



NetIQ Advanced Authentication Framework

Lumidigm 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 Lumidigm Authentication Provider	5
Pre-installation Procedure	5
Installing Lumidigm Authentication Provider	6
Configuring Lumidigm Authentication Provider via Group Policy	7
PIN Required	7
Removing Lumidigm Authentication Provider	9
Microsoft Windows 7/Microsoft Windows Server 2008 R2	9
Microsoft Windows 8.1/10	9
Installing and Removing Lumidigm Authentication Provider via Group Policy	10
Installing Lumidigm Authentication Provider via Group Policy	11
Removing Lumidigm Authentication Provider via Group Policy	15
Upgrading Lumidigm Authentication Provider via Group Policy	17
Troubleshooting	19
Cannot Install Lumidigm Authentication Provider	19
Index	20

Introduction

About This Document


Purpose of the Document


This Lumidigm 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 Lumidigm fingerprint type of authenticators.

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.

System Requirements


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

- Microsoft Windows 7 (x64/x86) SP1/Microsoft Windows 8.1 (x64/x86)
- Microsoft Windows 2008 Server R2 SP1
- Lumidigm fingerprint 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 Lumidigm Authentication Provider

NetIQ Advanced Authentication Framework™ package includes Lumidigm Authentication Provider, which allows you to use Lumidigm hardware authentication devices.

 Unlike NetIQ Advanced Authentication Framework components that may also be installed via Group Policy, Lumidigm Authentication Provider can only be installed through the Setup Wizard.

Pre-installation Procedure

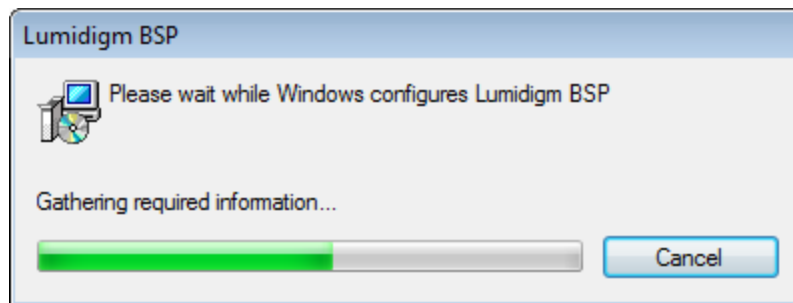
Before installing Lumidigm Authentication Provider you should make preparations. Follow the steps below and complete all pre-installation activities:

1. Mind that you should run the file that corresponds to the bitness of your computer (either [x64](#) or [x86](#)).
2. Install Lumi_NON_STR_Drivers_Setup_5.00.exe and LumiDvcSvc_5.00.exe from authenticators distributive kit.

Installing Lumidigm Authentication Provider

To install Lumidigm Authentication Provider:

1. Run the .exe file. **Lumidigm Authentication Provider** will be automatically installed on your computer.



- ✖ 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.
- ✖ For your Lumidigm fingerprint reader to work properly, you should install the corresponding driver. The driver should be installed on the client part.


Configuring Lumidigm Authentication Provider via Group Policy


If PIN is needed for authentication besides fingerprint, it will be required to enable the [PIN required](#) policy.

PIN Required

With the **PIN required** policy enabled, a PIN is required together with the fingerprint to authenticate. When the **Use domain password instead of PIN** policy is also configured, the domain password needs to be used in combination with fingerprint. It is also possible to enable **PIN Caching** with Authentication Provider. By default this policy is disabled.

The screenshot shows the 'PIN required' Group Policy configuration dialog box. The title bar reads 'PIN required'. Inside the dialog, there are two buttons: 'Previous Setting' and 'Next Setting'. Below these, there are three radio button options: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these options is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' dropdown menu. At the bottom of the dialog, there are two sections: 'Options:' and 'Help:'. The 'Options:' section is currently empty. The 'Help:' section contains the following text: 'With this policy enabled a PIN is required together with the fingerprint to authenticate. When the policy "use domain password instead of PIN" is also configured the domain password needs to be used in combination with the fingerprint. It is also possible to enable PIN Caching with this Authentication Provider. By default this policy is disabled.' At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

 To use domain password instead of PIN, enable the **Use domain password as PIN** policy.

 To enable the **PIN Required** policy together with the **Use domain password as PIN** policy, it is necessary to install Password Filter on all Domain Controllers. Otherwise if the password is reset, changed or generated automatically, the password will be desynchronized and it will be required to re-enroll authenticator.

To access the **PIN required** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> Lumidigm Authentication Provider**.

Registry settings:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\BioAPI\BSP\LumidigmBSP

PinRequired:

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

Removing Lumidigm Authentication Provider

In this chapter:

- [Microsoft Windows 7/Microsoft Windows Server 2008 R2](#)
- [Microsoft Windows 8.1](#)

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 **Lumidigm Authentication Provider** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Microsoft Windows 8.1/10

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

Installing and Removing Lumidigm Authentication Provider via Group Policy

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 is applicable to entire domain. It is not recommended to install/upgrade client components for all workstations at the same time.

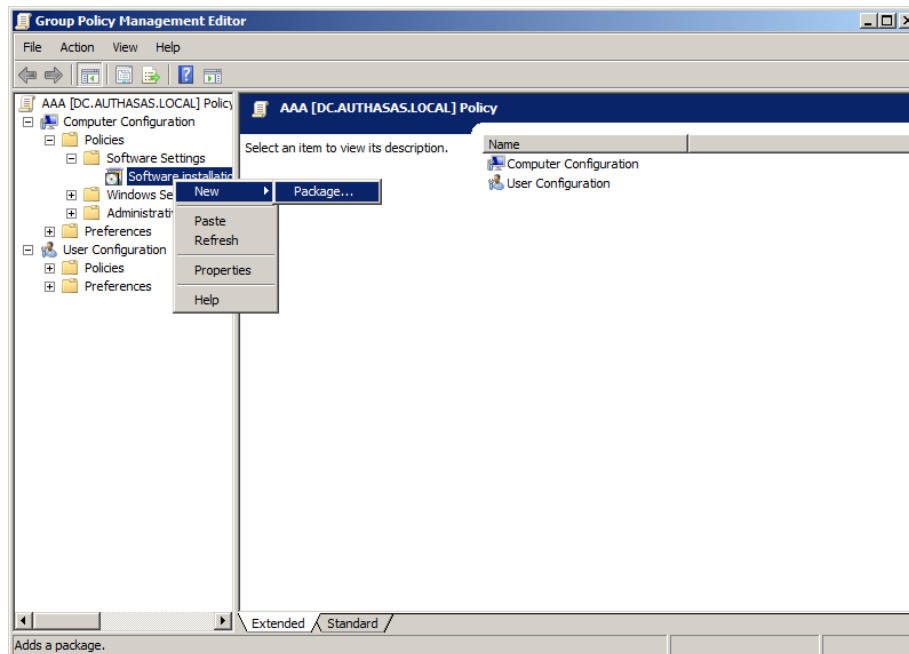
To create new Group Policy and configure it:

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. Clear the **Apply Group Policy** check box for the **Authenticated Users** group;
 - d. Add created group and select the **Apply Group Policy** check box for it.

Installing Lumidigm Authentication Provider via Group Policy

To install an Lumidigm authentication provider using the group policy:

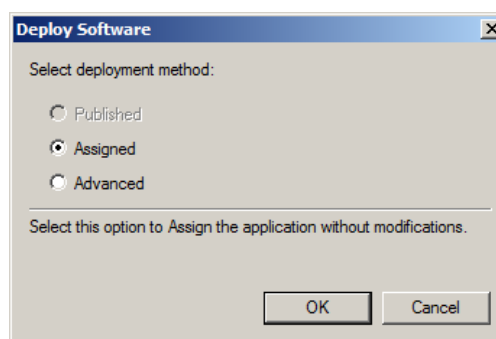
1. In GPME, in the selected GPO under **Computer configuration > Policies > Software Settings**, right-click **Software Installation** and select **New > Package**.



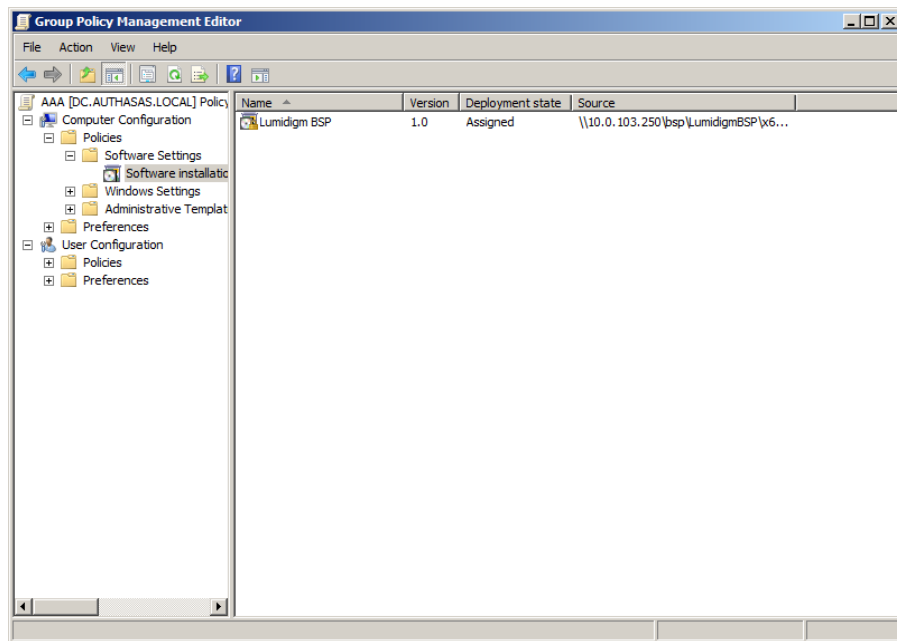
2. Specify the network path to the installer package.

 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**.

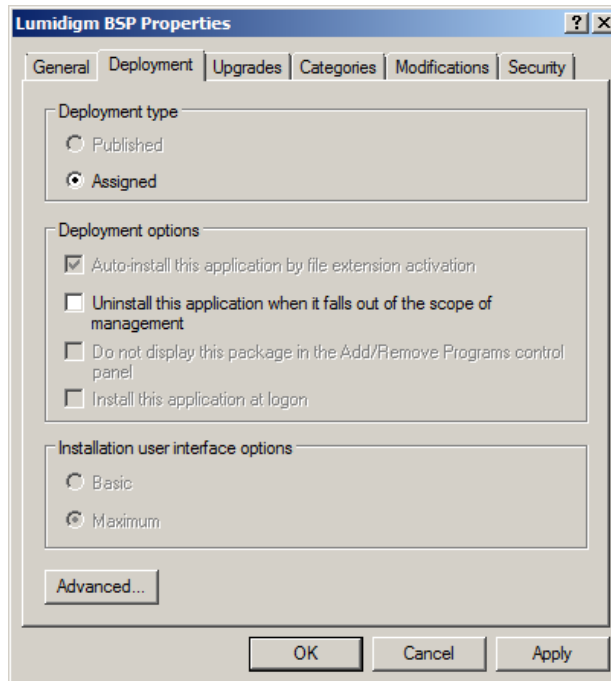


4. The installer package name, version, state and path are displayed in **Group Policy Management Editor**.

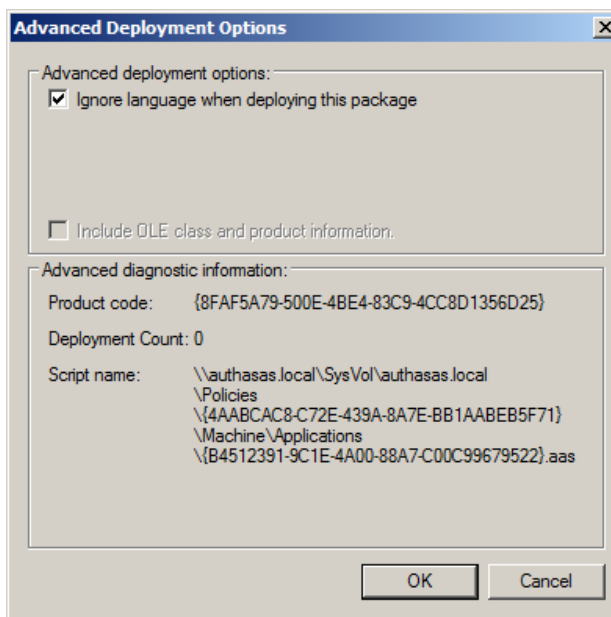


5. Open package properties:

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).

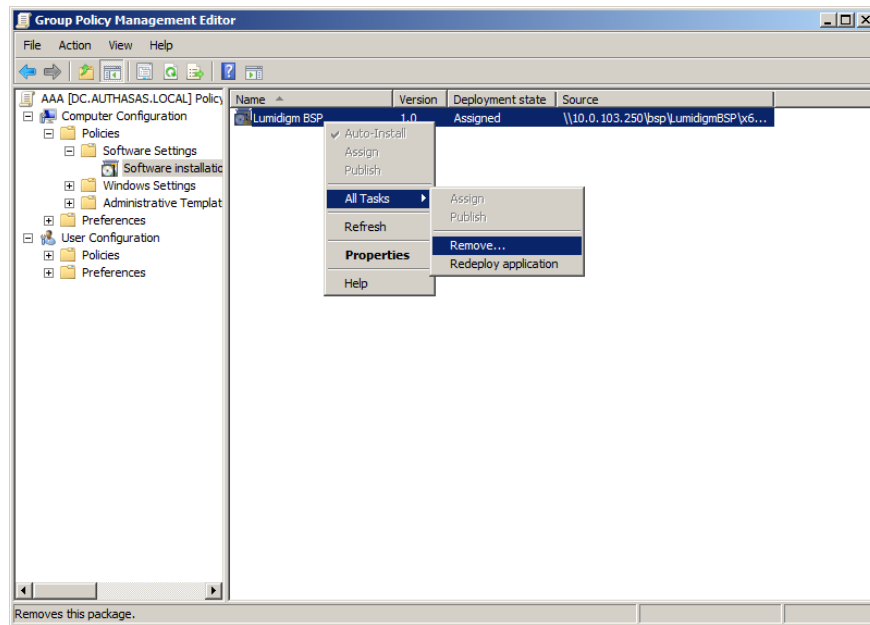
6. Add appropriate 64-bit installer to this group policy object and use settings 5a)-5b).

 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.

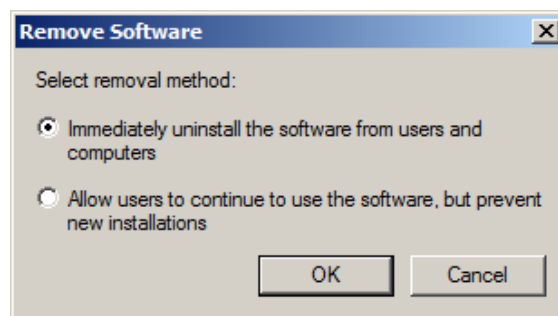
Removing Lumidigm Authentication Provider via Group Policy

To remove Lumidigm 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, select the **Immediately uninstall the software from users and computers** option and 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 cleared the **Uninstall this application when it falls out of the scope of management** check box as it was recommended, software will not be uninstalled after

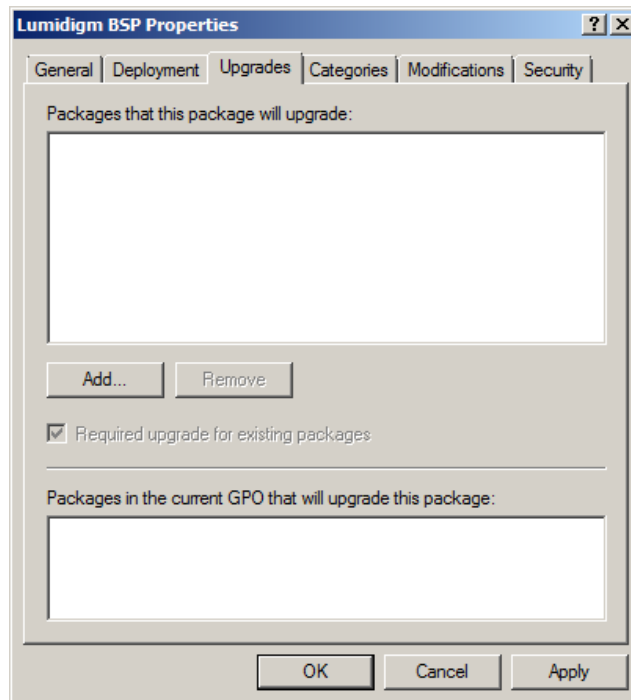
selecting the **Immediately uninstall the software from users and computers** option. In this case, you will need to uninstall it via **Programs and Features/Add or remove programs**. See the [Removing Lumidigm Authentication Provider](#) chapter.

Upgrading Lumidigm Authentication Provider via Group Policy

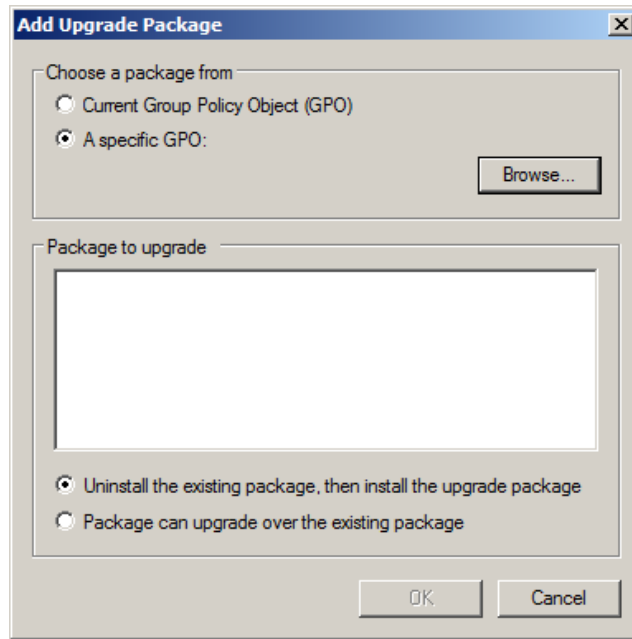
Option 1: You can add .msi package with new component version to an existing group policy object. However, this option does not prove to be good, because in case of any problems in new version of component, these problems spread on all computers in installation group.

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 the **Upgrades** tab of package properties.




3. Click the **Add** button.
4. In the **Add Upgrade Package** dialog, 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

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

Cannot Install Lumidigm Authentication Provider

Description:

Error appears when installing Lumidigm fingerprint authentication provider on your computer.

Cause:

- a. You are installing Lumidigm fingerprint authentication provider on the network drive.
- b. You have no space left on the disk.
- c. You are installing Lumidigm fingerprint authentication provider on the OS with the wrong bitness.

Solution:

- a. Change the installation path.
- b. Free the amount of disk space needed for installation.
- c. Check your OS's bitness (x64/x86) and run the corresponding installer (x64/x86).

Index

A

Authentication 1, 3-7, 10, 16, 18
Authenticator 3

C

Caching 7
Client 3
Control panel 9
Create 10, 17

D

Default 10
Domain 10

E

Error 19

G

GPMC 10
GPME 10-11, 15

L

Logon 3
Lumidigm 1, 3-11, 15, 17, 19

P

Package 11, 17
Password 8
PIN 7
Policy 5, 8, 10, 12

R

Remove 15

S

Security 10
Server 4
Software 11, 15

System 4

W

Windows 4

Windows 7 4, 9

Windows 8 9