



# NetIQ Advanced Authentication Framework

## **Smartphone Authentication Provider Installation Guide**

Version 5.1.0

# Table of Contents

	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
About This Document .....	3
<b>System Requirements</b> .....	<b>4</b>
<b>NetIQ Smartphone Architecture</b> .....	<b>6</b>
<b>Installing and Removing Smartphone Authentication Provider</b> .....	<b>9</b>
Installing Smartphone Authentication Provider .....	9
Removing Smartphone Authentication Provider .....	10
Microsoft Windows 7/Microsoft Windows Server 2008 R2 .....	10
Microsoft Windows 8.1/10/ Windows Server 2012/2012 R2 .....	10
Configuring Smartphone Authentication Provider via Group Policy .....	11
Smartphone Authentication Provider Policy .....	11
<b>Installing and Removing Smartphone Authentication Provider via Group Policy</b> .....	<b>13</b>
Installing Smartphone Authentication Provider via Group Policy .....	14
Removing Smartphone Authentication Provider Components via Group Policy .....	17
Upgrading Smartphone Authentication Provider Components via Group Policy .....	18
<b>Collecting Information From Mobile Devices</b> .....	<b>20</b>
Android .....	20
iOS .....	21
Windows Phone .....	22
<b>Troubleshooting</b> .....	<b>23</b>
Cannot Install Smartphone Authentication Provider .....	23
Error "Can't enroll device: the remote server returned an error: NotFound" on Smartphone .....	24
<b>Index</b> .....	<b>25</b>

# Introduction

## About This Document


### Purpose of the Document


This Smartphone Authentication Provider Installation Guide is intended for system administrators. In particular, it gives instructions as for how to install Smartphone type of authentication.

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

## Smartphone Authentication Provider

The following system requirements should be fulfilled:

- Microsoft Windows 7 Service Pack 1 (x64/x86)/ Microsoft Windows 8.1 (x64/x86)/ Microsoft Windows 10 (x64/x86)
- Microsoft Windows 2008 Server R2 SP1/Microsoft Windows Server 2012
- Smartphone authentication provider should be installed on the computer with already installed NetIQ Advanced Authentication Framework
- NetIQ Password Filter should be obligatory installed on all Domain Controllers in the domain



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

## NetIQ Smartphone Authenticator

- **Apple iOS:** iOS 6.1 and later
- **Google Android:** Android 4.x and 5.x and 3 megapixel camera with the function of focusing
- **Microsoft Windows Phone:** Windows Phone 8.x

The following push services should be available from devices:

- **Apple iOS:**  
Apple Push Notification Service (APNS)  
URI: <https://gateway.push.apple.com:2195>
- **Google Android:**  
Google Cloud Messaging Service (GCM)  
URI: <https://android.googleapis.com/gcm/send>
- **Microsoft Windows Phone:**  
Microsoft Push Notification Service for Windows Phone (MPNS)  
Variable URI, [https://hk2.notify.windows.com/?token=\\*](https://hk2.notify.windows.com/?token=*)



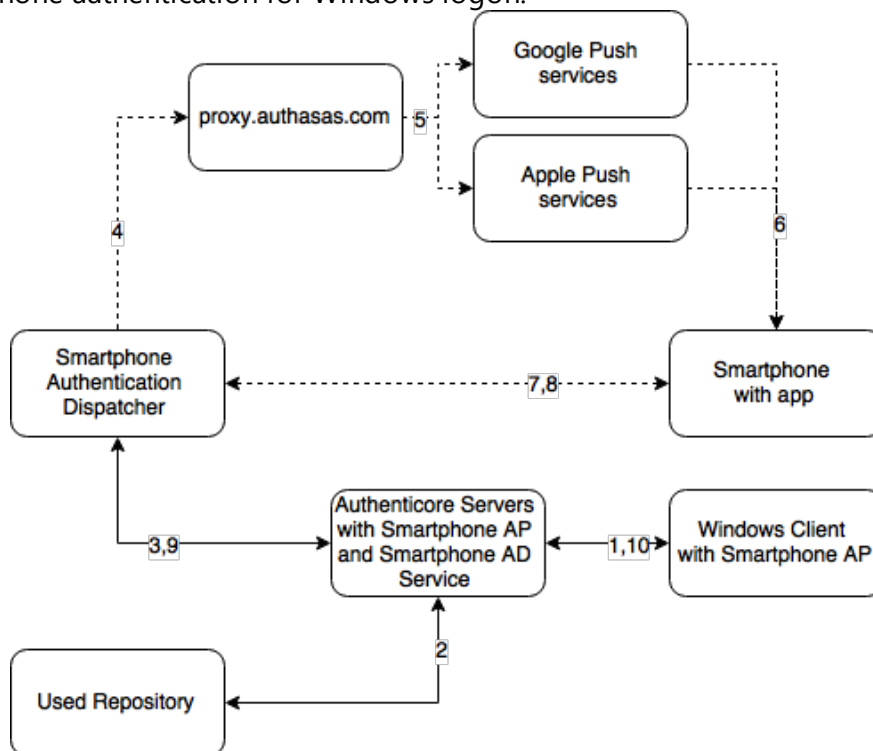
Google Cloud Messaging Service (GCM) is not supported by Google Android devices in some countries and by some specific models or these devices use another push service

provider by default. Such devices are not supported by NetIQ Advanced Authentication Framework.

## NetIQ Smartphone Architecture

This chapter contains information on an architecture with NetIQ Advanced Authentication Framework using Smartphone authentication method which provides strong authentication for desktops connected to the Active Directory domain. Smartphone authentication method can be presented in 2 ways:

- Smartphone authentication for Windows logon:

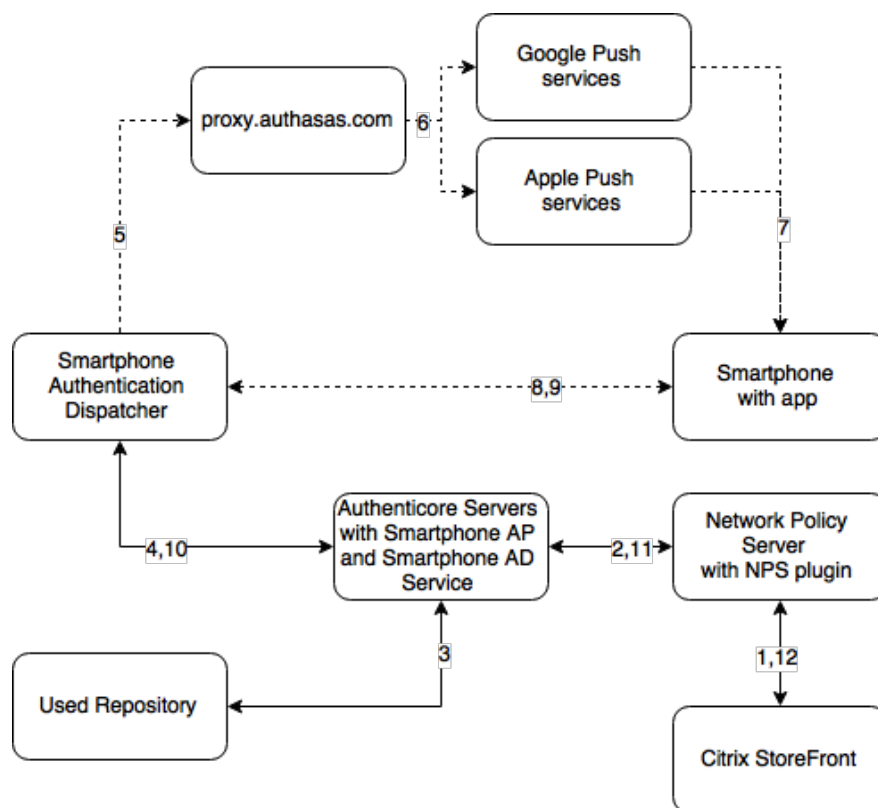


A user authenticates on his workstation (Windows Client) by selecting a Smartphone method and entering his username and password.

1. Windows Client validates the entered username and password on the Authenticore Server (dynamic RPC by default).
2. Smartphone Authentication Provider on the Authenticore Server reads the user's smartphone ID from the bioOobData attribute of the used storage (dynamic RPC).
3. Smartphone Authentication Provider sends the information to the Smartphone Authentication Dispatcher (HTTP or HTTPS, DispBspInterface registry parameter). Smartphone AD Service is always connected to the Smartphone Authentication Dispatcher using RPC (port number is specified in the DispDataPort registry parameter, by default 6000).


4. Smartphone Authentication Dispatcher sends a push message to proxy.authasas.com (HTTPS).
5. It defines to which push service it needs to forward the push message and forwards it (HTTPS).
6. The push message is being delivered to the user's smartphone.
7. Or the user can open the smartphone app manually and it checks for authentications directly on the Smartphone Authentication Dispatcher (HTTP or HTTPS, DispExternalMobileInterface registry parameter).
8. The user taps Accept/Reject and the Smartphone Dispatcher gets the answer (HTTP or HTTPS, DispMobileInterface registry parameter).
9. It redirects the answer to the Authenticore Server which validates the authentication (dynamic RPC).
10. The authentication is done/forbidden.

- Smartphone authentication via NPS plugin (example with Citrix StoreFront):



A user authenticates on the Citrix StoreFront sign-in page by entering his username and password.

1. Citrix StoreFront sends the entered username and password to the Network Policy Server.
2. NPS plugin on the Network Policy Server validates the entered username and password on the Authenticore Server (dynamic RPC by default).
3. Smartphone Authentication Provider on the Authenticore Server reads the user's smartphone ID from the bioOobData attribute of the used storage (dynamic RPC).
4. Smartphone Authentication Provider sends the information to the Smartphone Authentication Dispatcher (HTTP or HTTPS, DispBsplInterface registry parameter). Smartphone AD Service is always connected to the Smartphone Authentication Dispatcher using RPC (port number is specified in the DispDataPort registry parameter, by default 6000).
5. Smartphone Authentication Dispatcher sends a push message to proxy.authasas.com (HTTPS).
6. It defines to which push service it needs to forward the push message and forwards it (HTTPS).
7. The push message is being delivered to the user's smartphone.
8. Or the user can open the smartphone app manually and it checks for authentications directly on the Smartphone Authentication Dispatcher (HTTP or HTTPS, DispExternalMobileInterface registry parameter).
9. The user taps Accept/Reject and the Smartphone Dispatcher gets the answer (HTTP or HTTPS, DispMobileInterface registry parameter).
10. It redirects the answer to the Authenticore Server which validates the authentication (dynamic RPC).
11. Authenticore Server sends success/failure signal to the Network Policy Server.
12. Network Policy Server forwards it to the Citrix StoreFront.

 The stated above ways refer only to the situation with single dispatcher, during which ARR with load balancing is not used. In case of load balancing, interaction between Smartphone, Smartphone Authentication Dispatcher and Smartphone Authentication Provider is controlled by load balancer. For more information, see the [Multiple Dispatchers Support in v4.11](#) chapter.



# Installing and Removing Smartphone Authentication Provider

NetIQ Advanced Authentication Framework™ package includes Smartphone authentication provider, which allows you to control authentication with the help of NetIQ Smartphone Authenticator.

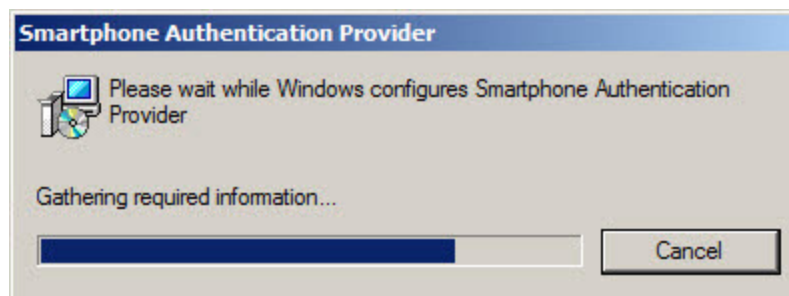
## Installing Smartphone Authentication Provider

Smartphone authentication provider connects to Smartphone authentication Dispatcher which can be installed on different machine. If both Smartphone authentication provider and Smartphone Authentication Dispatcher are installed on the same machine, it is possible to use rpc: [127.0.0.1:10114](http://127.0.0.1:10114).

✘ 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.

✘ Smartphone authentication provider can be installed both on the server and on the client part of NetIQ.

1. Run **SaProvider.msi**. Smartphone authentication provider will be automatically installed on your computer.



2. You should restart your system for the configuration changes made to Smartphone authentication provider to take effect. Click **Yes** to restart the system immediately or **No** if you plan to restart it later manually.

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

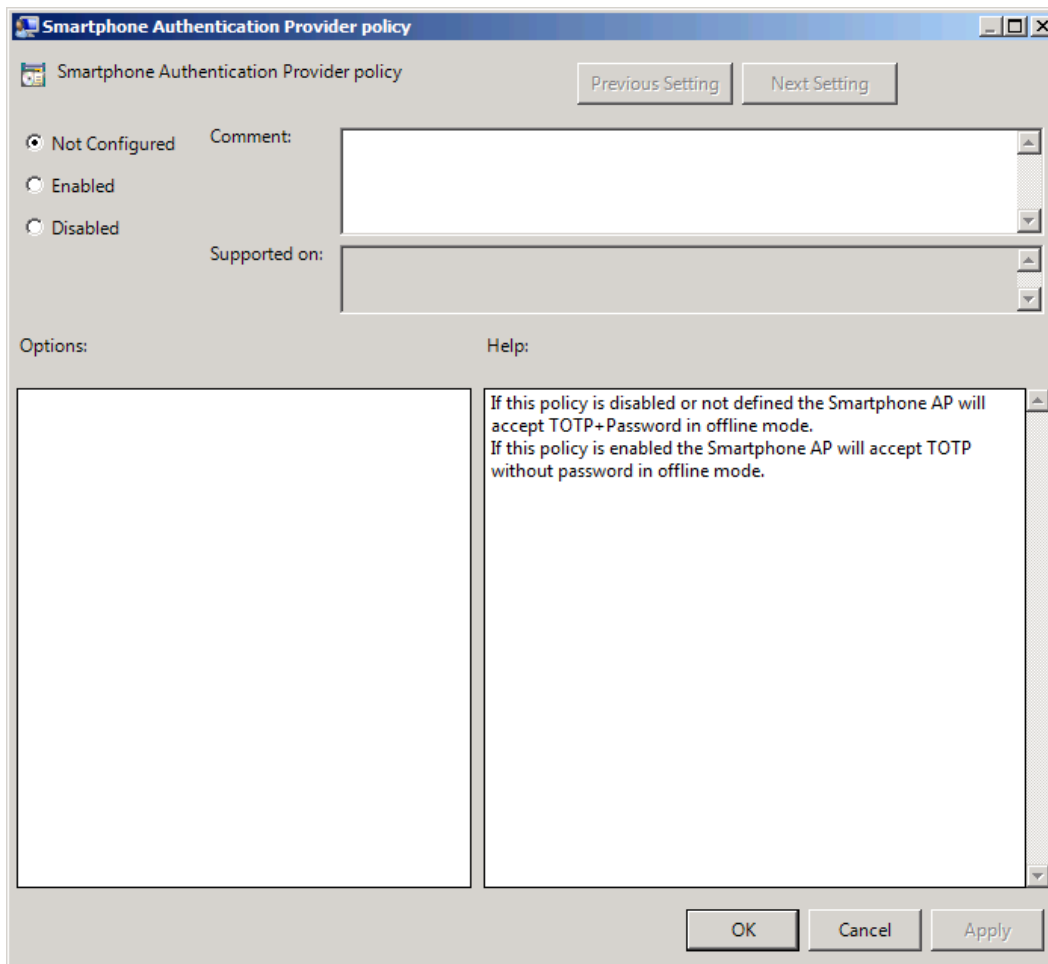
## Configuring Smartphone Authentication Provider via Group Policy

After the installation of Smartphone authentication provider, the [Smartphone Authentication Provider](#) policy is added to **Group Policy Management Editor**.

### Smartphone Authentication Provider Policy

The **Smartphone Authentication Provider** policy allows modifying Smartphone authentication provider properties in offline mode:

- If this policy is disabled or not defined, the Smartphone authentication provider will accept TOTP+Password.
- If this policy is enabled, the Smartphone authentication provider will accept TOTP without password.



The screenshot shows the "Smartphone Authentication Provider policy" configuration window. It features a title bar with standard window controls and a "Smartphone Authentication Provider policy" icon. Below the title bar are "Previous Setting" and "Next Setting" buttons. The main area contains three radio buttons: "Not Configured" (selected), "Enabled", 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 "Options:" and "Help:" sections. The "Help:" section contains the following text: "If this policy is disabled or not defined the Smartphone AP will accept TOTP+Password in offline mode. If this policy is enabled the Smartphone AP will accept TOTP without password in offline mode." At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

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

Registry settings:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\BioAPI\BSP\SaProvider


**SkipPasswordCheck:**

- type: REG\_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

# Installing and Removing Smartphone 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.

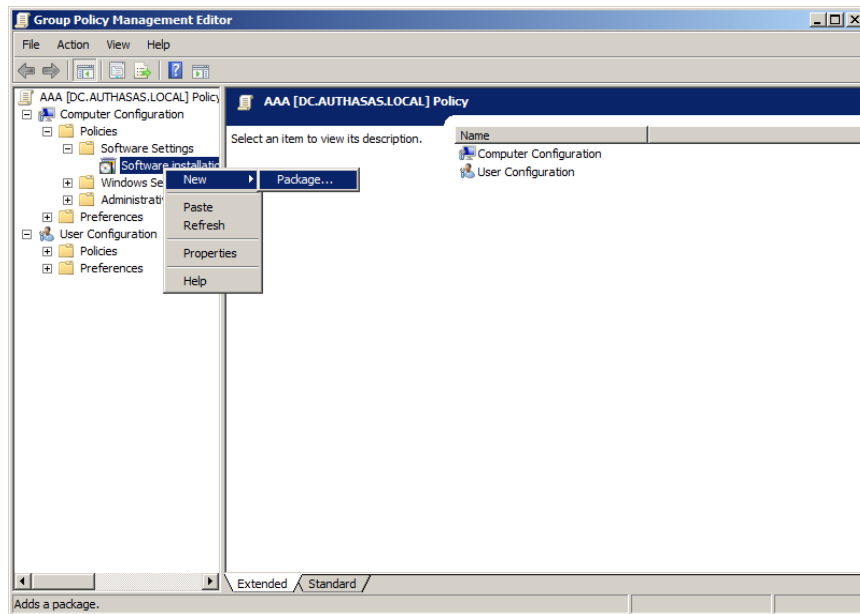
To create new **Group Policy** and configure it:

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 Smartphone Authentication Provider via Group Policy

To install Smartphone authentication provider using the group policy:

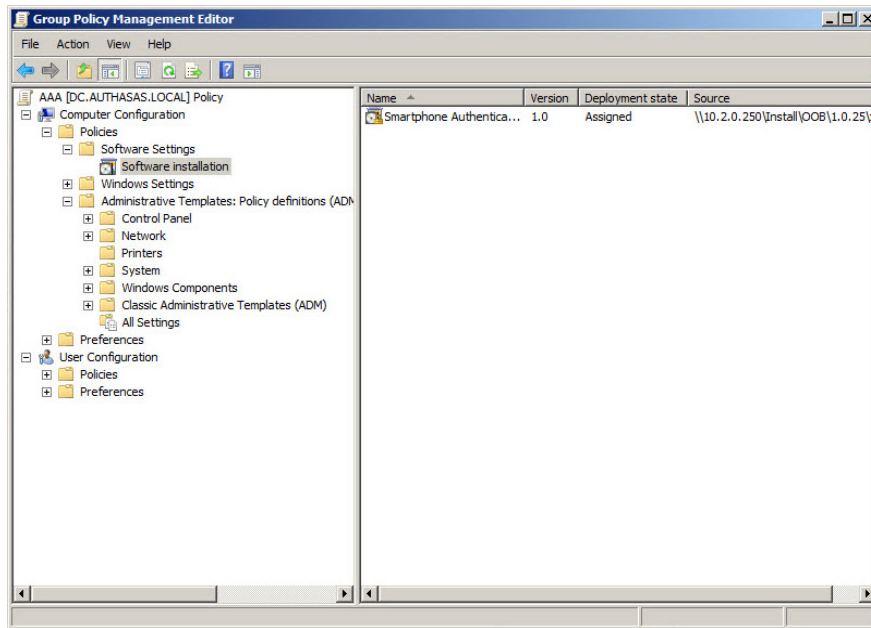
1. In GPME, in the selected GPO under **Computer configuration > Policies > Software Settings**, right-click **Software Installation** and select **New > Package**.



2. Specify the network path to the installer package.

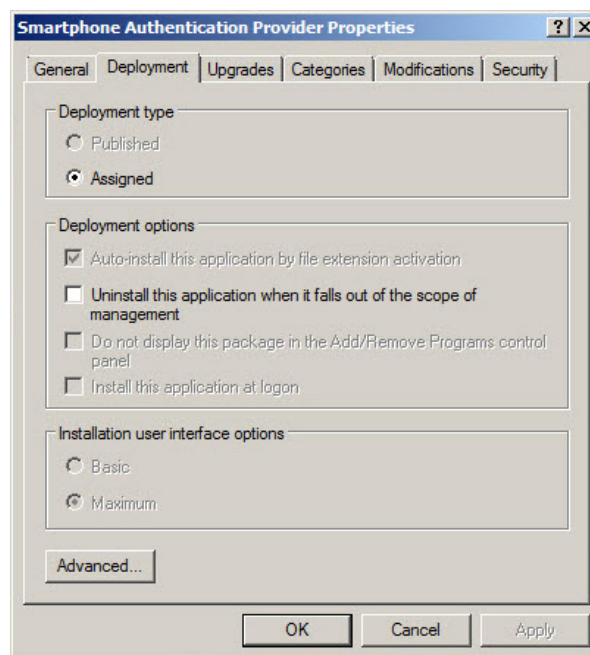
 The directory you are willing to install should be located on network drive.

3. In the **Deploy Software** dialog, select **Assigned** and click **OK**.
4. The installer package name, version, state and path are displayed in **Group Policy Management Editor**.

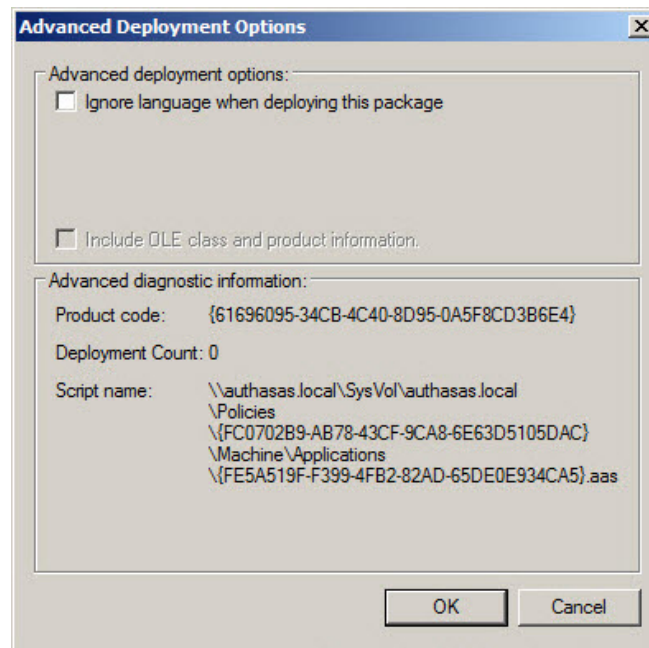


5. Open package properties:

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.

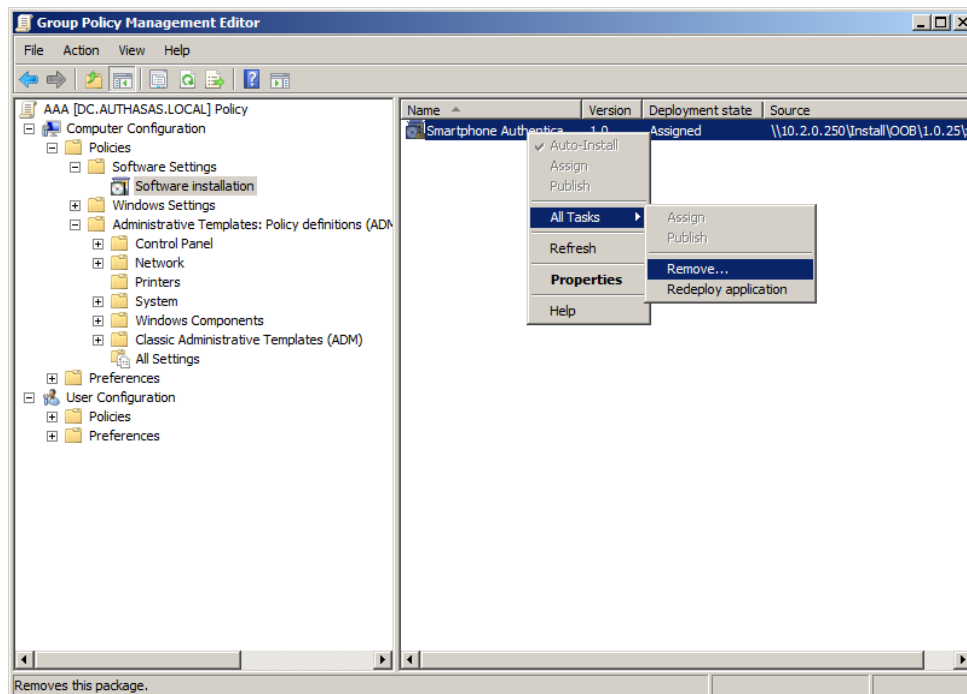


## Removing Smartphone Authentication Provider Components via Group Policy

To remove Smartphone 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.



3. In the **Remove Software** dialog, select **Immediately uninstall the software from users and computers** 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.

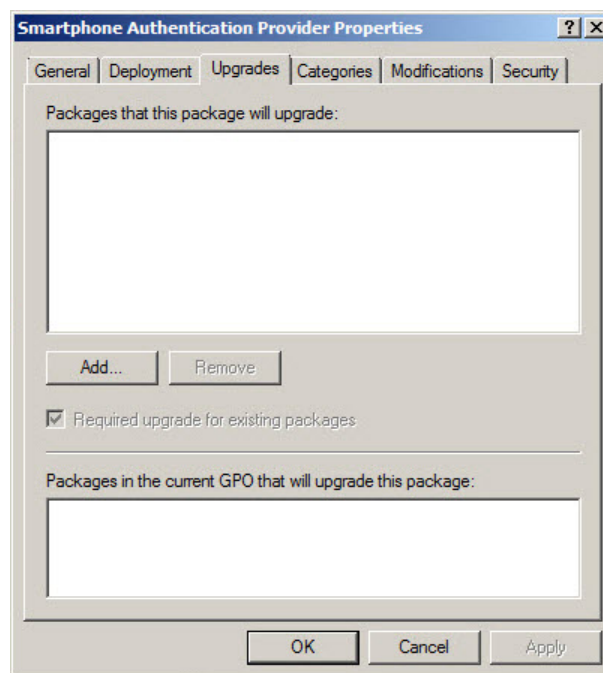
\* If you have cleared the **Uninstall this application when it falls out of the scope of management** check box as it was recommended, software will not be uninstalled after selecting **Immediately uninstall the software from users and computers**. In this case, you will need to uninstall it via **Programs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

## Upgrading Smartphone Authentication Provider Components via Group Policy

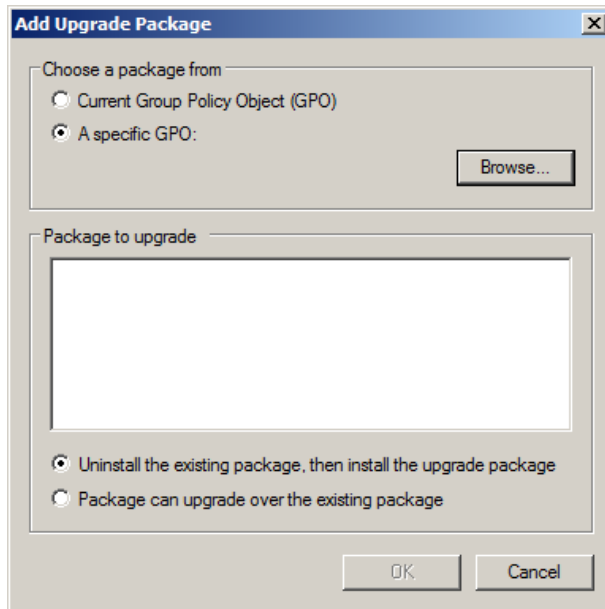
**Option 1:** You can add .msi package with new component version to an existing group policy object. However, this option does not prove to be good, because in case of any problems in new version of component, these problems spread on all computers in installation group.

**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 the **Upgrades** tab of package properties.




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



5. Select a GPO which was used for installation of previous NetIQ Advanced Authentication Framework version.

6. Select .msi package name;

7. Select **Uninstall the existing package, then install the upgrade package.**

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

## Collecting Information From Mobile Devices

While logging in using NetIQ Smartphone Authenticator, geo location data are being stored in NetIQ Advanced Authentication Framework backend with authentication data in Event log. The nature and data set may differ depending on the version of the mobile operating system.

To view information from mobile devices in Event Viewer:

1. Click the **Start** button.
2. Open **Control Panel** and select the **System and Security** section.
3. Open the **Administrative Tools** window and double-click **Event Viewer**.
4. Expand the **Applications and Services Logs** item.
5. Click **NetIQ Advanced Authentication Framework** and open the **Details** tab.

Information can be collected from mobile devices with the following mobile operating systems:

- [Android](#)
- [iOS](#)
- [Windows Phone](#)



GPS and GSM data can be stored only if these modules are supported by the mobile device. Sometimes geo location data may miss or may be incorrect.

## Android

The following data can be stored from Android mobile devices:

- OS version
- Board
- Bootloader
- Brand
- CPU abi
- CPU abi2
- Device
- Display
- Fingerprint
- Hardware
- Host

- ID
- Manufacturer
- Model
- Product
- Serial
- Tags
- Type
- User
- Device ID
- Device software version
- Line number
- Network county ISO
- Network operator
- Network operator name
- Phone type
- Sim country ISO
- Sim operator
- Sim operator name
- Sim serial number
- Sim state
- Subscriber ID
- Voice mail alpha tag
- Voice mail number
- Location service type
- Location latitude
- Location longitude
- Time zone display name
- Time zone id

## iOS

The following data can be stored from iOS mobile devices:

- Battery level
- Battery monitoring enable
- Battery state
- ID for vendor
- Localized model
- Multitasking supported
- Device name
- Device model

- System name
- System version
- Local time zone
- Timezone name
- Carrier name
- ISO country code
- Mobile country code
- Mobile network code
- Location longitude
- Location latitude

## Windows Phone

The following data can be stored from Windows Phone mobile devices:

- Location status
- Location latitude
- Location longitude
- Application current memory usage
- Application memory usage limit
- Application peak memory usage
- Device firmware version
- Device hardware version
- Device manufacturer
- Device name
- Device total memory
- Is keyboard deployed
- Is keyboard present
- Application working set limit
- Device unique id
- Is application preinstalled
- Physical screen resolution height
- Physical screen resolution width
- Original mobile operator name
- Raw DPI X
- Raw DPI Y
- Timezone name

# Troubleshooting

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

In this chapter:

- [Cannot Install Smartphone Authentication Provider](#)
- [Error “Can't enroll device: the remote server returned an error: NotFound” on Smartphone](#)

## Cannot Install Smartphone Authentication Provider

### Description:

Error appears when installing Smartphone authentication provider on your computer.

### Cause:

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

## Error "Can't enroll device: the remote server returned an error: NotFound" on Smartphone

### **Description:**

While scanning the QR code, the following error is displayed: "Can't enroll device: the remote server returned an error: NotFound ". Unlike <localhost>:8757, <localIpAddress>:8757 and <publicIpAddress>:8757 cannot be accessed in browser, even though access is being checked on the same server.

### **Cause:**

Probably you have configured the Direct Access on the server.

### **Solution:**

Please, remove the feature and try again.



# Index

---

## A

Active Directory 6  
Application 22  
Authentication 1, 3-4, 6, 9-11, 13-14, 17-18, 20, 23  
Authenticator 3-4, 9, 20

## C

Client 3, 6  
Control 20  
Control panel 10  
Create 13, 18

## D

Default 13  
Device 20-22  
Domain 13

## E

Error 23-24  
Event Viewer 20

## F

Fingerprint 20

## G

GPMC 13  
GPME 13-14, 17

## H

Hardware 20

## L

Logon 3

## M

Microsoft Windows Server 2012 10

---

Network 8, 21  
Notification 4

**N**

Package 14, 18  
Password 4  
Policy 8, 11-14

**P**

Remove 17

**R**

Security 13  
Server 4, 6  
Software 14, 17  
Support 8  
System 4, 20, 22

**S**

TOTP 11

**T**

User 21

**U**

Windows 4, 6, 20, 22  
Windows 7 4, 10  
Windows 8 10

**W**