NetIQ Access Manager - Advanced Authentication Plugin

Installation Guide

Version 5.1.0

Table of Contents

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.

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

Environment

Components that are required for installation:

- NetIQ Access Manager 4.0.1/NetIQ Access Manager 4.1

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 the downloaded **NAMPlugin_*.zip** to the IDP NAM instance and extract the contents.
2. Run **NetIQNAMAAPluginSetup.jar** in the root of the extracted directory.
   E.g., *java -jar ./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 NAAF appliance:
   - Specify NAAF appliance IP address or Domain Name: value: <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.
5. NetIQ Access Manager Advanced Authentication Plugin is successfully installed.

NAAF appliance uses HTTPS protocol by default.

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/gson-2.2.4.jar**, **libs/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**, **libs/gson-2.2.4.jar**, **libs/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/aaplugin/** 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/aaplugin/** folder of the NAM instance) in accordance with every newly added endpoint of the NetIQ Admin Interface. Currently the **id** and **secret** parameters cannot be updated.

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

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

✳ Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
   - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
   - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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

3. Add the following optional properties (KEY/Value):
    - **REPONAME**: the name of the repository that is used for NetIQ authentication framework
    - **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 v2.0.48 and earlier is /etc/authasas/config.xml, for NAM AA Plugin v2.0.49 and later - /etc/aaplugin/config.xml.

Please change the configuration file path manually on upgrade to NAM AA Plugin v2.0.49 and later. Click the **CONFIGFILE** property for the specific configured method, specify new property value and save changes.

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 **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

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