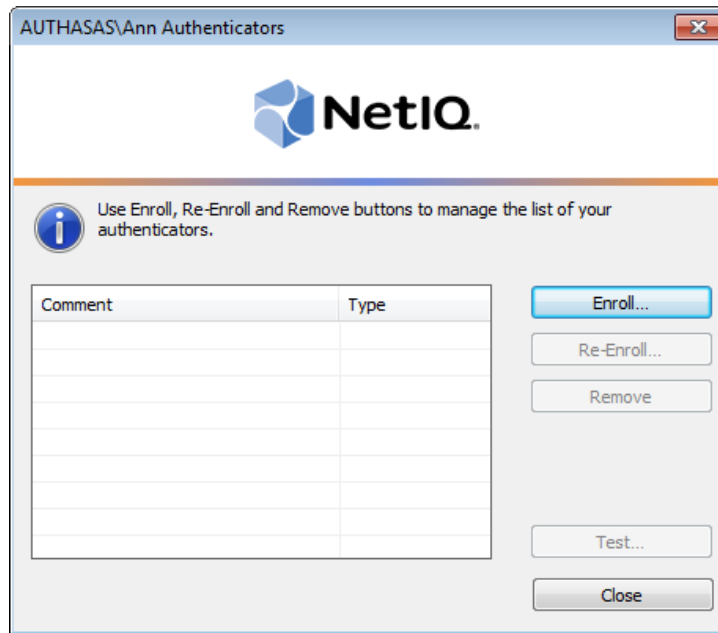


Enrolling FIDO U2F Authenticator

 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:

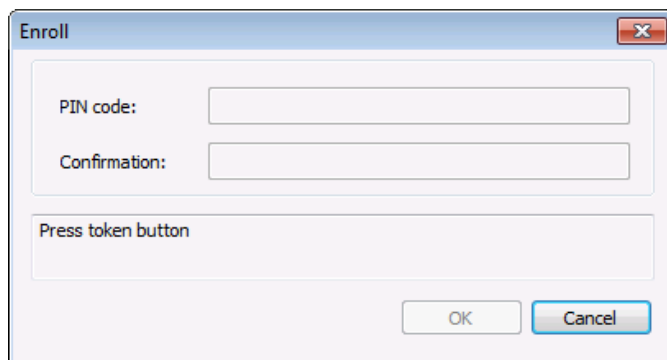
1. Click the **Enroll** button in the **Authenticators** window.



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



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



The screenshot shows a dialog box titled "Enroll". It has a close button (X) in the top right corner. Inside the dialog, there are two text input fields: the first is labeled "PIN code:" and the second is labeled "Confirmation:". Below these fields is a label "Press token button". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- * PIN caching is not supported by FIDO U2F authentication provider. You should enter PIN every time you authenticate with FIDO U2F authentication provider.
- * If the [Use domain password as PIN](#) policy is enabled, you will be prompted to enter your domain password instead of PIN.

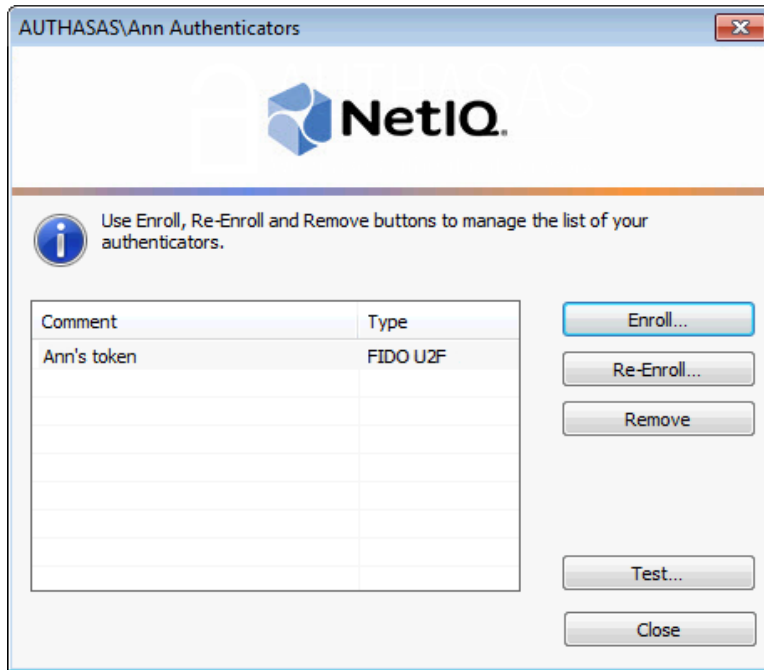
4. Control is passed to the **Enroll Authenticator** window. Entering commentary is optional. Click **Save**.




The screenshot shows a dialog box titled "Enroll Authenticator" with a close button (X) in the top right corner. The NetIQ logo is centered at the top. Below the logo, there is a "Type:" label followed by a dropdown menu showing "FIDO U2F". To the right of the dropdown is an "Enroll..." button. Below the dropdown is a "Comment:" label followed by a text area containing the text "Ann's token". To the right of the text area are two buttons: "Save" and "Cancel".

- * 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.

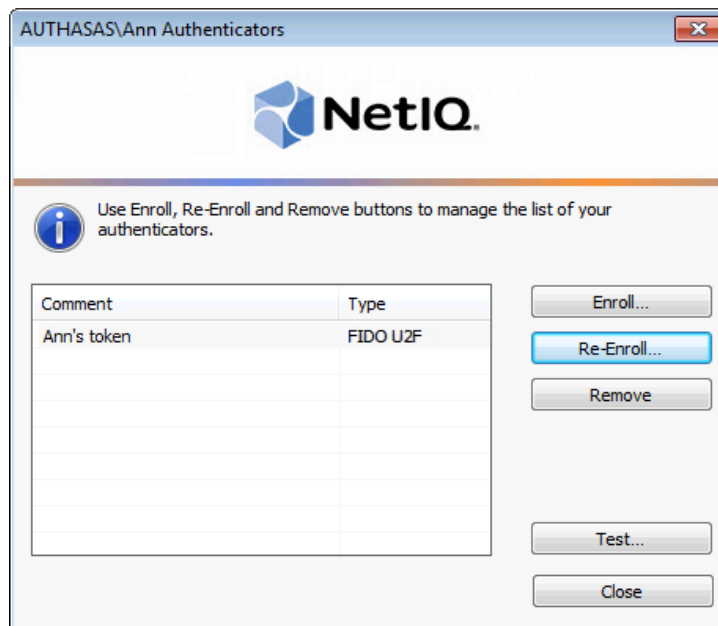


Re-enrolling FIDO U2F Authenticator

 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.



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

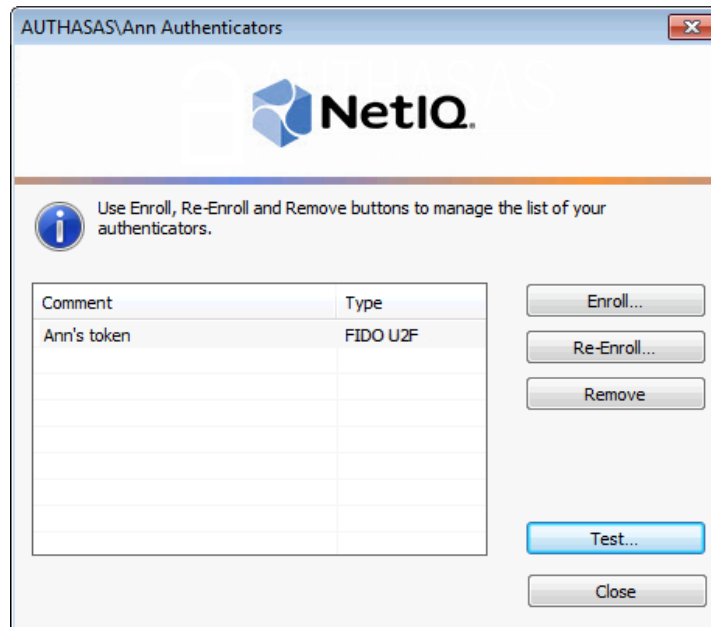


3. Fulfill the steps as during your initial enrollment process.

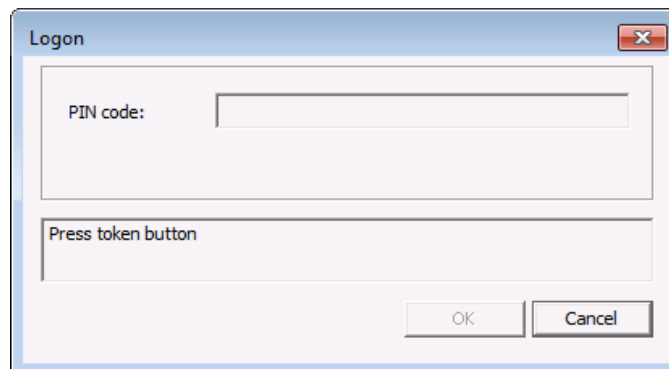
Testing FIDO U2F Authenticator

To test a created FIDO U2F authenticator:

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



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



* PIN caching is not supported by FIDO U2F authentication provider. You should enter PIN every time you authenticate with FIDO U2F authentication provider.

* If the [Use domain password as PIN](#) policy is enabled, you will be prompted to enter your domain password instead of PIN.

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



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



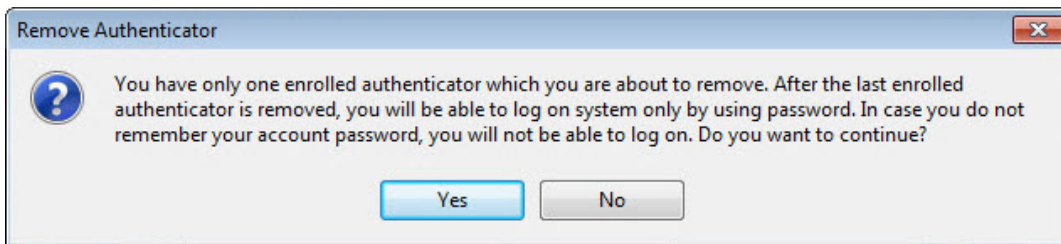
Removing FIDO U2F Authenticator

✖ 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:



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

Troubleshooting

 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**.
6. 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 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

A

Authentication 1, 3-4, 6, 15
Authenticator 3-4, 6, 8, 11, 13, 15, 17

C

Client 3
Control 4, 9

E

Enroll 4, 6, 11, 17

L

Logon 3, 13

M

Microsoft Windows Server 2012 4, 6

P

PIN 9, 13

R

Re-enroll 4
Remove 4, 6, 15

U

User 1, 4

W

Windows 7 4