# NetIQ Advanced Authentication Framework

## SMS Authentication Provider Installation Guide

Version 5.1.0

# Table of Contents

# Introduction

## About This Document

### Purpose of the Document

This SMS 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 SMS 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.

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

The following system requirements should be fulfilled:

- Microsoft Windows 7/ Microsoft Windows 8/ Microsoft Windows 8.1;
- Microsoft Windows 2003 Server (x64/x86) SP2/ Microsoft Windows 2003 Server R2 (x64/x86) SP2/ Microsoft Windows 2008 Server R2 SP1/ Microsoft Windows Server 2012;
- SMS authentication provider should be installed on the computer with already installed NetIQ Advanced Authentication Framework.

✱ SMS authentication provider should be installed on **every** Authenticore Server.

✱ SMS authentication provider's version 1.0.11 and earlier is not compatible with SMS authentication provider's version 1.0.12 and newer.

# Configuration

These settings should be applied on every Authenticore Server.

Any internet gateway supporting POST messages is supported.

SMS related registry keys retain after upgrades.

To configure SMS authentication method, follow these steps:

1. Open the following registry key: HKEY_LOCAL_ MACHINE\Software\Wow6432Node\BSP\{6D890379-EC8E-483F-A927-F3489303B37A}\SMS Service

Specify the following parameters in the registry to get SMS authentication provider working.

- Proxy settings (optional):

  **ProxyServer**: type: REG_SZ; value: <proxy server>
  **ProxyPassword**: type: REG_SZ; value: <additional password>
  **ProxyUserName**: type: REG_SZ; value: <additional username>

- GSM modem settings (available from version 1.0.11) (optional):

  **UseModem**: type: REG_SZ; value: Yes
  **ModemComPort**: type: REG_SZ; value: <com port>
  **ModemSmsText**: type: REG_SZ; value: <message text>
  **ModemSmsPin**: type: REG_SZ; value: <PIN of the modem>

- Settings in accordance with the selected service:

  **UserName** - user name.
  **Password**- user password.
  **RequestUri** - web address (http and https are supported).
  **RequestBody** - request which is sent to the phone.
  **DeliveryStatus** - detects whether SMS message is delivered or not. The value varies in accordance with the selected service:
  - to use SMS authentication method using Twilio, specify the following value: **DeliveryStatus**: type: REG_SZ; value (for JSON): "status": "queued"; value (for XML): <Status>queued</Status>
  - to use SMS authentication method using MessageBird, specify the following value:
    **DeliveryStatus**: type: REG_SZ; value: 01

**TelephoneNumberAttribute** - takes any attribute name from Active Directory. The value may vary according to the required telephone number field:

- to use the telephone number field from the **Telephones** tab of the **User Properties** in Active Directory Users and Computers, specify the following value:
  **TelephoneNumberAttribute**: type: REG_SZ; value: mobile
- to use the telephone number field from the **General** tab of the **User Properties** in Active Directory Users and Computers, specify the following value:
  **TelephoneNumberAttribute**: type: REG_SZ; value: telephoneNumber

To enable GET method, provide an empty RequestBody value and specify both values in RequestUri.

To enable POST method, provide a nonempty RequestBody value and specify only the service uri in RequestUri.

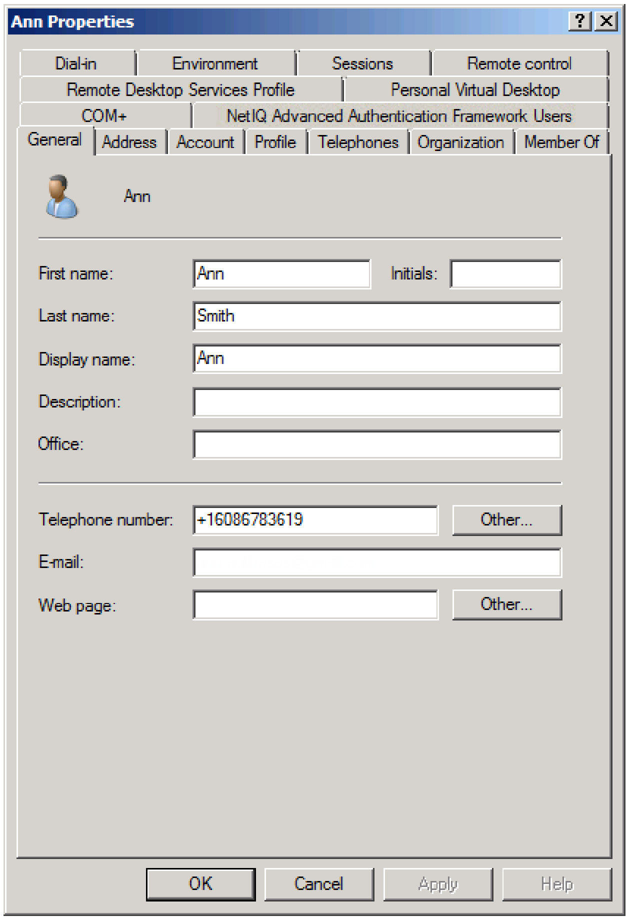
Parameters that are specified in <> should be filled in, parameters that are specified in [] should remain unchanged.

2. Open the following registry key HKEY_LOCAL_MACHINE\Software\Wow6432Node\BSP\{6D890379-EC8E-483F-A927-F3489303B37A}\TOTP Generation

Specify the following TOTP Generation settings (required):

**TOTPLength**: type: REG_DWORD; value: 0x00000006 (6)
**TOTPStep**: type: REG_DWORD; value: 0x0000003c (60)
**TOTPWindow**: type: REG_DWORD; value: 0x00000004 (4)

3. Specify the user's telephone number that will be used for authentication in the **General** tab of the **User Properties** in Active Directory Users and Computers.



First name: Ann

Initials:

Last name: Smith

Display name: Ann

Description:

Office:

Telephone number: +16086783619

E-mail:

Web page:

Verify the correctness of the specified telephone number in user's profile.

## Examples

SMS authentication method can be configured using Twilio or MessageBird services.

1. To configure SMS authentication method using Twilio, create account on Twilio website and get Account SID, AuthToken and From (Twilio phone number). Specify them in the registry to get SMS authentication provider working.

**Password**: type: REG_SZ; value: <AuthToken>
**RequestBody**: type: REG_SZ; value: From=<Twilio phone number>&To= [PHONENUMBER] &Body=<message text>: [TOTP]
**RequestUri**: type: REG_SZ; value: https://api.twilio.com/2010-04-01/Accounts/<Account SID>/Messages.json
**UserName**: type: REG_SZ; value: <Account SID>
**DeliveryStatus**: type: REG_SZ; value (for JSON): "status": "queued"; value (for XML): <Status>queued</Status>
**TelephoneNumberAttribute**:

- in case of usage of the telephone number field from the Telephones tab of the User Properties in Active Directory Users and Computers:
  **TelephoneNumberAttribute**: type: REG_SZ; value: mobile
- in case of usage of the telephone number field from the General tab of the User Properties in Active Directory Users and Computers:
  **TelephoneNumberAttribute**: type: REG_SZ; value: telephoneNumber

To enable GET method:
**RequestUri**: type: REG_ SZ; value: https://api.twilio.com/2010- 04- 01/Accounts/<Account SID>/Messages.json?From=<Twilio phone number>&To=[PHONENUMBER]&Body=<message text>: [TOTP]

2. To configure SMS authentication method using MessageBird, create account on MessageBird. Specify the following parameters in the registry to get SMS authentication provider working.

**RequestUri**: type: REG_SZ; value: http://api.messagebird.com/api/sms
**RequestBody**: type: REG_ SZ; value: username=<username>&password= <password>&body=<message text>: [TOTP] &sender=<account name>&destination= [PHONENUMBER]&test=0
**DeliveryStatus**: type: REG_SZ; value: 01
**TelephoneNumberAttribute**:

- in case of usage of the telephone number field from the **Telephones** tab of the User Properties in Active Directory Users and Computers:
  **TelephoneNumberAttribute**: type: REG_SZ; value: mobile

- in case of usage of the telephone number field from the **General** tab of the User Properties in Active Directory Users and Computers:
  **TelephoneNumberAttribute**: type: REG_SZ; value: telephoneNumber

To enable sending of flash SMS messages:
**RequestBody** : type: REG_ SZ; value: username=<username>&password= <password>&body=<message text>: [TOTP] &sender=<account name>&destination= [PHONENUMBER]&test=0&type=flash

To enable GET method:
**RequestUri**: type: REG_SZ; value: http://api.messagebird.com/api/sms?username=<username> &password=<password>& body=<message text>: [TOTP]&sender=<account name>&destination=[PHONENUMBER]&test=0

3. If the required SMS gateway is internal, it should have Internet access. If the required SMS gateway is public, Authenticore Server that interacts with it should have Internet access. There should be provided access to api.twilio.com or api.messagebird.com over the HTTPS protocol (in accordance with the used service). To check it, open the required web page using a browser of Authenticore Server.

The following ports will be used by default:

- for http - port 80;
- for https - port 443.

# Installing and Removing SMS Authentication Provider

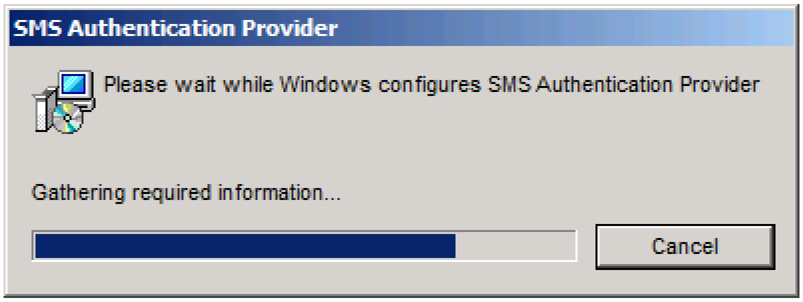
NetIQ Advanced Authentication Framework™ package includes SMS authentication provider, which allows you to control authentication with the help of personal or corporate phone.

## Installing SMS Authentication Provider

The start of installation can 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 SMS authentication provider:

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



SMS Authentication Provider

Please wait while Windows configures SMS Authentication Provider

Gathering required information...

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

# Removing SMS Authentication Provider

In this chapter:

## Microsoft Windows 7/Microsoft Windows Server 2008

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

## Microsoft Windows Server 2003

1. In the **Start** menu, select **Settings** > **Control Panel** > **Add or Remove Programs**.
2. Select **SMS Authentication Provider** and click **Remove**.
3. Confirm the removal.

## Microsoft Windows 8/Microsoft Windows Server 2012

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

# Installing and Removing SMS 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.

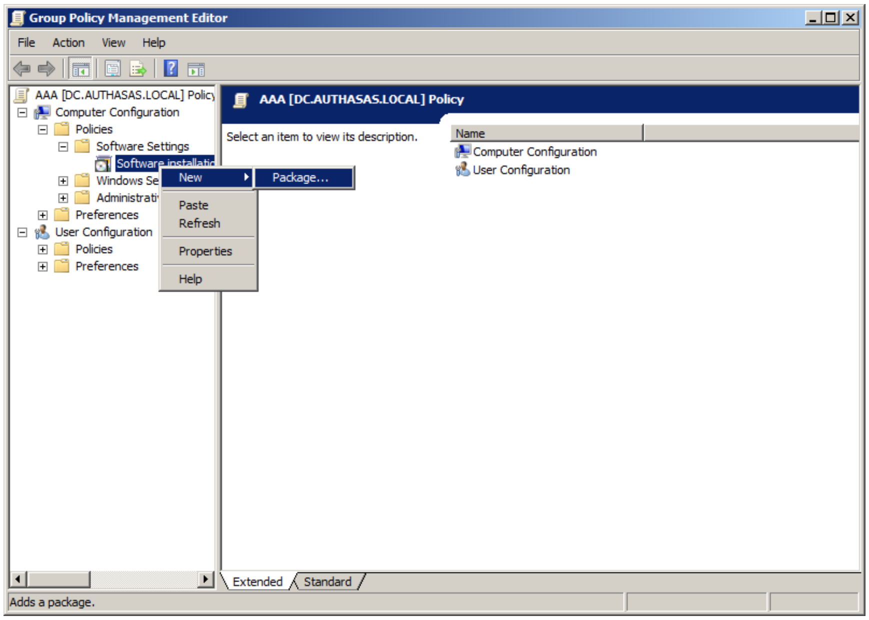
2. Connect them:

   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 SMS Authentication Provider via Group Policy

To install SMS 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**.



Select an item to view its description.

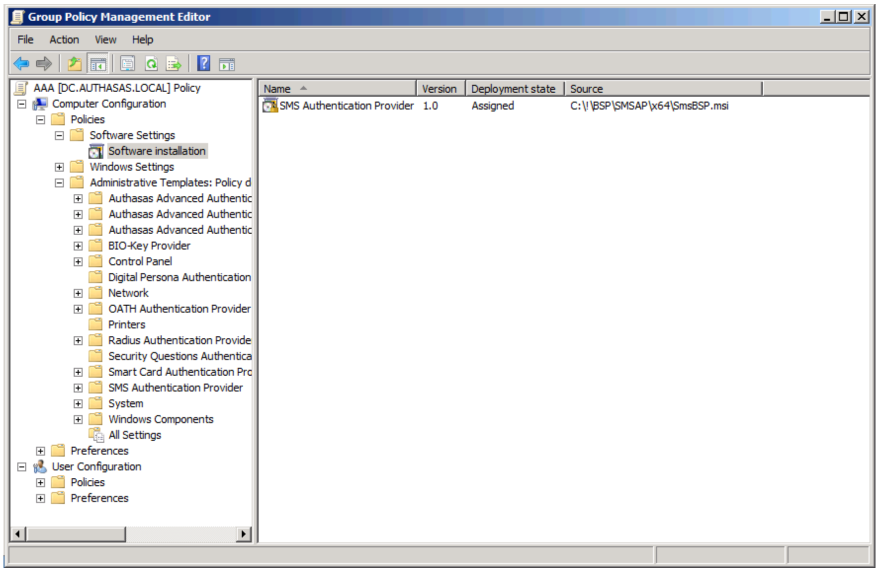
Adds a package.

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**.

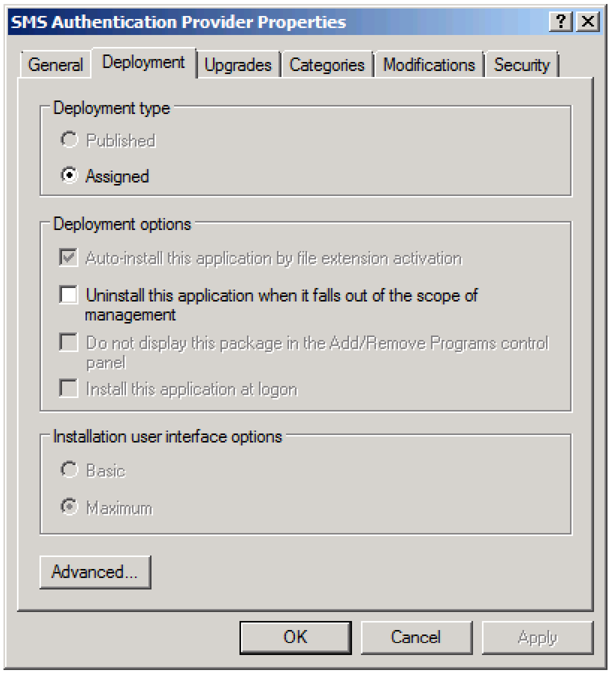


AAA [DC.AUTHASAS.LOCAL] Policy
- Computer Configuration
  - Policies
    - Software Settings
      - Software installation
    - Windows Settings
    - Administrative Templates: Policy d
      - Authasas Advanced Authentic
      - Authasas Advanced Authentic
      - Authasas Advanced Authentic
      - BIO-Key Provider
      - Control Panel
      - Digital Persona Authentication
      - Network
      - OATH Authentication Provider
      - Printers
      - Radius Authentication Provide
      - Security Questions Authentica
      - Smart Card Authentication Prc
      - SMS Authentication Provider
      - System
      - Windows Components
      - All Settings
  - Preferences
- User Configuration
  - Policies
  - Preferences

| Name | Version | Deployment state | Source |
|---|---|---|---|
| SMS Authentication Provider | 1.0 | Assigned | C:\I\BSP\SMSAP\x64\SmsBSP.msi |

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.



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

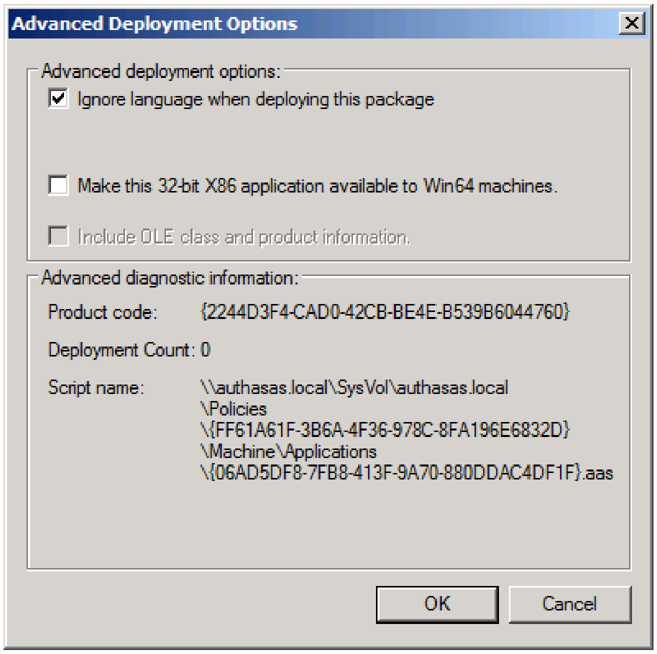
□ Install this application at logon

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

□ Make this 32-bit X86 application available to Win64 machines.

□ Include OLE class and product information.

Advanced diagnostic infomation:

Product code: {2244D3F4-CAD0-42CB-BE4E-B539B6044760}

Deployment Count: 0

Script name: \\authasas.local\SysVol\authasas.local\Policies\{FF61A61F-3B6A-4F36-978C-8FA196E6832D}\Machine\Applications\{06AD5DF8-7FB8-413F-9A70-880DDAC4DF1F}.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).

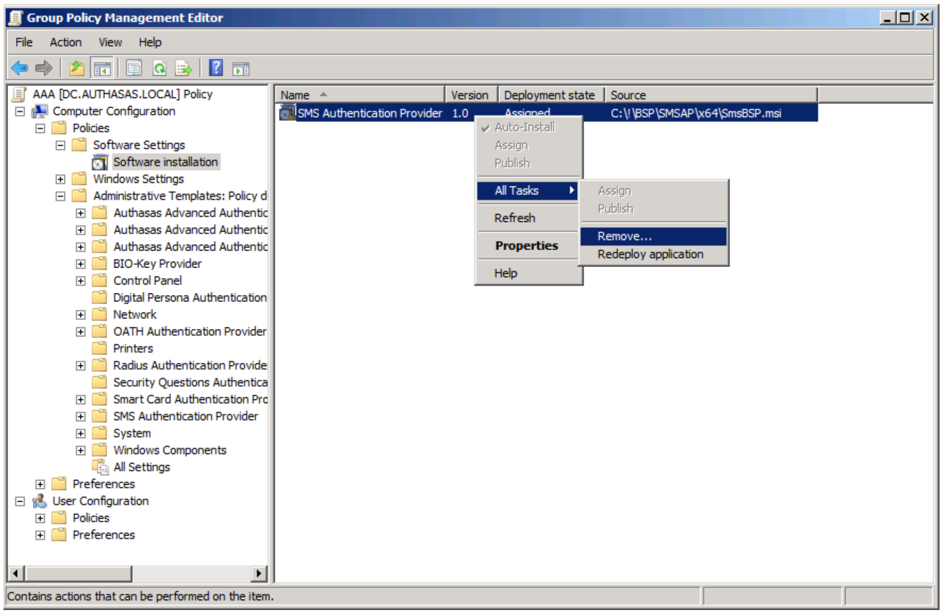
The assigned package is installed after you have updated the domain policy and restarted your computer. To update the domain policy immediately, use the `gpupdate /force` command.

## Removing SMS Authentication Provider Components via Group Policy

To remove SMS 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.



Group Policy Management Editor
File
Action
View
Help
AAA [DC.AUTHASAS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Software installation
Windows Settings
Administrative Templates: Policy d
Authasas Advanced Authentic
Authasas Advanced Authentic
Authasas Advanced Authentic
BIO-Key Provider
Control Panel
Digital Persona Authentication
Network
OATH Authentication Provider
Printers
Radius Authentication Provide
Security Questions Authentica
Smart Card Authentication Prc
SMS Authentication Provider
System
Windows Components
All Settings
Preferences
User Configuration
Policies
Preferences
Auto-Install
Assign
Publish
All Tasks
Refresh
Properties
Help
Assign
Publish
Remove...
Redeploy application
Contains actions that can be performed on the item.

| Name | Version | Deployment state | Source |
|---|---|---|---|
| SMS Authentication Provider | 1.0 | Assigned | C:\\BSP\SMSAP\x64\SmsBSP.msi |

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

The authenticator 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 SMS Authentication Provider chapter.

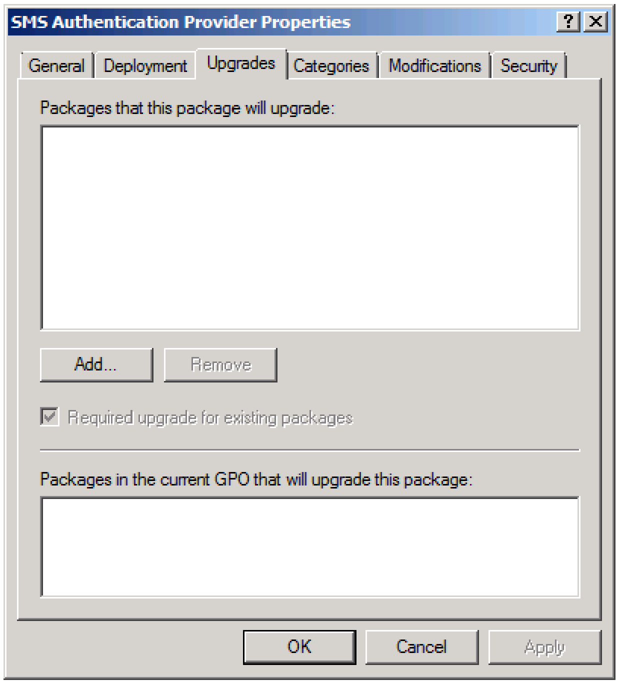
## Upgrading SMS Authentication Provider Components via Group Policy

**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.

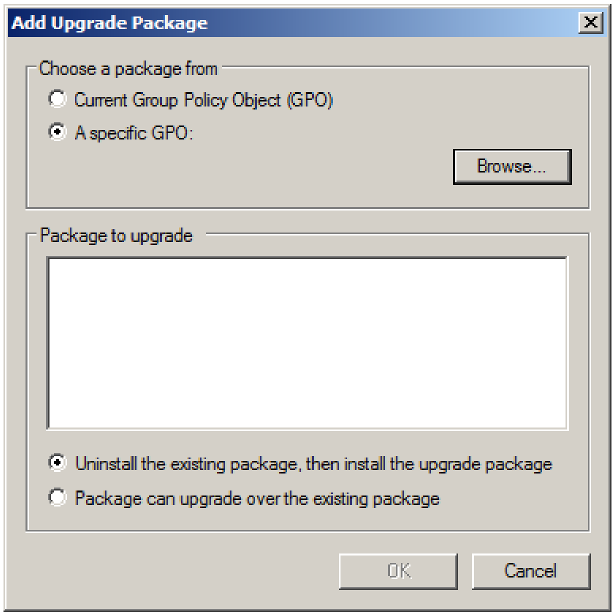
2. After having configured software installation, go to the **Upgrades** tab of package properties.


SMS Authentication Provider Properties
?
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 **A specific GPO**.



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

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 SMS Authentication Provider

**Description:**

Error appears when installing SMS authentication provider on your computer.

**Cause:**

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

# Index