NetIQ Access Manager - Advanced Authentication Plugin

Installation Guide

Version 5.2.0

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 6

Manual Mode 7

NAM Advanced Authentication Plugin Configurator Tool 8

NetIQ Authentication Support Configuration **9**

Email Method Support Configuration 10

Emergency Password Method Support Configuration 12

FIDO U2F Method Support Configuration 14

HOTP Method Support Configuration 16

Password Method Support Configuration 18

RADIUS Method Support Configuration 20

Security Questions Method Support Configuration 22

Smartcard Method Support Configuration 24

Smartphone Method Support Configuration 26

SMS Method Support Configuration 28

TOTP Method Support Configuration 30

Voice Call Method Support Configuration 32

Optional Properties 34

Logging In To NetIQ Access Manager **36**

Troubleshooting **37**

Debug Logging 37

An error "Incompatible installation detected" occurs during the NAM AA plugin upgrade 38

Index **39**

© NetIQ

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.

© *NetIQ*

Environment

Components that are required for installation:

- NetIQ Access Manager 4.0.1/NetIQ Access Manager 4.1
- NetIQ Advanced Authentication Server 5.2

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

© *NetIQ*

NetIQ Access Manager Advanced Authentication Plugin Installation

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

It is required to set **Require admin password to register endpoint/workstation** to **OFF** in **Endpoint management options** on NetIQ Advanced Authentication Administrative Portal. Otherwise the required endpoint won't be created.

NetIQ Access Manager Advanced Authentication Plugin can be installed in 2 modes:

- Automatic Mode
- Manual Mode

© *NetIQ*

Automatic Mode

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

1. Extract the contents of **NAMPlugin_*.zip** package and copy **NetIQNAMAAPluginSetup.jar** to /tmp directory of the IDP NAM instance.
2. Run **NetIQNAMAAPluginSetup.jar**.
   E.g., *java -jar /tmp/NetIQNAMAAPluginSetup.jar*.
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 "*A readme file...*" text, 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*.
   - The following text will be displayed: "*The directory already exists. Do you want to continue?*". To confirm installation, press 1.
   - Select packages you want to install. Press Y to select an applicable package, N – to deselect a package.
   - After the packages selection is done, press 1 to continue.
4. Follow the steps required to configure connection to NetIQAdvanced Authentication server:
   - The text "NAAF appliance IP address: [localhost]" is displayed, specify NetIQ Advanced Authentication server IP address.
   - If server uses HTTP protocol, press 0. If server uses HTTPS protocol, press 1.
   - Specify NAAF appliance port: value: <server port> (for HTTP - 80, for HTTPS - 443)*.
   - Press 1 to continue. The selected packages will start to unpack.
   - When you are suggested to generate an automatic installation script, press N to decline script generation.

NetIQ Advanced Authentication server uses HTTPS protocol by default.

© *NetIQ*

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**, **libs/*.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**, **libs/*.jar** to
   - **Linux:** /opt/novell/nam/idp/endorsed
   - **Windows:** C:\Program Files (x86)\Novell\Tomcat\endorsed
3. Copy files from **jsp** folder 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. Use the Configuration Tool to configure the connection to NetIQ Authentication Server.

.

© *NetIQ*

NAM Advanced Authentication Plugin Configurator Tool

NetIQ Access Manager Advanced Authentication Plugin contains the **Configurator tool** which is used by NAM AA Plugin installer to configure the connection to NetIQ Authentication Server. It can be also used when it's required to install the NAM AA Plugin manually or to change an existing NAM Advanced Authentication Plugin configuration. In this case it allows to avoid the repeated installation.

The Configuration tool can be used using the following way:

```
./java -jar /opt/novell/aaaconfigurator/configurator.jar
"<NetIQAdvancedAuthenticationServerIPAddress>" <Port>
<1forHTTPS|0forHTTP>
```

For example,

```
./java -jar /opt/novell/aaaconfigurator/configurator.jar
"192.168.56.223" 443 1
```

allows to configure NAM Advanced Authentication Plugin to use the NetIQ Advanced Authentication server with IP address 192.168.56.223 by HTTPS.

© *NetIQ*

NetIQ Authentication Support Configuration

It is required to enable the **NAM** event and specify all applicable chains in its settings in NetIQ Admin Interface.

In this chapter:

- NetIQ EMail + LDAP Authentication Support Configuration
- NetIQ Emergency Password + LDAP Authentication Support Configuration
- NetIQ FIDO U2F + LDAP Authentication Support Configuration
- NetIQ HOTP + LDAP Authentication Support Configuration
- NetIQ Password + LDAP Authentication Support Configuration
- NetIQ RADIUS + LDAP Authentication Support Configuration
- NetIQ Security Question + LDAP Authentication Support Configuration
- NetIQ Smartcard + 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 Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: EMail Contract
   b. **URI**: emailandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only EMail Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. EMail Method will provide a request of LDAP Password. After user enters it, an Email message with one-time password will be send and the user will be asked to enter an OTP from the Email message.
      - Add any standard method from the **Available Methods** list as the first one and EMail Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for EMail Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_EMail.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If Email contract is configured to use only Email method, it will be required to configure both **Password & Email** (two-factor) and **Email** (one-factor) chains in the **Chains** section and

© *NetIQ*

enable them in the **NAM** event of the NetIQ Admin Interface. If Email contract is configured to use combination of a standard method and Email method, it will be required to configure and enable only **Email** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Emergency Password Method Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Emergency Password Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aucore.nam.method.emergencypassword.EmergencyPasswordClass

2. Create a new authentication method for the class:
   a. **Display Name**: Emergency Password Method
   b. **Class**: Emergency Password Class
   c. Keep the **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: Emergency Password Contract
   b. **URI**: emrgpasswordandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only Emergency Password Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. Emergency Password Method will provide a request of LDAP Password. After user enters it, he/she will be asked to enter the Emergency Password.
      - Add any standard method from the **Available Methods** list as the first one and Emergency Password Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for Emergency Password Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
   a. **ID**: EmergencyPassword_ID
   b. **Text**: NetIQ Emergency Password Authentication
   c. **Image**: <Select Local Image>, then select **NAM_Emergency_password.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

© *NetIQ*

If Emergency Password contract is configured to use only Emergency Password method, it will be required to configure both **LDAP Password & Emergency Password** (two-factor) and **Emergency Password** (one-factor) chains in the **Chains** section and enable them in the **NAM** event of the NetIQ Administrative Portal. If Emergency Password contract is configured to use combination of a standard method and Emergency Password method, it will be required to configure and enable only **Emergency Password** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

FIDO U2F Method Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: U2F Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aucore.nam.method.fidou2f.FidoU2FClass

2. Create a new authentication method for the class:
   a. **Display Name**: U2F Method
   b. **Class**: U2F Class
   c. Keep the **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: U2F Contract
   b. **URI**: u2fandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only U2F Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. U2F Method will provide a request of LDAP Password. After user enters it, he/she will be asked to insert token and press its button.
      - Add any standard method from the **Available Methods** list as the first one and U2F Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for U2F Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
   a. **ID**: U2F_ID
   b. **Text**: NetIQ FIDO U2F Authentication
   c. **Image**: <Select Local Image>, then select **NAM_U2F.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

FIDO U2F is available starting from NAM AA plugin v2.0.76.

© *NetIQ*

If U2F contract is configured to use only U2F method, it will be required to configure both **Password & U2F** (two-factor) and **U2F** (one-factor) chains in the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If U2F contract is configured to use combination of a standard method and U2F method, it will be required to configure and enable only **U2F** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

By default FIDO U2F works only in Google Chrome. To use it in other browsers, it is required to install FIDO U2F Service. FIDO U2F requires web service for placing NetIQ Access Manager and enroll site in one domain. For more information, see the following article.

© *NetIQ*

HOTP Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: HOTP Contract
   b. **URI**: hotpandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only HOTP Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. HOTP Method will provide a request of LDAP Password. After user enters it, he/she will be asked to generate OTP by smartphone or hardware token and enter it (for YukiKey, the user will be asked to insert the token into the port and press its button).
      - Add any standard method from the **Available Methods** list as the first one and HOTP Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for HOTP Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_HOTP.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

© *NetIQ*

If HOTP contract is configured to use only HOTP method, it will be required to configure both **Password & HOTP** (two-factor) and **Counter based one time password** (one-factor) chains in the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If HOTP contract is configured to use combination of a standard method and HOTP method, it will be required to configure and enable only **Counter based one time password** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Password Method Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Password Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aucore.nam.method.password.PasswordClass

2. Create a new authentication method for the class:
   a. **Display Name**: Password Method
   b. **Class**: Password Class
   c. Keep the **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: Password Contract
   b. **URI**: passwordandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only Password Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. Password Method will provide a request of LDAP Password. After user enters it, he/she will be asked to enter the Password.
      - Add any standard method from the **Available Methods** list as the first one and Password Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for Password Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
   a. **ID**: Password_ID
   b. **Text**: NetIQ Password Authentication
   c. **Image**: <Select Local Image>, then select **NAM_Password.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If Password contract is configured to use only Password method, it will be required to configure both **LDAP Password & Password** (two-factor) and **Password** (one-factor) chains in

© *NetIQ*

the **Chains** section and enable them in the **NAM** event of the NetIQ Administrative Portal. If Password contract is configured to use combination of a standard method and Password method, it will be required to configure and enable only **Password** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

RADIUS Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: RADIUS Contract
   b. **URI**: radiusandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only RADIUS Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. RADIUS Method will provide a request of LDAP Password. After user enters it, he/she will be asked to authenticate via RADIUS server.
      - Add any standard method from the **Available Methods** list as the first one and RADIUS Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for RADIUS Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_RADIUS.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If RADIUS contract is configured to use only RADIUS method, it will be required to configure both **Password & Radius Client** (two-factor) and **Radius Client** (one-factor) chains in

© *NetIQ*

the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If RADIUS contract is configured to use combination of a standard method and RADIUS method, it will be required to configure and enable only **Radius Client** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Security Questions Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   b. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: SecurityQuestion Contract
   b. **URI**: securityquestionandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only SecurityQuestion Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. SecurityQuestion Method will provide a request of LDAP Password. After user enters it, he/she will be asked to enter answers to the list of security questions.
      - Add any standard method from the **Available Methods** list as the first one and SecurityQuestion Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for SecurityQuestion Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_SecurityQuestions.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If SecurityQuestion contract is configured to use only SecurityQuestion method, it will be required to configure both **Password & Security Questions** (two-factor) and

© *NetIQ*

Security Questions (one-factor) chains in the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If SecurityQuestion contract is configured to use combination of a standard method and SecurityQuestion method, it will be required to configure and enable only **Security Questions** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Smartcard Method Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Smartcard Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aucore.nam.method.smartcard.SmartcardClass

2. Create a new authentication method for the class:
   a. **Display Name**: Smartcard Method
   b. **Class**: Smartcard Class
   a. Keep the **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   b. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: Smartcard Contract
   b. **URI**: smartcardandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only Smartcard Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. Smartcard Method will provide a request of LDAP Password. After user enters it, he/she will be asked to tap the smartcard.
      - Add any standard method from the **Available Methods** list as the first one and Smartcard Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for Smartcard Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
   a. **ID**: SMARTCARD_ID
   b. **Text**: NetIQ Smartcard Authentication
   c. **Image**: <Select Local Image>, then select **NAM_Smartcard.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If Smartcard contract is configured to use only Smartcard method, it will be required to configure both **Password & Smartcard** (two-factor) and **Smartcard** (one-factor) chains in the

© *NetIQ*

Chains section and enable them in the **NAM** event of the NetIQ Admin Interface. If Smartcard contract is configured to use combination of a standard method and Smartcard method, it will be required to configure and enable only **Smartcard** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Smartphone Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: Smartphone Contract
   b. **URI**: smartphoneandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only Smartphone Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. Smartphone Method will provide a request of LDAP Password. After user enters it, he/she will be asked to accept the authentication on user's smartphone.
      - Add any standard method from the **Available Methods** list as the first one and Smartphone Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for Smartphone Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_Smartphone.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If Smartphone contract is configured to use only Smartphone method, it will be required to configure both **Password & Smartphone Out-of-Band** (two-factor) and **Smartphone** (one-

© *NetIQ*

factor) chains in the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If Smartphone contract is configured to use combination of a standard method and Smartphone method, it will be required to configure and enable only **Smartphone** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

SMS Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: SMS Contract
   b. **URI**: smsandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only SMS Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. SMS Method will provide a request of LDAP Password. After user enters it, SMS message with one-time password will be send and the user will be asked to enter an OTP from the SMS message.
      - Add any standard method from the **Available Methods** list as the first one and SMS Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for SMS Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_SMS.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If SMS contract is configured to use only SMS method, it will be required to configure both **Password & SMS OTP** (two-factor) and **SMS** (one-factor) chains in the **Chains** section and

© *NetIQ*

enable them in the **NAM** event of the NetIQ Admin Interface. If SMS contract is configured to use combination of a standard method and SMS method, it will be required to configure and enable only **SMS** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

TOTP Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   d. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: TOTP Contract
   b. **URI**: totpandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only TOTP Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. TOTP Method will provide a request of LDAP Password. After user enters it, he/she will be asked to enter OTP generated by NetIQ Smartphone Authenticator.
      - Add any standard method from the **Available Methods** list as the first one and TOTP Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for TOTP Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_TOTP.png** from the **icons** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If TOTP contract is configured to use only TOTP method, it will be required to configure both **Password & TOTP** (two-factor) and **Time based one time password** (one-factor) chains in

© *NetIQ*

the **Chains** section and enable them in the **NAM** event of the NetIQ Admin Interface. If TOTP contract is configured to use combination of a standard method and TOTP method, it will be required to configure and enable only **Time based one time password** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Voice Call Method 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 **Overwrite Temporary User** and **Overwrite Real User** checkboxes cleared.
   b. Add the used user store to **User Stores**.

3. Add applicable optional properties (KEY/Value).

4. Create a new authentication contract for the method in the **Configuration** tab:
   a. **Display name**: Voice call Contract
   b. **URI**: voicecallandldap/uri
   c. Configure **Methods**. Select one of the following options:
      - Add only Voice call Method from the **Available Methods** list. In this case the **Identifies User** checkbox must be selected. Voice call Method will provide a request of LDAP Password. After user enters it, he/she will get a call on the phone and will be asked to input the specified PIN.
      - Add any standard method from the **Available Methods** list as the first one and Voice call Method as the second one. In this case the **Identifies User** checkbox should be obligatory cleared for Voice call Method.
   d. Keep the **Satisfiable by External Provider** checkbox cleared.

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 **NAM_VoiceCall.png** folder of the NAM Plugin distribution kit.

6. Update both the IDP and the MAG.

7. Update NAM Server configuration.

If Voice call contract is configured to use only Voice call method, it will be required to configure both **Password & Voicecall** (two-factor) and **Voicecall** (one-factor) chains in the

© *NetIQ*

Chains section and enable them in the **NAM** event of the NetIQ Admin Interface. If Voicecall contract is configured to use combination of a standard method and Voicecall method, it will be required to configure and enable only **Voicecall** (one-factor) chain.

The following standard methods are supported by NAM plugin:

- Name/Password - Form
- Name/Password - Basic
- Secure Name/Password - Form
- Secure Name/Password - Basic

© *NetIQ*

Optional Properties

NetIQ Access Manager Advanced Authentication Plugin supports the following optional properties (KEY/Value) for authentication methods:

- **REPONAME**: the name of the repository that is used for NetIQ Advanced Authentication framework. This parameter may not be used if default repo is already selected in the **Login options** policy of NetIQ Advanced Authentication Framework server appliance.
- **CONFIGFILE**: path to configuration file. This parameter is used only if configuration file has different location. The default configuration file location for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.
- **RECHECKTIMEOUT**: timeout parameter that is used to prevent loops. The default value is 300 seconds. The minimum recommended value for:
    - **Email** method is 120 seconds
    - **FIDO U2F** method is 30 seconds
    - **HOTP** method is 30 seconds
    - **RADIUS** method is 30 seconds
    - **Security Question** method is 30 seconds
    - **Smartcard** method is 30 seconds
    - **Smartphone** method is 60 seconds
    - **SMS** method is 30 seconds
    - **TOTP** method is 30 seconds
    - **Voicecall** method is 30-60 seconds
- **ERRORJSP**: name of JSP page (without .jsp) for information on error. This is for critical errors and failures only, which are related to the authentication process (e.g. method is not enrolled). The default file is PluginErrorPage.jsp, it's located in /opt/novell/nids/lib/webapp/jsp (Linux), $INSTALL_PATH\Tomcat\webapps\nidp\jsp (Windows).
- **LDAPJSP**: name of LDAP authentication page (without .jsp). This parameter is used for customization and allows changing page for LDAP login for each method. The default file is LdapAuth.jsp, it's located in /opt/novell/nids/lib/webapp/jsp (Linux), $INSTALL_PATH\Tomcat\webapps\nidp\jsp (Windows).
- **METHODJSP**: name of method page (without .jsp). This parameter is used for customization and allows changing page for each method. The default file is <MethodName>Auth.jsp, it's located in /opt/novell/nids/lib/webapp/jsp (Linux), $INSTALL_PATH\Tomcat\webapps\nidp\jsp (Windows).
- **LDAPSYNCJSP**: name of page for LDAP password synchronization (without jsp). The default file is LDAPSyncPage.jsp, it's located in /opt/novell/nids/lib/webapp/jsp (Linux), $INSTALL_PATH\Tomcat\webapps\nidp\jsp (Windows).

© *NetIQ*

- **PWDMAXLENGTH**: parameter that is used to restrict maximum length of the password. The default value is 100 characters. This parameter can be used only for YubiKey tokens.
- **ENROLLURL**: URL to NetIQ Advanced Authentication Self-Service Portal. The default value is https://<NetIQAdvancedAuthenticationFramework_server_address>:<server_port>/account.

Parameters **ERRORJSP**, **LDAPJSP**, **METHODJSP**, **LDAPSYNCHJSP** and **ENROLLURL** are available starting from NetIQ Advanced Authentication Framework v5.2, NAM AA plugin v2.0.76.

© *NetIQ*

Logging In To NetIQ Access Manager

To log in to NetIQ Access Manager with Password + NetIQ authentication method, users should follow the steps:

1. Select an applicable authentication method.
2. Enter username in the following format:
    - **username** - if the default repo name is specified in NAAF appliance or REPONAME property is specified in authentication method settings in NAM
    - **reponame\username** - in other case
3. Enter password and click **Login**.
4. Authenticate with NetIQ method.
5. The session will be successfully authenticated.

To log in to NetIQ Access Manager with NetIQ authentication method after authentication with the standard method, verify whether default repo name is specified in NAAF appliance or REPONAME property is specified in authentication method settings in NAM. It should be obligatory specified. Users should follow the steps:

1. Select an applicable authentication method.
2. Enter username.
3. Authenticate with NetIQ method.
4. The session will be successfully authenticated.

To specify default repo name in NAAF appliance, follow the steps:

1. Go to NetIQ Admin Interface.
2. Open the **Policies** section.
3. Click the **Edit** button next to the **Login options** policy.
4. Specify an applicable repo name in the **Default repo name** text field.
5. Click the **Save** button.

© *NetIQ*

Troubleshooting

The article contains information on how to troubleshoot the common issues and how to get the debug logs.

- Debug logging.
- An error "Incompatible installation detected..." occurs during upgrade.

Debug Logging

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

The stated below optional parameters (KEY/Value) for authentication methods are available starting from NAM AA plugin 2.0.76 and later:

- **DEBUG**: parameter that allows to collect additional information in the log file. With this parameter enabled all data on server requests and server responses will be added to the log file.
  Value: 1, means that the debug logging is enabled.

- **LOGFILE**: path to plugin log file in case it should be saved in a different place.
  Value: full file path to the log file (e.g. /tmp/NAMAAplugin.log)

© NetIQ

An error "Incompatible installation detected" occurs during the NAM AA plugin upgrade

Description:

While trying to upgrade NetIQ Access Manager Advanced Authentication Plugin, I get the following error: "*Incompatible installation detected. Uninstall it first, or choose another directory to install to*". How can I uninstall the old version of NetIQ Access Manager Advanced Authentication Plugin and install a new one?

Solution:

To install a new version of NetIQ Access Manager Advanced Authentication Plugin, remove the following files manually:

- */opt/novell/Uninstaller/uninstaller.jar ?*
- */opt/novell/.installationinformation*

Run the installer once again.

© *NetIQ*

Index

A

Authentication 1, 3-10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 38
Authenticator 3, 30

C

Client 20
Create 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

D

Default 36

E

Edit 36

L

Local 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
Logon 3

O

OTP 28

P

Password 9-10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 36
Properties 34

R

RADIUS 9, 20, 34

S

Security 9, 22, 34
Server 7-8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32
Support 9-10, 14, 16, 24, 26, 28, 32

T

Tool 7
TOTP 9, 30, 34

© *NetIQ*

U

User 4, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32

W

Windows 7, 34

© *NetIQ*