NetIQ Access Manager - Advanced Authentication Plugin

Installation Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This NetIQ Access Manager Advanced Authentication Plugin 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.

ℹ️ **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.
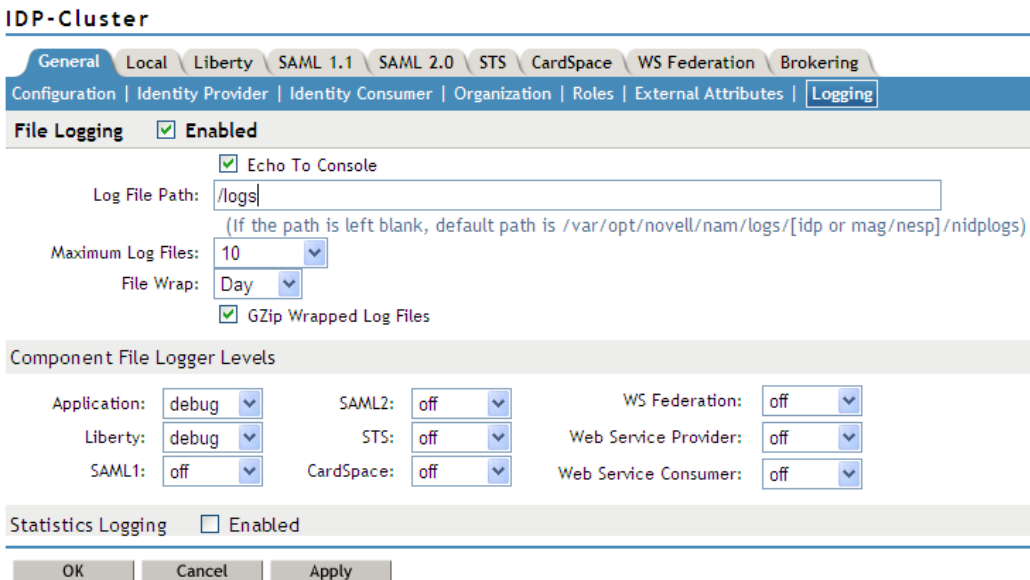
Environment

Components that are required for installation:

- NetIQ Access Manager 4.0.1/NetIQ Access Manager 4.1
- NetIQ Web Service 4.8 and later (all necessary authentication providers should be installed together with Web Service)
- NetIQ Password Filter should be obligatory installed on all Domain Controllers in the domain

✱ Flash support is available on Linux only when libblkid is installed and udev rules are set. Udev rules allow access to usb-devices for non-superusers.

✱ LogFile parameter should contain a full path to log file. If it contains only a file name without the actual path, it will be placed into a temporary folder by default. It will be possible to find a path only with "find / -name [logfilename]". Otherwise LogFile parameter will be placed to the folder that was created or chosen by the user.

© NetIQ

NetIQ Access Manager Advanced Authentication Plugin Installation

Install NAMAAPluginSetup.jar to the */opt/novell* folder on NetIQ Access Manager.

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

To install NetIQ Access Manager Advanced Authentication Plugin:

1. After the installation is started and the *"Welcome to the installation of NetIQ Access Manager – Advanced Authentication Plugin"*, the text is displayed. Press 1 to continue.
2. After the *"Consider it as a license..."* text, press 1 to accept.
3. When you are suggested to select target path, enter *opt/novell*.
4. If the directory already exists and is not empty, press 1 to continue, if you confirm the installation and deleting of all existing files.
5. Select the packs you want to install. Input 1 to select the required pack, 0 – to deselect the pack.
6. After the pack selection is done, press 1 to continue.
7. NetIQ Access Manager Advanced Authentication Plugin was installed successfully on /opt/novell.

The installation process looks like the following:

```
NAM:/jre/bin # ./java -jar /flash/NAM_Plugin/1.0.28/NAMAAPluginSetup.jar
Welcome to the installation of NetIQ Access Manager - Advanced Authentication Plugin 06.10.2013!
 - NetIQ
The homepage is at: http://www.netiq.com/
press 1 to continue, 2 to quit, 3 to redisplay
1
Consider it as a licence...
press 1 to accept, 2 to reject, 3 to redisplay
1
Select target path [/jre/bin]
/opt/novell
The directory already exists and is not empty! Are you sure you want to install here and delete all existing files?
Press 1 to continue, 2 to quit, 3 to redisplay
1
press 1 to continue, 2 to quit, 3 to redisplay
1

Select the packs you want to install:

[<required>] NAM Authentication Plugin Core (NAM Authentication Plugin Core)
[x] OATH Authentication  (OATH Authentication Plugin)
input 1 to select, 0 to deselect:
1
[x] Flash Drive Authentication  (Flash Drive Authentication Plugin)
input 1 to select, 0 to deselect:
1
[x] Smart Card Authentication  (Smart Card Authentication Plugin)
input 1 to select, 0 to deselect:
1

...pack selection done.
press 1 to continue, 2 to quit, 3 to redisplay
1
[ Starting to unpack ]
[ Processing package: NAM Authentication Plugin Core (1/4) ]
[ Processing package: OATH Authentication  (2/4) ]
[ Processing package: Flash Drive Authentication  (3/4) ]
[ Processing package: Smart Card Authentication  (4/4) ]
[ Unpacking finished ]
Install was successful
application installed on /opt/novell
[ Console installation done ]
NAM:/jre/bin #
```

6

NetIQ Access Manager Advanced Authentication Plugin Manual Installation

Unzip NAMAAPluginContent.zip into a temporary folder.

Plugin Core Files

Copy NAMAAPluginCore.jar (from the root of the temporary folder), webservices-rt.jar, webservices-api.jar (from the libs subfolder) to:

Linux: /opt/novell/nam/idp/webapps/nidp/WEB-INF/lib
Windows: C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib

Make sure that commons-codec-1.3.jar is presented in:

Linux: /opt/novell/nam/idp/webapps/nidp/WEB-INF/lib
Windows: C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\lib

Copy webservices-api.jar into the endorsed directory of Tomcat (if it doesn't exist, you have to create it):

Linux: /opt/novell/nam/idp/endorsed
Windows: C:\Program Files (x86)\Novell\Tomcat\endorsed

JSP Files

For Email Authentication Method Copy:

EmailLogin.jsp (from the EmailMethod subfolder).

For Flash Drive Authentication Method Copy:

FlashDriveLogin.jsp (from the FlashDriveMethod subfolder).

For OATH OTP Authentication Method Copy:

OathLogin.jsp (from the OathMethod subfolder).

For RADIUS Authentication Method Copy:

RadiusLogin.jsp (from the RadiusMethod subfolder).

For RTE Authentication Method Copy:

RteLogin.jsp (from the RteMethod subfolder).

For Security Questions Authentication Method Copy:

SecurityQuestionsLogin.jsp (from the SecurityQuestionsMethod subfolder).

For Smartcard Authentication Method Copy:

SmartCardLogin.jsp (from the SmartCardMethod subfolder).

For Smartphone Authentication Method Copy:

SmartphoneLogin.jsp (from the SmartphoneMethod subfolder).

For SMS Authentication Method Copy:

SmsLogin.jsp (from the SmsMethod subfolder).

For Voice Call Authentication Method Copy:

VoiceCallLogin.jsp (from the VoiceCallMethod subfolder).

To the destination folder:

Linux: /opt/novell/nids/lib/webapp/jsp
Windows: C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\jsp

Applet Files

Common Applet Files:

> commons-codec-1.3.jar (from either the FlashDriveMethod or the SmartCardMethod subfolders).

For Email Authentication Method Copy:

> EmailApplet.jar (from the EmailMethod subfolder).

For Flash Drive Authentication Method Copy:

> FlashDriveApplet.jar (from the FlashDriveMethod subfolder).

For OATH OTP Authentication Method Copy:

> OathApplet.jar (from the OathMethod subfolder).

For RADIUS Authentication Method Copy:

> RadiusApplet.jar (from the RadiusMethod subfolder).

For RTE Authentication Method Copy:

> RteApplet.jar (from the RteMethod subfolder).

For Security Questions Authentication Method Copy:

> SecurityQuestionsApplet.jar (from the SecurityQuestionsMethod subfolder).

For Smartcard Authentication Method Copy:

> SmartCardApplet.jar (from the SmartCardMethod subfolder).

For Smartphone Authentication Method Copy:

> SmartphoneApplet.jar (from the SmartphoneMethod subfolder).

For SMS Authentication Method Copy:

> SmsApplet.jar (from the SmsMethod subfolder).

For Voice Call Authentication Method Copy:

> VoiceCallApplet.jar (from the VoiceCallMethod subfolder).

To the destination folder:

Linux: /opt/novell/nam/idp/webapps/nidp/classUtils
Windows: C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\classUtils

NetIQ Authentication Support Configuration

In this chapter:

NetIQ Email 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.aaa.method.email.EmailClass

2. Create a new authentication method for the class:
    a. **Display Name**: Email Method
    b. **Class**: Email Class
    c. Select Active Directory for **User stores**.
    d. Add the following properties (KEY/Value):
    - **JSP**: EmailLogin (without jsp)
    - **DomainName**: <NetBIOSDomainName>
    - **Timeout**: 80000
    - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
    - **BypassCertificate**: True
    - **LogFile**: EmailMethod.log

ⓘ The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
    a. **Display name**: Email Contract
    b. **URI**: email/uri
    c. **Methods**: Email Method
    d. Click **Apply** and go to the **Authentication Card** tab.
    e. **ID**: EMAIL_ID
    f. **Text**: NetIQ Email Authentication
    g. **Image**: <Select Local Image>, then select **NAM_Email.png**

4. Update NAM Server configuration.

NetIQ Flash Drive Authentication Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Flash Drive Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aaa.method.flashdrive.FlashClass

2. Create a new authentication method for the class:
   a. **Display Name**: Flash Drive Method
   b. **Class**: Flash Drive Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: FlashDriveLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 25000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **Enabled1N**: true (to activate 1:N mode – no username required, it will be detected automatically)
   - **BypassCertificate**: true
   - **LogFile**: FlashDriveMethod.log

ℹ️ The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: Flash Drive Contract
   b. **URI**: flashdrive/uri
   c. **Methods**: Flash Drive Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: FLASHDRIVE_ID
   f. **Text**: NetIQ Flash Drive Authentication
   g. **Image**: <Select Local Image>, then select **NAM_FlashDrive.png**

4. Update NAM Server configuration.

NetIQ OATH OTP Authentication Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: OATH Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aaa.method.oath.OathClass

2. Create a new authentication method for the class:
   a. **Display Name**: OATH Method
   b. **Class**: OATH Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: OathLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 25000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **BypassCertificate**: True
   - **LogFile**: OathMethod.log

   ℹ The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: OATH Contract
   b. **URI**: oath/uri
   c. **Methods**: OATH Applet Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: OATH_ID
   f. **Text**: NetIQ OATH OTP Authentication
   g. **Image**: <Select Local Image>, then select **NAM_OATH.png**

4. Update NAM Server configuration.

NetIQ RADIUS 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.aaa.method.sms.RadiusClass

2. Create a new authentication method for the class:
   a. **Display Name**: RADIUS Method
   b. **Class**: RADIUS Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: RadiusLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 60000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **BypassCertificate**: True
   - **LogFile**: RadiusMethod.log

   The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: RADIUS Contract
   b. **URI**: radius/uri
   c. **Methods**: RADIUS Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: RADIUS_ID
   f. **Text**: NetIQ RADIUS Authentication
   g. **Image**: <Select Local Image>, then select **NAM_RADIUS.png**

4. Update NAM Server configuration.

NetIQ RTE Authentication Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: RTE Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aaa.method.rte.RteClass

2. Create a new authentication method for the class:
   a. **Display Name**: RTE Method
   b. **Class**: RTE Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: RteLogin (without jsp)
   - **WebserviceUsed**: true (if the **WebserviceUsed** parameter is set to true, RTE will work through NetIQ Web Service instead of Authenticore Server)
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc/bsc (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **LogFile**: RteLogin.log

3. Create a new authentication contract for the method:
   a. **Display name**: RTE Contract
   b. **URI**: rte/uri
   c. **Methods**: RTE Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: RTE_ID
   f. **Text**: NetIQ RTE Authentication
   g. **Image**: <Select Local Image>, then select **NAM_RTE.png**

4. Update NAM Server configuration.

NetIQ Security Questions Authentication Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Security Questions Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aaa.method.questions.SecurityQuestionsClass

2. Create a new authentication method for the class:
   a. **Display Name**: Security Questions Method
   b. **Class**: Security Questions Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: SecurityQuestionsLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 25000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **BypassCertificate**: True
   - **LogFile**: SecurityQuestions.log

   The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: Security Questions Contract
   b. **URI**: securityquestions/uri
   c. **Methods**: Security Questions Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: SECURITY_QUESTIONS_ID
   f. **Text**: NetIQ Security Questions Authentication
   g. **Image**: <Select Local Image>, then select **NAM_SecurityQuestions.png**

4. Update NAM Server configuration.

NetIQ Smartcard Authentication Support Configuration

1. Create a new authentication class with the following parameters:
   a. **Display name**: Smart Card Class
   b. **Java class**: Other
   c. **Java class path**: com.authasas.aaa.method.smartcard.CardClass

2. Create a new authentication method for the class:
   a. **Display Name**: Smart Card Method
   b. **Class**: Smart Card Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: SmartCardLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 25000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **Enabled1N**: true (to activate 1:N mode – no username required, it will be detected automatically)
   - **BypassCertificate**: true
   - **LogFile**: SmartCardMethod.log
   - **OmnikeyCardEnabled**: true (for OMNIKEY-reader compatible contactless cards)
   - **RfideasCardEnabled**: true (for RfIdeas-reader compatible cards)
   - **CspCardEnabled**: true (for CSP-compatible contact cards)

The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

The attributes **OmnikeyCardEnabled**, **RfideasCardEnabled** and **CspCardEnabled** enable or disable search for cards of specific types. If the attribute for a specific card type is missing or set to false, these cards will be searched.

The attributes **OmnikeyCardEnabled**, **RfideasCardEnabled** and **CspCardEnable** are available only for NAMAA Plugin 1.0.34 and later.

3. Create a new authentication contract for the method:
   a. **Display name**: Smart Card Contract
   b. **URI**: smartcard/uri
   c. **Methods**: Smart Card Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: SMARTCARD_ID

    f. **Text**: NetIQ Smartcard Authentication
   g. **Image**: <Select Local Image>, then select **NAM_SmartCard.png**

4. Update NAM Server configuration.

NetIQ Smartphone 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.aaa.method.smartphone.SmartphoneClass

2. Create a new authentication method for the class:
   a. **Display Name**: Smartphone Method
   b. **Class**: Smartphone Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: SmartphoneLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 90000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **BypassCertificate**: True
   - **LogFile**: Smartphone.log

   The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: Smartphone Contract
   b. **URI**: smartphone/uri
   c. **Methods**: Smartphone Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: SMARTPHONE_ID
   f. **Text**: NetIQ Smartphone Authentication
   g. **Image**: <Select Local Image>, then select **NAM_Smartphone.png**

4. Update NAM Server configuration.

NetIQ SMS 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.aaa.method.sms.SmsClass

2. Create a new authentication method for the class:
   a. **Display Name**: SMS Method
   b. **Class**: SMS Class
   c. Select Active Directory for **User stores**.
   d. Add the following properties (KEY/Value):
   - **JSP**: SmsLogin (without jsp)
   - **DomainName**: <NetBIOSDomainName>
   - **Timeout**: 300000
   - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
   - **BypassCertificate**: True
   - **LogFile**: SmsMethod.log

ℹ The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
   a. **Display name**: SMS Contract
   b. **URI**: sms/uri
   c. **Methods**: SMS Method
   d. Click **Apply** and go to the **Authentication Card** tab.
   e. **ID**: SMS_ID
   f. **Text**: NetIQ SMS Authentication
   g. **Image**: <Select Local Image>, then select **NAM_SMS.png**

4. Update NAM Server configuration.

NetIQ Voice Call 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.aaa.method.voicecall.VoiceCallClass

2. Create a new authentication method for the class:
    a. **Display Name**: Voice Call Method
    b. **Class**: Voice Call Class
    c. Select Active Directory for **User stores**.
    d. Add the following properties (KEY/Value):
    - **JSP**: VoiceCallLogin (without jsp)
    - **DomainName**: <NetBIOSDomainName>
    - **Timeout**: 90000
    - **WebserviceURL**: https://<hostname>:<port>/Service.svc?wsdl (name and port must correspond to the web service configuration and certificate, which was installed with it)
    - **BypassCertificate**: True
    - **LogFile**: VoiceCallMethod.log

  The **Timeout** value defines time period (in milliseconds) during which the NAM waits for an authentication response from the Authenticore Server.

3. Create a new authentication contract for the method:
    a. **Display name**: Voice Call Contract
    b. **URI**: voicecall/uri
    c. **Methods**: Voice Call Method
    d. Click **Apply** and go to the **Authentication Card** tab.
    e. **ID**: VOICE_CALL_ID
    f. **Text**: NetIQ Voice Call Authentication
    g. **Image**: <Select Local Image>, then select **NAM_VoiceCall.png**

4. Update NAM Server configuration.

Certificate Installation

1. Make sure that you are using the same certificate for the both client and server. If you are using the self-signed certificate, shipping with our web service, make sure that you are not using the certificate from the previous installation.

2. On a Windows PC where our web service is installed, add the certificate under *Trusted Root Certification* branch (using the *certmgr.msc* snap-in or via the IE certification dialog).

3. On a PC with a NAM Appliance add the same web service certificate to the following "cacerts" files:

/opt/novell/jdk1.6.0_30/jre/lib/security/cacerts
/jre/lib/security/cacerts

⊗ This path depends on the version of JDK.

the default password to the cacerts file is "*changeit*"
to add certificates use the keytool tool from the following location : */jre/bin/*

you can add the certificate by running the following commands:

./keytool -import -keystore /opt/novell/jdk1.6.0_30/jre/lib/security/cacerts -alias authasas -file PASS_TO_CERTIFICATE_FILE
./keytool -import -keystore /jre/lib/security/cacerts -alias authasas -file PASS_TO_CERTIFICATE_FILE

4. It is not necessary to add the certificate through the administration console UI, since it does not work.

Localization

NetQ Access Manager provides with an opportunity to translate any available string resources into other languages. To configure the display of text in another language, unpack an optional NAMAAResources.jar file and change its localization strings. Currently it consists 2 files. It is possible to create localization for any required language or to change an existing one.
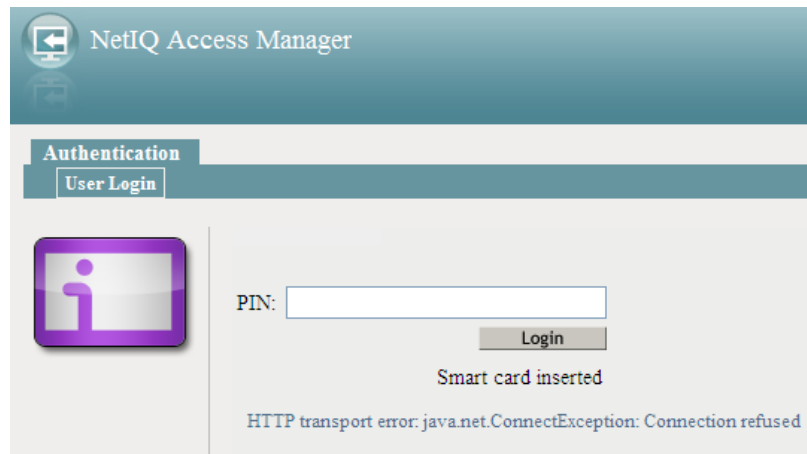
Troubleshooting

ℹ️ This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

NetIQ Web Service Is Not Installed, Not Configured or Protected By Firewall

Description:

Errors appear when using the NetIQ Web Service. The following window is displayed:

Cause:

a. NetIQ Web Service is not installed.
b. NetIQ Web Service is not configured.
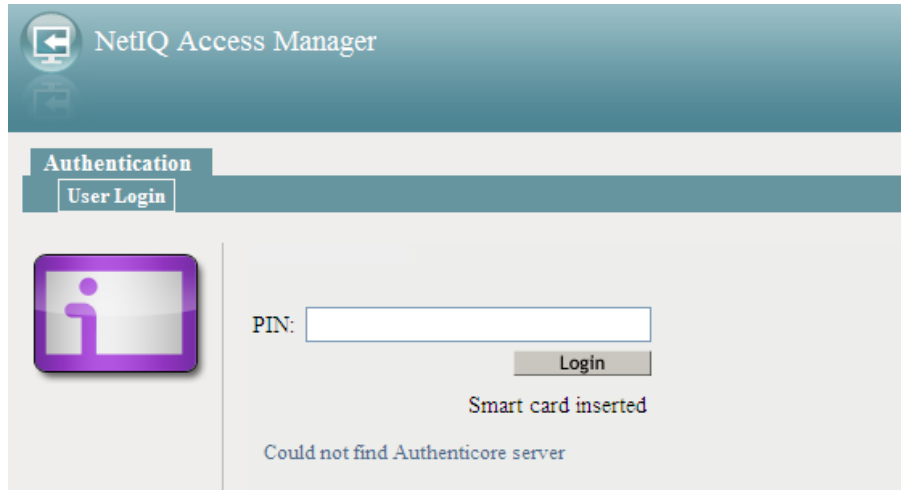c. NetIQ Web Service is protected by firewall.

Solution:

a. Installation of NetIQ Web Service is required.
b. NetIQ Web Service should be configured correctly.
c. Firewall should be disabled for correct work of NetIQ Web Server.

NetIQ Authenticore Server Is Not Installed, Not Configured or Protected By Firewall

Description:

NetIQ Authenticore Server cannot be found. The following window is displayed:

Cause:

   a. NetIQ Authenticore Server is not installed.
   b. NetIQ Authenticore Server is not configured correctly.
   c. NetIQ Authenticore Server is protected by firewall.

Solution:

   a. Installation of NetIQ Authenticore Server is required.
   b. NetIQ Authenticore Server should be configured correctly.
   c. Firewall should be disabled for correct work of NetIQ Authenticore Server.

NetIQ Access Manager Is Not Available

Description:

There is no access to NetIQ Access Manager. The following window is displayed:

Cause:

   a. There is no Internet access.
    b. NetIQ Access Manager is disabled.

Solution:

    a. Check the Internet access.
    b. Check whether NetIQ Access Manager is enabled.

Incorrect Password/Username of Active Directory Domain Administrator Was Set In NetIQ Access Manager

Description:

Password/username of Active Directory Domain Administrator is not acceptable. The following window is displayed:
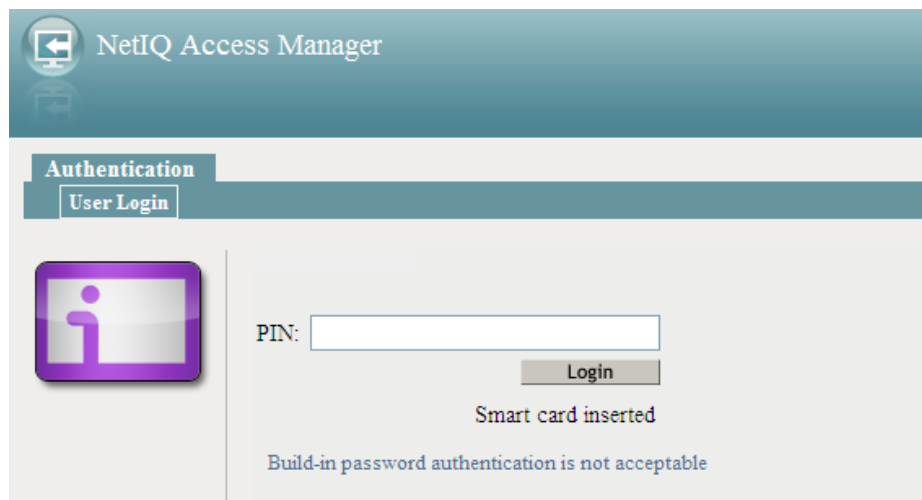
Cause:

    a. Incorrect settings of the IDP-cluster.
    b. Incorrect username and/or password.

Solution:

    a. Check the settings of the IDP-cluster.
    b. Enter correct username and/or password.

Active Directory Is Not Set In NetIQ Access Manager as a Default Type of Storage

Description:

Active Directory Domain Administrator is not used as a default type of storage in NetIQ Access Manager.

Cause:

a. Incorrect settings of the IDP-cluster;
b. Incorrect username and/or password of Active Directory Domain Administrator.

Solution:

a. Check the settings of the IDP-cluster.
b. Enter correct username and/or password of Active Directory Domain Administrator.

Server Replicas Are Not Configured or Wrong Configured

Description:

There is a warning in the Health field and the error is the Validation Status field is displayed:

Server replicas						
New | Delete | Validate						1 Item(s)
Name	IP Address	Port	Use SSL	Max. Connections	Validation Status	
DC	10.0.103.252	389		20	[LDAP: error code 80 - 80090304: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 20ee, v1db1]	

Cause:

Server Replicas are not configured or wrong configured.

Solution:

Configure correctly the Server Replicas menu.

Search Contexts Are Not Configured or Wrong Configured

Description:

There is a warning in the Health field which notifies of an error:

Cause:

Search Contexts are not configured or wrong configured.

Solution:

Configure correctly the Search Contexts menu.

Cannot Enroll Authenticator

Description:

Authenticator is not enrolled because:

a. The **Type** list in the **Enroll Authenticators** window is empty or OATH authenticator type is absent.
b. The **Enroll** button in the **Authenticators** window is greyed out.

Cause:

a. The OATH authenticator type is not supported (no proper authentication provider is installed).
b. The operation is forbidden or you have reached the limit on authenticators number.

Solution:

a. Contact NetIQ administrator.
b. No authenticators can be added. For more information, contact NetIQ administrator.

One-Time Password Doesn't Work

Description:

The generated one-time password doesn't work.

Cause:

a. Group policy is set on the other password generating period.
b. The password time is out.
c. Workstation time differs from time of Authenticore Server more than N minutes; N depends on **TOTP checking window** setting.

Solution:

a. Check group policy settings and make changes in your Mobile device token application.
b. Try another password.
c. Synchronize Workstation and Server time.

Index