



NetIQ Advanced Authentication Framework

FIDO U2F Authentication Provider Installation Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
System Requirements	4
Installing and Removing FIDO U2F Authentication Provider	5
Installing FIDO U2F Authentication Provider	5
RDS Farm Support	6
Configuring FIDO U2F Authentication Provider	7
Removing FIDO U2F Authentication Provider	9
Microsoft Windows 7/Microsoft Windows Server 2008 R2	9
Microsoft Windows 8.1/10/ Windows Server 2012/2012 R2	9
Installing and Removing FIDO U2F Authentication Provider via Group Policy	10
Installing FIDO U2F Authentication Provider via Group Policy	11
Removing FIDO U2F Authentication Provider via Group Policy	12
Upgrading FIDO U2F Authentication Provider Components via Group Policy	13
Troubleshooting	14
Cannot Install FIDO U2F Authentication Provider	14
Index	15

Introduction

About This Document

Purpose of the Document

This FIDO U2F Authentication Provider Installation 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 install FIDO U2F authentication provider.

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.

System Requirements

Before installing the product, check that the following system requirements are fulfilled:

- Microsoft Windows 7 (x64/x86) SP1
- Microsoft Windows Server 2008 R2 SP1/Microsoft Windows Server 2012
- FIDO U2F authentication provider should be installed on the computer with already installed NetIQ Advanced Authentication Framework



This authentication provider should be installed on **every** Authenticore Server.

Installing and Removing FIDO U2F Authentication Provider

NetIQ Advanced Authentication Framework™ package includes **FIDO authentication provider**, which allows you to use the FIDO U2F security key for authentication.

Installing FIDO U2F Authentication Provider



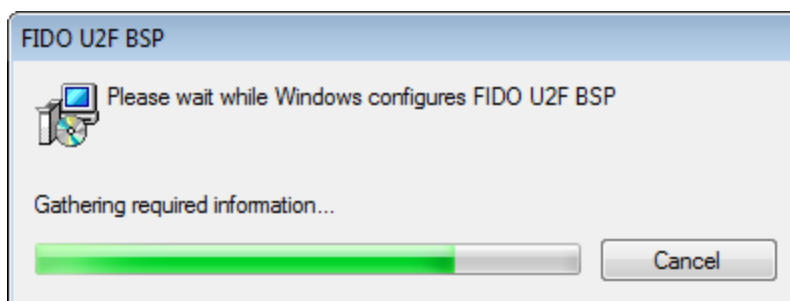
The start of installation may be frozen for a time up to 1 minute in the case of offline mode. This delay occurs due to check of digital signature of component.

To install FIDO U2F Authentication Provider:

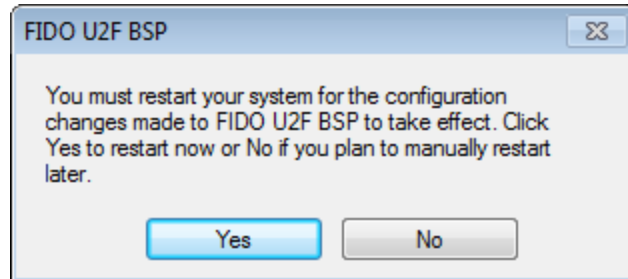
1. Extend schema on server with an applicable server role. If the configured server role is:
 - **AD DS**, schema extension should be performed on DC with **Schema Admins** privileges.
 - **AD LDS**, schema extension should be performed on the unique AD LDS with **Local Admins** privileges.

Follow the steps:

- a. Go to the **FidoU2FBSP** distributives folder.
 - b. Open the **Schema** folder.
 - c. If the configured server role is AD DS, open the **AD** folder. If the configured server role is AD LDS, open the **ADAM** folder.
 - d. Run the **bioU2fData.cmd** file.
 - e. Follow the schema extension.
2. Run the .msi file. **FIDO U2F Authentication Provider** will be automatically installed.



3. Restart your system for the configuration changes made to FIDO U2F authentication provider to take effect. Click **Yes** to restart the system immediately or **No** if you plan to restart it later manually.



! After upgrading FIDO U2F authentication provider, the FIDO U2F AP cache will be automatically cleared. FIDO U2F AP cache allows logging on the given computer using hardware authentication device when Domain Controller is not available. Domain Controller should be obligatory available during the first login after upgrade of FIDO U2F authentication provider.

RDS Farm Support

Before installing FIDO U2F authentication provider on the Remote Desktop Session Host (RD Session Host) server, follow the steps:


1. Install NetIQ Client and FIDO U2F AP on **every** RD Session Host server.
2. Install NetIQ Client and FIDO U2F AP on the thin client in the domain.

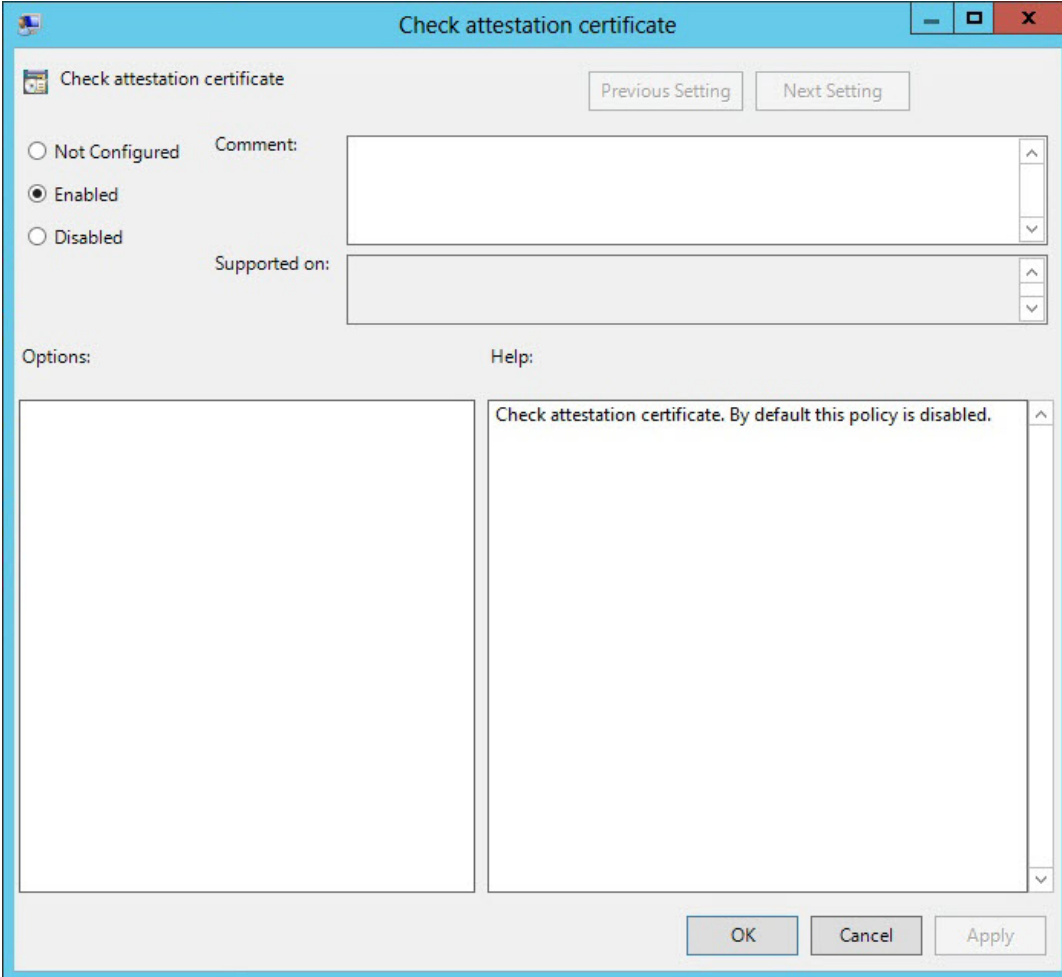
To avoid additional authentication on the thin client, check the [following article](#).

Configuring FIDO U2F Authentication Provider

After the installation of FIDO U2F authentication provider on the Authenticore Server, a new GPO called **FIDO U2F Authentication Provider** will be created.

The **Check attestation certificate** policy allows you to check attestation certificate, which was copied to an applicable directory during installation of FIDO U2F authentication provider. By default the policy is disabled. The certificate is required only if the policy is enabled.

 To add attestation certificate, open the [following certificate](#) and copy it to the directory on Authenticore Server(s): C:\ProgramData\BSP\FIDO U2F BSP\whitelist. Save the file with the **.crt** extension. The attestation certificate should be obligatory saved on **every** Authenticore Server.



The screenshot shows the 'Check attestation certificate' configuration window. It has a title bar with standard Windows window controls. Inside, there's a header section with 'Check attestation certificate' and two buttons: 'Previous Setting' and 'Next Setting'. Below this, there are three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a list box. At the bottom, there are two large text areas: 'Options:' on the left and 'Help:' on the right. The 'Help:' text area contains the text 'Check attestation certificate. By default this policy is disabled.' At the very bottom, there are three buttons: 'OK', 'Cancel', and 'Apply'.

To access the **Check attestation certificate** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> FIDO U2F Authentication Provider**.

Registry settings:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\BioAPI\BSP\FidoU2FBSP

CheckAttestationCertificate:

- value type: REG_DWORD
- value data: 0x00000001 (1)
- description: 1 means that the policy is enabled



The policy should be applied only on Authenticore Servers.

Removing FIDO U2F Authentication Provider

In this chapter:

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

Microsoft Windows 7/Microsoft Windows Server 2008 R2

1. In the **Start** menu, select **Control panel** and then double-click **Programs and Features**.
2. Select **FIDO U2F Authentication Provider** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Microsoft Windows 8.1/10/ Windows Server 2012/2012 R2

1. Right click the **Start** button, select **Programs and Features**.
2. Select **FIDO U2F Authentication Provider** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Installing and Removing FIDO U2F Authentication Provider via Group Policy



It is recommended that Microsoft Windows Server 2003 users should install **Group Policy Management Console**.

To install/remove NetIQ Advanced Authentication Framework Modules, use:

- **Group Policy Management Console (GPMC)**, which is installed by default on a Domain Controller. To open GPMC, click **Start** and select **Administrative Tools > Group Policy Management**.
- **Group Policy Management Editor (GPME)**, which can be opened from GPMC. To open GPME, under domain right-click the group policy object (GPO) you are using to install the software and select **Edit**.



It is highly recommended that you do not use Default Group Policy, because it's applicable to entire domain. It is not recommended to install/upgrade client components for all workstations at the same time.

To create new group policy and configure it:

1. Create new global security group and new group policy object.
2. Connect them:
 - a. Open created group policy object properties;
 - b. Go to the **Security** tab;
 - c. Remove **Apply Group Policy** option for **Authenticated Users** group;
 - d. Add created group and mark **Apply Group Policy** option for it.

Installing FIDO U2F Authentication Provider via Group Policy

To install FIDO U2F authentication provider using the group policy:

1. In GPME, in the selected GPO under **Computer configuration > Policies > Software Settings**, right-click **Software Installation** and select **New > Package**.
2. Specify the network path to the installer package.



The directory you are willing to install should be located on network drive.

3. In the **Deploy Software** dialog, select the **Assigned** option and click **OK**.
4. The installer package name, version, state and path are displayed in **Group Policy Management Editor**.
5. Open package properties:
 - a. On the **Deployment** tab: clear the **Uninstall this application when it falls out of the scope of management** check box. It is done to prevent undesirable uninstallation in case of problems as well as for the upgrade to go properly.
 - b. On the **Deployment** tab: click the **Advanced** button and select the **Ignore language when deploying this package** check box. If you do not select this check box, the package will be installed only on OS with package's language.
 - c. Clear the **Make this 32-bit X86 application available to Win64 machines** check box (if this option is available).
6. Add appropriate 64-bit installer to this group policy object and use settings 5a-5b.





The assigned package is installed after you have updated the domain policy and restarted your computer. To update the domain policy immediately, use the `gpupdate /force` command.

Removing FIDO U2F Authentication Provider via Group Policy

To remove FIDO U2F authentication provider using the group policy:

1. In GPME, under **Computer Configuration > Software Settings > Software installation**, right-click the deployed package and select **All tasks > Remove**.
2. In the **Remove Software** dialog, click **Immediately uninstall the software from users and computers** and then click **OK**.

 The package is removed after you have updated the domain policy and restarted your computer. To update the domain policy immediately, use the `gpupdate /force` command.

 If you have removed option **Uninstall this application when it falls out of the scope of management** as it was recommended, software will not be uninstalled after selecting **Immediately uninstall the software from users and computers**. In this case, you will need to uninstall it via **Programs and Features/Add or remove programs**. Also see [Removing FIDO U2F Authentication Provider](#) chapter.

Upgrading FIDO U2F Authentication Provider Components via Group Policy

Option 1: You can add .msi package with new component version to an existing group policy object. However, this option does not prove to be good, because in case of any problems in new version of component, these problems spread on all computers in installation group.


Option 2: The more reliable upgrading procedure implies creating new group policy object for new installers:

1. Create new installation group and new Group Policy Object (GPO), add a new .msi package in it.
2. After having configured software installation, go to **Upgrades** tab of package properties.
3. Click the **Add** button.
4. In the **Add Upgrade Package** dialog, please select the **A specific GPO** option.
5. Select a GPO which was used for installation of previous NetIQ Advanced Authentication Framework version.
6. Select .msi package name.
7. Select the **Uninstall the existing package, then install the upgrade package** option.



Make sure that your new GPO is above the old one in the GPO list.

Troubleshooting

 This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

Cannot Install FIDO U2F Authentication Provider

Description:

Error appears when installing FIDO U2F authentication provider on your computer.

Cause:

- a. You have no space left on the disk.
- b. You are installing FIDO U2F authentication provider on the OS with the wrong bitness.
- c. You are installing card authentication provider before installing NetIQ Advanced Authentication Framework.

Solution:

- a. Free the amount of disk space needed for installation.
- b. Check your OS's bitness (x64/x86) and run the corresponding installer (x64/x86).
- c. Install NetIQ Advanced Authentication Framework first.

Index

A

Authentication 1, 3-5, 7, 9-14
Authenticator 3

C

Client 3, 6
Console 10
Control panel 9
Create 10, 13

D

Default 10
Domain 6, 10

E

Error 14

G

GPMC 10
GPME 10-12

L

Local 5
Logon 3

M

Microsoft Windows Server 2003 10
Microsoft Windows Server 2008 4
Microsoft Windows Server 2012 9

P

Package 11, 13
Policy 8, 10-11

R

Remote 6
Remove 10, 12

S

Security 10
Server 4, 7
Software 11-12
Support 6
System 4

W

Windows 7 4, 9
Windows 8 9