NetIQ Advanced Authentication Framework

Digital Persona Authentication Provider Installation Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This Digital Persona 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 Digital Persona 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.

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, 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:

- Windows 7 (x64/x86) SP1/ Microsoft Windows 8 (x86/x64)/ Microsoft Windows 8.1 (x86/x64);
- Digital Persona 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 Digital Persona Authentication Provider

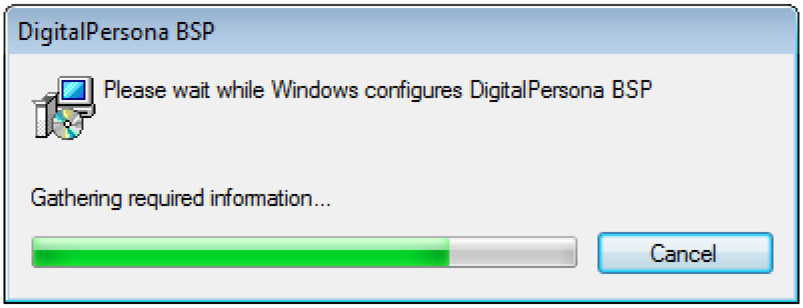
NetIQ Advanced Authentication Framework™ package includes Digital Persona Authentication Provider, which allows you to use Digital Persona hardware authentication devices.

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

Installing Digital Persona Authentication Provider

To install Digital Persona Authentication Provider:

1. Run **DigitalPersonaBSPInstall.exe** from Digital Persona authentication provider distributive kit. **Digital Persona Authentication Provider** and **Digital Persona RTE** will be automatically installed on your computer.



DigitalPersona BSP

Please wait while Windows configures DigitalPersona BSP

Gathering required information...

✱ If you need MSI for bulk installation instead of **DigitalPersonaBSPInstall.exe**, you can install **DigitalPersonaBSP.msi** and **rte.msi**.

✱ 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.

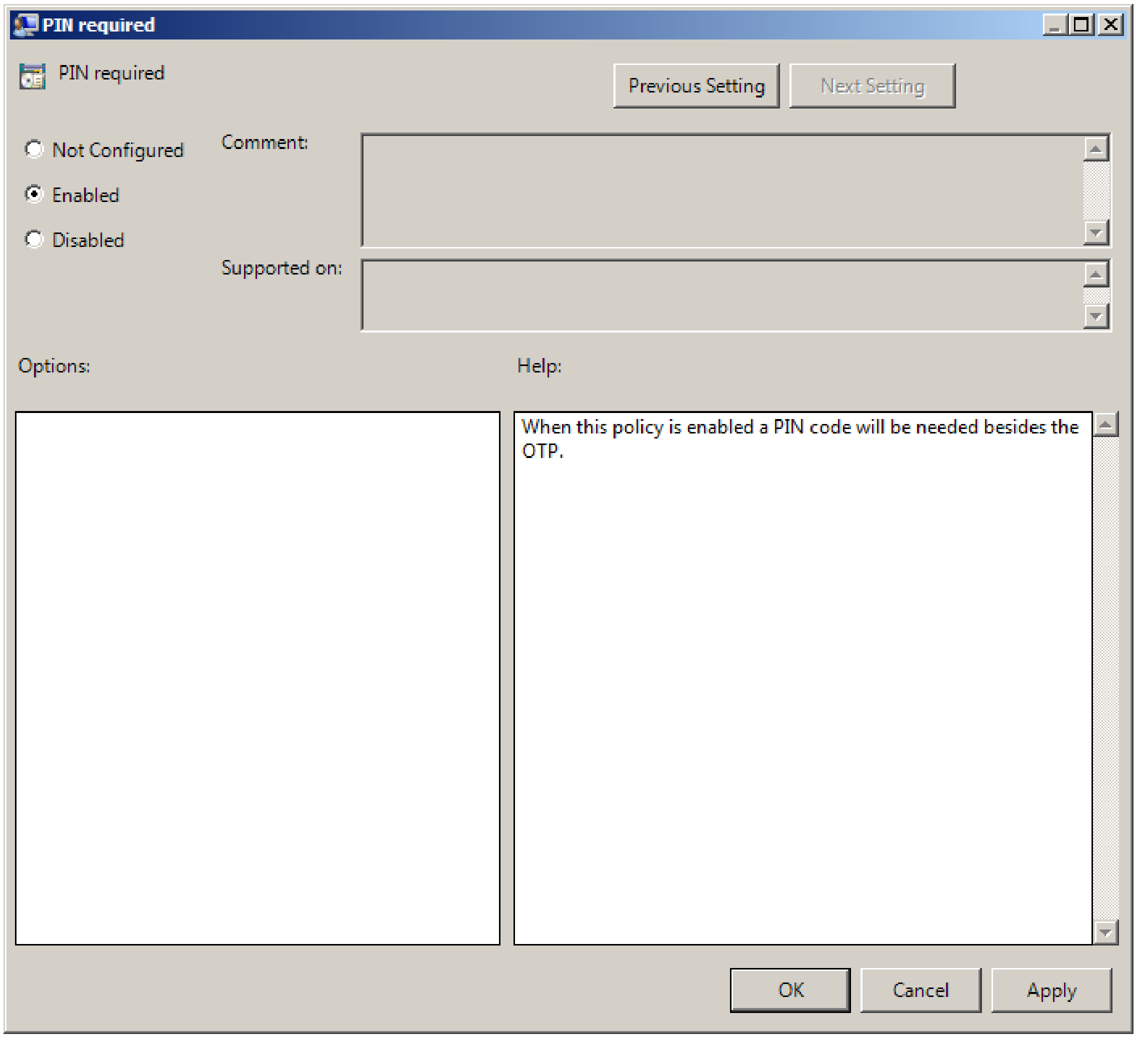
✱ For your Digital Persona fingerprint reader to work properly, you should install the corresponding driver. The driver should be installed on the client part.

Configuring Digital Persona Authentication Provider via Group Policy

If a PIN code is needed for authentication besides fingerprint, it is required to enable the PIN Required policy.

PIN required

When the **PIN required** policy is enabled, a PIN code will be needed for authentication besides fingerprint.



○ Not Configured
● Enabled
○ Disabled

When this policy is enabled a PIN code will be needed besides the OTP.

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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BioAPI\BSP\OathBSP
parameter: PinRequired (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

Removing Digital Persona Authentication Provider

In this chapter:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2012

Microsoft Windows Server 2008

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

Microsoft Windows Server 2012

1. In the **Search** menu, select **Apps > Control Panel > Programs > Programs and Features**.
2. Select **Digital Persona Authentication Provider** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Installing and Removing Digital Persona Authentication Provider via Group Policy

It is recommended for Microsoft Windows Server 2003 users to 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 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.

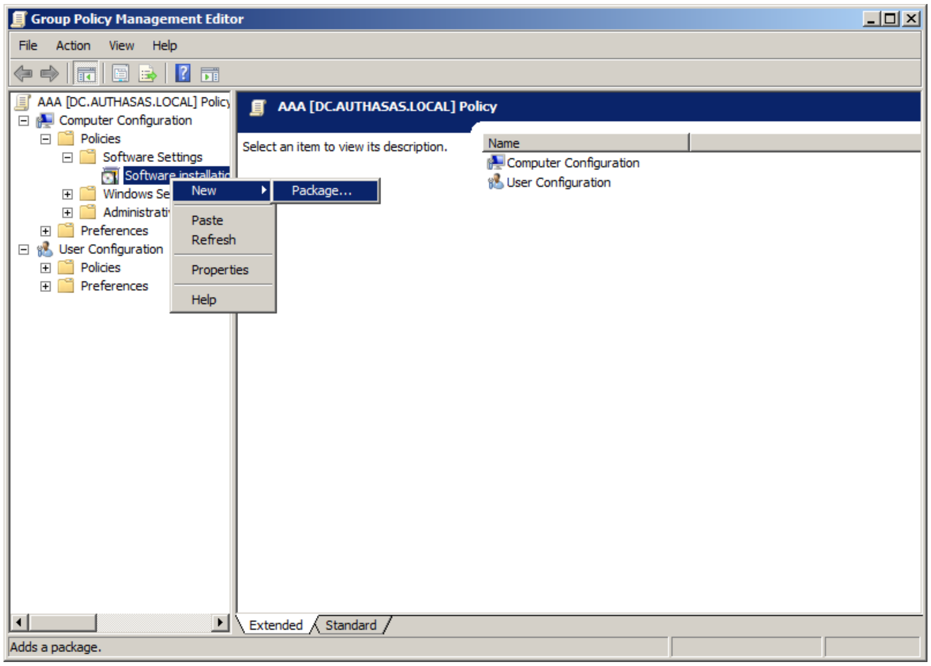
2. Connect them:

   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 Digital Persona Authentication Provider via Group Policy

To install an Digital Persona authentication provider using the group policy:

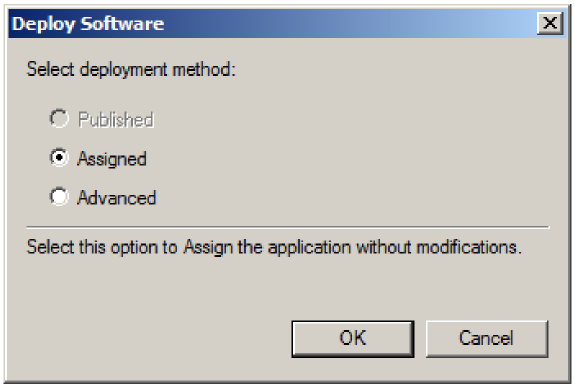
1. In GPME, in the selected GPO under **Computer configuration > Policies > Software Settings**, right-click **Software Installation** and select **New > Package**.



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**.


Deploy Software

Select deployment method:

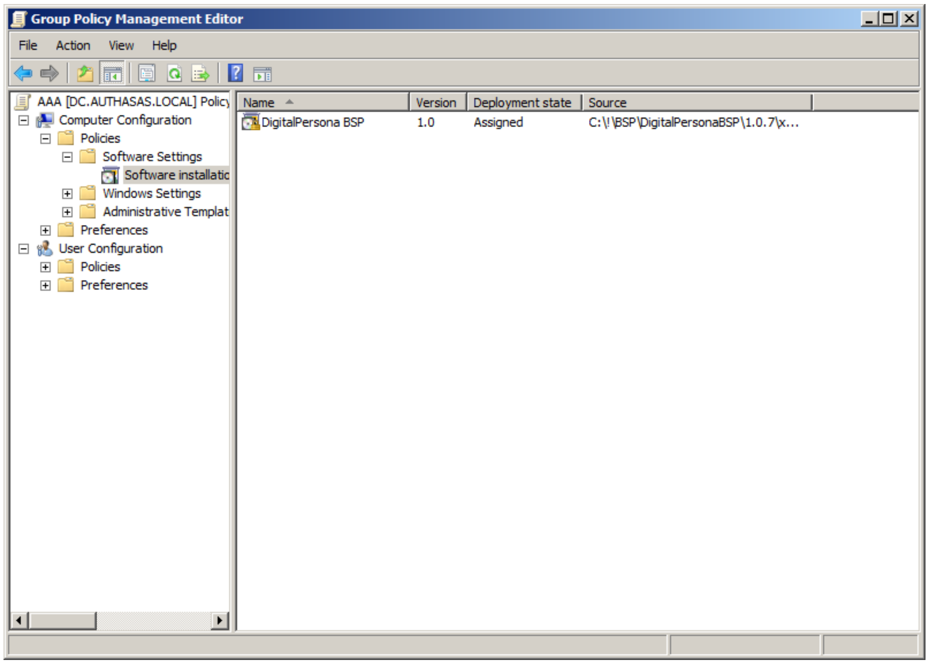
○ Published

● Assigned

○ Advanced

Select this option to Assign the application without modifications.

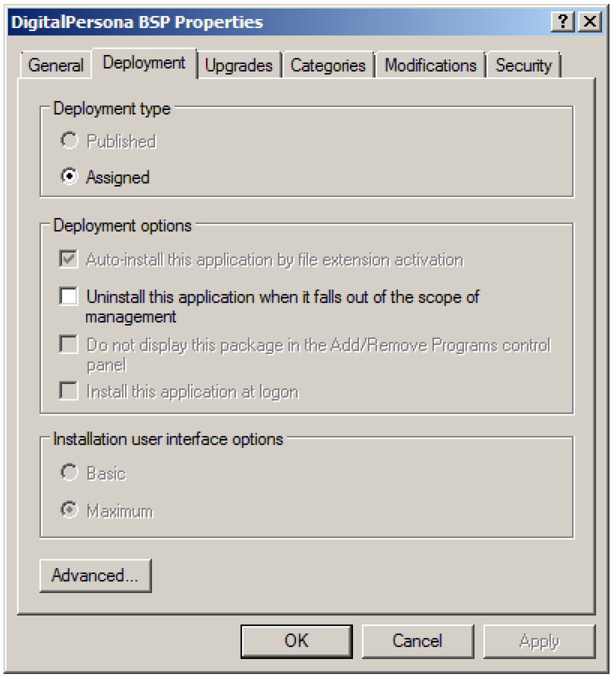
4. The installer package name, version, state and path are displayed in **Group Policy Management Editor**.



Name	Version	Deployment state	Source
DigitalPersona BSP	1.0	Assigned	C:\!\BSP\DigitalPersonaBSP\1.0.7\x...

5. Open package properties:

a) On the **Deployment** tab: clear the **Uninstall this application when it falls out of the scope of management** box. It is done to prevent undesirable uninstallation in case of problems as well as for the upgrade to go properly.



Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

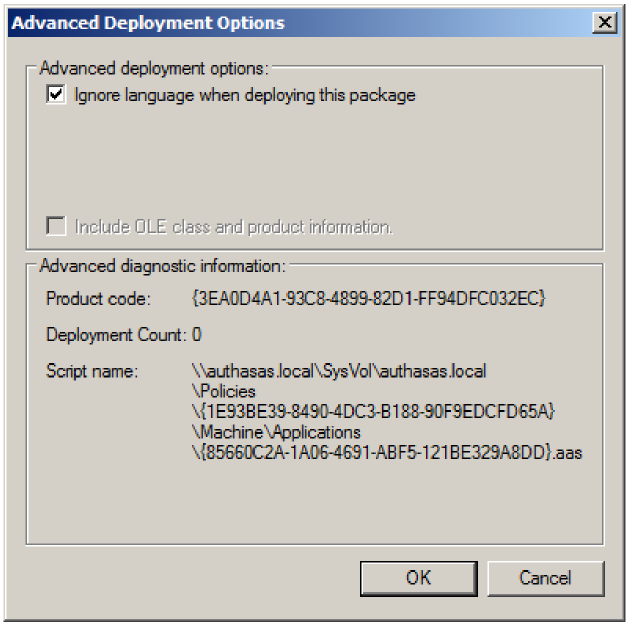
□ Install this application at logon

Installation user interface options

○ Basic

● Maximum

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.



Advanced deployment options:

☑ Ignore language when deploying this package

□ Include OLE class and product information.

Advanced diagnostic information:

Product code: {3EA0D4A1-93C8-4899-82D1-FF94DFC032EC}

Deployment Count: 0

Script name: \\authasas.local\SysVol\authasas.local
\Policies
\{1E93BE39-8490-4DC3-B188-90F9EDCFD65A}
\Machine\Applications
\{85660C2A-1A06-4691-ABF5-121BE329A8DD}.aas

c) Clear the **Make this 32-bit X86 application available to Win64 machines** check box (if this option is available).

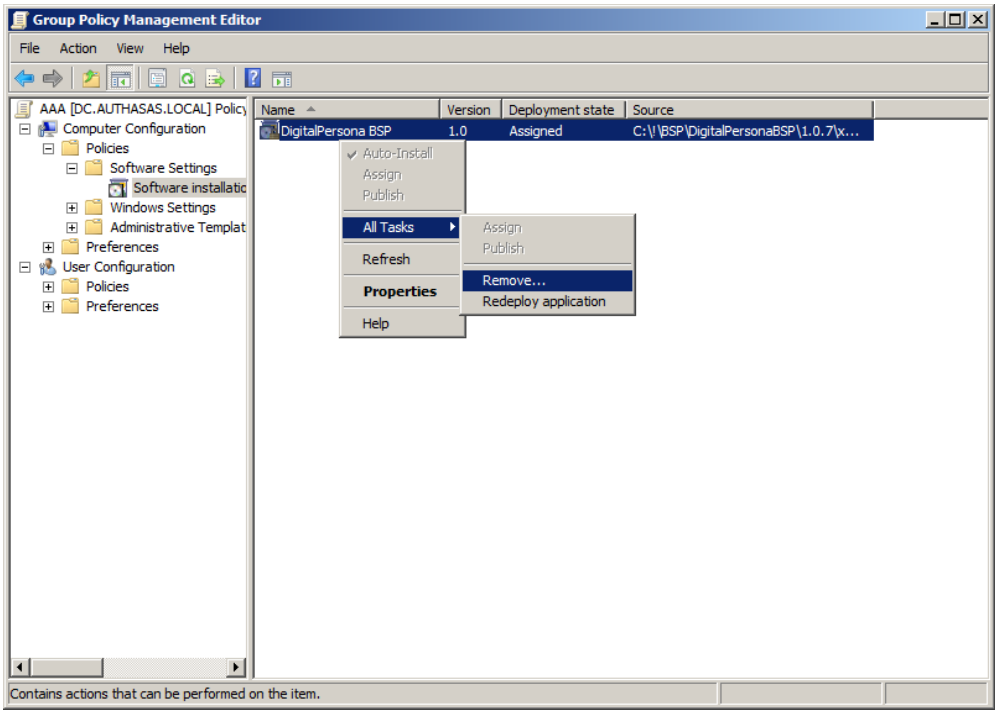
6. Add appropriate 64-bit installer to this group policy object and use settings 5a)-5b).

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 Digital Persona Authentication Provider via Group Policy

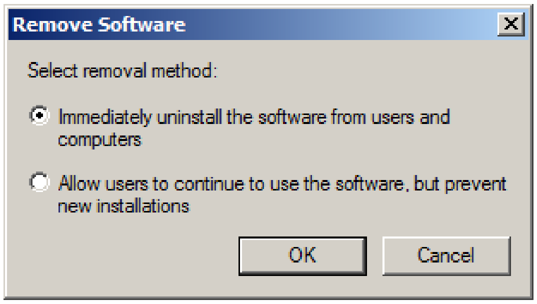
To remove Digital Persona authentication provider using the group policy:

1. In GPOE, under **Computer Configuration > Software Settings > Software installation**, right-click the deployed package and select **All tasks > Remove**.



Name	Version	Deployment state	Source
DigitalPersona BSP	1.0	Assigned	C:\!\BSP\DigitalPersonaBSP\1.0.7\x...

2. In the **Remove Software** dialog, select the **Immediately uninstall the software from users and computers** option and click **OK**.



Select removal method:

● Immediately uninstall the software from users and computers

○ Allow users to continue to use the software, but prevent new installations

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 Digital Persona Authentication Provider chapter.

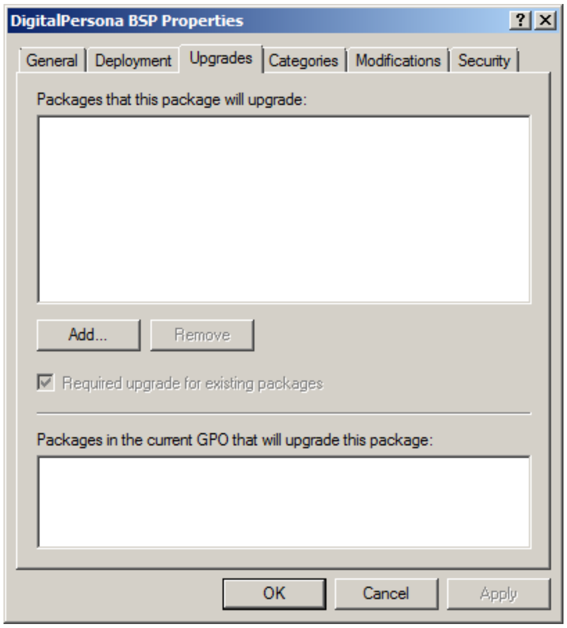
Upgrading Digital Persona Authentication Provider via Group Policy

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.

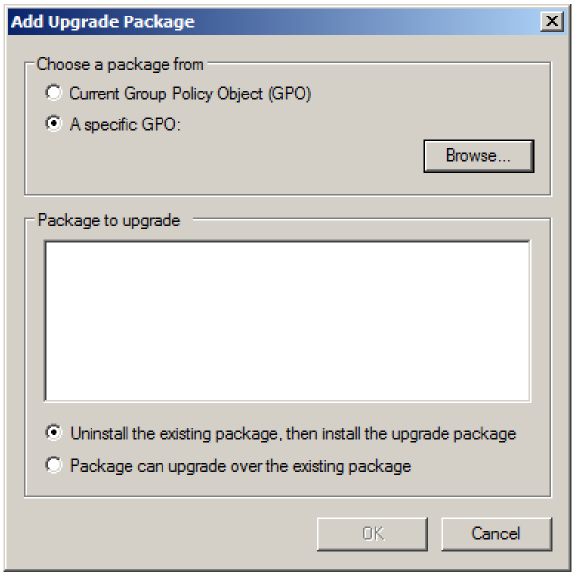
2. After having configured software installation, go to the **Upgrades** tab of package properties.


DigitalPersona BSP Properties
?
X
General
Deployment
Upgrades
Categories
Modifications
Security
Packages that this package will upgrade:
Add...
Remove
Packages in the current GPO that will upgrade this package:
OK
Cancel
Apply

☑ Required upgrade for existing packages

3. Click the **Add** button.

4. In the **Add Upgrade Package** dialog, select the **A specific GPO** option.



Choose a package from

○ Current Group Policy Object (GPO)

● A specific GPO:

Package to upgrade

● Uninstall the existing package, then install the upgrade package

○ Package can upgrade over the existing package

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 Digital Persona Authentication Provider

Description:

Error appears when installing Digital Persona fingerprint authentication provider on your computer.

Cause:

a. You are installing Digital Persona fingerprint authentication provider on the network drive.
b. You have no space left on the disk.
c. You are installing Digital Persona 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