



NetIQ Advanced Authentication Framework

RADIUS Authentication Provider User's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Managing RADIUS Authenticator	4
Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2	4
Microsoft Windows XP/Microsoft Windows Server 2003	7
Microsoft Windows 8/Microsoft Windows Server 2012	10
Enrolling RADIUS Authenticator	12
Re-enrolling RADIUS Authenticator	15
Testing RADIUS Authenticator	17
Removing RADIUS Authenticator	19
Troubleshooting	20
Cannot Enroll Authenticator	21
Cannot Logon with RADIUS Authenticator	21
Index	22

Introduction

About This Document

Purpose of the Document

This RADIUS 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 RADIUS 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.

Managing RADIUS Authenticator

✖ Please note that RADIUS doesn't work with cached authenticators after network disconnection. This happens because being out of the network, user with cached authenticator still needs access to the RADIUS Server, which is unavailable.

✖ For more information about caching, see Caching Authenticators chapter of NetIQ Advanced Authentication Framework Client – User's Guide.

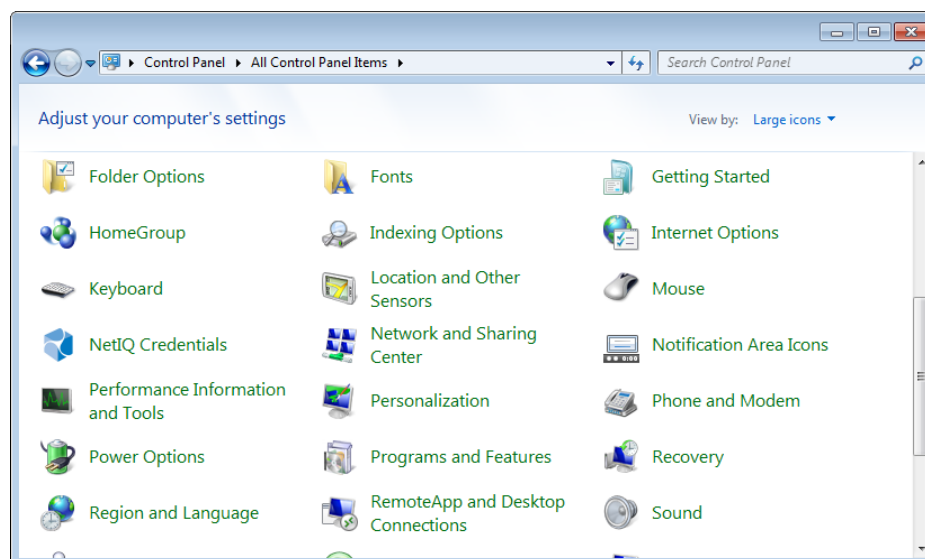
Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

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

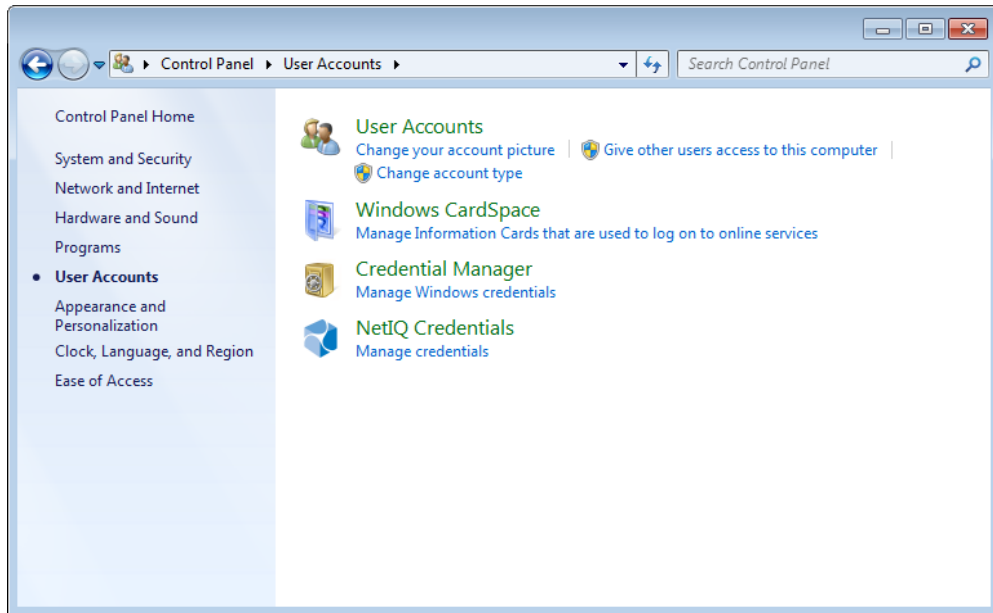
i The Authentication Wizard window is shown at system start if there are no enrolled authenticators.

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

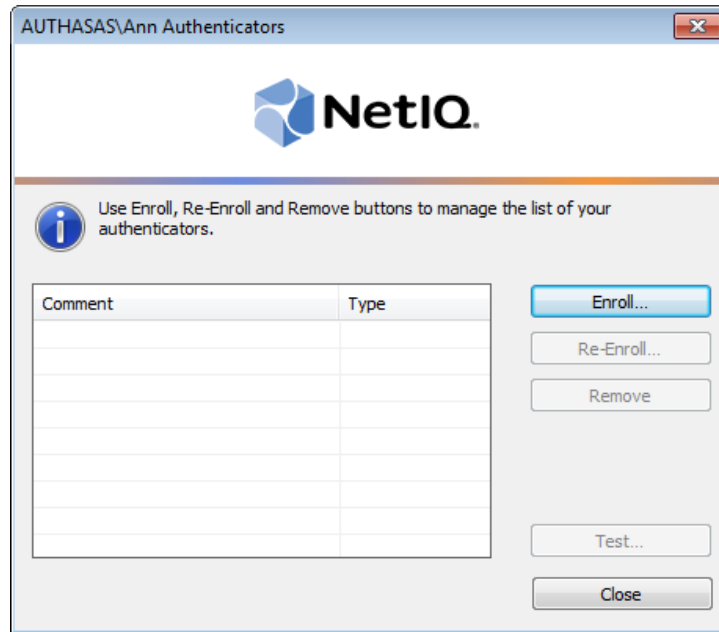
1. In the **Authorization** window, choose authentication method.

✖ 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.

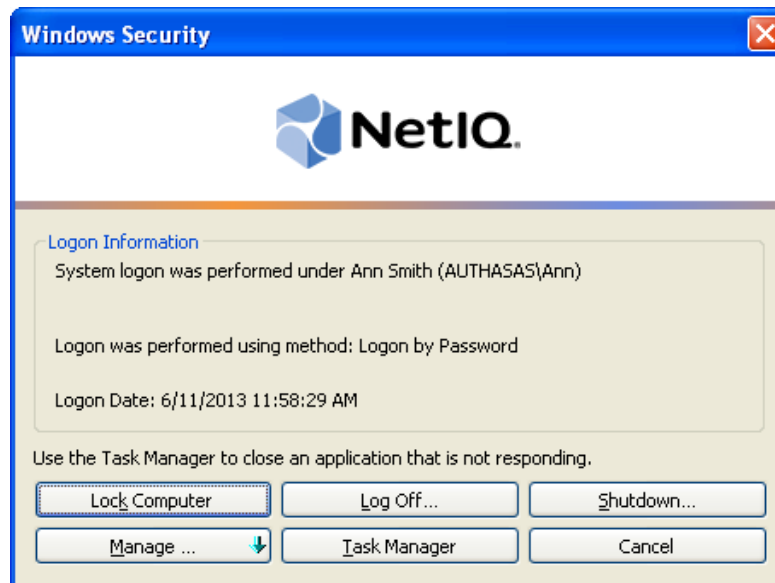


Microsoft Windows XP/Microsoft Windows Server 2003

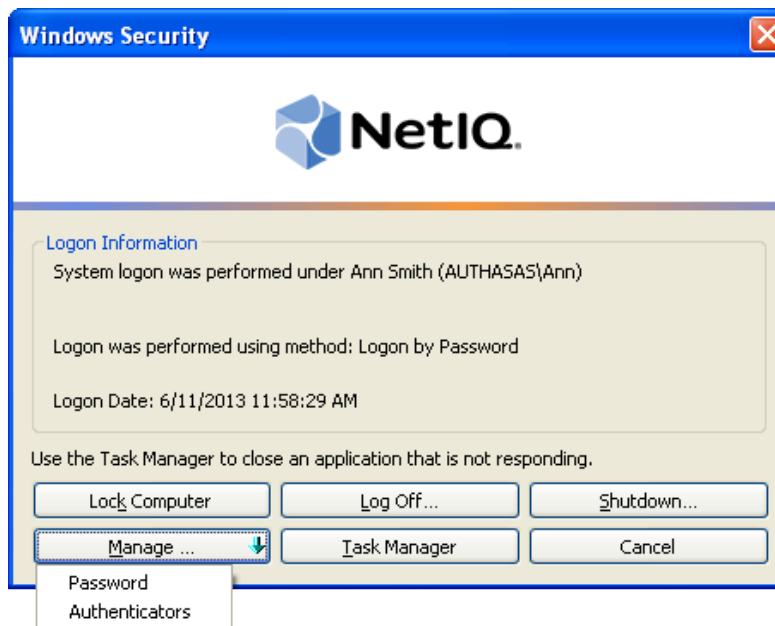
Authenticator management options are available in the Authenticators window.

To open the **Authenticators** window

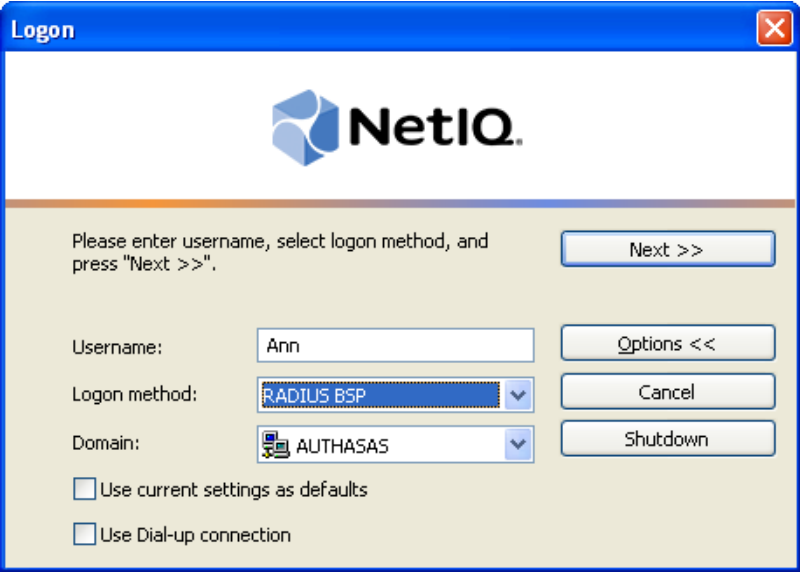
1. From your desktop, press **[Ctrl]+[Alt]+[Del]**. The **Windows Security** window is displayed.



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



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

The image shows a Windows-style dialog box titled "Logon" with a blue header bar and a close button in the top right corner. The main area has a light beige background. At the top center is the NetIQ logo, which consists of a blue cube icon followed by the text "NetIQ.". Below the logo, there is a line of text: "Please enter username, select logon method, and press 'Next >>'." To the right of this text is a button labeled "Next >>". Below the text, there are three input fields: "Username:" with the text "Ann" entered, "Logon method:" with a dropdown menu showing "RADIUS BSP" selected, and "Domain:" with a dropdown menu showing "AUTHASAS" selected. To the right of these fields are three buttons: "Options <<", "Cancel", and "Shutdown". At the bottom left, there are two checkboxes: "Use current settings as defaults" and "Use Dial-up connection", both of which are currently unchecked.

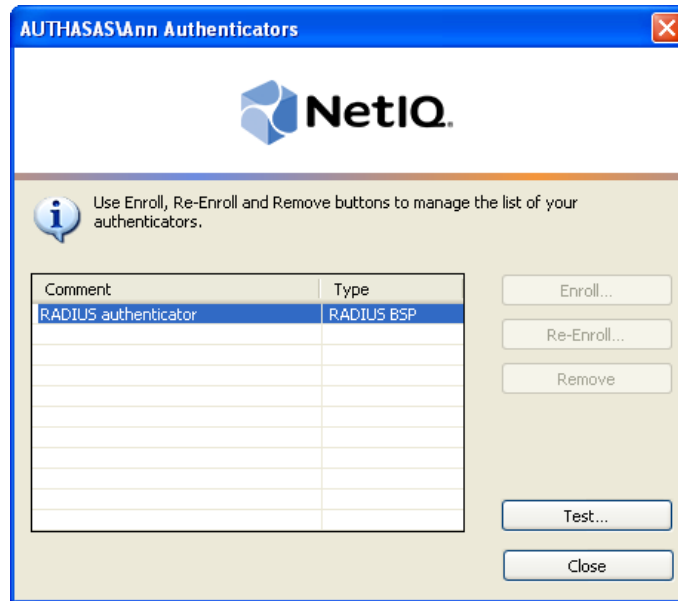
- From the **Logon method** list, select a logon method (an authenticator type or **Logon by password**).

- Click **Next**.

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

- ✖ 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.

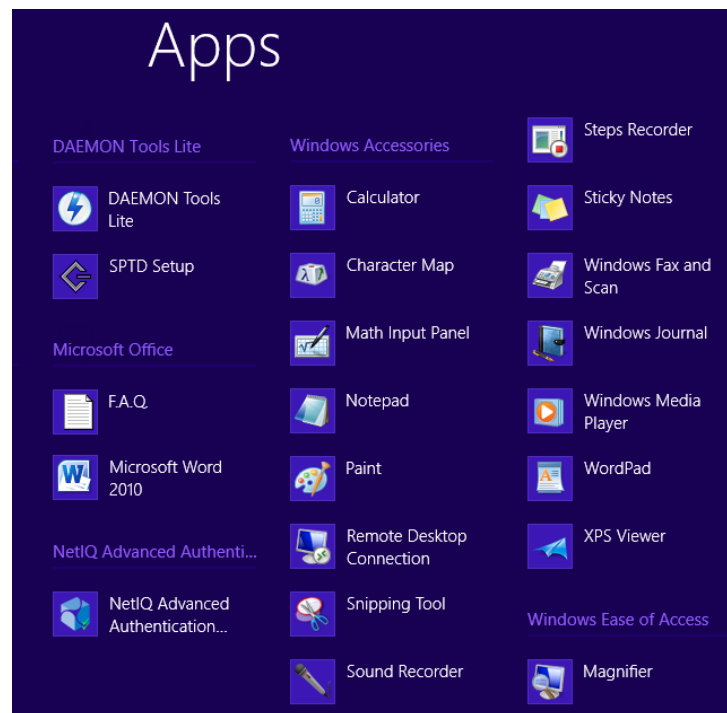


Microsoft Windows 8/Microsoft Windows Server 2012

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

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

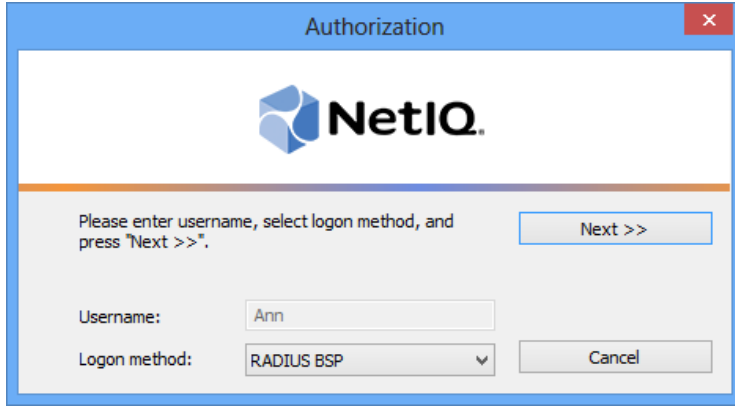
To open the **Authenticators**, in the **Search** menu select **Apps > NetIQ Advanced Authentication Framework....**



To open **Manage 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).



Authorization



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

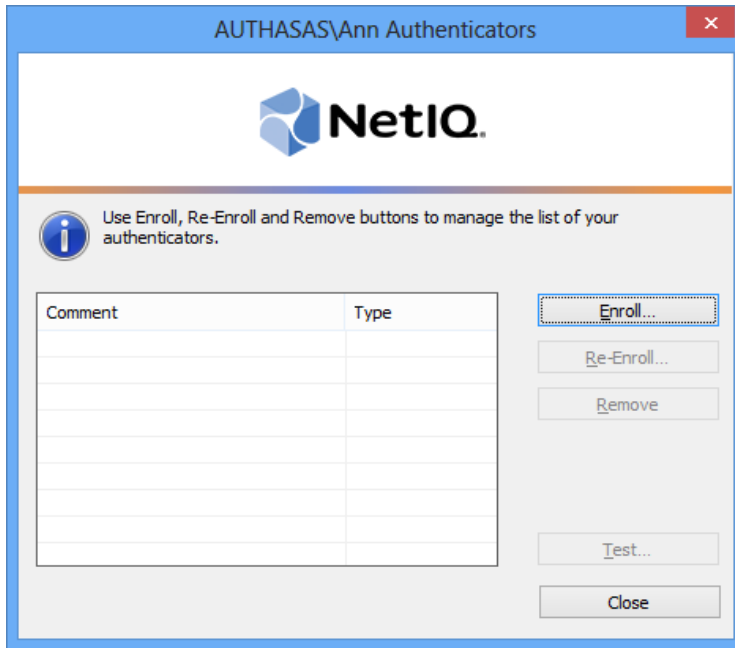
Next >>

Username:

Logon method:

Cancel

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

Enroll...

Re-Enroll...

Remove

Test...

Close

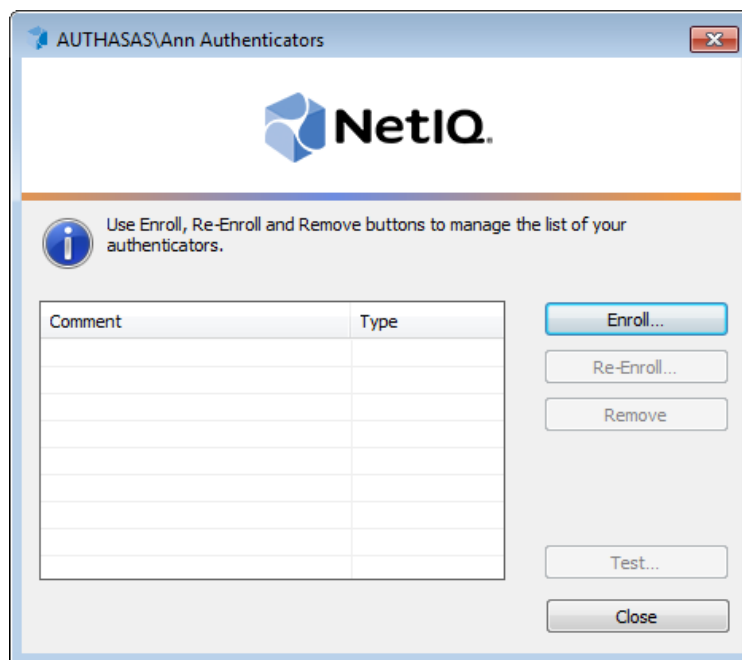
Enrolling RADIUS Authenticator

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

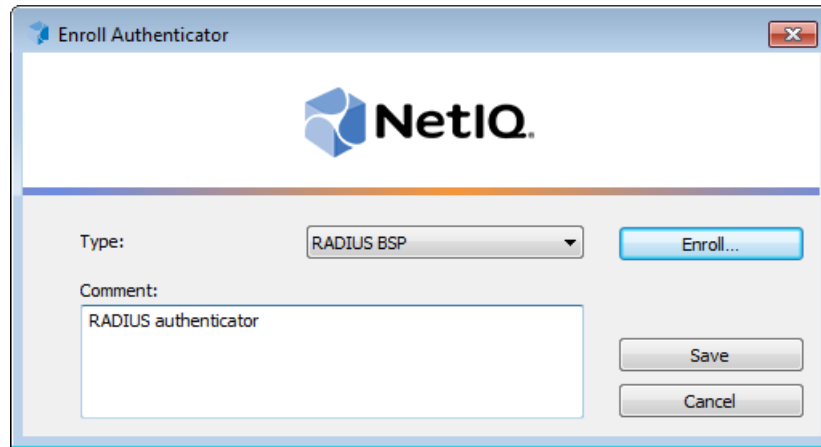
✖ NetIQ administrator defines the maximum number of authenticators you can have which means you cannot enroll any more authenticators once you have reached the limit.

To enroll a RADIUS authenticator:

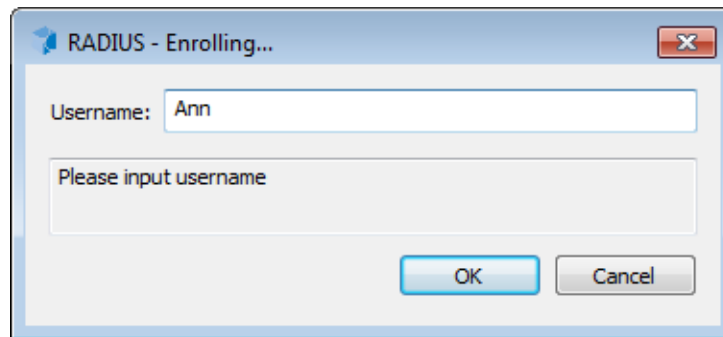
1. Click **Enroll...** button in the **Authenticators** window.



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

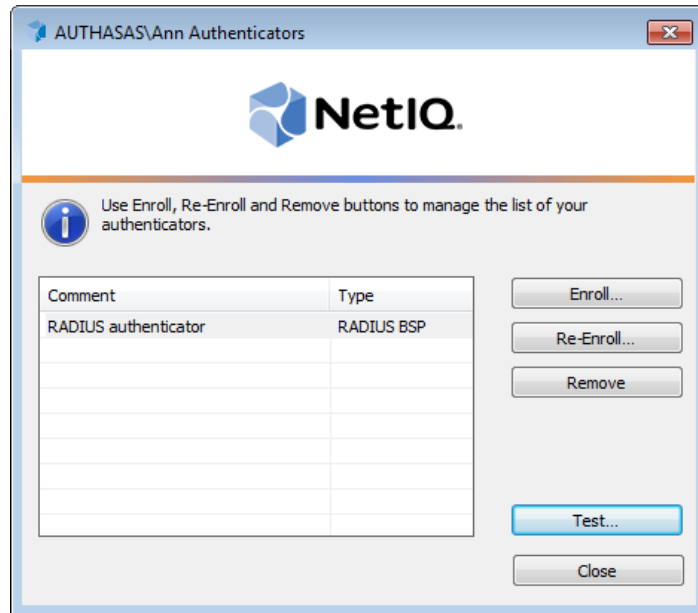


3. Type in domain username.



 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.

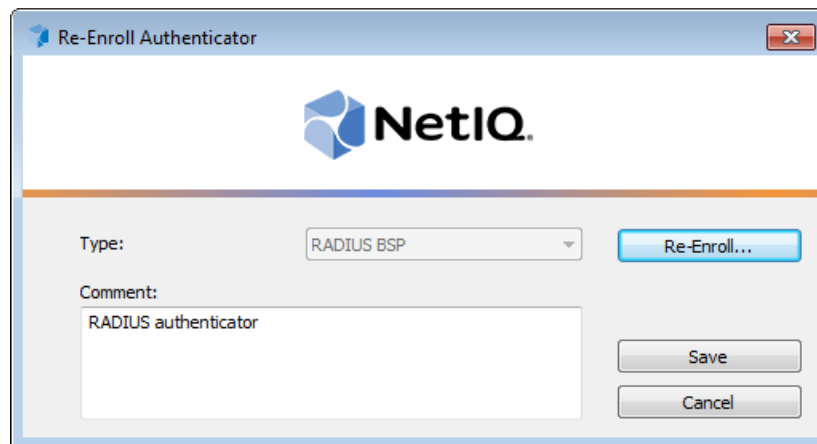


Re-enrolling RADIUS Authenticator

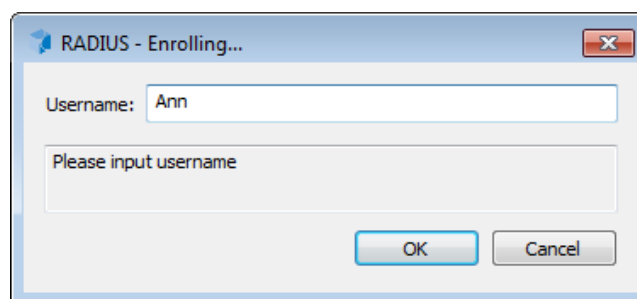
 This operation may be forbidden by NetIQ administrator. In such cases the Re-Enroll button in the Authenticators window is greyed out.

In order to re-enroll a created RADIUS authenticator:

1. Select **RADIUS BSP** in the list of authenticators, click **Re-Enroll...** in the **Authenticators** window.
2. Click **Re-Enroll...** in the **Re-Enroll Authenticators** window.



3. Type in domain username.



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

Re-Enroll Authenticator



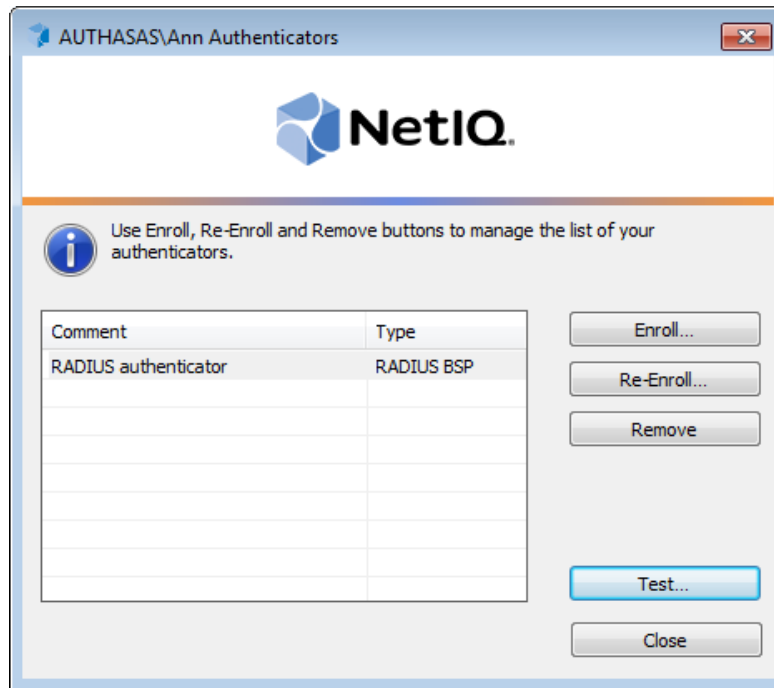
Type:

Comment:

Testing RADIUS Authenticator

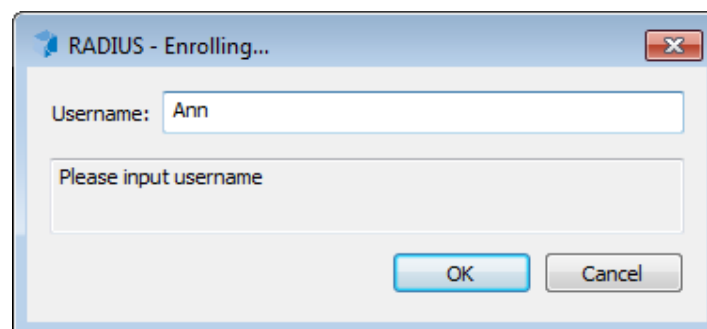
To test a created RADIUS authenticator

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



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

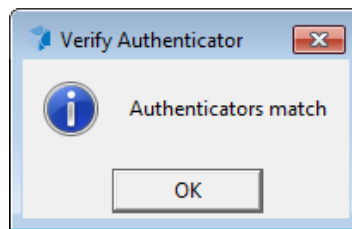
2. In the **Verifying** window enter domain user password.



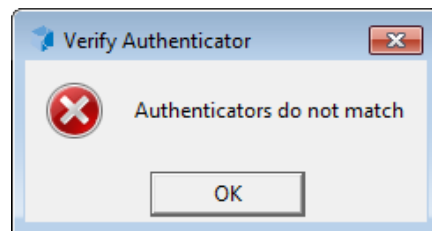
i Depending on the RADIUS server settings, you may not have to enter the domain password. It will depend on the technology you used for remote access using RADIUS server (for example, RSA tokens, Vasco, Cryptocard, Phonefactor, SMS Passcode etc.).

i If NetIQ NPS plugin is installed on Network Policy Server server, the user will need to use OTP instead of domain password.

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



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



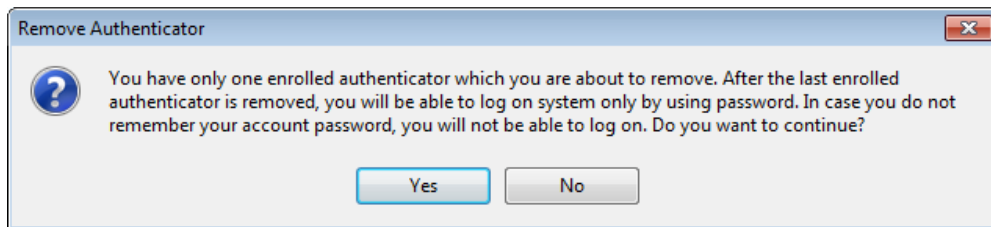
Removing RADIUS Authenticator

✖ 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



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 RADIUS authenticator type is absent.
- b) The **Enroll** button in the **Authenticators** window is greyed out.

Cause:

- a) The RADIUS 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.

Cannot Logon with RADIUS Authenticator

Description:

You cannot logon using RADIUS authenticator.

Cause:

Your computer is not inserted to the list of RADIUS clients.

Solution:

Add your computer to the list of RADIUS clients.

Index

A

Authentication 1, 3-4, 10, 19
Authenticator 3-4, 7, 10, 12, 15, 17, 19, 21

C

Caching 4
Client 3-4
Control 4

E

Enroll 5, 10, 15, 17, 21

L

Logon 3, 8, 21

M

Manage 5, 7, 10
Microsoft Windows Server 2003 7
Microsoft Windows Server 2008 4

N

Network 18

R

RADIUS 1, 3-4, 12, 15, 17, 19, 21
Re-enroll 5, 17
Remove 5, 10, 19

S

Server 4

U

User 4

W

Windows 7
Windows 8 10

Windows Vista 4
Windows XP 7