

NetIQ Advanced Authentication Framework

Digital Persona Authentication Provider Installation Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	
About This Document	
System Requirements	4
Installing and Removing Digital Persona Authentication Provider	
Installing Digital Persona Authentication Provider	5
Configuring Digital Persona Authentication Provider via Group Policy	6
Number of Fingers to Enroll	6
PIN Required	7
Removing Digital Persona Authentication Provider	
Microsoft Windows 7	9
Microsoft Windows 8.1	9
Installing and Removing Digital Persona Authentication Provider via Group Policy	10
Installing Digital Persona Authentication Provider via Group Policy	11
Removing Digital Persona Authentication Provider via Group Policy	15
Upgrading Digital Persona Authentication Provider via Group Policy	17
Troubleshooting	19
Cannot Install Digital Persona Authentication Provider	19
Index	20

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.

Simportant 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:

- Windows 7 (x64/x86) SP1/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.

Onlike 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
Cancel

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.

Sor 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

The following policies allow you to modify enrollment parameters of Digital Persona authentication provider:

- Number of fingers to enroll
- PIN required

Number of Fingers to Enroll

The **Number of fingers to enroll** policy allows you to specify the number of fingers a user can enroll. A user can enroll from 1 to 10 fingers. This policy is valid only for Digital Persona authentication provider.

💭 NumFingersToEnroll		
NumFingersToEnroll	Previous Setting Next Setting	
 Not Configured Comment: Enabled Disabled Supported on: 		N N N
Options:	Help:	
MinNumFingersToEnroll 1 MaxNumFingersToEnroll 10	NumFingersToEnroll_Explain	×
	OK Cancel	Apply

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)Policies\BioAPI\BSP\DigitalPersonaBSP **MaxNumFingersToEnroll**:

- type: REG_DWORD;
- value: 0x0000000a (10);
- description: 10 displays the maximum number of fingers to enroll.

MinNumFingersToEnroll:

- type: REG_DWORD;
- value: 0x0000001 (1);
- description: 1 displays the minimum number of fingers to enroll.

If the policy is not configured or is disabled, a user can enroll as many fingers he/she wants (from 1 to 10).

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.

🔙 PIN required						×
PIN required		Previous Se	etting Ne	ext Setting		
C Not Configured Enabled Disabled	Comment:				2	-
O Disabled	Supported on:				-	
Options:		Help:				
		With this policy enabled fingerprint to authentic password instead of PIN needs to be used in con possible to enable PIN (By default this policy is	ate. When the N" is also confi nbination with Caching with t	policy "use don gured the doma the fingerprint.	nain iin password It is also	×
			ОК	Cancel	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.

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)Policies\BioAPI\BSP\DigitalPersonaBSP **PinRequired**:

- type: REG_DWORD;
- value: 0x0000001 (1);
- description: 1 means that the policy is enabled.

Removing Digital Persona Authentication Provider

In this chapter:

- Microsoft Windows 7
- Microsoft Windows 8.1

Microsoft Windows 7

- 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 8.1

- 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**.

File Action View Help AAA [DC.AUTHASAS.LOCAL] Policy Computer Configuration Policies Windows Set Paste Refresh Policies Policies Policies Help Extended Extended Standard	🗐 Group Policy Management Editor	_ _ _ _ _ _ _ _ _ _ _
AAA [DC.AUTHASAS.LOCAL] Policy Computer Configuration Conf	File Action View Help	
Computer Configuration Computer Configuration Software settings Windows Se Windows Se Preferences Sect an item to view its description. Package Package Package Package Package Package Preferences Help		
	Computer Configuration Software Settings Software instabilist Mame Select an item to view its description. Select	tion
Adds a package.		

2. Specify the network path to the installer package.

 \mathfrak{B} 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:	
C Published	
Assigned	
O Advanced	
Select this option to Assign the application without modifications.	
OK Cancel	

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** box. It is done to prevent undesirable uninstallation in case of problems as well as for the upgrade to go properly.

DigitalPersona BSP Properties					
General Deployment Upgrades Categories Modifications Security					
Deployment type					
C 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					
C Basic					
C Maximum					
Advanced					
OK Cancel Apply					

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.

A	dvanced Deployr	nent Options	X				
	Advanced deployment options:						
	🗖 Include OLE	class and product information.					
	Advanced diagno	stic information:					
	Product code:	{3EA0D4A1-93C8-4899-82D1-FF94DFC032EC}					
	Deployment Cour	nt: 0					
	Script name:	\\authasas.local\SysVol\authasas.local \Policies \{1E938E39-8490-4DC3-8188-90F9EDCFD65A} \Machine\Applications \{85660C2A-1A06-4691-ABF5-121BE329A8DD}.aas	3				
		OK Cancel					

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**.

📕 Group Policy Management Edito	or				
File Action View Help					
🗢 🔿 🖄 📅 📮 🧟 😖 🖡	? 🖬				
AAA [DC.AUTHASAS.LOCAL] Policy		Version	Deployment state		
 E Computer Configuration Policies 	DigitalPersona BSP	1.0	Assigned	C:\!\BSP\DigitalPersonaBSP\1.0.7\x	
🖃 🚞 Software Settings	Assign				
Software installatic ⊕ 🧰 Windows Settings	Publish				
🕀 📔 Administrative Templat	All Tasks	As:	sign		
	Refresh	Put	olish	_	
Ser Corriguration E Policies	Properties		move		
🕀 🚞 Preferences	Help	Re	deploy application		
Contains actions that can be performed	on the item.				

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

Remove Software
Select removal method:
 Immediately uninstall the software from users and computers
C Allow users to continue to use the software, but prevent new installations
OK Cancel

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 <u>Removing</u>_ 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	×
General Deployment Upgrades Categories Modifications Security	
Packages that this package will upgrade:	
Add Remove	
nou	
Required upgrade for existing packages	
Packages in the current GPO that will upgrade this package:	
	-
OK Cancel Apply	

- 3. Click the **Add** button.
- 4. In the Add Upgrade Package dialog, select the A specific GPO option.

Add Upgrade Package
Choose a package from
C Current Group Policy Object (GPO)
A specific GPO:
Browse
Package to upgrade
 Uninstall the existing package, then install the upgrade package Package can upgrade over the existing package
OK Cancel

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.

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

Troubleshooting

1 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

	Α	
Authentication 1, 3-7, 9-11, 15, 17, 19 Authenticator 3		
	C	
Caching 7 Client 3 Console 10 Control 9		
Control panel 9 Create 10, 17		
	D	
Default 10 Domain 10		
	E	
Enroll 6 Error 19		
	G	
GPMC 10 GPME 10-11		
	L	
Logon 3		
	Μ	
Microsoft Windows Server 2003 10		
	Ρ	
Package 11, 17 Password 8 PIN 6-7		
Policy 5, 10, 12		
	R	
Remove 15		

RTE 5

Security 10 Server 4 Software 11, 15 System 4

W

S

Windows 7 4, 9 Windows 8 9