Administrator Guide

NetIQ Advanced Authentication Framework Server

Version 5.2.0

MICRO FOCUS

Legal Notice

1 Introduction

1.1 About This Document

Purpose of the Document

This Deployment Guide is intended for system administrators and describes the procedure of NetIQ Advanced Authentication Framework Server appliance deployment.

Document Conventions

- 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.

2 NetIQ Advanced Authentication Framework Overview

In this chapter:

2.1 About NetIQ Advanced Authentication Framework

NetIQ Advanced Authentication Framework™ is a software solution that enhances the standard user authentication process by providing an opportunity to logon with various types of authenticators.

Why choose NetIQ Advanced Authentication Framework™?

NetIQ Advanced Authentication Framework™...

- ...makes the authentication process easy and secure (no complex passwords, “secret words”, etc.)
- ...prevents unauthorized use of your computer
- ...protects you from fraud, phishing and similar illegal actions online
- ...can be used to provide secure access to your office

2.2 NetIQ Server Appliance Functionality

Benefits of using NetIQ Server appliance are evident. NetIQ Server appliance...

- ...is cross-platform
- ...contains an inbuilt RADIUS server
- ...supports integration with NetIQ Access Manager
- ...does not require scheme extending
- ...provides administrators with a capability of editing the configured settings through web-based NetIQ Admistrative Portal

2.3 Architecture

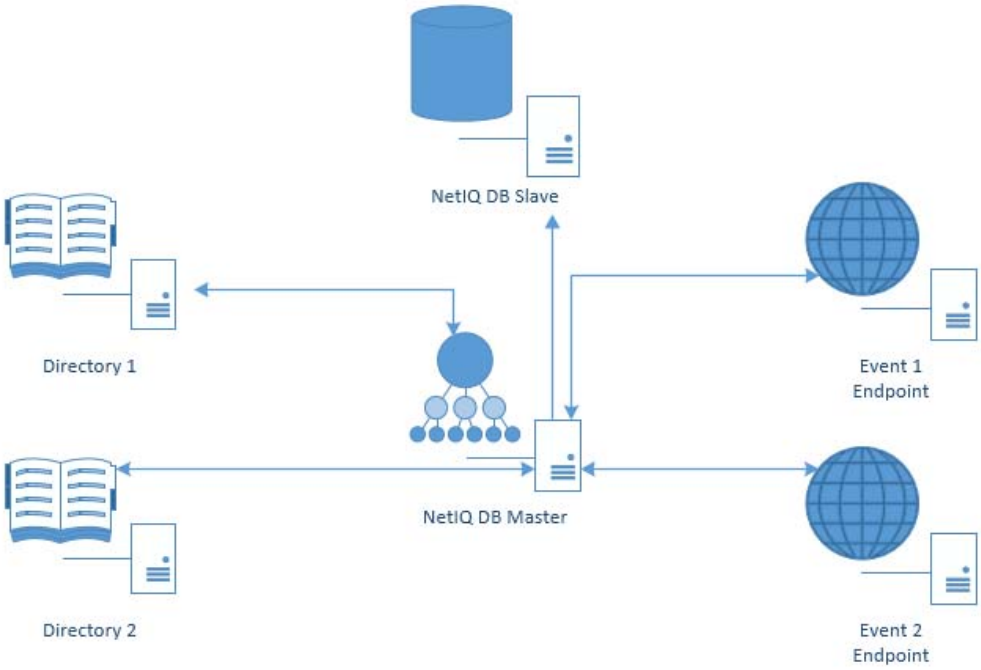
In this chapter:

2.3.1 Basic Architecture

This diagram shows the basic architecture with NetIQ Advanced Authentication Framework v5. NetIQ DB Master contains an inbuilt RADIUS Server that can authenticate any RADIUS client using one of chains configured for the event. Basic architecture is recommended only for testing purposes or proof of concept.

2.3.2 Enterprise Architecture

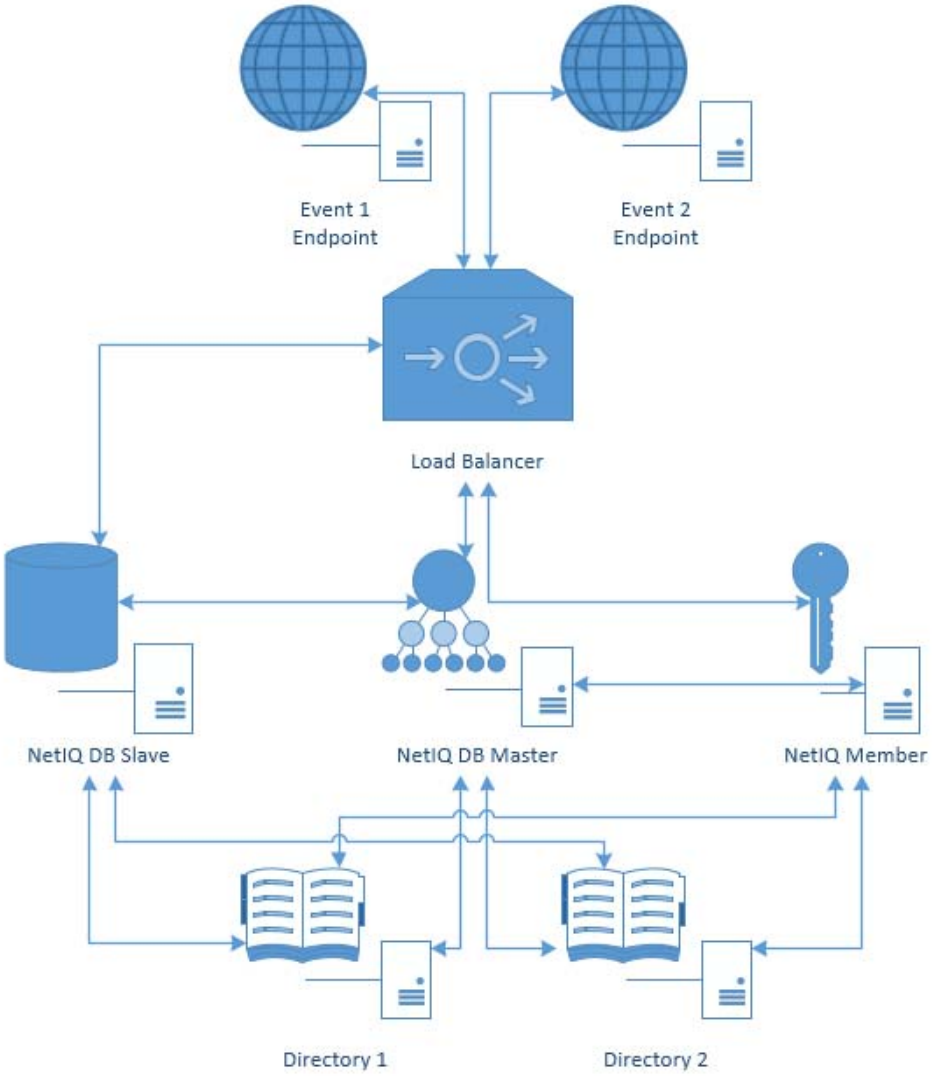
The following diagram shows interaction between DB Master, several directories and events. DB Master interacts at the same time with DB Slave, which contains the copy of the DB Master database. If DB Master dies, DB Slave will take over (hot slave).



2.3.3 Enterprise Architecture with Load Balancer

NOTE: For more information on how to configure Load Balancer, check the How to configure load balancer for NetIQ Advanced Authentication cluster.

The following diagram shows interaction between the components of enterprise architecture and server with Load Balancer. Load Balancer may call DB Master or Member servers. Please note that Member server is a server that does not have its own database. Its data is stored on DB Master.



2.4 Terms

In this chapter:

- Authentication Method
- Authentication Chain
- Authentication Event

2.4.1 Authentication Method

Authentication Method verifies the identity of someone who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions.

2.4.2 Authentication Chain

Authentication Chain is a combination of authentication methods. User needs to pass all methods in order to be successfully authenticated. E.g., if you create a chain which has LDAP Password and SMS in it, the user will first need to enter his/her LDAP Password. If the password is correct, the system will send SMS with an One-Time-Password to the mobile of the user. The user needs to enter the correct OTP in order to be authenticated.

It is possible to create any chain. So for high secure environments it is possible to assign multiple methods to one chain to achieve better security.

Authentication can consist of 3 different factors. These are:

- Something you know: password, PIN, security questions
- Something you have: smartcard, token, telephone
- Something you are: biometrics like fingerprint or iris

Multi-Factor or Strong Authentication is when 2 out of the 3 factors are used. A password with a token, or a smartcard with a fingerprint are considered to be multi-factor authentication. A password and a PIN is not consideed to be multi-factor as they are in the same area.

Authentication chains are linked to user groups in your repositories. So only a certain group can be allowed to use the specific authentication chain.

2.4.3 Authentication Event

Authentication Event is triggered by an external device or application which needs to perform authentication. It can be triggered by a RADIUS Client (Citrix Netscaler, Cisco VPN, Juniper VPN, etc) or API request. Each event can be configured with one or more authentication chains which will provide user with a capability to authenticate.

Within the NetIQ framework, an authentication event is configured in the Events section. It is possible to enable or disable an event, and to add method-chains to the event. With specific events it is possible to assign clients to the event.

3 System Requirements

IMPORTANT: NetIQ Advanced Authentication Framework (NAAF) is a self-contained Linux based Appliance. The appliance is installed from a single ISO and can be installed on bare metal hardware or on the hypervisor of your choice (VMware, Hyper-V, etc).

Before installing the product, check that the following system requirements are fulfilled:

Minimum hardware requirements for each appliance:

- 40 GB disk space
- 2 Cores CPU
- 2 GB RAM

Recommended hardware requirements for each appliance:

- 60 GB disk space
- 4 Cores CPU
- 4 GB RAM

Supported browsers for NetIQ Advanced Authentication Framework Administrative Portal, Self Service Portal and Helpdesk Portal:

- Microsoft Internet Explorer 10, 11.
- Microsoft Edge 20.0 and later.
- Google Chrome 40.0 and later.
- Mozilla Firefox 36.0 and later.
- Apple Safari 8 and later.

Check system requirements for client components and plugins in related documentation.

4 NetIQ Server Appliance Deployment

NetIQ Server Appliance is intended for processing requests for authentication coming from the NetIQ Advanced Authentication Framework system users.

In this chapter:

4.1 Installing NetIQ Server Appliance

Perform NetIQ Server appliance installation using one of the following modes:

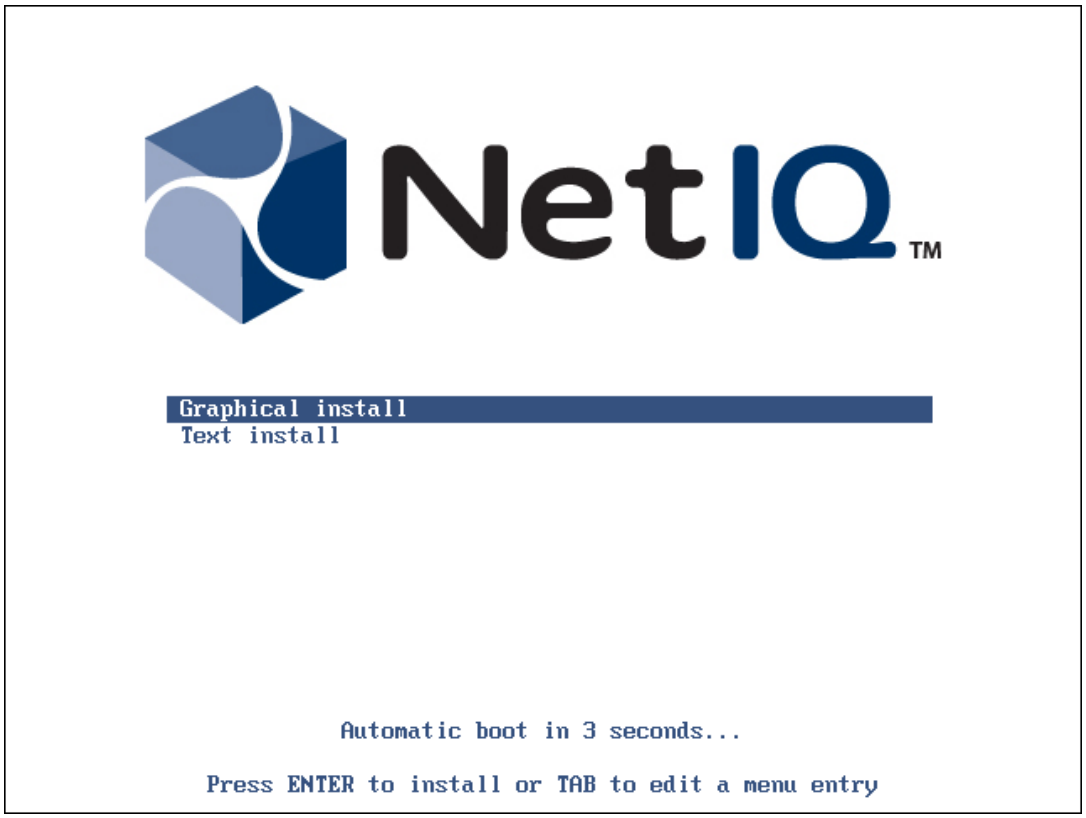
4.1.1 Graphic Mode

IMPORTANT: The *Graphical install* menu entry will be selected automatically within several seconds after the launch of the Setup Wizard.

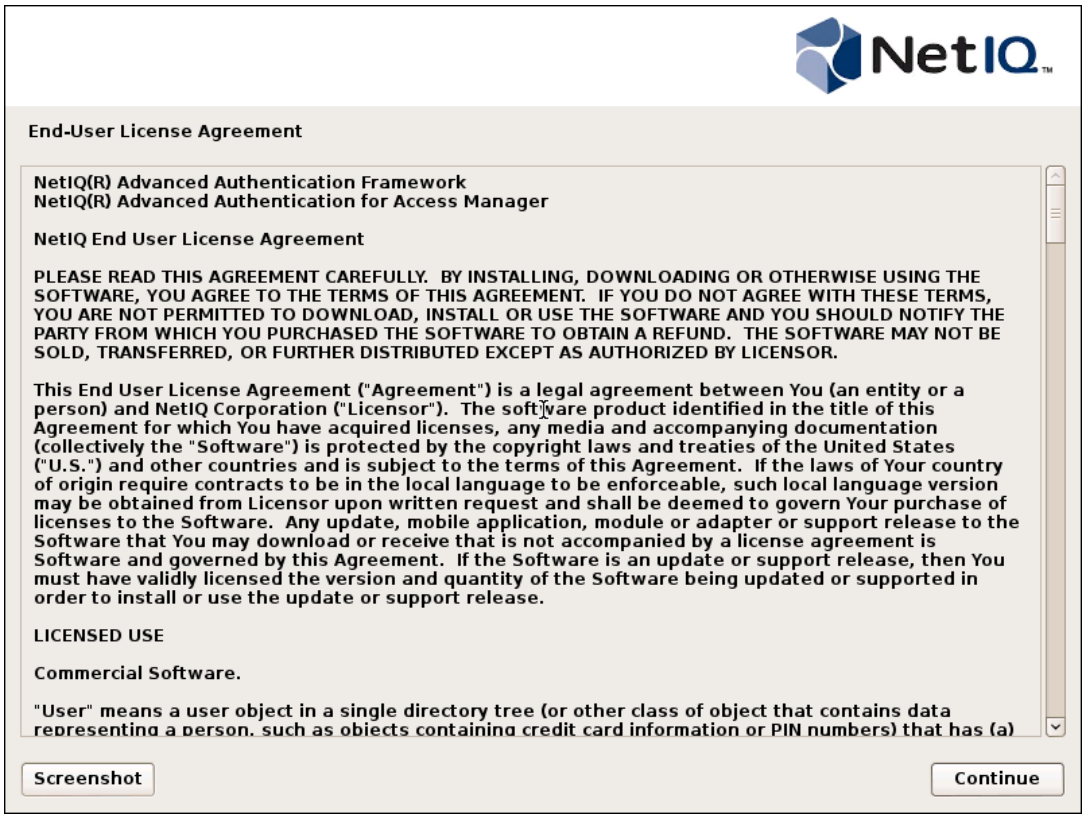
NOTE: To cancel the installation, click the *Cancel* button. The button is available only for certain processes of installation.

To install NetIQ Server appliance in the graphic mode:

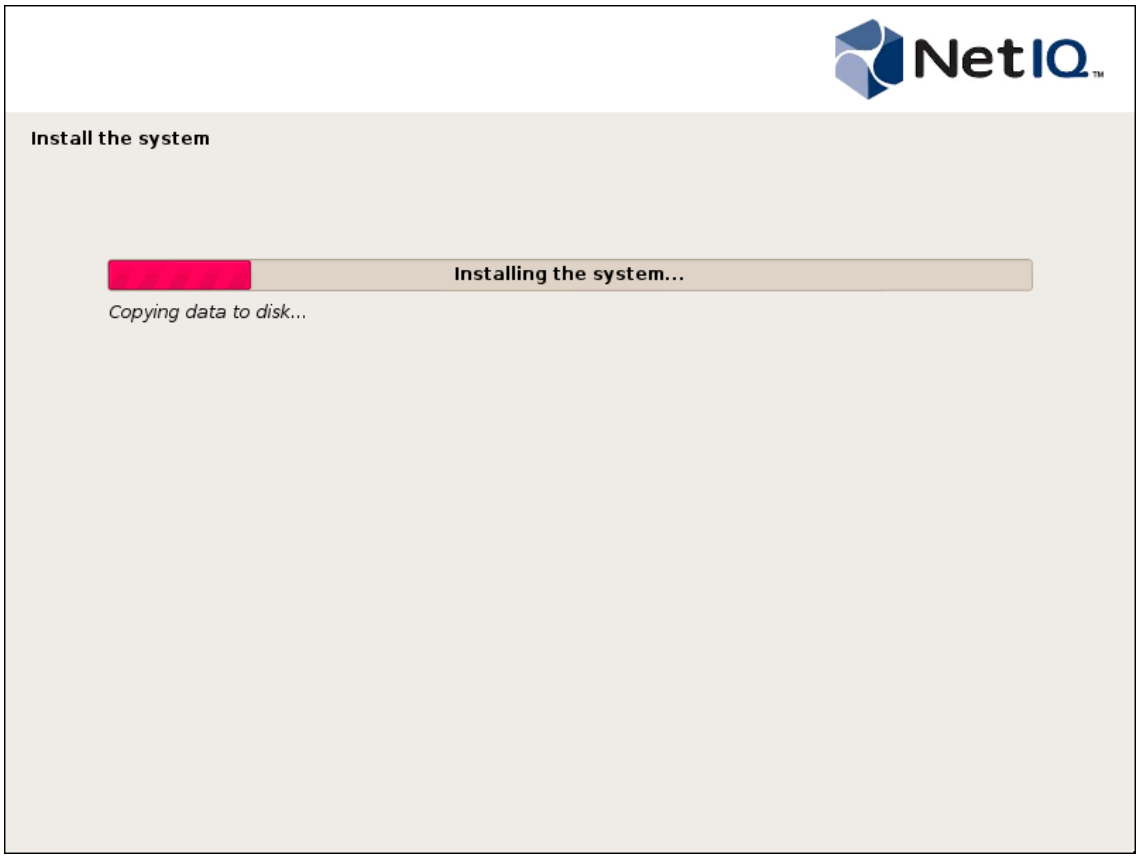
1. Select the *Graphical install* menu entry in the Setup Wizard and press *ENTER*.



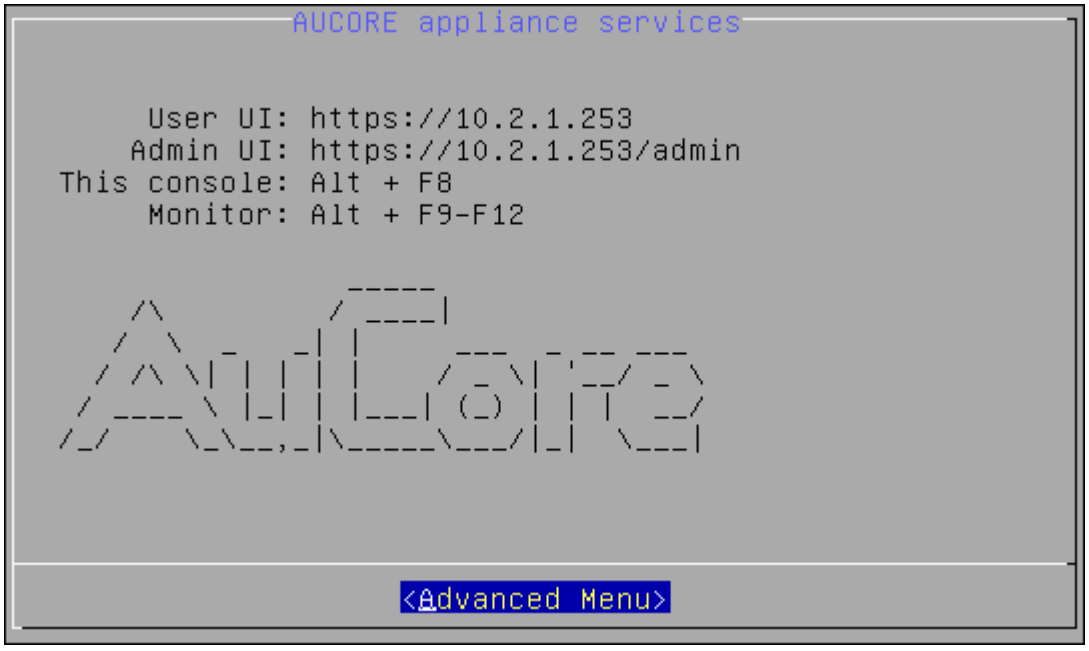
2. Read the license agreement. Select *I agree* at the bottom and click *Continue*.



3. The installation will be automatically started.



4. Wait until the system reboots. The *Configuration Console* will be started.

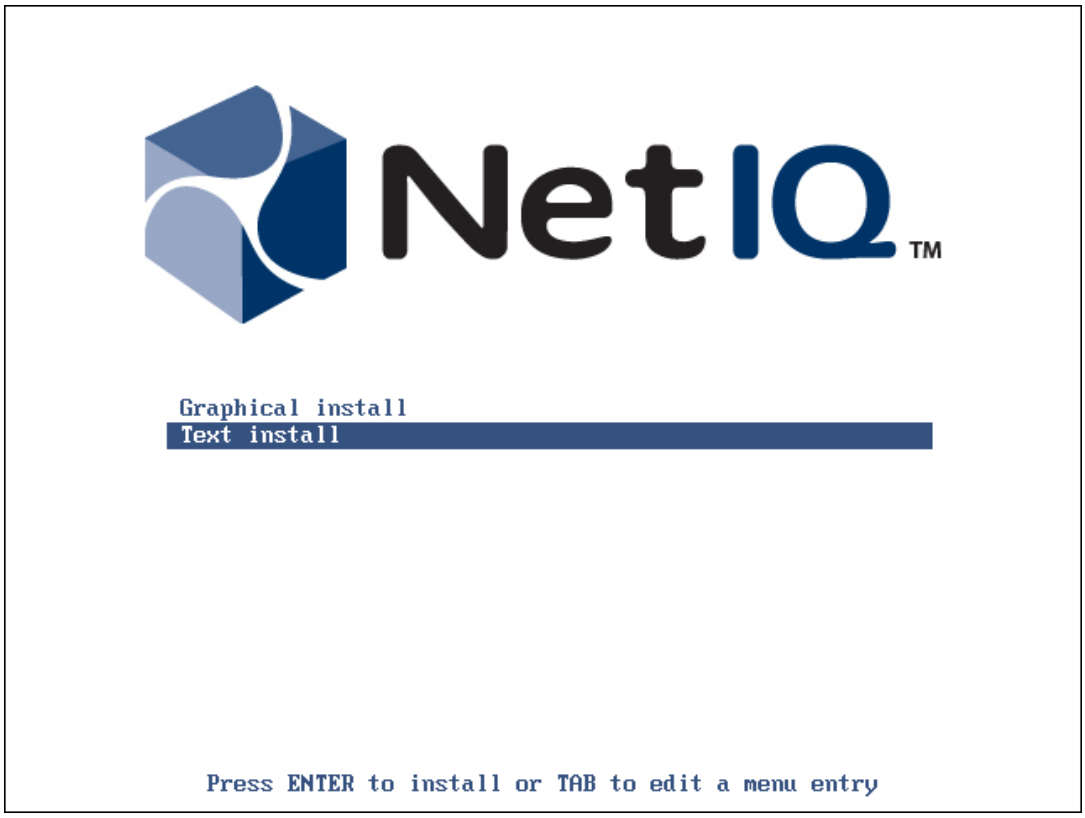


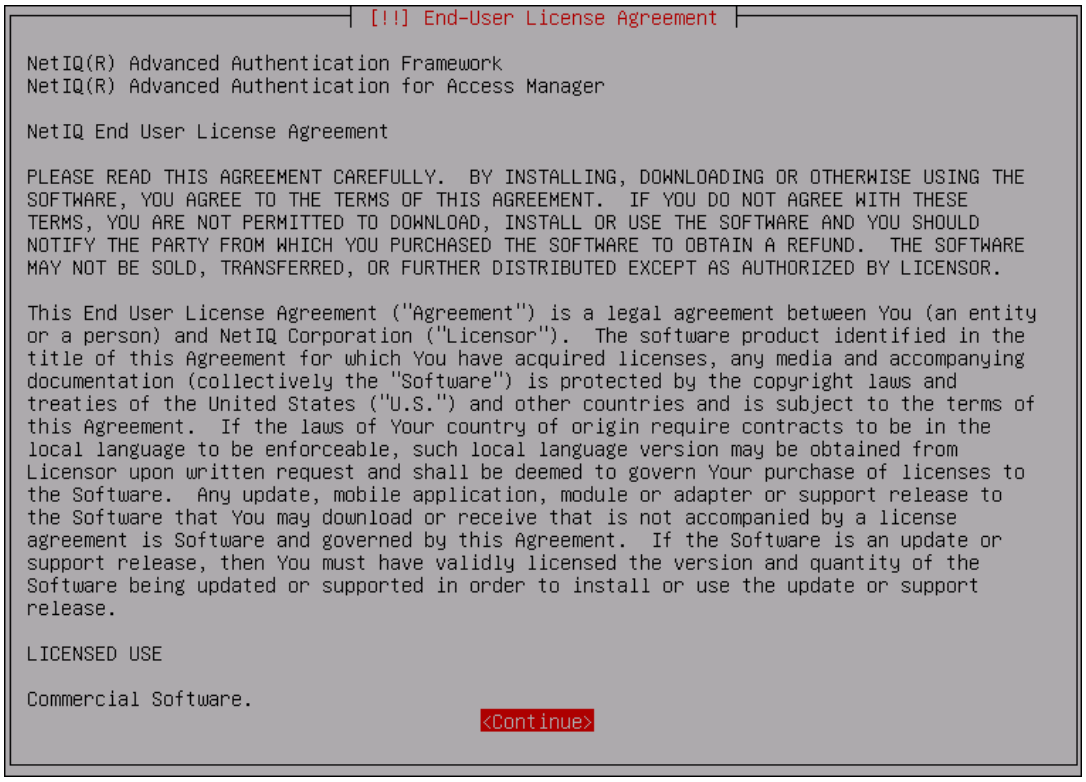
4.1.2 Text Mode

IMPORTANT: It is required to select the *Text install* menu entry within several seconds after the launch of the Setup Wizard. Otherwise the *Graphical install* menu entry will be selected automatically and NetIQ Server appliance will be installed in the graphic mode.

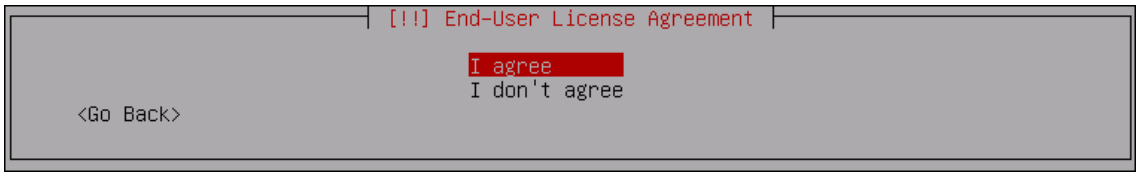
To install NetIQ Server appliance in the text mode:

1. Select the *Text install* menu entry in the Setup Wizard and press *ENTER*.

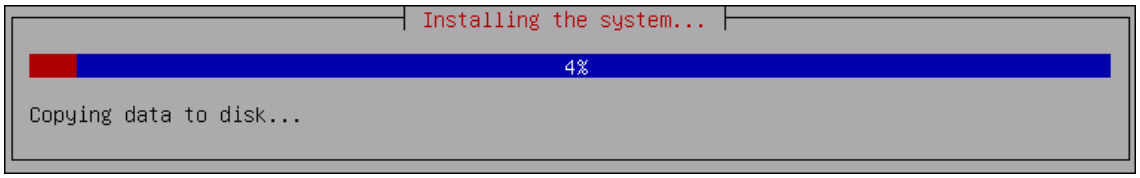




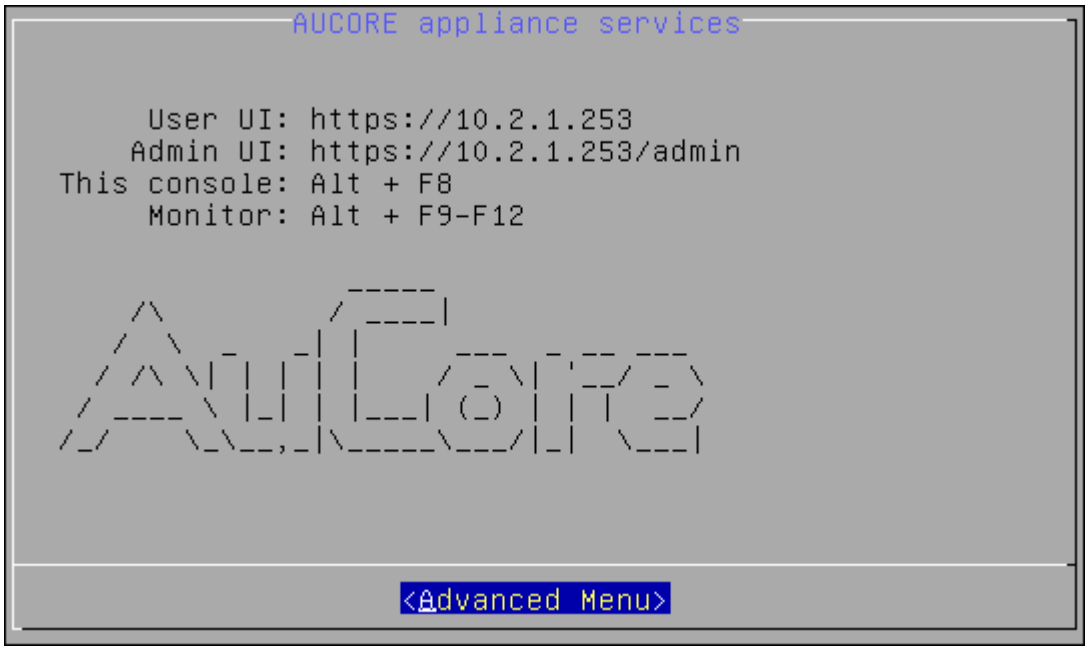
2. Select *I agree* to continue installation.



3. The installation will be automatically started.



4. Wait until the system reboots. The *Configuration Console* will be started.

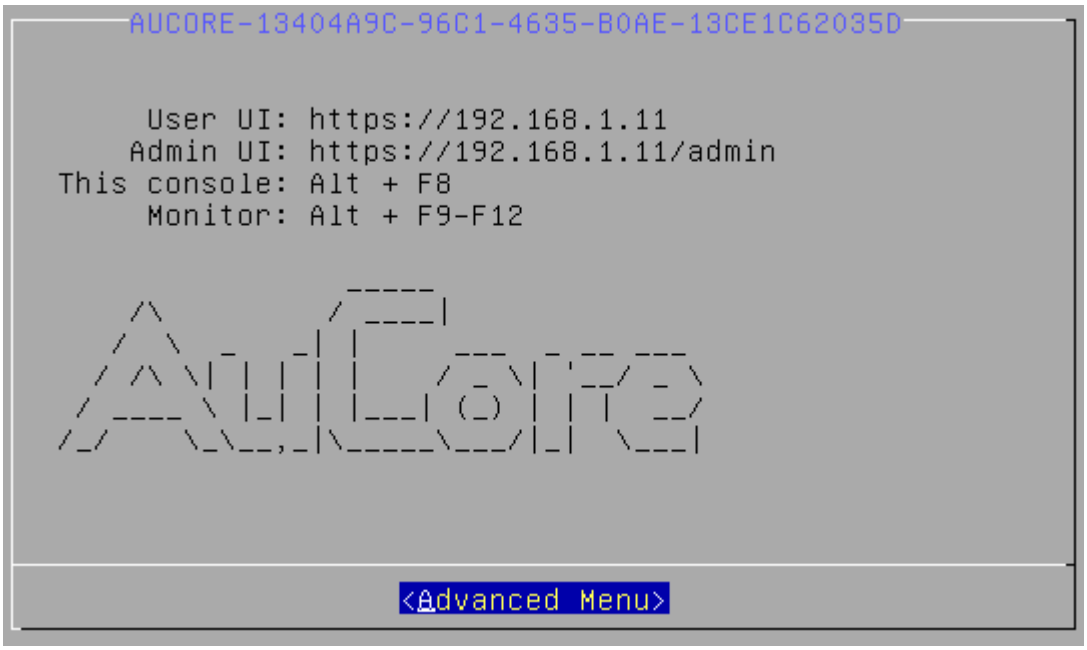


4.2 Configuration Console

The *Configuration Console* is intended for managing NetIQ Server appliance, namely:

- Configuring Host Name
- Configuring Appliance Networking
- Configuring Time and NTP Servers
- Rebooting Appliance
- Shutting Down Appliance

The *Configuration Console* is launched after NetIQ Server appliance installation. It contains Admin UI and User UI addresses.

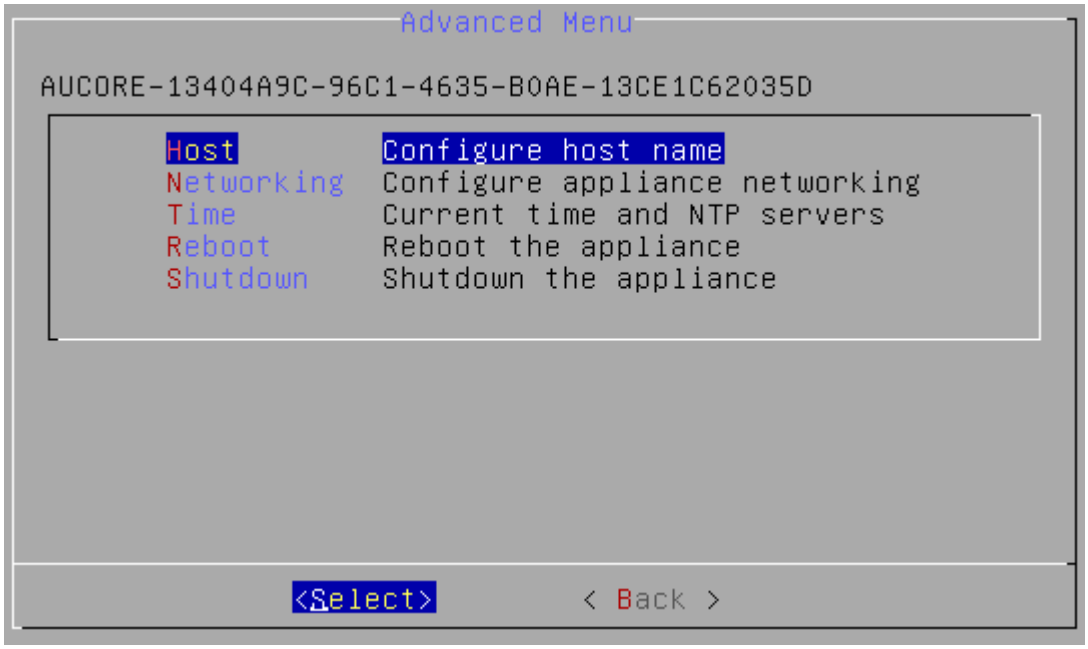


To proceed to NetIQ Server appliance management, select *Advanced Menu*.

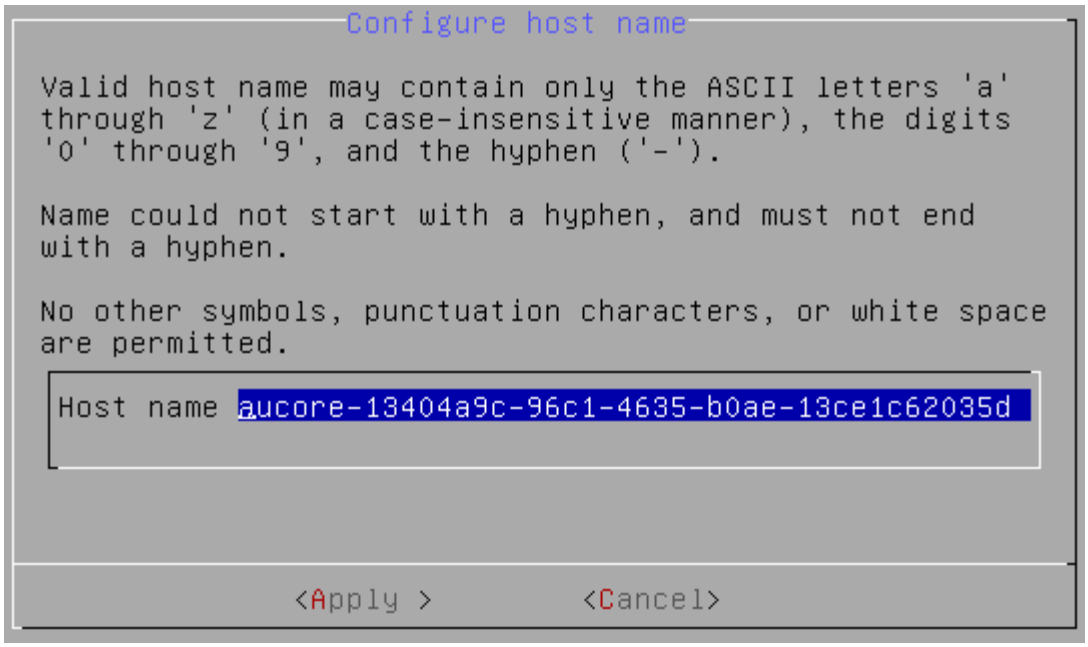
4.2.1 Configuring Host Name

To configure NetIQ Server appliance host name via Configuration Console, follow the steps:

1. Go to the *Advanced Menu* of the *Configuration Console*.
2. Select *Host*.



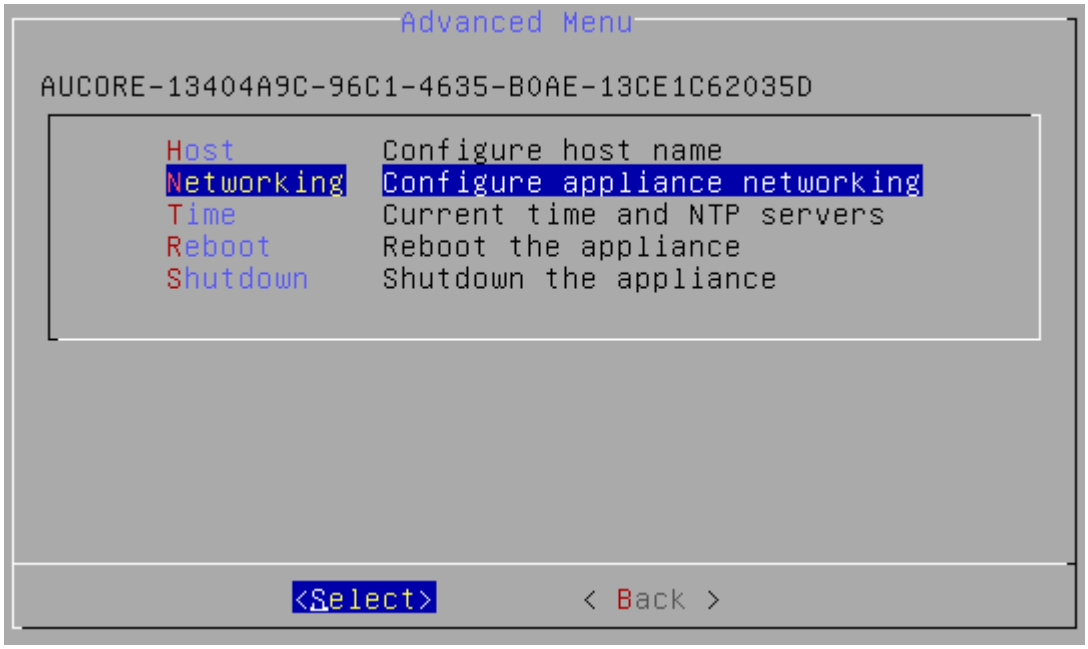
3. Specify an applicable host name and press *ENTER* to apply changes.



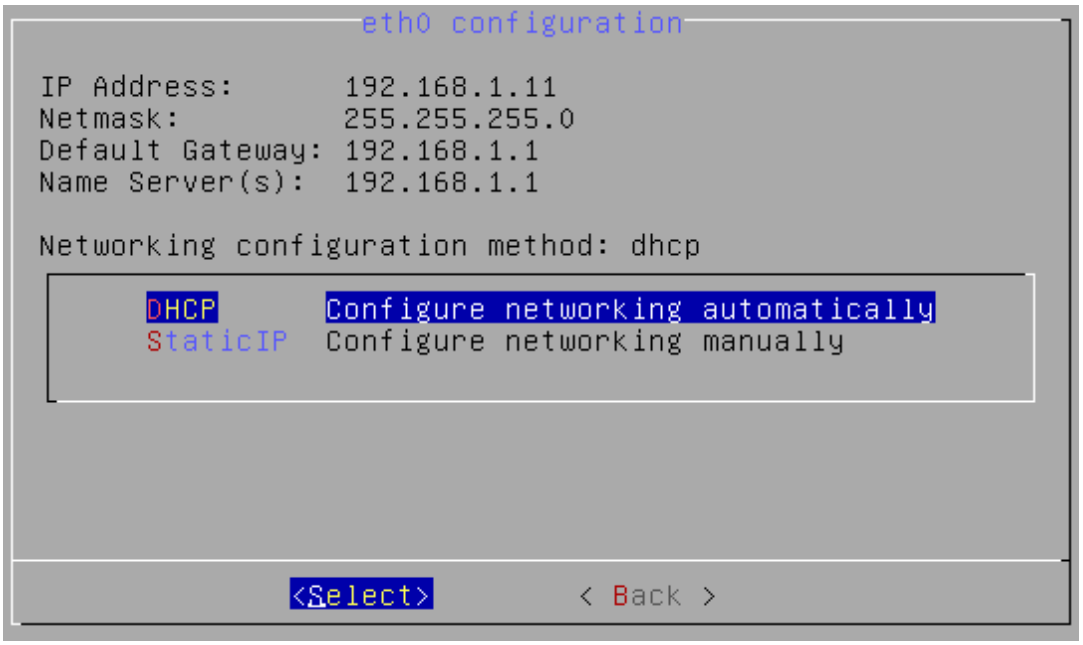
4.2.2 Configuring Appliance Networking

To configure NetIQ Server appliance networking via Configuration Console, follow the steps:

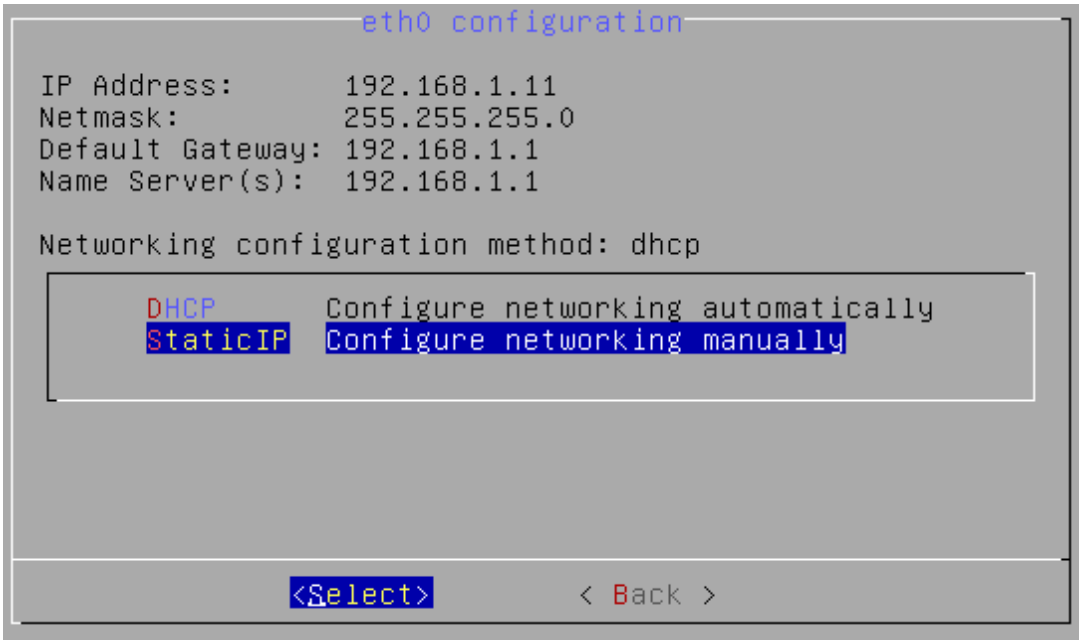
1. Go to the *Advanced Menu* of the *Configuration Console*.
2. Select *Networking*.



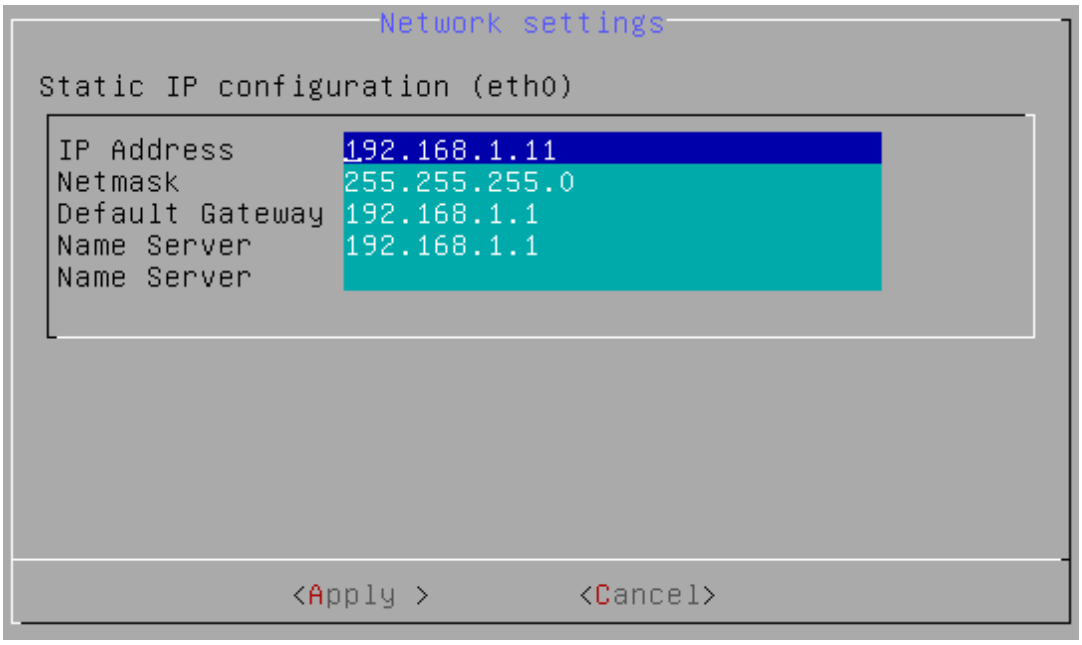
3. Select an applicable networking configuration method:
   - *DHCP* - to configure networking automatically.



- *StaticIP* - to configure networking manually.



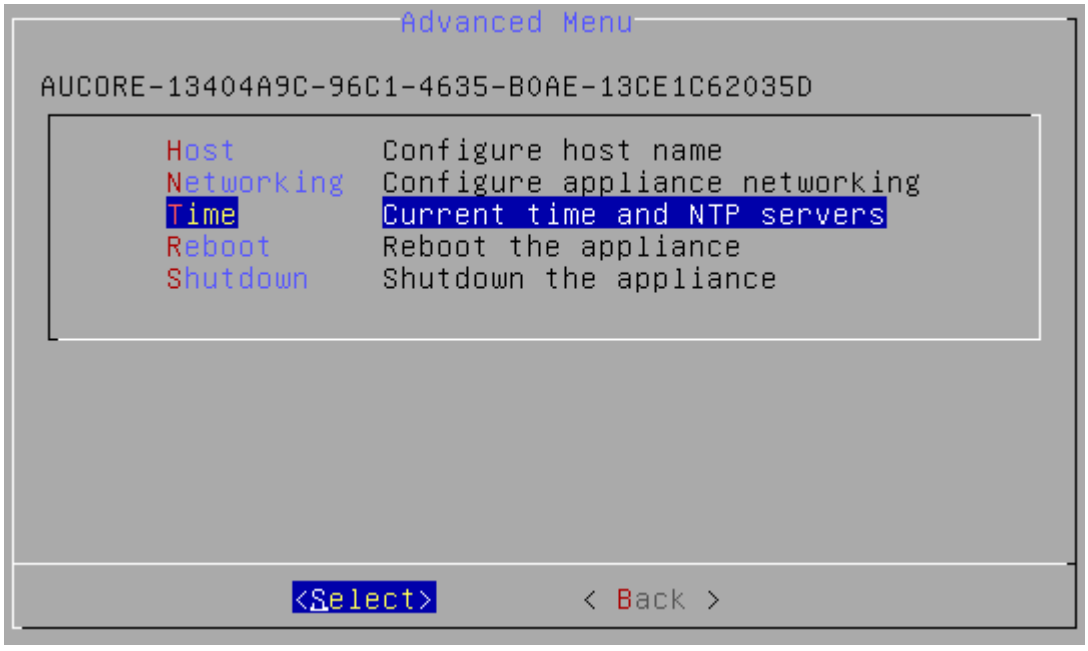
Specify all required parameters manually and press *ENTER* to apply changes.



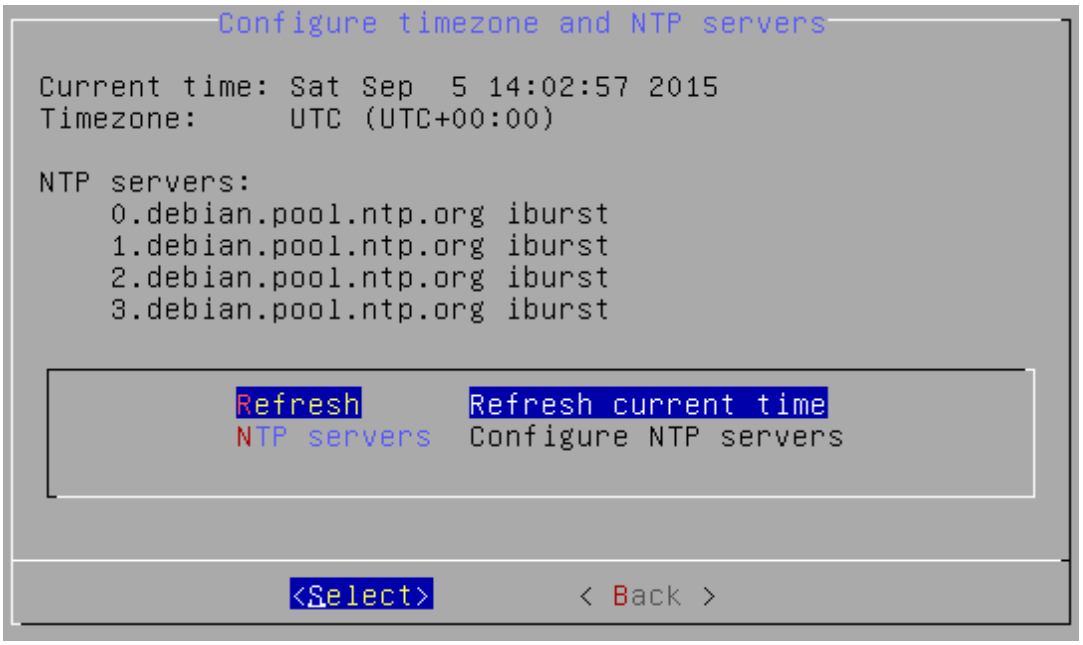
4.2.3 Configuring Time and NTP Servers

To configure NetIQ Server appliance time and NTP servers via Configuration Console, follow the steps:

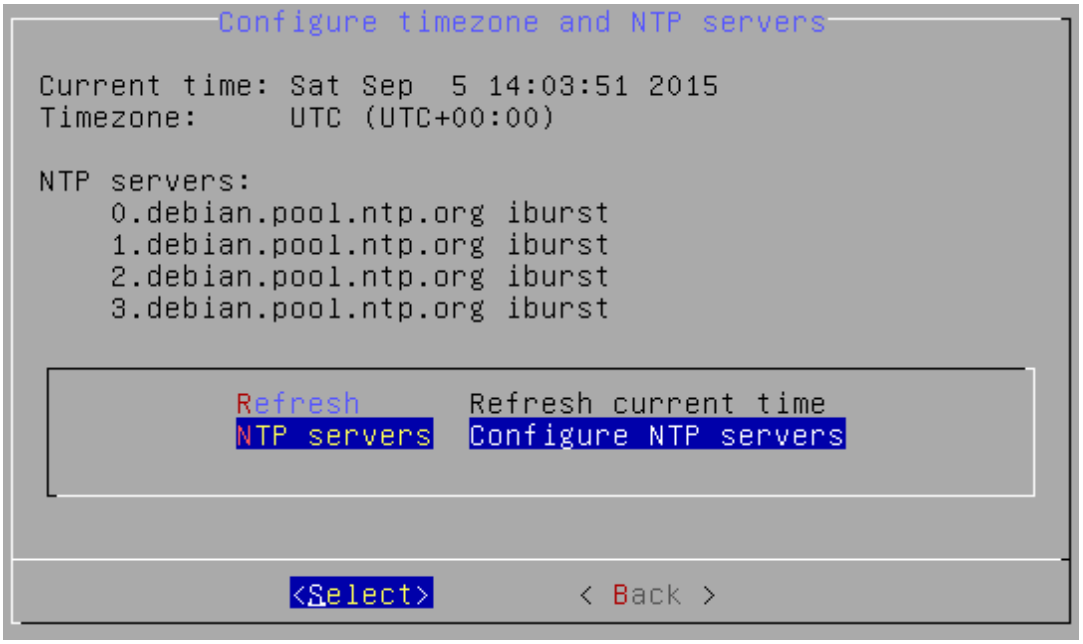
1. Go to the *Advanced Menu* of the *Configuration Console*.
2. Select *Time*.



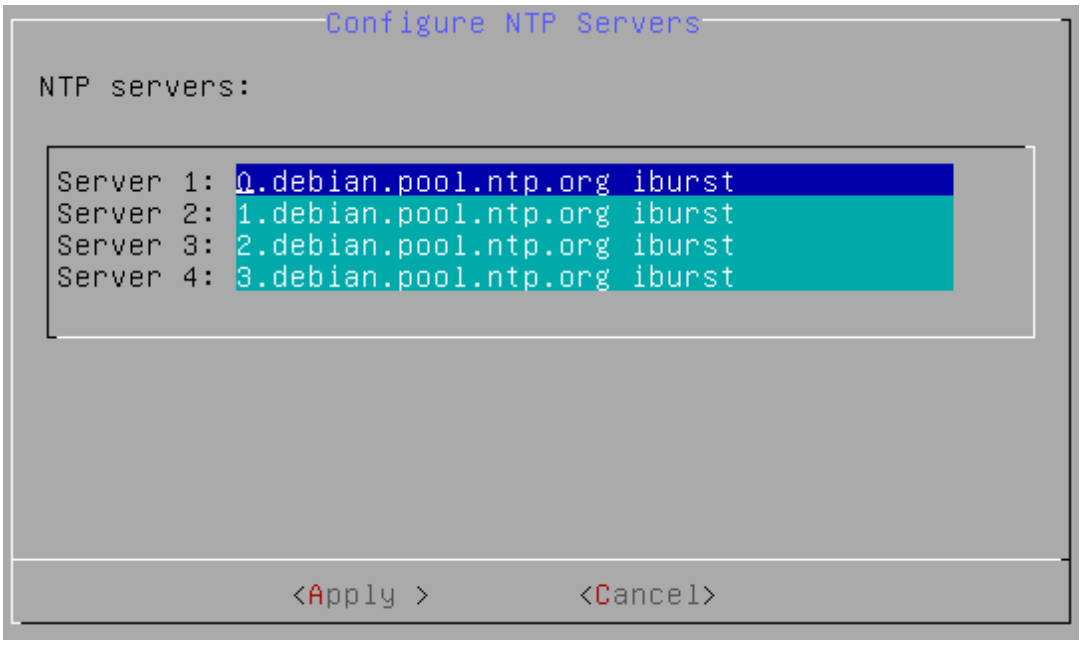
3. Select one of the following options:
   - *Refresh* to refresh current time.



- *NTP servers* to configure NTP servers.



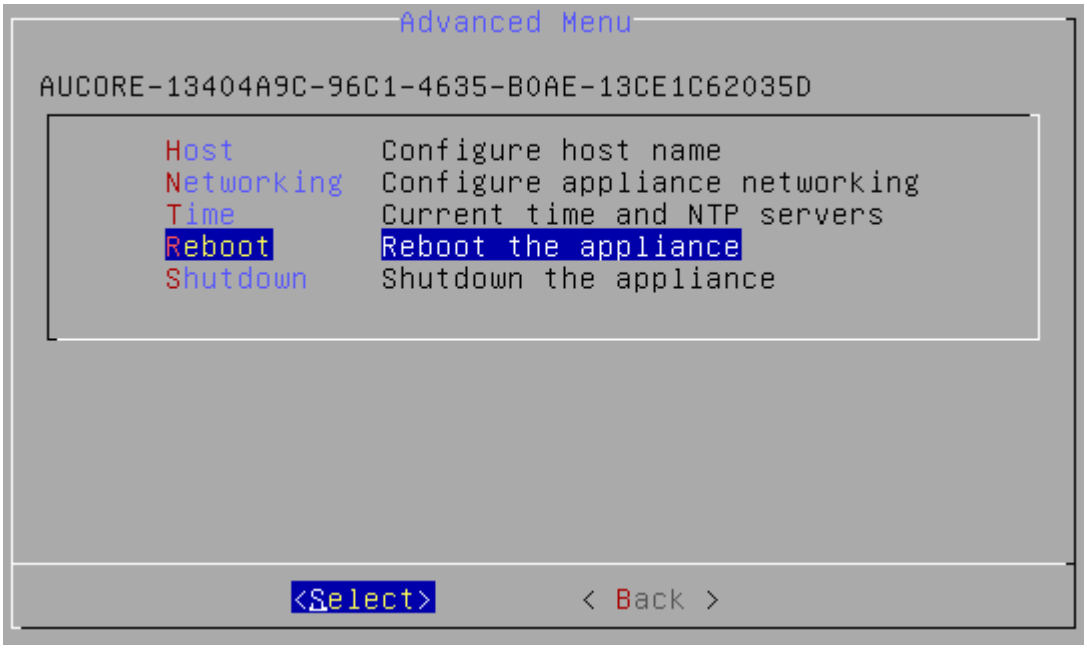
Specify applicable addresses for NTP servers and press *ENTER* to apply changes.



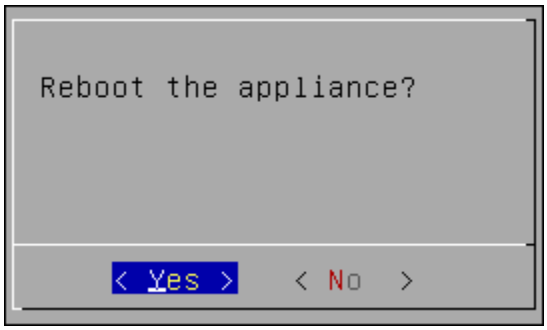
4.2.4 Rebooting Appliance

To reboot NetIQ Server appliance via Configuration Console, follow the steps:

1. Go to the *Advanced Menu* of the *Configuration Console*.
2. Select *Reboot*.



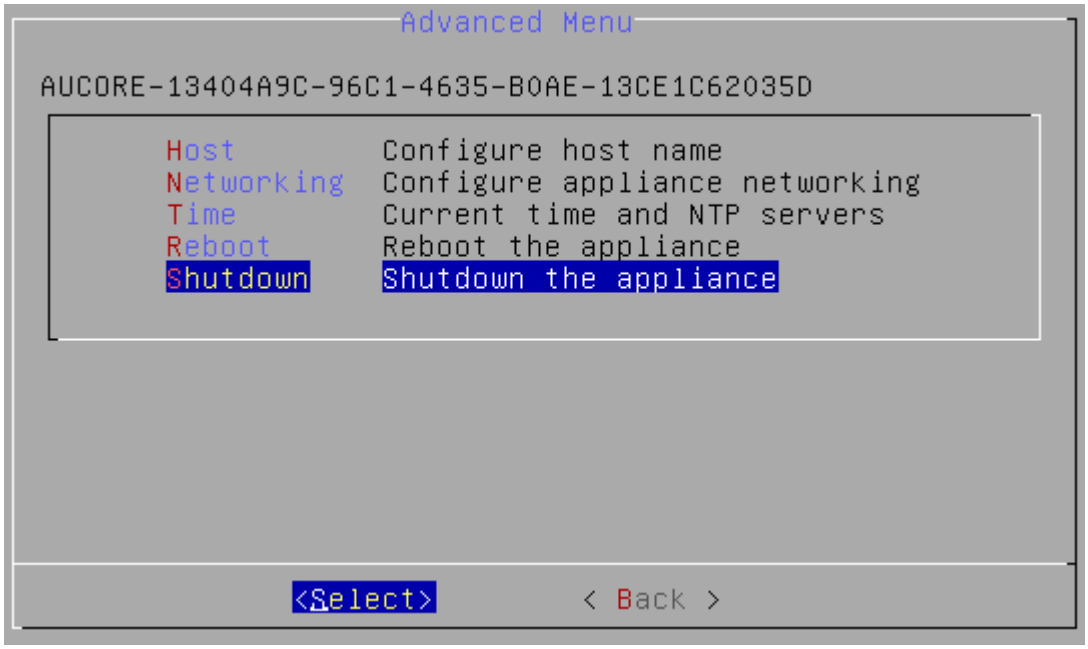
3. The confirmation message will be displayed. Select *Yes* to continue.



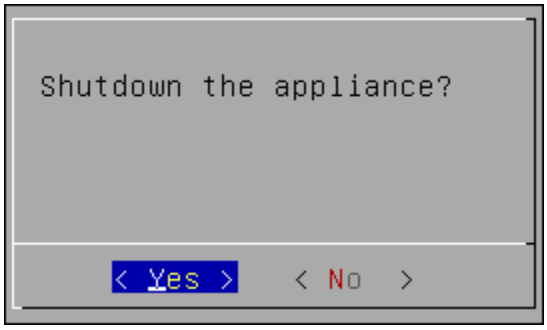
4.2.5 Shutting Down Appliance

To shut down NetIQ Server appliance via Configuration Console, follow the steps:

1. Go to the *Advanced Menu* of the *Configuration Console*.
2. Select *Shutdown*.



3. The confirmation message will be displayed. Select *Yes* to continue.

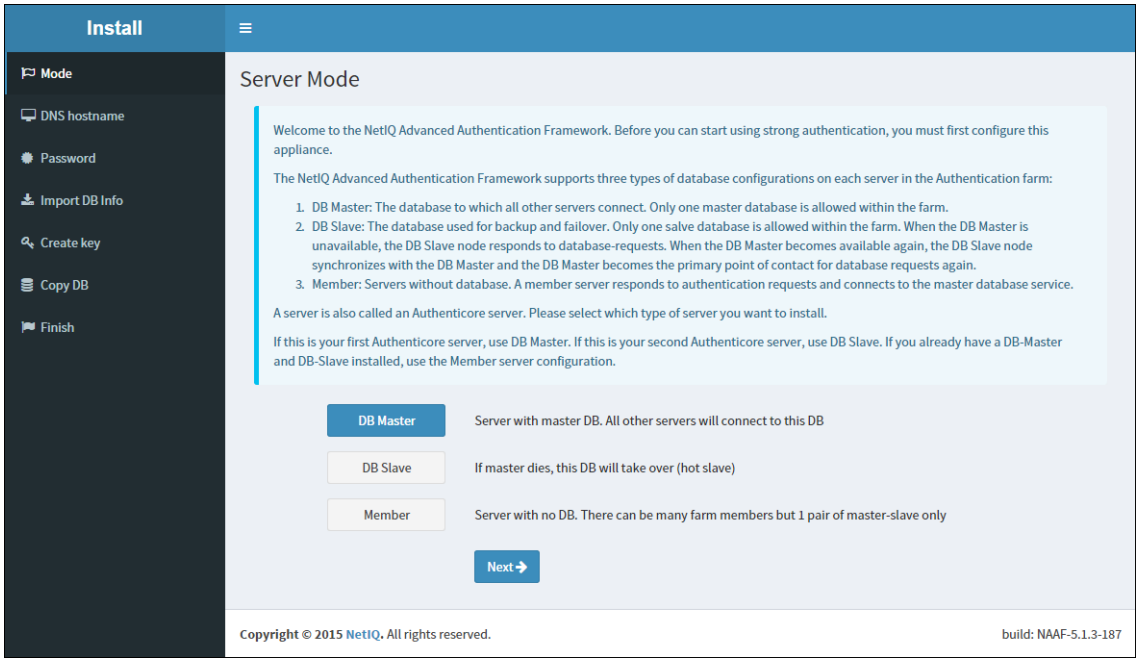


4.3 Configuring DB Master Server

After the installation of NetIQ Advanced Authentication Server appliance, it is required to configure the mode the appliance will run. The first server must be the *DB Master*. This is the server with master database. DB Slave server and Member servers are connected to the master database.

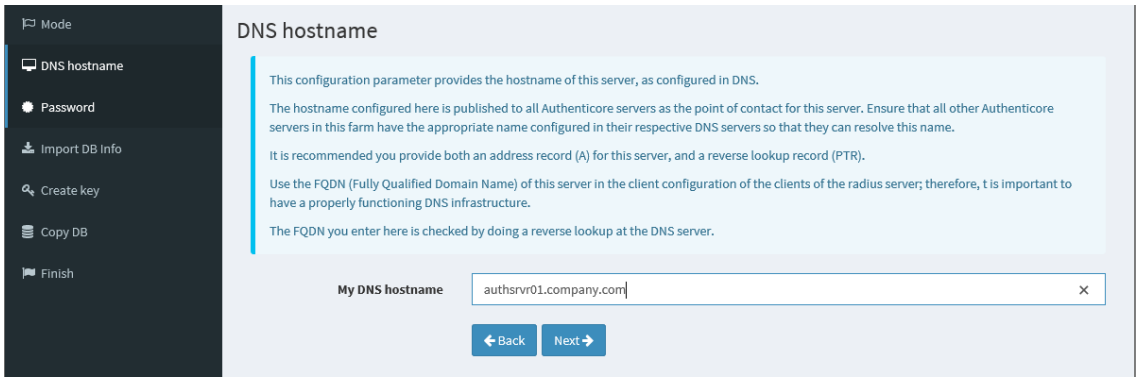
To configure the *DB Master* server:

1. Go to the NetIQ Administrative Portal. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the *DB Master* server mode and click *Next* to continue.

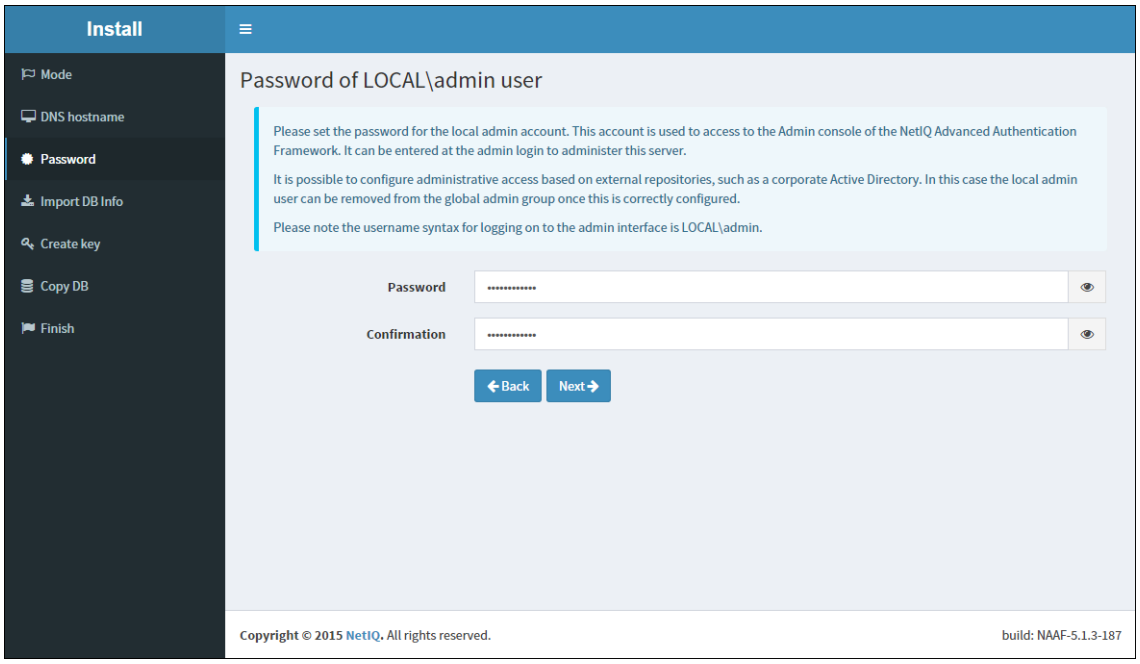


3. Specify the server DNS hostname. Click *Next* to continue.

WARNING: It's not recommended to specify an IP address instead of DNS hostname, because it's not possible to change the information later.

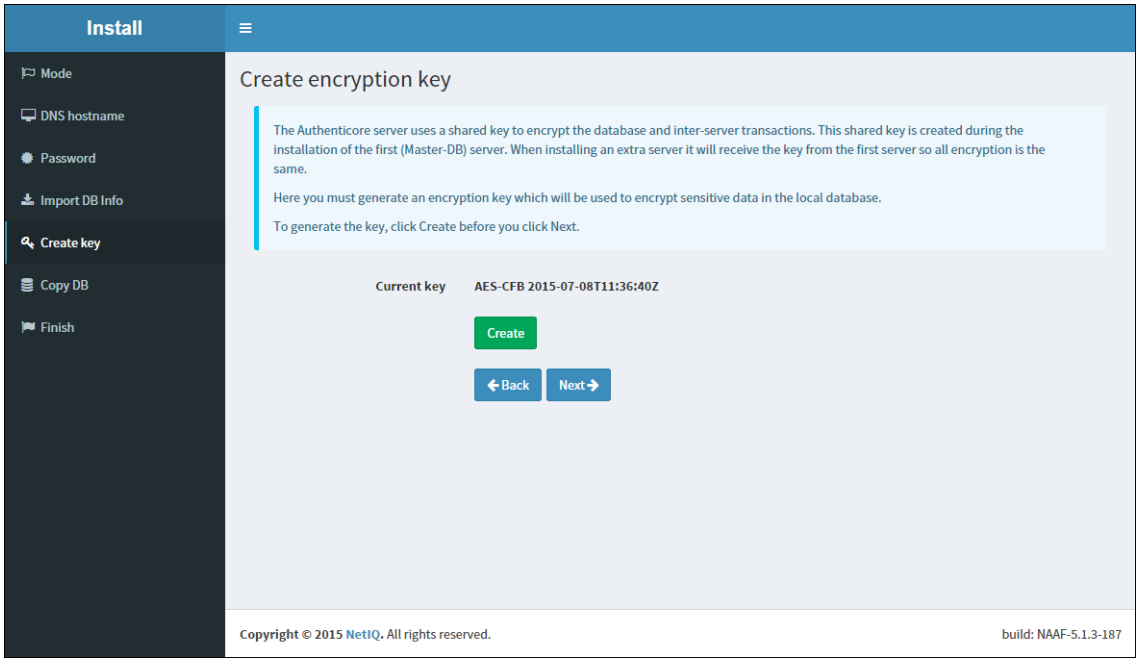


4. Specify the password of the LOCAL\admin user and confirm it. Click *Next* to continue.

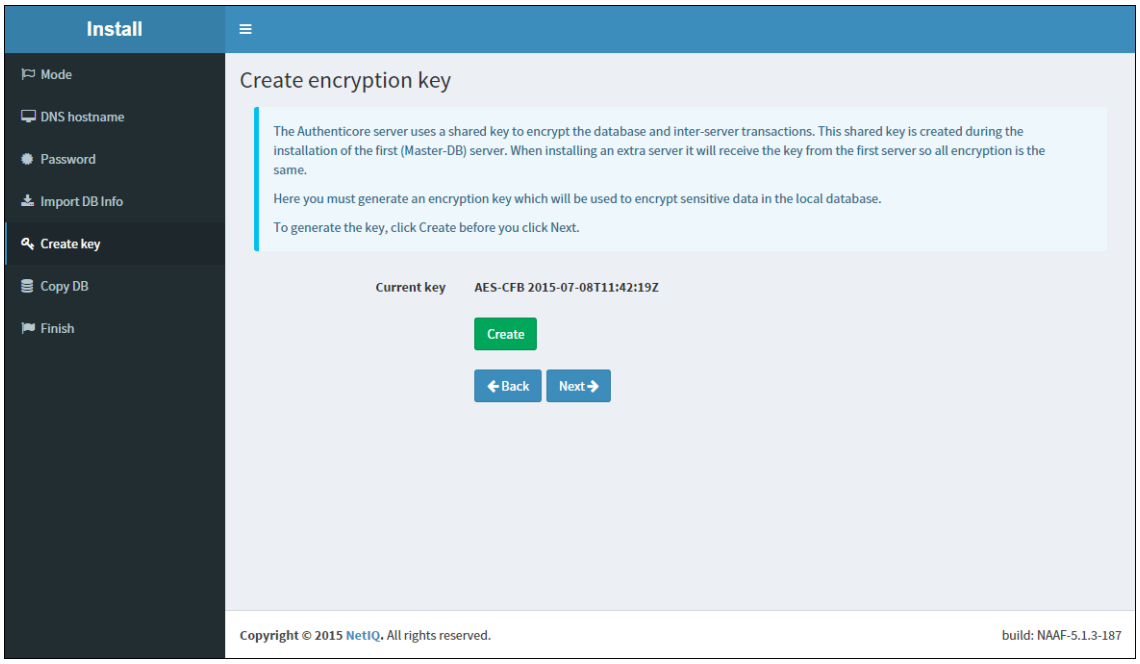


IMPORTANT: If you plan to use a Hardware Security Module from Yubico, Configuring YubiHSM.

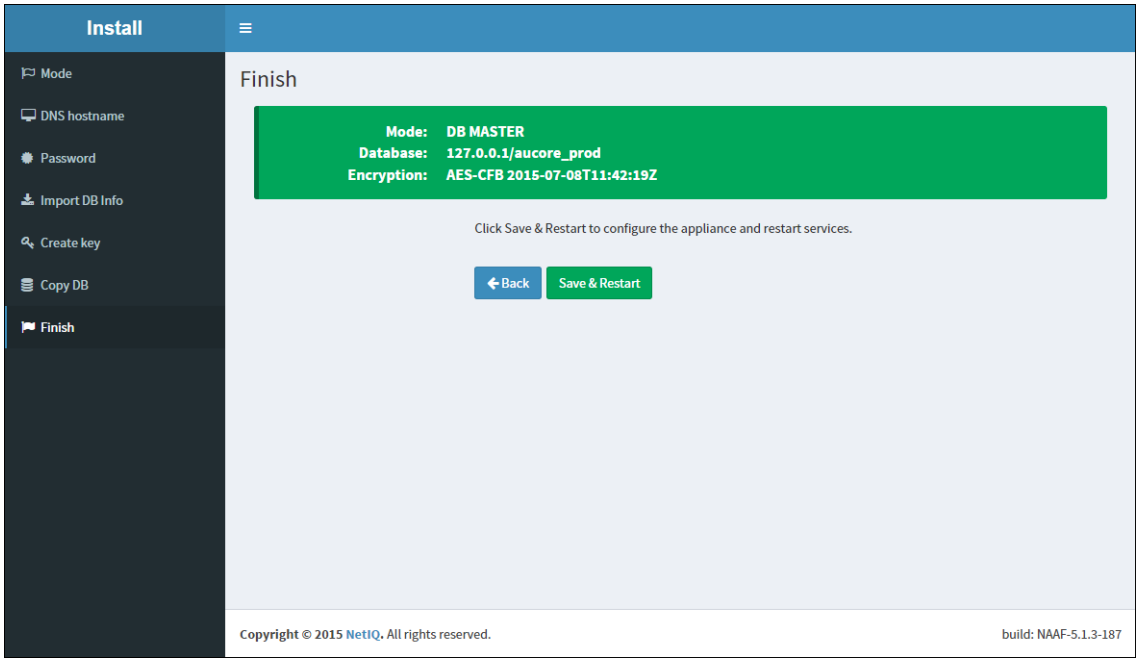
5. Click the *Create* button to generate encryption key file.



6. After generating an encryption key file, click *Next* to continue.



7. Click the *Save & Restart* button to write configuration and restart services. Services will be restarted within 30 seconds.

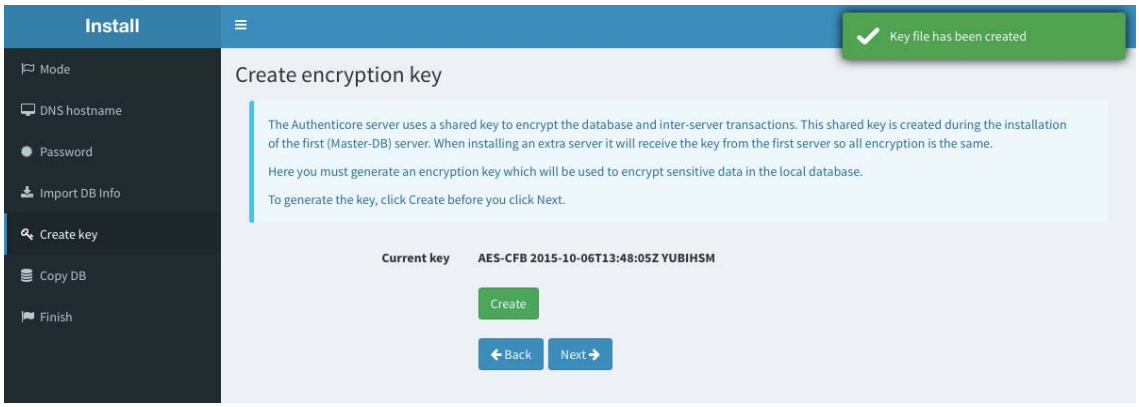


4.3.1 Configuring YubiHSM

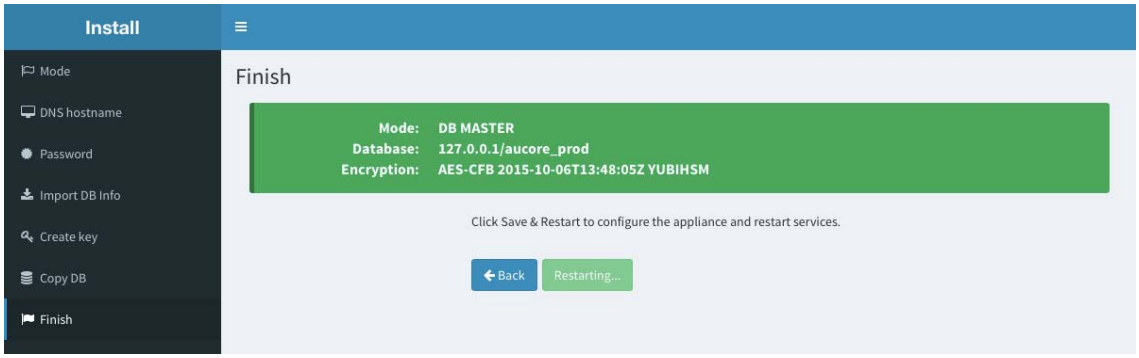
YubiHSM is a hardware security module developed by Yubico (https://www.yubico.com/products/yubihsm/). It allows to store an encryption key for NetIQ Advanced Authentication Server instead of storing them on appliance locally.

To configure usage of the hardware security module you need to follow the instruction during Configuring DB Master Server configuration of Configuring DB Master Server:

1. Hold the YubiHSM touch area and connect the device to the server physically. Continue to hold the touch area within 3 seconds when the YubiHSM is connected to activate the configuration mode. The LED starts to flash when you have entered the configuration mode.
2. Click the *Create* button to create the encryption key using the YubiHSM. In some seconds an encryption key will be created on the YubiHSM. In the *Current key* name you will see a `YUBIHSM` postfix .



3. Click *Next*.
4. Click *Save & Restart* to write configuration and restart services. Services will be restarted within 30 seconds.

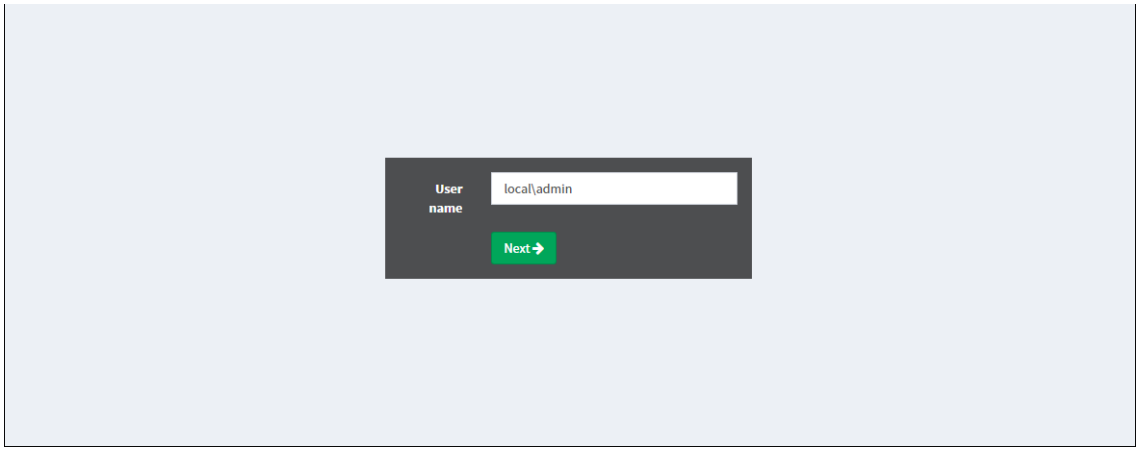


IMPORTANT: If you use a YubiHSM on the DB Master server, on DB Slave server another YubiHSM must be used. In such case installation of DB Slave server without YubiHSM is not supported. There is no step to create an enterprise key during configuration of DB Slave server, the connected YubiHSM will be configured during copying of the master's database to the DB Slave server.

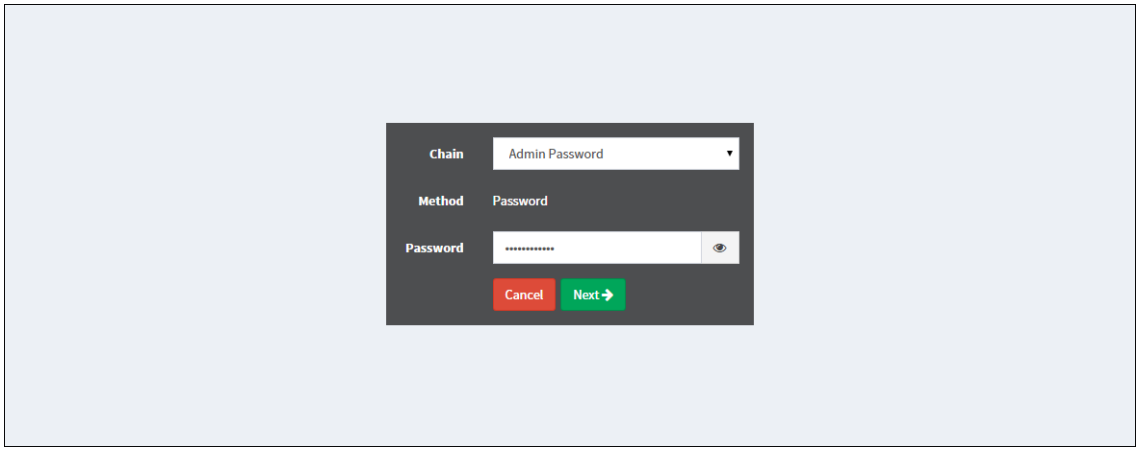
4.4 First Login To NetIQ Administrative Portal

After setting up an applicable server mode, the NetIQ Administrative Portal is displayed. To log in to NetIQ Administrative Portal, follow the steps:

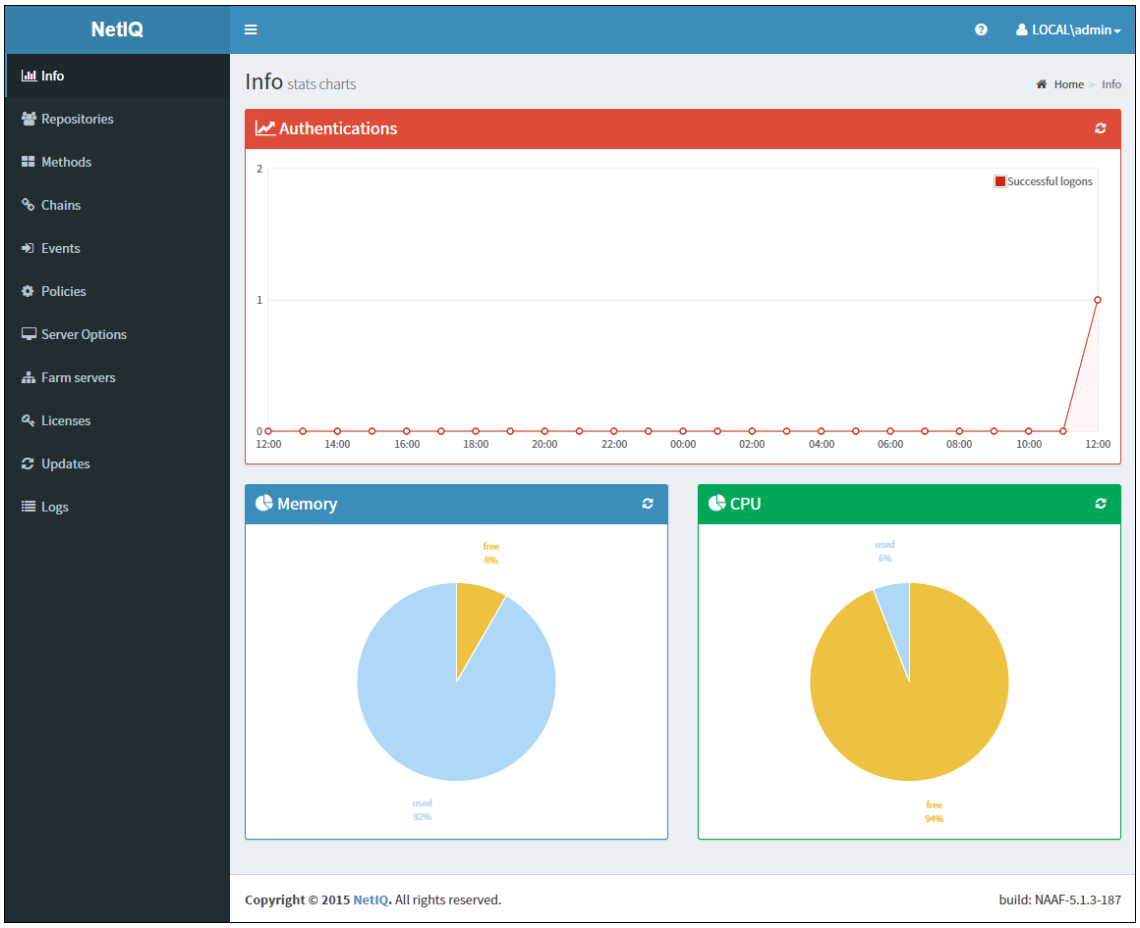
1. Enter administrator's login in the following format: repository\user (*local\admin* by default). Click *Next* to continue.



2. The *Admin Password* chain is automatically pre-selected by the system as the only available method. Enter the password you specified while setting up the DB Master server mode and click *Next* to log in.



3. The main page of NetIQ Admin Interface is displayed.



4.5 Configuring NetIQ Advanced Authentication Server Appliance

IMPORTANT: NetIQ Advanced Authentication Administrative Portal contains the Help option which contains detailed instructions on how to configure all settings for your authentication framework. You are provided with a capability to call the Help option by clicking the icon in the upper right corner of NetIQ Advanced Authentication Administrative Portal. The Help section provides you with information on the specific section you are working on.

After the installation of NetIQ Advanced Authentication Server appliance and configuring an applicable server mode, administrator is provided with a capability to configure NetIQ Advanced Authentication Server appliance through NetIQ Advanced Authentication Administrative Portal. To configure NetIQ Advanced Authentication Server, it is required to follow the steps:

1. Adding Repository
2. Configuring Methods
3. Creating Chain
4. Configuring Events
5. Managing Endpoints

6. Configuring Events
7. Configuring Server Options
8. Adding License

4.5.1 Adding Repository

A *repository* is the place where your users are stored. NetIQ Advanced Authentication Framework will not change your existing repository. It is only used to read user information. The storage of authentication templates and configuration settings all happens inside the appliance and is fully encrypted.

The Authentication framework supports any LDAP compliant directory. This can be *Active Directory Domain Services*, *NetIQ eDirectory*, *Active Directory Lightweight Directory Services* and in later versions any LDAP complaint directory.

NOTE: If you use NetIQ eDirectory the *Require TLS for Simple Bind with Password* option must be unchecked in LDAP Configuration settings of eDirectory. Otherwise you may get the error "Can't bind to LDAP: confidentialityRequired".

When adding a new repository the users in that repository can be matched to authentication chains. Only read rights are needed for the repository.

Please fill in the correct credentials and click *Add Server*. Here you can add the different servers in your network. The list will be used as a pool of servers, each time the connection is open a random server is chosen in the pool and unavailable servers will be discarded.

After you click *Save*, all information will be verified and saved.

To add repository that will be used for NetIQ Advanced Authentication, follow the steps:

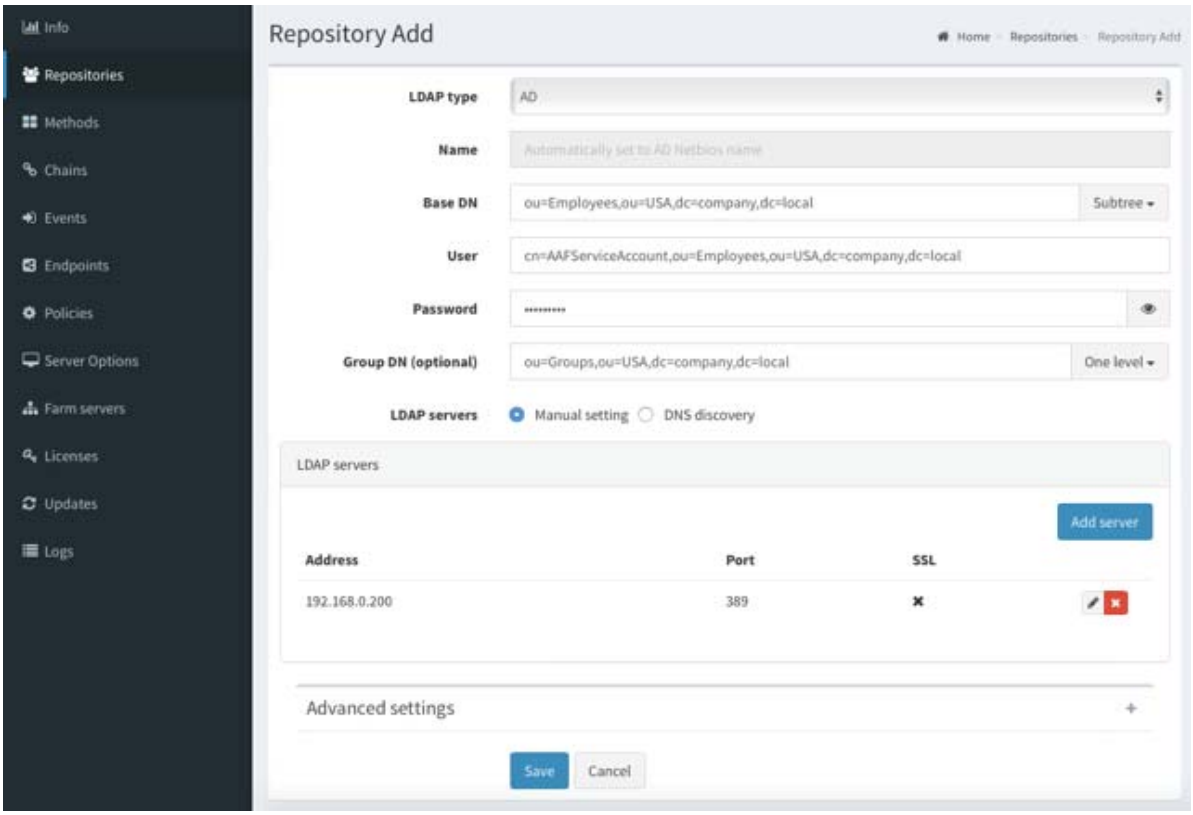
1. Open the *Repositories* section.
2. Click *Add*.
3. Select an applicable repository type from the *LDAP type* drop down list.

   The repository type can be *AD* for Active Directory Domain Services, *AD LDS* for Active Directory Lightweight Domain Services, *eDirectory* for NetIQ eDirectory.

   For AD a repository name will be automatically set to Netbios name of domain. For AD LDS and eDirectory you need to enter it manually in the *Name* text box.
4. Specify a container for the users in the *Base DN* text box. When you select the *Subtree* option, NetIQ Advanced Authentication Framework performs a search for users in all children nodes. You can change the search scope by selecting the *Search one level only* option.
5. Specify a user account in the *User* text box and enter the password of the user in the *Password* text box. Ensure that the user's password has no expiry.
6. You can specify a container for the groups in the *Group DN (optional)* text box. When you select the *Subtree* option, NetIQ Advanced Authentication Framework performs a search for the groups in all children nodes. You can change the search scope by selecting the *Search one level only* option.
7. Switch to *DNS discovery* option if you want to find LDAP servers automatically. In this case you need to fill the *DNS zone* and *Site name* fields and click *Perform DNS Discovery*.

   If you want to add the LDAP servers manually leave the *Manual setting* option checked and click *Add server*

8. Specify an LDAP server's address and port. Select the *SSL* check box to use SSL technology (if applicable). Click *Save*, next to server's credentials. Add additional servers (if applicable).
9. You can also expand the *Advanced Settings* section if you need to configure custom attributes. The following attributes are supported: User lookup attributes, User name attributes, User mail attributes, User mobile phone attributes, Group lookup attributes, Group name attributes.
10. Click *Save* to verify and save the specified credentials.
11. Click *Sync now* in block with the added repository.



You can later change the existing repositories by clicking *Edit* and you can add a new repository by clicking *Add*.

To check the sync status click *Edit* for the used Repository and see information in the *Last sync* section. Click *Full sync* to perform the full sync.

NOTE: NetIQ Advanced Authentication Framework performs automatic synchronization of changed objects (fastsync) hourly (NetIQ eDirectory doesn't support it), the complete synchronization (fullsync) is performing weekly.

4.5.2 Advanced Settings

To access the section of Repository configuration expand the Advanced Settings by clicking the + button. The settings allow to customize attributes which NetIQ Advanced Authentication Framework reads from repository.

User lookup attributes

NetIQ Advanced Authentication Framework checks the specified attributes for an entered user name.

Default attributes: cn, sAMAccountName, userPrincipalName.

User name attributes

NetIQ Advanced Authentication Framework shows a name from a first non-empty specified field for an entered user name.

Default attributes: cn, sAMAccountName, userPrincipalName.

User mail attributes

NetIQ Advanced Authentication Framework checks the specified attributes to get a user's email address.

Default attributes: mail, otherMailbox.

User mobile phone attributes

NetIQ Advanced Authentication Framework checks the specified attributes to get a user's phone number.

Default attributes: mobile, otherMobile.

Group lookup attributes

NetIQ Advanced Authentication Framework checks the specified attributes for an entered group name.

Default attributes: cn, sAMAccountName.

Group name attributes

NetIQ Advanced Authentication Framework shows a name from a first non-empty specified field for an entered group name.

Default attributes: cn, sAMAccountName.

NOTE: The sAMAccountName and userPrincipalName attributes are supported for only AD DS repository. In AD LDS and eDirectory repositories they are not supported.

4.5.3 Used Attributes

The chapter describes which attributes the appliance uses in the used directories.

NOTE: The sAMAccountName and userPrincipalName attributes are supported for only AD DS repository. In AD LDS and eDirectory repositories the attributes are omitted.

---

1. LDAP queries for repository sync

1.1. AD DS and AD LDS queries

1.1.1. Search users

```
(&(usnChanged>=217368)(&(objectClass=user)(|(cn=*)(sAMAccountName=*)(userPrincipal
Name=*))))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'otherMobile', 'mobile', 'userAccountControl', 'cn', 'usnChanged',
'userPrincipalName', 'msDS-User-Account-Control-Computed', 'objectGUID', 'mail',
'otherMailbox', 'GUID']
```

1.1.2. Search groups

```
(&(usnChanged>=217368)(&(objectClass=group)(|(cn=*)(sAMAccountName=*))))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'userAccountControl', 'cn', 'usnChanged', 'msDS-User-Account-Control-Computed',
'objectGUID', 'GUID']
```

1.2. eDirectory queries

The queries are the same as for AD DS and AD LDS, except for 'usnChanged' (this filter is not used).

1.2.1. Search users

```
(&(objectClass=user)(|(cn=*)(sAMAccountName=*)(userPrincipalName=*)))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'otherMobile', 'mobile', 'userAccountControl', 'cn', 'userPrincipalName', 'msDS-
User-Account-Control-Computed', 'objectGUID', 'mail', 'otherMailbox', 'GUID']
```

1.2.2. Search groups

```
(&(objectClass=group)(|(cn=*)(sAMAccountName=*)))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'userAccountControl', 'cn', 'msDS-User-Account-Control-Computed', 'objectGUID',
'GUID']
```

2. LDAP queries during logon

For AD LDS queries the attributes are same as for AD DS except for 'objectSid' (the filter

is not used in queries about membership in groups).

In the examples below, the username is pjones, base_dn is DC=company,DC=com

2.1. AD DS and AD LDS queries

2.1.1. Basic user information

```
(&(objectClass=user)(|(cn=pjones)(sAMAccountName=pjones)(userPrincipalName=pjones)
))
```

Requested attributes:

```
(&(objectClass=user)(objectGUID=\0f\d1\14\49\bc\cc\04\44\b7\bf\19\06\15\c6\82\55))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

2.1.2 Group membership information for user

AD specific query using objectSid filter:

```
(|(member=CN=pjones,CN=Users,DC=company,DC=com)(objectSid=S-1-5-21-3303523795-
413055529-2892985274-513))
```

Requested attributes:

```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

2.3 Iteratively query about each group received from above query

```
(member=CN=Performance Monitor Users,CN=Builtin,DC=company,DC=com)
```

Requested attributes:

```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

2.2. eDirectory queries

2.2.1. Basic user information

```
(&(objectClass=user)(|(cn=pjones)(sAMAccountName=pjones)(userPrincipalName=pjones)
))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

```
(&(objectClass=user)(GUID=\57\b6\c2\c1\b9\7f\4b\40\b9\70\5f\9a\1d\76\6c\d2))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

2.2.2. Group membership information for user

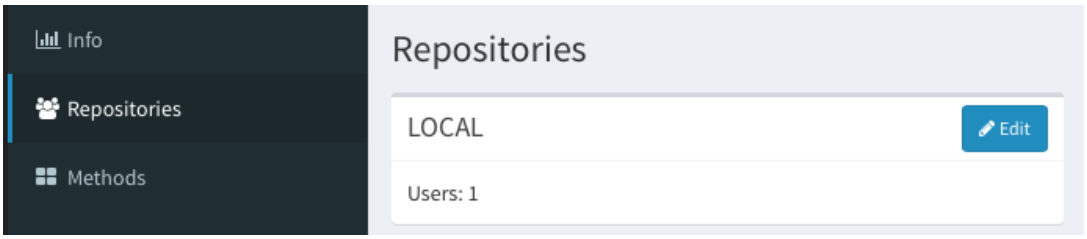
```
(member=cn=pjones,o=AAF)
```

Requested attributes:

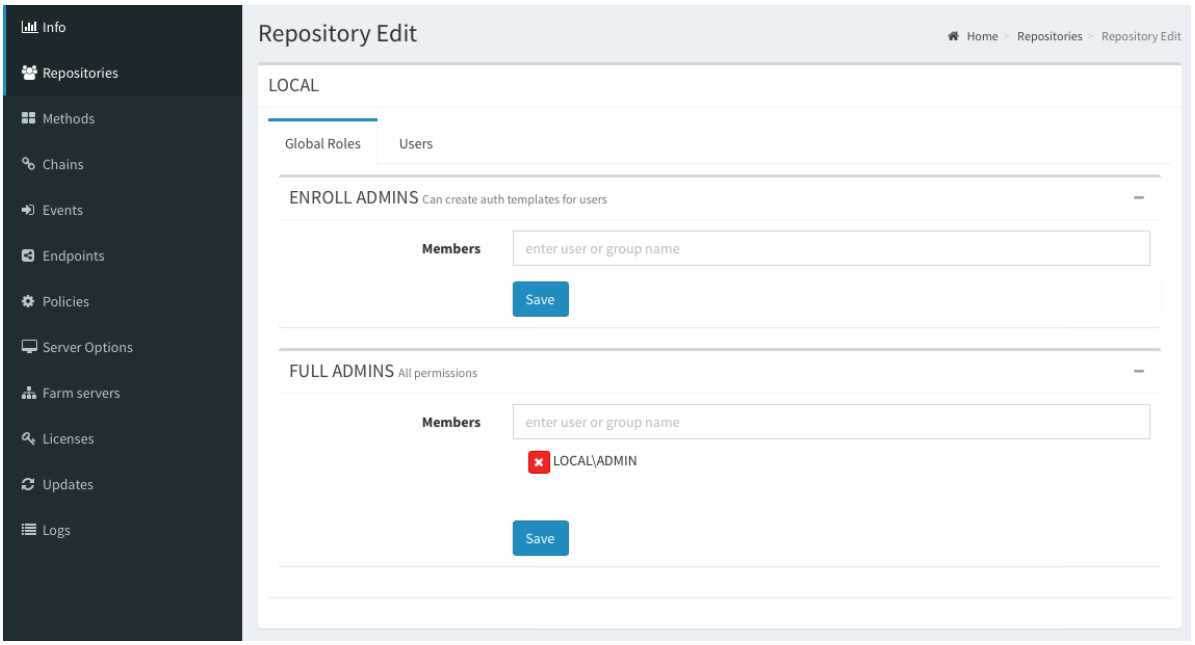
```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

4.5.4 Local Repository

To access the Local repository settings click *Edit* in LOCAL repository block of Repository section.

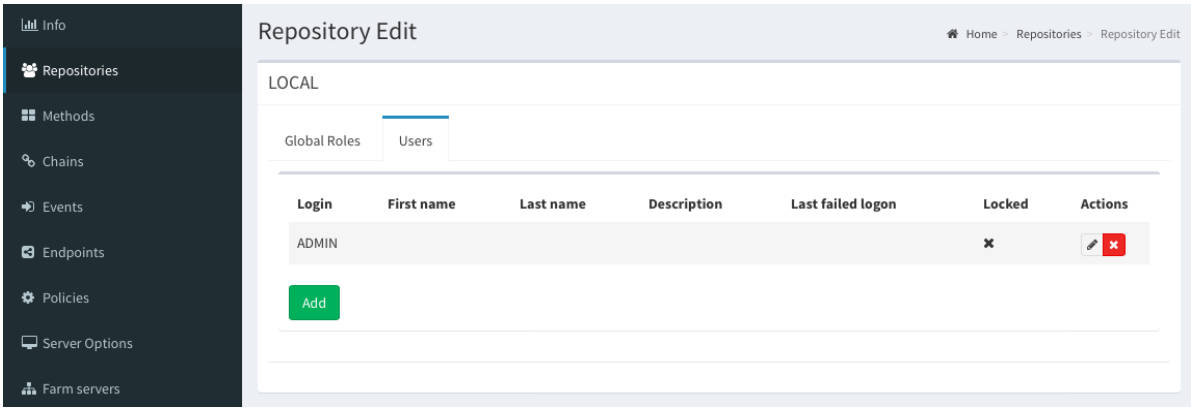


On the *Global Roles* tab it's possible to manage Security Officers (ENROLL ADMINS) and NetIQ Advanced Authentication Framework Administrators (FULL ADMINS).

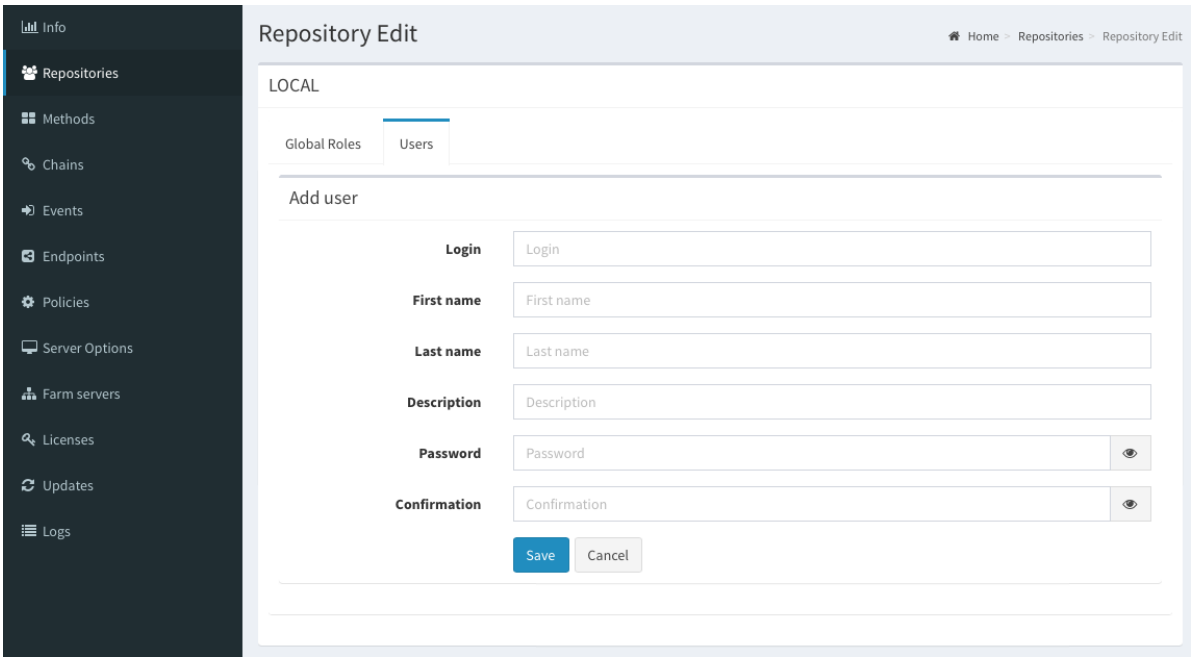


By default there are no ENROLL ADMINS and LOCAL\ADMIN is only one account specified as FULL ADMIN. You may change this by adding the user names from local or the used repositories in Members fields. Then click *Save* to apply the changes.

On the *Users* tab it's possible to manage the local users.



To add the new local account click *Add* button. Then you will need to specify a user name, first name, last name, description and the user's password.



4.5.5 Configuring Methods

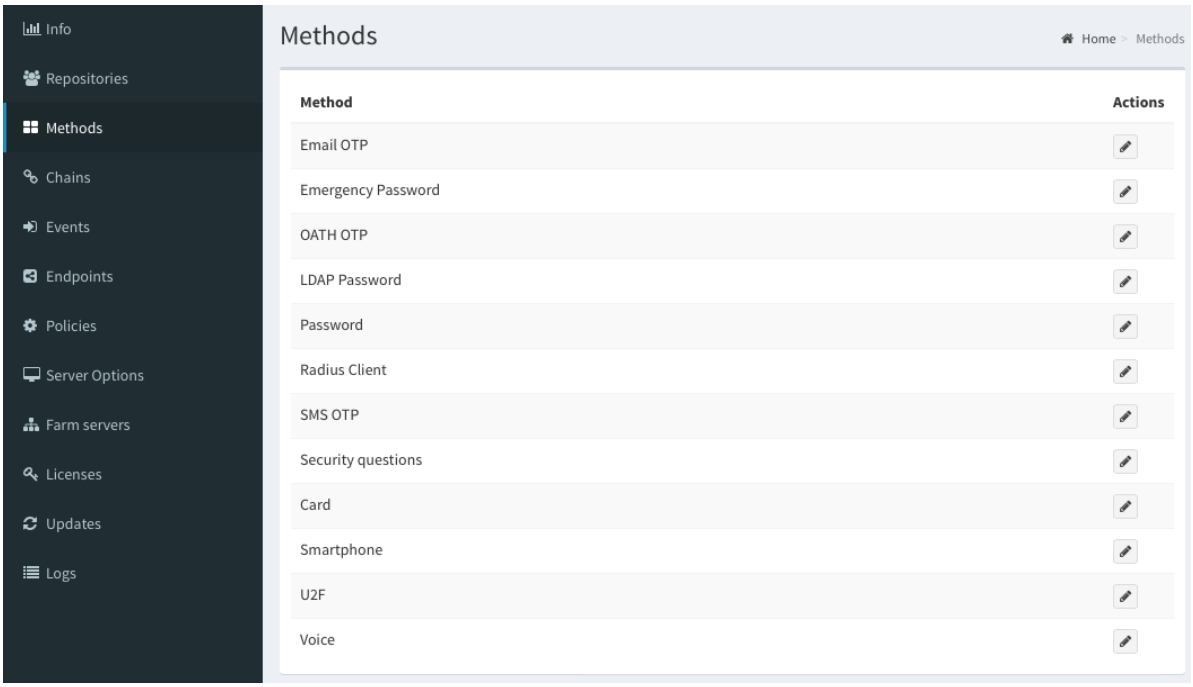
The Methods page shows a list of the authentication methods which contain settings.

To configure an applicable authentication method for NetIQ Advanced Authentication framework, follow the steps:

1. Open the *Methods* section. The list of available authentication methods will be displayed.
2. Click the *Edit* button next to an applicable authentication method.
3. Edit configuration settings for a specific authentication method.
4. Click *Save* at the bottom of the *Methods* view to save changes.

In the section you can find the following settings:

- Email OTP - Email message and One-Time Password related settings
- Emergency Password - security settings of Emergency Password method
- OATH OTP - OATH TOTP/HOTP related settings, also CSV/PSKC bulk import and token assignment
- LDAP Password - an option which allows to save LDAP Password.
- Password - security settings of local password
- Radius Client - settings for to a third-party RADIUS server
- SMS OTP - One-Time Password related settings for SMS method
- Security Questions - security questions and its security settings
- Smartphone - Smartphone method settings
- FIDO U2F - an option which allows to enable check of attestation certificate
- Voice Call - security settings of Voice Call method



An authentication method itself cannot be linked to an event. You will need to create an Authentication Chain in order to configure the authentication for the user. It is however possible to make an Authentication Chain with just one method in it.

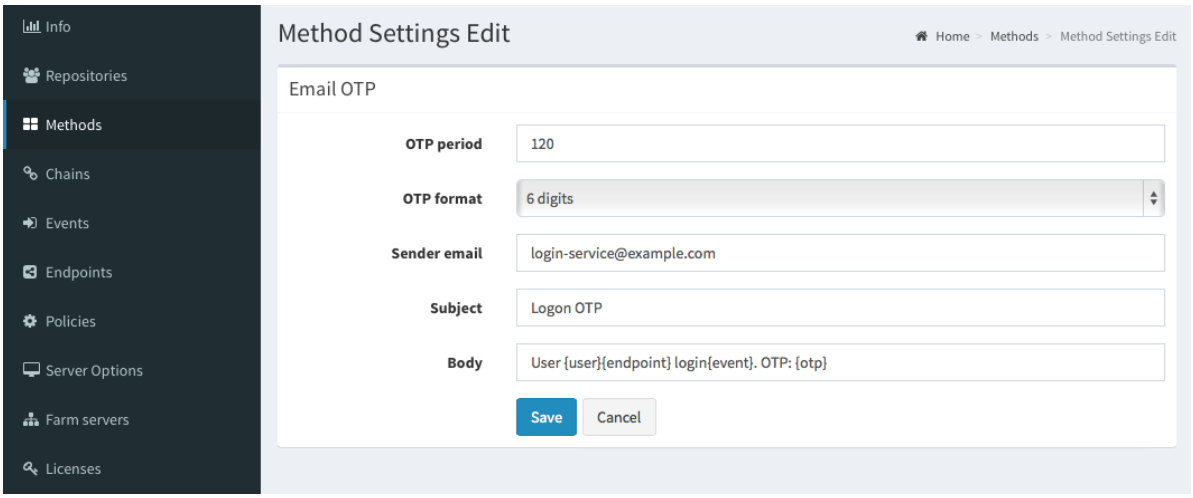
For example if you want to create Password and OTP authentication then you would create a chain with the Password and OTP methods in it. However if for a certain event the use of only OTP is enough then you can make an Authentication Chain with just OTP in it.

4.5.6 Email OTP

The Email OTP authentication method will send an email to the user's e-mail address with a One-Time-Password (OTP). The user will receive this OTP and needs to enter it on the device where authentication is happening. This authentication method is best used with a second method like Password or LDAP Password in order to achieve multi-factor authentication and to prohibit malicious users from sending SPAM to a user's email box with authentication requests.

The following configuration options are available:

- *OTP Period*: the lifetime of an OTP token in seconds. By default 120 seconds.
- *OTP Format*: the length of an OTP token. By default 8 digits.
- *Sender email*: the sender email address.
- *Subject*: the subject of the mail sent to the user.
- *Body*: the text in the email that is sent to the user. The following variables can be used:
  - {user} - the username of the user
  - {endpoint} - the device the user is authenticating to
  - {event} - the name of the event where the user is trying to authenticate to
  - {otp} - this is the actual One-Time-Password

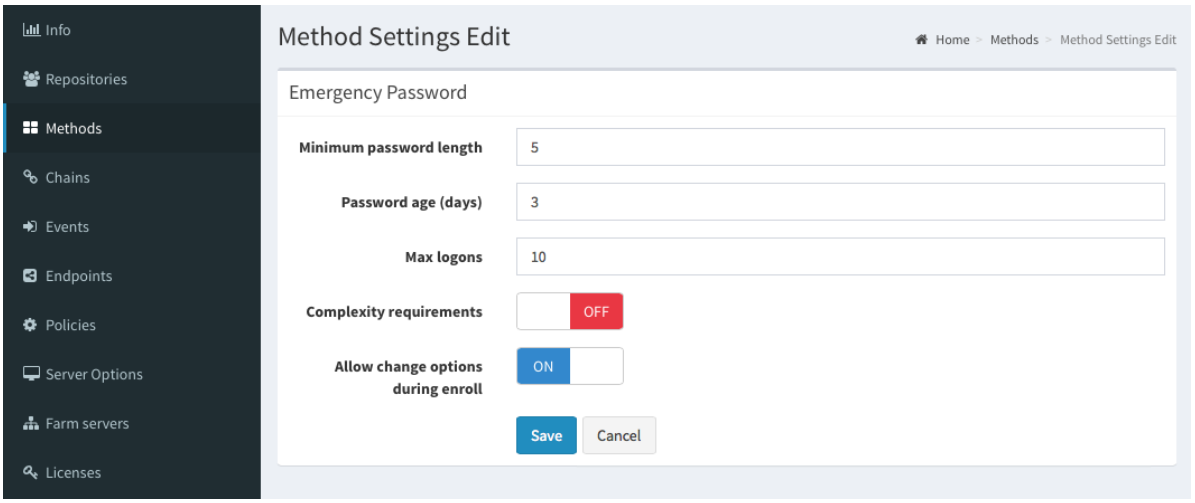


4.5.7 Emergency Password

The settings allows to configure the Emergency Password authentication method. The method can be used as temporarily solution for the users who forgot smartphone or lost a card. Enrollment of the method is allowed only by security officers. Users are not permitted to enroll it.

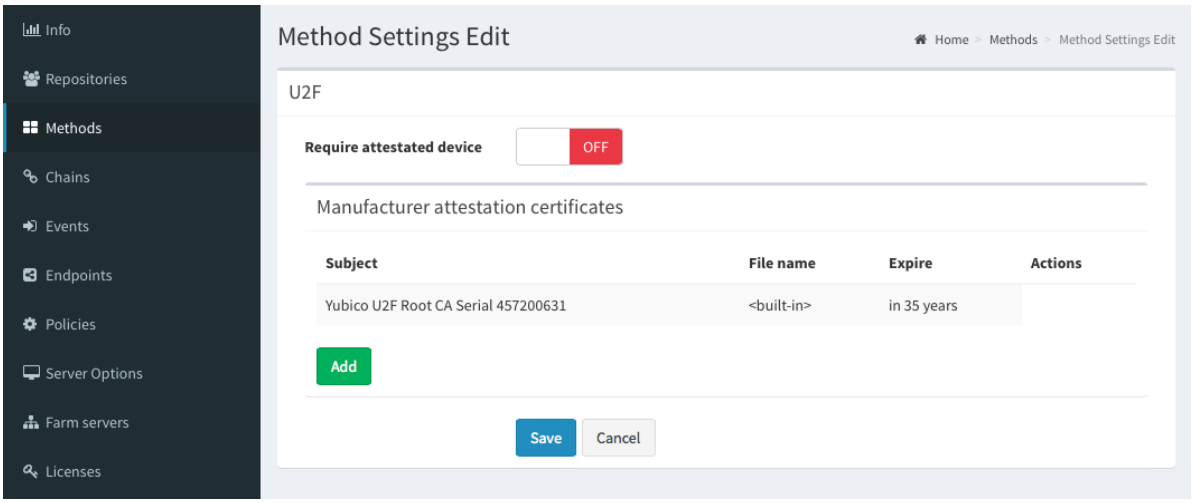
It's possible to manage the following security options:

1. *Minimum password length*. 5 characters by default. Usage of shorter passwords is not allowed.
2. *Password age (days)*. 3 days by default. It means the password will expire in 3 days.
3. *Max logons*. 10 logons by default. The password becomes expired after 10 logons.
4. *Complexity requirements*. The option is disabled by default. If it's enabled the password must complain at least 3 of 4 checks:
   - it should contain at least one uppercase character,
   - it should contain at least one lowercase character,
   - it should contain at least one digit,
   - it should contain at least one special symbol.
5. *Allow change options during enroll*. If the option is enabled a security officer will be able to set *Start date*, *End date* and *Maximum logons* manually. The manual configuration overrides the settings in Emergency Password method.



4.5.8 FIDO U2F

The section contains certificate settings related to FIDO U2F authentication method. By default NetIQ Advanced Authentication framework doesn't require the attestation certificate for authentication by FIDO U2F compliant token. If you plan to enable the feature, ensure that you have a valid attestation certificate added for your FIDO U2F compliant tokens. A Yubico attestation certificate is preconfigured in the NetIQ Advanced Authentication appliance. Use *Add* button to add a device manufacturer certificate, which must be in PEM format. To enable check of attestation certificate switch the *Require attestated device* option to ON.



IMPORTANT: Usage of single factor FIDO U2F chain is not supported in Mac OS Client. It should be always combined with LDAP Password and the FIDO U2F method should be last in the used chain, i.e. LDAP Password+FIDO U2F.

To use the FIDO U2F authentication in NetIQ Access Manager it's required to configure an external web service to perform enrollment and authentication for one domain name. Configuring a Web Server in order to use the FIDO U2F authentication in NetIQ Access Manager

The YubiKey tokens may start to flash with delay when token is initialized in combo-mode (e.g. OTP+U2F). It may decrease user performance, as users have to wait when the token start to flash before enrollment or authentication. Therefore it's recommended to flash the tokens in U2F only mode if the rest modes are not needed.

Configuring a Web Server in order to use the FIDO U2F authentication in NetIQ Access Manager

NOTE: This article is applicable for Debian 8 Jessie. The procedure may differ for other distributives.

These instructions will help you to configure web server in order to use FIDO U2F authentication in NetIQ Access Manager. According to FIDO U2F specification, enrollment and authentication must be performed for one domain name. NetIQ Access Manager and NetIQ Advanced Authentication Framework appliance are located on different servers, as a result it is required to configure web server which will perform port forwarding to:

- NetIQ Advanced Authentication Framework appliance for the FIDO U2F enrollment
- NetIQ Access Manager for further authentication using FIDO U2F tokens

Installing Nginx Web Server

To install Nginx web server to use it for URL forwarding, add these two lines to the */etc/apt/sources.list* file:

```
deb http://packages.dotdeb.org jessie all
deb-src http://packages.dotdeb.org jessie all
```

Preparing SSL Certificate

To prepare SSL certificate, please run these commands:

```
mkdir –p /etc/nginx/ssl
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/
proxy.key -out /etc/nginx/ssl/proxy.crt
```

Nginx Proxy Configuration

To prepare Nginx proxy configuration, add the following to the */etc/nginx/sites-available/proxy* file:

```
server {
listen 443 ssl;
error_log /var/log/nginx/proxy.error.log info;
server_name nam.company.local;
ssl_certificate /etc/nginx/ssl/proxy.crt;
ssl_certificate_key /etc/nginx/ssl/proxy.key;
location ~ ^/account {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_pass https://<appliance_IP>$uri?$args;
}
location ~ ^/static {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
```

```
proxy_pass https://<appliance_IP>$uri?$args;
}
location ~ ^/admin {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_pass https://<appliance_IP>$uri?$args;
}
location / {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_read_timeout 300;
proxy_pass https://<NAM_IP>;
}
}
```

Create link and restart nginx service using the following commands:

```
ln -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled/proxy
service nginx reload
```

DNS Entries

Please make sure that NAM name server corresponds to IP address of web server.

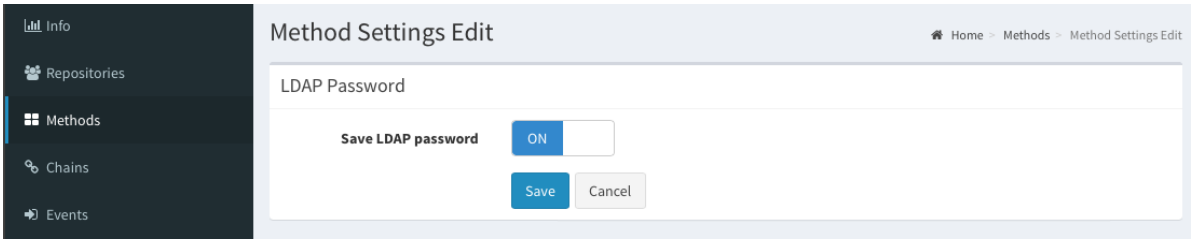
Enrollment

To enroll U2F, please open link https://<NAM_FQDN>/account. You will be forwarded to the enroll page of NetIQ Advanced Authentication Framework server appliance.

LDAP Password

The settings allows to configure security options for LDAP passwords (passwords stored in the used repository).

The option allows to save LDAP Password in user data during a first logon, so the further authentications using chains without LDAP Password can be performed using only NetIQ Advanced Authentication Frameworkauthentication method until the password will be expired and changed.



OATH OTP

OATH stands for Initiative for Open Authentication and is an industry-wide collaboration to develop an open reference architecture using open standards to promote the adoption of strong authentication using One-Time-Passwords.

Advanced Authentication Framework supports two different types of OATH OTP and these are:

- HOTP: counter based OTP
- TOTP: time based OTP

To access the settings open NetIQ Advanced Authentication, *Methods* section, click *Edit* button next to OATH OTP.

For the *HOTP* variant you can specify the following parameters:

1. *OTP format*, it determines how many digits the OTP token has. By default it's 6 digits. It can be changed to 4,6,7 or 8 digits. The value should be the same as the tokens you are using.
2. *OTP window* allows to specify a value, how much OTPs the Advanced Authentication Server will generate starting from the current HOTP counter value to match an HOTP entered by user during authentication. The default value is 10.This is required for the case when users use the tokens not only for authentication using NetIQAdvanced Authentication, in each case of usage the HOTP counter increases on 1, so the counter will be out of sync between the token and Advanced Authentication Server. Also users can press the token button accidentally.

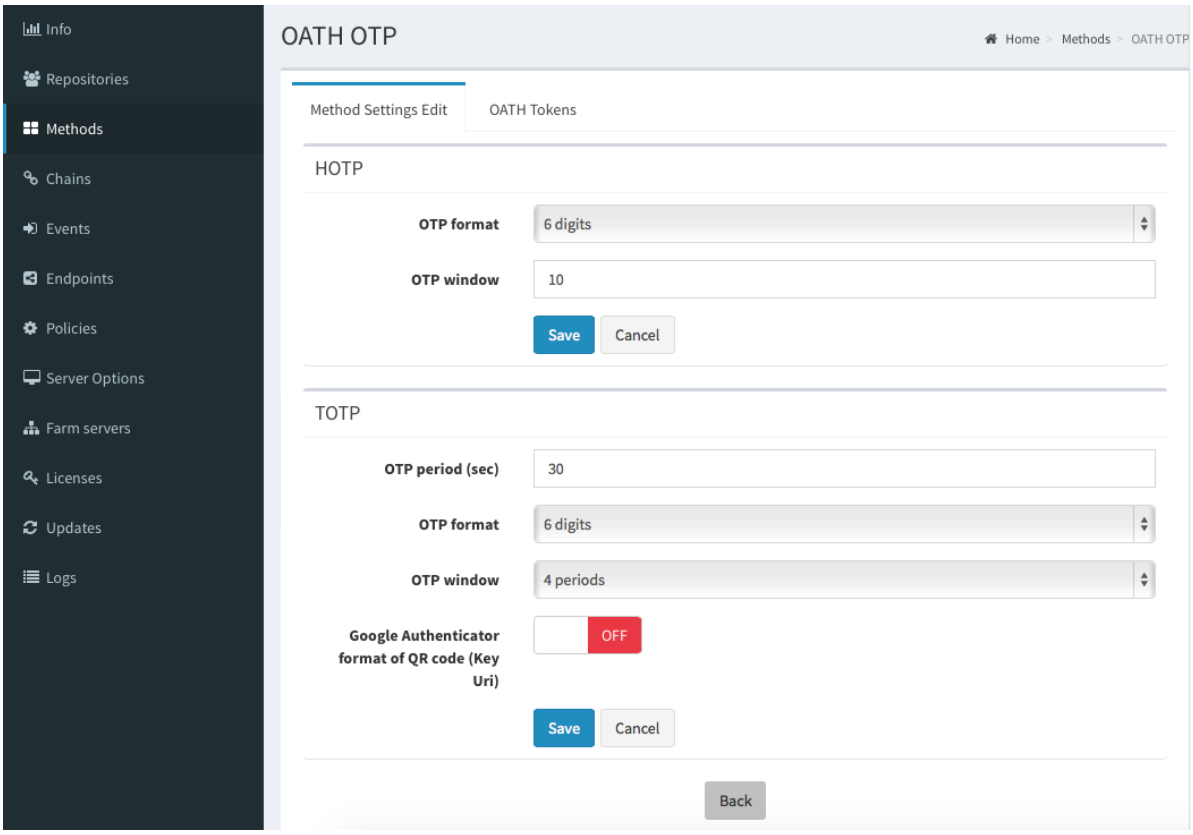
WARNING: Increasing of HOTP window value to more than 100 is not recommended, because it may decrease security by causing false matches.

During enrollment or HOTP counters synchronization in Self-Service Portal the *Enrollment HOTP window* equal to 100 000 is used. This is necessary because the HOTP tokens may be used during a long period before enrollment in NetIQ Advanced Authentication and its value is unknown and could be even equal to some thousands. This is secure as users need to provide 3 consequent HOTPs.

The *TOTP* settings contain the following parameters:

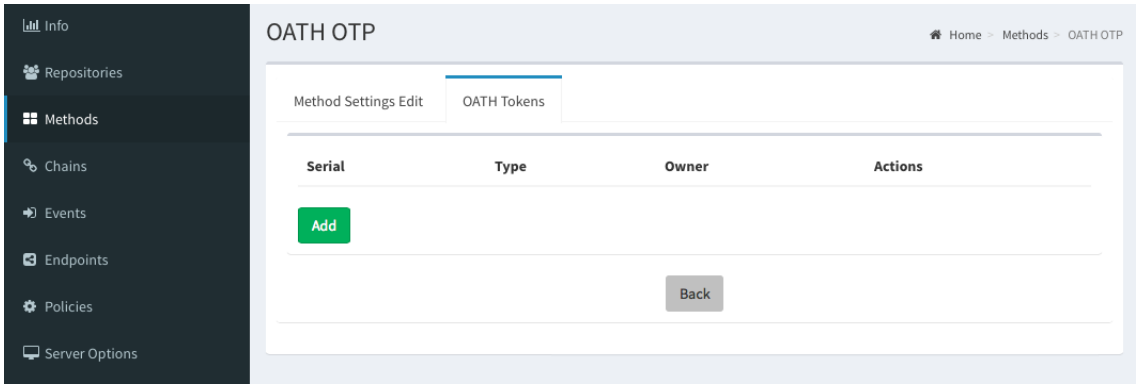
1. *OTP period (sec)* allows to specify how often a new OTP is generated. A default value is 30 seconds.
2. *OTP format* determines how many digits the OTP token has. By default it's 6 digits. It can be changed to 4,6,7 or 8 digits. The value should be the same as the tokens you are using.
3. *OTP window*, it allows to determine how many period may be used by Advanced Authentication Server for TOTP generation. E.g. we have a period of 30 and a window of 4, then the token is valid for 4*30 seconds before current time and 4*30 seconds after current time, which is 4 minutes. These configurations are used because time can be out-of-sync between the token and the server and that will otherwise impact the authentication.
4. *Google Authenticator format of QR code (Key Uri)*. By default the NetIQ Auth smartphone app can be used to scan a QR code for enrollment of software token. The format of QR code is not supported by other apps. It's possible to switch NetIQ Advanced Authentication to use the Google Authenticator app instead of NetIQ Authsmartphone app using the option.

IMPORTANT: OTP format must be set to 6 digits when you use the Google Authenticator format of QR code.



Advanced Authentication Framework also supports the import of PSKC or CSV files. These are token files with token information in them. To do this follow the instruction below:

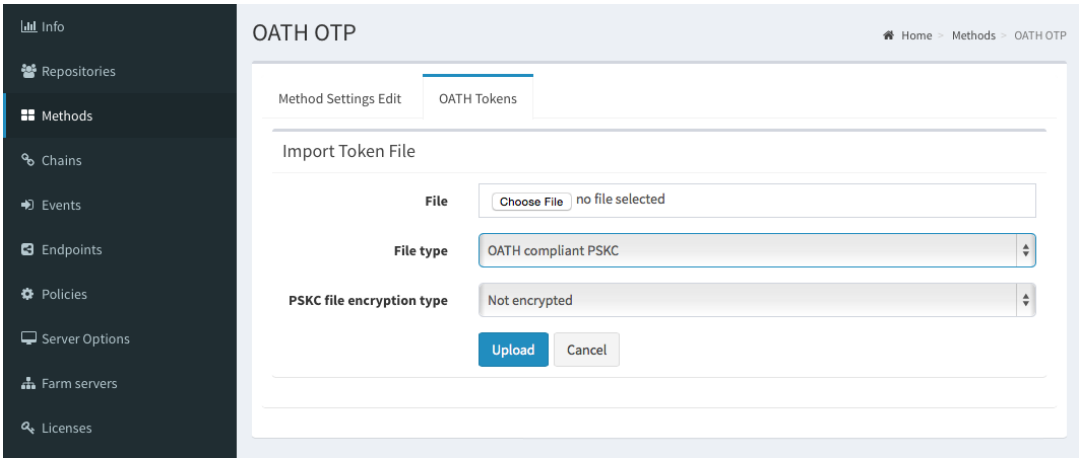
1. Go to the *OATH Token* tab.



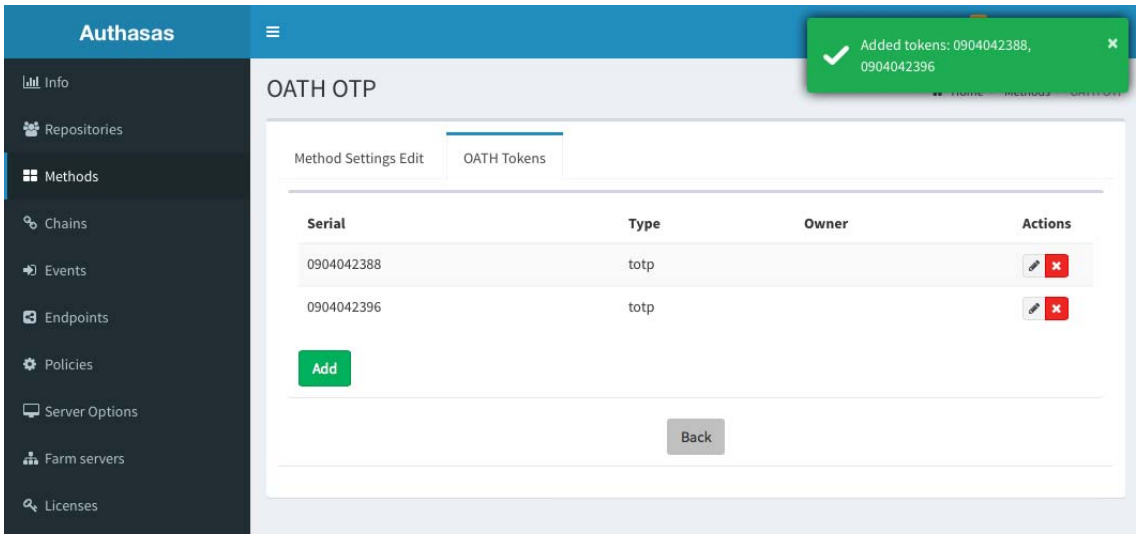
2. Click *Add* button.
3. Click *Choose File* and add a PSKC or CSV file.
4. Choose a proper *File type*. It can be
   - *OATH compliant PSKC* (e.g. for HID OATH TOTP compliant tokens).
   - *OATH csv*, the CSV must complain the format described Format of CSV file which is supported for import of OATH compliant tokens. It's not possible to use the YubiKey CSV files.

- *Yubico csv*, it's required to use the default `Traditional format` of the CSV (check YubiKey Personalization Tool - Settings tab - Logging Settings).

IMPORTANT: Yubico csv with the tokens which personalized not to input the OATH Token Identifier is not supported.



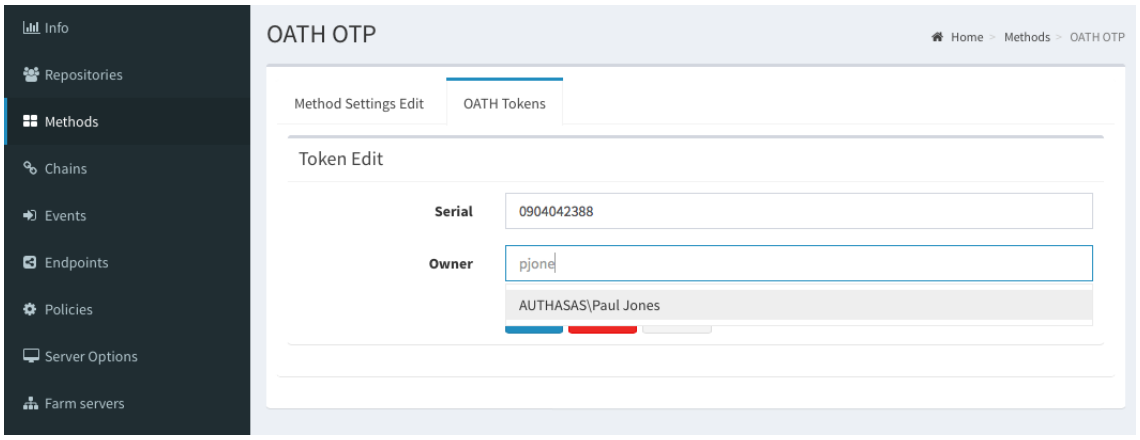
5. It's possible to add the encrypted PSKC files. For the case switch *PSKC file encryption type* from Not Encrypted to *Password* or *Pre-shared key* and provide the information.
6. Click *Upload* to import tokens from the file.



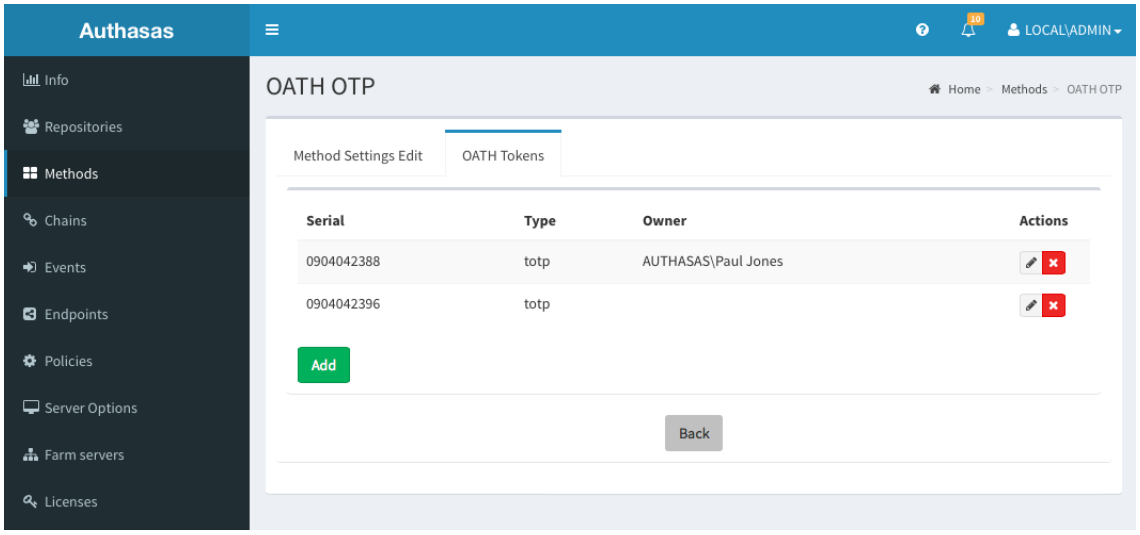
NOTE: NetIQ Advanced Authentication gets an *OTP format* from the imported tokens file and stores the information in the enrolled authenticator. So it's not required to change the default common value of OTP format on the *Method Settings Edit* tab.

When the tokens are already imported you see the list and it's required to assign the tokens to users. If can be done in two ways:

1. Click *Edit* button next to token and select *Owner*. Click *Save* button to apply the changes.



2. A user can enter the token's serial number during enrollment in the NetIQ Advanced Authentication Self-Service Portal.



Format of CSV file which is supported for import of OATH compliant tokens

A CSV file which is importing as *OATH csv* file type in (NetIQAdvanced Authentication Administrative Portal - *Methods* - *OATH OTP* - *OATH Tokens* tab) should fields with the following parameters:

- token’s serial number,
- token’s seed
- a type of the token: TOTP or HOTP (optional, by default HOTP)
- OTP length (optional, by default 6 digits)
- time step (optional, by default 30 seconds)

Comma is a delimiter.

Example of CSV:

```
Token001, 15d2fa517d3c6b791bd4cc2044c241429307001f
Token002, 8c557fc050721037fd31e1d3345b5d3263263e0f, totp, 8
Token003, 658208efea5ac49d5331ba781e66f2c808cccc8e, hotp, 6
Token004, 89f0dfe1c90379da6a11aaca2fc1070f606efe36, totp, 6, 60
```

IMPORTANT: For the *YubiKey* tokens it's required to use *Traditional format* of the CSV (check *YubiKey Personalization Tool* - *Settings* tab - *Logging Settings*). Use *Yubico csv* file type (NetIQ Advanced Authentication Administrative Portal - *Methods* - *OATH OTP* - *OATH Tokens* tab).

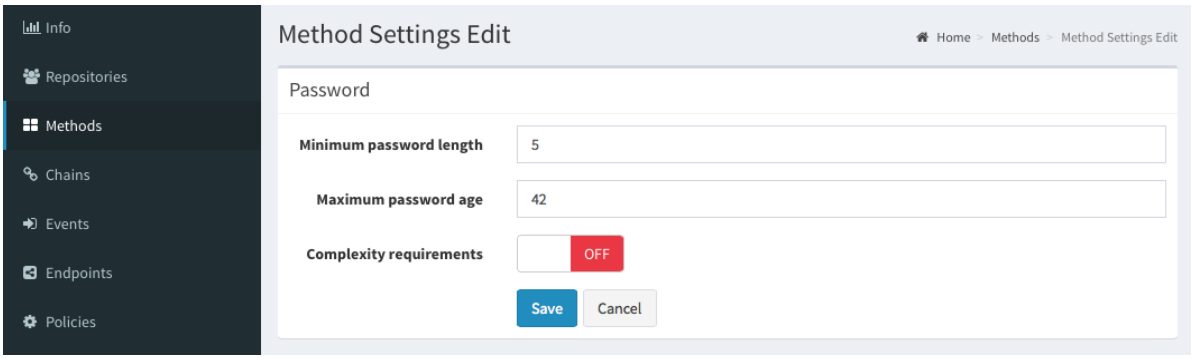
4.5.9 Password

The settings allows to configure security options for passwords stored in the appliance. They are applied, for example, for the appliance administrator and other local accounts.

NOTE: It's not recommended to use the Password method in chains which contain one factor. It's secure to combine it with other factors.

It's possible to manage the following settings:

1. *Minimum password length*.
2. *Maximum password age*. 42 days by default. It means the password will expire in 42 days. If it's set to 0 the password will not expire.
3. *Complexity requirements*. The option is disabled by default. If it's enabled the password must complain at least 3 of 4 checks:
   - it should contain at least one uppercase character,
   - it should contain at least one lowercase character,
   - it should contain at least one digit,
   - it should contain at least one special symbol.



IMPORTANT: Notifications about expiring passwords are not yet supported in v5.2. So the local administrator will not be able to sign-in to the NetIQ Advanced Authentication Administrative Portal and users who use the method will not be able to authenticate after the password expiration. To fix it the administrator/user should go to the Self-Service Portal and change his/her password.

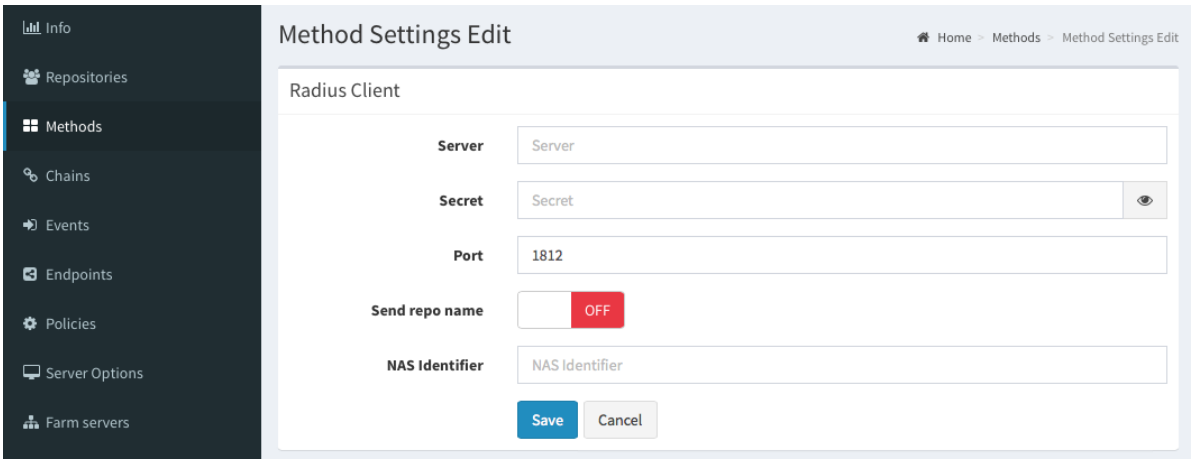
4.5.10 Radius Client

With the Radius Client Authentication Method the authentication framework will forward the authentication request to a third party RADIUS server. This can be any RADIUS server. A specific example of when to use this Authentication Method is if you have a working token solution like RSA, or Vasco and want to migrate your users to the Advanced Authentication framework. Some users will be able to still use the old tokens and new users can use any of the other supported Authentication Methods.

To use this method you will need to create an RADIUS Client on the third party RADIUS server with the hostname of IP address of this appliance. If you have multiple appliances you should add them all as RADIUS Clients.

The following configuration options are available:

- *Server*: the hostname or IP address of the third party RADIUS server.
- *Secret*: shared secret between the RADIUS server and the Authentication Framework.
- *Port*: port to where the RADIUS authentication request is sent. The default is 1812.
- *Send repo name*. If it's enabled, a repository name will be automatically used with a username. For example, company\pjones
- *NAS Identifier*, the attribute is optional.



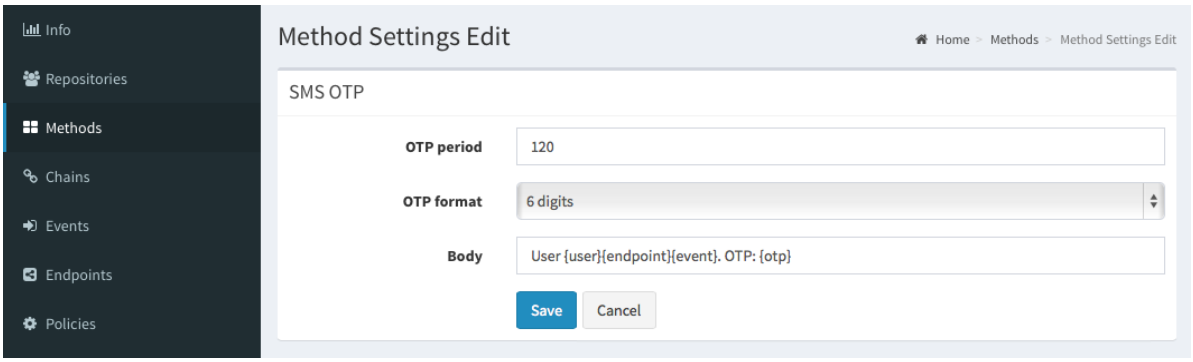
4.5.11 SMS OTP

The SMS OTP authentication method will send an SMS text to the user's mobile phone with a One-Time-Password (OTP). The user will receive this OTP and needs to enter it on the device where the authentication is happening. This authentication method is best used with a second method like Password or LDAP Password in order to achieve multi-factor authentication and to prohibit malicious users from sending SPAM a user's phone with authentication requests.

The following configuration options are available:

- *OTP Period*: the lifetime of an OTP token in seconds. By default 120 seconds.
- *OTP Format*: the length of an OTP token. By default 8 digits.
- *Body*: the text in the SMS that is sent to the user. The following variables can be used:
  - {user} - the username of the user
  - {endpoint} - the device the user is authenticating to

- {event} - the name of the event where the user is trying to authenticate to
- {otp} - this is the actual One-Time-Password



4.5.12 Security Questions

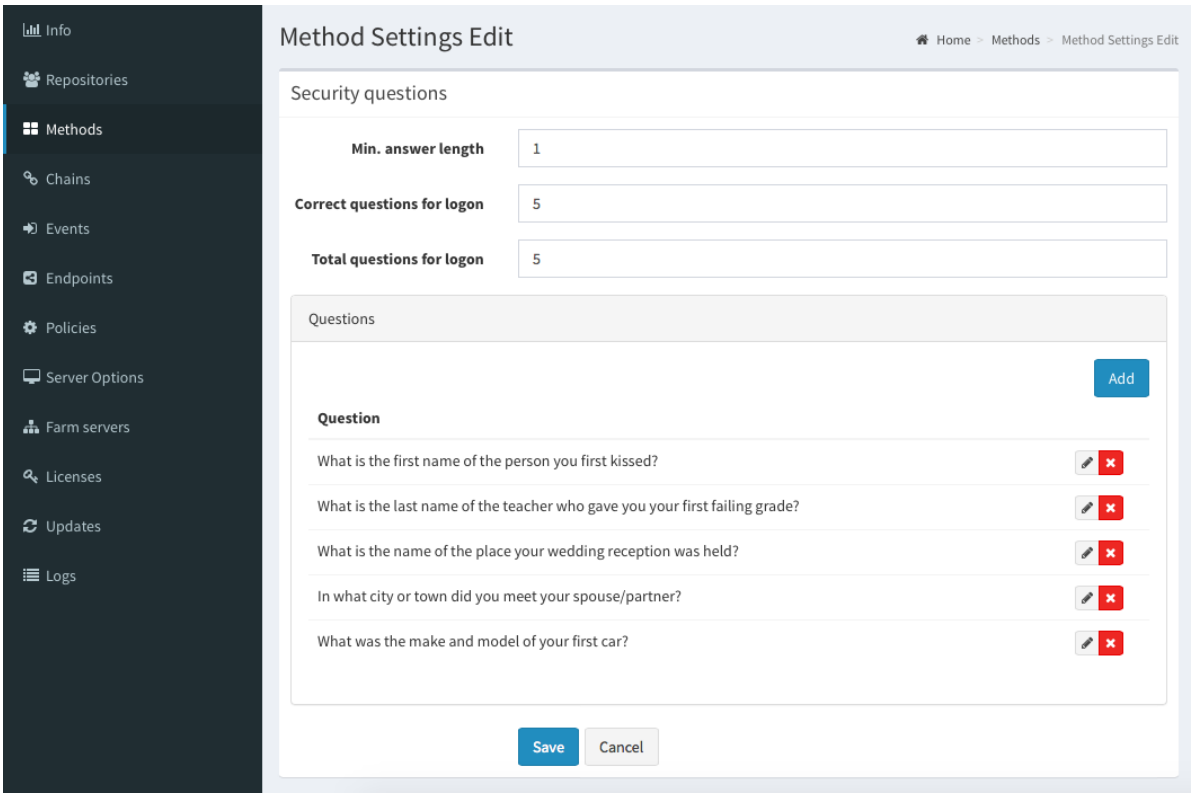
This Authentication Method is mostly used in fall-back scenarios where a user does not have access to his normal strong authentication method. The authentication method works in such a way that a user needs to answer a series of questions that are pre-defined in this configuration section. When the user tries to authenticate using the Security Questions he or she will be provided with a random set out of these pre-defined questions. By answering the questions correctly the user will get access. Below you can configure how many of the answers should be correct before the user gains access.

IMPORTANT: This authentication method is not seen as secure and if possible should not be used.

When you decide to use this Authentication Method please follow some guidelines.

It is essential that we use good questions. Good security questions meet five criteria. The answers to a good security question are:

1. *Safe*: cannot be guessed or researched
2. *Stable*: does not change over time
3. *Memorable*: can be remembered
4. *Simple*: is precise, easy, consistent
5. *Many*: has many possible answers



Some examples of good, fair, and poor security questions according to goodsecurityquestions.com are given below. For a full list please visit this website.

GOOD

What is the first name of the person you first kissed?

What is the last name of the teacher who gave you your first failing grade?

What is the name of the place your wedding reception was held?

In what city or town did you meet your spouse/partner?

What was the make and model of your first car?

FAIR

What was the name of your elementary / primary school?

In what city or town does your nearest sibling live?

What was the name of your first stuffed animal, doll, or action figure?

What time of the day were you born? (hh:mm)

What was your favorite place to visit as a child?

POOR

What is your pet's name?

In what year was your father born?

In what county where you born?

What is the color of your eyes?

What is your favorite _____?

The following configuration options are available:

- Min. answer length: the minimum number of characters an answer should consist of.
- Correct questions for logon: the number of questions a user should answer correctly to get access.
- Total questions for logon: the number of questions the user needs to answer.

So when Correct questions for logon is set to 3 and the Total questions for logon is set to 5 then the user only needs to enter 3 correct questions out of a set of 5.

4.5.13 Smartphone

The Smartphone authentication method uses an app on your smartphone to do out-of-band authentication. This means that the authentication is happening over a different channel than the initiating authentication request.

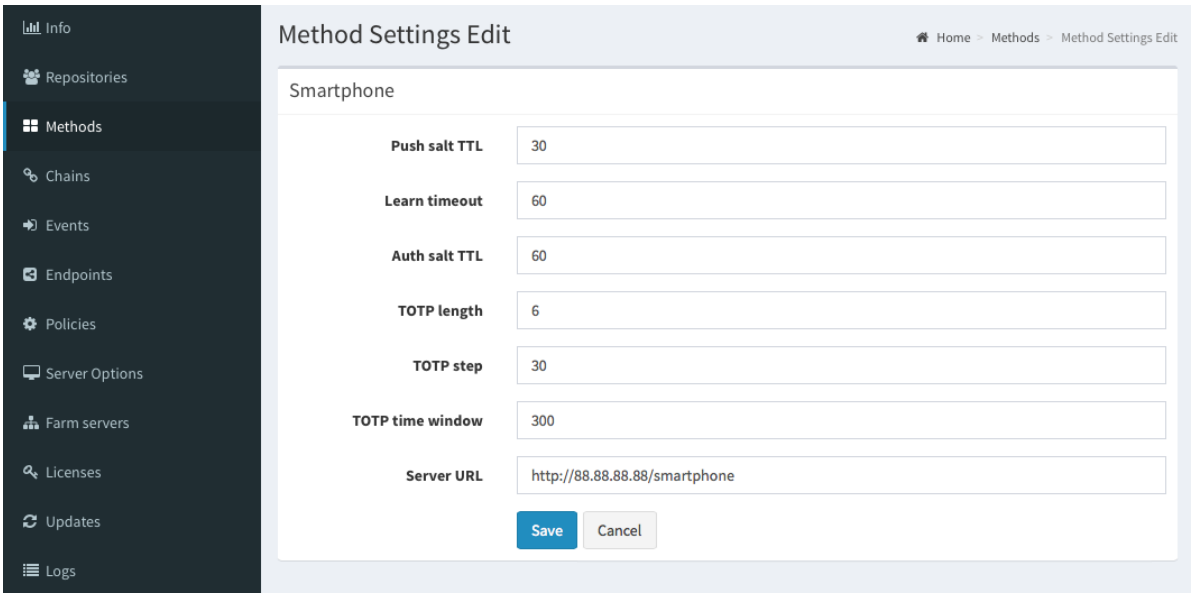
For example, if you are logging into a website, then the Smartphone authentication method will send a push message to your mobile phone. When opening the NetIQ Advanced Authentication Framework app the user will be presented with an Accept and a Reject button where he can decide what to do. If the user pushes the Accept button the authentication request will be sent over the mobile network (secure) back to the Authentication framework. Without typing over an OTP code the user will be granted access.

When the smartphone doesn't have a data connection, a backup OTP authentication can be used.

This Authentication Method is best used in combination with another method like Password or LDAP Password in order to achieve multi factor authentication and protect the user from getting SPAM push messages.

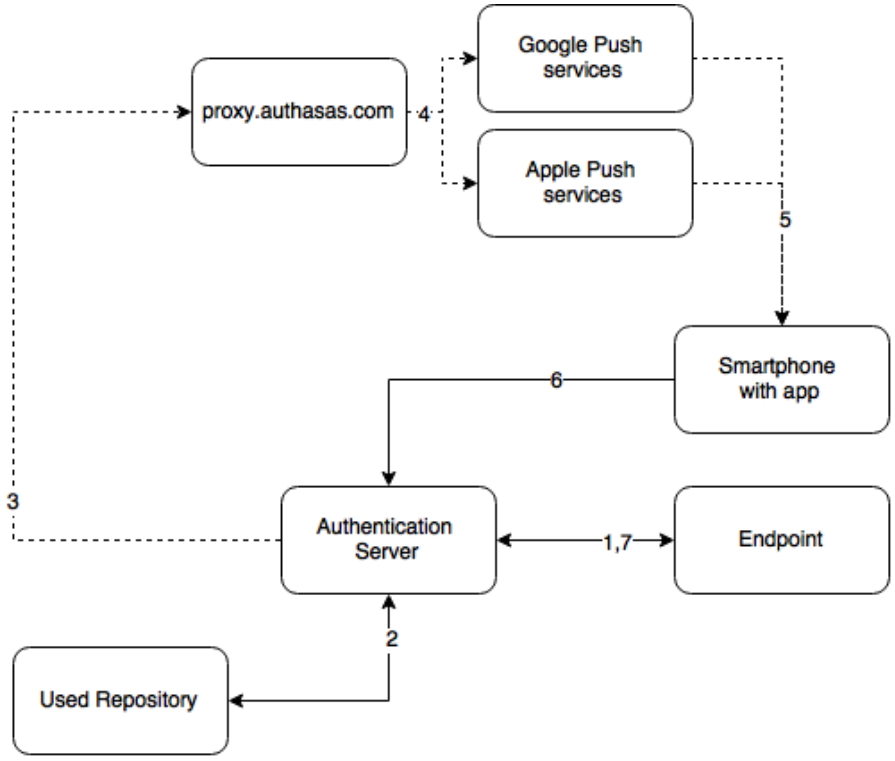
The following configuration options are available:

- *Push salt TTL*: the lifetime of an authentication request sent to the smartphone.
- *Learn timeout*: the time the QR code used for enrolment is valid for the user to scan.
- *Auth salt TTL*: the lifetime in which the out-of-band authentication needs to be accepted before authentication fails.
- *TOTP Length*: the length of the OTP token used for backup authentication
- *TOTP step* : the time a TOTP is shown on screen before the next OTP is generated. Default 30
- *TOTP time window*: the time in seconds in which the TOTP entered is accepted. Default 300
- *Server URL*: URL to where the smartphone app will connect for authentication. Please use http only for testing and use https in a production environment. You will need a valid certificate when using https.



Authentication flow

The following chart demonstrates the authentication flow:



A user is authenticating on endpoint (which can be the user's laptop with NetIQ Windows Client installed or a website etc.) by Smartphone method.

1. The endpoint calls the NetIQ Advanced Authentication Server.
2. It validates the provided user's credentials.
3. NetIQ Advanced Authentication Server sends a push message to proxy.authasas.com.

4. It defines an appropriate push service for the using smartphone platform and forwards the push message to it.
5. The push message will be delivered to the user's smartphone. This is not required for a successful authentication and is only to inform the user.
6. When the user opens the app, the app checks at the NetIQ Advanced Authentication Server if there is an authentication needed. If this is the case it will show the Accept and Reject buttons. This answer is send to the server.
7. NetIQ Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTPS protocol is used for the communication.

Access configuration

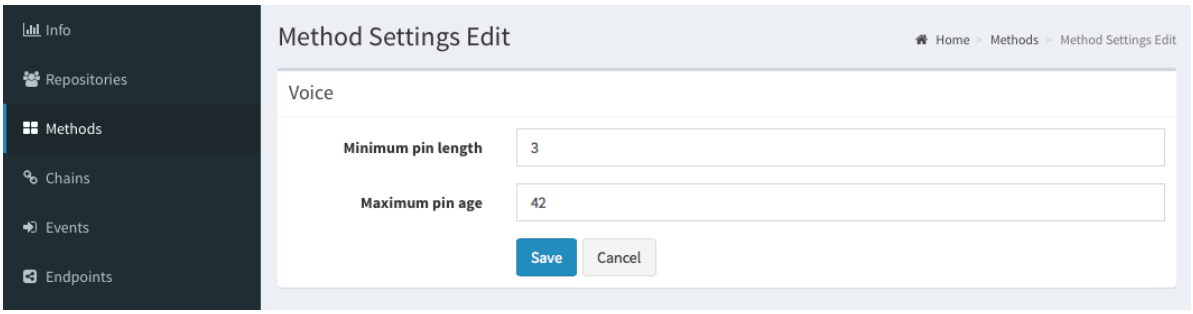
- NetIQ Advanced Authentication Server must be accessible by the specified *Server URL* address from smartphones (HTTPS, outbound).
- NetIQ Advanced Authentication Server must have a permitted outbound connection to proxy.authasas.com (HTTPS).

4.5.14 Voice Call

The section contain security settings for Voice Call authentication method. NetIQ Advanced Authentication will call user and the user will need to enter a pin code, which should be predefined in NetIQ Advanced Authentication Self-Service Portal during the authenticator enrollment.

It's possible to manage the following settings:

1. *Minimum pin length*. 3 digits by default. Usage of shorter pins is not allowed.
2. *Maximum pin age*. 42 days by default. It means that the pin will expire in 42 days and will need to be changed in the NetIQ Advanced Authentication Self-Service Portal. If it's set to 0 the pin will not expire.



IMPORTANT: Notifications about expiring pins are not yet supported in v5.2.

4.5.15 Creating Chain

Authentication chains are combinations of authentication methods. Users will need to pass all methods in order to be successfully authenticated.

So when you create a chain that has LDAP Password and SMS in it then the user will first need to enter their LDAP Password. When this is correct the system will send an SMS with a One-Time-Password to the mobile phone of the user and the user will need to enter the correct OTP in order to be authenticated.

It is possible to create any chain you want. For highly secure environments you can assign multiple methods to one chain to achieve better security.

Authentication can consist of 3 different factors. These are:

1. *Something you know*: password, PIN, security questions
2. *Something you have*: smartcard, token, telephone
3. *Something you are*: biometrics like fingerprint or iris

Something is seen as Multi-Factor or Strong Authentication when 2 out of the 3 factors are used. So a password with a token, or a smartcard with a fingerprint are seen as multi-factor. A password and a PIN is not seen as multi-factor as they are in the same area.

Authentication chains are linked to user groups in your repositories. You can allow only a certain group to be able to use the specific authentication chain.

To create a new chain or edit an existing one that NetIQ authentication framework will work with, follow the steps:

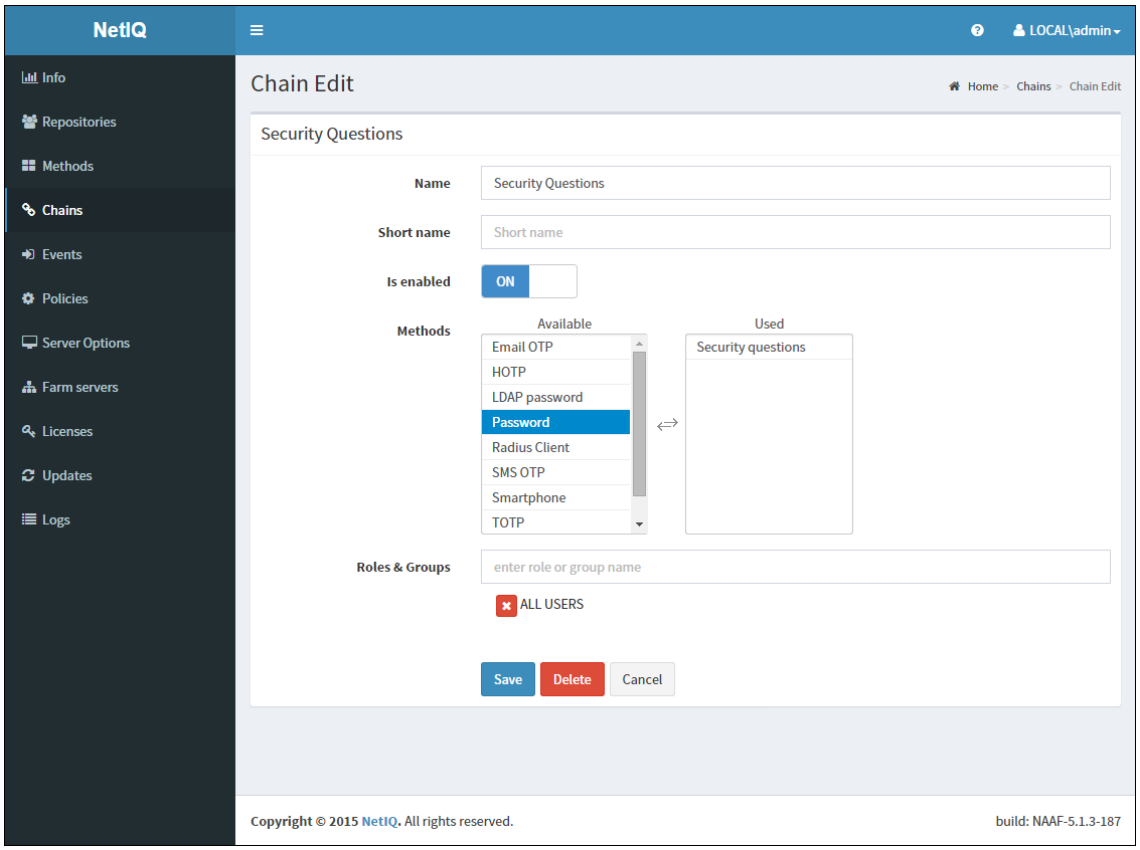
1. Open the *Chains* section.
2. Click the *Add* button at the bottom of the *Chains* view to create a new authentication chain (or click the *Edit* button next to an applicable authentication chain).
3. Specify a name of the Chain in the *Name* text field.
4. Specify a *Short name*. The short name used by a user to switch to this chain. For example, if you call LDAP Password & SMS chain "sms" then a user can type in "<username> sms" and he will be forced to use SMS as the chain. This can be helpful in cases when the primary chain is not available.
5. Select whether the current authentication chain is available for use or not available by clicking the *Is enabled* toggle button.
6. The *Methods* section allows to setup a prioritized list of authentication methods. For example, an LDAP Password+ HOTP method first asks the user for the LDAP password and after that for his OTP code. HOTP + LDAP Password first asks for the OTP code and then for the LDAP password.
7. Specify groups that will be allowed to use the current authentication chain in the *Roles & Groups* text field.

   IMPORTANT: It's not recommended to use the groups from which you will not be able to exclude users (like `All Users` group in Active Directory), because you will not be able to free up a user's license.

   ---

8. Use the option *Apply if used by endpoint owner* if the Chain should be used only by Managing Endpoints.

9. Click *Save* at the bottom of the *Chains* view to save the configuration.



IMPORTANT: If you have configured more than one chain using one method (e.g. "LDAP Password", "LDAP Password+Smartphone") and assigned it to the same group of users and the same Event, the top chain will be always used if the user has all methods in the chain enrolled.

4.5.16 Configuring Events

Here you can configure the supported applications / events to where the NetIQ Advanced Authentication server will authenticate. The following predefined events are available.

AdminUI

This event is used for accessing this Administrative Portal. You can configure which chains can be used to get access to /admin.

Authentication Management

This event configures the chains that can be used to access the Self-Service Portal. Users can enroll any of the methods that are configured for any chain they are a member of the group assigned to the chain.

You may post a LDAP Password chain to the bottom of the used chains list to secure access to the portal for users who already has enrolled methods.

Helpdesk

This event is used for accessing the Helpdesk Portal by security officers.

MacOS logon

This event configures the chains that can be used to log on in Apple Mac OS.

NAM

The NetIQ Advanced Authentication server supports integration with NetIQ Access Manager (https://www.netiq.com/products/access-manager/). NetIQ Access Manager Advanced Authentication plugin must be installed and configured on a NAM appliance and User Stores must be added for the used repositories.

NCA

The NetIQ Advanced Authentication server supports integration with NetIQ CloudAccess (https://www.netiq.com/products/cloudaccess/). CloudAccess must be configured to use NetIQAdvanced Authentication as an authentication card and User Stores must be added for the used repositories. Check the NetIQ CloudAccess documentation.

Radius Server

The NetIQ Advanced Authentication server contains a built-in RADIUS server that is able to authenticate any RADIUS client using one of chains configured for the event.

Windows logon

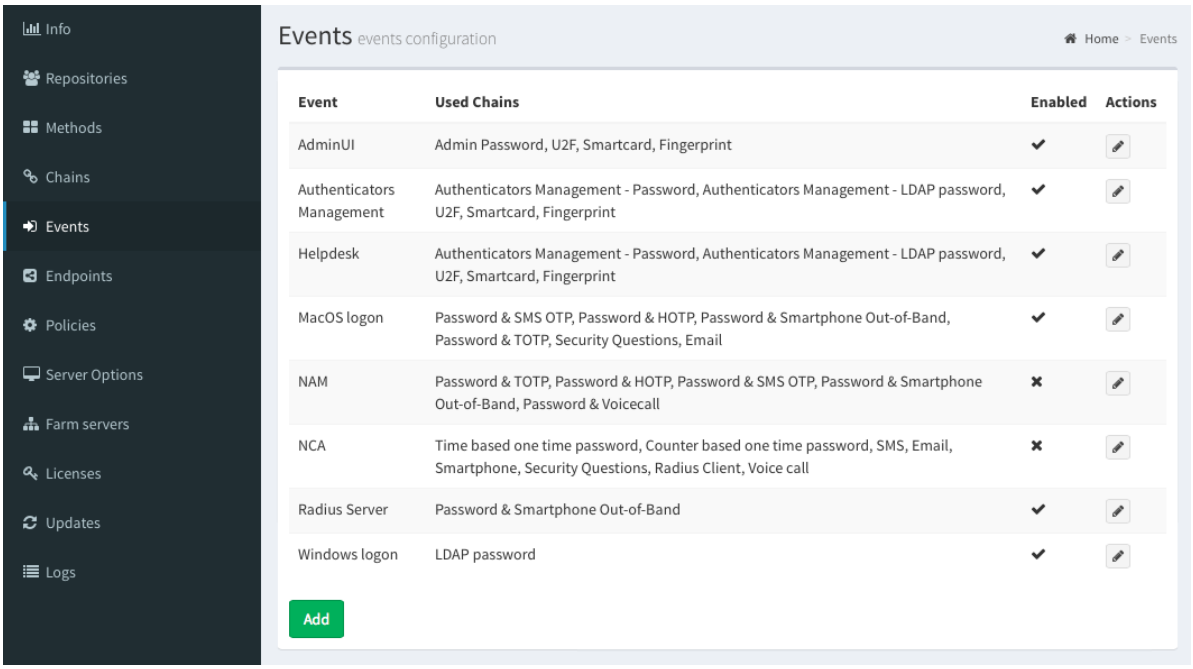
This event configures the chains that can be used to log on in Microsoft Windows.

In an event you can configure a prioritized list of chains that can be used to get access to that specific event.

To configure an authentication event for NetIQ Advanced Authentication framework, follow the steps:

1. Open the *Events* section.
2. Click the *Edit* button next to an applicable event.
3. Select whether the current event is enabled or disabled by clicking the *Is enabled* toggle button.
4. Select chains that will be assigned to the current event.
5. Select required endpoints from *Endpoint whitelists*.
6. Click *Save* at the bottom of the *Events* view to save configuration.

If you need to revert the changes to defaults use the *Initialize default chains* button.



TIP: It's recommended to have a single chain with Emergency Password method at a top of the Used chains list in Authenticators Management event and other events which are used by users. The chain will be ignored while user doesn't have the Emergency Password enrolled. The user will be able to use the Emergency Password immediately when security officer enrolled the user the Emergency Password authenticator.

4.5.17 Radius Server

The NetIQ Advanced Authentication server contains a built-in RADIUS server that is able to authenticate any RADIUS client using one of chains configured for the event.

IMPORTANT: Currently the built-in RADIUS Server supports only PAP.

The RADIUS Server supports all authentication methods except Card, FIDO U2F, Fingerprint.

The RADIUS Server works only on DB Master Server.

To configure an authentication event for NetIQ Advanced Authentication framework, follow the steps:

1. Open the *Events* section.
2. Click the *Edit* button next to the Radius Server event.
3. Ensure that the event has *Is enabled* option set to ON.
4. Select chains that will be assigned to the event*.
5. Select Radius from *Endpoint whitelists*.
6. Click *Add* button to add a Radius Client assigned to the event:
   - Specify the Radius Client name in the *Name* text field.
   - Enter an *IP address* of the Radius Client.
   - Enter the Radius Client *Secret* and *Confirmation*.

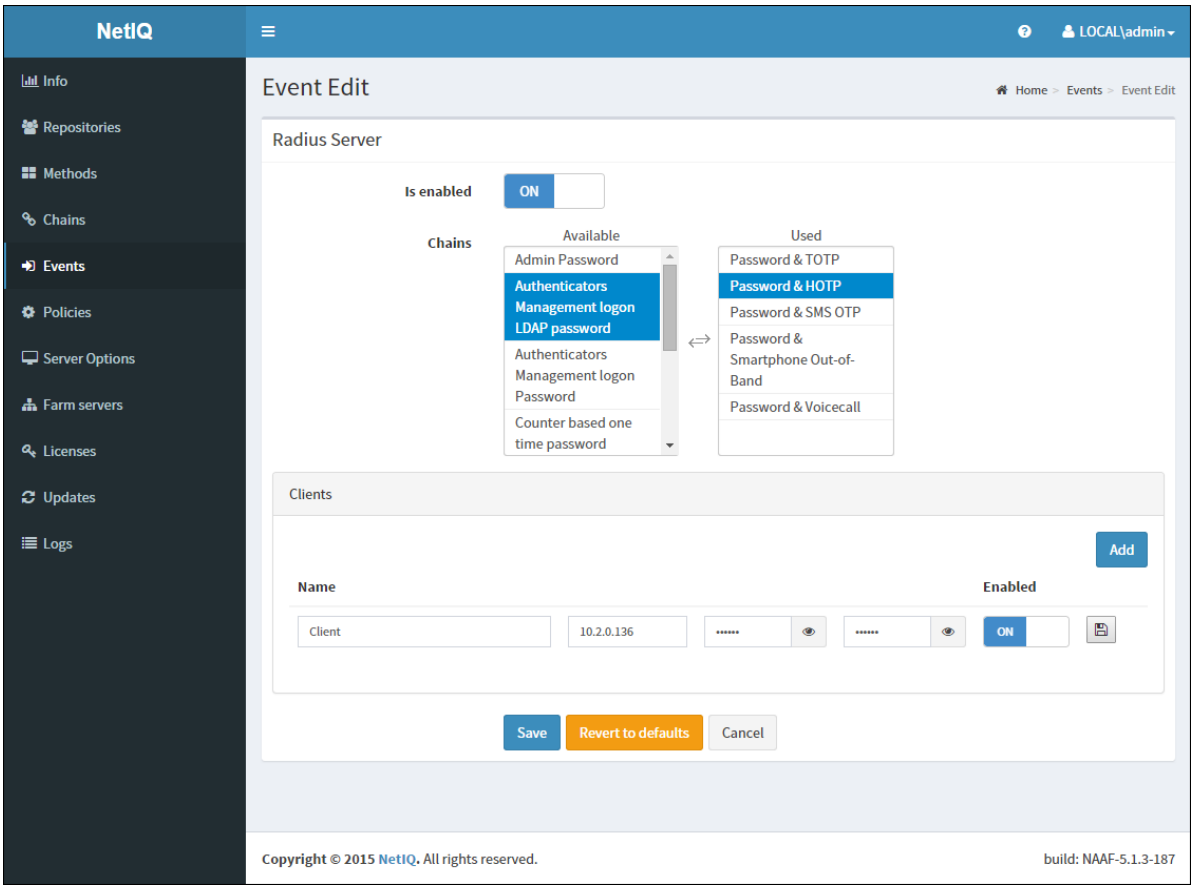
- Ensure that the Radius Client is set to *ON*.
- Click the save button next to the Radius Client.
- Add more Radius Clients if necessary.

7. Click *Save* at the bottom of the *Events* view to save configuration.

IMPORTANT: When you specify more than one Chain to use with the Radius Server, follow one of the described ways:

---

1. Each assigned Chain of the RADIUS event may be assigned to a different LDAP group. E.g. LDAP Password+Smartphone chain is assigned to a Smartphone users group, LDAP Password+HOTP chain is assigned to a HOTP users group. If a RADIUS user is a member of the both groups, a top group will be used.
2. It's possible to use the RADIUS authentication using any Chain when entering `<username> <chain shortname>` in username field. E.g. `pjones sms`. Ensure that you have the short names specified for the used Chains. Usage of the option may be not admissible in your RADIUS client (like in FortiGate).



IMPORTANT: If you use the `LDAP Password+Smartphone` chain it's possible to use an offline authentication by entering the following data in the password field: <LDAP Password>&<Smartphone OTP>. E.g. Q1w2e3r4&512385. The same use case is supported for LDAP Password+OATH TOTP and LDAP Password+OATH HOTP from v5.2.

NOTE: The Advanced Authentication Framework stores the Radius Event settings only on a server where administrator performs the configuration (usually this is DB Master server). After conversion of DB Slave server to DB Master server the configuration may be lost. Open the Radius Event settings and click Save to apply the configuration.

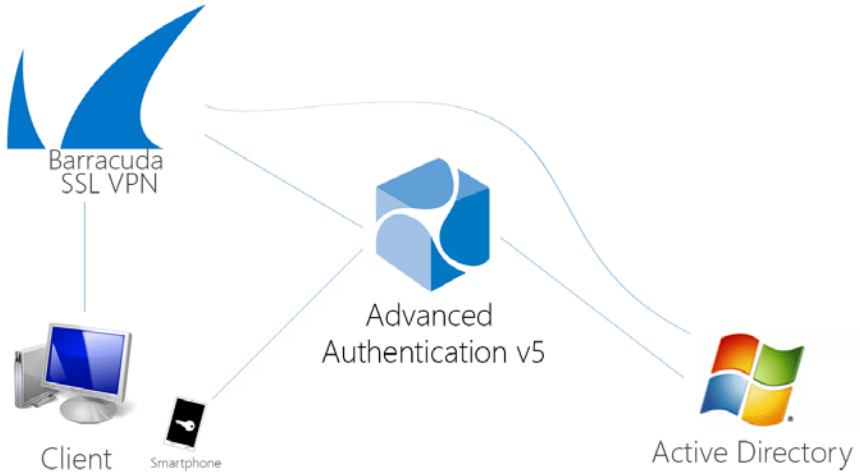
The related articles:

- Configuring integration with Barracuda SSL VPN
- Configuring integration with Citrix NetScaler
- Configuring integration with Dell SonicWall SRA EX-Virtual appliance
- Configuring integration with FortiGate
- Configuring integration with OpenVPN

Configuring integration with Barracuda SSL VPN

These instructions will help you to configure integration of NetIQ Advanced Authentication Framework Appliance Edition with the Barracuda SSL VPN virtual appliance to refuse non-secure passwords in Barracuda SSL VPN connection.

The advanced authentication in Barracuda SSL VPN is represented on the following diagram.



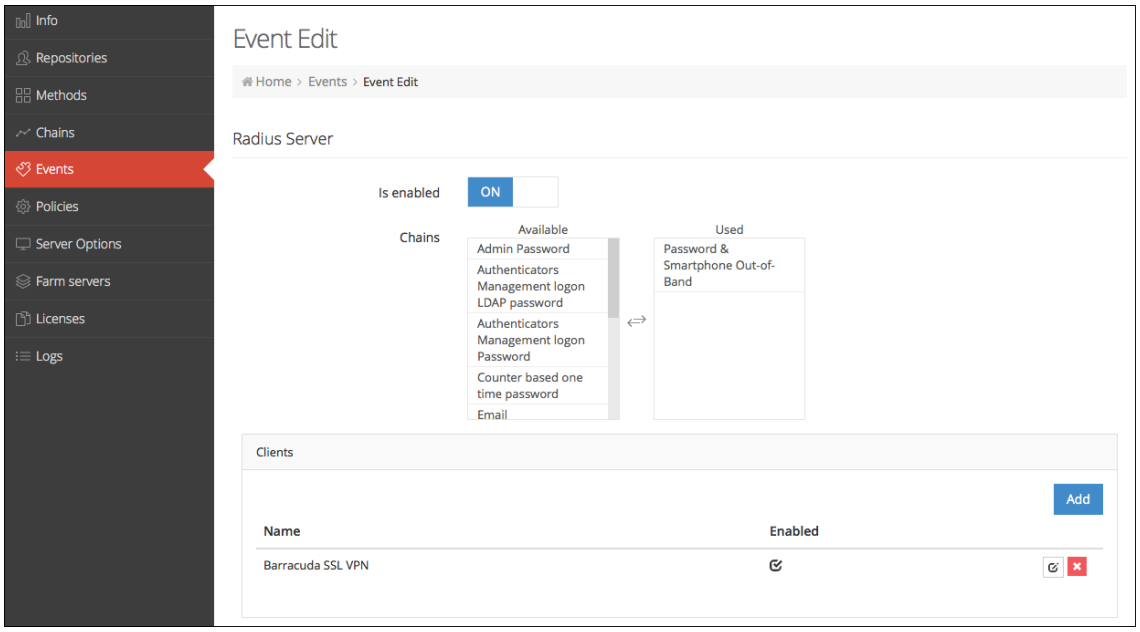
To get started, ensure that you have:

- Barracuda SSL VPN appliance v380 or above (Firmware version 2.6.1.7 was used to prepare these instructions)
- NetIQ v5 appliance (version 5.1.2 was used to prepare these instructions) with the already configured repository

Configure the NetIQ RADIUS server:

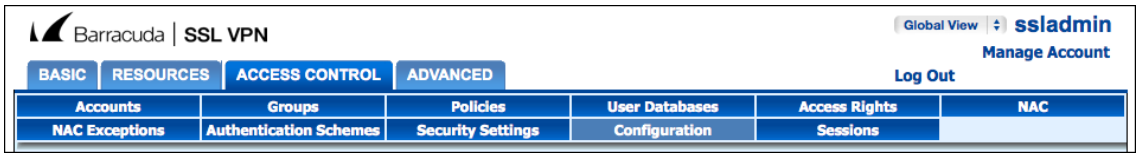
1. Open the NetIQ Admin Interface.
2. Go to the *Events* section.
3. Open properties of the *Radius Server* event.
4. Set the *Radius Server* event to the *ON* mode.

5. Select one or more chains from the list of *Used* chains (make sure that they are enabled and set to the users group in the *Chains* section).
6. Add a *Client*, enter an IP address of the Barracuda SSL VPN appliance, specify a secret, confirm it and set the *Enabled* option.
7. Click the *Save* button in the *Client* string. Click the *Save* button at the bottom of the *Events* view to save changes.

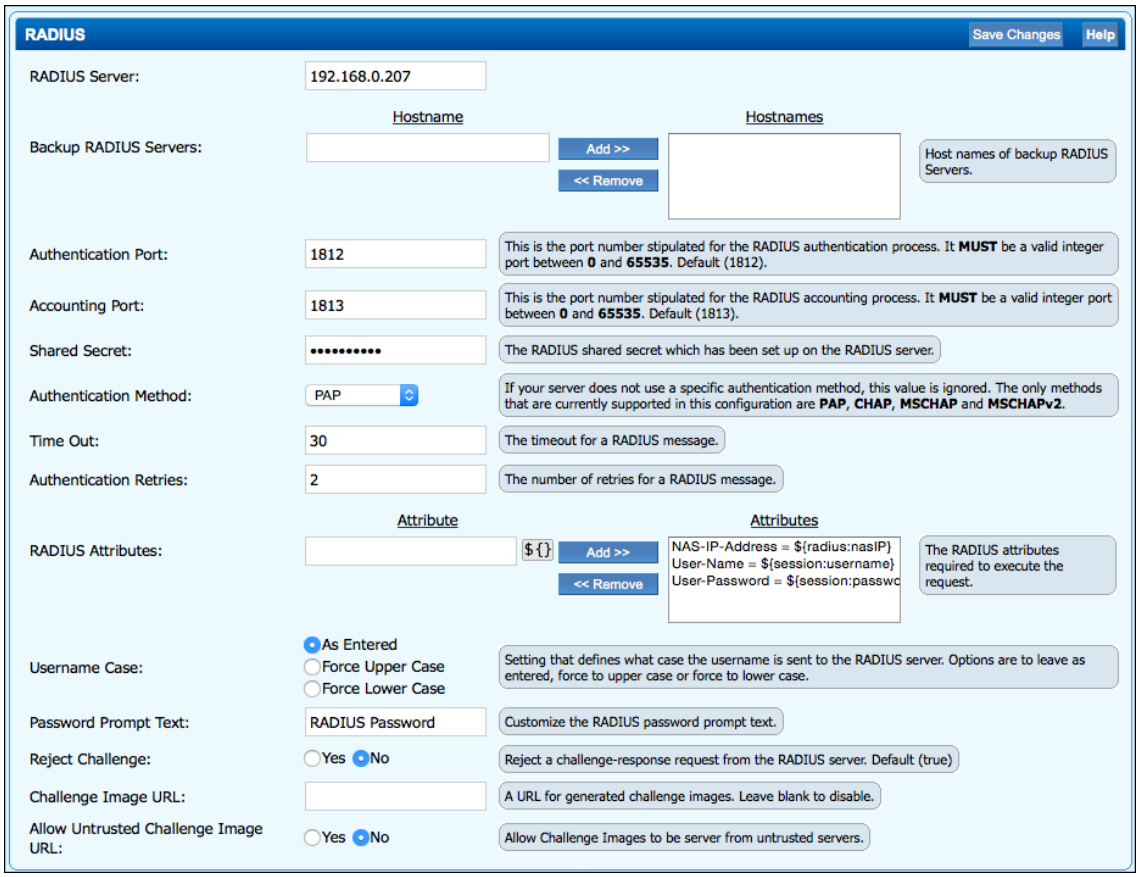


Configure the Barracuda SSL VPN appliance:

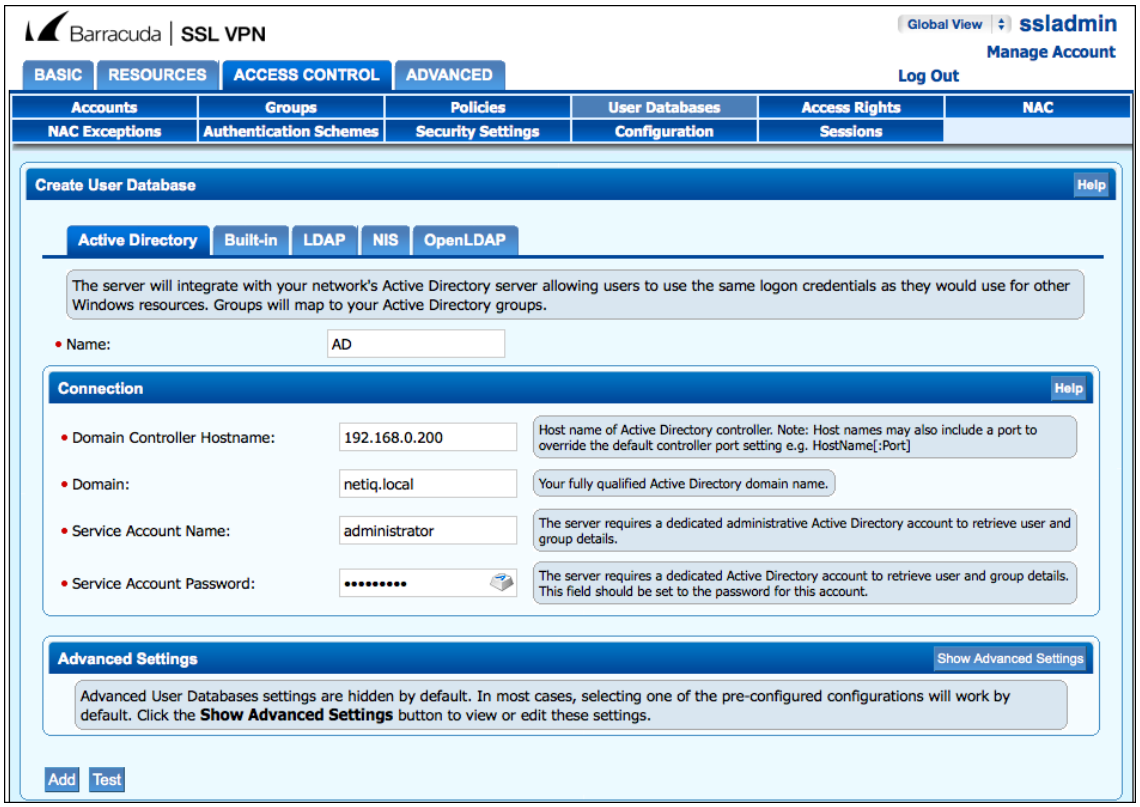
1. Sign-in to the Barracuda SSL VPN Configuration portal as *ssladmin*.
2. Browse menu *Access Control -> Configuration*.



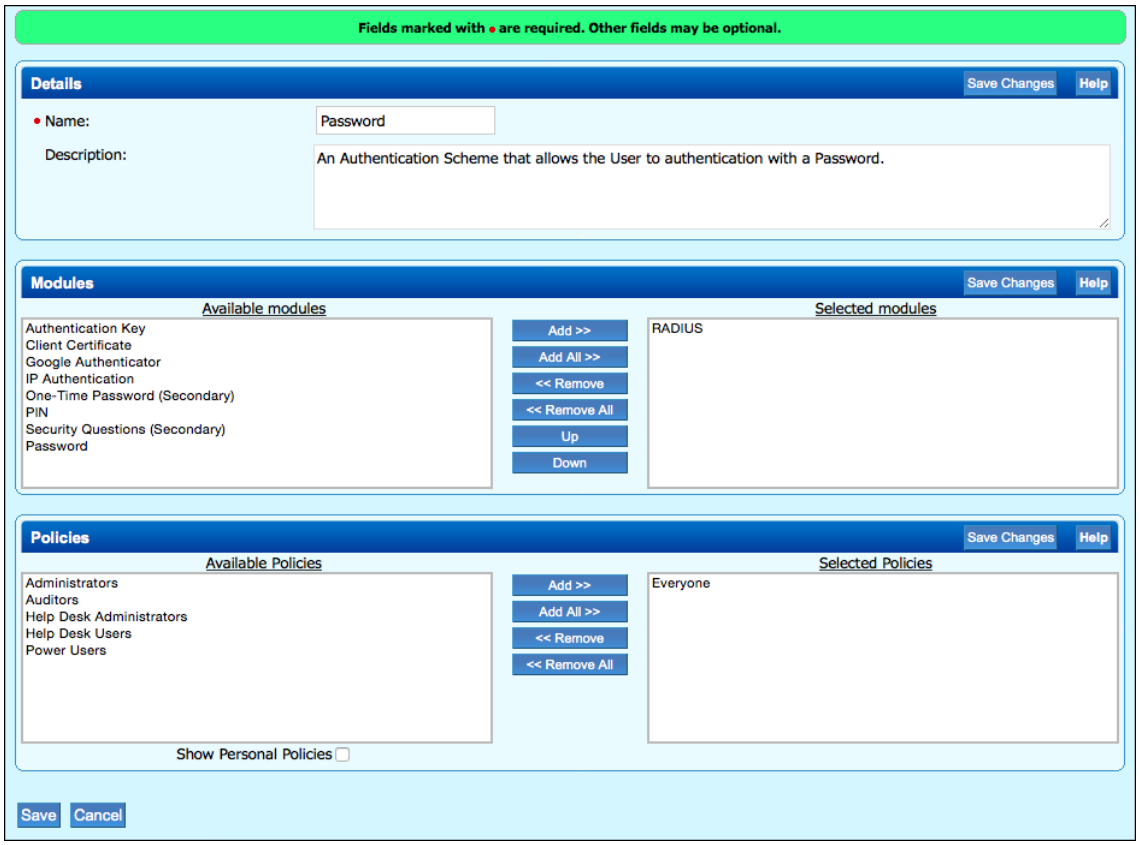
3. Scroll down to *RADIUS* section.
4. Enter NetIQ Advanced Authentication Framework appliance IP address in the *RADIUS Server* text field.
5. Specify a shared secret in the *Shared Secret* text field.
6. Set *Authentication Method* to *PAP*.
7. Set *Reject Challenge* to *No* to allow challenge response.



8. Click *Save Changes*.
9. Switch to *Access Control -> User Databases*.
10. Create User Database using the same storage as you are using in the NetIQ Advanced Authentication Framework.



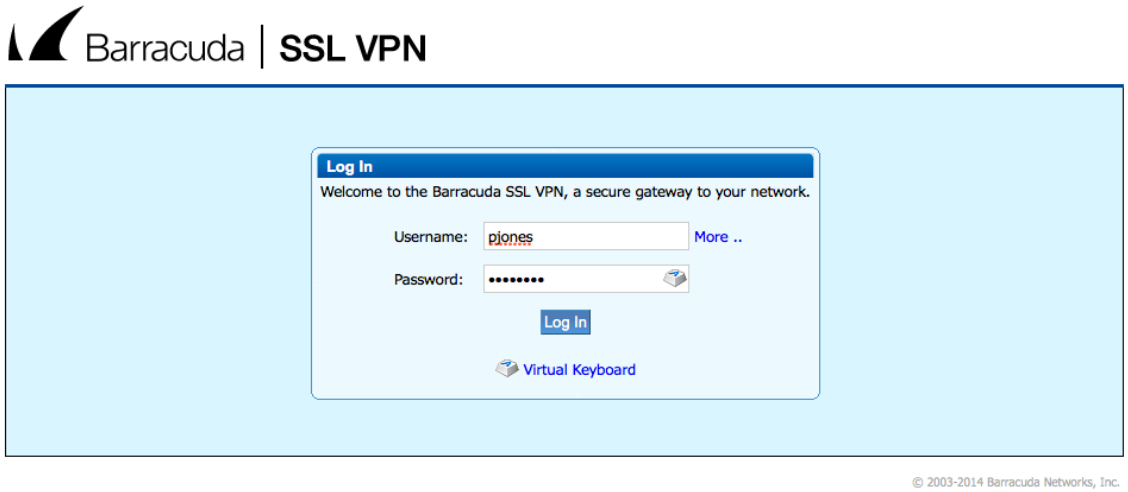
11. Switch to *Access Control - Authentication Schemes*.
12. In the bottom of the view, click *Edit* in front of *Password* scheme for the added User Database.
13. Move *RADIUS* from *Available modules* to *Selected modules*.
14. Remove the *Password* module from the *Selected modules*.



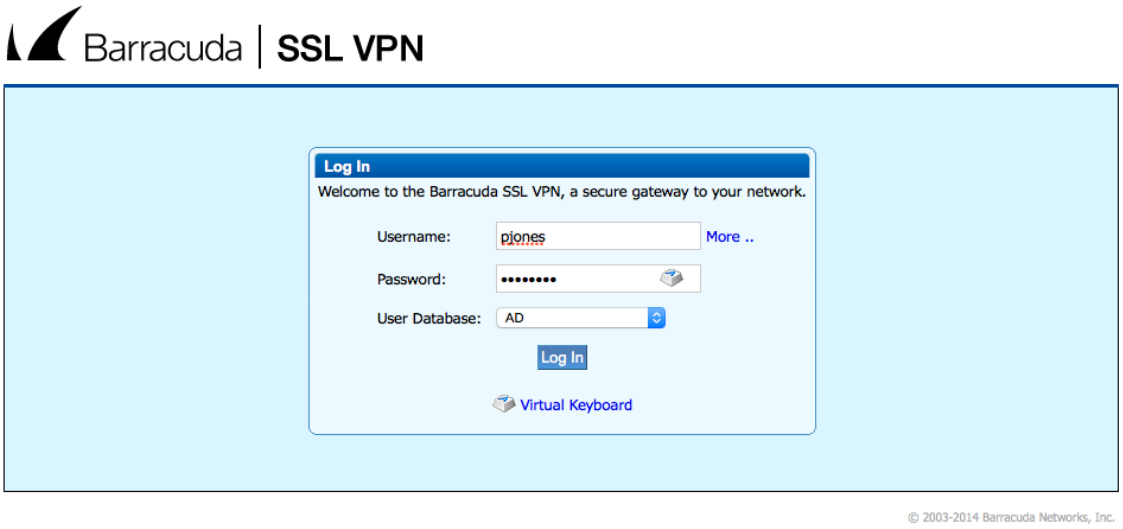
15. Apply the changes.

How to authenticate in Barracuda SSL VPN using the NetIQ Advanced Authentication Framework:

1. Enter user's credentials.



2. Click *More* and select the configured User Database (if the database is not selected by default).



3. Click *Log In* and approve the authentication on the user's smartphone.

NOTE: Advanced authentication can be configured with other authentication chains.

Configuring integration with Citrix NetScaler

These instructions will help you to configure integration of NetIQ Advanced Authentication Framework Appliance Edition with the Citrix NetScaler VPX to refuse non-secure passwords.

The advanced authentication in Citrix NetScaler is represented on the following diagram.

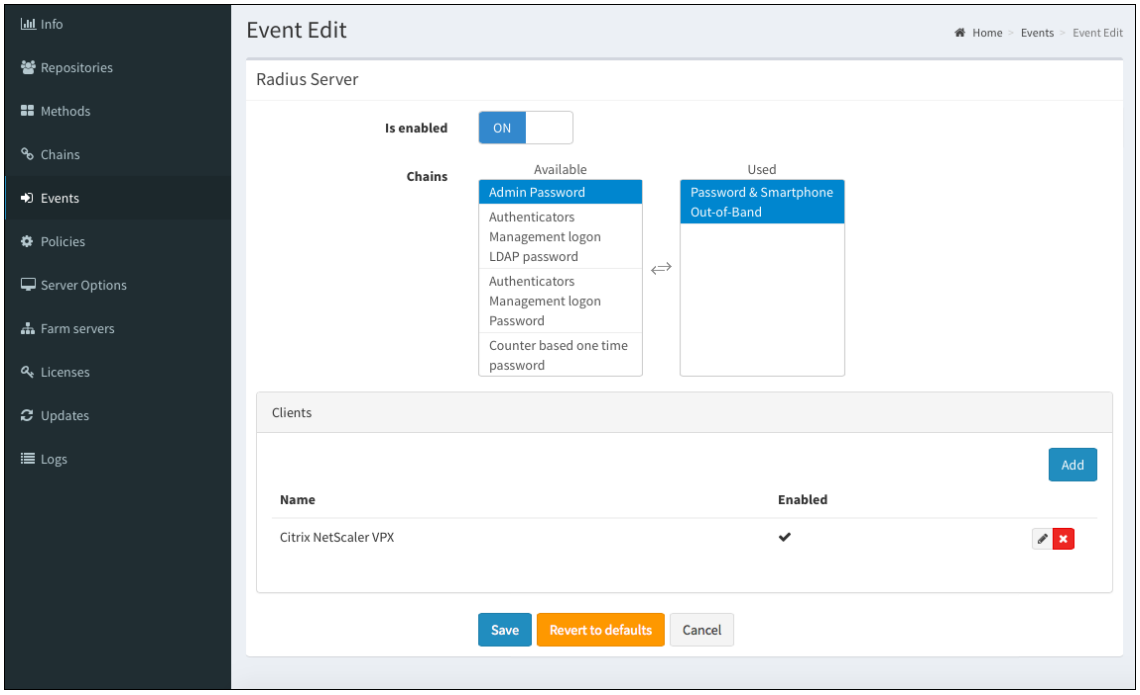
To get started, ensure that you have:

- Citrix NetScaler VPX (version NS11.0 was used to prepare these instructions)
- NetIQ v5 appliance

Configure the NetIQ RADIUS server:

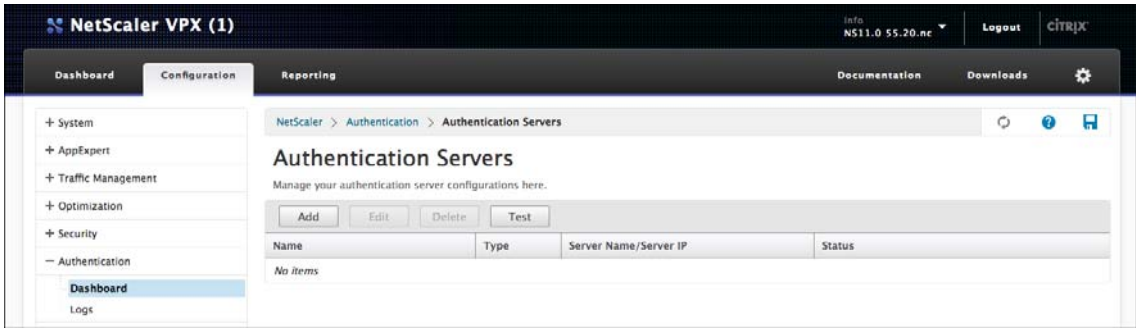
1. Open the NetIQ Admin Interface.

2. Go to the *Events* section.
3. Open properties of the *Radius Server* event.
4. Set the *Radius Server* event to the *ON* mode.
5. Select one or more chains from the list of *Used* chains (make sure that they are enabled and set to the users group in the *Chains* section).
6. Add a *Client*, enter an IP address of the Citrix NetScaler VPX, specify a secret, confirm it and set the *Enabled* option.
7. Click the *Save* button in the *Client* string. Click the *Save* button at the bottom of the *Events* view to save changes.



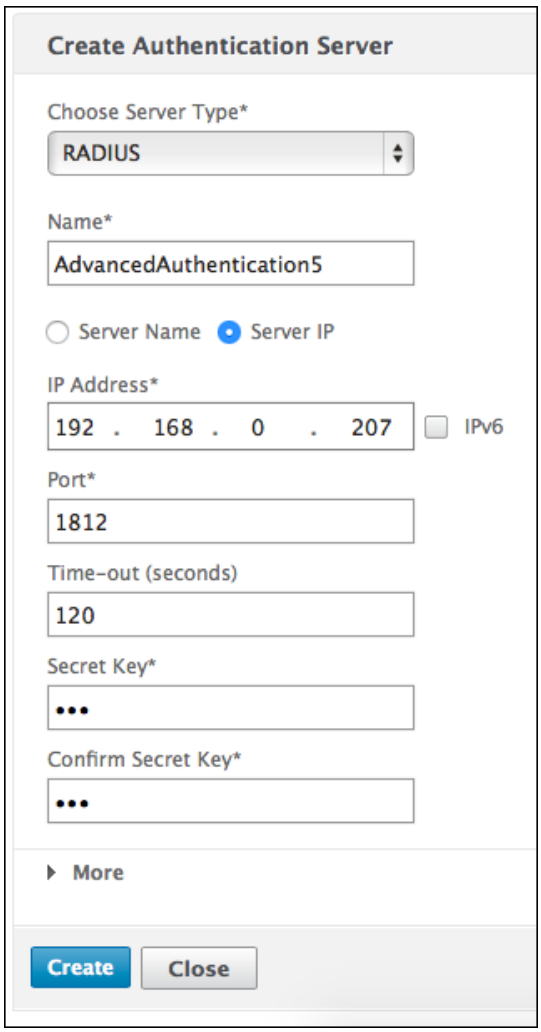
Configure the Citrix NetScaler appliance:

1. Sign-in to the Citrix NetScaler configuration portal as *nsroot*.
2. Browse menu *Configuration -> Authentication -> Dashboard*.



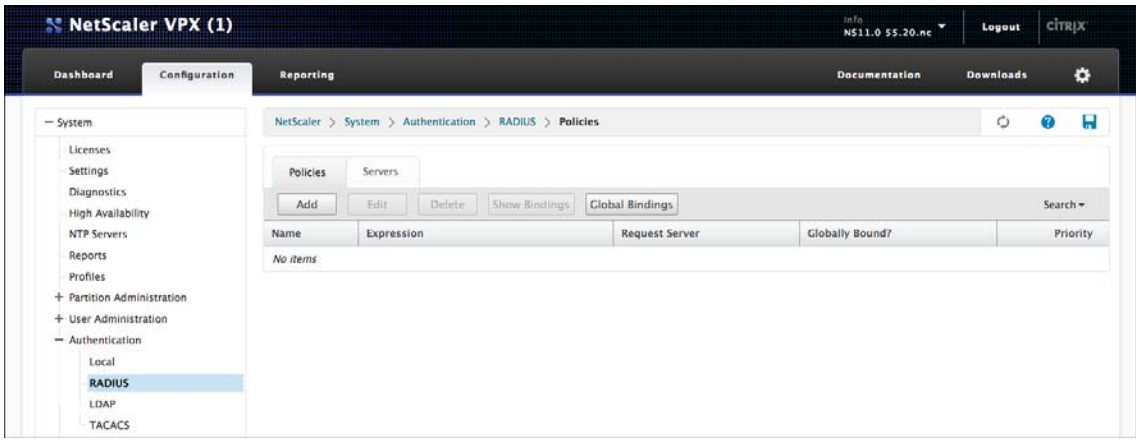
3. Click *Add*.
4. Select *RADIUS* from the *Choose Server Type* dropdown menu.

5. Specify the *Name* of the Advanced Authentication server, its *IP Address*, *Secret Key* and *Confirm Secret Key*, change *Time-out (seconds)* to 120-180 seconds in case of usage of the Smartphone, SMS, Email or Voice Call methods.



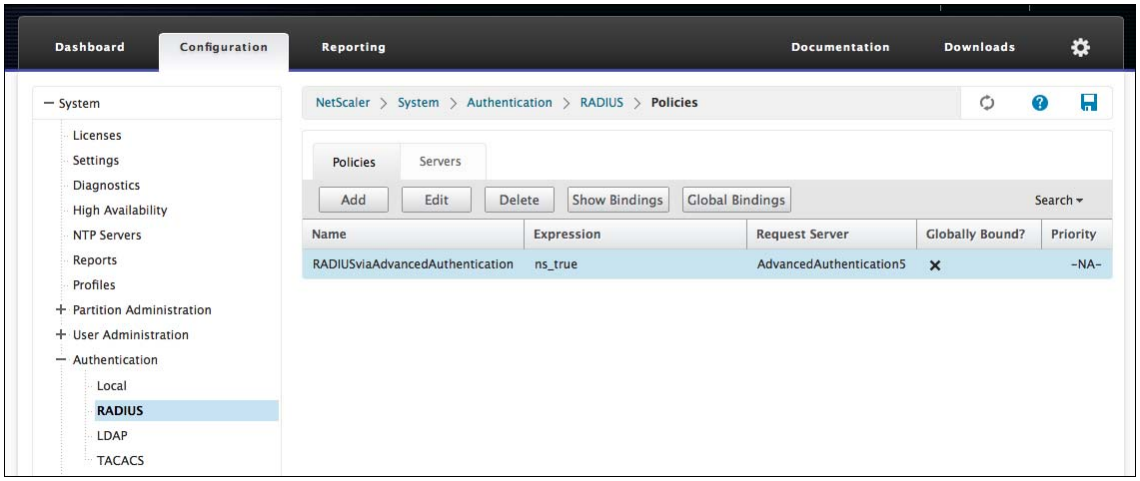
6. Click *More* and ensure that *pap* is selected in the *Password Encoding* dropdown menu.
7. Click *Create*. If connection to the RADIUS server is valid, the *Up* status will be displayed.

8. Browse menu *Configuration -> System -> Authentication -> RADIUS -> Policy*.

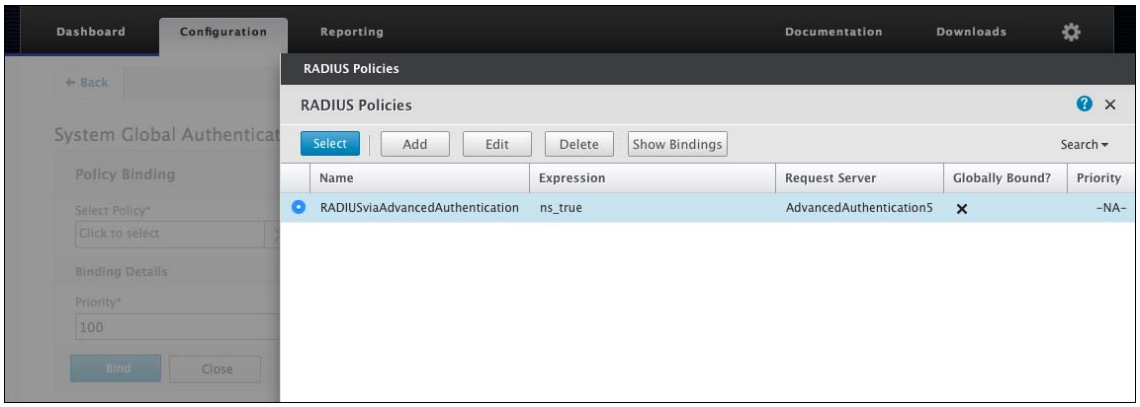


9. Click *Add*.
10. Specify the *Name* of the Authentication RADIUS Policy, select the created RADIUS server from the *Server* dropdown menu, select *ns_true* from the *Saved Policy Expressions* list.

11. Click *Create*.
12. Select the created policy and click *Global Bindings*.



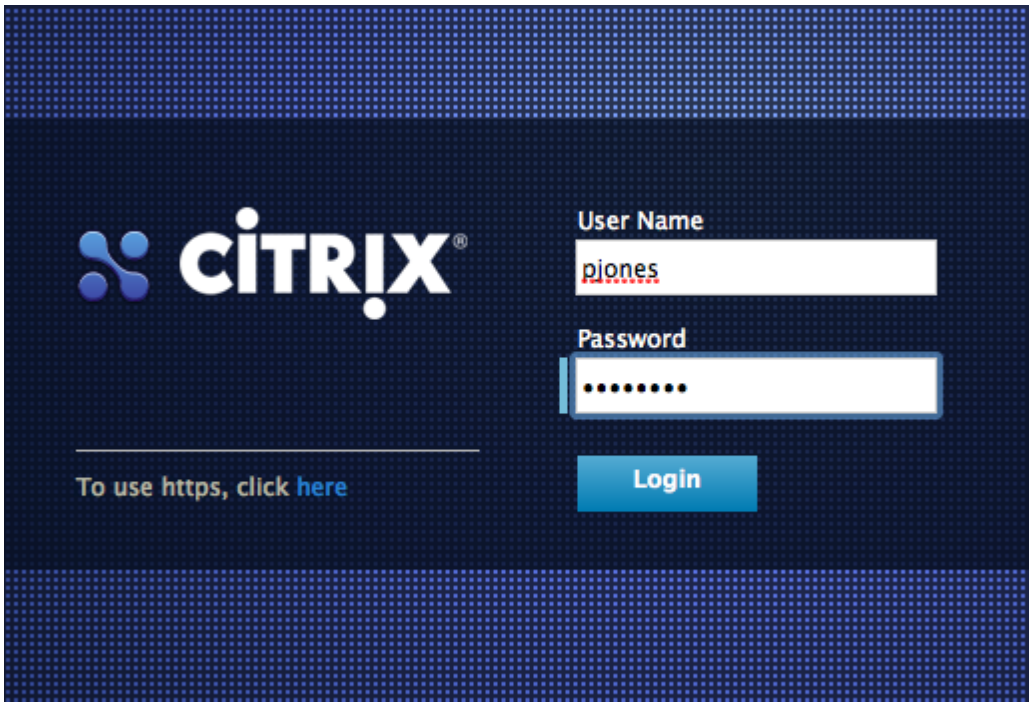
13. Click the *Select Policy* field.
14. Select the created policy.



15. Click *Bind*.
16. Click *Done*. The check mark will be displayed in the *Globally Bound* column.

How to authenticate in Citrix NetScaler using the NetIQ Advanced Authentication Framework:

1. Enter user's credentials and click *Login*.



2. Accept authentication on your smartphone.

NOTE: Advanced authentication can be configured with other authentication chains.

Configuring integration with Dell SonicWall SRA EX-Virtual appliance

These instructions will help you to configure integration of NetIQ Advanced Authentication Framework Appliance Edition with the Dell SonicWall SRA EX-Virtual appliance to refuse non-secure passwords in Dell SonicWall SRA connection.

The advanced authentication in Dell SonicWall is represented on the following diagram.

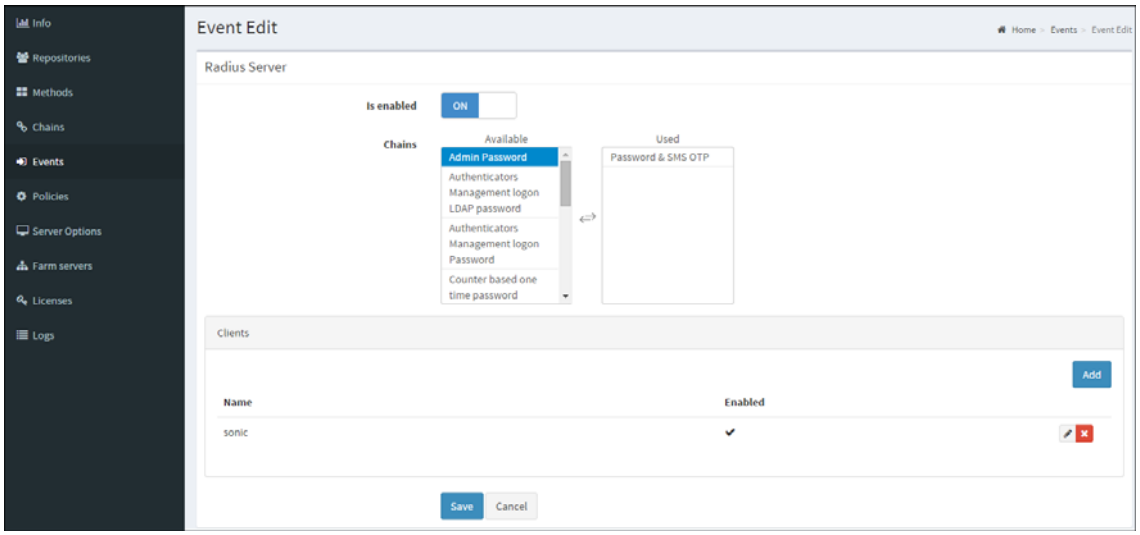
To get started, ensure that you have:

- Dell SonicWall SRA EX-Virtual appliance v11.2.0-258
- NetIQ v5 appliance

Configure the NetIQ RADIUS server:

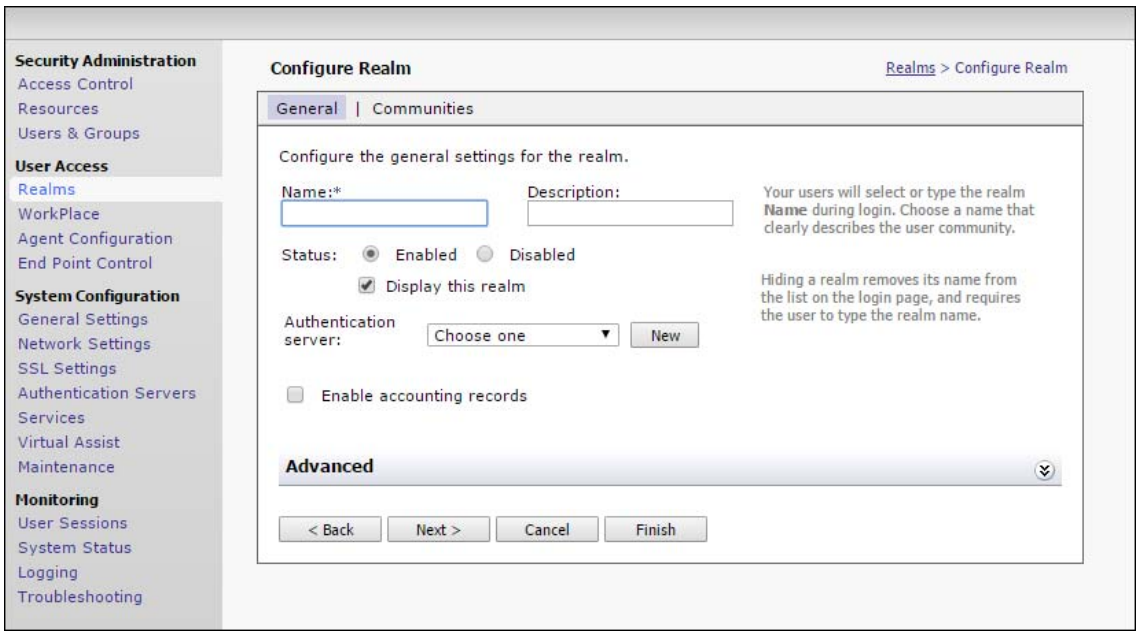
1. Open the NetIQ Admin Interface.
2. Go to the *Events* section.
3. Open properties of the *Radius Server* event.
4. Set the *Radius Server* event to the *ON* mode.
5. Select one or more chains from the list of *Used* chains (make sure that they are enabled and set to the users group in the *Chains* section).
6. Add a *Client*, enter an IP address of the Dell SonicWall SRA appliance, specify a secret, confirm it and set the *Enabled* option.

7. Click the *Save* button in the *Client* string. Click the *Save* button at the bottom of the *Events* view to save changes.

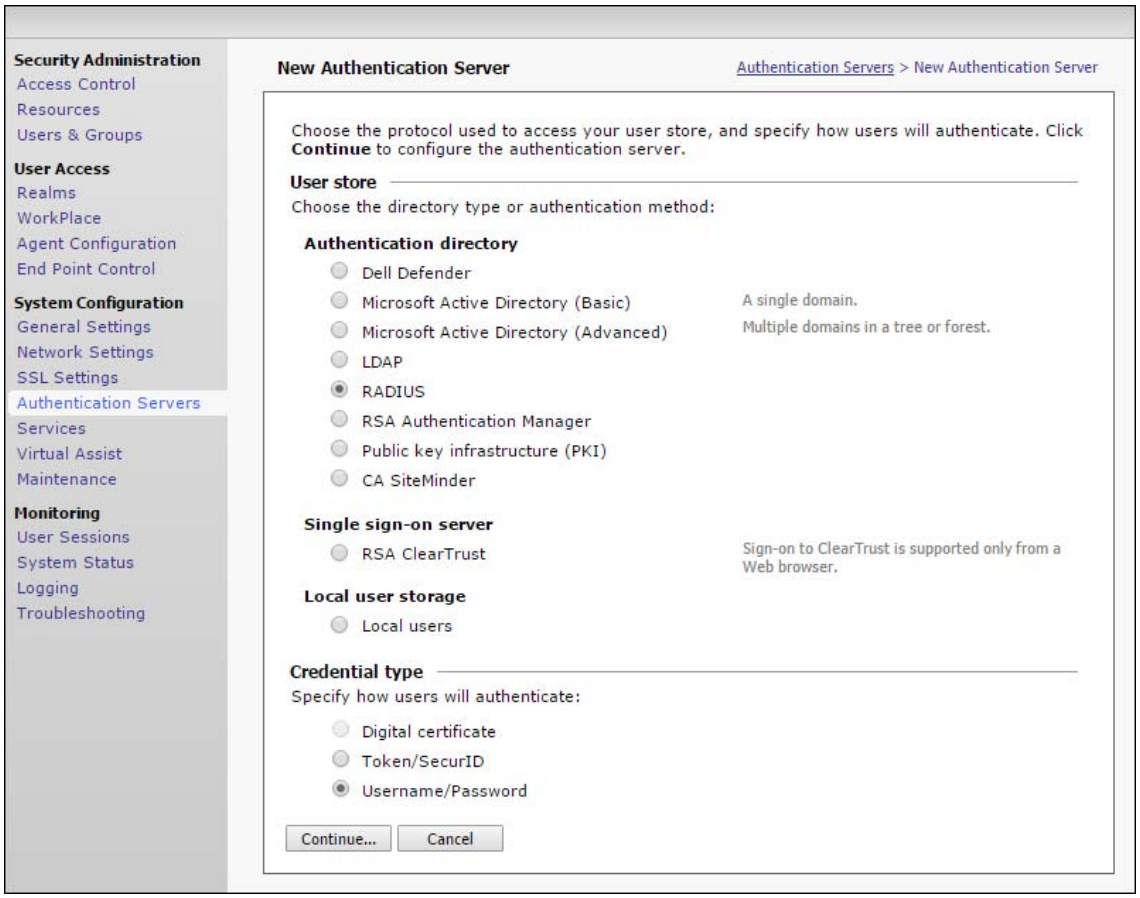


Configure the Dell SonicWall SRA appliance:

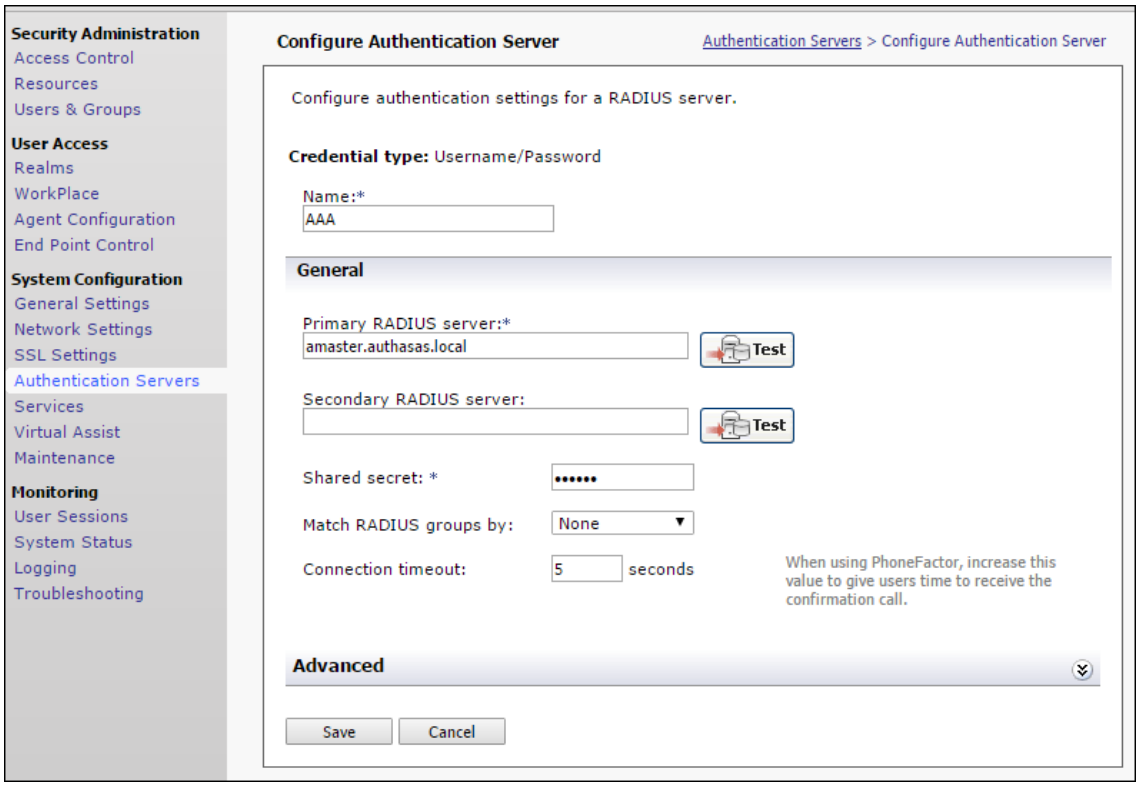
1. Sign-in to the Dell SonicWall SRA Management Console as *admin*.
2. Browse menu *User Access -> Realms*.
3. Create *New realm*.



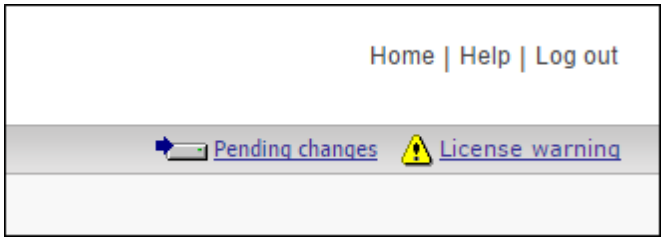
4. Create a *New Authentication Server*, set the *Radius* authentication directory.



5. Set *Radius Server* and *Shared key*.



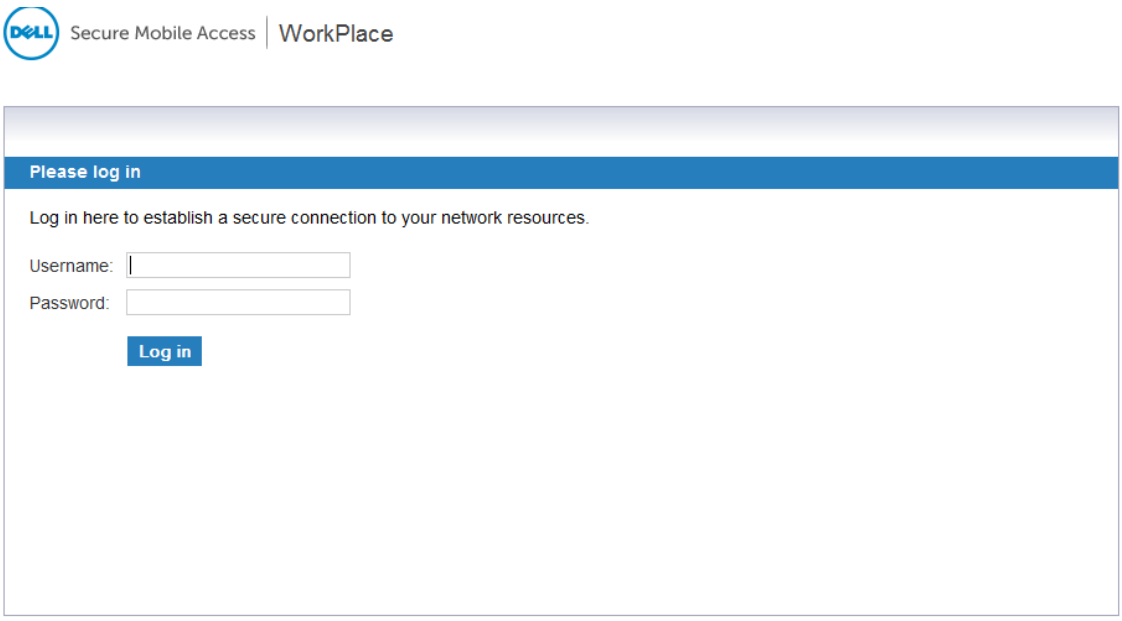
6. Save and apply configuration.



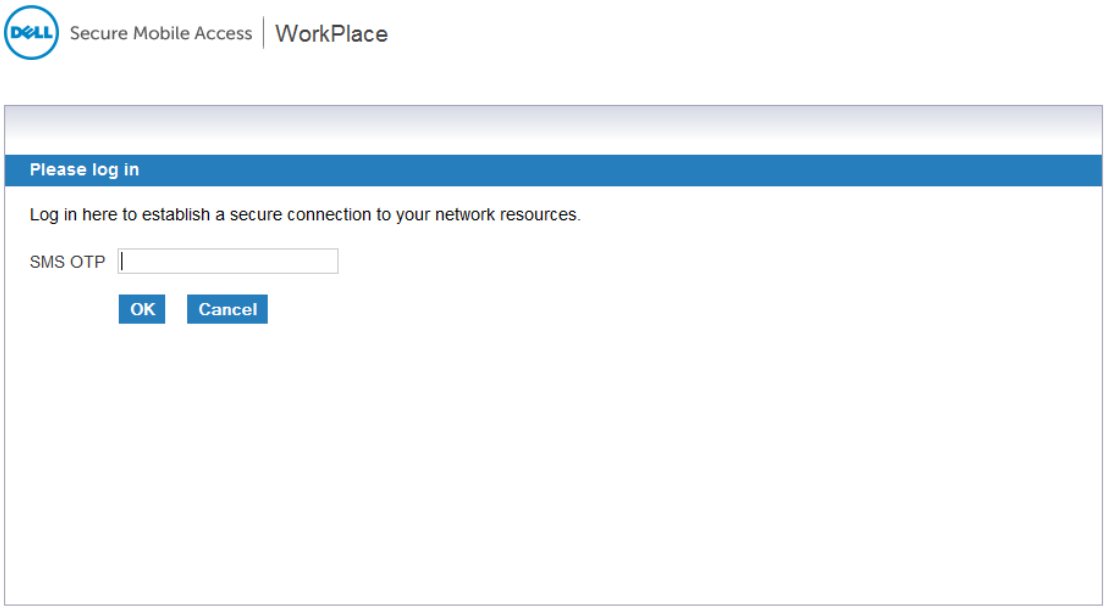
7. Browse menu *User Access -> Realms*. Review realm diagram.

How to authenticate in Dell SonicWall workspace using the NetIQ Advanced Authentication Framework:

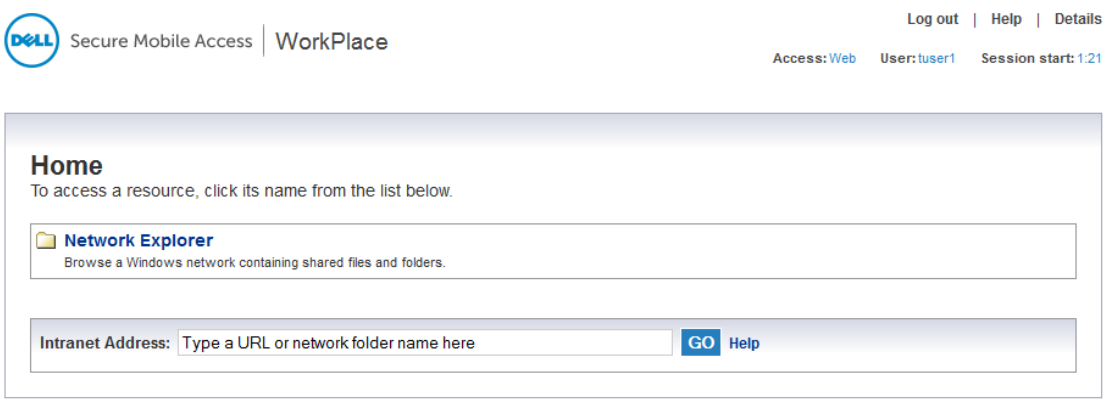
1. Open browser and go to workplace. Enter your username and ldap password.



2. Enter *SMS OTP* and click *OK*.



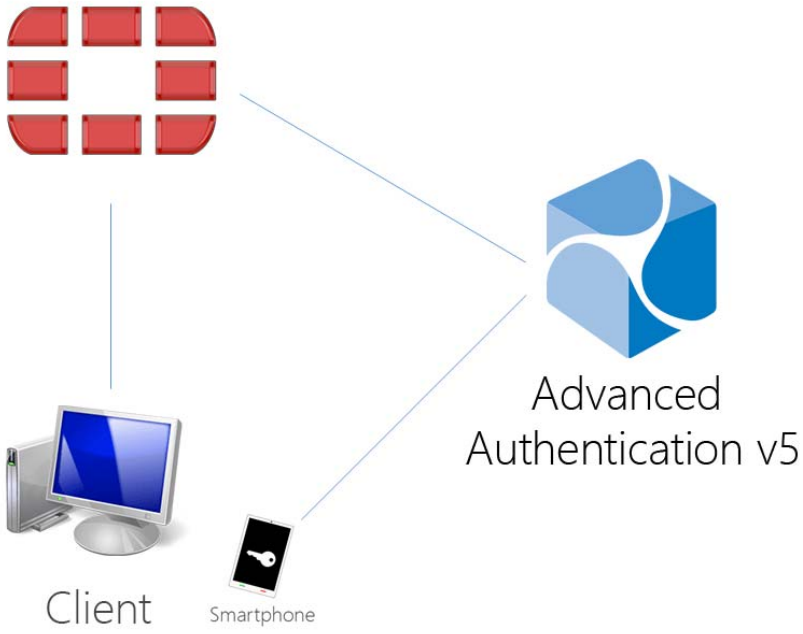
3. You are successfully logged in to the workplace.



Configuring integration with FortiGate

These instructions will help you to configure integration of NetIQ Advanced Authentication Framework Appliance Edition with the Fortinet FortiGate to refuse non-secure passwords.

The advanced authentication in Fortinet FortiGate is represented on the following diagram.

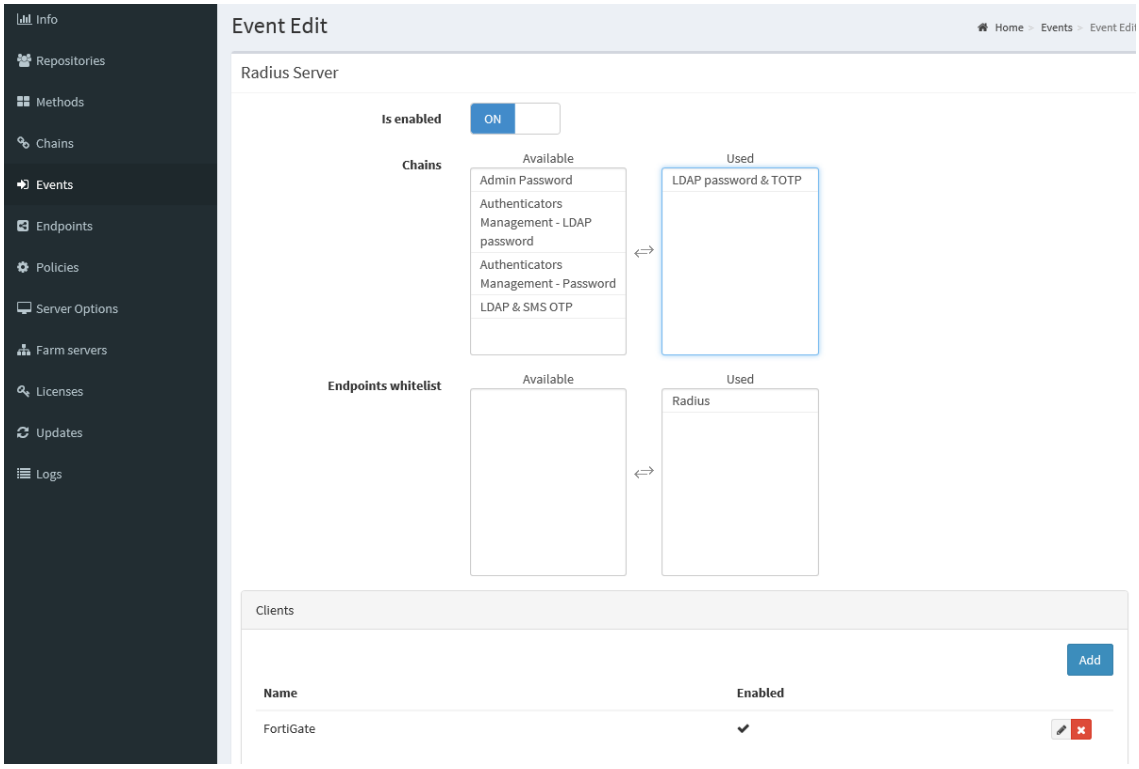


To get started, ensure that you have:

- Fortinet FortiGate virtual appliance v5 (Firmware version 5.2.5, build 8542 was used to prepare these instructions)
- NetIQ v5 appliance

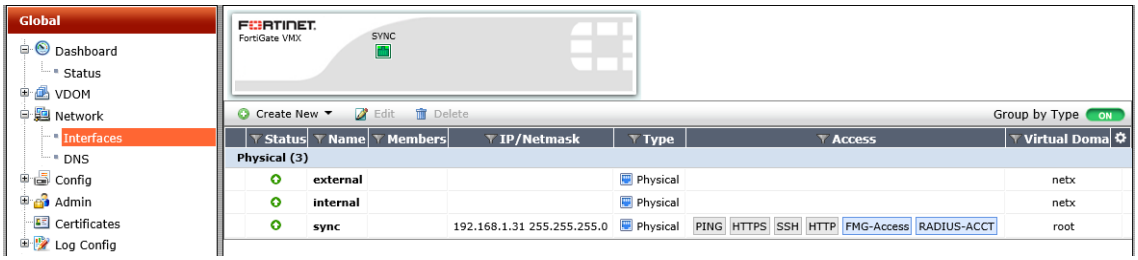
Configure the NetIQ RADIUS server:

1. Open the NetIQ Advanced Authentication Administrative Portal.
2. Go to the *Events* section.
3. Open properties of the *Radius Server* event.
4. Set the *Radius Server* event to the *ON* mode.
5. Select one or more chains from the list of *Used* chains (make sure that they are enabled and set to the users group in the *Chains* section).
6. Add a *Client*, enter an IP address of the FortiGate appliance, specify a secret, confirm it and set the *Enabled* option.
7. Click the *Save* button in the *Client* string. Click the *Save* button at the bottom of the *Events* view to save changes.

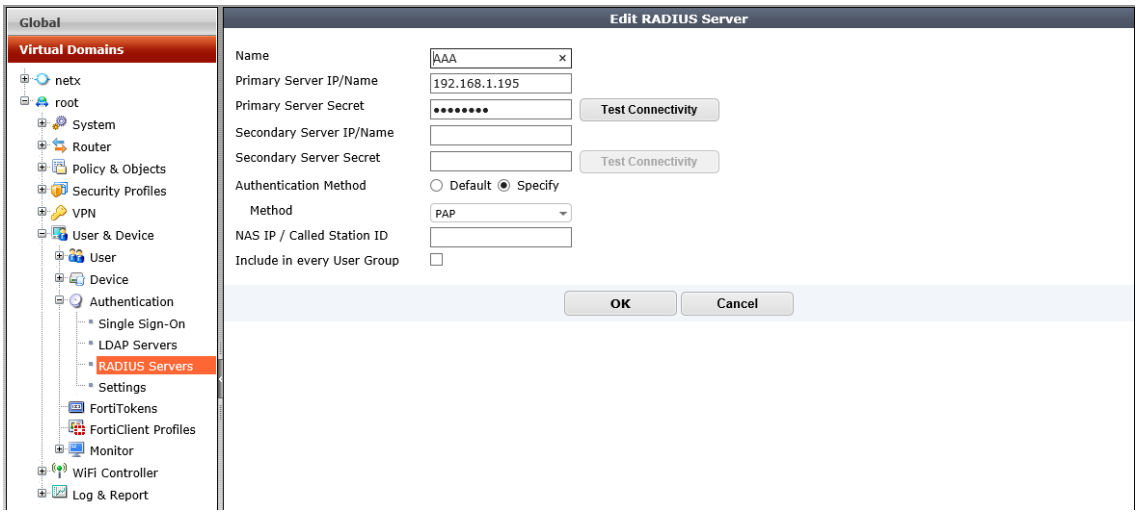


Configure the FortiGate appliance:

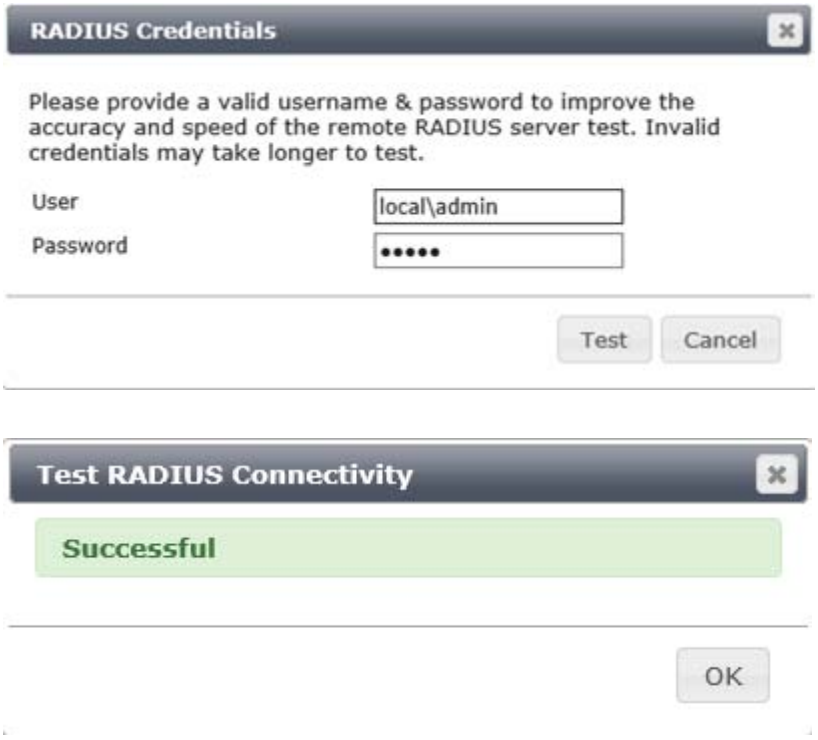
1. Sign-in to FortiGate configuration portal as admin.
2. Check which Virtual Domain bound to the network interface.



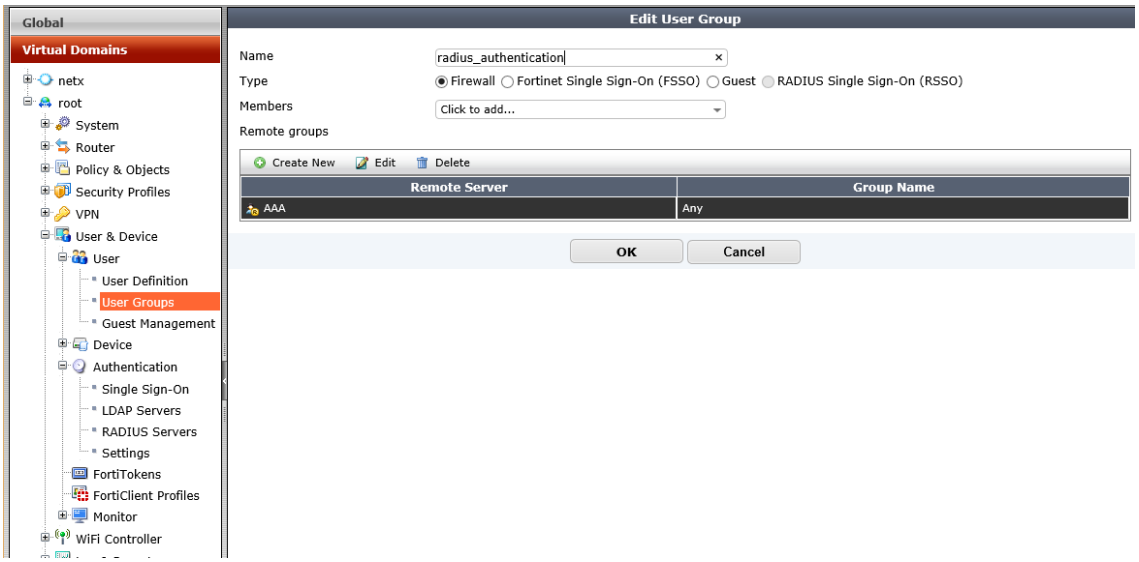
3. Open Radius Server configuration for an appropriate Virtual Domain and setup required settings.



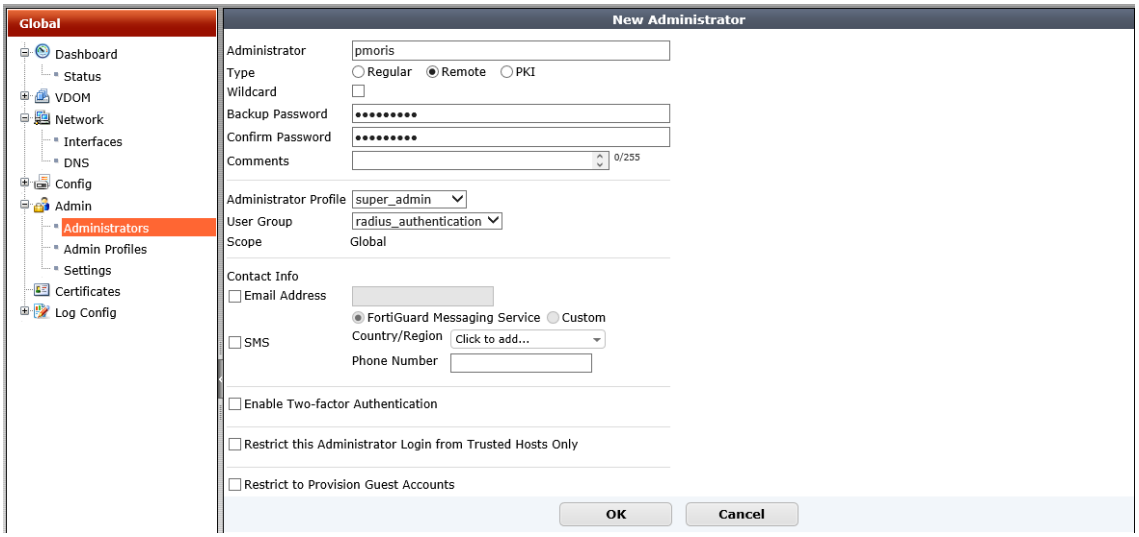
4. Click *Test Connectivity* button, enter credentials of Advanced Authentication Framework administrator to test the connection.



5. Create a user group and bind it to remote authentication server.



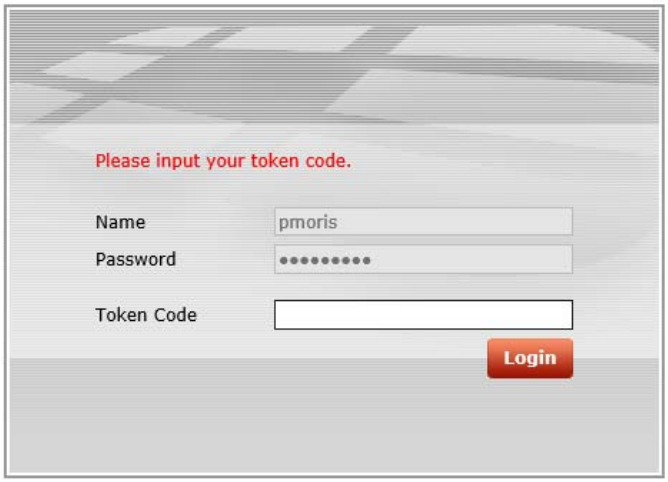
6. Create user and place is in the created group.



How to authenticate in FortiGate using the NetIQ Advanced Authentication Framework:

1. Enter user's credentials and click *Login*.

2. Enter OTP and click *Login*.

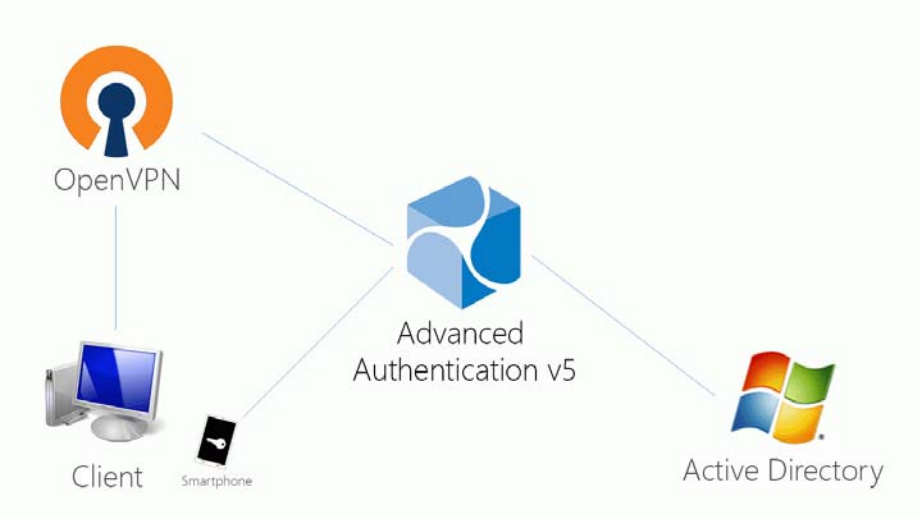


NOTE: The Token Code field has a 16 digits limitation, so you may get problems when using the YubiKey tokens which enters 18-20 digits code.

Configuring integration with OpenVPN

These instructions will help you to configure integration of NetIQ Advanced Authentication Framework Appliance Edition with the OpenVPN virtual appliance to refuse non-secure passwords in OpenVPN connection.

The advanced authentication in OpenVPN is represented on the following diagram.



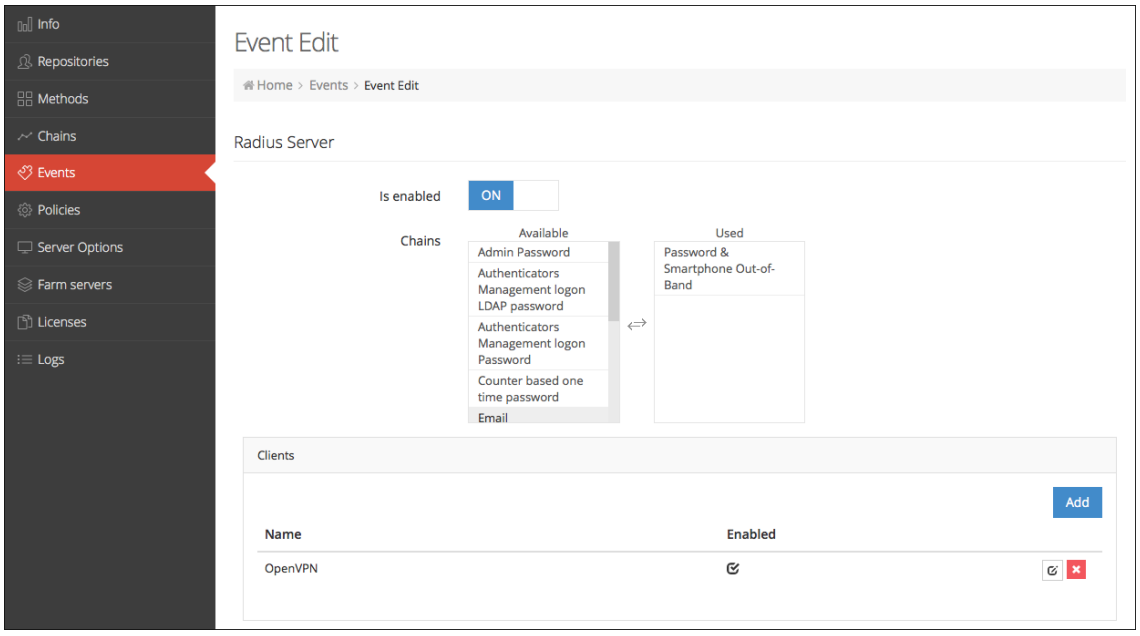
To get started, ensure that you have:

- OpenVPN v2 appliance (version 2.0.10 was used to prepare these instructions)
- NetIQ v5 appliance (version 5.1.1 was used to prepare these instructions) with the already configured repository

Configure the NetIQ RADIUS server:

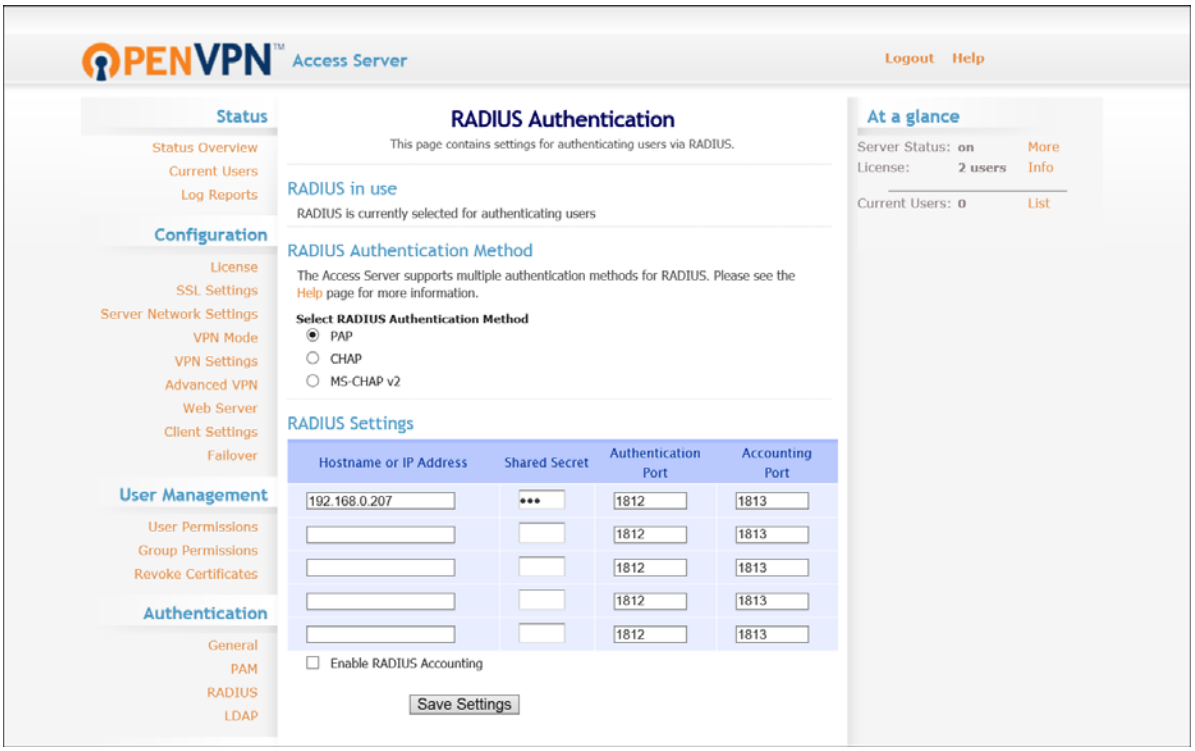
1. Open the NetIQ Admin Interface.
2. Go to the *Events* section.
3. Open properties of the *Radius Server* event.
4. Set the *Radius Server* event to the *ON* mode.
5. Select one or more chains from the list of *Used* chains (make sure that they are enabled and set to the users group in the *Chains* section).
6. Add a *Client*, enter an IP address of the OpenVPN appliance, specify a secret, confirm it and set the *Enabled* option.

7. Click the *Save* button in the *Client* string. Click the *Save* button at the bottom of the *Events* view to save changes.



Configure the OpenVPN appliance:

1. Open the *OpenVPN Access Server* site.
2. Go to the *Authentication - RADIUS* section.
3. Enable the *RADIUS* authentication.
4. Select *PAP* authentication method.
5. Add an IP address of the NetIQ v5 appliance and enter the secret.



If you have one *Used* chain selected in the *Radius Server* settings, to connect to OpenVPN, please enter the <repository name>\<username> or only <username> if you have set the default repo name in *Policies - Login options* section of the NetIQ v5 appliance.

If you have multiple *Used* chains selected, to connect to OpenVPN, in the username field after the entered <username> and space you need to enter a *Short name* of the necessary chain (the *Short name* can be selected in *Chains* section of the NetIQ v5 appliance).

Please note that some of the available authentication methods require correct time on the OpenVPN appliance. You can sync the time of the OpenVPN appliance using the following commands:

```
/etc/init.d/ntp stop
```

```
/usr/sbin/ntpdate pool.ntp.org
```

After 3 successful authentications with SMS AP to OpenVPN the user account was locked

Description:

We are using SMS authentication method to connect to OpenVPN. But after 3 successful authentications the user account was locked by OpenVPN.

Solution:

This problem is not related to NetIQ Advanced Authentication Framework. OpenVPN supposes each attempt of challenge response (request of additional data in chain) as an error.

The solution is to change acceptable number of failures. Check the Authentication failure lockout policy article for more information.

4.5.18 Managing Endpoints

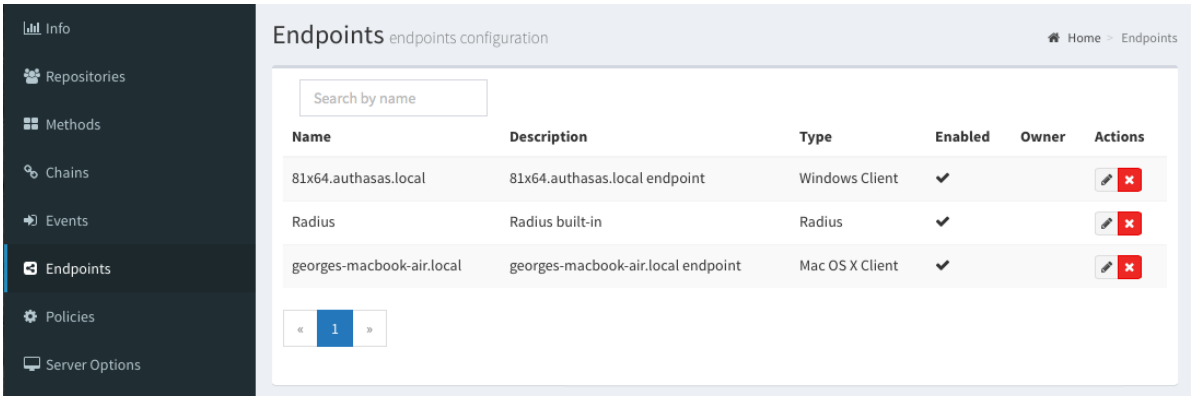
In this section you can manage existing endpoints. Endpoint means a place where the NetIQ Advanced Authentication server will authenticate. It can be a certain workstation with Microsoft Windows for Windows Client endpoint, or NetIQ Access Manager appliance for NAM endpoint.

Such endpoints will be automatically added during installation of NAM Advanced Authentication plugin or after installation of Windows Client.

Only the Radius endpoint is predefined and available in Endpoints section by defaut.

The following endpoint types are supported:

1. NAM
2. NCA
3. Radius
4. Mac OS X Client (Local Hostname will be used as endpoint name)
5. Windows Client (DNS name will be used as endpoint name)



To manage an authentication endpoint for NetIQAdvanced Authentication framework, follow the steps:

1. Open the *Endpoints* section.
2. Click the *Edit* button next to an applicable endpoint.
3. It's possible to rename the endpoint, change its description or endpoint type.
4. Select whether the current endpoint is enabled or disabled by clicking the *Is enabled* toggle button.
5. Specify an *Endpoint Owner* if you have configured a specific chain to be used by Endpoint owner only. This is a user account who should be able to use a different Creating Chain other than regular users use for authentication.
6. Click *Save* at the bottom of the *Events* view to save configuration.

NOTE: After uninstallation of the Windows Client or MacOS Client its endpoint will not be removed. You may remove it manually in the Endpoint section.

If you upgraded from v5.1.3 to v5.2 you have the two endpoints:

---

1. Endpoint41

Description: Well-known endpoint (id 41414141)

Type: Other

Purpose: support of legacy NetIQ CloudAccess plugin.

2. Endpoint42

Description: Well-known endpoint (id 42424242)

Type: Other

Purpose: support of legacy NetIQ Access Manager plugin.

The old NetIQ Access Manager and NetIQ CloudAccess plugins worked with the hardcoded endpoint ID and secret. In v5.2 endpoints must be registered. This breaks backwards compatibility with old plugins. These two legacy endpoints allow to keep the old plugins working.

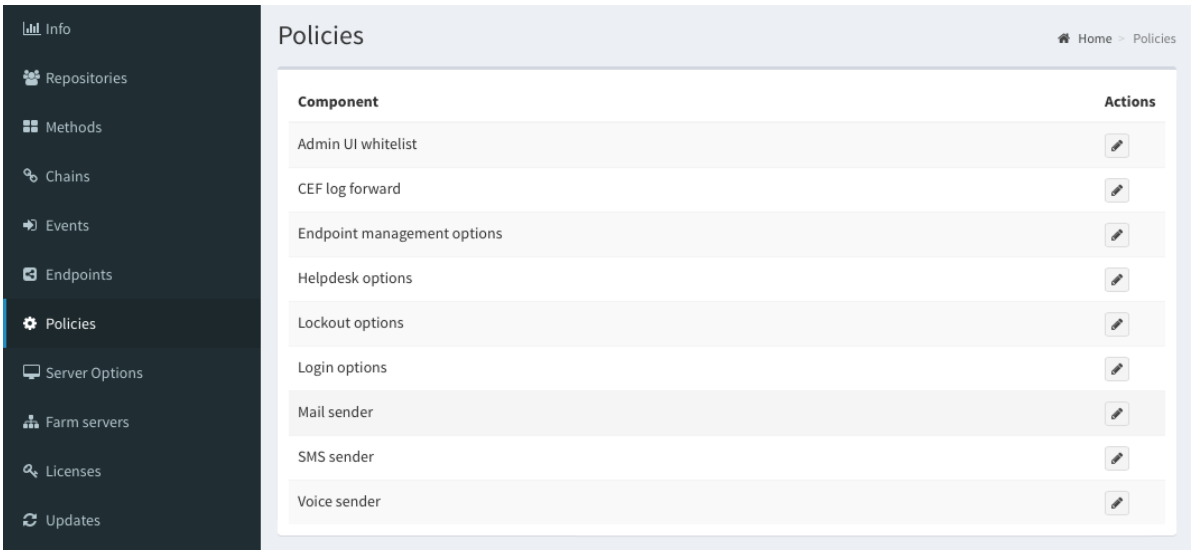
4.5.19 Configuring Policies

To configure an applicable policy for NetIQ Advanced Authentication framework, follow the steps:

1. Open the *Policies* section. The list of available authentication methods will be displayed.
2. Click the *Edit* button next to an applicable policy.
3. Edit configuration settings for a specific policy.
4. Click *Save* at the bottom of the *Policies* view to save changes.

In the section you can find the following settings:

- *Restricting Access to the Administrative Portal* - security settings which allows to limit using of NetIQ Administrative Portal only for permitted IP addresses.
- *Configuring Logs Forwarding* - settings to configure an external syslog server.
- *Requiring authentication data during registration of endpoint* - an option to require authentication data for Endpoint creation. It must be disabled when installing NetIQ Access Manager Advanced Authentication plugin.
- *Helpdesk Options* - a security option which allows to disable asking for user's credential when a security officer is managing the user's authenticators.
- *Lockout Options* - security settings which allows to lock user after some authentication failures.
- *Login Options* - allows to specify the default repositories, to avoid of necessity to enter a repository name in username field.
- *Mail Server Settings* - SMTP server settings.
- *SMS Service Provider Settings* - settings for external SMS service provider, contains predefined settings for Twilio, MessageBird.
- *Voice Call Service Provider Settings* - Twilio settings for Voice Call method; an option to allow enrollment for users without telephone number.



IMPORTANT: The configured policies will be applied for all servers.

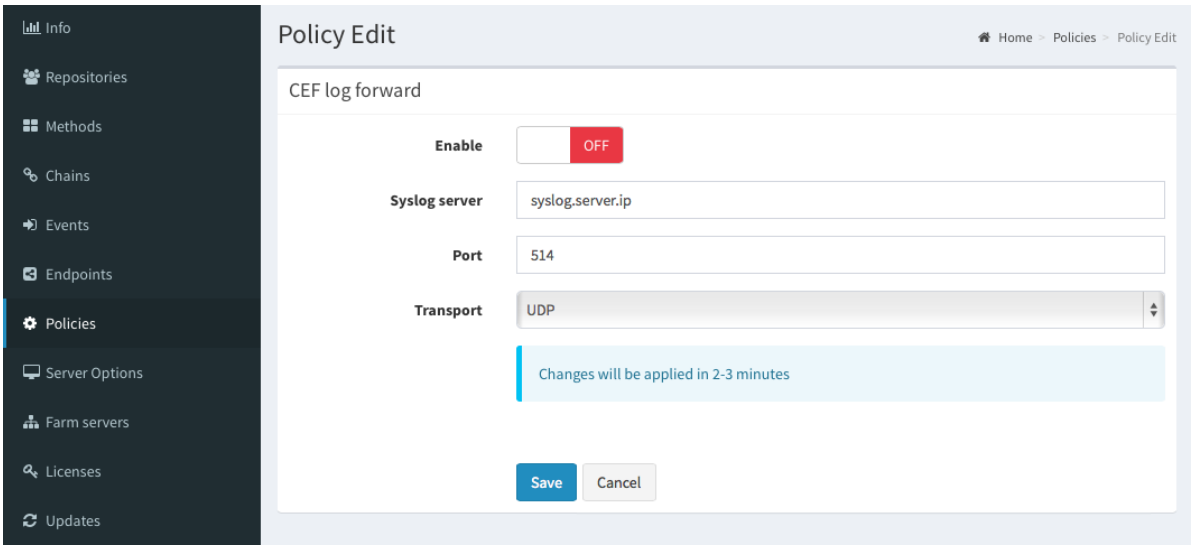
4.5.20 Configuring Logs Forwarding

The *CEF log forwarding* settings are located in the *Policies* section.

The settings allows to configure forwarding of logs to an external Syslog server. The central logging server may be used for log forwarding. To configure it, follow the steps:

1. Open the *Policies* section.
2. Click the *Edit* button next to the *CEF log forward* policy.
3. Select the *Enable* checkbox.
4. Specify the IP address of the remote logging server in the *Syslog server* text field.
5. Specify the port of the remote logging server in the *Port* text field.
6. Select an applicable transfer protocol from the *Transport* dropdown.
7. Click *Save* at the bottom of the *Policies* view to save changes. The changes will be applied in 2-3 minutes.

IMPORTANT: The same Syslog configuration is used for each server type. Each server type in the appliance records its own log file.



Events from all facilities are recorded to syslog. E.g., Advanced Authentication Server Core, Kernel, Daemon, etc.

The following Server Core events are being recorded in the log file:

- Failed to join endpoint
- No rights to join endpoint
- Endpoint joined
- Failed to remove endpoint
- No rights to remove endpoint
- Endpoint remove
- Failed to create endpoint session
- Endpoint session ended
- Failed to create endpoint session
- Invalid endpoint secret
- Endpoint session started
- Failed to create local user
- Local user was created
- Failed to remove local user
- Local user was removed
- Repository configuration was changed
- Failed to add repository
- New repository was added
- Request failed
- Server started
- Server stopped
- Server unexpectedly stopped
- Failed to assign template to the user
- Template was assigned to the user

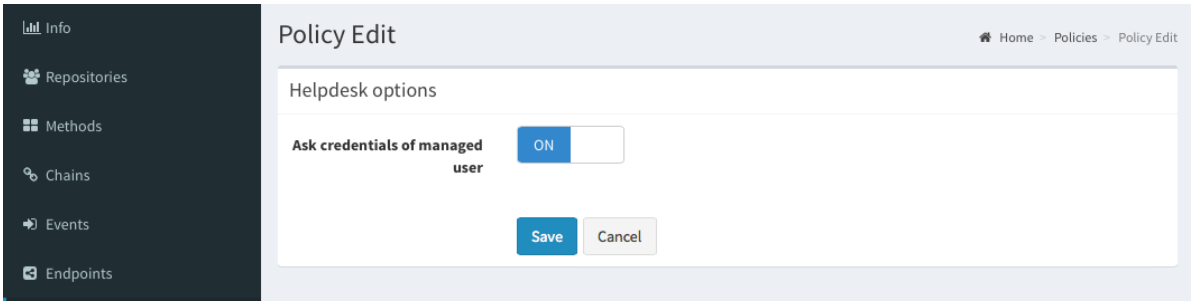
- Failed to change template
- Template was changed
- Failed to enroll template for the user
- Template was enrolled for the user
- Failed to link template
- Template was linked
- Failed to remove template link
- Template link was removed
- Failed to remove template
- Template was removed
- Failed to create user
- User was created
- User can't enroll the assigned template
- User enroll the assigned template
- User was failed to authenticate
- User logon started
- User was successfully logged on
- User was switched to different method
- User do not want logon by phone but Twilio calling
- User read app data
- User write app data

4.5.21 Helpdesk Options

The *Helpdesk options* are located in the *Policies* section.

The options provide security settings for security officers who manage users' authenticators in Helpdesk Portal.

With the enabled *Ask credentials of management user* option the security officers should provide credentials of users before its management. When the option is set to OFF a security officer doesn't need to provide credentials of managed user. This may be not secure, but user management can be done much faster when the option is disabled.

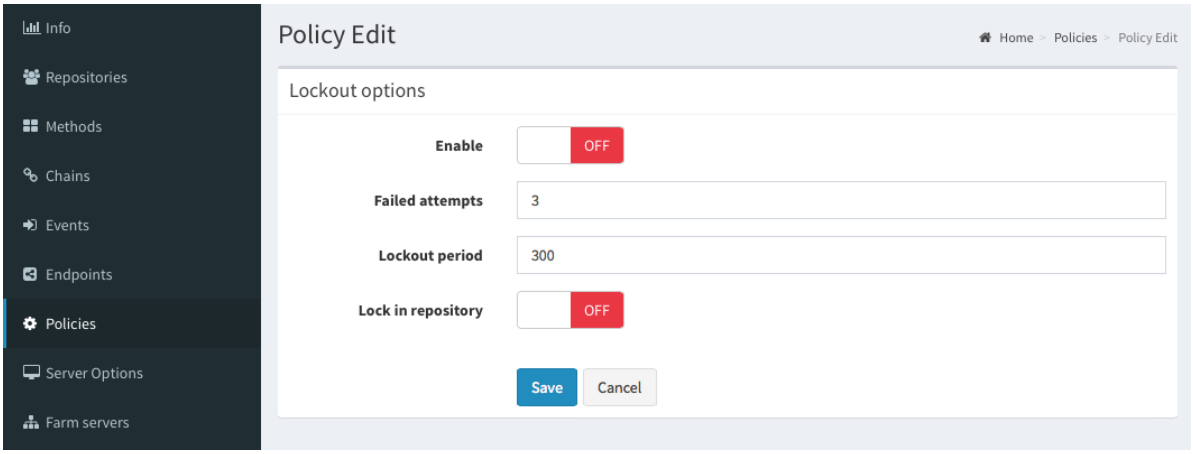


4.5.22 Lockout Options

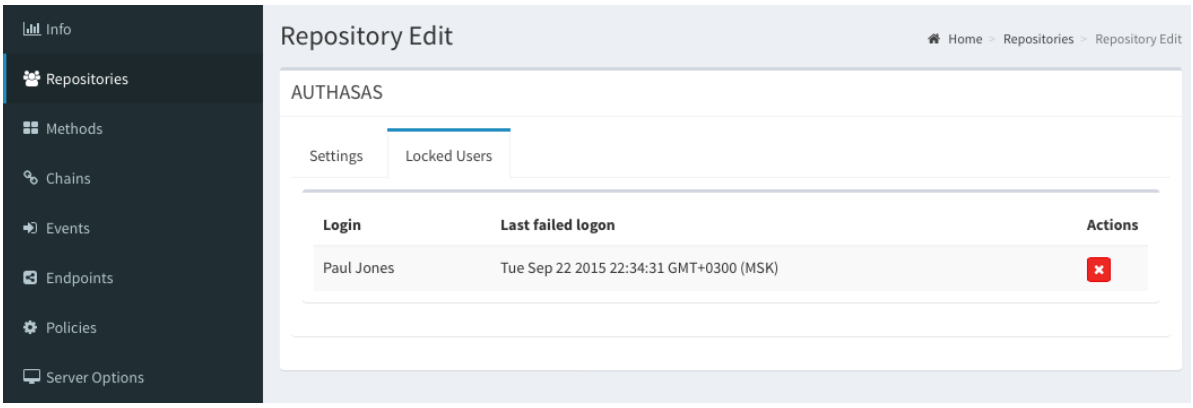
The *Lockout options* are located in the *Policies* section.

The options allows to configure the user account lockout in case of reaching limit on failure attempts. It may be used to prevent of guessing the one-time passwords. It's possible to configure the following settings:

1. *Enable*, the option enables the lockout settings.
2. *Failed attempts*, it allows to setup a limit of authentication attempt failures after which the user account will be locked. 3 attempts by default.
3. *Lockout period*, it allows to configure a period within which the user will be locked and not possible to authenticate. 300 seconds by default.
4. *Lock in repository*, the option allows to lock the user account in repository. The Lockout period option is not used for the case. It will be required for system administrator to unlock the user manually in the repository.



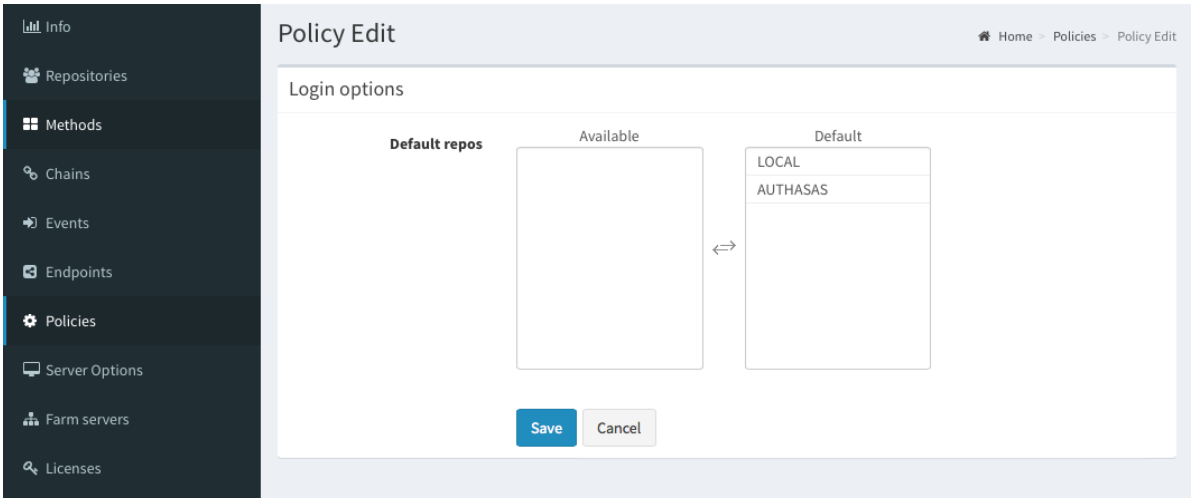
It's possible to manage the locked users (only the users who are not locked in repository). To do it switch to the *Repositories* section. Click *Edit* button for the used repository. Switch to *Locked Users* tab. Click *Remove* button next to account name to unlock the user account.



4.5.23 Login Options

The *Login options* are located in the *Policies* section.

Here it's possible to configure the *Default* repositories. Using the Default repositories it's not required to enter repository name before a username for authentication. So instead of `company\pjones` it will be possible to enter only `pjones`, instead of `local\admin` it will be possible to use `admin`.



4.5.24 Mail Server Settings

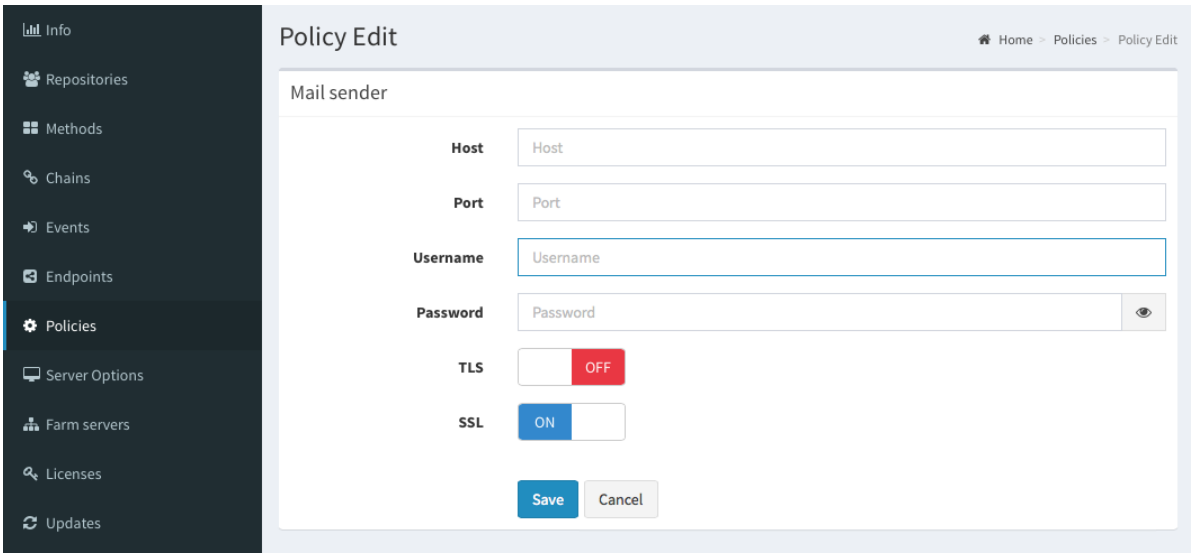
The *Mail sender* settings are located in the *Policies* section.

The section contains the mail server settings. It's used by Email OTP to send the email messages with one-time passwords to users.

It's required to configure the following settings:

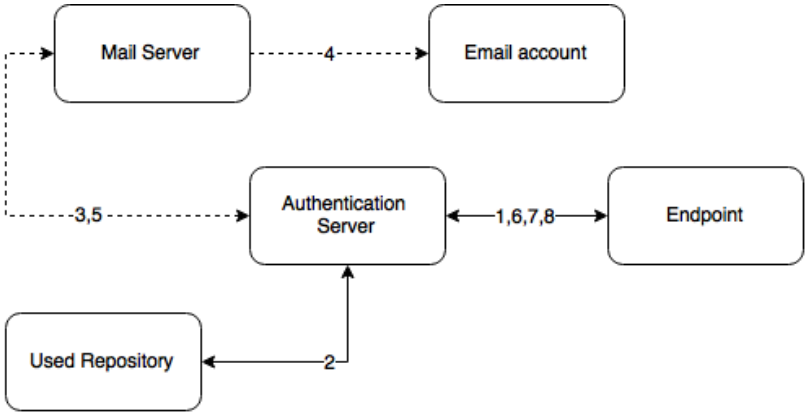
1. *Host*, the outgoing mail server name (e.g. smtp.company.com)
2. *Port*, the used port number (e.g. 465)
3. *Username*, username of an account which will be used to send the authentication email messages (e.g. noreply or noreply@company.com)
4. *Password*, password for the specified account
5. *TLS* and *SSL* is used to specify a cryptographic protocol used by the mail server.

Click *Save* to apply the changes.



Authentication flow

The following chart demonstrates the authentication flow:



A user is authenticating on endpoint (which can be the user's laptop with NetIQ Windows Client installed or a website etc.) by Email method.

1. The endpoint calls the NetIQ Advanced Authentication Server.
2. It validates the provided user's credentials and gets an email address of the user from a used Repository.
3. NetIQ Advanced Authentication Server sends the request to a configured Mail Server to send an Email message with generated content which includes a one-time password (OTP) for authentication.
4. Mail Server sends the message to the user's email address.
5. Mail Server sends the 'sent' signal to the NetIQ Advanced Authentication Server.
6. NetIQ Advanced Authentication Server sends a request to enter an OTP on the endpoint side.
7. The user enters an OTP from the email message. The NetIQ Advanced Authentication Server gets the OTP.
8. NetIQ Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTPS protocol is used for the internal communication.

Access configuration

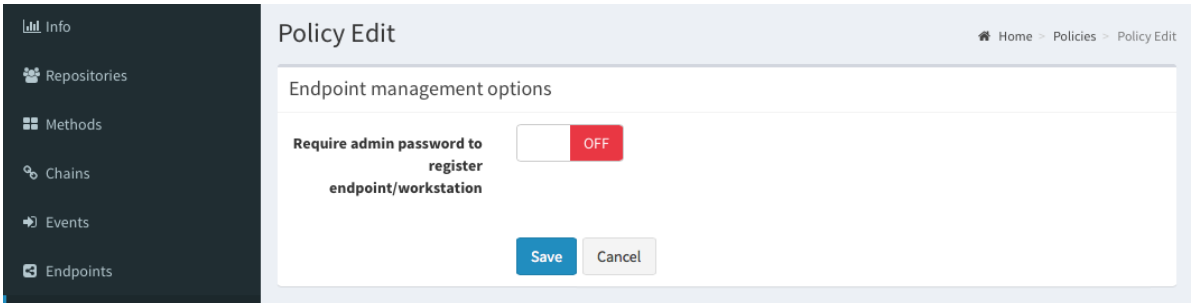
NetIQ Advanced Authentication Server - Mail Server (SMTP, outbound).

4.5.25 Requiring authentication data during registration of endpoint

The *Endpoint management options* are located in the *Policies* section.

If the option *Require admin password to register endpoint/workstation* is enabled, the NetIQ Advanced Authentication will require endpoints to provide the local administator's credentials during installation of endpoint component.

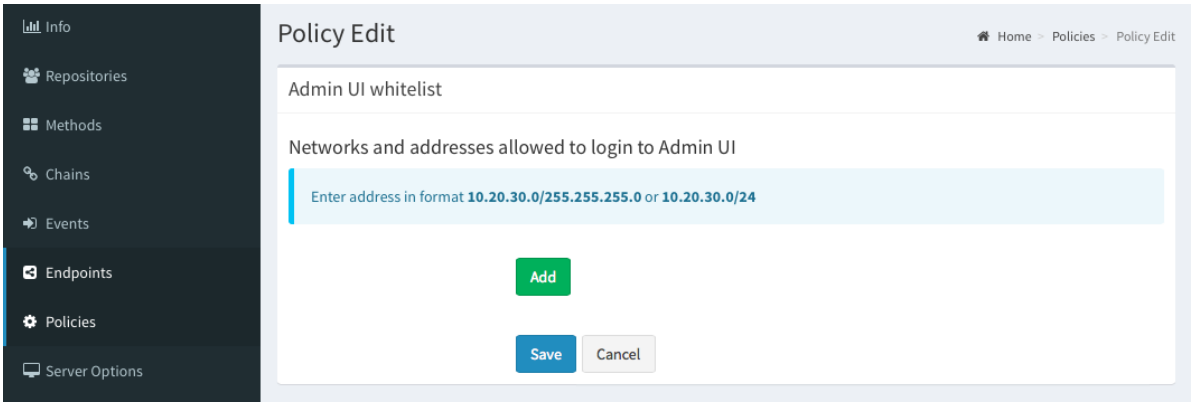
The option must be disabled when installing the NetIQ Access Manager Advanced Authentication Plugin or NetIQ Windows Client or NetIQ MacOS Client. Otherwise the endpoints will not be created.



4.5.26 Restricting Access to the Administrative Portal

The *Admin UI whitelist* settings are located in the *Policies* section.

The settings allows to configure access to the NetIQ Advanced Authentication Administrative Portal only for permitted IP addresses. By default the restrictions are not set. To configure the restrictions click *Add* button. Enter address in format 10.20.30.0/255.255.255.0 or 10.20.30.0/24. NetIQ Advanced Authentication has an automatic check which allows to prevent administrators from losing access to the Administrative Portal. If your IP address is out of the range you will see a message: `Your IP address is not whitelisted. You will lose access! Please add your IP.` To apply the changes click *Save* button.



4.5.27 SMS Service Provider Settings

The *SMS sender* settings are located in the *Policies* section.

The section contains the SMS service provider settings. It's used by SMS OTP to send the SMS messages with one-time passwords to users. NetIQ Advanced Authentication contains the predefined settings for Twilio and MessageBird services.

To configure SMS sender settings for *Twilio* service select the Twilio in *Sender service* dropdown box and fill the following fields:

1. Account sid
2. Auth token
3. Sender phone

The information you may get on the Twilio website (https://www.twilio.com/).

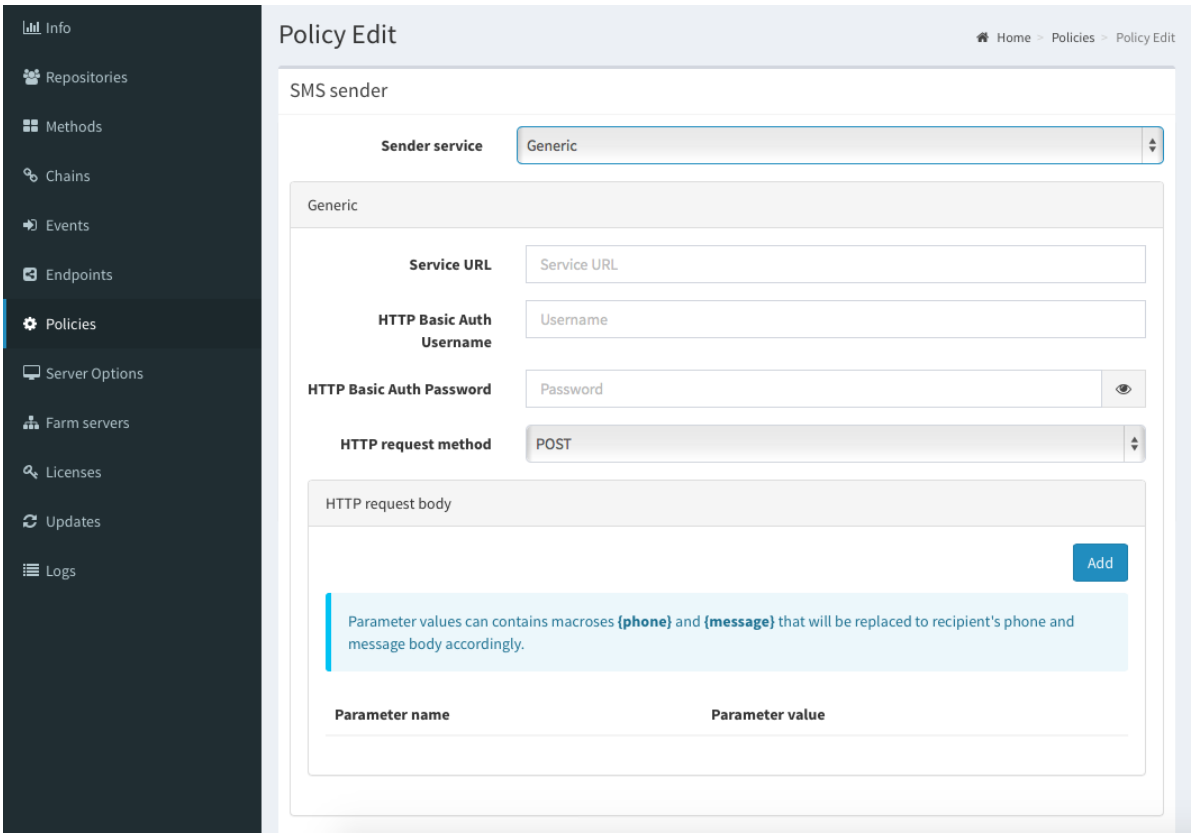
To configure SMS sender settings for *MessageBird* service select the Messagebird in *Sender service* dropdown box and fill the following fields:

1. Username
2. Password
3. Sender name

The information you may get on the MessageBird website (https://www.messagebird.com/).

IMPORTANT: MessageBird API v2 is not supported. To activate MessageBird API v1, go to the MessageBird account, click *Developers* from the left navigation bar and open the API access (https://www.messagebird.com/settings/developers/access) tab. Click *Do you want to use one of our old API's (MessageBird V1, Mollie or Lumata)? Click here*.

To configure SMS sender manually select *Generic* in *Sender service* dropdown box and follow the instruction below:



1. Specify a *Service URL* value. E.g., for Clickatell http://api.clickatell.com/http/sendmsg?.
2. Leave the *HTTP Basic Auth Username* and *HTTP Basic Auth Password* fields empty.
3. Select *POST* from the *HTTP request method* dropdown box.
4. Click *Add* and create the following parameters in *HTTP request body* section.
   - name: *user*

     value: name of your account
   - name: *password*

     value: current password that is set on the account
   - name: *to*

     value: {phone}
   - name: *text*

     value: {message}
   - name: *api_id*, this is a parameter issued upon addition of an HTTP sub-product to your Clickatell account. A single account may have multiple API IDs associated with it.
   - name: *from*

     value: sender's phone number

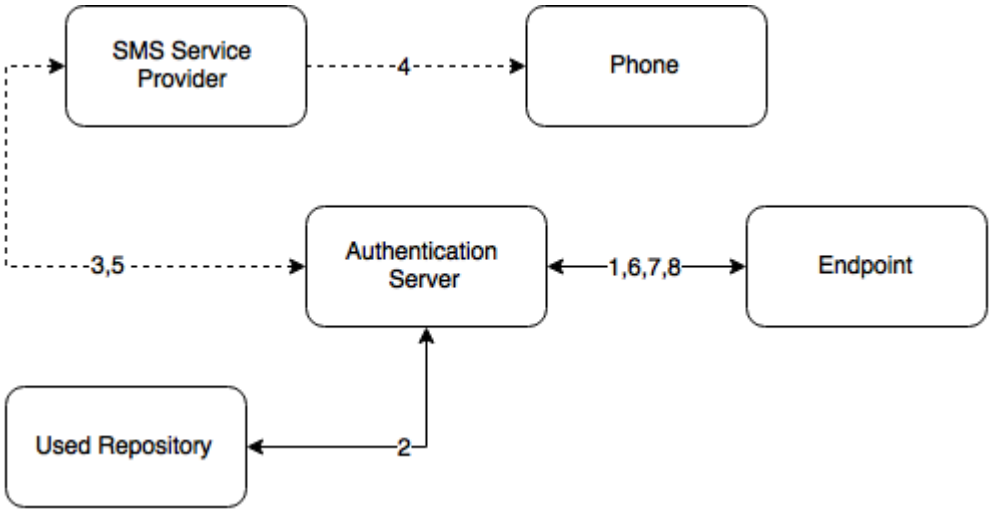
   For more information on additional parameters for Clickatell, check Clickatell HTTP/S SMS API documentation.

NOTE: The parameters may differs for different SMS service providers. But the `{phone}` and `{message}` variables are obligatory.

Click *Save* at the bottom of the view to save changes.

Authentication flow

The following chart demonstrates the authentication flow:



A user is authenticating on endpoint (which can be the user's laptop with NetIQ Windows Client installed or a website etc.) by SMS method.

1. The endpoint calls the NetIQ Advanced Authentication Server.
2. It validates the provided user's credentials and gets a phone number of the user from a used Repository.
3. NetIQ Advanced Authentication Server sends the request to a configured SMS Service Provider to send an SMS message with generated content which includes a one-time password (OTP) for authentication.
4. SMS Service Provider sends the SMS message to the user's phone.
5. SMS Service Provider sends the 'sent' signal to the NetIQ Advanced Authentication Server.
6. NetIQ Advanced Authentication Server sends a request to enter an OTP on the endpoint side.
7. The user enters an OTP from the SMS message. The NetIQ Advanced Authentication Server gets the OTP.
8. NetIQ Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTP/HTTPS protocol is used for the communication.

Access configuration

NetIQ Advanced Authentication Server - SMS Service Provider (HTTP/HTTPS, outbound).

4.5.28 Voice Call Service Provider Settings

The *Voice sender* settings are located in the *Policies* section.

The section contains the Voice Call method settings. It's used by Voice Call. NetIQ Advanced Authentication supports the Twilio service.

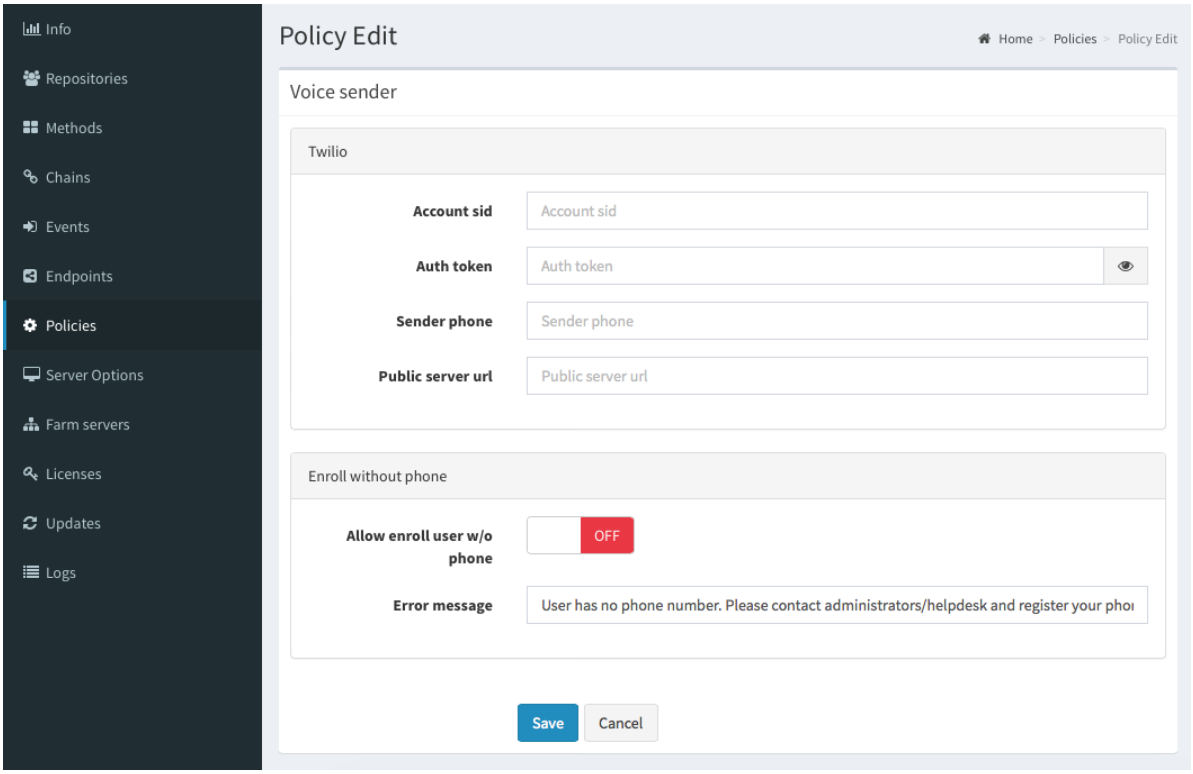
The following fields must be filled in *Twilio* section:

1. Account sid
2. Auth token
3. Sender phone
4. Public server url

The information regarding fields 1-3 you may get on the Twilio website (https://www.twilio.com/). The *Public server url* must contain a public URL to where the Twilio service will connect for authentication. It's possible to use http protocol for testing purposes, but for production environment it's recommended to use https protocol. You need to have a valid certificate when using https.

The *Enroll without phone* section allows to configure behavior when a user is trying to enroll the Voice Call authenticator, but the user's repository data doesn't contain a phone number. If *Allow enroll user w/o phone* option is set to OFF such user will not be able to enroll the Voice Call authenticator and the user will get an error message, which can be specified in *Error message* field.

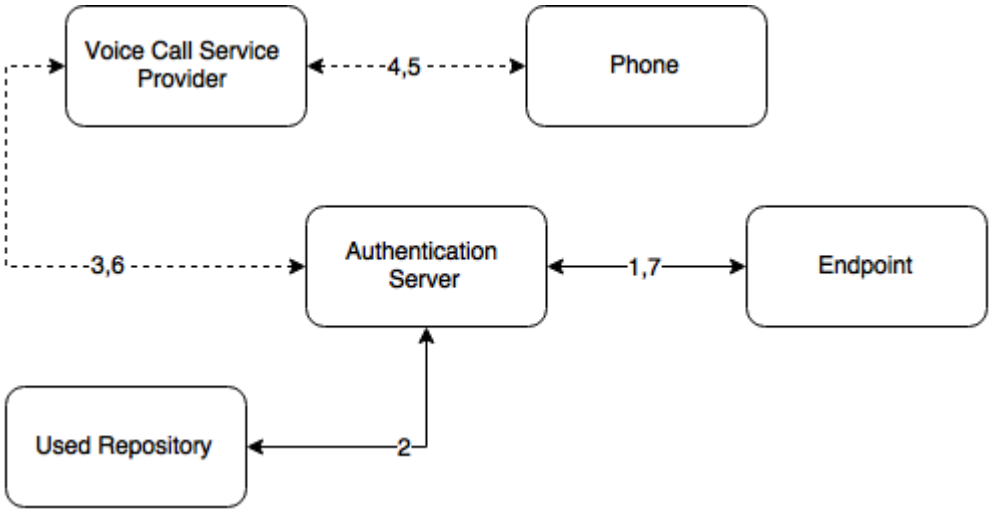
Click *Save* to apply the changes.



IMPORTANT: The users may get the calls with voice speaking `Application error`. It may happen because of not correct settings or invalid certificate. Ensure that the certificate is valid and not expired. Invalid certificate cannot be applied by Twilio.

Authentication flow

The following chart demonstrates the authentication flow:



A user is authenticating on endpoint (which can be the user's laptop with NetIQ Windows Client installed or a website etc.) by SMS method.

1. The endpoint calls the NetIQ Advanced Authentication Server.
2. It validates the provided user's credentials and gets a phone number of the user from a used Repository.
3. NetIQ Advanced Authentication Server sends the request to a configured Voice Call Service Provider (Twilio) to call the user.
4. Voice Call Service Provider calls the user.
5. The user picks up the phone, listens to the answerphone and enters the PIN code followed by hash sign.
6. Voice Call Provider sends the entered PIN code to the NetIQ Advanced Authentication Server.
7. NetIQ Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTP/HTTPS protocol is used for the communication.

Access configuration

NetIQ Advanced Authentication Server - Voice Call Service Provider (HTTP/HTTPS, inbound/ outbound).

4.5.29 Configuring Server Options

NetIQ Advanced Authentication Server uses an HTTPS protocol. You should create a certificate file (PEM or CRT) and apply the existing SSL certificate on the server.

IMPORTANT: Smartphone and Voice Call authentication providers work only with valid SSL certificate, self-signed certificate will not work.

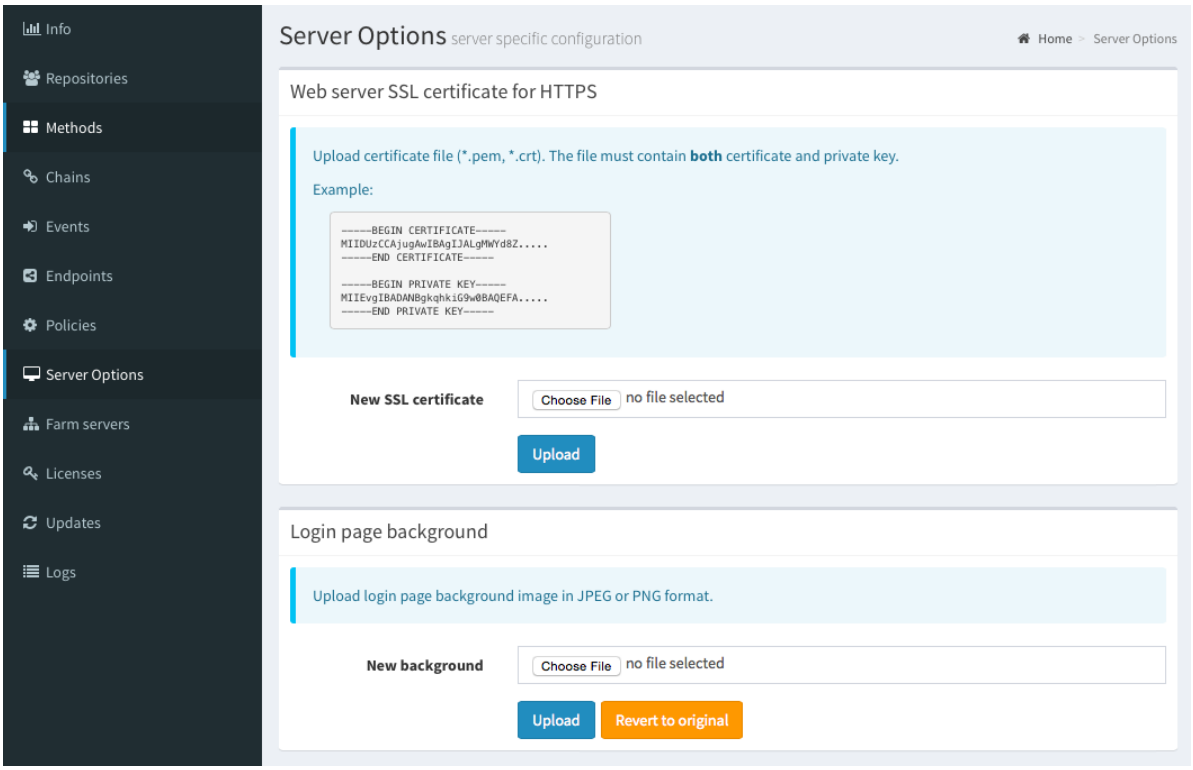
To specify the protocol that will be used by NetIQ Server, follow the steps:

1. Open the *Server Options* section.

2. Click the *Choose File* button and select a new SSL certificate. The file must contain the both certificate and private key.
3. Click *Upload* to upload the selected SSL certificate.

It's possible to set a custom login page background. It should be a JPEG or PNG image, a recommended resolution is 1920x774 px, 72 dpi. It's not recommended to use backgrounds which size exceeds 100KB. To apply a custom login page background, follow the steps:

1. Click *Choose File* in *Login page background* section.
2. Select the background file.
3. Click *Upload* to upload and apply the custom background.

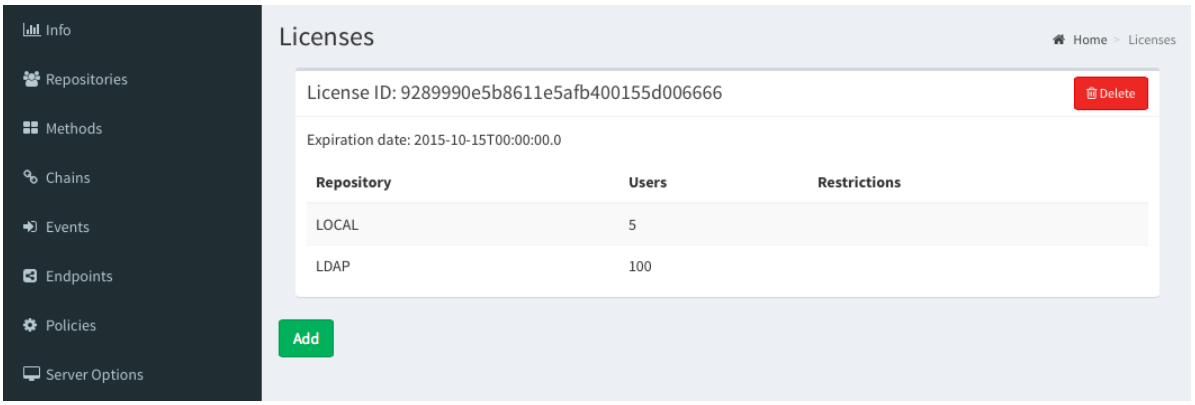


If you want to revert the settings to original click the *Revert to original* button.

4.5.30 Adding License

IMPORTANT: The temporary license is active for 30 days and will expire at the specified date. Authentication and access to the NetIQ Advanced Authentication Authentication Methods Enrollment will be inaccessible when the license is expired. Please contact your seller in advance to get and apply a permanent license.

If you need more time to get a permanent license, before expiration of the temporary license log on by local admin to the NetIQ Advanced Authentication Authentication Methods Enrollment to change the administrator's password. Otherwise in 42 days after the appliance deployment access to the appliance will be lost (Password).



To add the license for NetIQ Advanced Authentication Framework, follow the steps:

1. Open the *Licenses* section.
2. Click the *Choose File* button and select the valid license.
3. Click *Upload* to upload the license.

NetIQ Advanced Authentication takes a user's license within a first authentication. It occurs also if a user is logging in to the Self-Service Portal for a first time or a security officer is logging in to manage the user's authenticators.

TIP: To free up a user's license, exclude the user from a group which was assigned to the used chains. Then perform a synchronization for the repository in the Repositories section.

4.6 Default Ports for NetIQ Server Appliance

IMPORTANT: Ports 443 and 80 are used inside the NetIQ Server appliance and cannot be changed.

Port forwarding is supported but is not recommended. In this case the entire appliance will be available via the Internet. It is recommended to use reverse proxy to map only specific URLs.

NetIQ Server Appliance uses the following RFC standard ports by default:

Service	Port	Protocol	Usage
RADIUS	1812	TCP, UDP	Authentication
RADIUS	1813	TCP, UDP	Accounting
E-Mail Service	Variable	HTTPS	E-Mail Traffic
Voice Call Service	Variable	HTTPS	Voice Call Traffic
REST	443	HTTPS	All Communications
Smartphone	Variable	HTTPS	All Communications
Admin UI	443	HTTPS	All Communications
Enroll UI	443	HTTPS	All Communications
Server Update	443	HTTPS	Update channel: appliance - update server (191.239.210.107)

Service	Port	Protocol	Usage
Database replication	5432	TCP, UDP	Database replication between Master DB and Slave DB servers

IMPORTANT: Any port can be used in case of reverse proxying. E.g., https://dnsname:888/smartphone. There is reverse proxy redirect from port 888 to port 443 internally to appliance. Port 888 is used from outside, but port 443 is used inside the appliance.

4.7 Configuring Additional NetIQ Servers

In production environment it's strongly recommended to use more than one Authentication Server for the fault tolerance, load balancing and redundancy. You may install some NetIQ Server appliances. If you already have a Configuring DB Master Server server installed you can configure a new server to take one of the following roles:

- DB Slave Server is the copy of the server with master database. If the DB Master server is lost, the DB Slave may be converted to DB Master.
- Member Server is the web server without database.

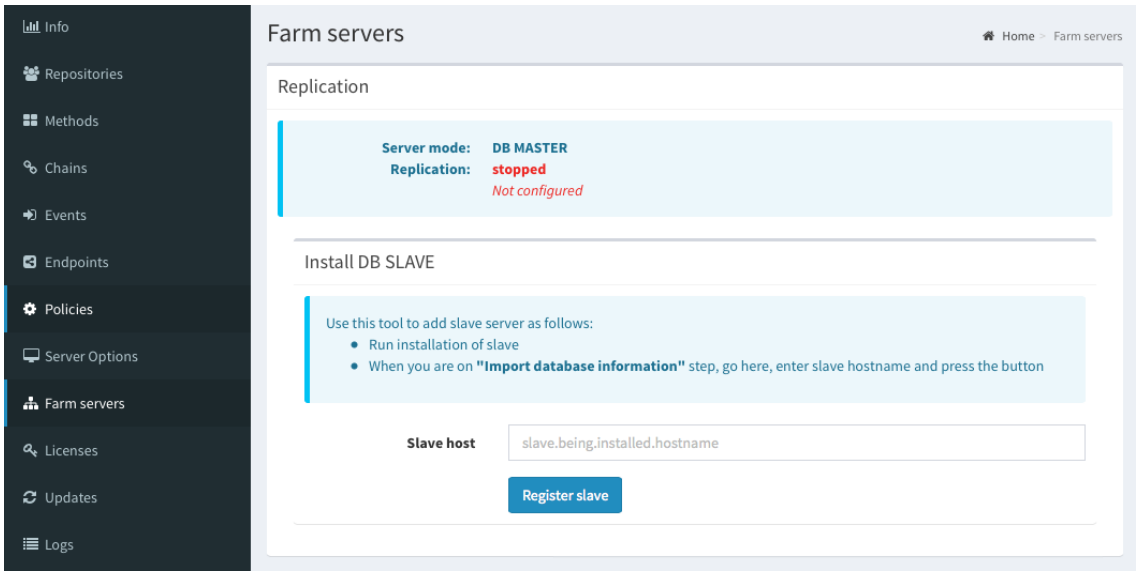
When you have the DB Slave server and Member server you may want to configure a *Load Balancer*. How to configure load balancer for NetIQ Advanced Authentication cluster.

Check an information about Architecture.

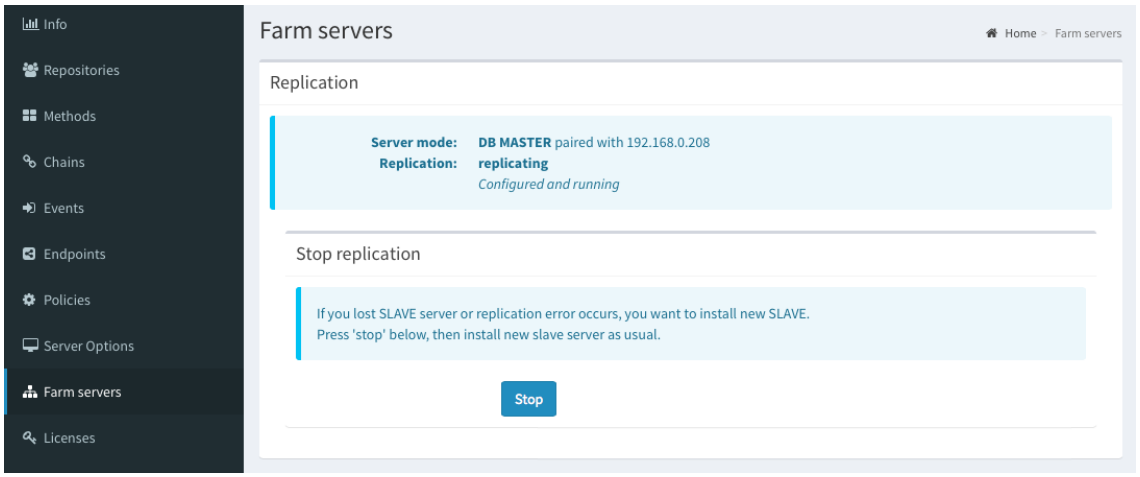
4.7.1 Managing Authentication Servers

The Farm servers section is used to manage *DB Slave* and *Member servers*. It's possible to manage the following actions:

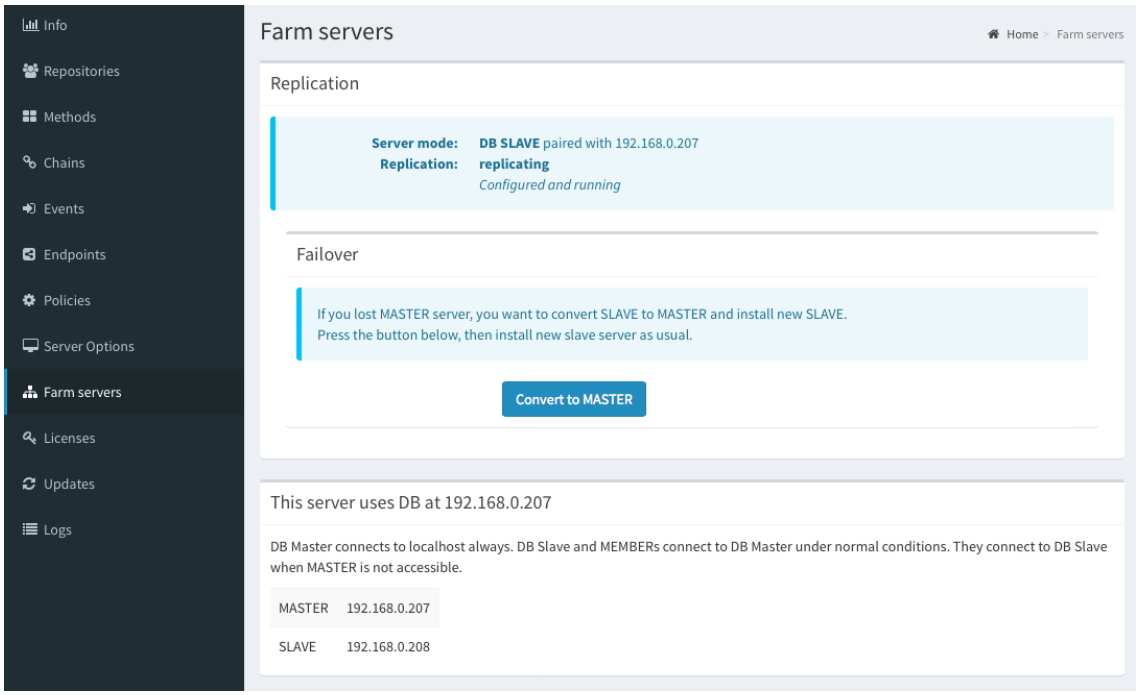
1. DB Slave Server.
2. Member Server.
3. *Check replication status*. If you have a DB Slave server, you may check status of replication between DB Master and DB Slave servers on top of the Farm servers section. If you see `replicating`, `configured and running`, it means that everything works properly. You may also see the red status `stopped`, `Not configured`. In this case in production environment it's strongly recommended to configure a DB Slave server.



4. *Stop replication* if you want to break replication with existing DB Slave. It may be used if you lost a used DB Slave server or want to install a new DB Slave server. To do it open the Farm servers section on DB Master server and click *Stop* button. You will need to wait few minutes after it.

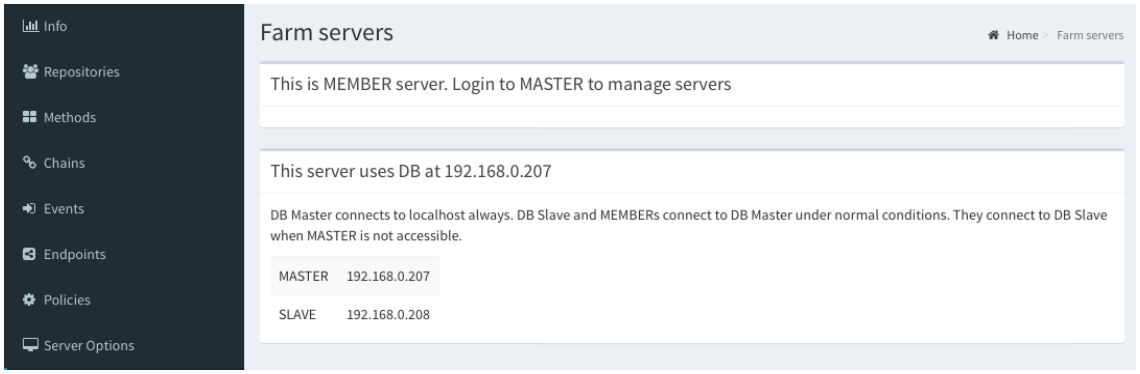


5. *Convert DB Slave to DB Master*. If you lost a used DB Master server you may open the Farm servers section on your DB Slave server and click *Convert to MASTER* button to make a new DB Master server from the current DB Slave.



IMPORTANT: The Advanced Authentication Framework stores the Radius Event settings only on a server where administrator performs the configuration (usually this is DB Master server). After conversion of DB Slave server to DB Master server the configuration may be lost. Open the Radius Event settings and click Save to apply the configuration.

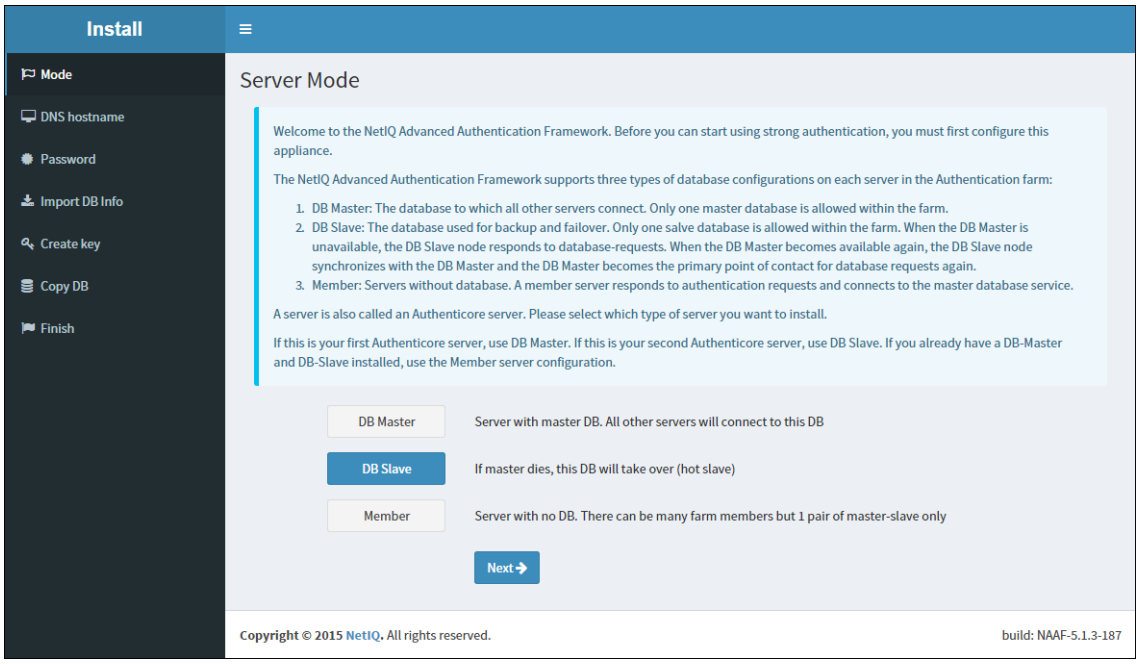
6. *Check information about DB Master and DB Slave servers*. On bottom of the Farm servers section you may find information about currently used DB Master and DB Slave servers.



4.7.2 DB Slave Server

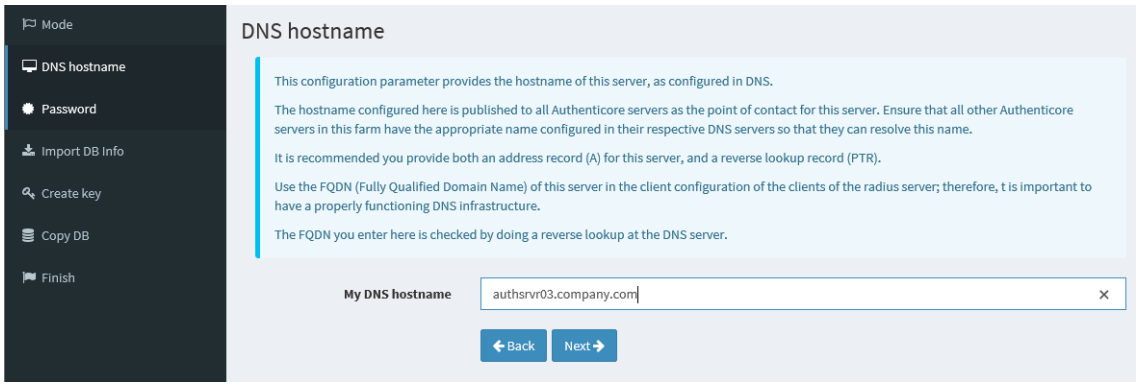
To configure the *DB Slave* server:

1. Go to the NetIQ Administrative Portal. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the *DB Slave* server mode and click *Next* to continue.

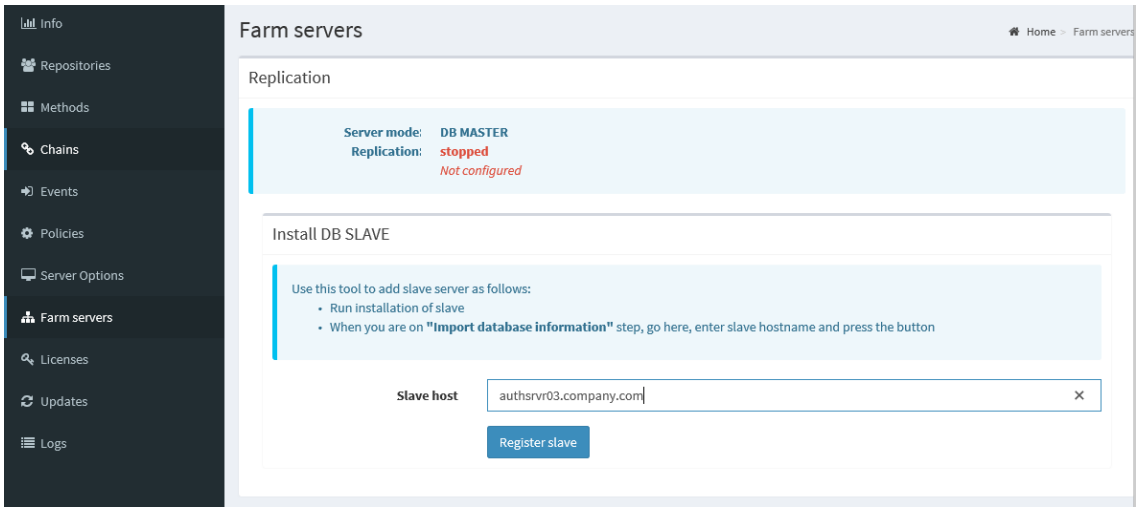


3. Specify the server DNS hostname. Click *Next* to continue.

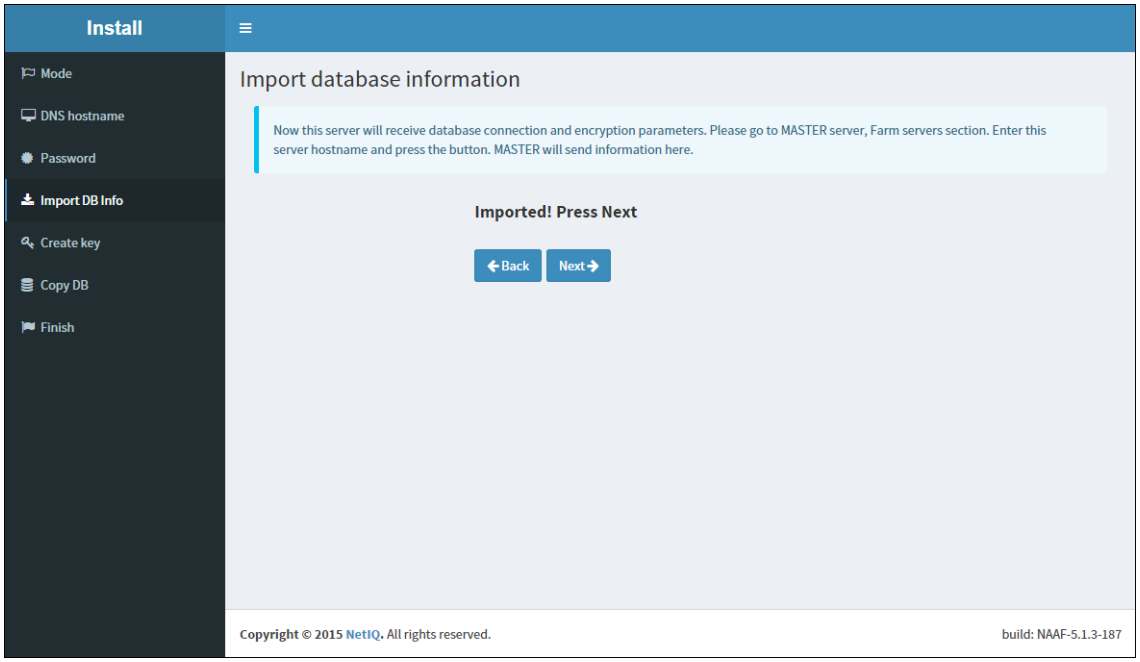
WARNING: It's not recommended to specify an IP address instead of DNS hostname, because it's not possible to change the information later.



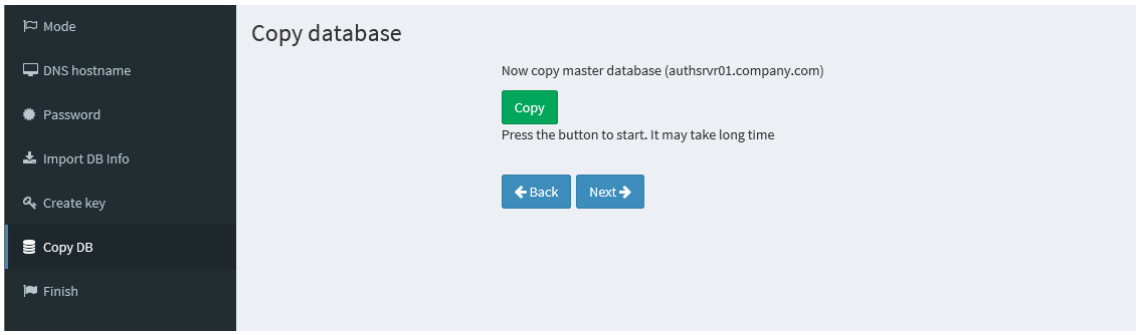
4. Go to the NetIQ Admin Interface of the DB Master server and open the *Farm servers* section. Enter the hostname of this server in the *Slave host* text field and click the *Register slave* button.



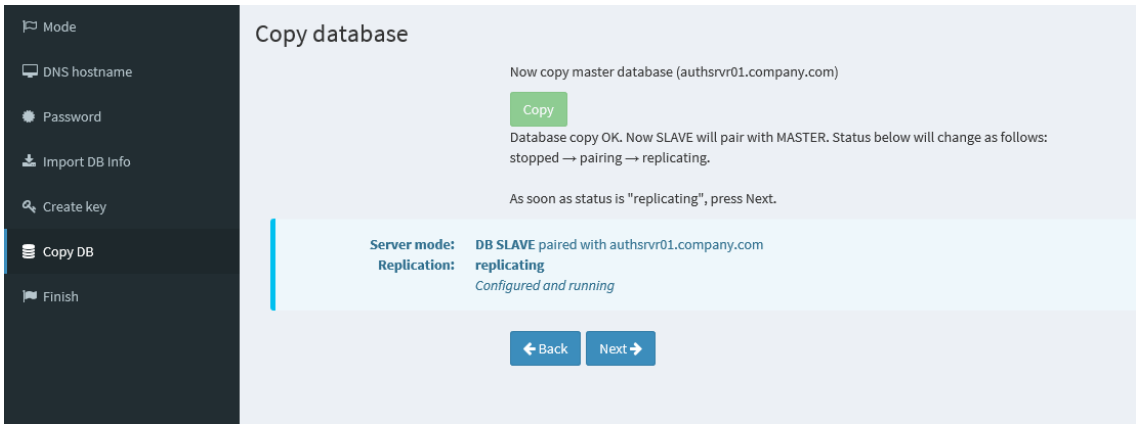
The DB Slave server starts copying database information from the DB Master server. Once the database information is imported, click *Next* to continue.



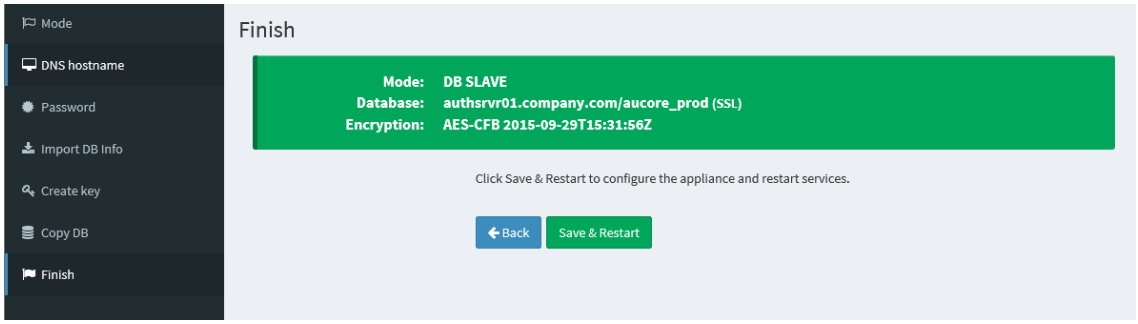
5. Click the *Copy* button to copy master database.



Once the status is moved to *replicating*, click *Next* to continue.



6. Click the *Save & Restart* button to write configuration and restart services. Services will be restarted within 30 seconds.



IMPORTANT: Only one DB Slave server can be installed.

If you lost your DB Slave server, go to the NetIQ Admin Interface of the DB Master server, open the *Farm servers* section and click *Stop*. Install a new DB Slave server.

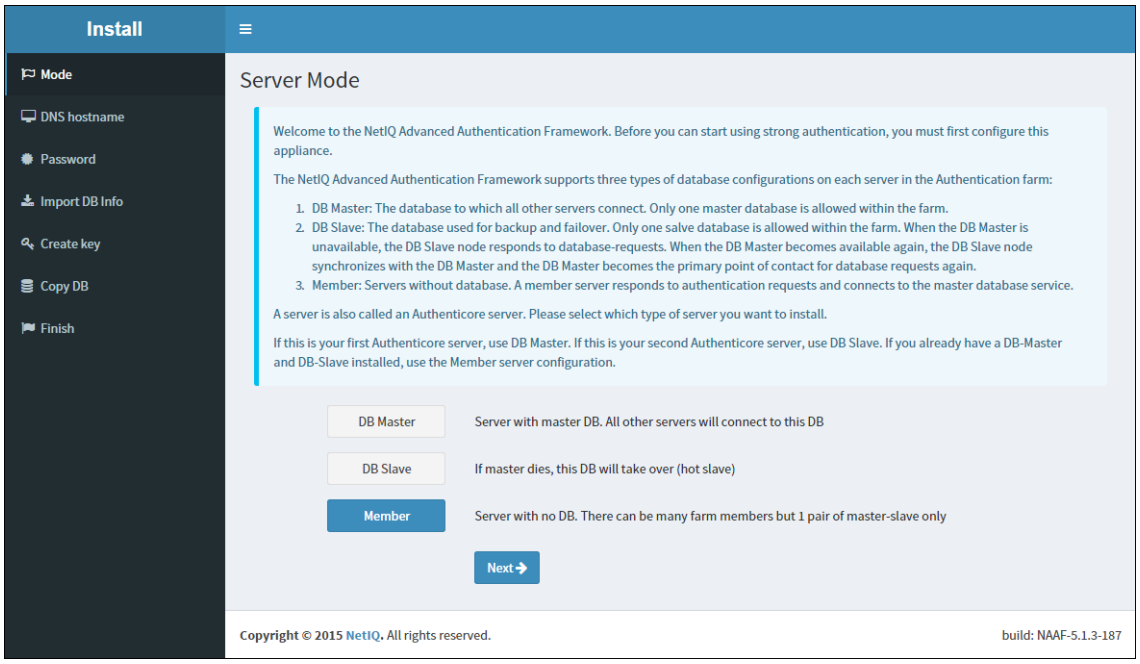
If you lost your DB Master server, you can convert DB Slave server to DB Master. Go to the NetIQ Administrative Portal of the DB Slave server, open the *Farm servers* section and click *Convert to Master*. After the server is converted, install a new DB Slave server.

4.7.3 Member Server

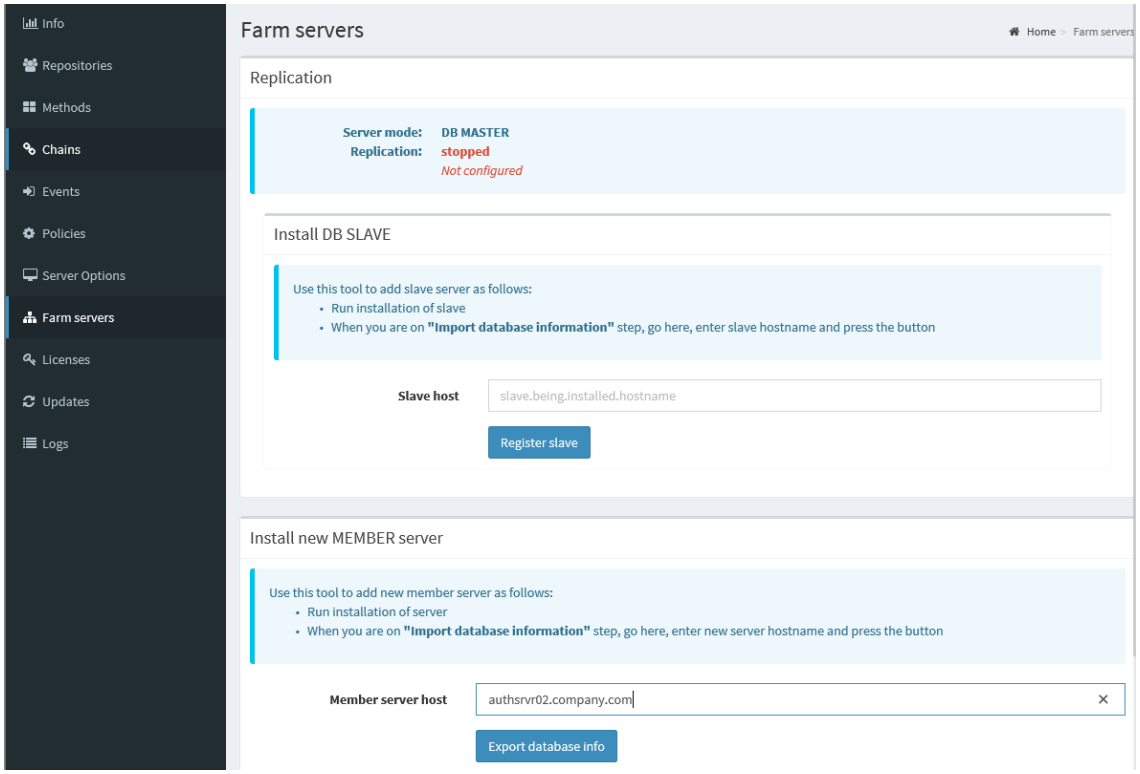
IMPORTANT: Multiple Member servers can be installed.

To configure the *Member* server:

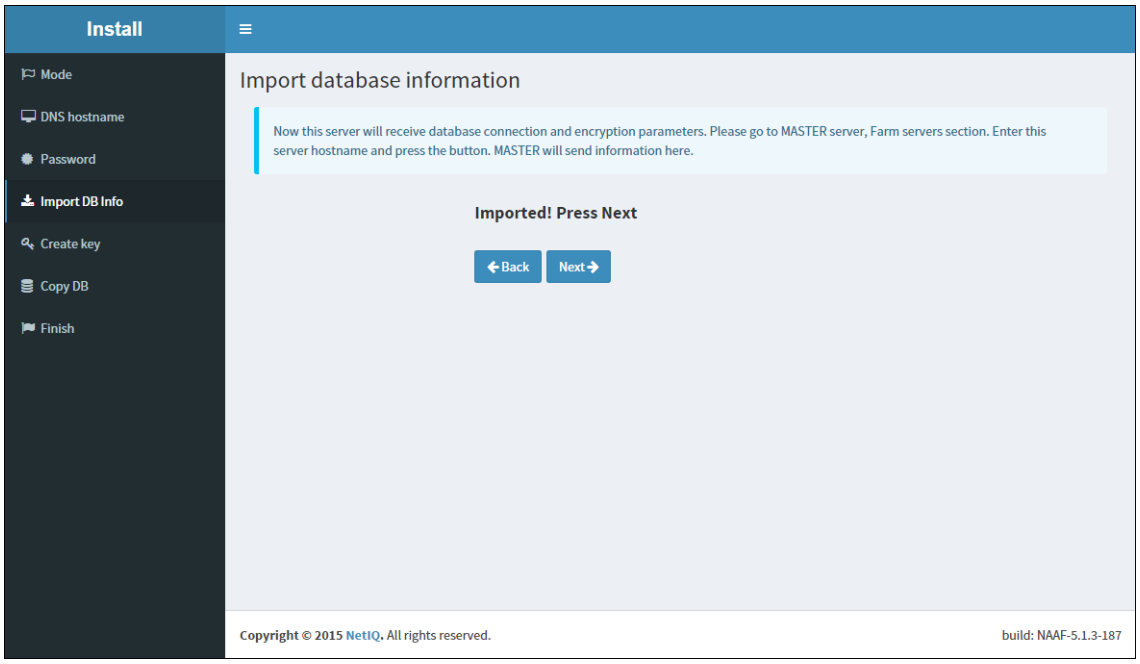
1. Go to the NetIQ Administrative Portal. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the *Member* server mode and click *Next* to continue.



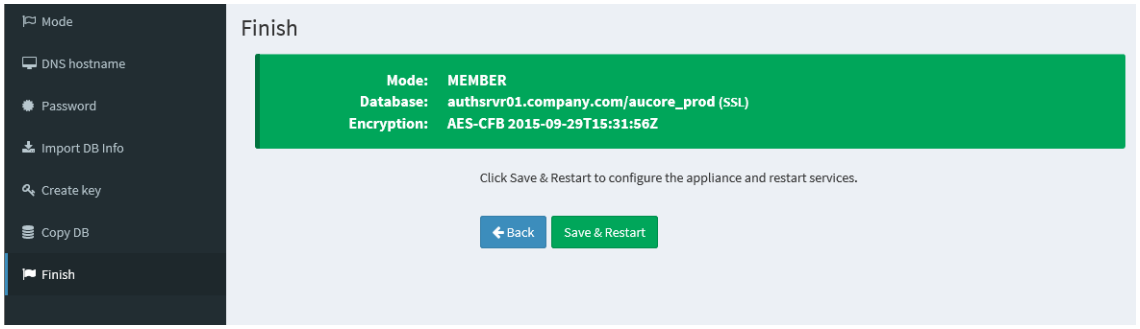
3. Go to the NetIQ Administrative Portal of the DB Master server and open the *Farm servers* section. Enter the hostname of this server in the *Member server host* text field and click the *Export database info* button.



The Member server starts copying database information from the DB Master server. Once the database information is imported, click *Next* to continue.



4. Click the *Save & Restart* button to write configuration and restart services. Services will be restarted within 30 seconds.



4.7.4 How to configure load balancer for NetIQ Advanced Authentication cluster

Load balancer can be installed and configured via third party software. Below is an example of how to install and configure nginx as load balancer on Ubuntu 14.

Target configuration:

	Hostname	IP address	Role	Operation System
Domain controller	win-dc	192.168.1.42	AD DS, DNS	Windows Server 2008 R2
NAAF 5.1 master	naafmaster	192.168.1.43	NAAF Master server	NAAF 5.1.2
NAAF 5.1 slave	naafslave	192.168.1.41	NAAF Slave server	NAAF 5.1.2
Load balancer	loadbalancer	192.168.1.40	Nginx load balancer	Ubuntu 14

Before starting the configuration, please make sure that the following requirements are fulfilled:

- Repository is configured in NetIQ Advanced Authentication appliance.
- Both NetIQ Advanced Authentication servers are installed and configured as Master and Slave.
- Appropriate entries are added to DNS.
- Ubuntu 14 is installed.

To configure Load Balancer for NetIQ cluster, it is required to install nginx on Ubuntu 14 and configure it.

Installing nginx on Ubuntu 14

To install nginx on Ubuntu 14, follow the steps:

1. Open the following source list:
   - sudo nano /etc/apt/sources.list
2. Add necessary entries:
   - `deb http://nginx.org/packages/ubuntu/ trusty nginx`
   - `deb-src http://nginx.org/packages/ubuntu/ trusty nginx`
3. Update repository and install nginx:
   - apt-get update
   - `apt-get install nginx`
4. Start nginx and make sure that web server is working:
   - `sudo service nginx restart`
5. Open your browser and go to web server http://192.168.1.40 or http://loadbalancer.

Configuring nginx

The following load balancing mechanisms/methods are supported in nginx:

- *round-robin* - requests to the application servers that are distributed in a round-robin fashion
- *least-connected* - next request assigned to the server with the least number of active connections
- *ip-hash* - a hash-function that is used to determine what server should be selected for the next request (based on the client's IP address)

This article describes only round-robin configuration. To configure nginx, follow the steps:

1. Backup original configuration file: `sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf_original`.

2. Open the *nginx.conf* file and replace with following:

```
user nginx;
error_log /var/log/nginx/error.log warn; # error log location
pid /var/run/nginx.pid; # process id file
# limit number of open sockets. Debian default max is 1024, ensure nginx not
open all the sockets.
worker_processes 1;
events {
worker_connections 900; # 512 is default
}
# worker_processes auto; # ssl needs CPU
http {
include /etc/nginx/mime.types;
default_type application/octet-stream;
log_format main '$remote_addr - $remote_user [$time_local] "$request" '
'$status $body_bytes_sent "$http_referer" '
'"$http_user_agent" "$http_x_forwarded_for"';
access_log /var/log/nginx/access.log main; # access log location
sendfile on;
# keepalive default is 75
# keepalive_timeout 10;
gzip on;
gzip_static on;
gzip_comp_level 5;
gzip_disable msie6;
gzip_min_length 1000;
gzip_proxied expired no-cache no-store private auth;
gzip_vary on;
gzip_types text/plain text/css application/json application/javascript
text/xml application/xml application/rss+xml application/atom+xml;
ssl_certificate /etc/nginx/cert.pem;
ssl_certificate_key /etc/nginx/cert.pem;
ssl_session_cache shared:SSL:2m; # 1m stores 4000 sessions, default expire 5
min
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # disable TLSv3 - POODLE vulnerability
resolver 192.168.1.42 valid=300s ipv6=off; # ip address of DNS
resolver_timeout 10s;
upstream web {
#server naafmaster.company.local:443 resolve;
#server naafslave.company.local:443 resolve;
server 192.168.1.43:443;
server 192.168.1.41:443;
}
server {
#listen 80;
listen 443 ssl;
location / {
proxy_pass https://web;
proxy_set_header HOST $host;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
}
}
```

3. Copy certificate from any NetIQ Advanced Authentication server in cluster from the directory */etc/nginx/cert.pem* to the same directory on load balancer.
4. Go to https://loadbalancer/admin page and make sure that connection was redirected to NetIQ cluster.

IMPORTANT: Nginx can be installed and configured on any Linux supported by nginx.

Additional information on nginx configuration can be found at http://nginx.org/en/docs/ (http://nginx.org/en/docs/).

4.8 Authentication Methods Enrollment

NetIQ Server supports the following ways to enroll the authentication methods:

- *Automatic enrollment* which is supported for *SMS*, *Email*, *RADIUS* and *LDAP Password* methods.

  The methods will be enrolled automatically if Chains containing them are assigned to any Event.

- *Enrollment by Administrator* is supported for *OATH Tokens*.

  An administrator can import tokens from PSKC or CSV files in *NetIQ* Advanced Authentication *Administrative Portal* - *Methods* - *OATH OTP* - *OATH Tokens* tab. From the same view it's possible to assign tokens to the specific users.

- *Enrollment by Security Officer*

  A security officer can access the *NetIQ*Advanced Authentication *Helpdesk Portal* by the following address: https://<*NetIQ* `Server`>/helpdesk where it's possible to enroll the authentication methods for users. A security officer must be a member of *Enroll Admins* group (*Repositories* - click *Edit* on *LOCAL* - *Global Roles* tab) to perform management of users' authenticators.

- *Enrollment by User*

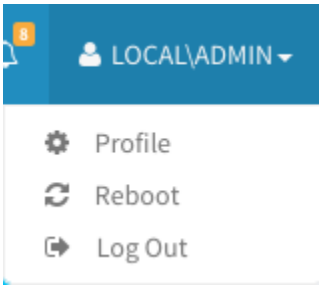
  A user can access the *NetIQ*Advanced Authentication *Self-Service Portal* by the following address: https://<*NetIQ* `Server`>/account where it's possible to enroll any of permitted authentication methods.

5 Advanced Authentication Server Maintenance

This section is intended for system administrators and contains information about maintenance of environment which contains the solution.

To restart the NetIQ Advanced Authentication Server appliance open the NetIQ Advanced Authentication Administrative Portal and use a menu of top right corner. Right click the user name and click *Reboot*.

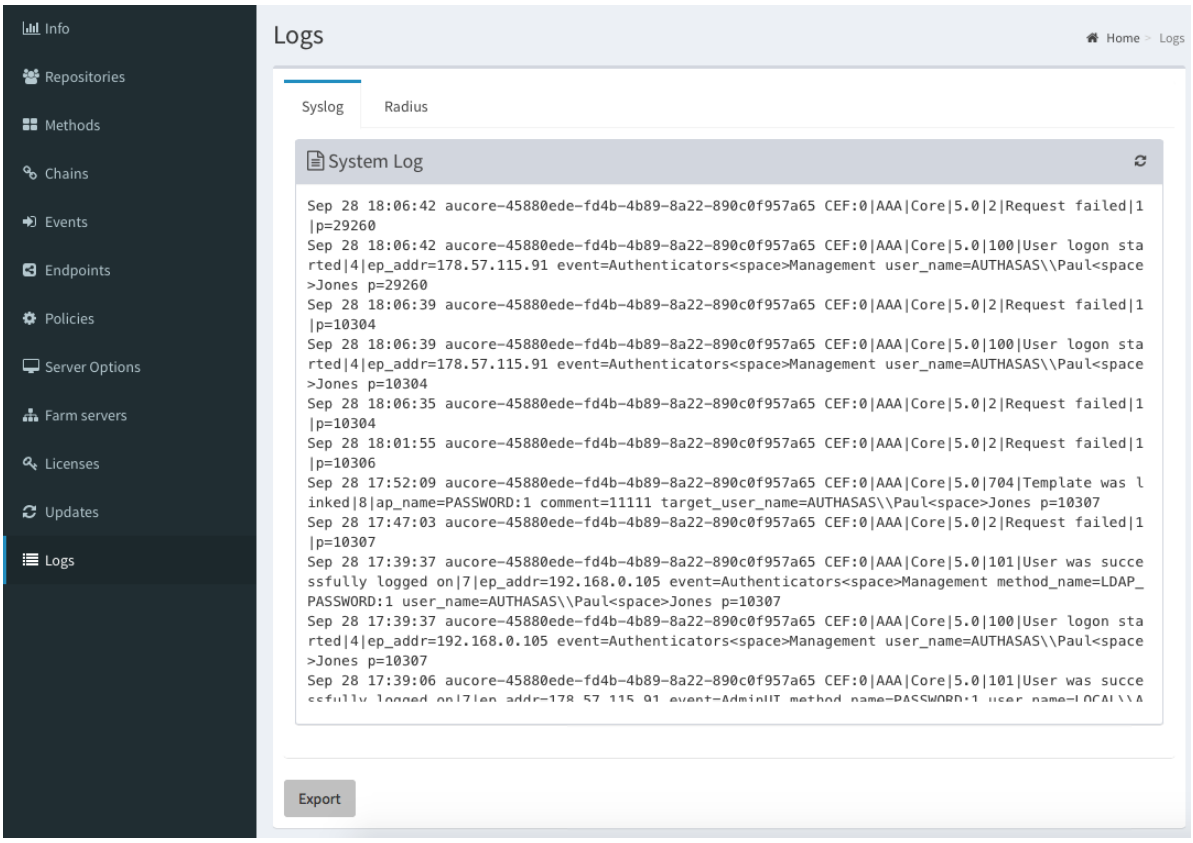
Using the *Profile* menu item you can also switch to the Self-Service Portal. To log out from the Administrative Portal use the *Log Out* button.



In this chapter:

5.1 Logging

The *Logs* section contains *System log* and *RADIUS Server log*. They are available on the appropriate tabs.



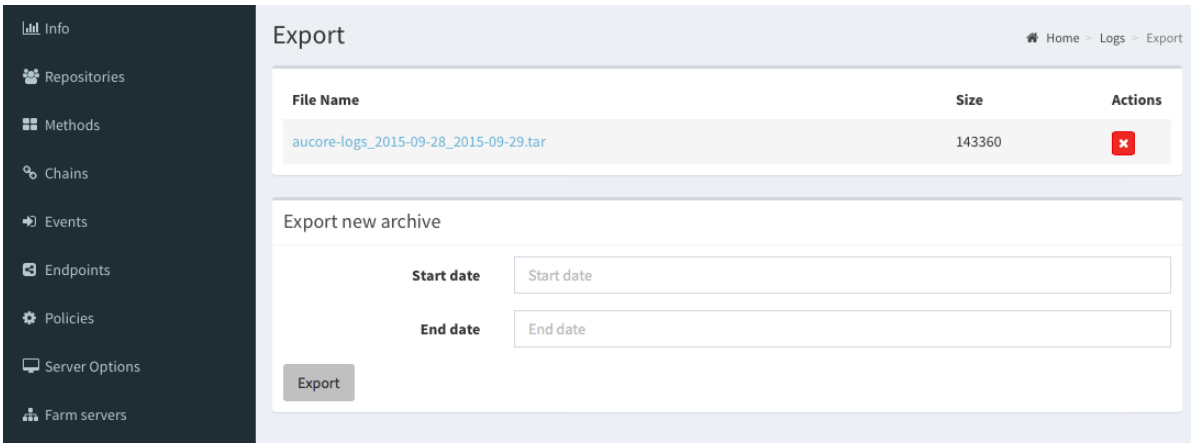
The System log contains the following information events:

- Failed to join endpoint
- No rights to join endpoint
- Endpoint joined
- Failed to remove endpoint
- No rights to remove endpoint
- Endpoint remove
- Failed to create endpoint session
- Endpoint session ended
- Failed to create endpoint session
- Invalid endpoint secret
- Endpoint session started
- Failed to create local user
- Local user was created
- Failed to remove local user
- Local user was removed
- Repository configuration was changed
- Failed to add repository
- New repository was added
- Request failed

- Server started
- Server stopped
- Server unexpectedly stopped
- Failed to assign template to the user
- Template was assigned to the user
- Failed to change template
- Template was changed
- Failed to enroll template for the user
- Template was enrolled for the user
- Failed to link template
- Template was linked
- Failed to remove template link
- Template link was removed
- Failed to remove template
- Template was removed
- Failed to create user
- User was created
- User can't enroll the assigned template
- User enroll the assigned template
- User was failed to authenticate
- User logon started
- User was successfully logged on
- User was switched to different method
- User do not want logon by phone but Twilio calling
- User read app data
- User write app data

It's possible to export the log files. To perform it follow the steps below:

1. Scroll down on the Logs page and click *Export* button.
2. Specify a *Start date* and *End date* to determine the required logging period.
3. Click *Export* button. A *File Name* block will appear.
4. Click on a name of the logs package (aucore-logs_<logging_period>.tar) to download it.

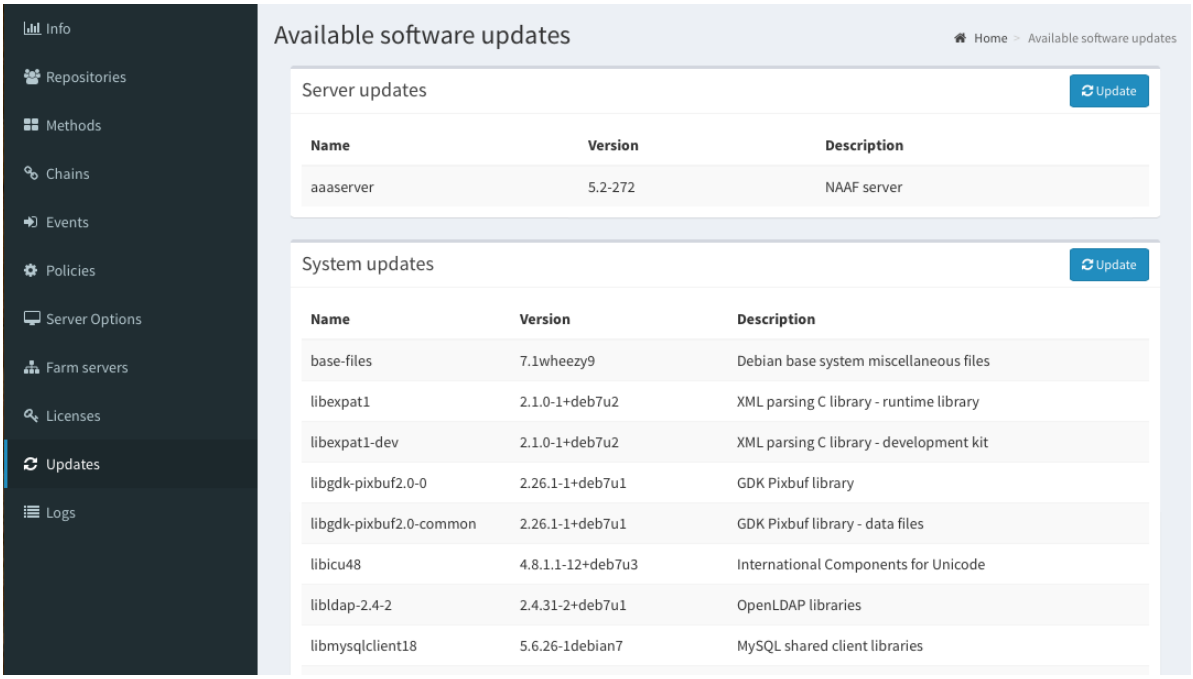


To configure logs forwarding to a third-party syslog server Configuring Logs Forwarding.

5.2 NetIQ Advanced Authentication Framework Updates

IMPORTANT: After upgrade of NetIQ Advanced Authentication 5.1.3 with already configured repositories to 5.2, open *Repositories* section and click *Sync now* button for the configured repositories. Wait few minutes while synchronization is performed.

To check for updates open the NetIQ Advanced Authentication Administrative Portal and switch to *Updates* section. You may get a list of operating system updates, because NetIQ Advanced Authentication checks for these updates automatically. To check for the NetIQ Advanced Authentication Server updates, please click *Check for updates* button.



NOTE: Operating systems updates must be applied before the NetIQ Advanced Authentication Server updates.

IMPORTANT: Upgrade must be done in period of lowest users/ security officers activity and in shortest time period. It's recommended to minimize the time period when NetIQ Advanced Authentication DB Master server is upgraded, but the DB Slave servers are not, because replication of non-synced DBs may break the DB Slave servers.

To perform the update please follow the instruction:

1. Make snapshots for all NetIQ Advanced Authentication servers. Try to do it in minimal time period.
2. Stop load balancer, or if you don't use it turn off the NetIQ Advanced Authentication DB Slave server, turn off the NetIQ Advanced Authentication Member servers.
3. Upgrade the NetIQ Advanced Authentication DB Master server, restart it.

   IMPORTANT: After upgrade of DB Master to v5.2 it's required to log on to web services of DB Slave and Member servers using uppercase name of repository and user name. E.g. LOCAL\ADMIN or ADMIN. When the upgrade is done you will be again able to use lower case names. The user names and repository names in v5.2 are not case sensitive.
4. Turn on the NetIQ Advanced Authentication DB Slave server one-by-one and upgrade it, restart it.
5. Turn on the NetIQ Advanced Authentication Member servers one-by-one and upgrade them, restart them.
6. Start load balancer.
7. Wait 17 minutes when all servers are upgraded and check Farm Servers tab in Administrative Portal on the both DB Master and DB Slave Servers to ensure that the replication still works. In case of problems with replication, reinstall DB Slave Server.
8. Ensure that the users are still able to authenticate on their endpoints.
9. Upgrade plugins if applicable.
10. Upgrade few test endpoints and use them during few days, collecting a feedback.
11. Upgrade the rest endpoints.

IMPORTANT: You may get the error "`Configured and running. Replication conflict. Fix: stop replication and reinstall DB2 server`" on the *Farm servers* section. To fix this it's required to re-install the NetIQ Advanced Authentication DB Slave server.

6 Troubleshooting

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

In this chapter:

6.1 Fatal error while trying to deploy ISO file and install in graphic mode

Description:

While trying to install NetIQ Server appliance, we get the following fatal error: `"Server is already active for display 0. If this server is no longer running, remove /tmp/ .XO-lock and start again"`.

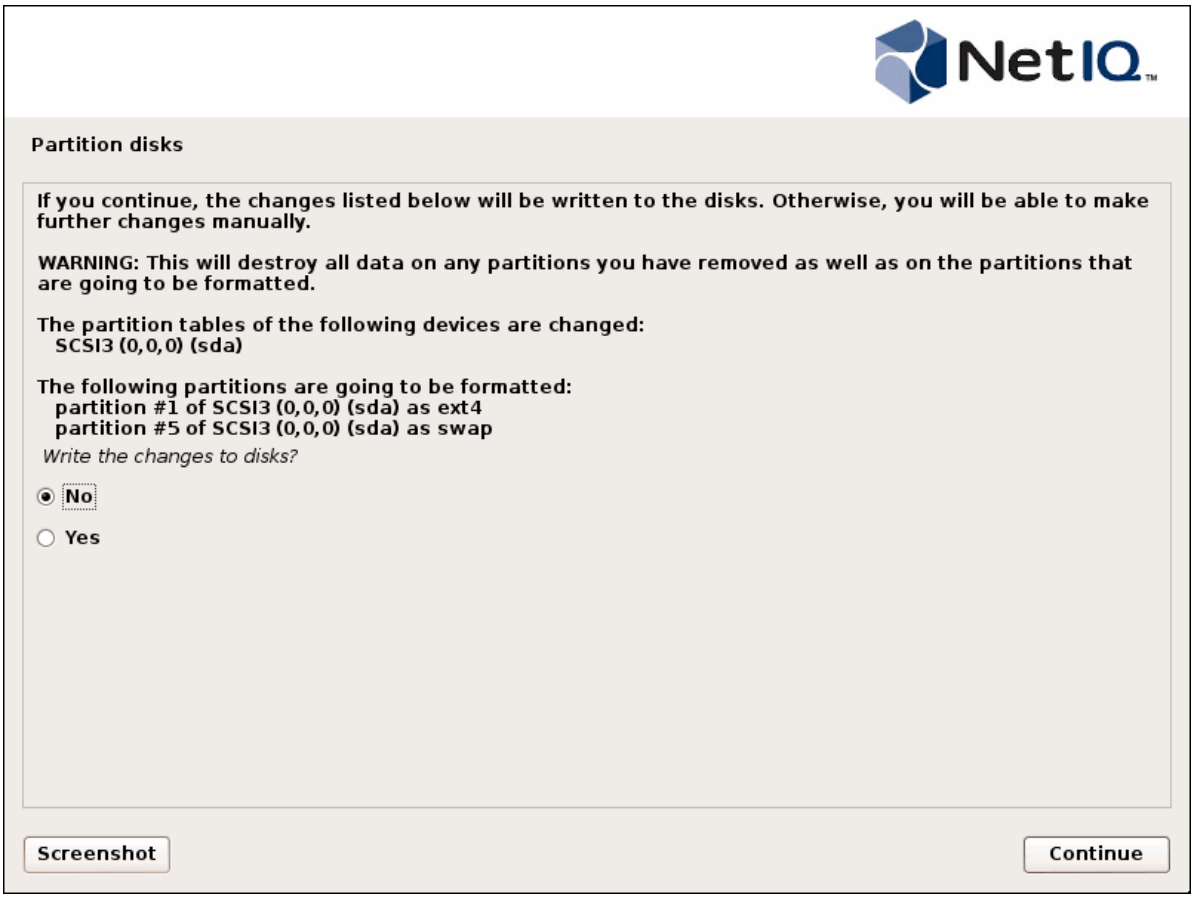
Solution:

This message is asking to cancel installation. You clicked *Continue* without selecting *I agree* at the bottom of *End User License Agreement*. As a result *I don't agree* was automatically preselected and *Yes* was selected on the next screen. Please run the installer, select *I agree* and continue installation.

6.2 Partition Disks

Description:

The following dialog box is installed during the installation of the NetIQ Server:



Cause:

You are installing NetIQ Server on the drive which contains data already.

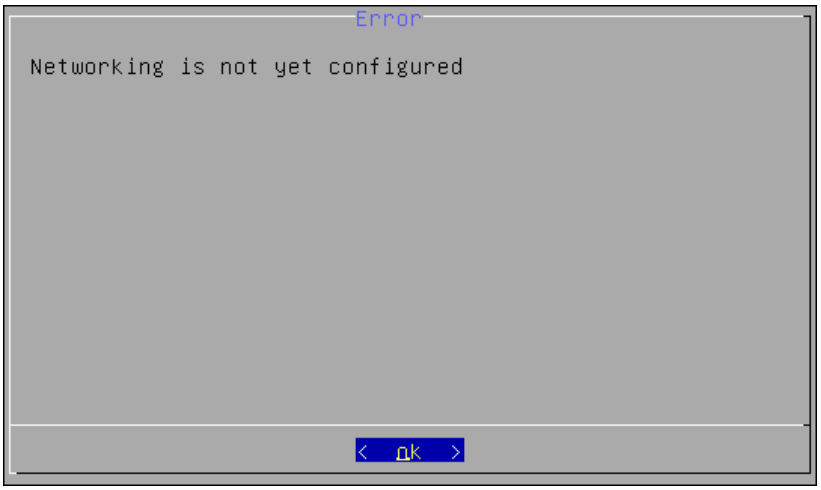
Solution:

NetIQ Server installer suggests you to perform disk partitioning. It will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted. To perform disk partitioning, select *Yes* and click *Continue*.

6.3 Networking Is Not Configured

Description:

After the installation of NetIQ Server appliance, the following error is displayed:



Cause:

Your network is not using DHCP protocol.

Solution:

Select *OK* and configure networking manually using the *Configuration Console*. For more information, see the Configuring Appliance Networking chapter.

6.4 Error "Using a password on the command line interface can be insecure"

Description:

I have set up DB Master and proceeded to setting up DB Slave. While copying the DB Master database, the following error is displayed: `"Error. (Exception) Warning: Using a password on the command line interface can be insecure. Warning: Using a password on the command line interface can be insecure. mysqldump: Got error: 1045: Access denied for user 'aunet'@'192.168.3.47' (using password: YES) when trying to connect".` 192.168.3.47 is the IP address of DB Slave.

Cause:

The error occurs due to the incorrect reverse DNS and incorrect hostname specified during installation:

- while installing the DB Master, the pre-populated *aucore.your-router* DNS hostname was selected
- DB Slave is up and re-registered the *aucore* host in DHCP/DNS on the router
- the pre-populated *aucore.your-router* DNS hostmane was selected on DB Slave

Solution:

The pre-populated DNS names cannot be used during the installation. In such case you must enter IP address. DNS hostnames should be specified on the corporate DNS server.