



NetIQ Access Manager - Advanced Authentication Plugin

Installation Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Environment	4
NetIQ Access Manager Advanced Authentication Plugin Installation	5
Automatic Mode	5
Manual Mode	6
JSP Files	7
NetIQ Authentication Support Configuration	8
NetIQ EMail + LDAP Authentication Support Configuration	9
NetIQ HOTP + LDAP Authentication Support Configuration	10
NetIQ RADIUS + LDAP Authentication Support Configuration	11
NetIQ Security Question + LDAP Authentication Support Configuration	12
NetIQ Smartphone + LDAP Authentication Support Configuration	13
NetIQ SMS + LDAP Authentication Support Configuration	14
NetIQ TOTP + LDAP Authentication Support Configuration	15
NetIQ Voice Call + LDAP Authentication Support Configuration	16
Debug Logging	17
Index	18

Introduction

About This Document

Purpose of the Document

This Installation Guide is intended for system administrators and describes how to install NetIQ Access Manager Advanced Authentication Plugin.

Document Conventions

This document uses the following 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, and buttons are put in bold type, e.g.: the **Logon** window.


Environment

Components that are required for installation:

- NetIQ Access Manager 3.2.2 / 4.0.1

 User Store should be configured for the used repo in the NAM appliance.

NetIQ Access Manager Advanced Authentication Plugin Installation

 Root permissions are required for the installation of NetIQ Access Manager Advanced Authentication Plugin.

NetIQ Access Manager can be installed in 2 modes:

- | [Automatic Mode](#)
- | [Manual Mode](#)

Automatic Mode

To install NetIQ Access Manager Advanced Authentication Plugin in the automatic mode:

1. Copy **NetIQNAMAAPPluginSetup.jar** to the NAM instance.
2. Install **NetIQNAMAAPPluginSetup.jar** using the **java -jar** command.
3. Follow the steps required for NetIQ Access Manager Advanced Authentication Plugin installation:
 - | After the installation is started and the *"Welcome to the installation of NetIQ Access Manager - Advanced Authentication Plugin"* text is displayed, press 1 to continue.
 - | After the *"Consider it as a license..."* text, press 1 to accept.
 - | When you are suggested to select target path, enter */opt/novell*.
 - | If the directory already exists and is not empty, press 1 to continue, if you confirm the installation and removal of all existing files.
 - | Select the packs you want to install. Press 1 to select an applicable pack, 0 – to deselect a pack.
 - | After the pack selection is done, press 1 to continue.
4. Follow the steps required for configuration of connection to NetIQ Advanced Authentication Framework - Authenticore Server v5:
 - | Specify **Server address**: value: <server IP address>.
 - | Specify **Server port**: value: <server port> (for HTTPS - 443, for HTTP - 80).
 - | If server uses HTTPS protocol, press 1. If server uses HTTP protocol, press 0.
 - | Specify **Administrator name**: value: local\<server local admin>.
 - | Specify **Administrator password**: value <local admin's password>
 - | Press 1 to finish NetIQ Access Manager Advanced Authentication Plugin configuration.
5. NetIQ Access Manager Advanced Authentication Plugin will be successfully installed.


Manual Mode

To install NetIQ Access Manager Advanced Authentication Plugin in the manual mode:

1. Copy files from distributive content location **auCoreLib.jar**, **NAMPluginAuCore.jar**, **lib/gson-2.2.4.jar**, **lib/commons-codec-1.9.jar** to
 - ┆ **Linux:** /opt/novell/nam/idp/webapps/nidp/WEB-INF/lib
 - ┆ **Windows:** C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib
2. Copy files from distributive content location **auCoreLib.jar**, **lib/gson-2.2.4.jar**, **lib/commons-codec-1.9.jar** to
 - ┆ **Linux:** /opt/novell/nam/idp/endorsed
 - ┆ **Windows:** C:\Program Files (x86)\Novell\Tomcat\endorsed
3. Copy files from **jsp** folder (see the [JSP Files](#) chapter to view the list of all jsp files for each method) of distributive location to
 - ┆ **Linux:** /opt/novell/nids/lib/webapp/jsp
 - ┆ **Windows:** C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp
4. Copy additional assets from **assets/images** and **assets/js** folders in distributive location to
 - ┆ **Linux:** /opt/novell/nids/lib/webapp/images
 - ┆ **Windows:** C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\images
5. Follow the steps to configure the connection to NetIQ Advanced Authentication Framework - Authenticore Server v5:
 - ┆ Create the **config.xml** file in the **/etc/authasas/** folder of the NAM instance (default location, can be changed manually).
 - ┆ Modify the **config.xml** file:

```
<configuration>
  <server>
    <url>{server IP address or its domain name}</url>
    <port>{server port: for HTTPS - 443, for HTTP - 80}</port>
    <https>{flag which determines the usage of an applicable connection
type: for HTTPS - 1, for HTTP - 0}</https>
  </server>
  <endpoint>
    <id>{endpoint id created by admin at the server, by default -
42424242424242424242424242424242}</id>
    <secret>{secret endpoint specified by admin during the creation of
endpoint at the server, by default - 12345678}</secret>
  </endpoint>
</configuration>
```

- | Save the modified file.
- | While configuring an applicable authentication method, add the **CONFIGFILE** property with the specified path to the **config.xml** file.

 The **id** and **secret** parameters should be updated in the **config.xml** file (located in the **/etc/authasas/** folder of the NAM instance) in accordance with every newly added endpoint at the NetIQ Advanced Authentication Framework - Authenticore Server v5.

JSP Files

For Email + LDAP Authentication Method Copy:

- | EMailAuthStep1.jsp
- | EMailAuthStep2.jsp

For HOTP + LDAP Authentication Method Copy:

- | HOTPAuthStep1.jsp
- | HOTPAuthStep2.jsp

For RADIUS + LDAP Authentication Method Copy:

- | RadiusAuthStep1.jsp
- | RadiusAuthStep2.jsp

For Security Question+ LDAP Authentication Method Copy:

- | SecQuestionAuthStep1.jsp
- | SecQuestionAuthStep2.jsp

For Smartphone + LDAP Authentication Method Copy:

- | SmartphoneOTPAuthStep1.jsp
- | SmartphoneOTPAuthStep2.jsp

For SMS + LDAP Authentication Method Copy:

- | SMSAuthStep1.jsp
- | SMSAuthStep2.jsp

For TOTP + LDAP Authentication Method Copy:

- | TOTPAuthStep1.jsp
- | TOTPAuthStep2.jsp

For Voice Call + LDAP Authentication Method Copy:

- | VoiceCallAuthStep1.jsp
- | VoiceCallAuthStep2.jsp

NetIQ Authentication Support Configuration

In this chapter:

- | [NetIQ EMail + LDAP Authentication Support Configuration](#)
- | [NetIQ HOTP + LDAP Authentication Support Configuration](#)
- | [NetIQ RADIUS + LDAP Authentication Support Configuration](#)
- | [NetIQ Security Question + LDAP Authentication Support Configuration](#)
- | [NetIQ Smartphone + LDAP Authentication Support Configuration](#)
- | [NetIQ SMS + LDAP Authentication Support Configuration](#)
- | [NetIQ TOTP + LDAP Authentication Support Configuration](#)
- | [NetIQ Voice Call + LDAP Authentication Support Configuration](#)

NetIQ EMail + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** Email Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.email.EMailClass
2. Create a new authentication method for the class:
 - a. **Display Name:** EMail Method
 - b. **Class:** EMail Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 1. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** EMail Contract;
 - b. **URI:** emailandldap/uri;
 - c. **Methods:** EMail Method;
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** EMAIL_ID;
 - b. **Text:** NetIQ Email Authentication;
 - c. **Image:** <Select Local Image>, then select **NAMAA_EMail.png**.
6. Update NAM Server configuration.

NetIQ HOTP + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** HOTP Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.oauth.HOTPClass
2. Create a new authentication method for the class:
 - a. **Display Name:** HOTP Method
 - b. **Class:** HOTP Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 1. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** HOTP Contract
 - b. **URI:** hotpandldap/uri
 - c. **Methods:** HOTP Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** HOTP_ID
 - b. **Text:** NetIQ HOTP Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_HOTP.png**
6. Update NAM Server configuration.

NetIQ RADIUS + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** RADIUS Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.radius.RadiusClass
2. Create a new authentication method for the class:
 - a. **Display Name:** RADIUS Method
 - b. **Class:** RADIUS Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 - i. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** RADIUS Contract
 - b. **URI:** radiusandldap/uri
 - c. **Methods:** RADIUS Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** RADIUS_ID
 - b. **Text:** NetIQ RADIUS Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_RADIUS.png**
6. Update NAM Server configuration.

NetIQ Security Question + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** SecurityQuestion Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.securityquestion.SecurityQuestionClass
2. Create a new authentication method for the class:
 - a. **Display Name:** SecurityQuestion Method
 - b. **Class:** SecurityQuestion Class
 - a. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - b. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 - a. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** SecurityQuestio Contract
 - b. **URI:** securityquestionandldap/uri
 - c. **Methods:** SecurityQuestion Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** SECURITYQUESTION_ID
 - b. **Text:** NetIQ Security Question Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_SecurityQuestions.png**
6. Update NAM Server configuration.

NetIQ Smartphone + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** Smartphone Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.smartphone.SmartphoneClass
2. Create a new authentication method for the class:
 - a. **Display Name:** Smartphone Method
 - b. **Class:** Smartphone Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 - i. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** Smartphone Contract
 - b. **URI:** smartphoneandldap/uri
 - c. **Methods:** Smartphone Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** SMARTPHONE_ID
 - b. **Text:** NetIQ Smartphone Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_Smartphone.png**
6. Update NAM Server configuration.

NetIQ SMS + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** SMS Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.sms.SMSClass
2. Create a new authentication method for the class:
 - a. **Display Name:** SMS Method
 - b. **Class:** SMS Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 - i. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** SMS Contract
 - b. **URI:** smsandldap/uri
 - c. **Methods:** SMS Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** SMS_ID
 - b. **Text:** NetIQ SMS Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_SMS.png**
6. Update NAM Server configuration.

NetIQ TOTP + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** TOTP Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.oauth.TOTPClass
2. Create a new authentication method for the class:
 - a. **Display Name:** TOTP Method
 - b. **Class:** TOTP Class
 - c. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - d. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 - i. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** TOTP Contract
 - b. **URI:** totpandldap/uri
 - c. **Methods:** TOTP Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** TOTP_ID
 - b. **Text:** NetIQ TOTP Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_TOTP.png**
6. Update NAM Server configuration.

NetIQ Voice Call + LDAP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** Voice call Class
 - b. **Java class:** Other
 - c. **Java class path:** com.authasas.aucore.nam.method.voicecall.VoiceCallClass
2. Create a new authentication method for the class:
 - a. **Display Name:** Voice call Method
 - b. **Class:** Voice call Class
 - a. Keep the **Identifies User** checkbox selected. Select the **Overwrite Temporary User** and **Overwrite Real User** checkboxes.
 - b. Add the used user store to **User Stores**.
3. Add the following property (KEY/Value):
 1. **CONFIGFILE:** path to configuration file (this parameter is used only if configuration file has different location, the default location is /etc/authasas/config.xml)
4. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** Voice call Contract
 - b. **URI:** voicecallandldap/uri
 - c. **Methods:** Voice call Method
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** VOICECALL_ID
 - b. **Text:** NetIQ Voice call Authentication
 - c. **Image:** <Select Local Image>, then select **NAMAA_VoiceCall.png**
6. Update NAM Server configuration.

Debug Logging

The logs are stored in `/var/opt/novell/nam/logs/idp/tomcat/catalina.out`. Please check the file in case of any problems with authentication.

Index

A

Administrator 5
Authentication 1, 3, 5-16
Authenticator 3

C

Card 9-10, 13-14, 16
Create 6, 9-16

L

Local 9-16
Logon 3

R

RADIUS 7-8, 11

S

Security 7-8, 12
Server 5-6, 9-16
Support 8

T

TOTP 7-8, 15

U

User 4, 9-16

W

Windows 6