
Installation Guide

Access Manager - Advanced Authentication Plug-in

Version 5.3

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 Environment	9
2 Access Manager Advanced Authentication Plug-in Installation	11
2.1 Automatic Mode	11
2.2 Manual Mode	12
2.3 NAM Advanced Authentication Plug-in Configurator Tool	12
2.4 NAM Advanced Authentication Plug-in Removal	13
3 Advanced Authentication Support Configuration	15
3.1 Dynamic Configuration	15
3.2 Email Method Support Configuration	17
3.3 Emergency Password Method Support Configuration	18
3.4 FIDO U2F Method Support Configuration	19
3.5 HOTP Method Support Configuration	20
3.6 Password (PIN) Method Support Configuration	21
3.7 RADIUS Method Support Configuration	22
3.8 Security Questions Method Support Configuration	23
3.9 Smartcard Method Support Configuration	24
3.10 Smartphone Method Support Configuration	25
3.11 SMS Method Support Configuration	26
3.12 TOTP Method Support Configuration	27
3.13 Voice Call Method Support Configuration	28
3.14 Optional Properties	29
4 Logging In To Advanced Authentication Access Manager	31
5 Troubleshooting	33
5.1 Debug Logging	33
5.2 An error "Incompatible installation detected" occurs during the NAM AA plug-in upgrade	33

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

The Installation Guide has been designed for all users and describes how to install Access Manager Advanced Authentication plug-in and the system requirements that must be fulfilled before the installation.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

1 Environment

Components that are required for installation:

- ♦ NetIQ Access Manager 4.2
- ♦ Advanced Authentication Server 5

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

2 Access Manager Advanced Authentication Plug-in Installation

IMPORTANT: Root permissions on Advanced Authentication Access Manager are required for the installation of Access Manager Advanced Authentication plug-in.

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

Access Manager Advanced Authentication plug-in can be installed in 2 modes:

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

To uninstall the NAM Advanced Authentication plug-in, refer to [NAM Advanced Authentication Plug-in Removal](#).

2.1 Automatic Mode

To install Access Manager Advanced Authentication plug-in in the automatic mode:

1. Extract the contents of `NAMPlugin_*.zip` package and copy `NetIQNAMAAPPluginSetup.jar` to /tmp directory of the IDP NAM instance.
2. Switch to the `/opt/novell/java/jre/bin/` directory.
3. Run `NetIQNAMAAPPluginSetup.jar`. E.g., `java -jar /tmp/NetIQNAMAAPPluginSetup.jar`.
4. Follow the steps required for Access Manager Advanced Authentication plug-in 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.
5. Follow the steps required to configure connection to Advanced Authentication server:
 - ♦ The text "NAAF appliance IP address: [localhost]" is displayed, specify 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.

IMPORTANT: Advanced Authentication server uses HTTPS protocol by default.

2.2 Manual Mode

To install Access Manager Advanced Authentication plug-in 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/edorsed`
 - ♦ **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 [NAM Advanced Authentication Plug-in Configurator Tool](#) to configure the connection to Advanced Authentication Server.

2.3 NAM Advanced Authentication Plug-in Configurator Tool

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

Before performing the action you need to switch to the `/opt/novell/java/jre/bin/` directory.

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 plug-in to use the Advanced Authentication server with IP address 192.168.56.223 by HTTPS.

2.4 NAM Advanced Authentication Plug-in Removal

To uninstall the Advanced Authentication Access Manager Advanced Authentication plug-in, perform the following steps:

- ♦ For Linux operating system:
 1. Copy the `uninstall.sh` file from <NAM Advanced Authentication plug-in distributive>/uninstaller to the target system.
 2. Run `uninstall.sh <installation_path>` (the default path is `/opt/novell`) to remove the plug-in.
- ♦ For Microsoft Windows operating system:
 1. Copy the `uninstall.bat` file from <NAM Advanced Authentication plug-in distributive>\uninstaller to the target system.
 2. Run `uninstall.bat "<installation_path>"` to remove the plug-in.

3 Advanced Authentication Support Configuration

IMPORTANT: It is required to enable the NAM event and specify all applicable chains in its settings in Advanced Authentication Admin Interface.

In this chapter:

- ♦ [Dynamic Configuration](#)
- ♦ [Email Method Support Configuration](#)
- ♦ [Emergency Password Method Support Configuration](#)
- ♦ [FIDO U2F Method Support Configuration](#)
- ♦ [HOTP Method Support Configuration](#)
- ♦ [Password \(PIN\) Method Support Configuration](#)
- ♦ [RADIUS Method Support Configuration](#)
- ♦ [Security Questions Method Support Configuration](#)
- ♦ [Smartcard Method Support Configuration](#)
- ♦ [Smartphone Method Support Configuration](#)
- ♦ [SMS Method Support Configuration](#)
- ♦ [TOTP Method Support Configuration](#)
- ♦ [Voice Call Method Support Configuration](#)

3.1 Dynamic Configuration

IMPORTANT: The functionality is supported from NAM Advanced Authentication plug-in v2.0.121.

The dynamic configuration is a universal configuration which is required to be configured on NAM. It reads the configured chains for the NAM event from the Advanced Authentication Server. After the authentication done with a password in NAM, a user receives a list of chains which can be used for further authentication.

NOTE: If you have configured few chains which contain one method, put the more secure chains to the top of NAM event. E.g. if you have two chains added: TOTP (single) and LDAP Password+TOTP, put the LDAP Password+TOTP higher than TOTP in the list of used chains of NAM event. This is important to filter the less secure chains. In this case only LDAP Password+TOTP will be available in the list, because the Advanced Authentication filters and ignores the less secure chains.

To change the chains, you are not required to change any settings in NAM. You need to update the chains list for the NAM event in the Advanced Authentication - Administrative Portal.

NOTE: The following methods are supported in the Dynamic configuration only (there are no separate classes for them):

- ♦ Fingerprint
- ♦ PKI

For both the methods, you must install Advanced Authentication Device Service.

To configure the dynamic configuration perform the following steps:

1. Create a new authentication class with the following parameters:
 - a. **Display name:** Dynamic Class
 - b. **Java class:** Other
 - c. **Java class path:** com.athasas.aucore.nam.method.dynamic.DynamicAuthenticationClass
2. Create a new authentication method for the class:
 - a. **Display Name:** Dynamic Method
 - b. **Class:** Dynamic Class
 - c. Keep the **Overwrite Temporary User** and **Overwrite Real User** check boxes cleared.
 - d. Add the used user store to **User Stores**.
3. Add applicable **optional properties** (KEY/Value).
4. Add the following properties (KEY/Value).
 - ♦ **EVENTNAME:** A name of the event used, by default the event name is NAM.
 - ♦ **SKIPCHAINS** (any value). If property is presented the plug-in will skip the authentication chain selection and will always use a top chain from the list.
5. Create a new authentication contract for the method in the **Configuration** tab:
 - a. **Display name:** Dynamic Contract
 - b. **URI:** dynamic/uri
 - c. Configure **Methods**. Select one of the following options:
 - ♦ Add only Dynamic Method from the **Available Methods** list. In this case, you must select the **Identifies User** check box. Dynamic Method provides a request of an LDAP Password. After the user enters the password, the user will be asked to provide next method.
 - ♦ Add any standard method from the **Available Methods** list as the first one and Dynamic Method as the second one. In this case, you must clear the **Identifies User** check box for Dynamic Method.
 - d. Clear the **Satisfiable by External Provider** check box.
6. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** DYNAMIC_ID
 - b. **Text:** NetIQ Authentication
 - c. **Image:** <Select Local Image>, then select `NAM_Dynamic.png` from the **icons** folder of the NAM plug-in distribution kit.
7. Update both the IDP and the MAG.
8. Update NAM Server configuration.

3.2 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** check boxes 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** check box 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** check box should be obligatory cleared for EMail Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.3 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** check boxes 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** check box 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** check box should be obligatory cleared for Emergency Password Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication 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 plug-in:

- ♦ Name/Password - Form
- ♦ Name/Password - Basic

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

3.4 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** check boxes 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** check box 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** check box should be obligatory cleared for U2F Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: FIDO U2F is available starting from NAM AA plug-in v2.0.76.

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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

- ♦ 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 Advanced Authentication Access Manager and enroll site in one domain. For more information, see [Configuring a Web Server in order to use the FIDO U2F authentication in Advanced Authentication Access Manager](#) in the **Server Administrator Guide**.

3.5 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** check boxes 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** check box 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** check box should be obligatory cleared for HOTP Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal 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 plug-in:

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

3.6 Password (PIN) Method Support Configuration

1. Create a new authentication class with the following parameters:
 - a. **Display name:** Password (PIN) 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 (PIN) Method
 - b. **Class:** Password (PIN) Class
 - c. Keep the **Overwrite Temporary User** and **Overwrite Real User** check boxes 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 (PIN) Contract
 - b. **URI:** passwordandldap/uri
 - c. Configure **Methods**. Select one of the following options:
 - ♦ Add only Password (PIN) Method from the **Available Methods** list. In this case the **Identifies User** check box must be selected. Password (PIN) Method will provide a request of LDAP Password. After user enters it, he/she will be asked to enter the Password (PIN).
 - ♦ Add any standard method from the **Available Methods** list as the first one and Password (PIN) Method as the second one. In this case the **Identifies User** check box should be obligatory cleared for Password (PIN) Method.
 - d. Keep the **Satisfiable by External Provider** check box cleared.
5. Specify applicable values for the new authentication card in the **Authentication Card** tab:
 - a. **ID:** Password_ID
 - b. **Text:** NetIQ Password (PIN) Authentication
 - c. **Image :** <Select Local Image>, then select **NAM_Password.png** from the **icons** folder of the NAM plug-in distribution kit.

6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: If Password (PIN) contract is configured to use only Password (PIN) method, it will be required to configure both **LDAP Password & Password (PIN)** (two-factor) and **Password (PIN)** (one-factor) chains in the **Chains** section (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. If Password (PIN) contract is configured to use combination of a standard method and Password (PIN) method, it will be required to configure and enable only **Password (PIN)** (one-factor) chain.

The following standard methods are supported by NAM plug-in:

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

3.7 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.athasas.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** check boxes 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** check box 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** check box should be obligatory cleared for RADIUS Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.8 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
 - c. Keep the **Overwrite Temporary User** and **Overwrite Real User** check boxes 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**: 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** check box 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** check box should be obligatory cleared for SecurityQuestion Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.9 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
 - c. Keep the **Overwrite Temporary User** and **Overwrite Real User** check boxes 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**: 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** check box 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** check box should be obligatory cleared for Smartcard Method.
- d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 **Chains** section (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.10 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.athasas.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** check boxes 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** check box 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** check box should be obligatory cleared for Smartphone Method.
- d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.11 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.athasas.aucore.nam.method.sms.SMSSClass
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** check boxes 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** check box 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** check box should be obligatory cleared for SMS Method.
- d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.12 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** check boxes 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** check box 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 Advanced Authentication 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** check box should be obligatory cleared for TOTP Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.13 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
 - c. Keep the **Overwrite Temporary User** and **Overwrite Real User** check boxes 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**: 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** check box 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** check box should be obligatory cleared for Voice call Method.
 - d. Keep the **Satisfiable by External Provider** check box 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 plug-in distribution kit.
6. Update both the IDP and the MAG.
7. Update NAM Server configuration.

IMPORTANT: 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 (the two-factor chain must be higher than an appropriate one-factor chain) and enable them in the NAM event of the Advanced Authentication Administrative Portal. 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 plug-in:

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

3.14 Optional Properties

Access Manager Advanced Authentication plug-in supports the following optional properties (KEY/Value) for authentication methods:

- ♦ **REPONAME**: the name of the repository that is used for Advanced Authentication. This parameter may not be used if default repo is already selected in the **Login options** policy of Advanced Authentication 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 plug-in 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).
- ♦ **LDAPSYNCHJSP**: 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).
- ♦ **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 Advanced Authentication Self-Service Portal. The default value is https://<NetIQAdvancedAuthenticationFramework_server_address>:<server_port>/account.

IMPORTANT: Parameters **ERRORJSP**, **LDAPJSP**, **METHODJSP**, **LDAPSYNCHJSP** and **ENROLLURL** are available starting from Advanced Authentication v5.2, NAM AA plug-in v2.0.76.

4 Logging In To Advanced Authentication Access Manager

To log in to Advanced Authentication Access Manager with Password + Advanced Authentication 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
 - ♦ **reponamelusername** - in other case
3. Enter password and click **Login**.
4. Authenticate with Advanced Authentication method.
5. The session will be successfully authenticated.

To log in to Advanced Authentication Access Manager with Advanced 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 Advanced Authentication method.
4. The session will be successfully authenticated.

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

1. Go to Advanced Authentication 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.
-

5 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 the NAM AA plug-in upgrade](#).

5.1 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 plug-in 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 plug-in 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`)

5.2 An error "Incompatible installation detected" occurs during the NAM AA plug-in upgrade

Description:

While trying to upgrade Access Manager Advanced Authentication plug-in, 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 Access Manager Advanced Authentication plug-in and install a new one?

Solution:

To install a new version of Access Manager Advanced Authentication plug-in, remove the following files manually:

- ♦ `/opt/novell/Uninstaller/uninstaller.jar` ?
- ♦ `/opt/novell/.installationinformation`

Run the installer once again.

