NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

Introduction

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

Warning. This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

Important notes. This sign indicates important information you need to know to use the product successfully.

Notes. This sign indicates supplementary information you may need in some cases.

Tips. This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items and buttons are put in bold type, e.g.: the **Logon** window.

System Requirements

 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
- 1 GB RAM

Supported browsers for Admin Web Console and Enrollment Portal:

- Internet Explorer 10.0 and later
- Google Chrome 40.0 and later
- Mozilla Firefox 36.0 and later
- Opera 27.0 and later

NetIQ Advanced Authentication Framework Overview

In this chapter:

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

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 Admin Interface

Architecture

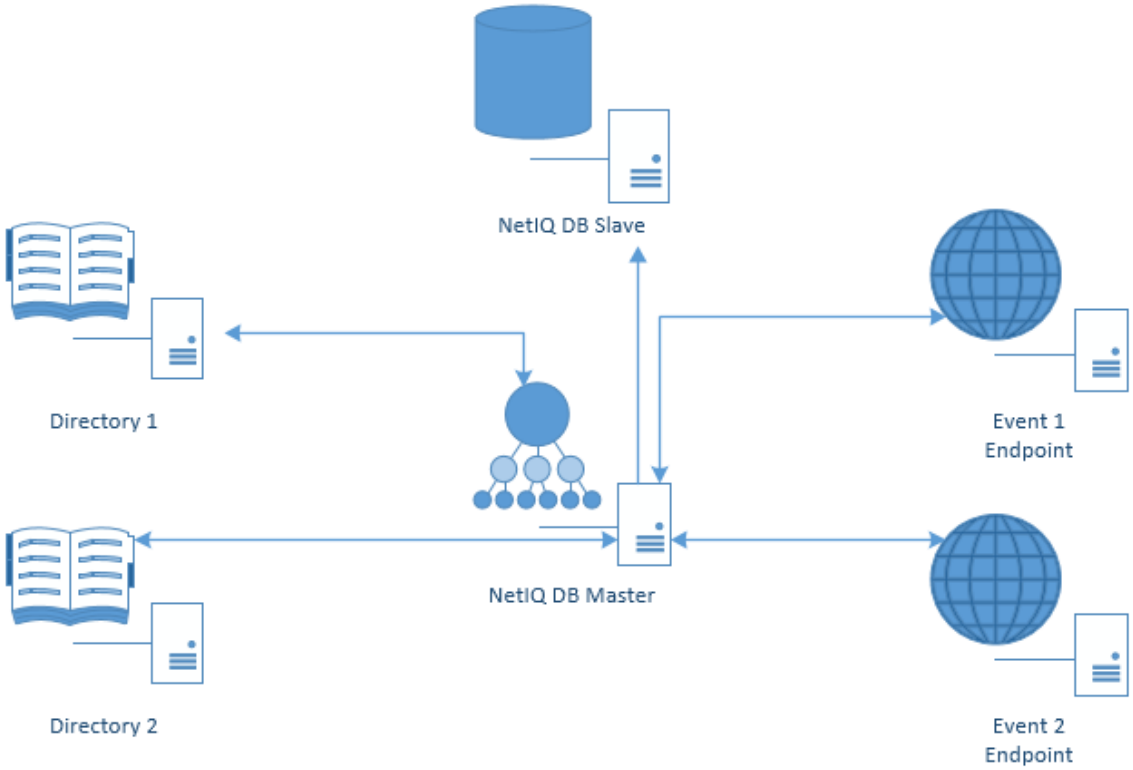
In this chapter:

Basic Architecture

This diagram shows the basic architecture with Authasas Advanced Authentication v5. Authasas 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.

Enterprise Architecture

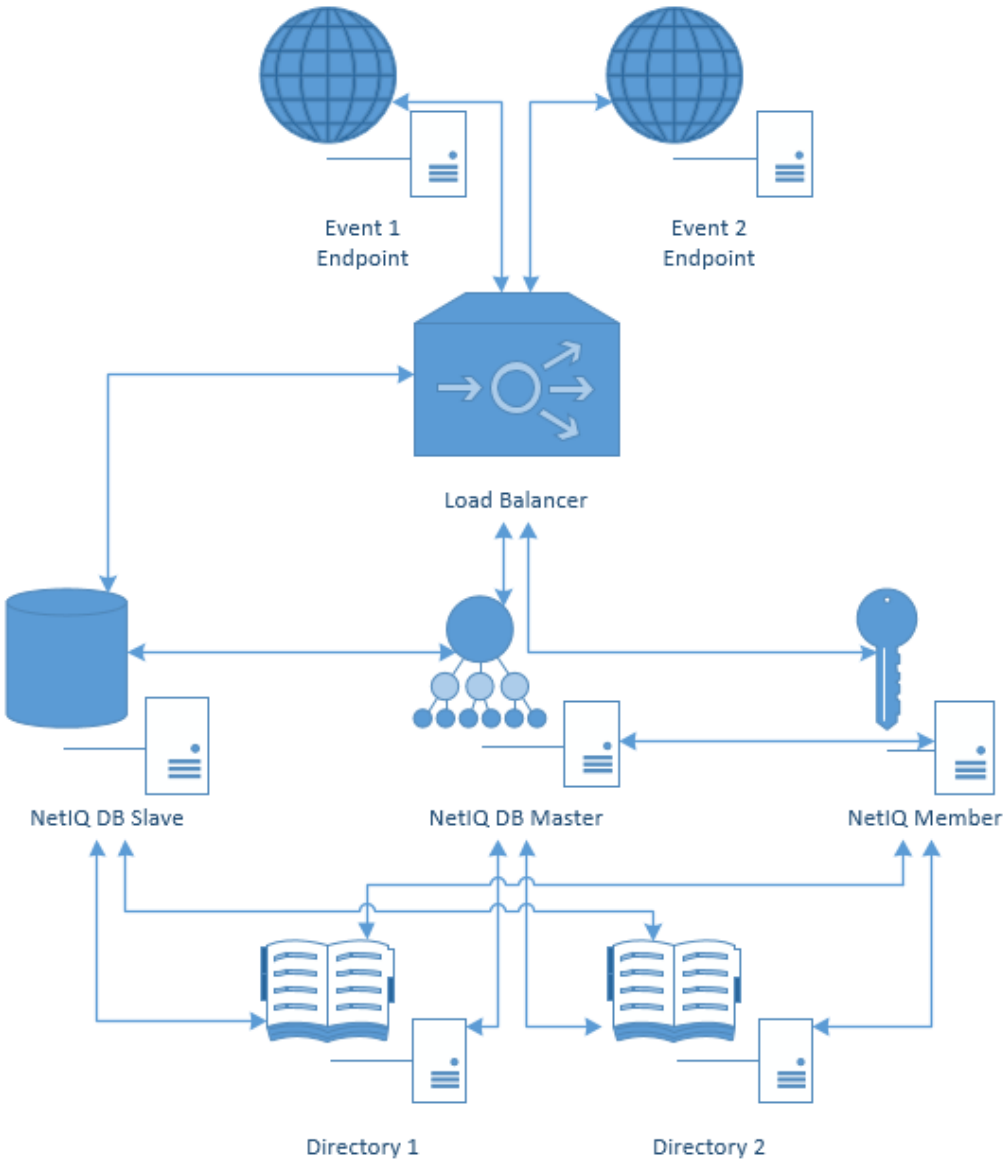
The following diagram shows interaction between DB Master, several directories and events. DB Master interacts at the same time with DB Slave, which contains the copy of the DB Master database. If DB Master dies, DB Slave will take over (hot slave).



Enterprise Architecture with Load Balancer

For more information on how to configure Load Balancer, check the following article.

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.



Terms

In this chapter:

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.

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.

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.

NetIQ Server Appliance Deployment

In this chapter:

Installing NetIQ Server Appliance

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

- Graphic Mode
- Text Mode

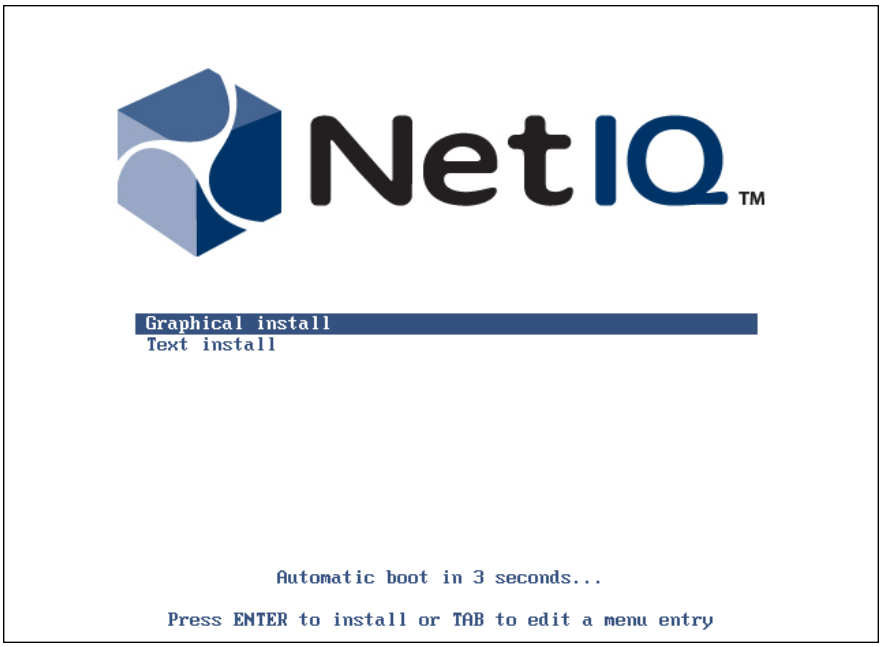
Graphic Mode

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

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

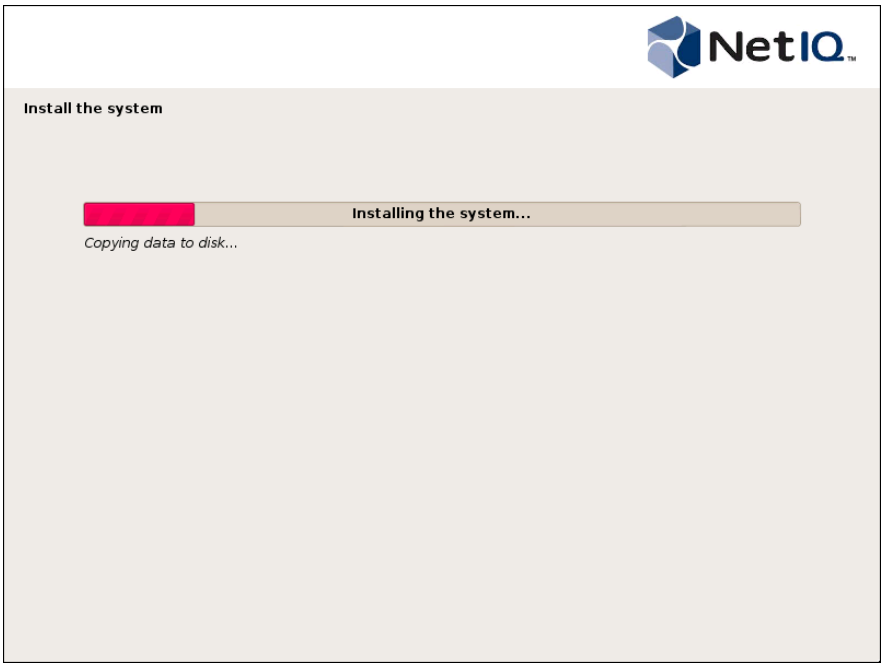
To install NetIQ Server appliance in the graphic mode:

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

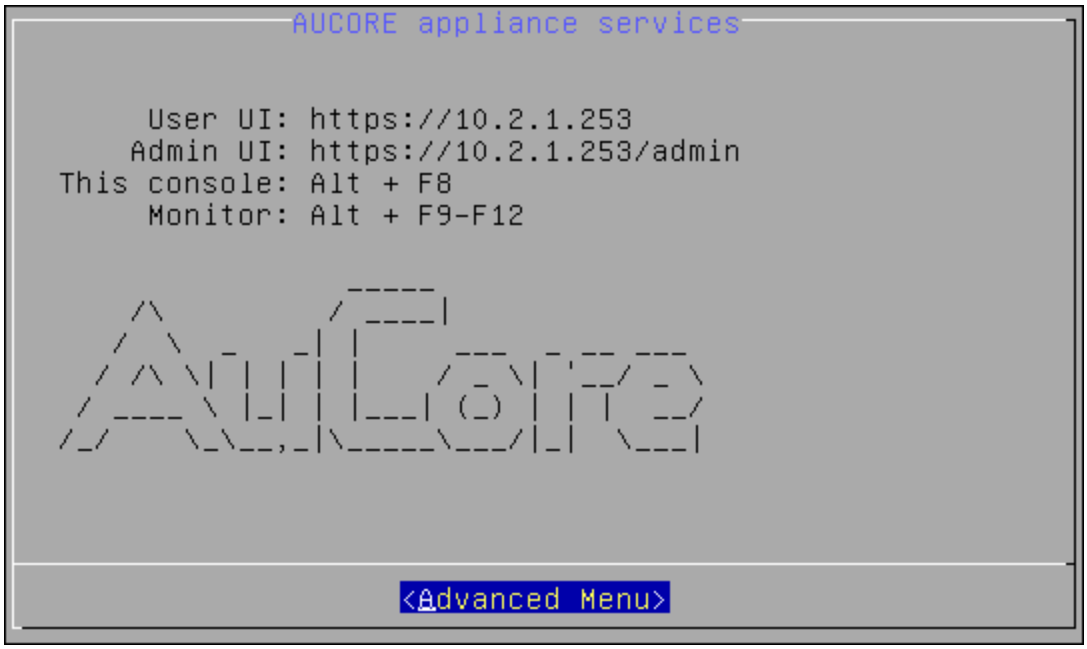


2. Read the license agreement. Select **I agree** at the bottom and click **Continue**.

3. The installation will be automatically started.



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

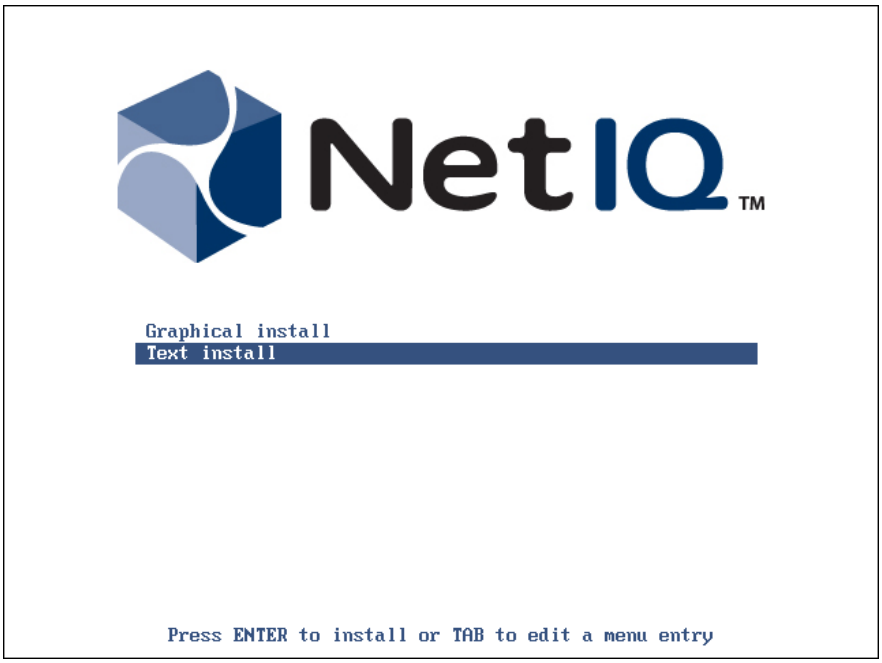


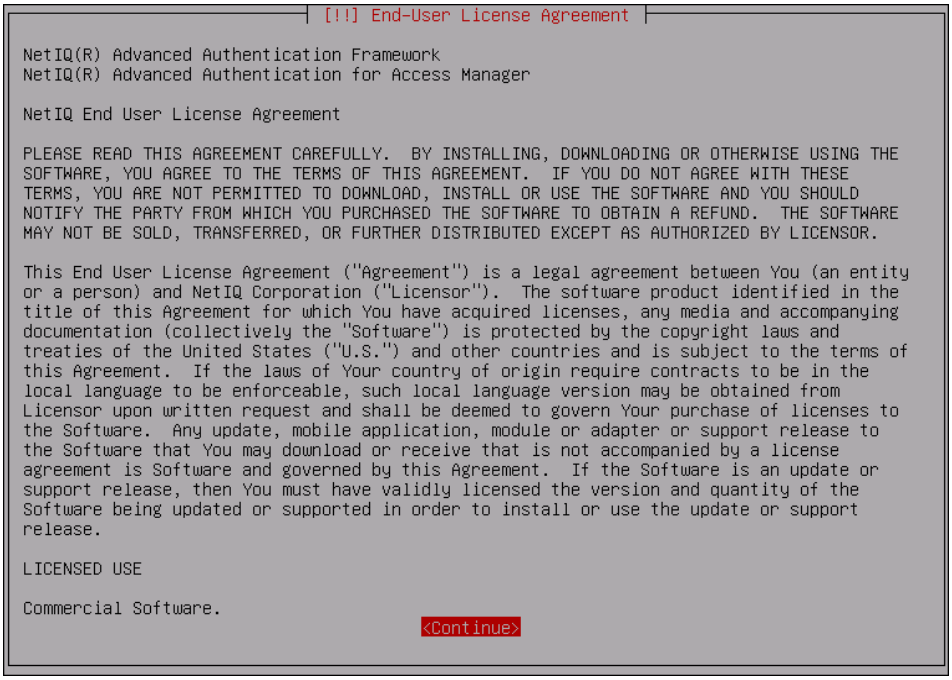
Text Mode

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.

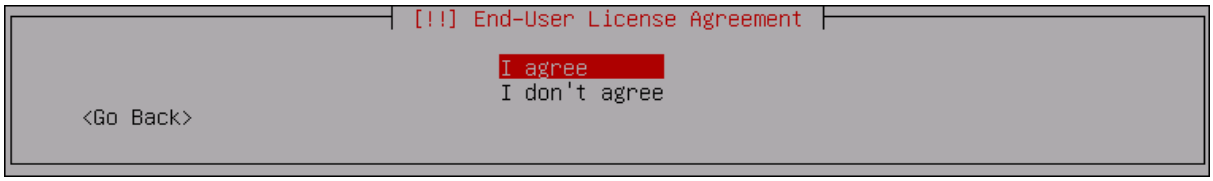
To install NetIQ Server appliance in the text mode:

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

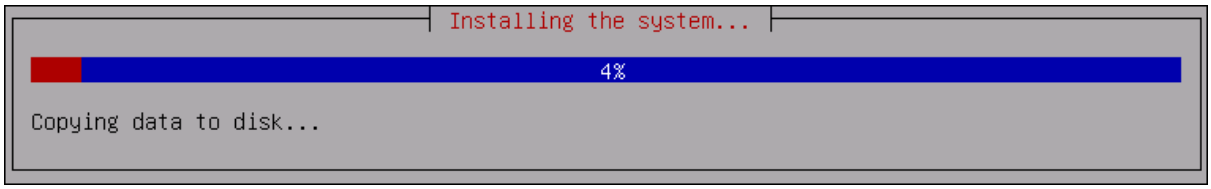




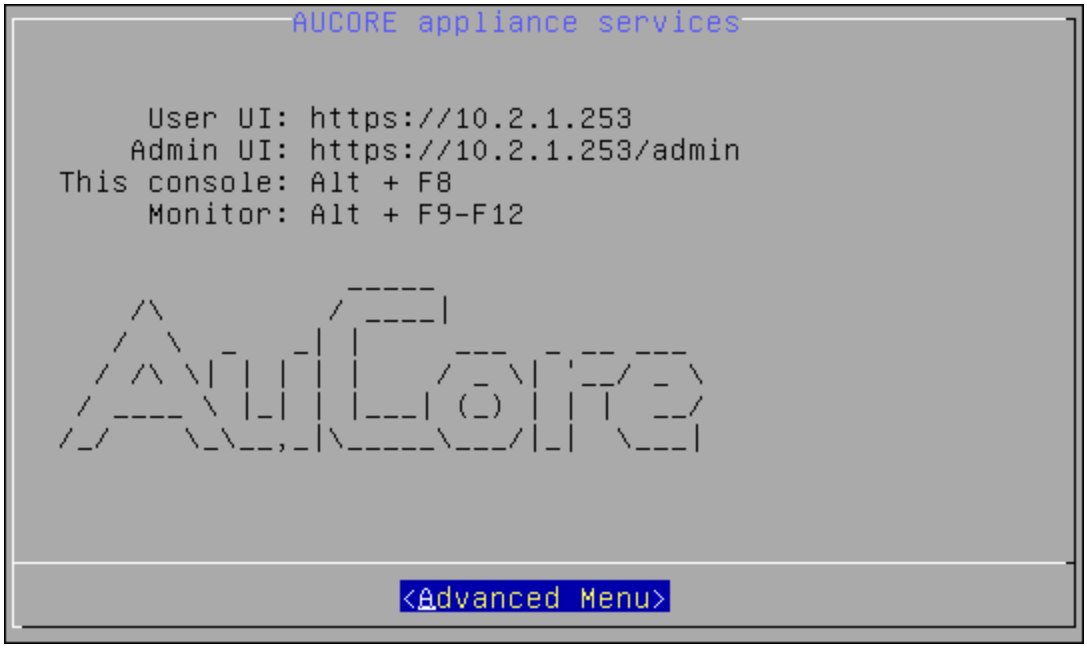
2. Select **I agree** to continue installation.



3. The installation will be automatically started.



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

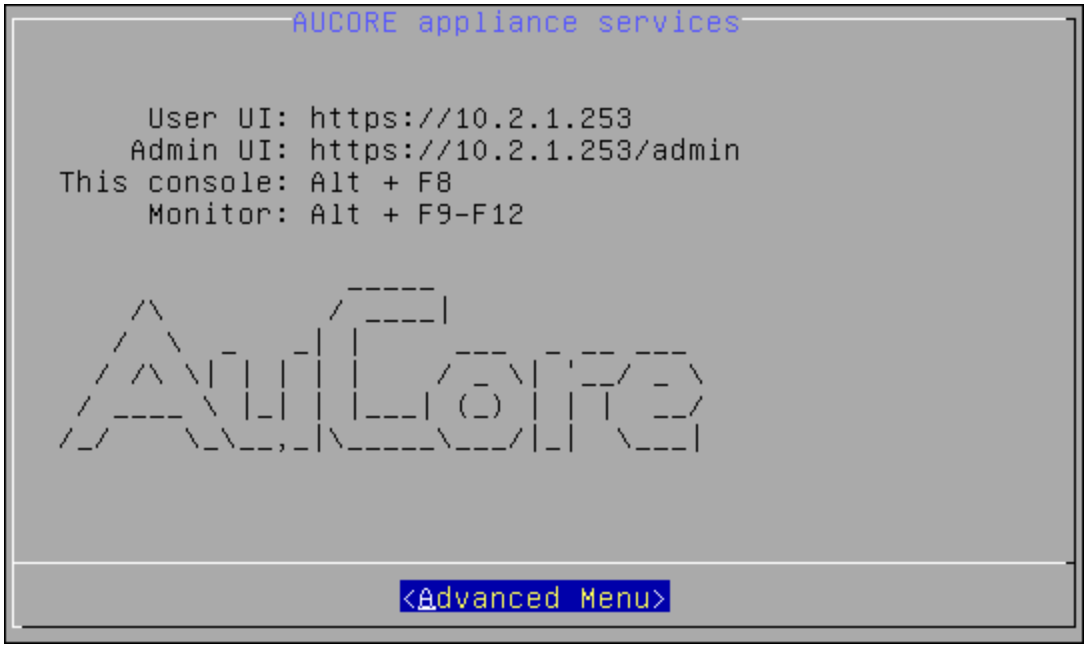


Configuration Console

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

- 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.

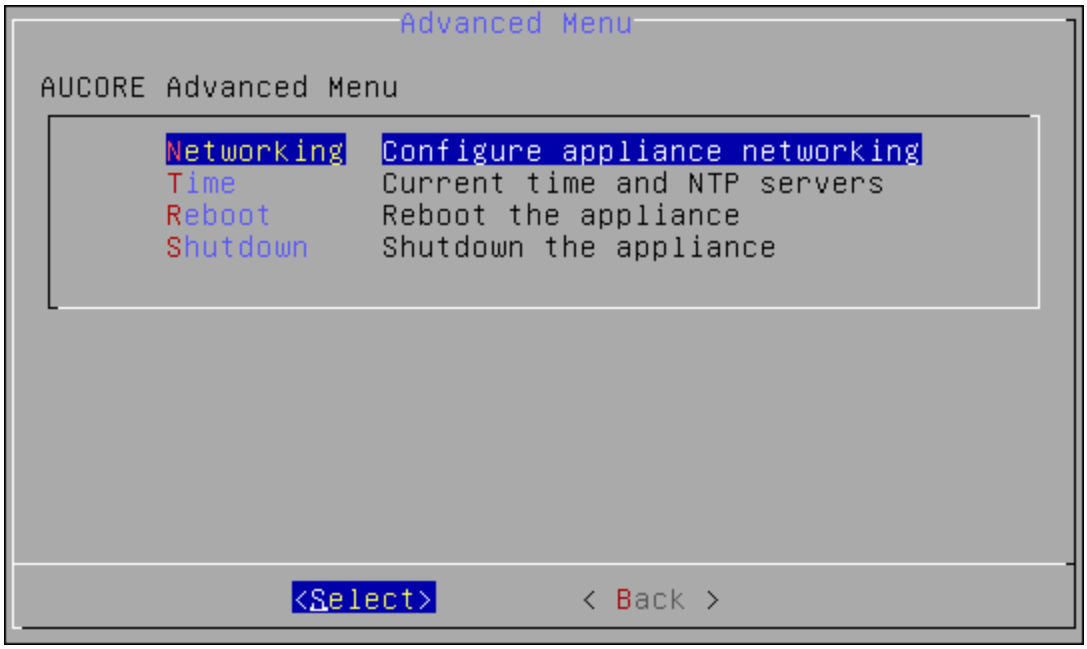


To proceed to NetIQ Server appliance management, select **Advanced Menu**.

Configuring Appliance Networking

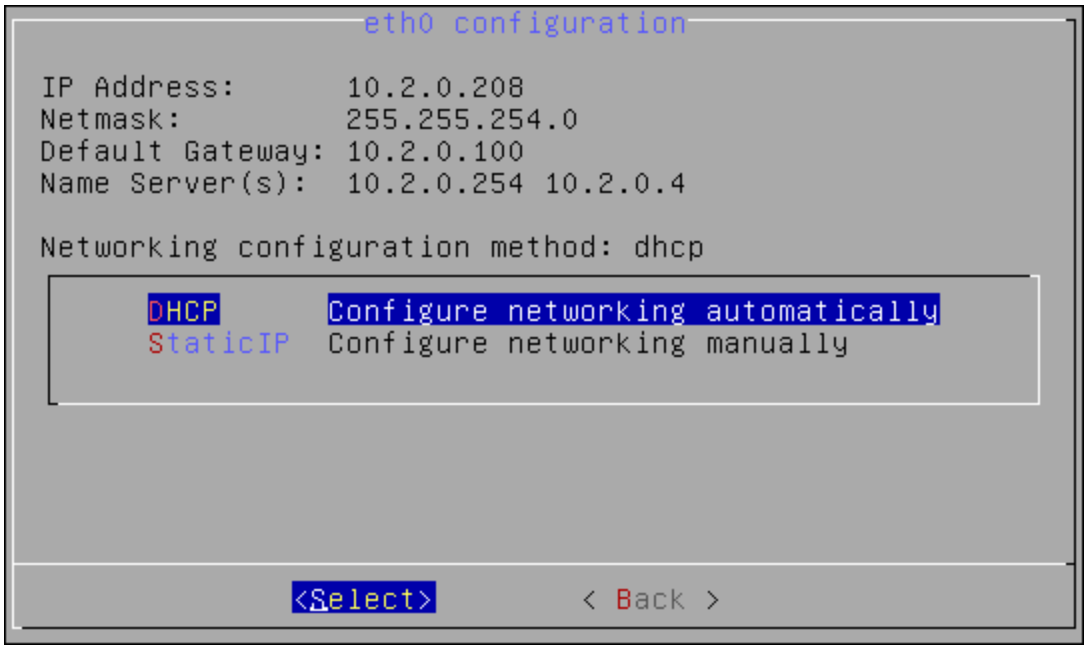
To configure NetIQ Server appliance networking via Configuration Console, follow the steps:

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

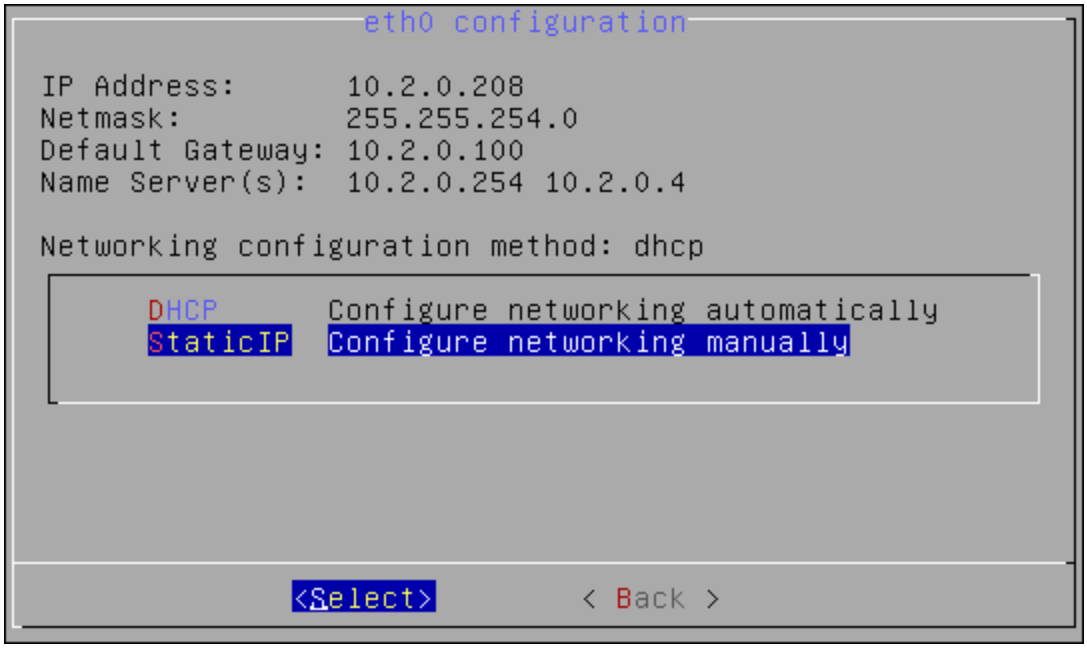


3. Select an applicable networking configuration method:

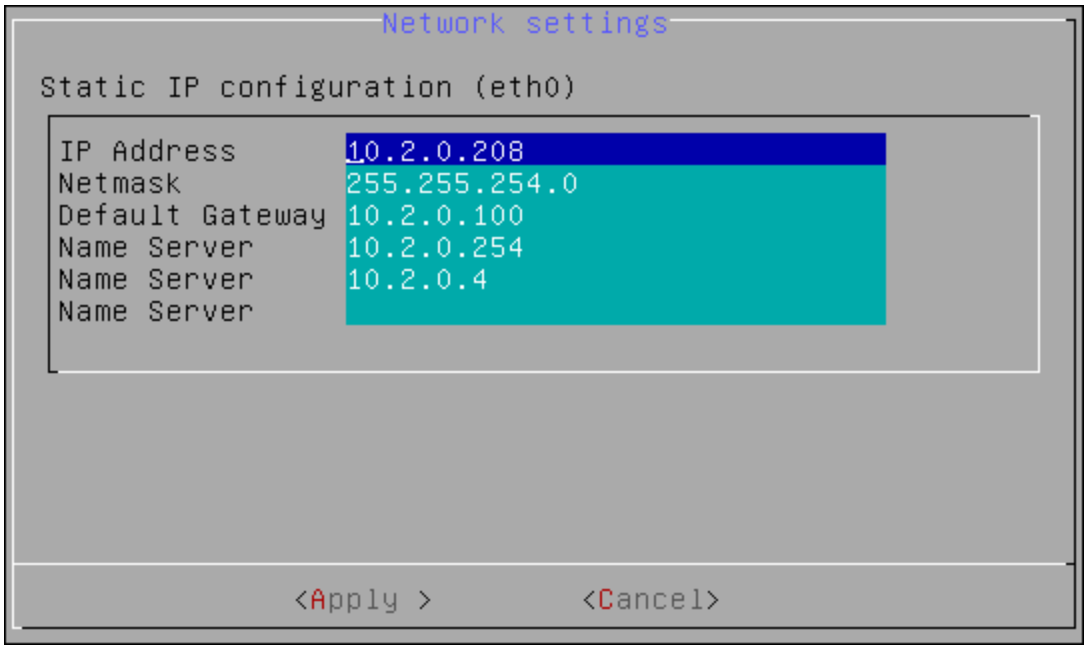
- **DHCP** - to configure networking automatically.



- **StaticIP** - to configure networking manually.



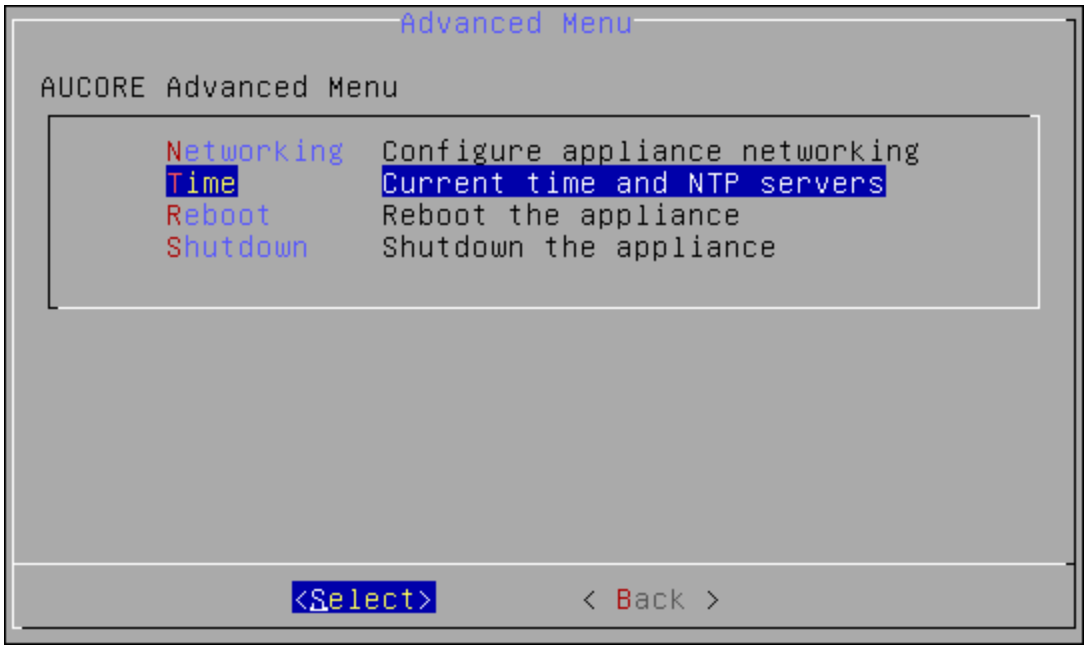
Specify all required parameters manually and press **ENTER** to apply changes.


Network settings
Static IP configuration (eth0)
IP Address 10.2.0.208
Netmask 255.255.254.0
Default Gateway 10.2.0.100
Name Server 10.2.0.254
Name Server 10.2.0.4
Name Server
<Apply >
<Cancel>

Configuring Time and NTP Servers

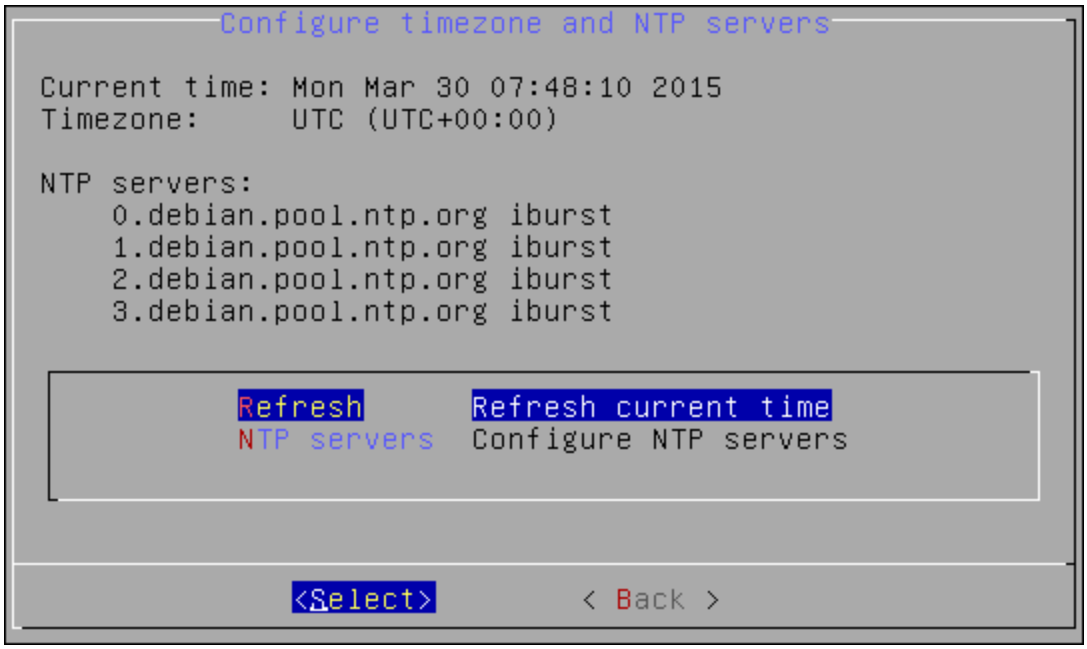
To configure NetIQ Server appliance timezone and NTP servers via Configuration Console, follow the steps:

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

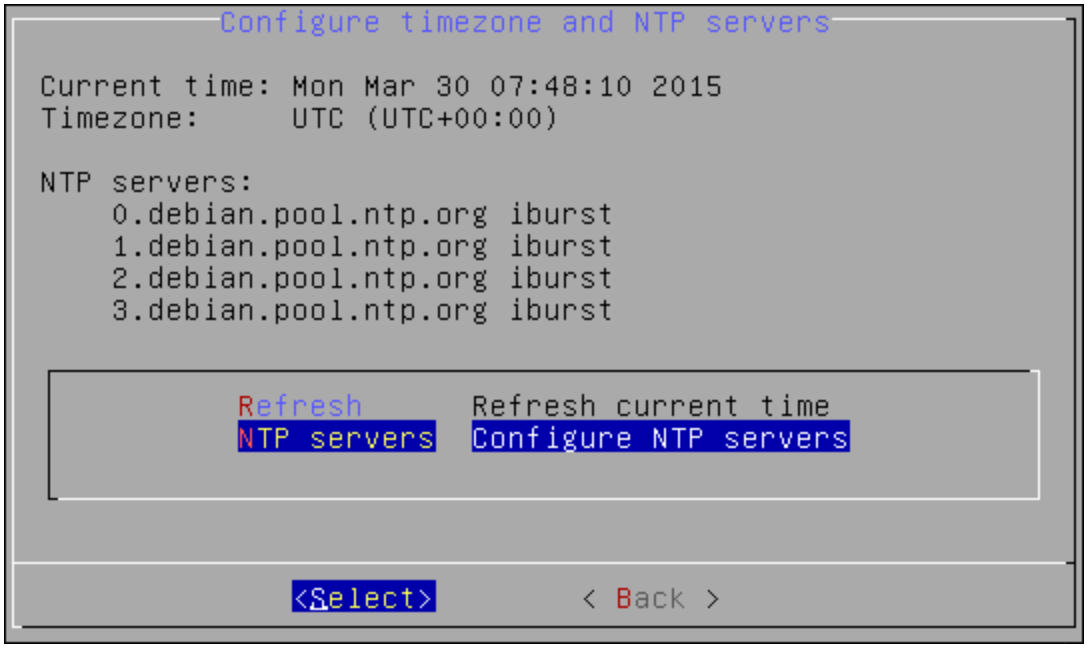


3. Select one of the following options:

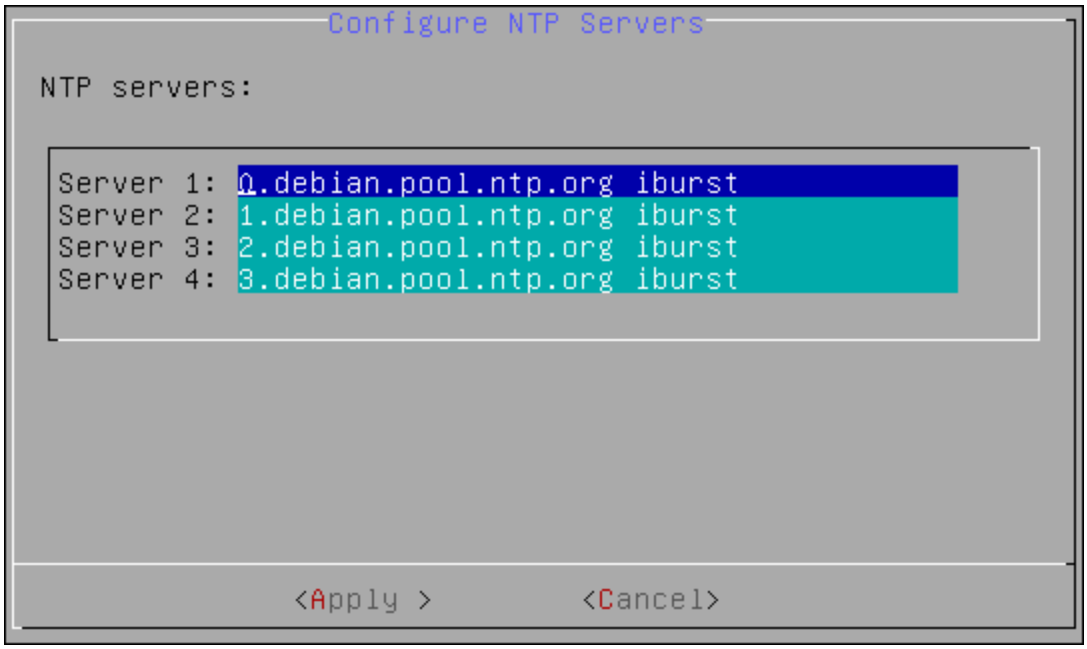
- **Refresh** to refresh current time.



- **NTP servers** to configure NTP servers.



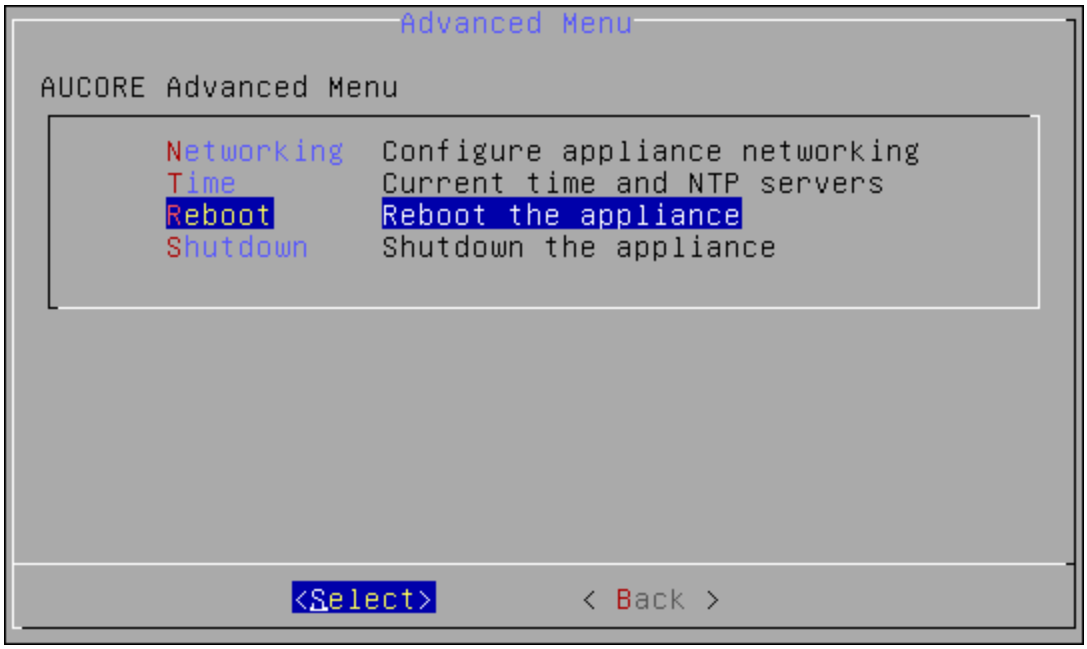
Specify applicable addresses for NTP servers and press **ENTER** to apply changes.


Configure NTP Servers
NTP servers:
Server 1: 0.debian.pool.ntp.org iburst
Server 2: 1.debian.pool.ntp.org iburst
Server 3: 2.debian.pool.ntp.org iburst
Server 4: 3.debian.pool.ntp.org iburst
<Apply >
<Cancel>

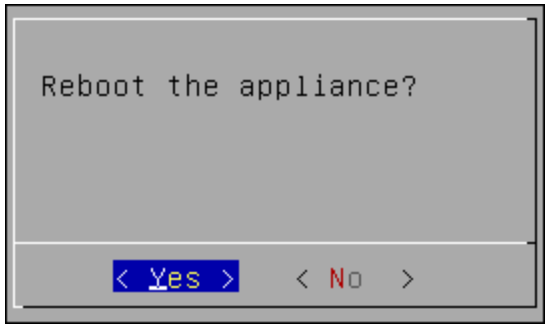
Rebooting Appliance

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

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



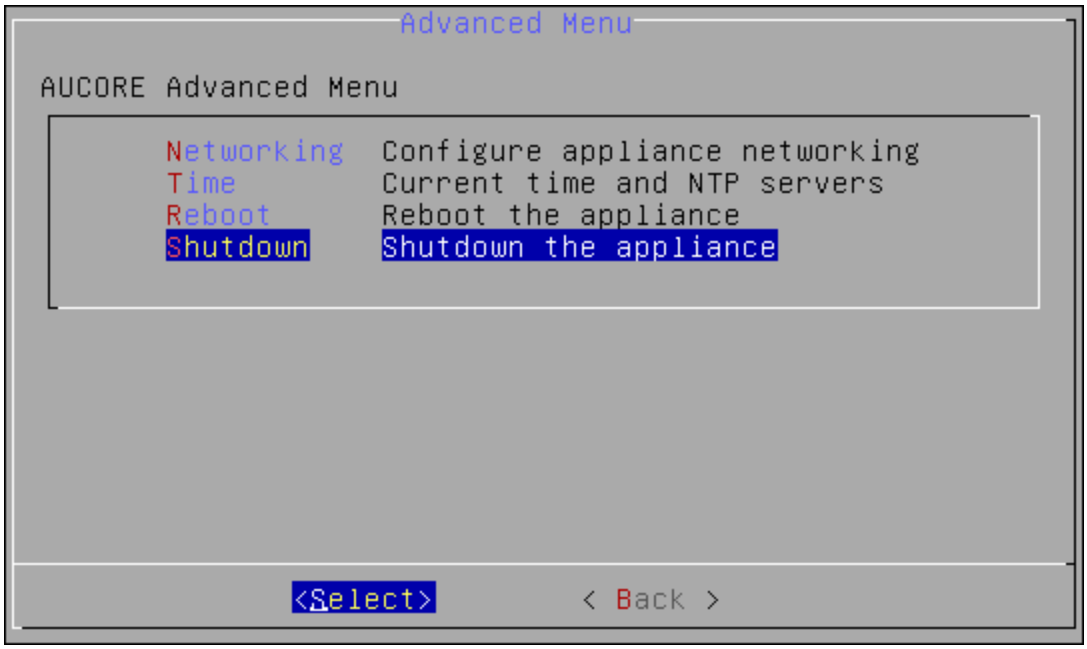
3. The confirmation message will be displayed. Select **Yes** to continue.



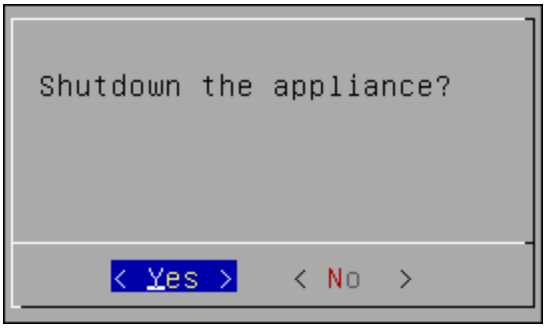
Shutting Down Appliance

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.



Setting up NetIQ Server Appliance Mode

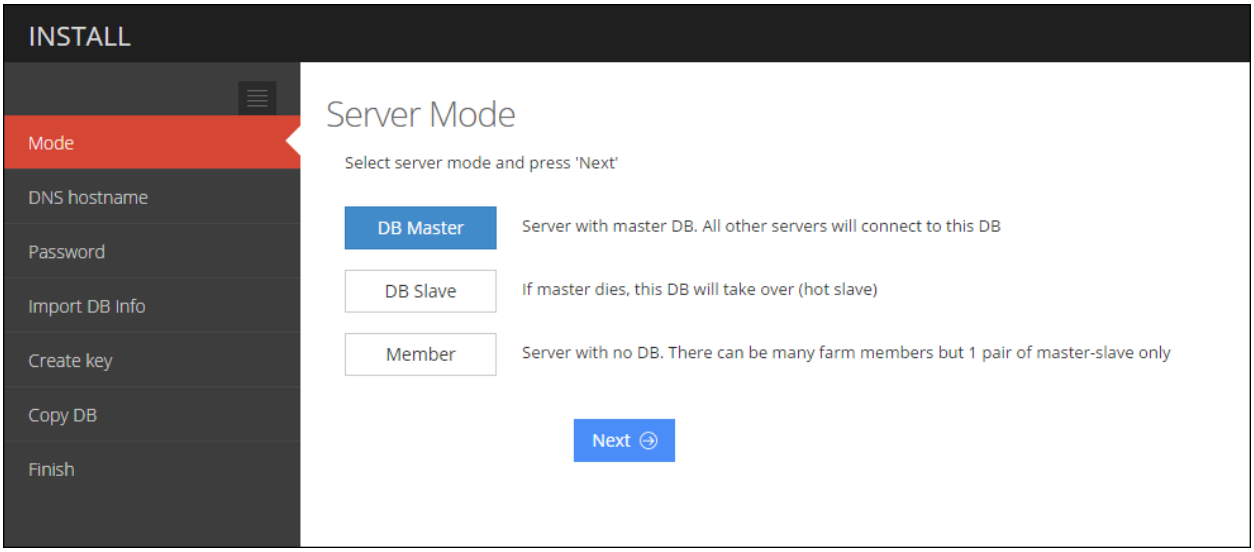
After the installation of NetIQ Server appliance, it is required to configure the mode the appliance will run. Select one of the following server modes:

- ***DB Master*** is the server with master database. All DB Slave and Member servers are connected to the master database.
- ***DB Slave*** 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*** is the web server without database.

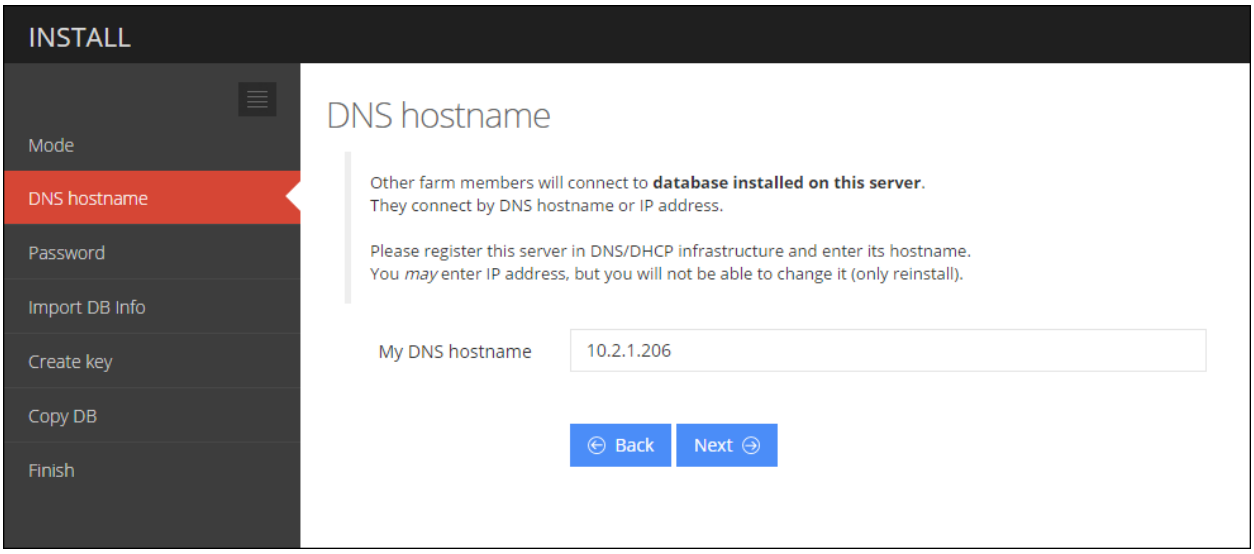
DB Master

To configure the **DB Master** server:

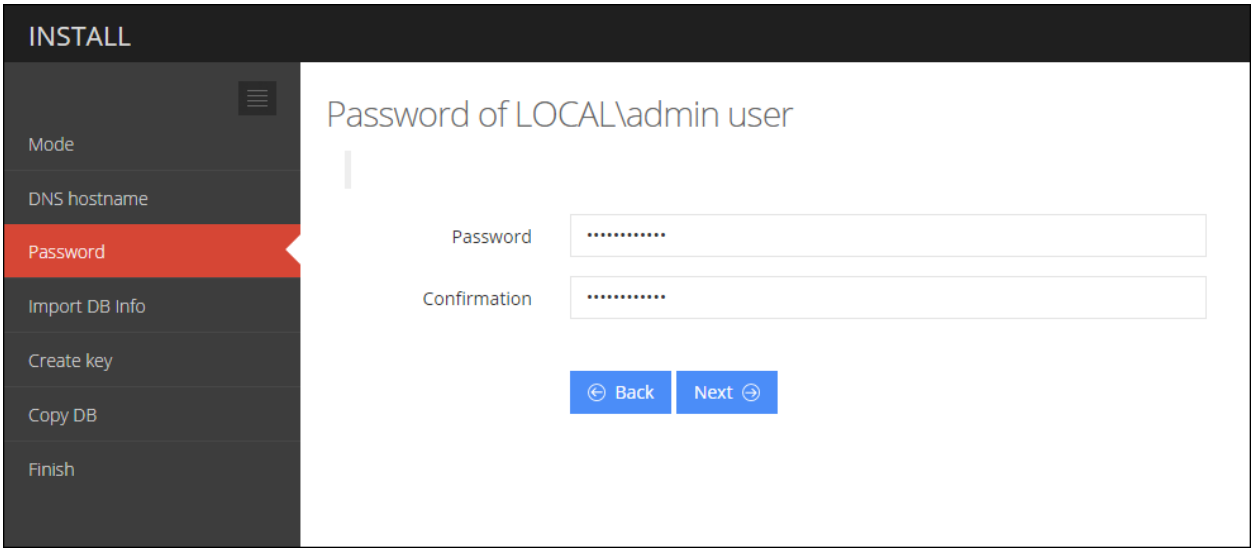
1. Go to the NetIQ Admin Interface. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the **DB Master** server mode and click **Next** to continue.



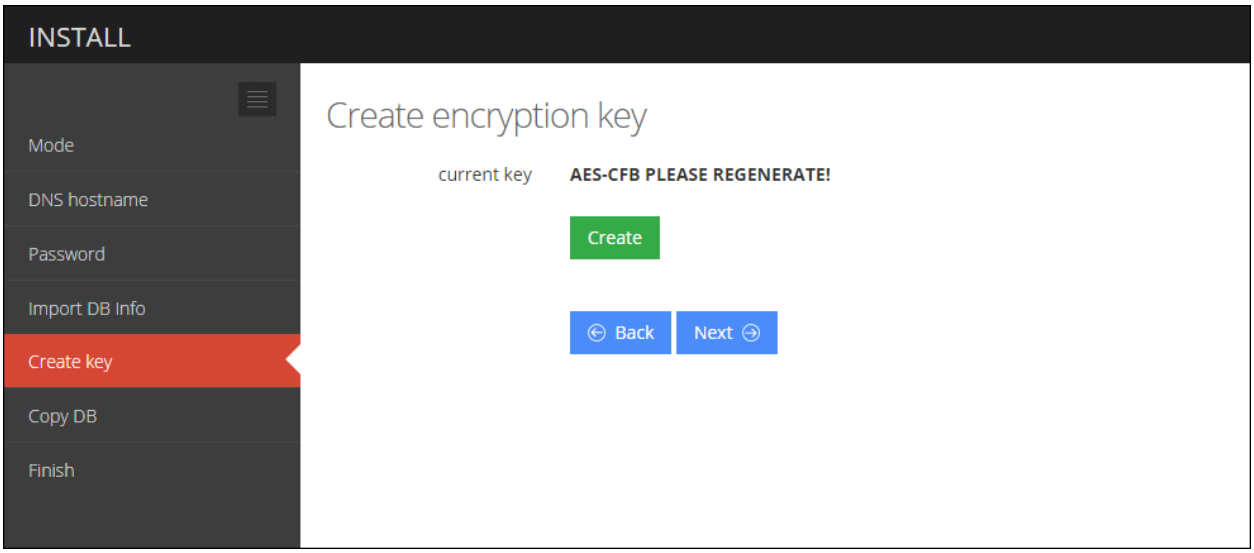
3. Specify the server DNS hostname or IP address. Click **Next** to continue.



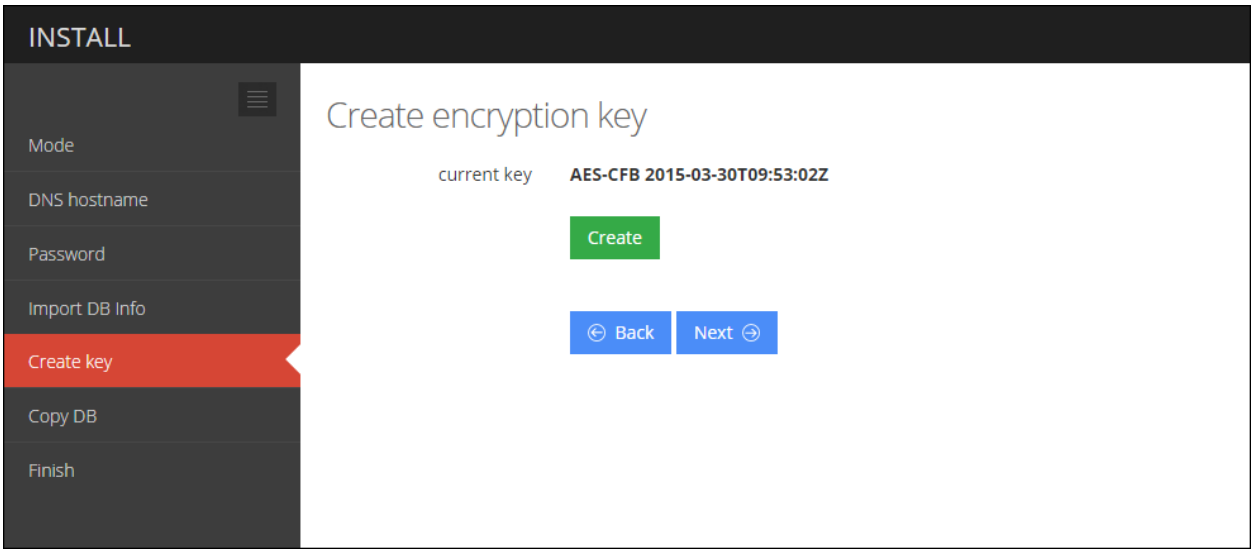
4. Specify the password of the LOCAL\admin user and confirm it. Click **Next** to continue.



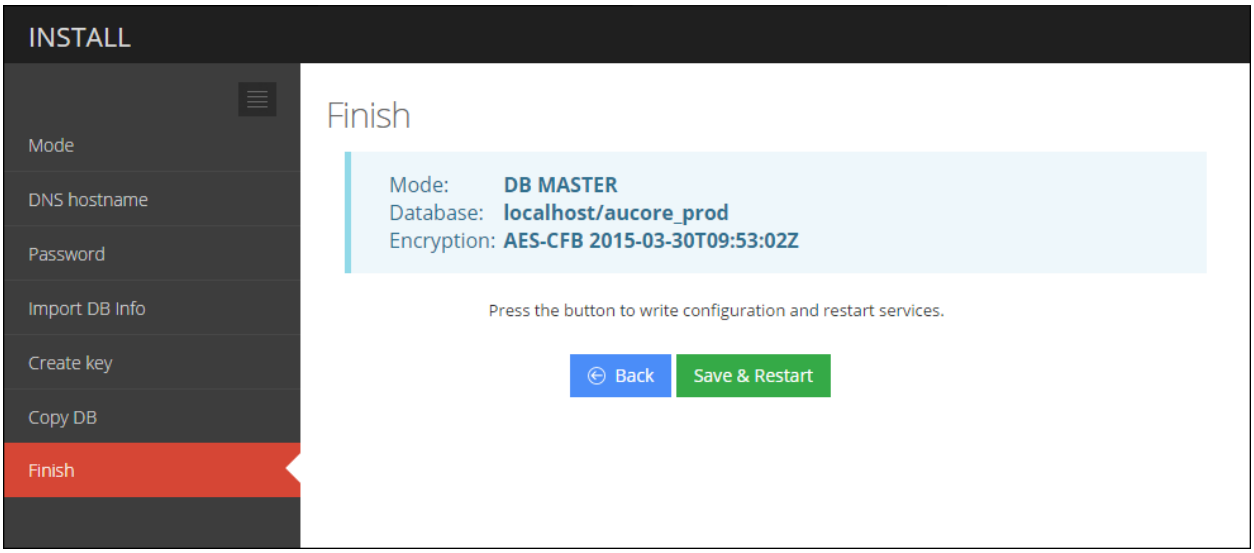
5. Click the **Create** button to generate encryption key file.



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



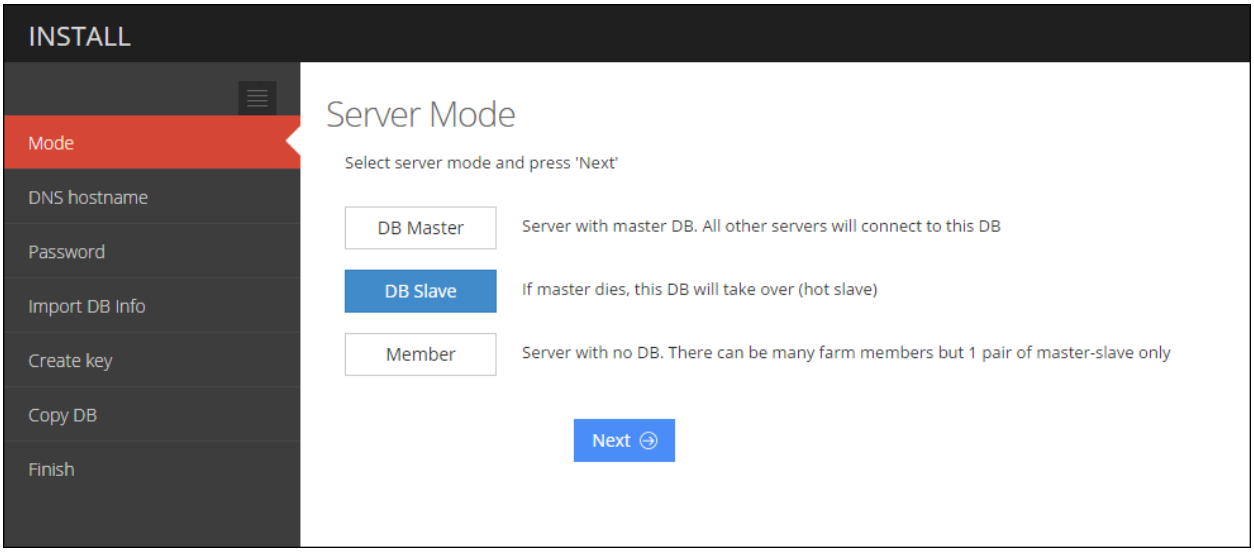
7. Click the **Save & Restart** button to write configuration and restart services. Services will be restarted within 30 seconds.



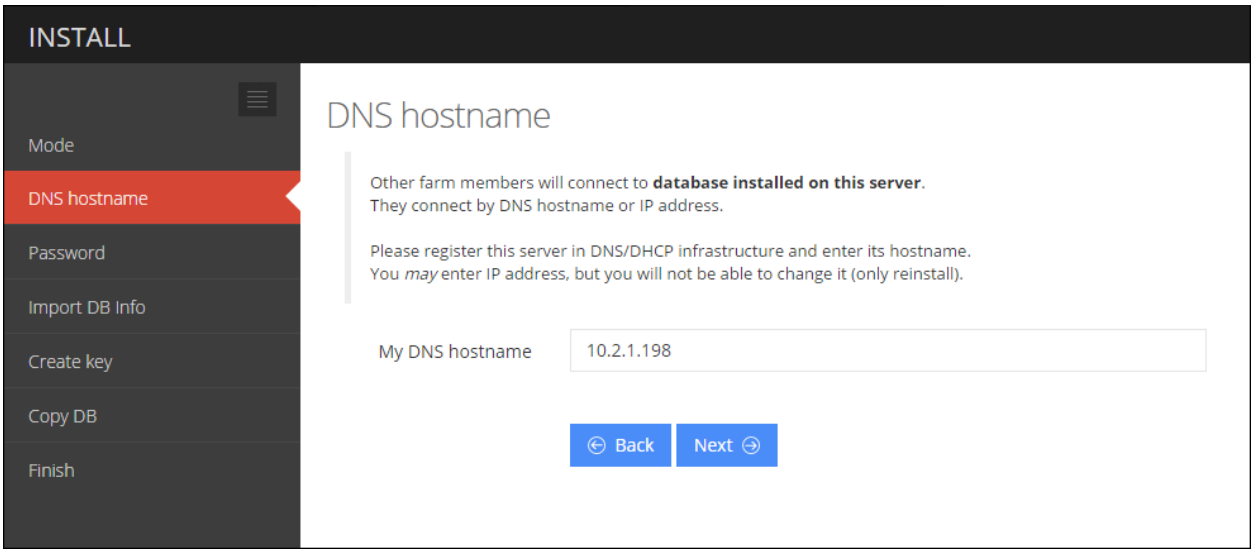
DB Slave

To configure the **DB Slave** server:

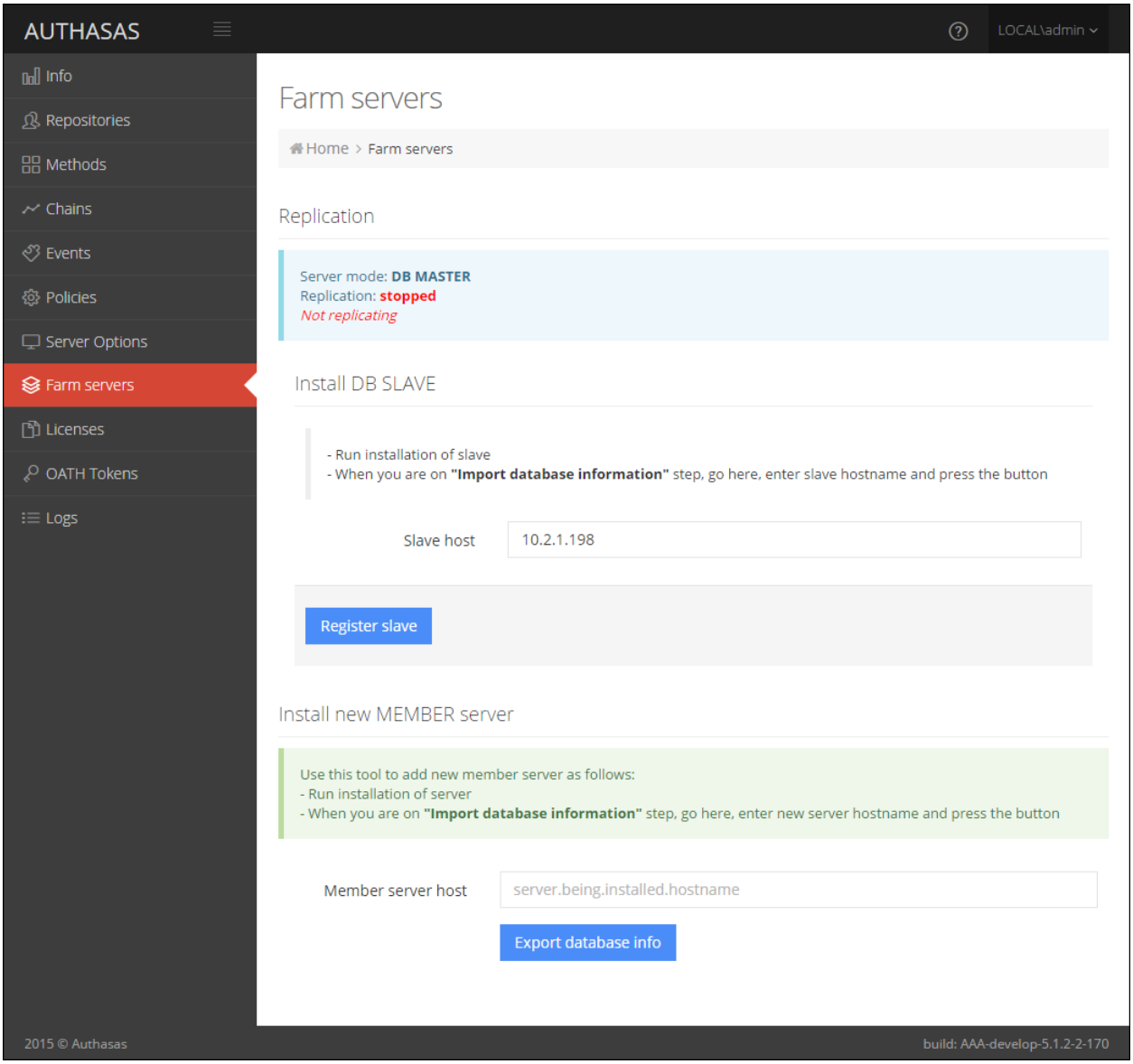
1. Go to the NetIQ Admin Interface. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the **DB Slave** server mode and click **Next** to continue.



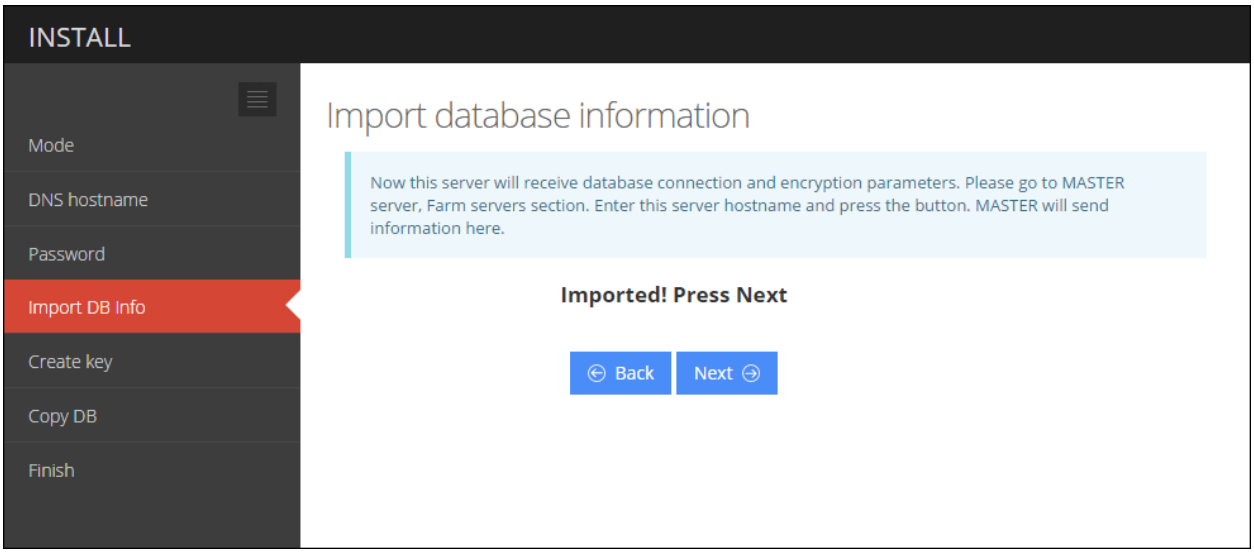
3. Specify the server DNS hostname or IP address. Click **Next** to continue.



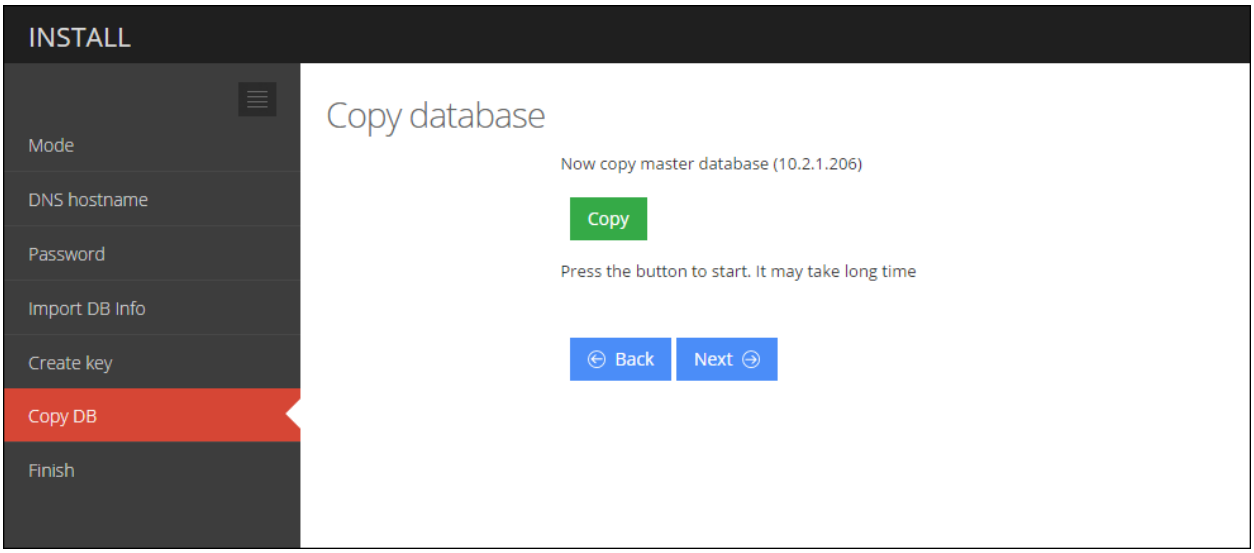
4. Go to the NetIQ Admin Interface of the DB Master server and open the **Farm servers** section. Enter the hostname of this server in the **Slave host** text field and click the **Register slave** button.



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

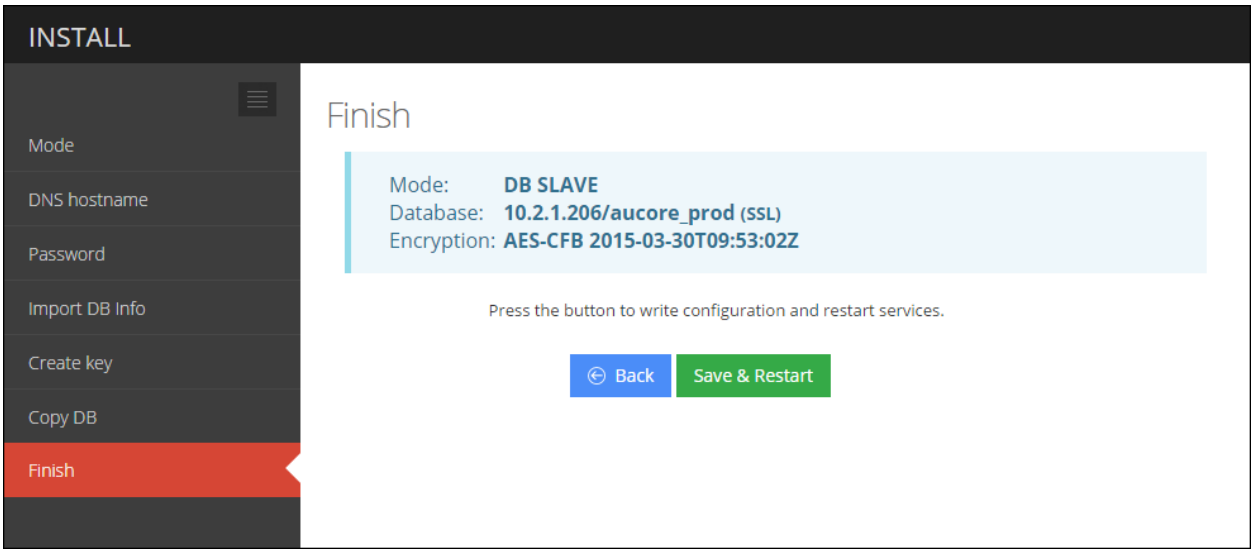


5. Click the **Copy** button to copy master database.



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.



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.

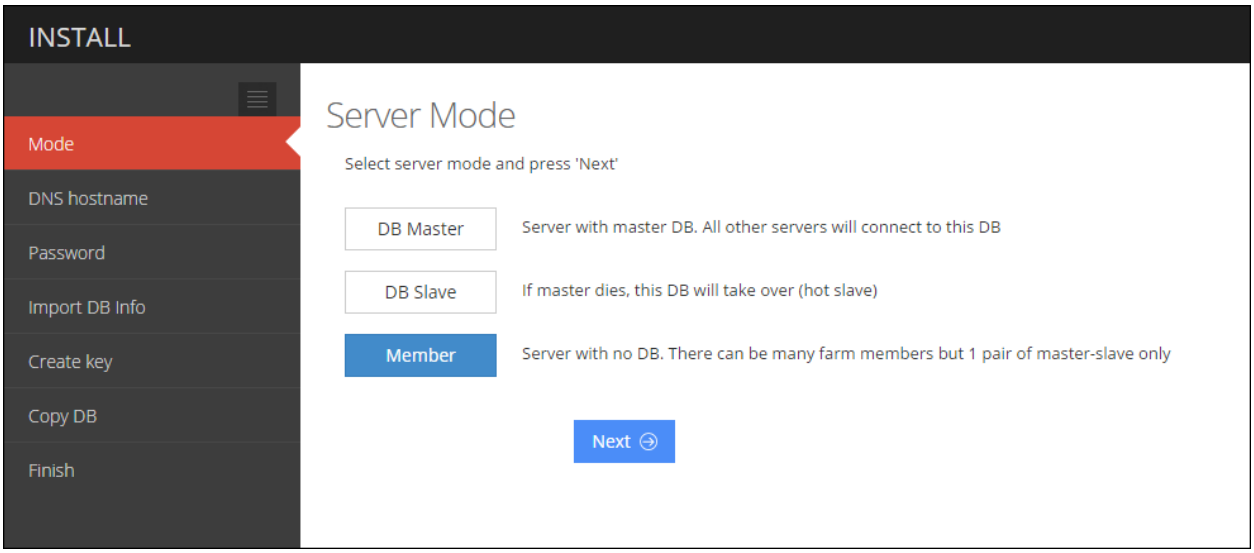
If you lost your DB Master server, you can convert DB Slave server to DB Master. Go to the NetIQ Admin Interface of the DB Slave server, open the **Farm servers** section and click **Convert to Master**. After the server is converted, install a new DB Slave server.

Member

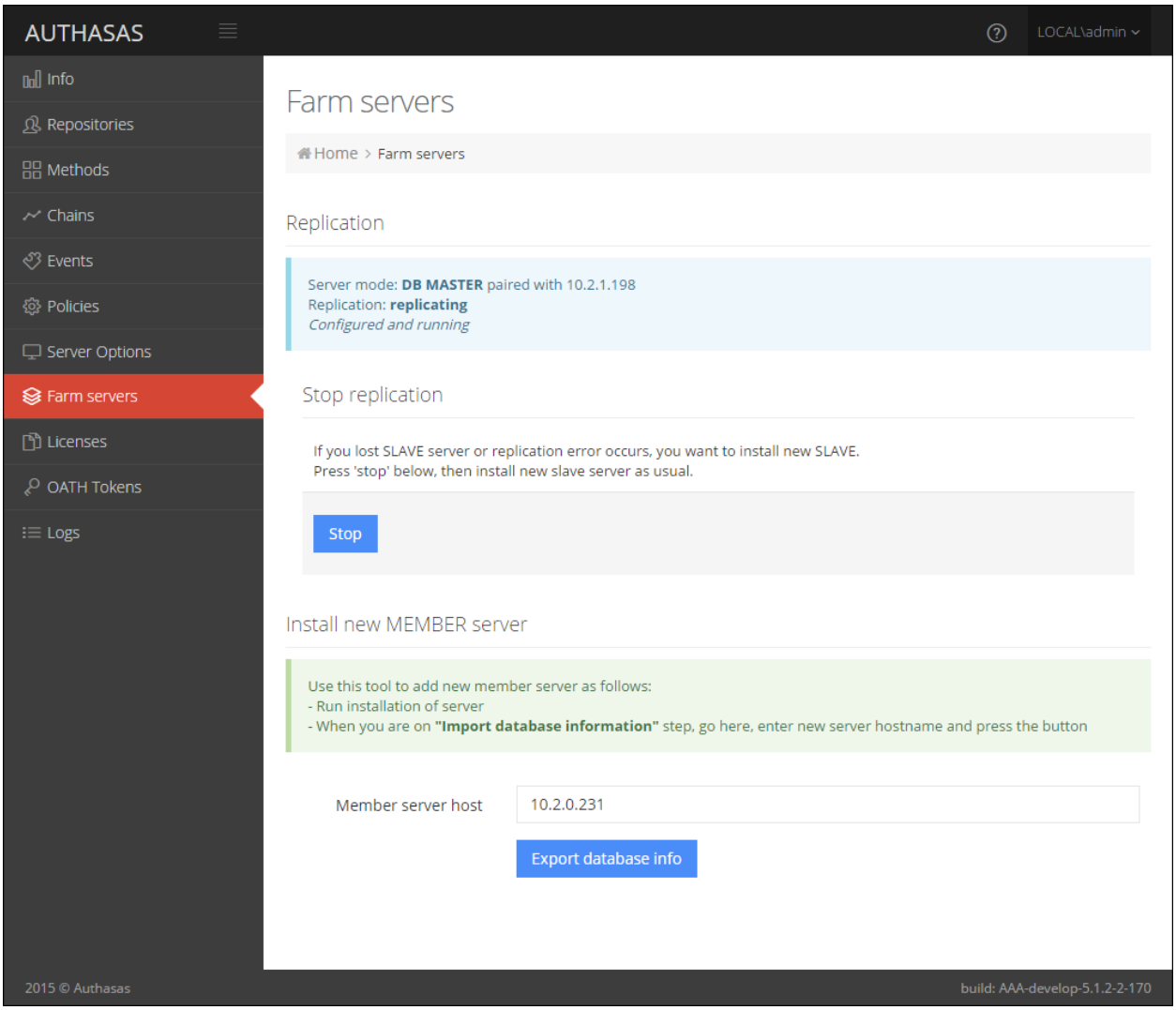
Multiple Member servers can be installed.

To configure the **Member** server:

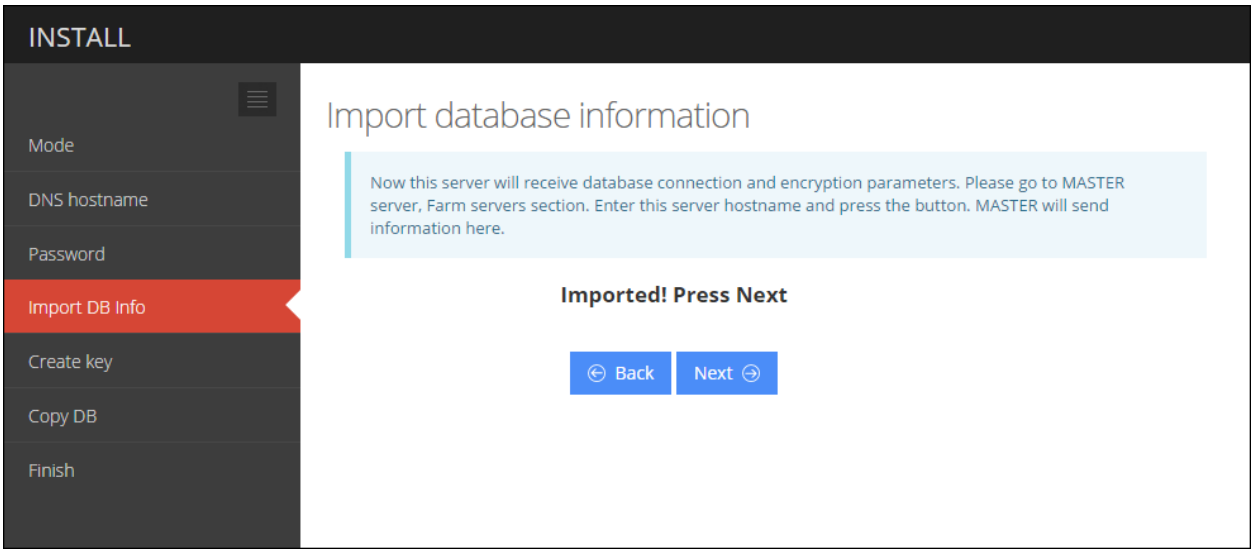
1. Go to the NetIQ Admin Interface. Enter the URL in the browser's navigation bar in the following format: https://<IP Address>/admin/ (the required URL is displayed after NetIQ Server installation).
2. Select the **Member** server mode and click **Next** to continue.



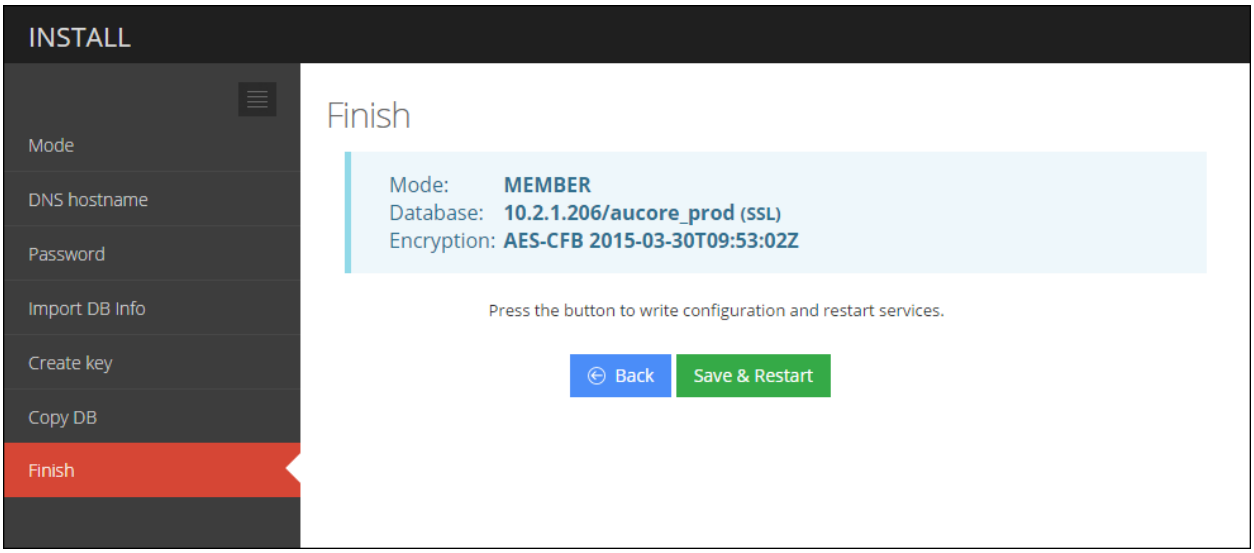
3. Go to the NetIQ Admin Interface of the DB Master server and open the **Farm servers** section. Enter the hostname of this server in the **Member server host** text field and click the **Export database info** button.



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



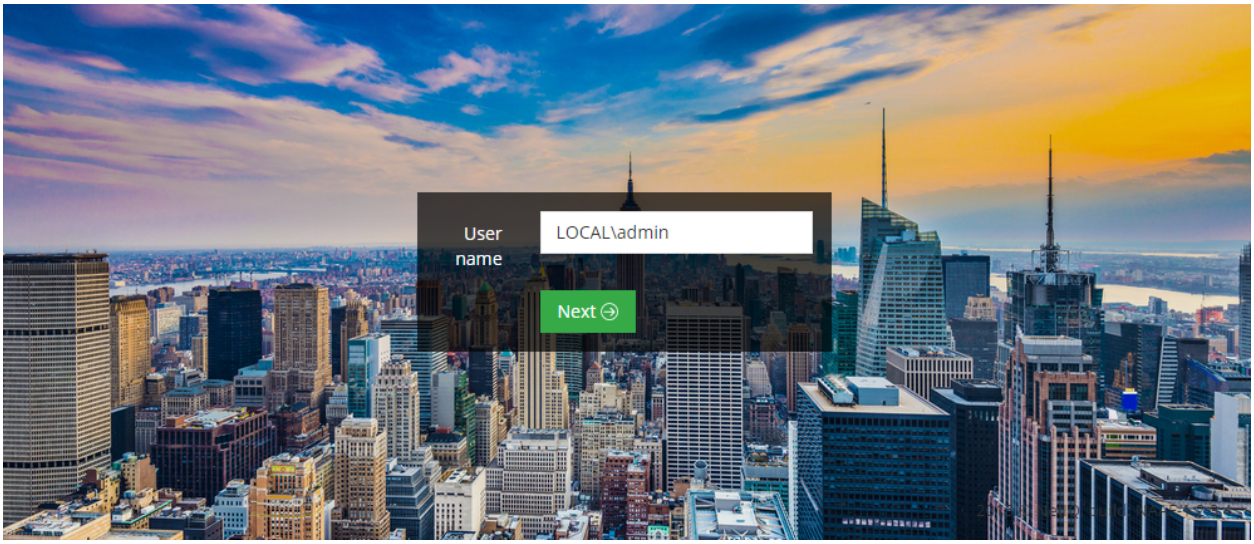
4. Click the **Save & Restart** button to write configuration and restart services. Services will be restarted within 30 seconds.



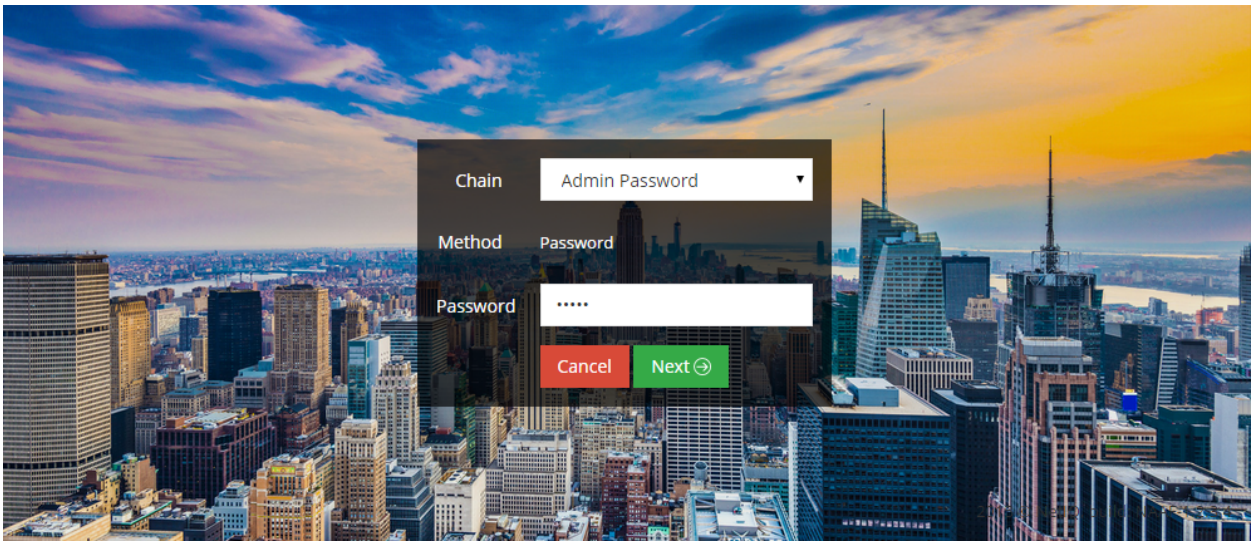
First Login To NetIQ Admin Interface

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

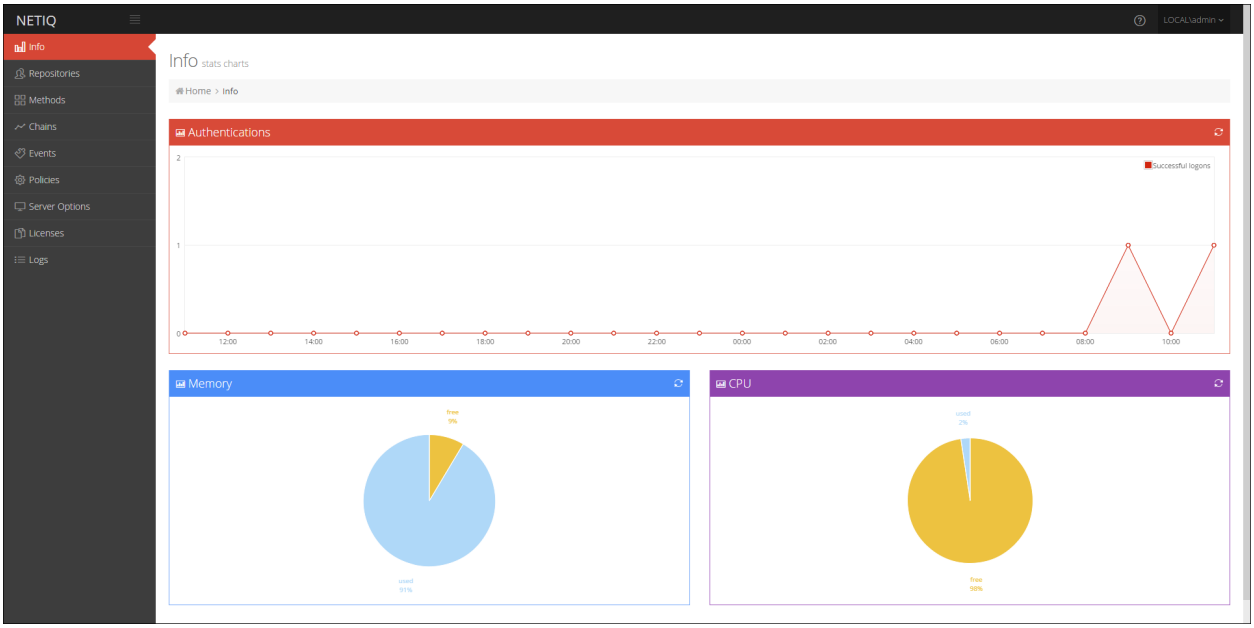
1. Enter administrator's login in the following format: repository\user (**local\admin** by default). Click **Next** to continue.



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.



Configuring NetIQ Server Appliance

 NetIQ Admin Interface 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 Help icon in the upper right corner of NetIQ Admin Interface. The Help section provides you with information on the specific section you are working on.

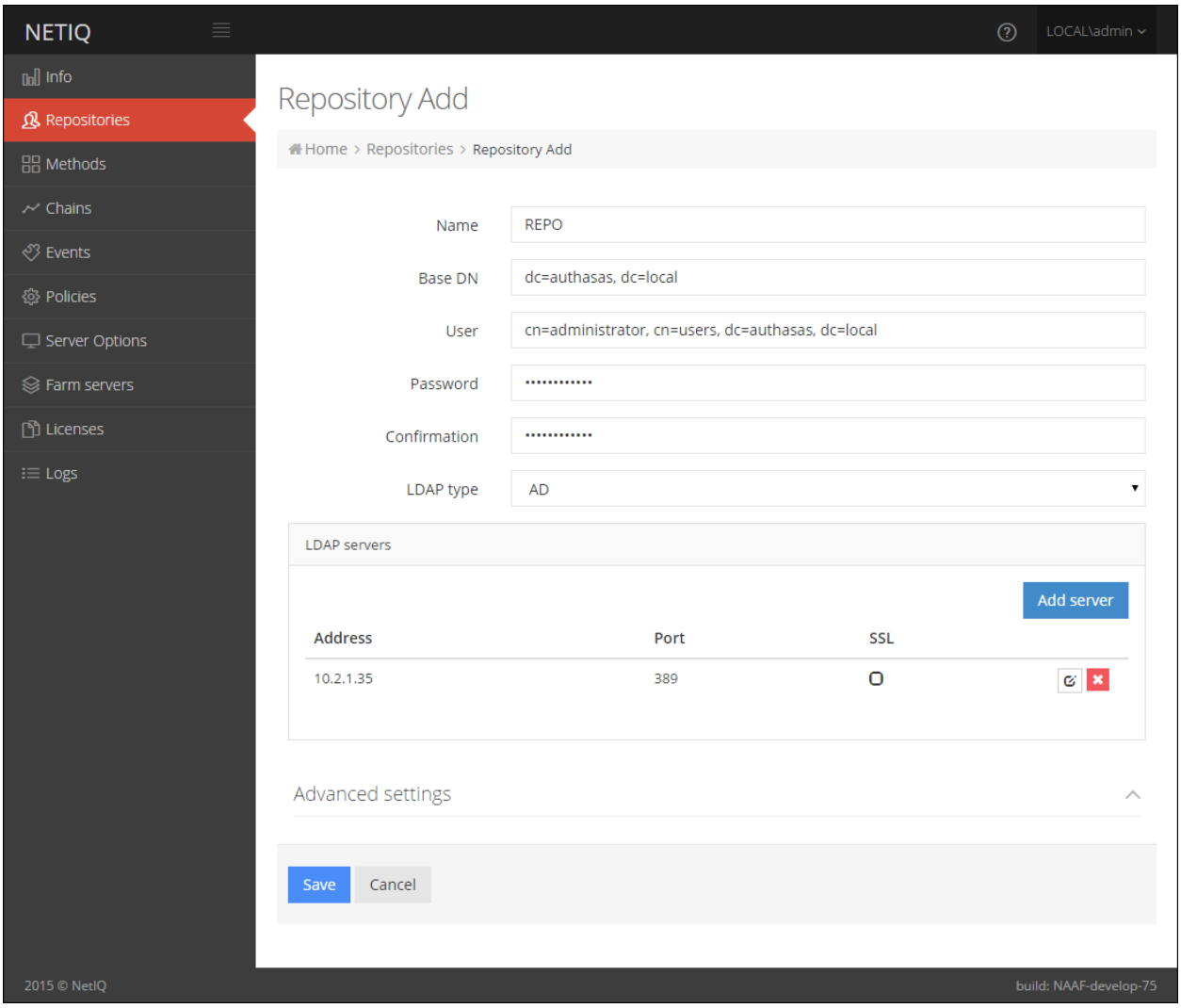
After the installation of NetIQ Server appliance and configuring an applicable server mode, administrator is provided with a capability to configure NetIQ Server appliance through NetIQ Admin Interface. To configure NetIQ Server appliance, it is required to follow the steps:

1. Add repository
2. Configure authentication methods
3. Create authentication chains
4. Configure authentication events
5. Configure required policies
6. Specify an applicable protocol
7. Add the license

Adding Repository

To add repository that will be used for NetIQ authentication framework, follow the steps:

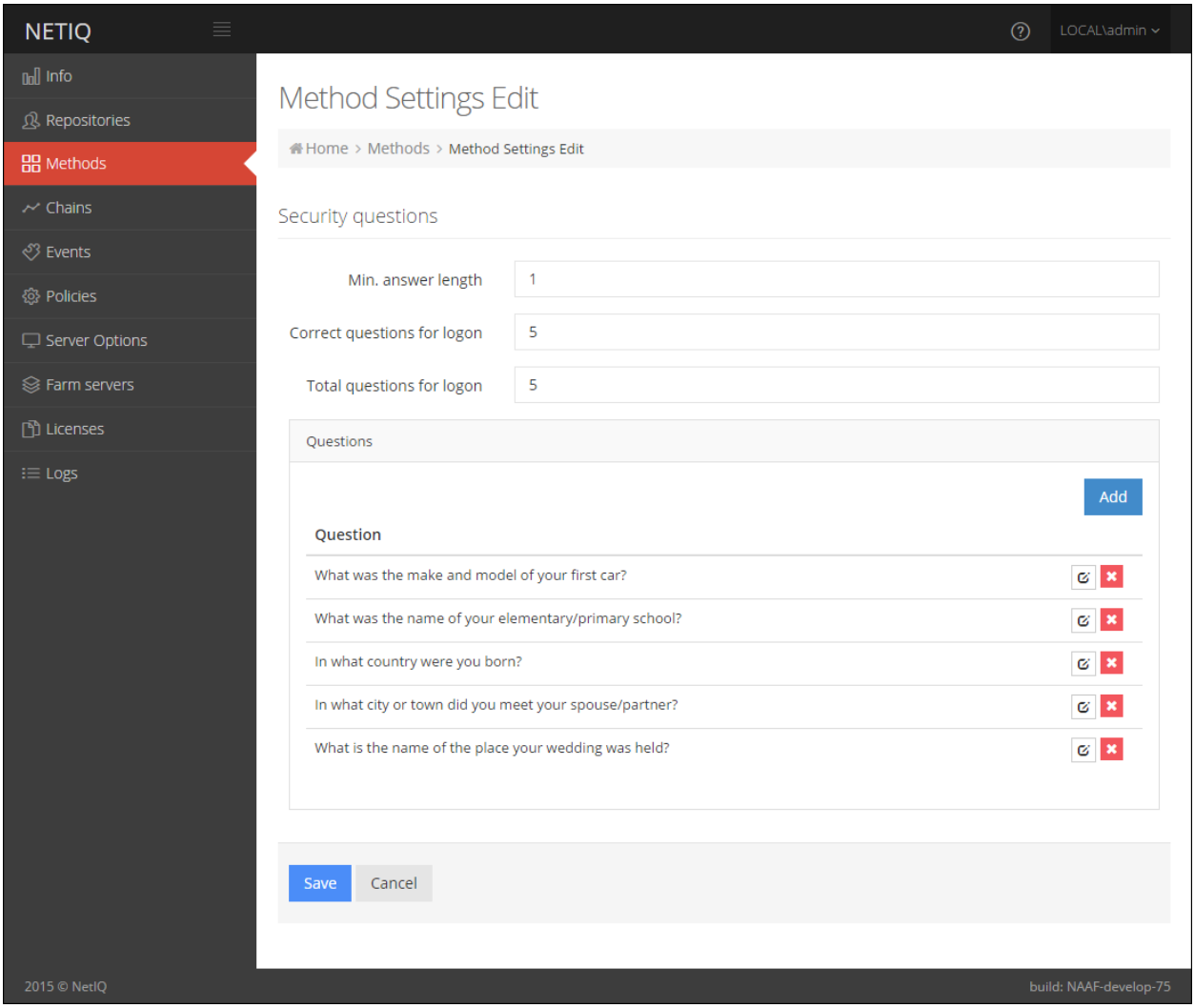
1. Open the **Repositories** section.
2. Click the **Add** button.
3. Fill in the **Name**, **Base DN**, **User**, **Password**, **Confirmation** text fields. Select an applicable repository type from the **LDAP type** dropdown.
4. Click the **Add server** button.
5. Specify server's address and port. Select the **SSL** checkbox to use SSL technology (if applicable). Click the **Save** button next to server's credentials. Add additional servers (if applicable).
6. Click **Save** at the bottom of the **Repositories** view to verify and save the specified credentials.


NETIQ
LOCAL\admin
Info
Repositories
Methods
Chains
Events
Policies
Server Options
Farm servers
Licenses
Logs
Repository Add
Home > Repositories > Repository Add
Name
REPO
Base DN
dc=authasas, dc=local
User
cn=administrator, cn=users, dc=authasas, dc=local
Password
Confirmation
LDAP type
AD
LDAP servers
Add server
Address
Port
SSL
10.2.1.35
389
Advanced settings
Save
Cancel
2015 © NetIQ
build: NAAF-develop-75

Configuring Method

To configure an applicable authentication method for NetIQ 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.

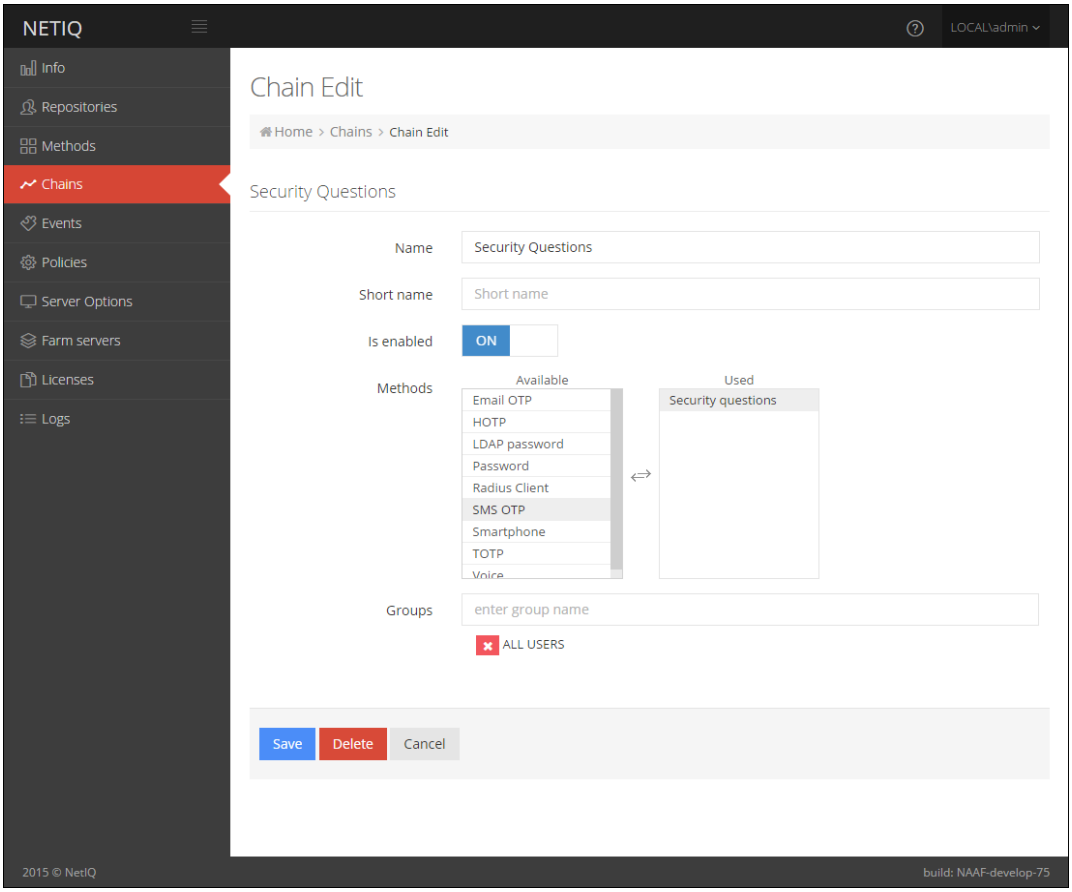


Creating Chain

The specified chains will connect to events.

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 **Edit** button next to an applicable authentication chain (or click the **Add** button at the bottom of the **Chains** view to create a new authentication chain).
3. Fill in the **Name** and **Short name** text fields.
4. Select whether the current authentication chain is enabled or disabled by clicking the **Is enabled** toggle button.
5. Select methods that will be assigned to the chain.
6. Specify groups that will be allowed to use the current authentication chain in the **Groups** text field.
7. Click **Save** at the bottom of the **Chains** view to save the configuration.

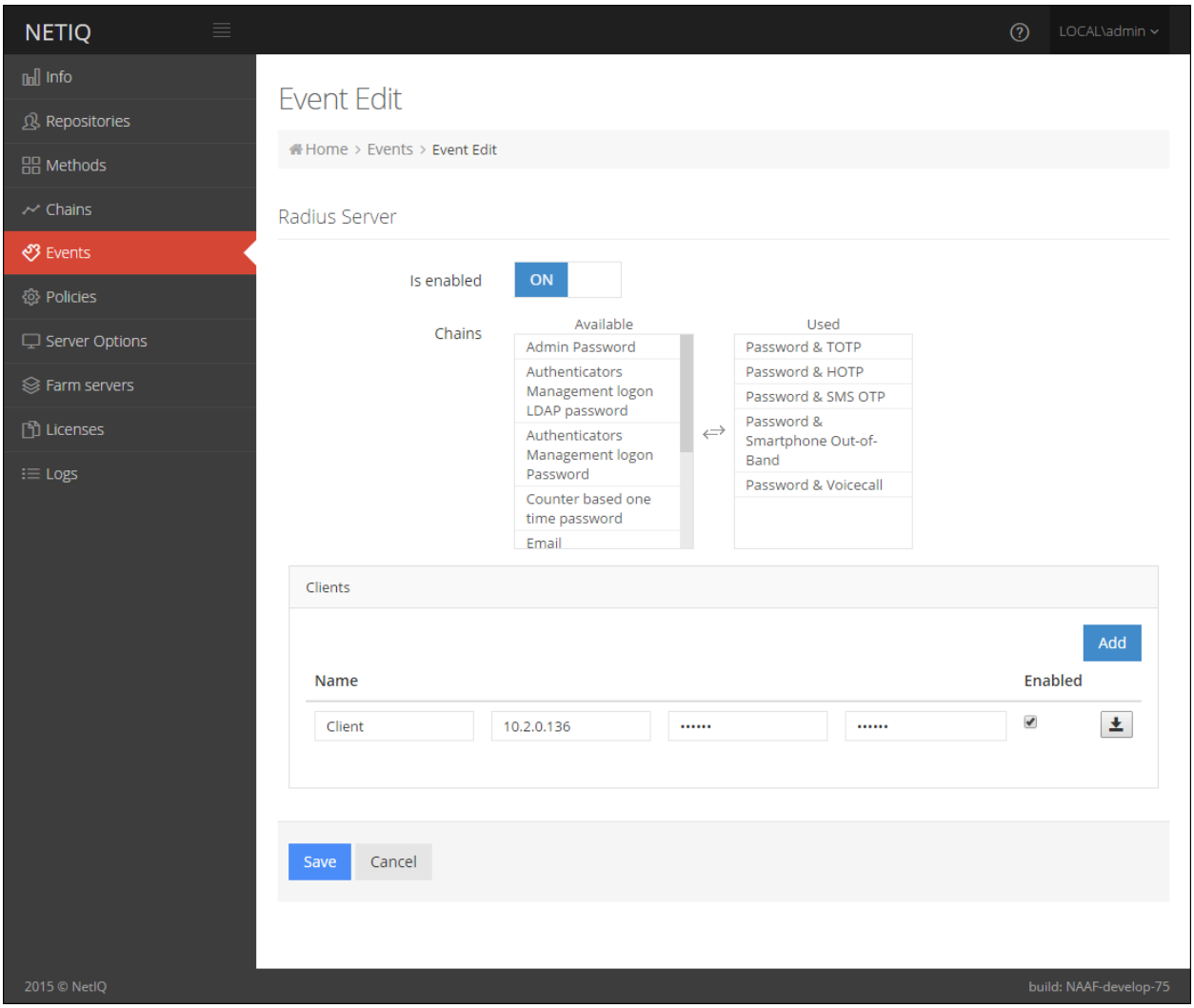


Configuring Event

The supported events are currently RADIUS Server, NAM and NCA.

To configure an authentication event for NetIQ 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 methods that will be assigned to the current event.
5. If available, add clients assigned to the current event.
6. Click **Save** at the bottom of the **Events** view to save configuration.

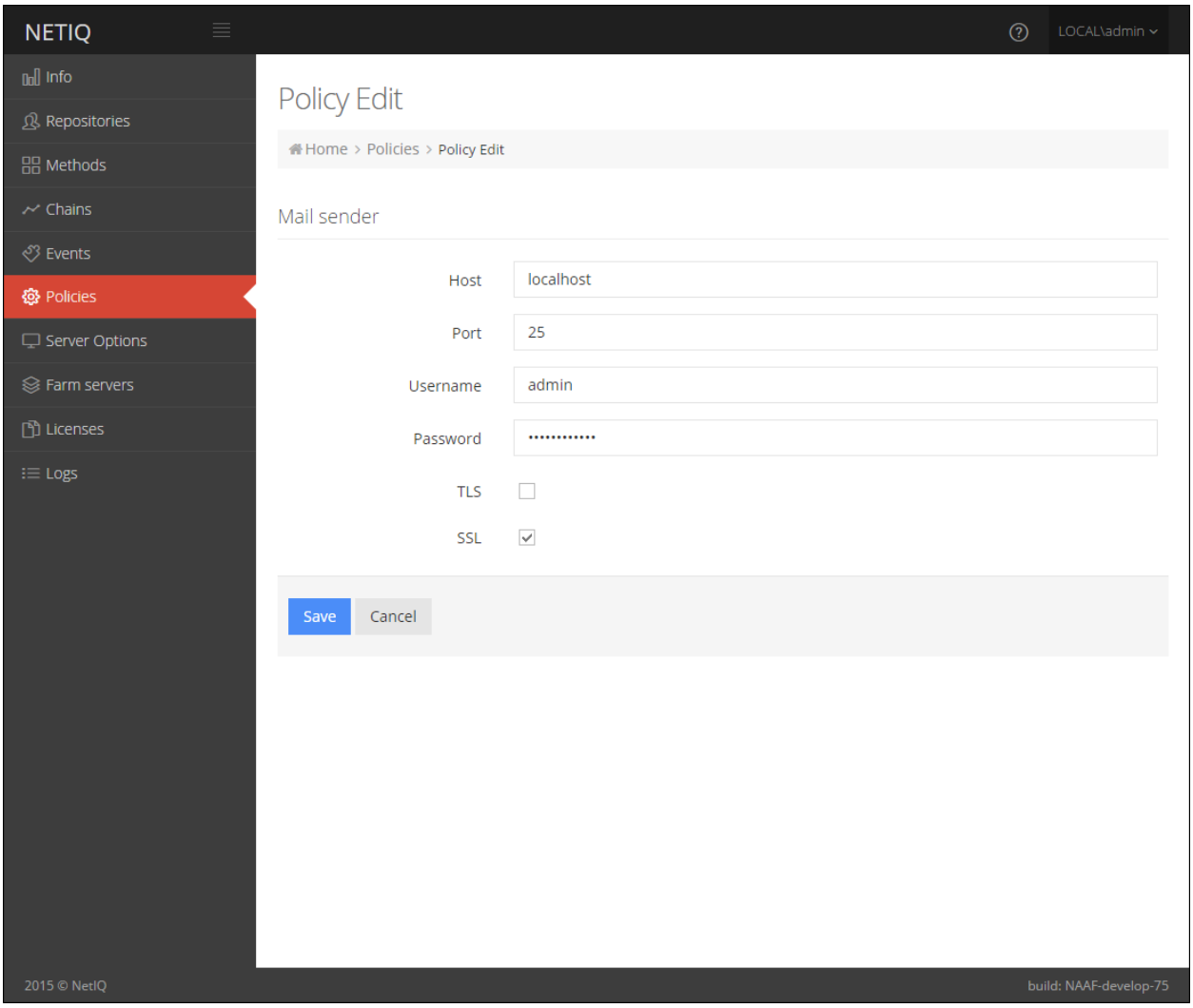


Configuring Policy

The configured policies will be applied for all servers.

To configure an applicable policy for NetIQ 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.



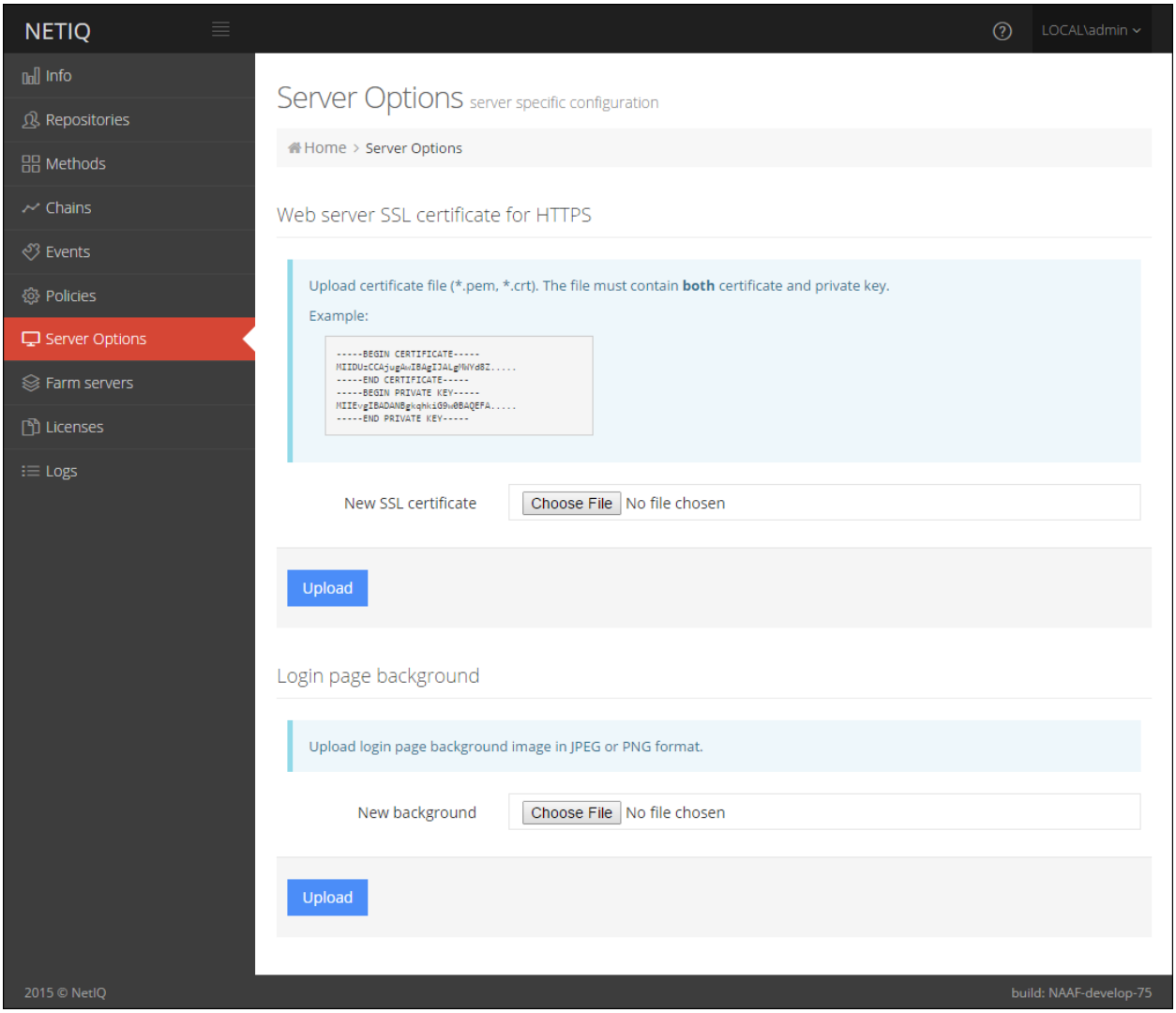
Configuring Server Options

By default the NetIQ Server uses an HTTP protocol. To switch to HTTPS mode, create a certificate file (PEM or CRT) and apply the existing SSL certificate on the server.

Smartphone and Voicecall 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 the new SSL certificate.
3. Click **Upload** to upload the selected SSL certificate.

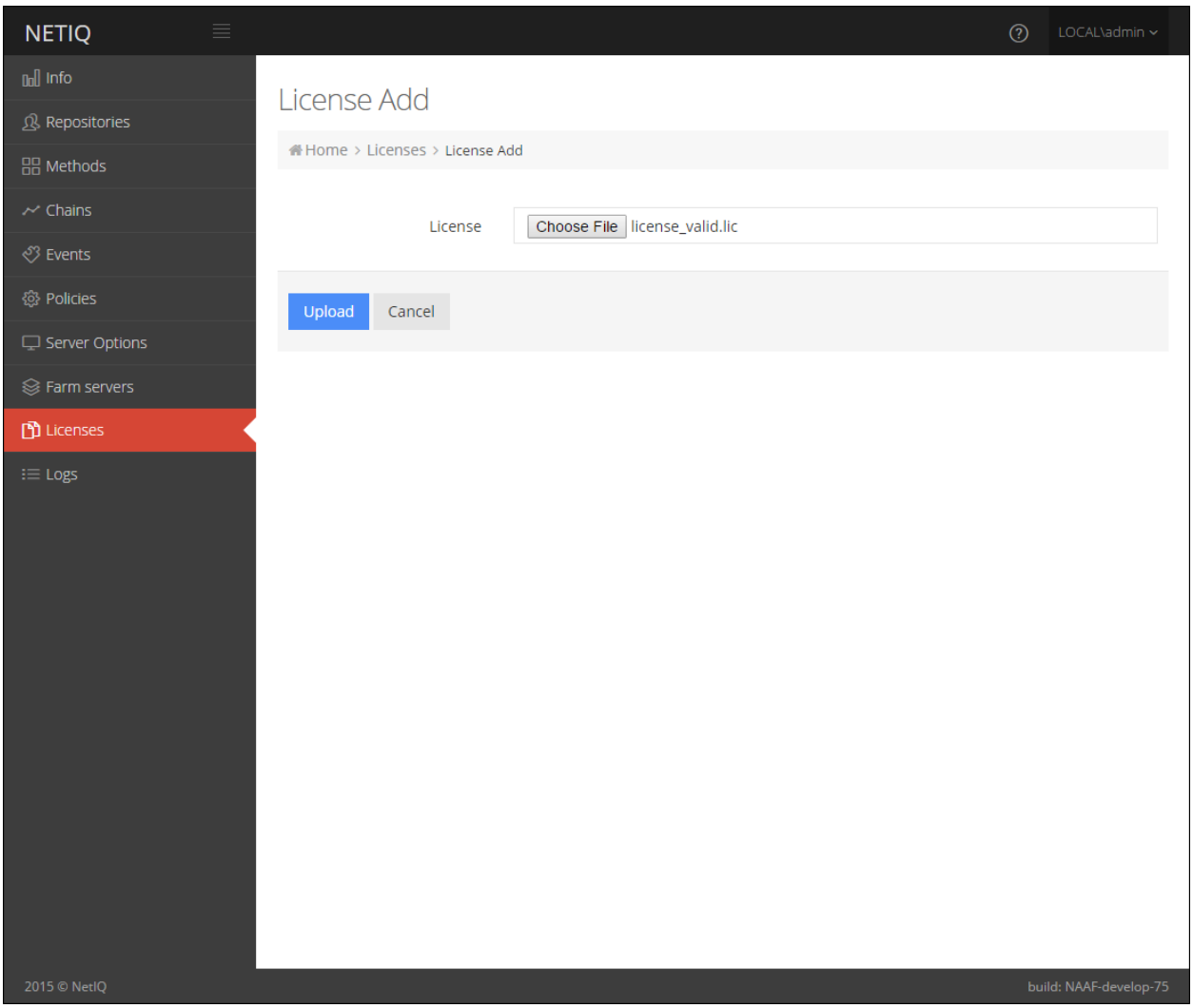


Adding License

The temporary license is active for 30 days and will expire at the specified date.

To add the license for NetIQ 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.



Default Ports for NetIQ Server Appliance

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 reserve 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 Com-munications
Smartphone	443	HTTPS	All Com-munications
Admin UI	443	HTTPS	All Com-munications
Enroll UI	443	HTTPS	All Com-munications

Variable ports depend on service and client setup.

Troubleshooting

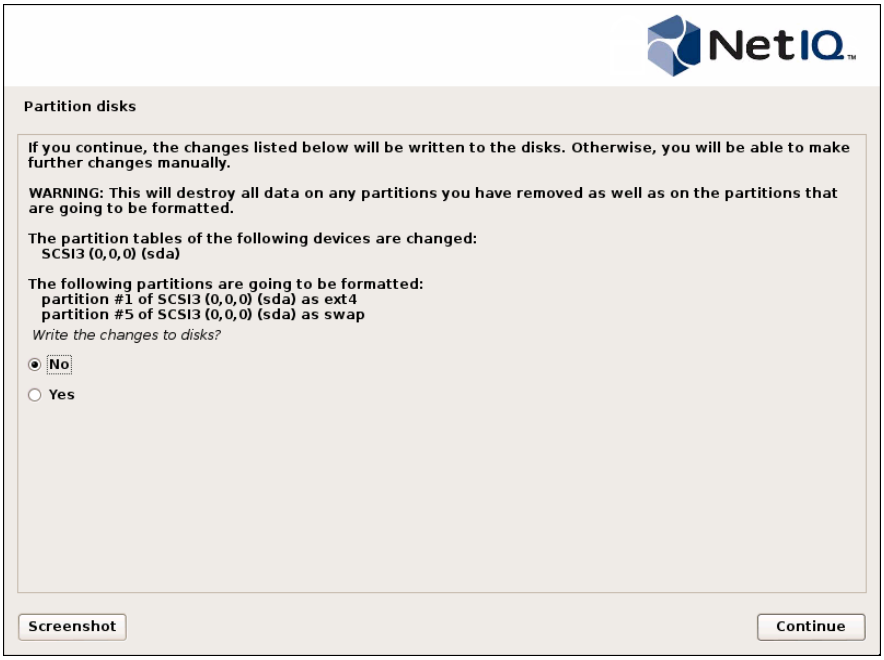
 This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

In this chapter:

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.

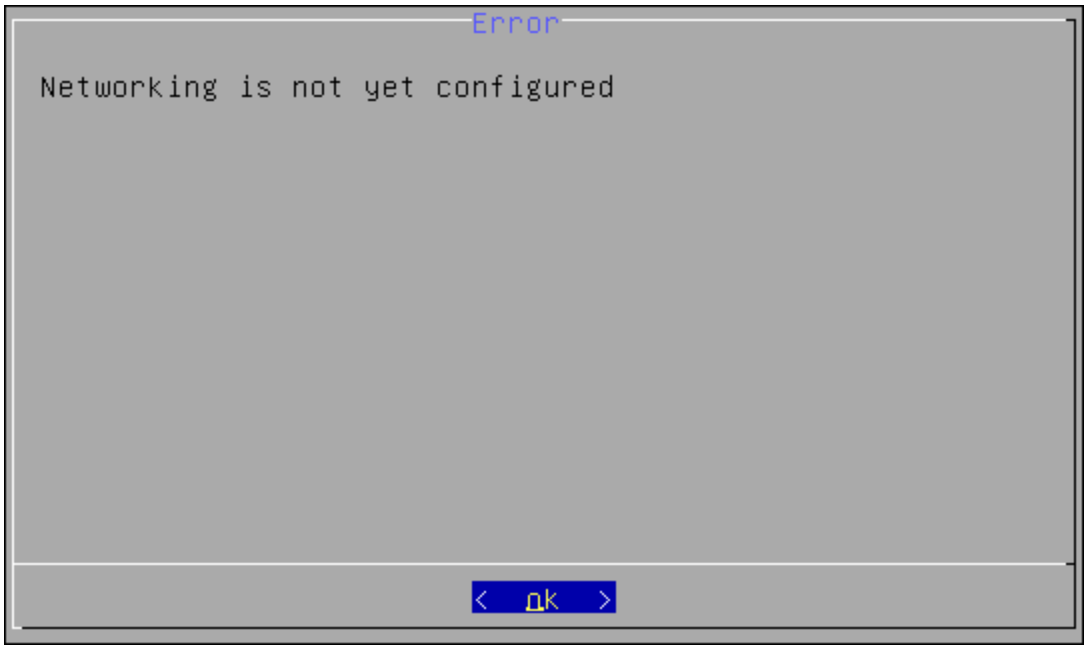
Solution:

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**.

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.

Index

U