



NetIQ Advanced Authentication Framework

Smartphone Authentication AD Service 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 Smartphone Authentication AD Service	5
Installing Smartphone Authentication AD Service	5
Extending Schema for Smartphone Authentication AD Service	9
Removing Smartphone Authentication AD Service	10
Microsoft Windows Server 2008 R2	10
Microsoft Windows Server 2012/Microsoft Windows 2012 R2	10
Index	11

Introduction

About This Document


Purpose of the Document


This Smartphone Authentication AD Service Installation Guide is intended for all system administrators and describes how to install Smartphone Authentication AD Service.

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

The following system requirements should be fulfilled:

- Microsoft Windows Server 2008 R2 SP1/Microsoft Windows Server 2012/Microsoft Windows Server 2012 R2




Smartphone Authentication AD service should be installed on **every** Authenticore Server.

Installing and Removing Smartphone Authentication AD Service

Smartphone Authentication AD service is designed to provide connection between Smartphone Authentication Dispatcher and an applicable data storage. Smartphone Authentication AD service stores every new push ID, which is sent from the mobile device, in the data storage of Smartphone Authentication Dispatcher. If Smartphone Authentication AD service is not running, the push notification will not be sent to the mobile device with the installed NetIQ Smartphone Authenticator.

Installing Smartphone Authentication AD Service

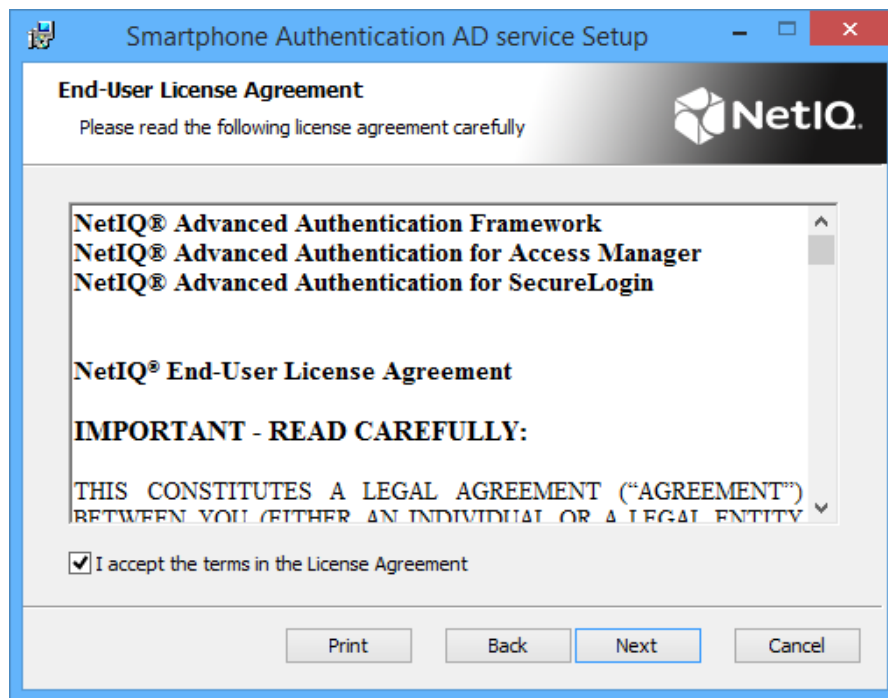
 The start of installation may be frozen for a time up to 1 minute in the case of offline mode. This delay occurs due to check of digital signature of component.

To install Smartphone Authentication AD service:

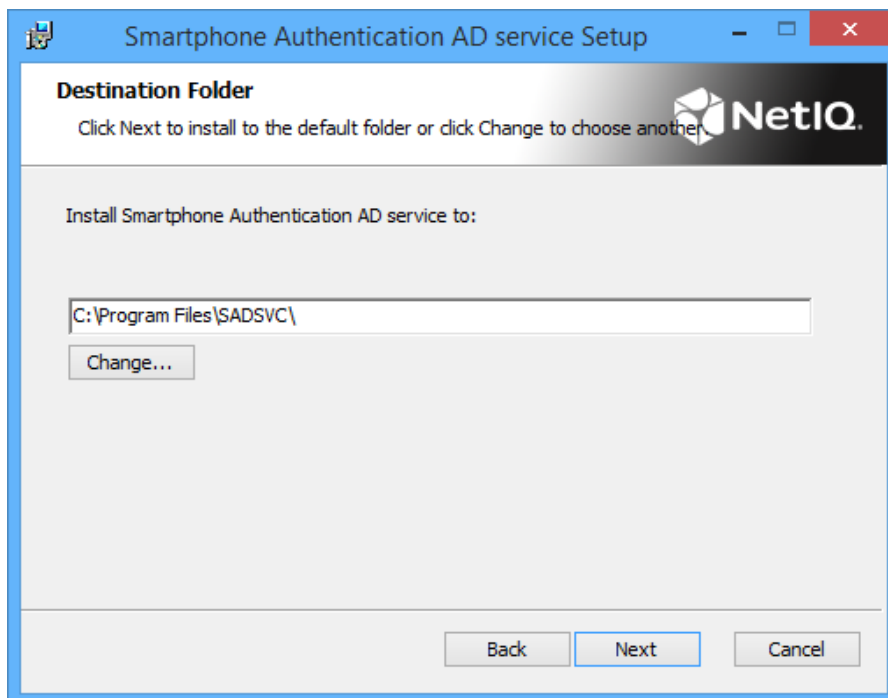
1. Run **SmartphoneAdServiceSetup.msi**. The **Smartphone Authentication AD service Setup** window will be displayed. Click **Next** to continue.



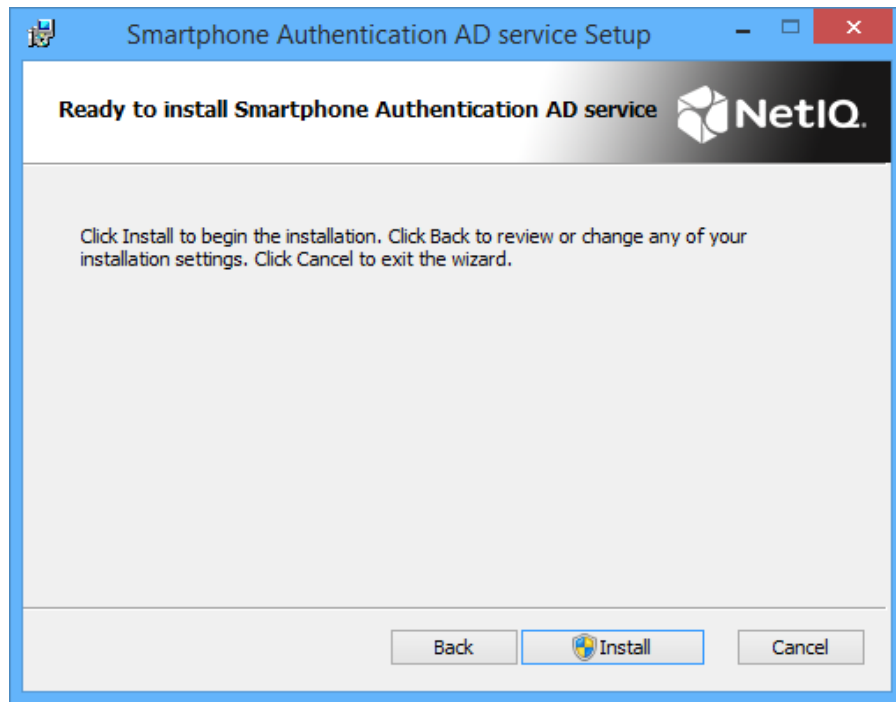
2. Read the **License Agreement**. Select the **I accept the terms in the License Agreement** checkbox and click **Next** to continue.



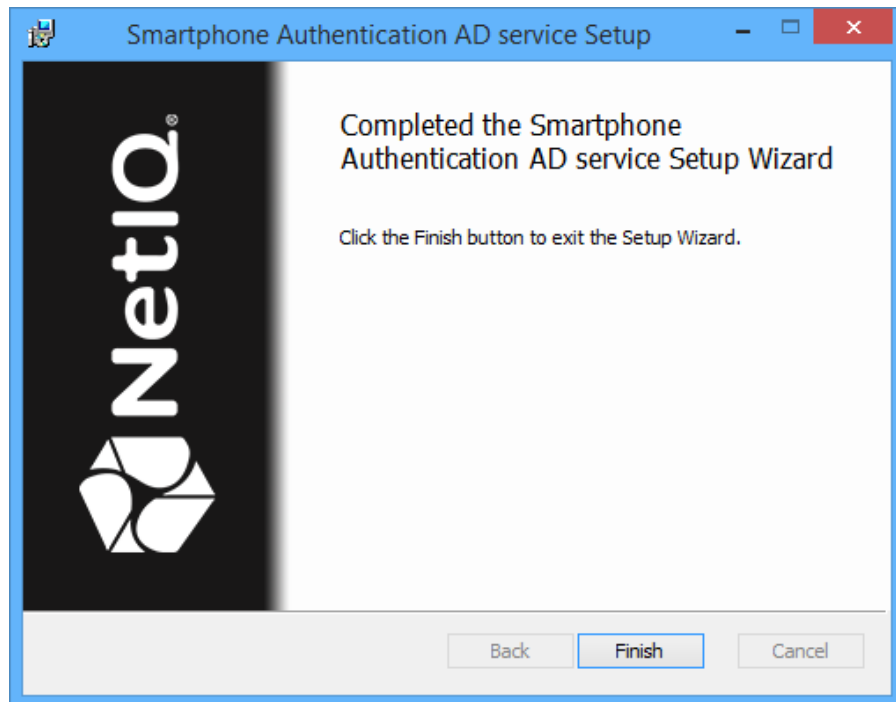
3. Click **Next** to install to the default folder or click **Change** to choose another.



4. Click **Install** to begin the installation. Click **Back** to review or change any of your installation settings. Click **Cancel** to exit the wizard.



5. Please wait while the Setup Wizard installs Smartphone Authentication AD service.
6. Click **Finish** to exit the Setup Wizard.



Extending Schema for Smartphone Authentication AD Service

After the installation of Smartphone Authentication AD service, it is required to extend schema. Schema should be extended on the 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.

To extend schema for Smartphone Authentication AD service, follow the steps:

1. Go to the **ASA** distributives folder.
2. Open the **Schema** folder.
3. If the configured server role is AD DS, open the **AD** folder. If the configured server role is AD LDS, open the **ADAM** folder.
4. Run the **bioOobData.cmd** file.
5. Follow the schema extension.

Removing Smartphone Authentication AD Service

In this chapter:

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

Microsoft Windows Server 2008 R2

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

Microsoft Windows Server 2012/Microsoft Windows 2012 R2

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

Index

A

Authentication 1, 3-5, 9-10
Authenticator 3, 5

C

Client 3
Control 10
Control panel 10

L

License 6
Local 9
Logon 3

M

Microsoft Windows Server 2008 4, 10
Microsoft Windows Server 2012 10

S

Server 4
System 4