



# NetIQ Advanced Authentication Framework

## **Voice Call 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 Voice Call Architecture</b> .....	<b>5</b>
<b>Configuration</b> .....	<b>6</b>
<b>Installing and Removing Voice Call Authentication Provider</b> .....	<b>9</b>
Installing Voice Call Authentication Provider .....	9
Removing Voice Call Authentication Provider .....	10
Microsoft Windows 7/Microsoft Windows Server 2008 R2 .....	10
Microsoft Windows Server 2003/2003 R2 .....	10
Microsoft Windows 8.1/Microsoft Windows Server 2012 .....	10
<b>Installing and Removing Voice Call Authentication Provider via Group Policy</b> .....	<b>11</b>
Installing Voice Call Authentication Provider via Group Policy .....	12
Removing Voice Call Authentication Provider Components via Group Policy .....	15
Upgrading Voice Call Authentication Provider Components via Group Policy .....	16
<b>Troubleshooting</b> .....	<b>18</b>
Cannot Install Voice Call Authentication Provider .....	18
<b>Index</b> .....	<b>19</b>

# Introduction

## About This Document


### Purpose of the Document


This Voice Call 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 Voice Call 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

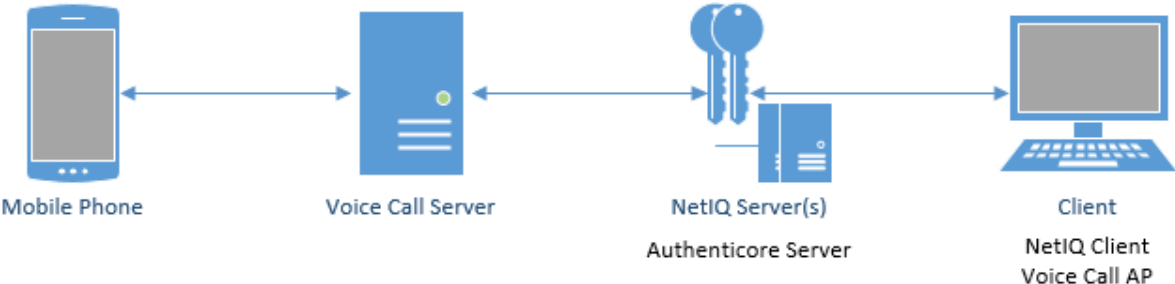
The following system requirements should be fulfilled:

- Microsoft Windows 7 (x64/x86) SP1/Microsoft Windows 8.1 (x86/x64)
- 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
- Voice Call authentication provider should be installed on the computer with already installed NetIQ Advanced Authentication Framework

 Voice Call authentication provider should be installed on **every** Authenticore Server.

# NetIQ Voice Call Architecture

In this chapter there is shown an architecture with NetIQ Advanced Authentication Framework using Voice Call authentication method which provides strong authentication for desktops connected to the Active Directory domain. Voice Call authentication method provides with a capability to control authentication using personal or corporate phone and can be presented in the following way:



# Configuration

 These settings should be applied on **every** Authenticore Server.

To configure Voice Call authentication method, follow these steps:

1. Create account on [Twilio](#) website and get **AccountSid**, **AuthToken** and **From** (Twilio's phone number). Specify them in registry to get Voice Call authentication provider working. The following parameters should be also specified obligatory:

**Host** - Voice Call AP Server host.

E.g., type: REG\_SZ; value: <Voice Call AP Server host>

**Port** - Voice Call AP Server port.

E.g., type: REG\_SZ; value: <Voice Call AP Server port>

**TextBefore** - text that is played after the call is gotten on the phone.

E.g., type: REG\_SZ; value: Please enter your PIN code followed by the hash sign.

**TextAfter** - text that is played after the PIN code is input.


E.g., type: REG\_SZ; value: Your response has been received, thank you.

**TextError** - text that is played in case the specified PIN code was not input in time.

E.g., type: REG\_SZ; value: We didn't receive any input. Goodbye!

**TextAppError** - text that is played in case an application error occurred.

E.g., type: REG\_SZ; value: Sorry, an error occurred.

 Parameters enclosed in angle brackets (<parameter>) should be replaced with applicable values (including angle brackets).

The following parameters can be specified additionally:

**ExternHost** - external Voice Call AP Server host which is used in case Voice Call Server is outside the local network.

E.g., type: REG\_SZ; value: http://<ExternalIPAddress>:<VoiceCallServerPortNumber>.

**NumDigits** - number of digits that are used for PIN code.

E.g., type: REG\_DWORD; value: 0x00000005 (5).

**Voice** - type of voice that is used for playing messages.

E.g., type: REG\_SZ; value: Alice.

**FinishOnKey** - key that is tapped after entering the specified PIN code.

E.g., type: REG\_SZ; value: #.

**Timeout** - time in seconds that is allotted for input of the specified PIN code.


E.g., type: REG\_DWORD; value: 0x0000000f (15).

**TalkWithMachine** - function that enables or disables answer with voice.

E.g., type: REG\_DWORD; value: 0x00000000 (0).


**Language** - language that is used for playing messages.

E.g., type: REG\_SZ; value: en\_GB.

 The list of languages that are supported by Voice Call authentication provider is the following: da-DK, de-DE, en-AU, en-CA, en-GB, en-IN, en-US, ca-ES, es-ES, es-MX, fi-FI, fr-CA, fr-FR, it-IT, ja-JP, ko-KR, nb-NO, nl-NL, pl-PL, pt-BR, pt-PT, ru-RU, sv-SE, zh-CN, zh-HK, zh-TW. These languages may be used **only** with the voice of "ALICE". In case of using other types of voice, the list of languages that are supported by Voice Call authentication provider will be limited.

2. Specify the registry key and set the following parameters in the **Parameters** folder of:

- for 32-bit OS: HKEY\_LOCAL\_MACHINE\SOFTWARE\BSP\ {AAD4287A- 8741- 8745- B6C5- 9FB056A56CE1}
- for 64-bit OS: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\BSP\ {AAD4287A- 8741-8745-B6C5-9FB056A56CE1}


 Until the version 1.0.25 inclusively it was required to specify the registry key and set the parameters in the **Parameters** folder. Starting from the version 1.0.26 it is strongly recommended not to forget to change the name while upgrading the version of Voice Call Authentication Provider.

3. Countries, where Voice Call authentication provider will be used, should be specified in [account settings](#).

4. 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.

The screenshot shows the 'Ann Properties' dialog box with the following fields and values:

Field	Value
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.


5. Authenticore Servers should have access to Voice Call Server. Voice Call Server should have a Public IP with Internet access.



# Installing and Removing Voice Call Authentication Provider

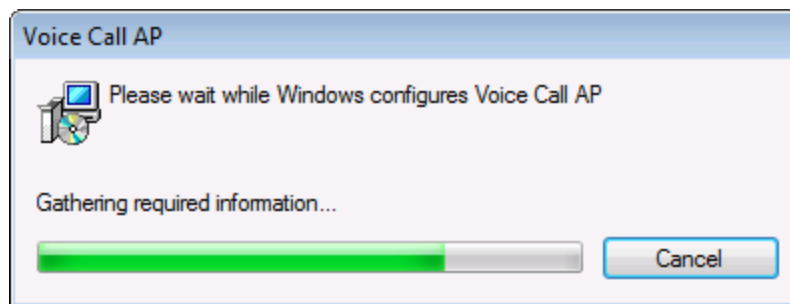
NetIQ Advanced Authentication Framework™ package includes Voice Call authentication provider, which allows you to control authentication with the help of personal or corporate phone.

## Installing Voice Call 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 Voice Call authentication provider:

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



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

## Removing Voice Call Authentication Provider

In this chapter:

- [Microsoft Windows 7/Microsoft Windows Server 2008 R2](#)
- [Microsoft Windows Server 2003/2003 R2](#)
- [Microsoft Windows 8.1/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 **Voice Call Authentication Provider** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.


### Microsoft Windows Server 2003/2003 R2


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

### Microsoft Windows 8.1/Microsoft Windows Server 2012


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

# Installing and Removing Voice Call 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.

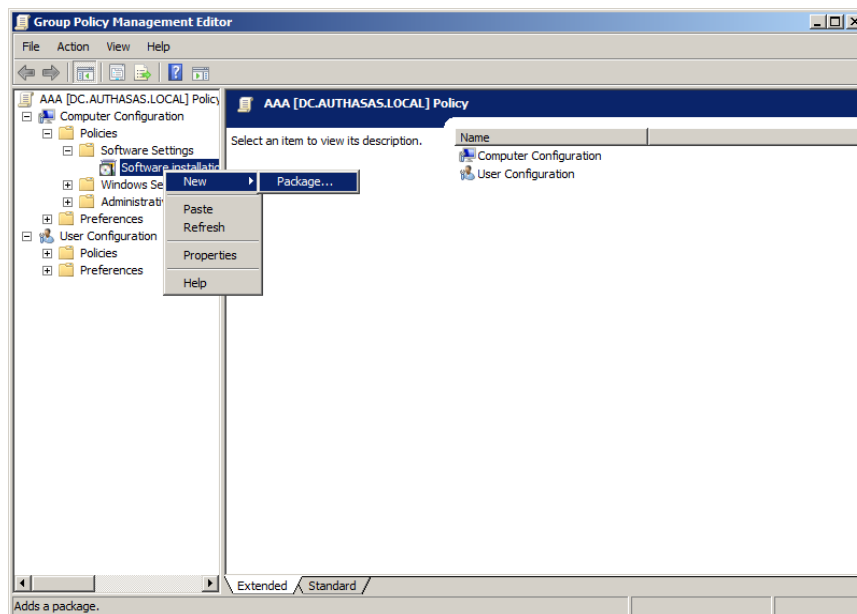
To create new **Group Policy** and configure it:

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 Voice Call Authentication Provider via Group Policy

To install Voice Call 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**.



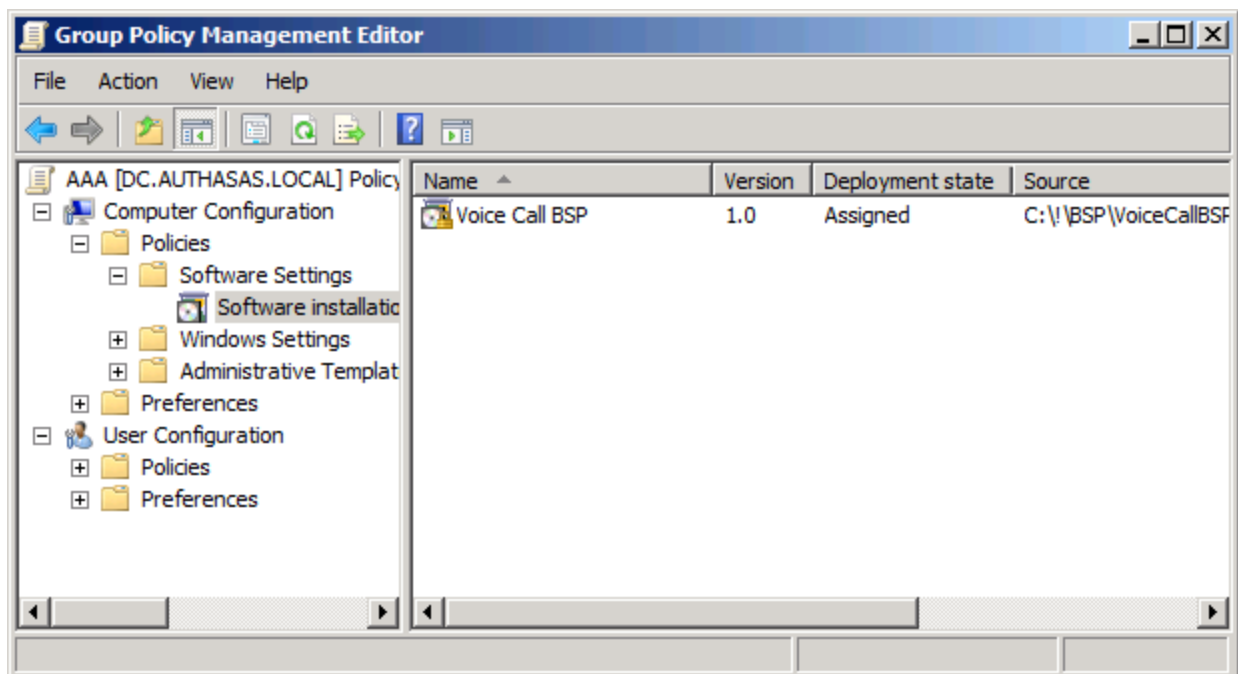
2. Specify the network path to the installer package.



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

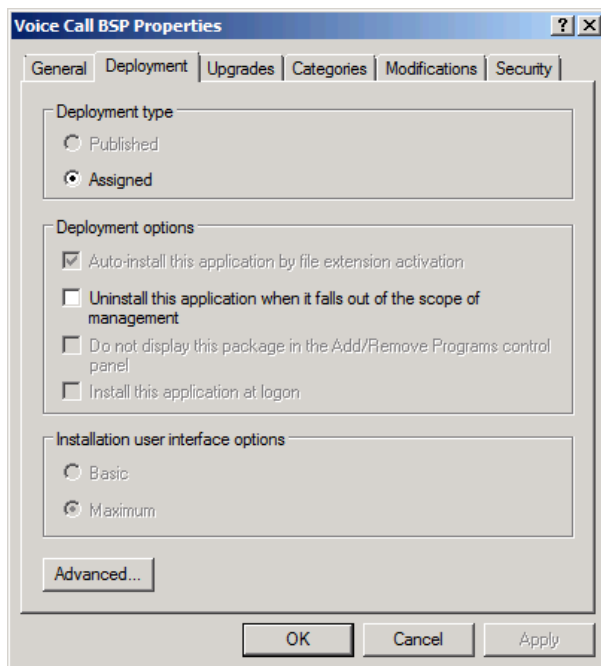
3. In the **Deploy Software** dialog, select **Assigned** and click **OK**.

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

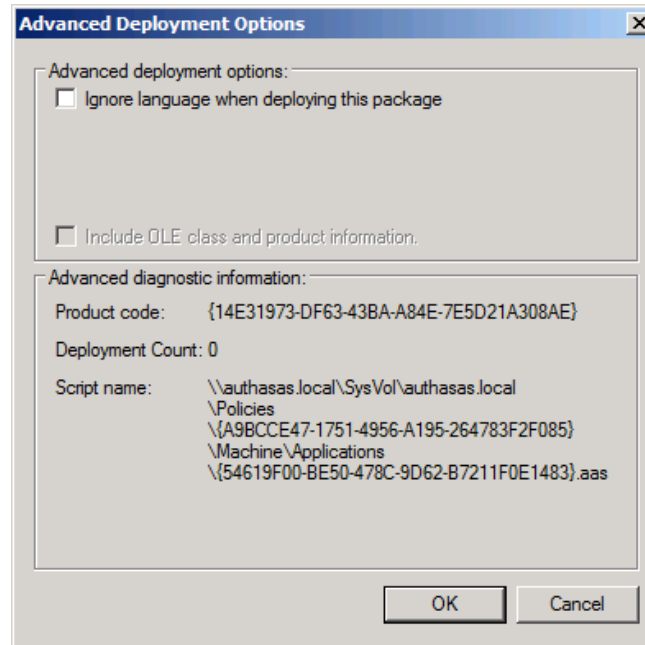


5. Open package properties:

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).



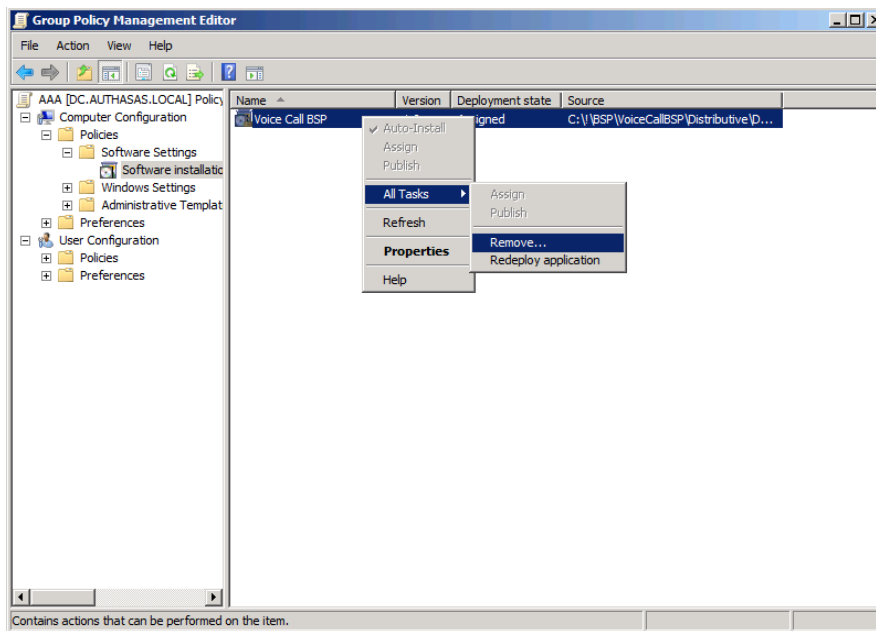
The assigned package is installed after you have updated the domain policy and restarted your computer. To update the domain policy immediately, use the `gpupdate /force` command.

## Removing Voice Call Authentication Provider Components via Group Policy

To remove Voice Call 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 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.

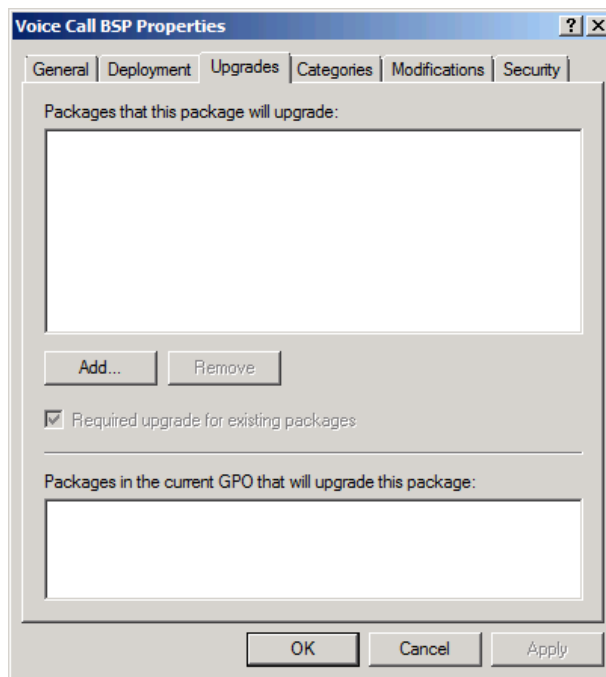
\* If you have cleared the **Uninstall this application when it falls out of the scope of management** check box as it was recommended, software will not be uninstalled after selecting **Immediately uninstall the software from users and computers**. In this case, you will need to uninstall it via **Programs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

## Upgrading Voice Call 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.

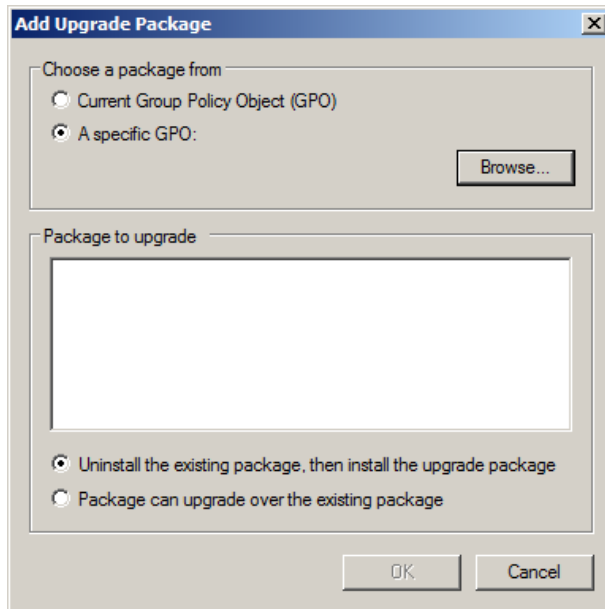
**Option 2:** The more reliable upgrading procedure implies creating new group policy object for new installers:

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.

## 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 Voice Call Authentication Provider

**Description:**

Error appears when installing Voice Call authentication provider on your computer.

**Cause:**

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

---

## A

Active Directory 5, 7  
Authentication 1, 3-5, 7, 9-12, 15-16, 18  
Authenticator 3

## C

Client 3  
Console 11  
Control 10  
Control panel 10  
Create 6, 11, 16

## D

Default 11  
Domain 11

## E

Error 18

## G

GPMC 11  
GPME 11-12, 15

## L

Logon 3

## M

Microsoft Windows Server 2003 10-11

## P

Package 12, 16  
PIN 6  
Policy 11-12

## R

Remove 10, 15

---

## S

Security 11  
Server 4, 6  
Settings 10  
Software 12, 15  
System 4

## U

User 7

## W

Windows 4  
Windows 7 4, 10  
Windows 8 10