



NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
System Requirements	4
NetIQ Advanced Authentication Framework Overview	5
About NetIQ Advanced Authentication Framework	5
NetIQ Server Appliance Functionality	5
Architecture	6
Basic Architecture	6
Enterprise Architecture	7
Enterprise Architecture with Load Balancer	8
Terms	9
Authentication Method	9
Authentication Chain	9
Authentication Event	10
NetIQ Server Appliance Deployment	11
Installing NetIQ Server Appliance	12
Graphic Mode	12
Text Mode	14
Configuration Console	17
Configuring Appliance Networking	18
Configuring Time and NTP Servers	21
Rebooting Appliance	24
Shutting Down Appliance	25
Setting up NetIQ Server Appliance Mode	26
DB Master	27
DB Slave	30
Member	34
First Login To NetIQ Admin Interface	37
Configuring NetIQ Server Appliance	39
Adding Repository	40
Configuring Method	42
Creating Chain	43
Configuring Event	44
Configuring Policy	45
Configuring Server Options	46
Adding License	47
Default Ports for NetIQ Server Appliance	48
Troubleshooting	49
Partition Disks	50
Networking Is Not Configured	51
Index	52

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 Server Appliance Functionality](#)
- [Architecture](#)
- [Terms](#)

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

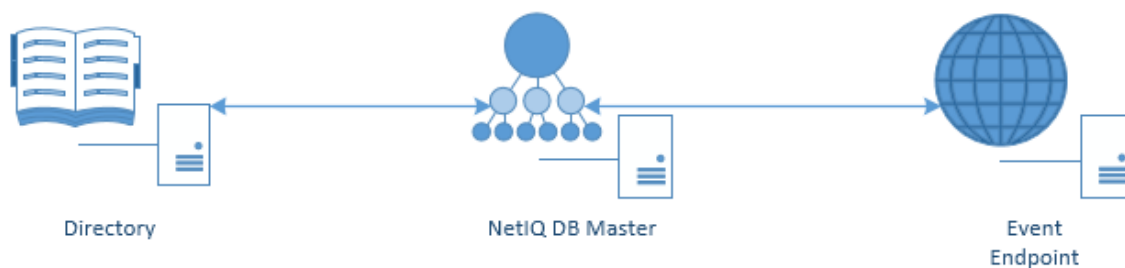
Architecture

In this chapter:

- [Basic Architecture](#)
- [Enterprise Architecture](#)
- [Enterprise Architecture with Load Balancer](#)

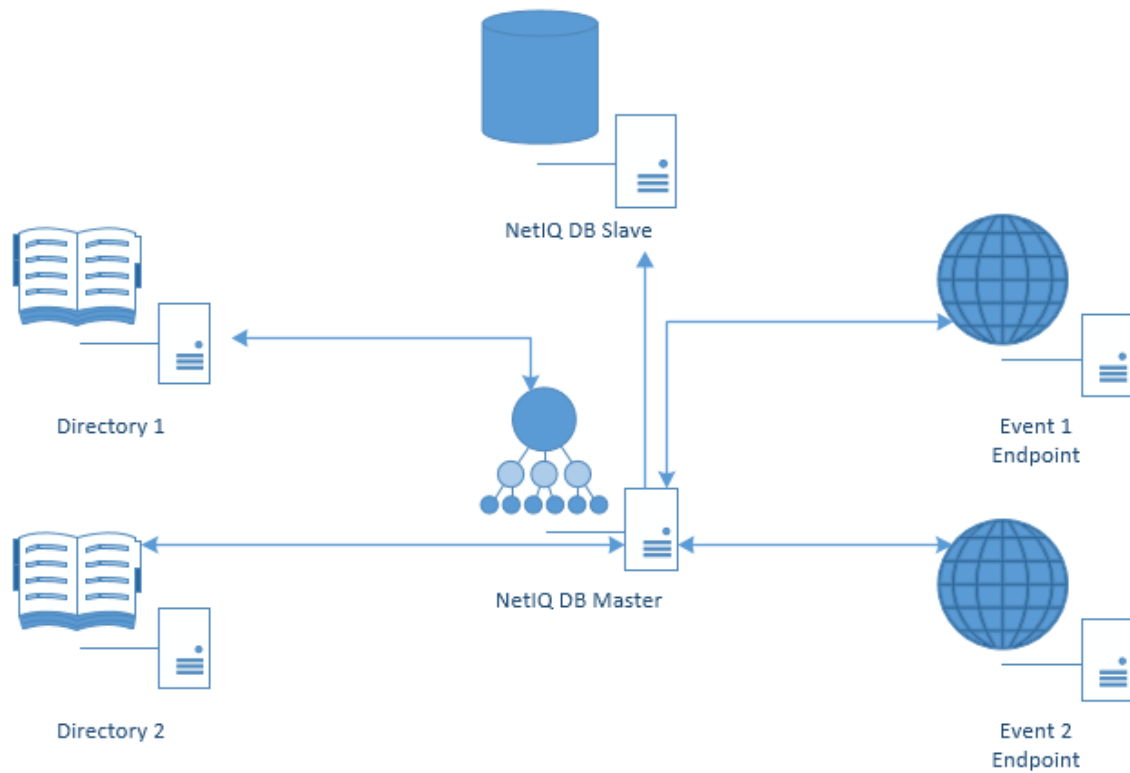
Basic Architecture

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

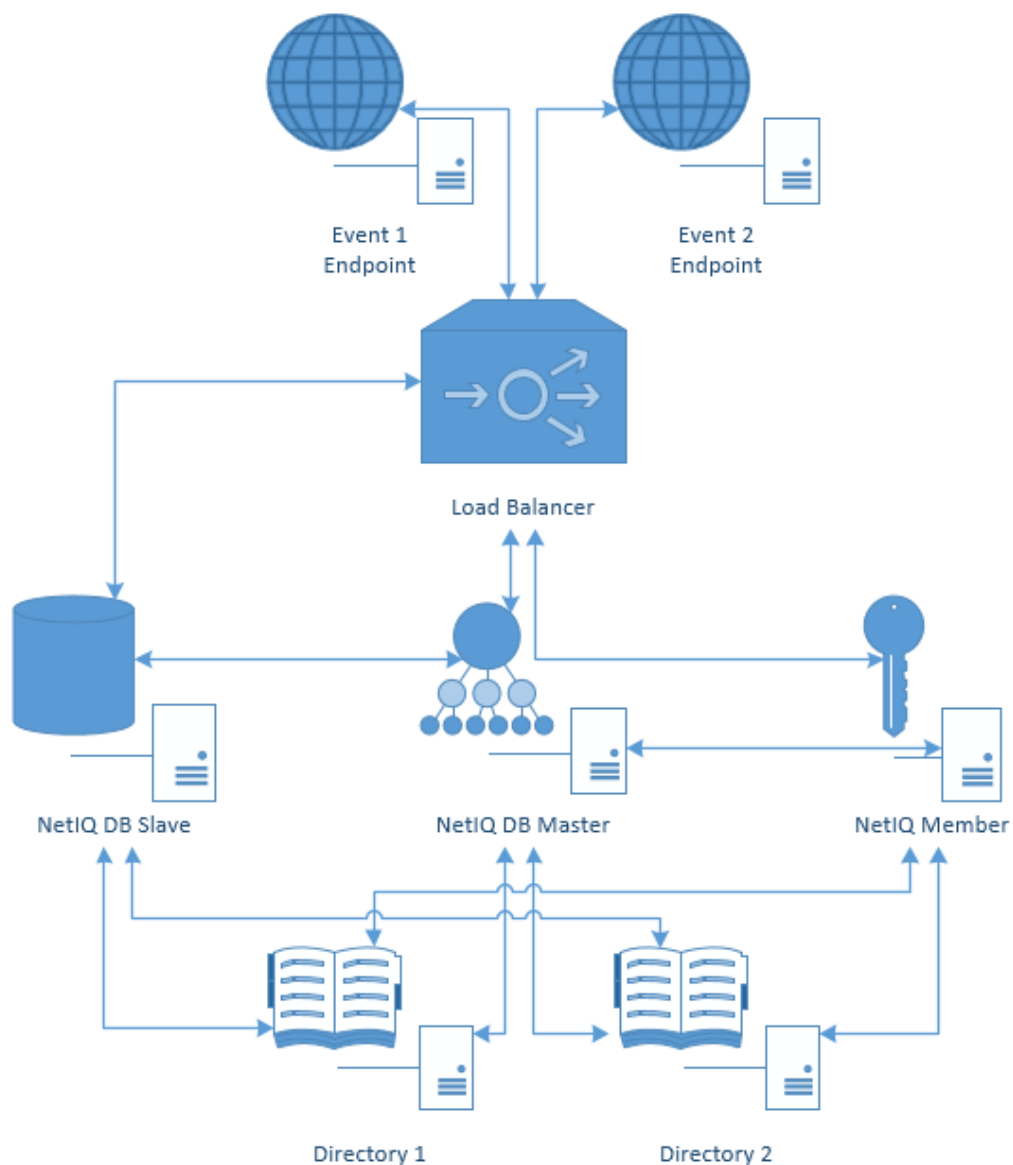
The following diagram shows interaction between DB Master, several directories and events. DB Master interacts at the same time with DB Slave, which contains the copy of the DB Master database. If DB Master dies, DB Slave will take over (hot slave).



Enterprise Architecture with Load Balancer

i 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 Chain](#)
- [Authentication Event](#)

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 considered 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](#)
- [Configuration Console](#)
- [Setting up Server Mode](#)
- [First Login to NetIQ Admin Interface](#)
- [Configuring NetIQ Server Appliance](#)

Installing NetIQ Server Appliance

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

- [Graphic Mode](#)
- [Text Mode](#)

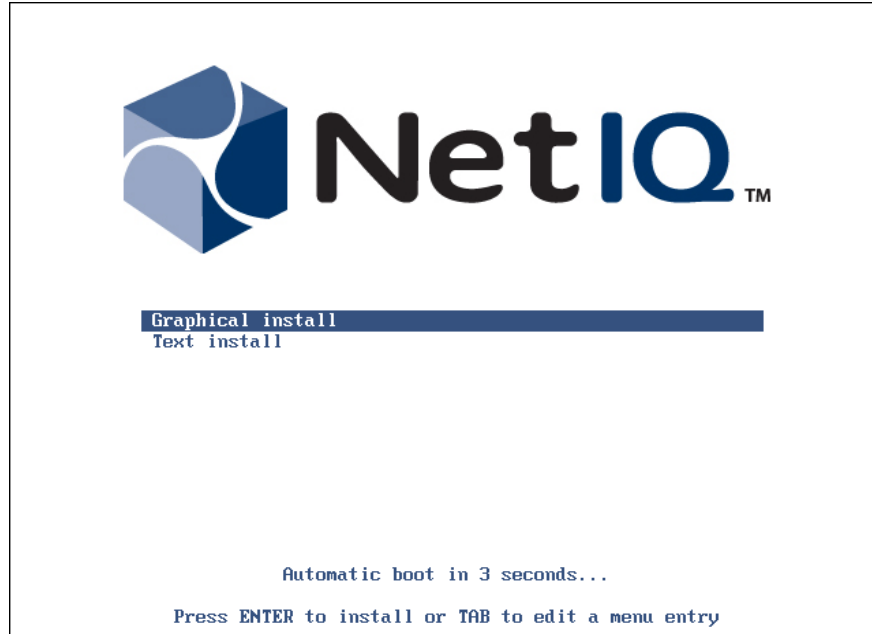
Graphic Mode

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

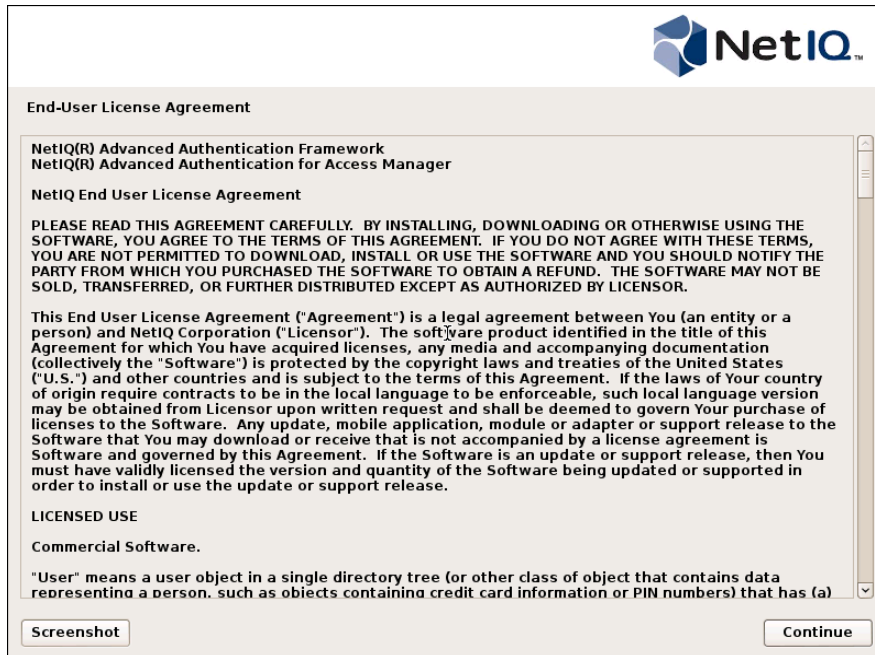
 To cancel the installation, click the **Cancel** button. The button is available only for certain processes of installation.

To install NetIQ Server appliance in the graphic mode:

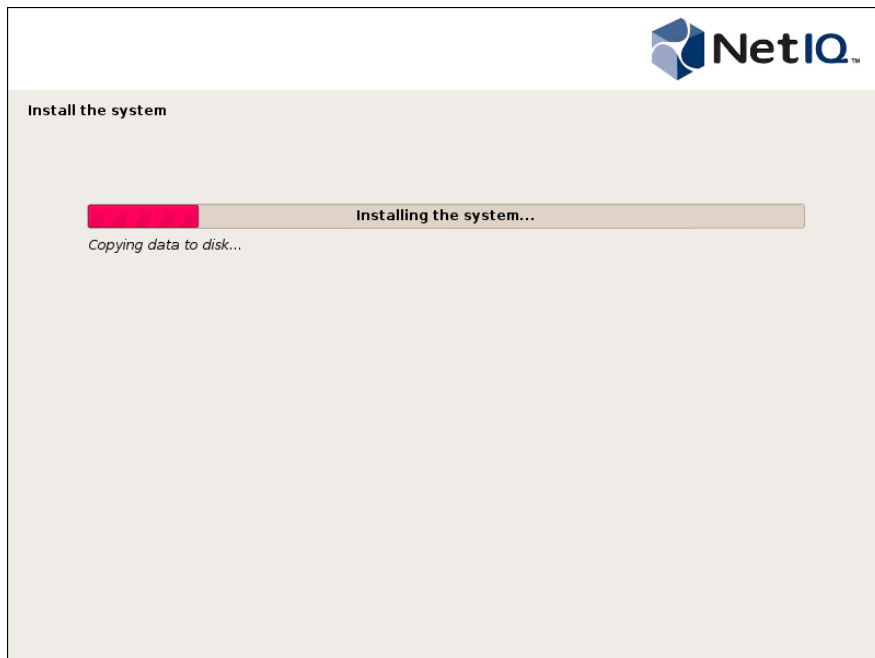
1. Select the **Graphical install** menu entry in the Setup Wizard and press **ENTER**.



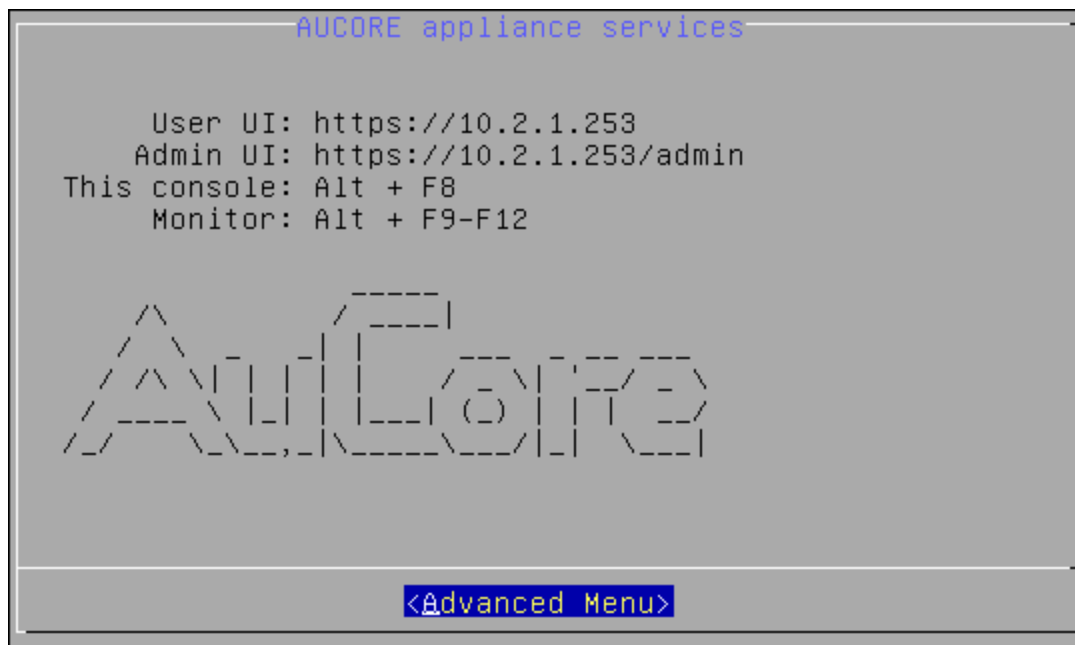
2. Read the license agreement. Select **I agree** at the bottom and click **Continue**.




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**.



Graphical install
Text install

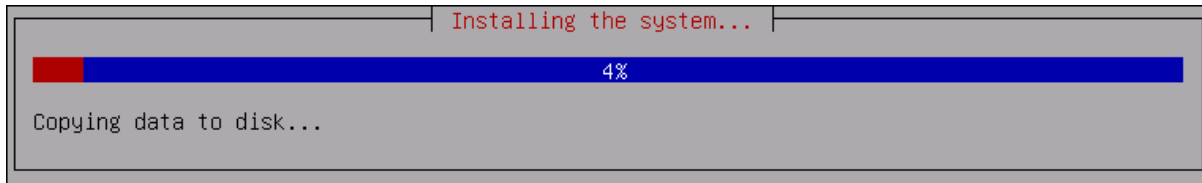
Press ENTER to install or TAB to edit a menu entry

[!!!] End-User License Agreement	
NetIQ(R) Advanced Authentication Framework NetIQ(R) Advanced Authentication for Access Manager	
NetIQ End User License Agreement	
PLEASE READ THIS AGREEMENT CAREFULLY. BY INSTALLING, DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, YOU ARE NOT PERMITTED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE AND YOU SHOULD NOTIFY THE PARTY FROM WHICH YOU PURCHASED THE SOFTWARE TO OBTAIN A REFUND. THE SOFTWARE MAY NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED EXCEPT AS AUTHORIZED BY LICENSOR.	
This End User License Agreement ("Agreement") is a legal agreement between You (an entity or a person) and NetIQ Corporation ("Licensor"). The software product identified in the title of this Agreement for which You have acquired licenses, any media and accompanying documentation (collectively the "Software") is protected by the copyright laws and treaties of the United States ("U.S.") and other countries and is subject to the terms of this Agreement. If the laws of Your country of origin require contracts to be in the local language to be enforceable, such local language version may be obtained from Licensor upon written request and shall be deemed to govern Your purchase of licenses to the Software. Any update, mobile application, module or adapter or support release to the Software that You may download or receive that is not accompanied by a license agreement is Software and governed by this Agreement. If the Software is an update or support release, then You must have validly licensed the version and quantity of the Software being updated or supported in order to install or use the update or support release.	
LICENSED USE	
Commercial Software.	
<input type="button" value="Continue"/>	

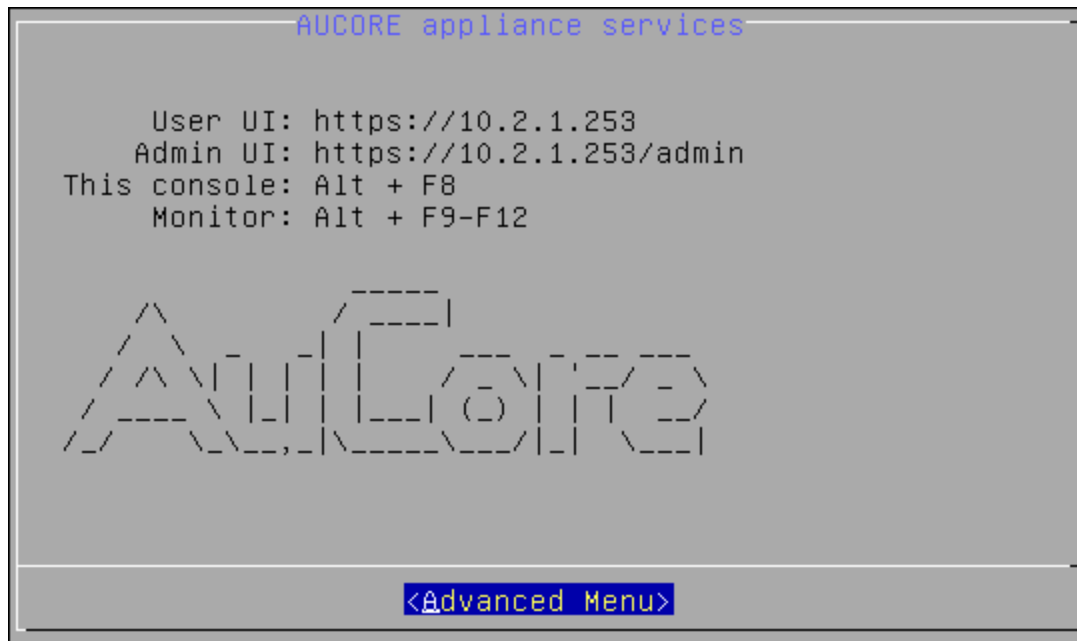
2. Select **I agree** to continue installation.

[!!!] End-User License Agreement	
<input checked="" type="radio"/> I agree <input type="radio"/> I don't agree	
<input type="button" value="Go Back"/>	

3. The installation will be automatically started.



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

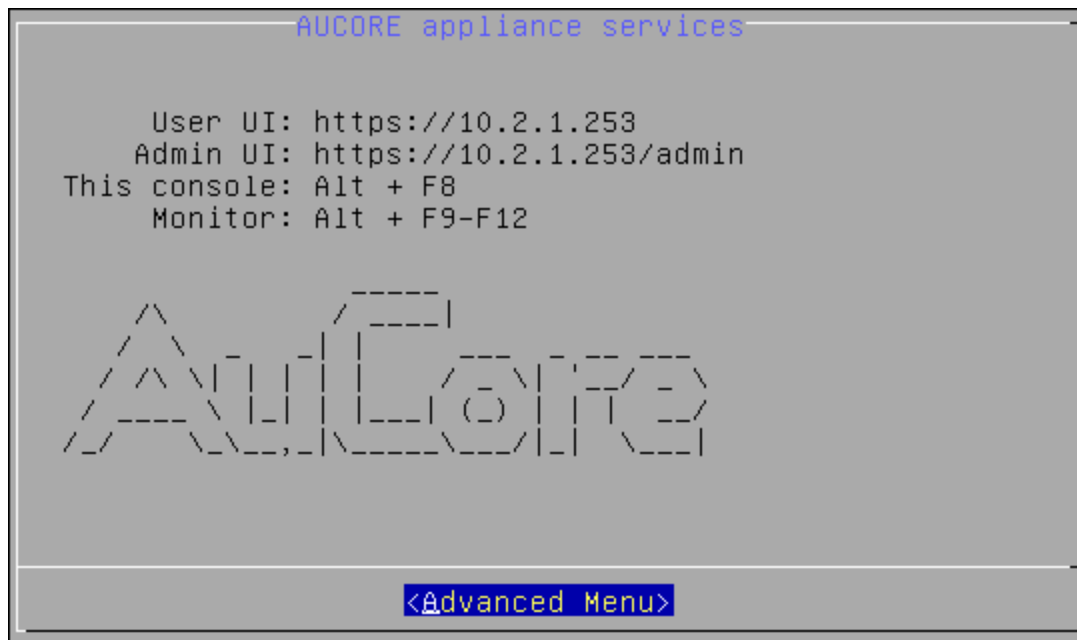


Configuration Console

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.

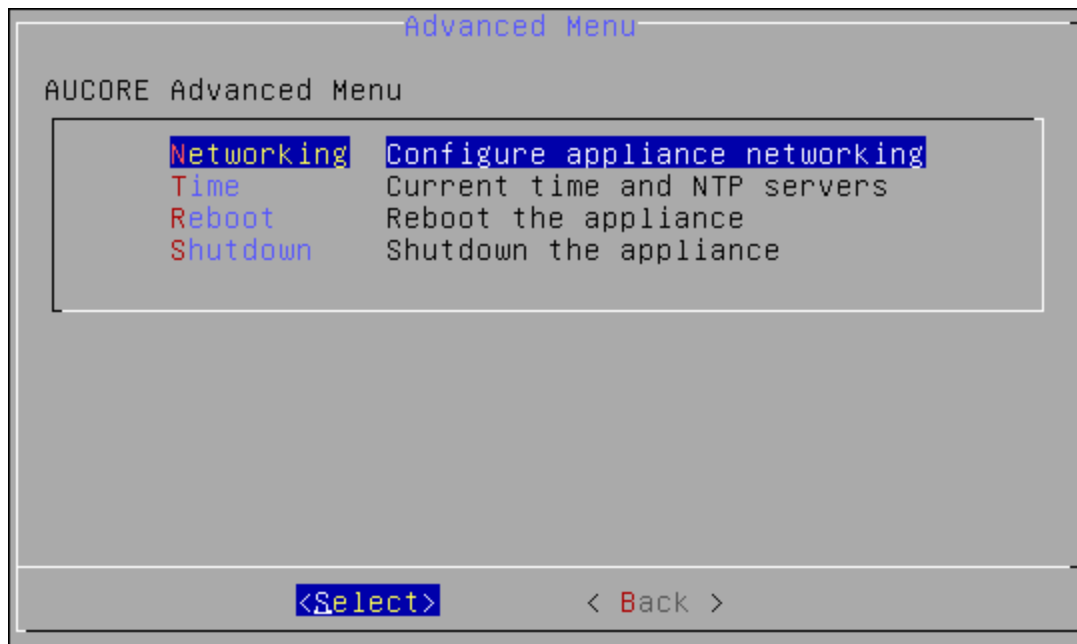


To proceed to NetIQ Server appliance management, select **Advanced Menu**.

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.

eth0 configuration

IP Address: 10.2.0.208
Netmask: 255.255.254.0
Default Gateway: 10.2.0.100
Name Server(s): 10.2.0.254 10.2.0.4

Networking configuration method: dhcp

DHCP	Configure networking automatically
StaticIP	Configure networking manually

<Select> < Back >

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

eth0 configuration

IP Address: 10.2.0.208
Netmask: 255.255.254.0
Default Gateway: 10.2.0.100
Name Server(s): 10.2.0.254 10.2.0.4

Networking configuration method: dhcp

DHCP	Configure networking automatically
StaticIP	Configure networking manually

<Select> < Back >

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

Network settings

Static IP configuration (eth0)

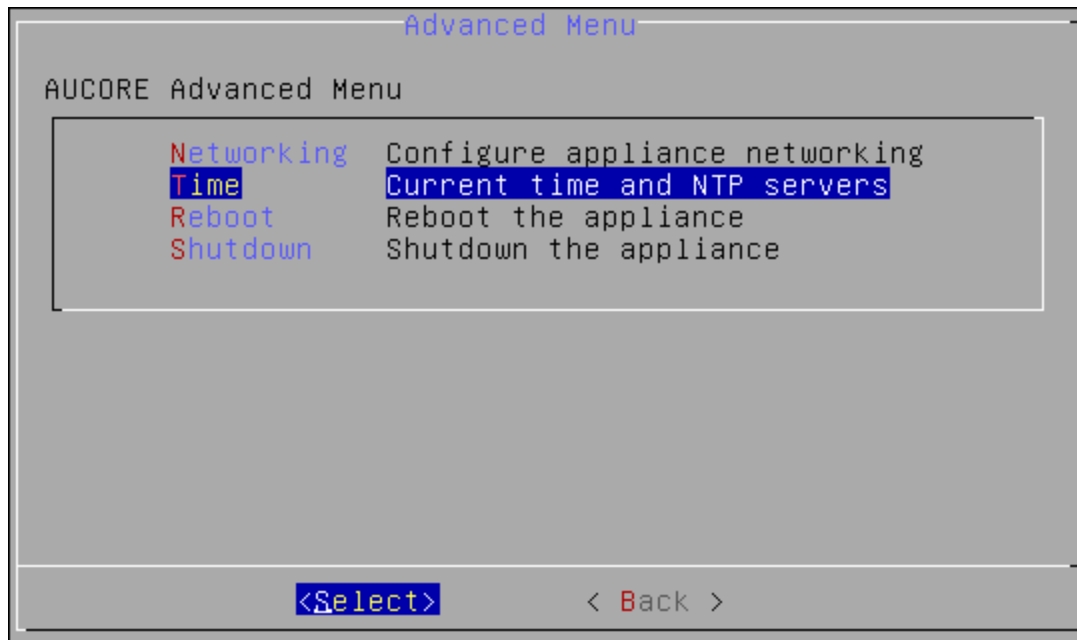
IP Address	10.2.0.208
Netmask	255.255.254.0
Default Gateway	10.2.0.100
Name Server	10.2.0.254
Name Server	10.2.0.4
Name Server	

<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.

Configure timezone and NTP servers

Current time: Mon Mar 30 07:48:10 2015
 Timezone: UTC (UTC+00:00)

NTP servers:

0.debian.pool.ntp.org iburst
 1.debian.pool.ntp.org iburst
 2.debian.pool.ntp.org iburst
 3.debian.pool.ntp.org iburst

Refresh NTP servers

Refresh current time
Configure NTP servers

<Select> < Back >

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

Configure timezone and NTP servers

Current time: Mon Mar 30 07:48:10 2015
 Timezone: UTC (UTC+00:00)

NTP servers:

0.debian.pool.ntp.org iburst
 1.debian.pool.ntp.org iburst
 2.debian.pool.ntp.org iburst
 3.debian.pool.ntp.org iburst

Refresh NTP servers

Refresh current time
Configure NTP servers

<Select> < Back >

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

Configure NTP Servers

NTP servers:

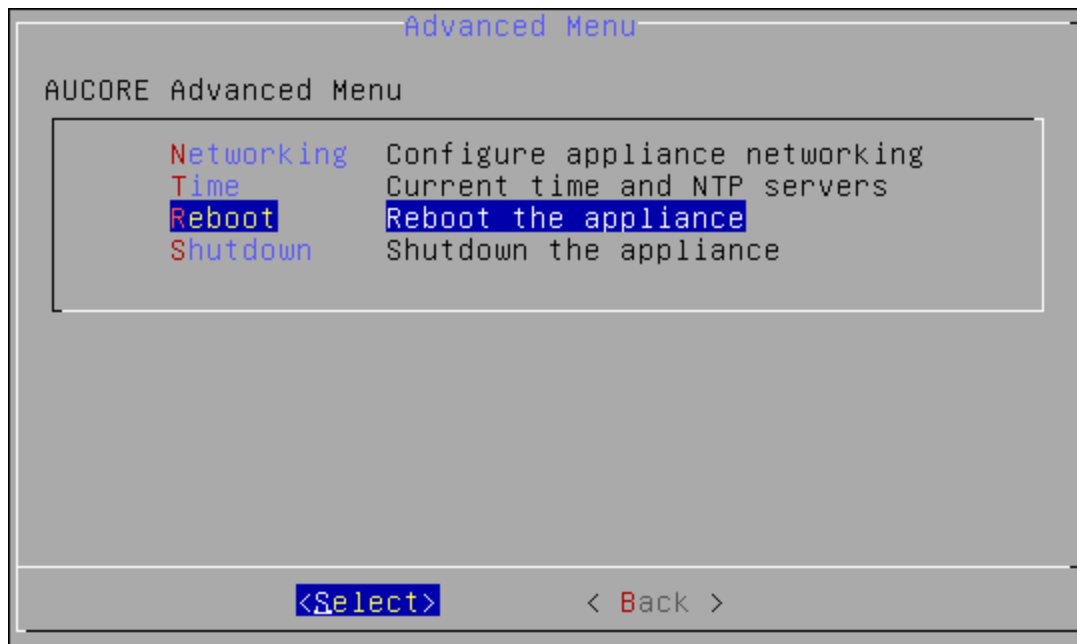
Server 1:	0.debian.pool.ntp.org	iburst
Server 2:	1.debian.pool.ntp.org	iburst
Server 3:	2.debian.pool.ntp.org	iburst
Server 4:	3.debian.pool.ntp.org	iburst

<Apply > <Cancel>

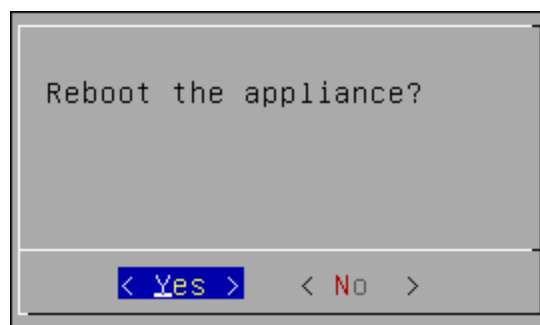
Rebooting Appliance

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

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



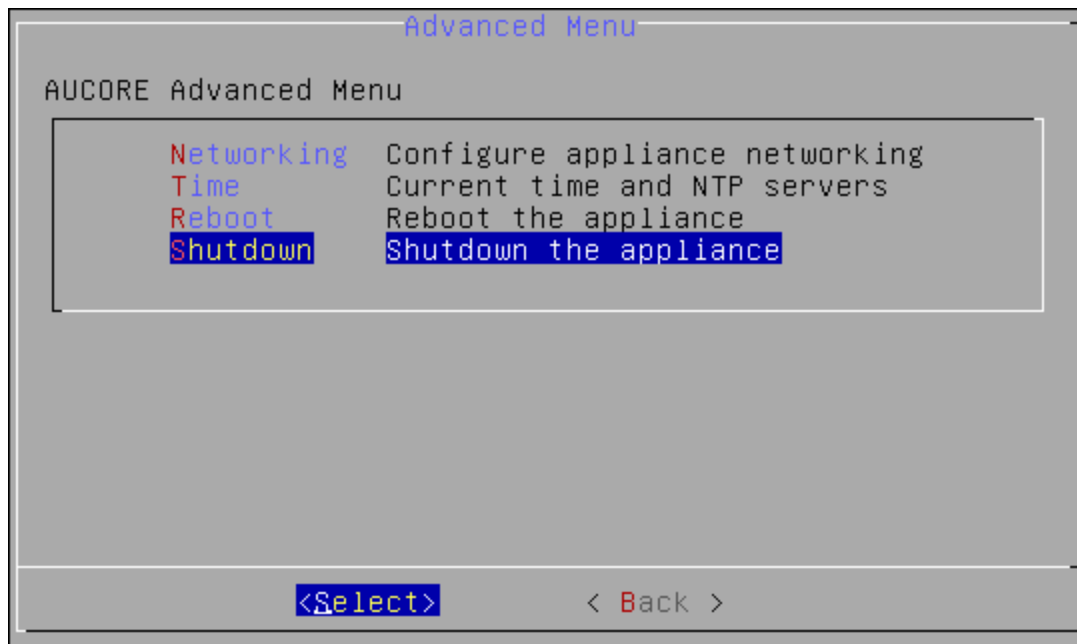
3. The confirmation message will be displayed. Select **Yes** to continue.



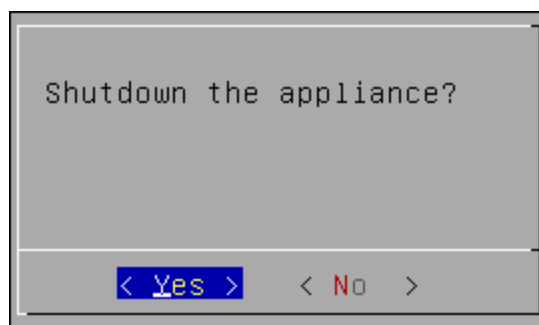
Shutting Down Appliance

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.

The screenshot shows the 'INSTALL' screen with a sidebar on the left containing the following options: Mode, DNS hostname, Password, Import DB Info, Create key, Copy DB, and Finish. The 'Mode' option is selected and highlighted in red. The main content area is titled 'Server Mode' and includes the instruction 'Select server mode and press 'Next''. There are three buttons: 'DB Master' (highlighted in blue), 'DB Slave', and 'Member'. To the right of each button is a description: 'DB Master' is 'Server with master DB. All other servers will connect to this DB'; 'DB Slave' is 'If master dies, this DB will take over (hot slave)'; and 'Member' is 'Server with no DB. There can be many farm members but 1 pair of master-slave only'. A blue 'Next' button with a right arrow is at the bottom right.

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

The screenshot shows the 'INSTALL' screen with the same sidebar as the previous step. The 'DNS hostname' option is selected and highlighted in red. The main content area is titled 'DNS hostname' and includes the instruction 'Other farm members will connect to **database installed on this server**. They connect by DNS hostname or IP address.' Below this, it says 'Please register this server in DNS/DHCP infrastructure and enter its hostname. You may enter IP address, but you will not be able to change it (only reinstall).' There is a text input field labeled 'My DNS hostname' containing the value '10.2.1.206'. At the bottom, there are two blue buttons: 'Back' with a left arrow and 'Next' with a right arrow.

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

The screenshot shows the 'INSTALL' window with a sidebar on the left containing the following options: Mode, DNS hostname, Password, Import DB Info, Create key, Copy DB, and Finish. The 'Password' option is highlighted in red. The main area is titled 'Password of LOCAL\admin user' and contains two input fields labeled 'Password' and 'Confirmation', both filled with dots. Below the fields are two blue buttons: 'Back' with a left arrow and 'Next' with a right arrow.

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

The screenshot shows the 'INSTALL' window with the sidebar options: Mode, DNS hostname, Password, Import DB Info, Create key, Copy DB, and Finish. The 'Create key' option is highlighted in red. The main area is titled 'Create encryption key' and displays 'current key AES-CFB PLEASE REGENERATE!'. Below this text is a green 'Create' button. At the bottom are two blue buttons: 'Back' with a left arrow and 'Next' with a right arrow.

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

INSTALL

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Create encryption key

current key **AES-CFB 2015-03-30T09:53:02Z**

Create

BackNext

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

INSTALL

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Finish

Mode: **DB MASTER**

Database: **localhost/aucore_prod**

Encryption: **AES-CFB 2015-03-30T09:53:02Z**

Press the button to write configuration and restart services.

BackSave & Restart

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.

The screenshot shows the 'INSTALL' screen with a sidebar on the left containing the following menu items: Mode, DNS hostname, Password, Import DB Info, Create key, Copy DB, and Finish. The 'Mode' item is highlighted in red. The main content area is titled 'Server Mode' and includes the instruction 'Select server mode and press 'Next''. There are three selectable options: 'DB Master' (described as 'Server with master DB. All other servers will connect to this DB'), 'DB Slave' (described as 'If master dies, this DB will take over (hot slave)' and highlighted with a blue border), and 'Member' (described as 'Server with no DB. There can be many farm members but 1 pair of master-slave only'). A blue 'Next' button with a right arrow is located at the bottom right of the main content area.

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

The screenshot shows the 'INSTALL' screen with the same sidebar as the previous step, but now the 'DNS hostname' item is highlighted in red. The main content area is titled 'DNS hostname' and includes the following text: 'Other farm members will connect to **database installed on this server**. They connect by DNS hostname or IP address.' and 'Please register this server in DNS/DHCP infrastructure and enter its hostname. You may enter IP address, but you will not be able to change it (only reinstall)'. Below this text is a label 'My DNS hostname' followed by a text input field containing the value '10.2.1.198'. At the bottom right, there are two blue buttons: 'Back' with a left arrow and 'Next' with a right arrow.

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 screenshot displays the AUTHASAS NetIQ Admin Interface. On the left is a dark sidebar with a menu containing: Info, Repositories, Methods, Chains, Events, Policies, Server Options, **Farm servers** (highlighted in red), Licenses, OATH Tokens, and Logs. The main content area is titled 'Farm servers' and includes a breadcrumb 'Home > Farm servers'. Under the 'Replication' section, it shows 'Server mode: DB MASTER' and 'Replication: stopped' in red, with a note 'Not replicating'. Below this is the 'Install DB SLAVE' section, which contains instructions: '- Run installation of slave' and '- When you are on "Import database information" step, go here, enter slave hostname and press the button'. A text field labeled 'Slave host' contains '10.2.1.198'. A blue 'Register slave' button is positioned below the field. The 'Install new MEMBER server' section follows, with instructions: '- Run installation of server' and '- When you are on "Import database information" step, go here, enter new server hostname and press the button'. A text field labeled 'Member server host' contains 'server.being.installed.hostname'. A blue 'Export database info' button is located below the field. The footer shows '2015 © Authasas' on the left and 'build: AAA-develop-5.1.2-2-170' on the right.

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

INSTALL

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Import database information

Now this server will receive database connection and encryption parameters. Please go to MASTER server, Farm servers section. Enter this server hostname and press the button. MASTER will send information here.

Imported! Press Next

← Back

Next →

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

INSTALL

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Copy database

Now copy master database (10.2.1.206)

Copy

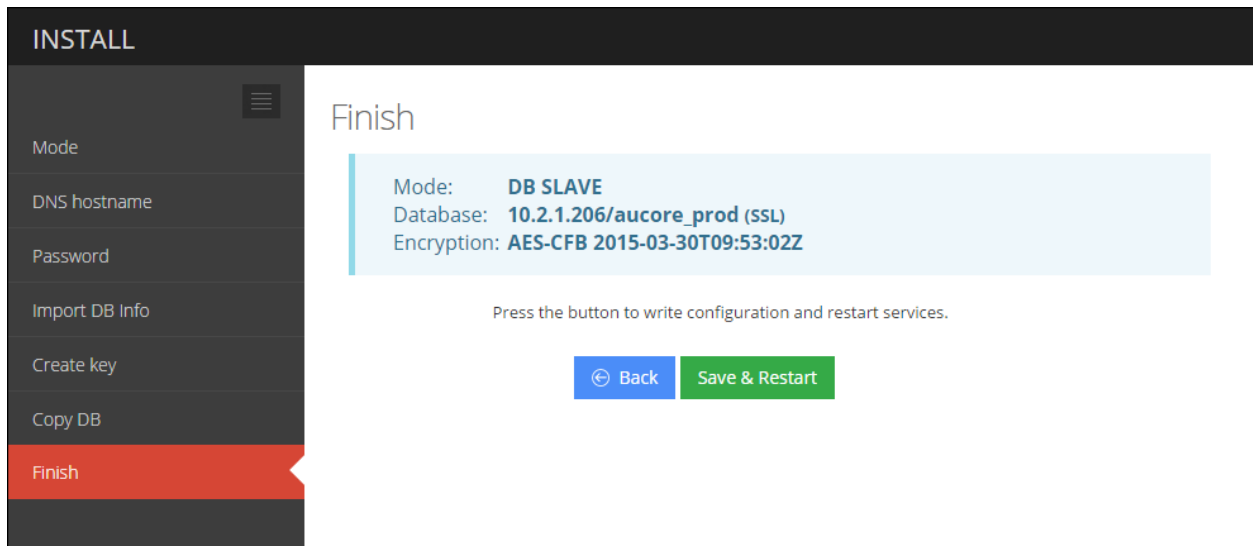
Press the button to start. It may take long time




← Back

Next →


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

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



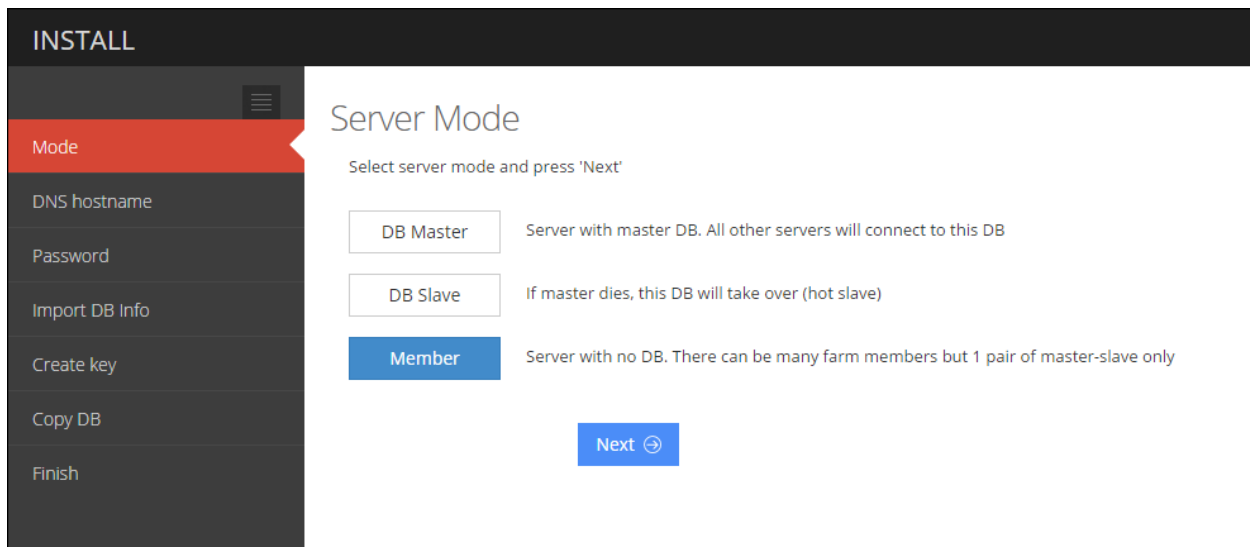
-  Only one DB Slave server can be installed.
-  If you lost your DB Slave server, go to the NetIQ Admin Interface of the DB Master server, open the **Farm servers** section and click **Stop**. Install a new DB Slave server.
-  If you lost your DB Master server, you can convert DB Slave server to DB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

AUTHASAS

LOCAL\admin

Info

Repositories

Methods

Chains

Events

Policies

Server Options

Farm servers

Licenses

OATH Tokens

Logs

Farm servers

Home > Farm servers

Replication

Server mode: **DB MASTER** paired with 10.2.1.198
Replication: **replicating**
Configured and running

Stop replication

If you lost SLAVE server or replication error occurs, you want to install new SLAVE.
Press 'stop' below, then install new slave server as usual.

Stop

Install new MEMBER server

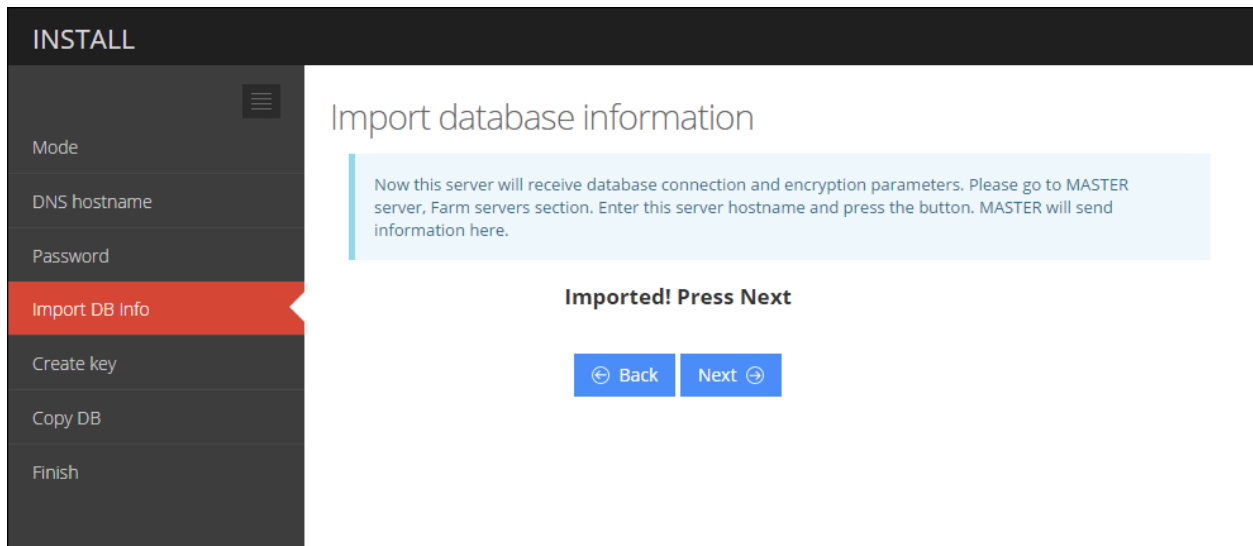
Use this tool to add new member server as follows:
- Run installation of server
- When you are on "**Import database information**" step, go here, enter new server hostname and press the button

Member server host10.2.0.231

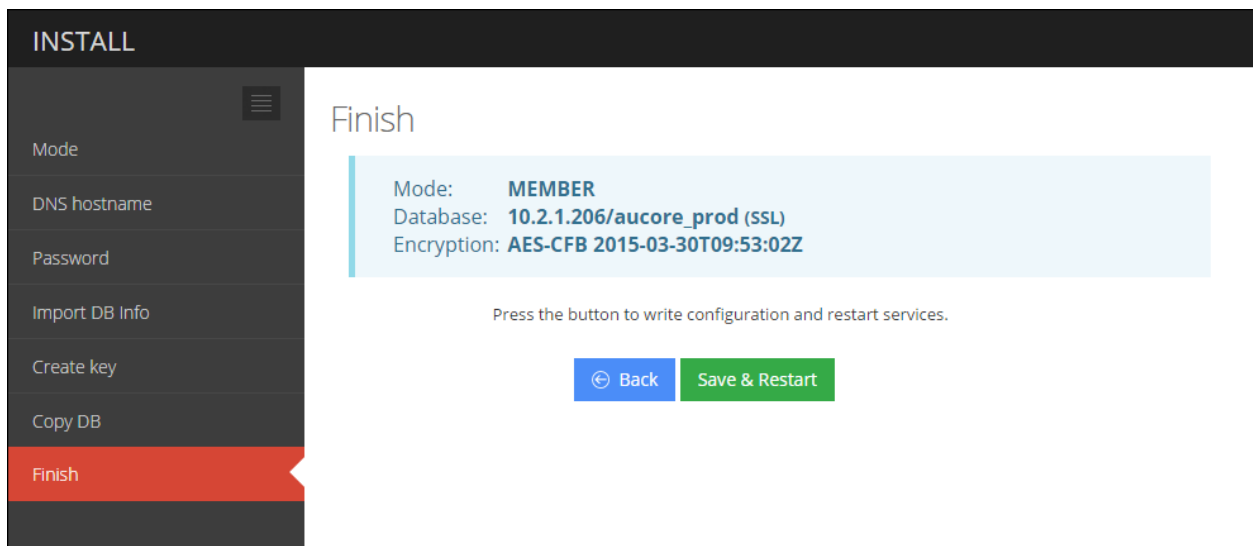
Export database info

2015 © Authasasbuild: AAA-develop-5.1.2-2-170

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



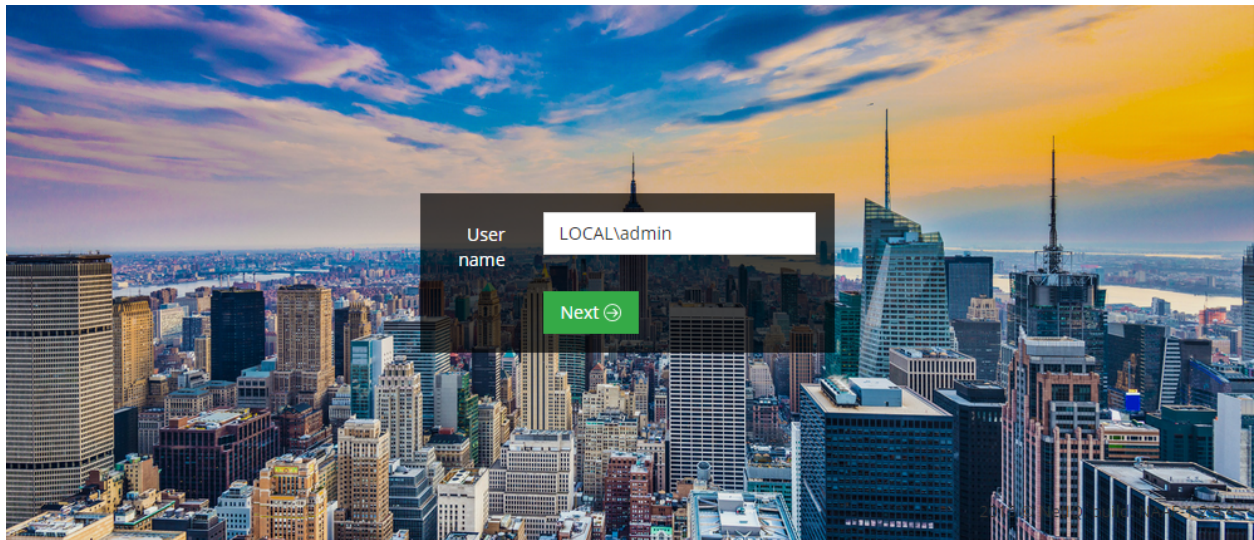
4. Click the **Save & Restart** button to write configuration and restart services. Services will be restarted within 30 seconds.



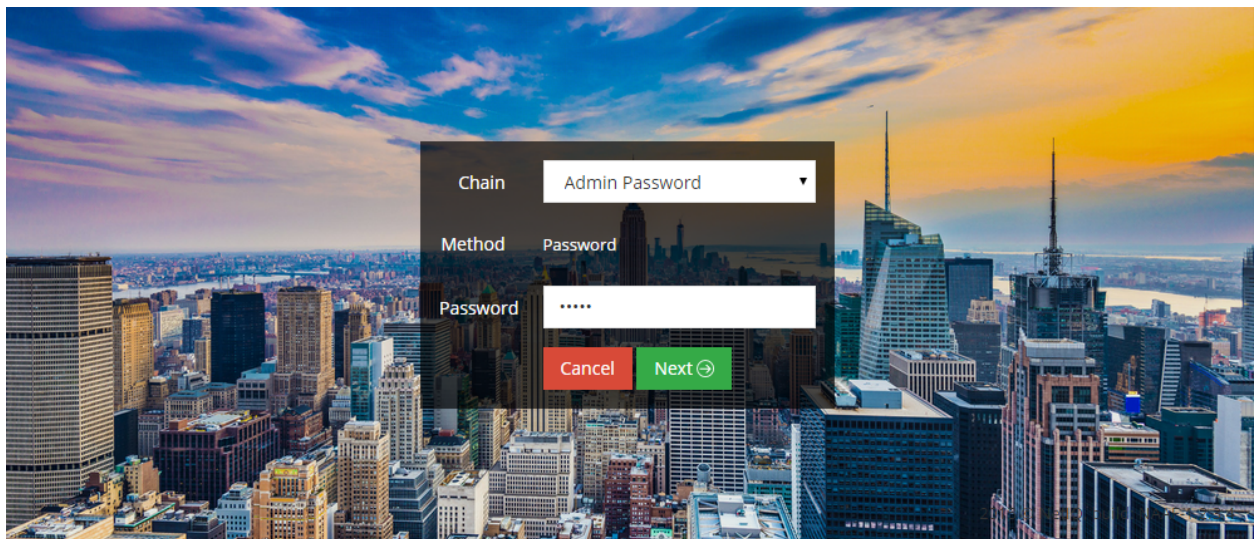
First Login To NetIQ Admin Interface

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

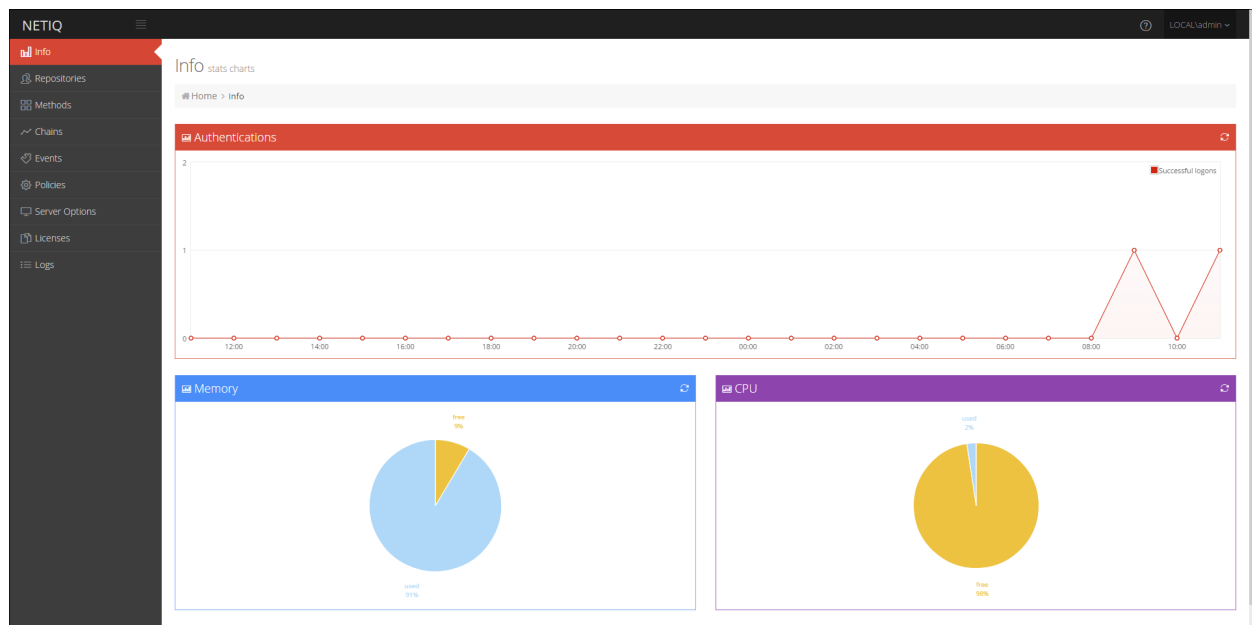
1. Enter administrator's login in the following format: repository\user (**local\admin** by default). Click **Next** to continue.



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	<input type="checkbox"/>	<div><div></div><div></div></div>

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.

NETIQ LOCAL\admin

Info
Repositories
Methods
Chains
Events
Policies
Server Options
Farm servers
Licenses
Logs

Method Settings Edit

Home > Methods > Method Settings Edit

Security questions

Min. answer length:

Correct questions for logon:


Total questions for logon:

Questions	
	Add
Question	
What was the make and model of your first car?	Edit Delete
What was the name of your elementary/primary school?	Edit Delete
In what country were you born?	Edit Delete
In what city or town did you meet your spouse/partner?	Edit Delete
What is the name of the place your wedding was held?	Edit Delete

[Save](#) [Cancel](#)

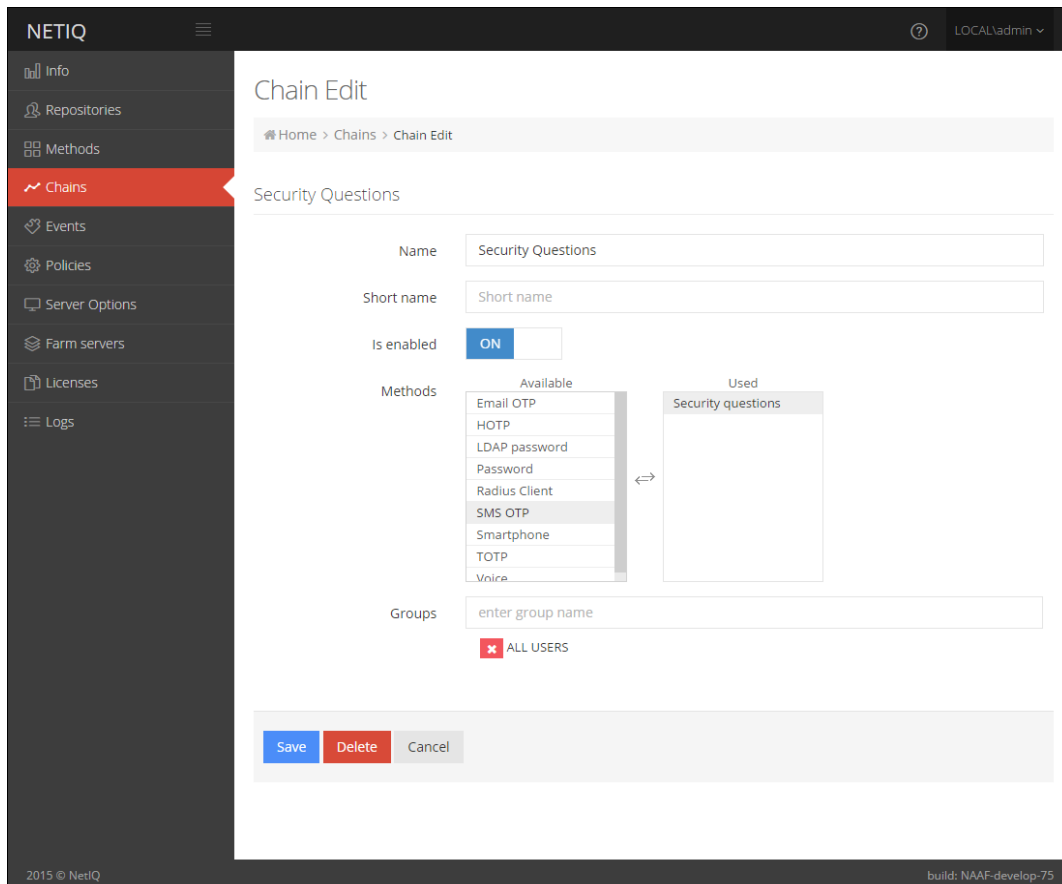
2015 © NetIQ build: NAAF-develop-75

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.



The screenshot shows the 'Chain Edit' interface in the NetIQ console. The left sidebar contains navigation links: Info, Repositories, Methods, Chains (highlighted), Events, Policies, Server Options, Farm servers, Licenses, and Logs. The main content area is titled 'Chain Edit' and shows the configuration for a chain named 'Security Questions'. The breadcrumb trail is 'Home > Chains > Chain Edit'. The 'Security Questions' section includes the following fields:

- Name:** Security Questions
- Short name:** Short name
- Is enabled:** ON (toggle button)
- Methods:** A list of available methods (Email OTP, HOTP, LDAP password, Password, Radius Client, SMS OTP, Smartphone, TOTP, Voice) and a 'Used' section containing 'Security questions'. A double-headed arrow indicates the relationship between the two lists.
- Groups:** A text field with the placeholder 'enter group name' and a red asterisk icon next to 'ALL USERS'.

At the bottom of the form are three buttons: 'Save' (blue), 'Delete' (red), and 'Cancel' (gray). The footer of the console shows '2015 © NetIQ' on the left and 'build: NAAF-develop-75' on the right.

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.

The screenshot shows the NetIQ Event Edit configuration page. The left sidebar contains a navigation menu with options: Info, Repositories, Methods, Chains, Events (highlighted), Policies, Server Options, Farm servers, Licenses, and Logs. The main content area is titled 'Event Edit' and shows the configuration for the 'Radius Server' event. The 'Is enabled' toggle is set to 'ON'. Below this, there are two columns: 'Available' and 'Used'. The 'Available' column lists methods: Admin Password, Authenticators, Management logon, LDAP password, Authenticators, Management logon, Password, Counter based one time password, and Email. The 'Used' column lists methods: Password & TOTP, Password & HOTP, Password & SMS OTP, Password & Smartphone Out-of-Band, and Password & Voicecall. Below these columns is a 'Clients' section with a table for adding clients. The table has columns for Name, Client ID, and Enabled status. An 'Add' button is located at the top right of the Clients section. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

NETIQ

LOCAL\admin

Event Edit

Home > Events > Event Edit

Radius Server

Is enabled **ON**

Chains

Available	Used
Admin Password	Password & TOTP
Authenticators	Password & HOTP
Management logon	Password & SMS OTP
LDAP password	Password & Smartphone Out-of-Band
Authenticators	Password & Voicecall
Management logon	
Password	
Counter based one time password	
Email	

Clients


Name	Client	Enabled
	10.2.0.136	<input checked="" type="checkbox"/>

Add

Save **Cancel**

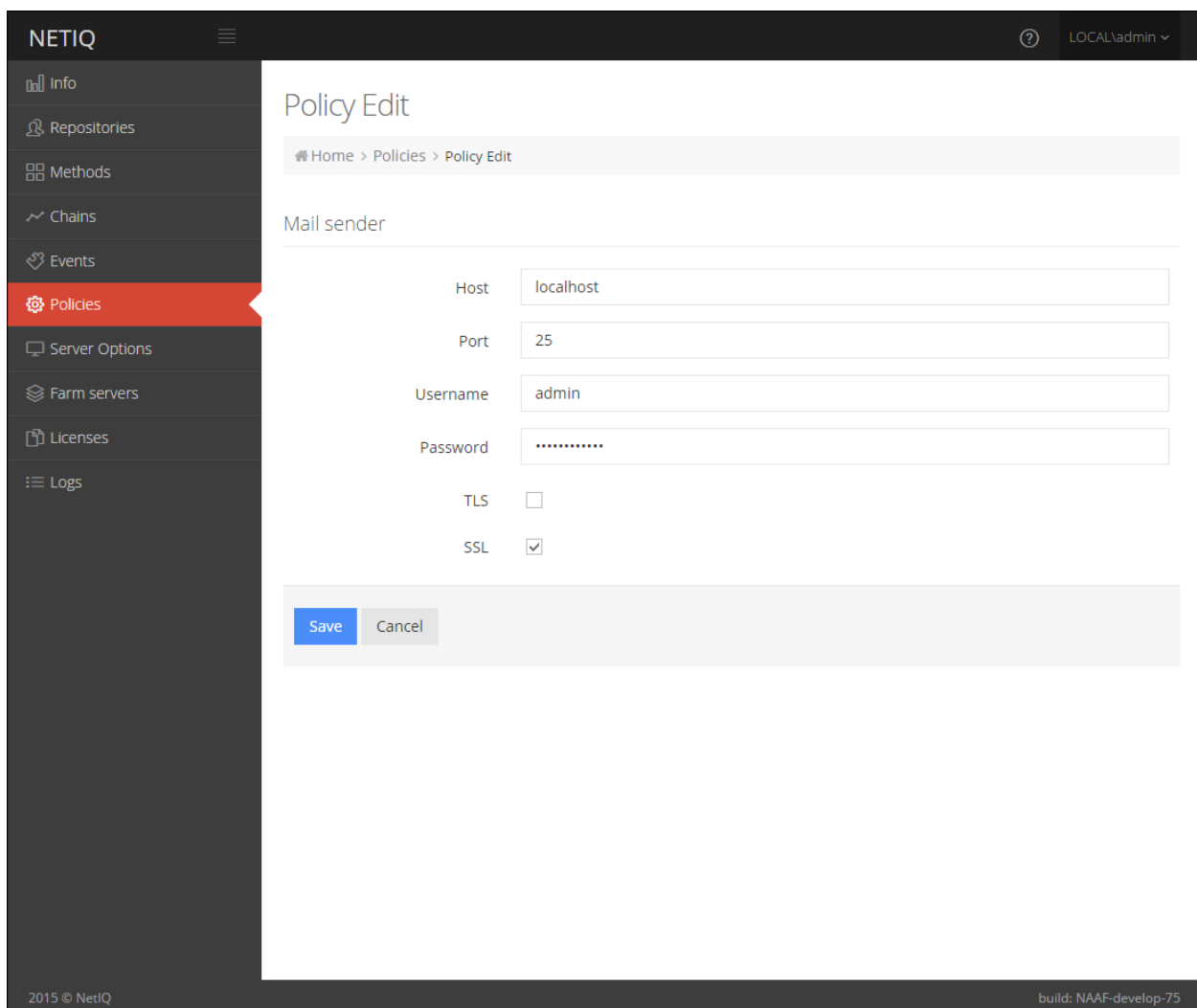
2015 © NetIQ build: NAAF-develop-75

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.



The screenshot shows the NetIQ web interface. On the left is a dark sidebar with a menu containing: Info, Repositories, Methods, Chains, Events, Policies (highlighted in red), Server Options, Farm servers, Licenses, and Logs. The main content area is titled "Policy Edit" and has a breadcrumb trail "Home > Policies > Policy Edit". Below the title is a section labeled "Mail sender" containing several form fields: "Host" with the value "localhost", "Port" with "25", "Username" with "admin", and "Password" with masked characters "*****". Below these are two checkboxes: "TLS" (unchecked) and "SSL" (checked). At the bottom of the form are two buttons: "Save" (in blue) and "Cancel" (in grey). The footer of the interface shows "2015 © NetIQ" on the left and "build: NAAF-develop-75" on the right.

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.

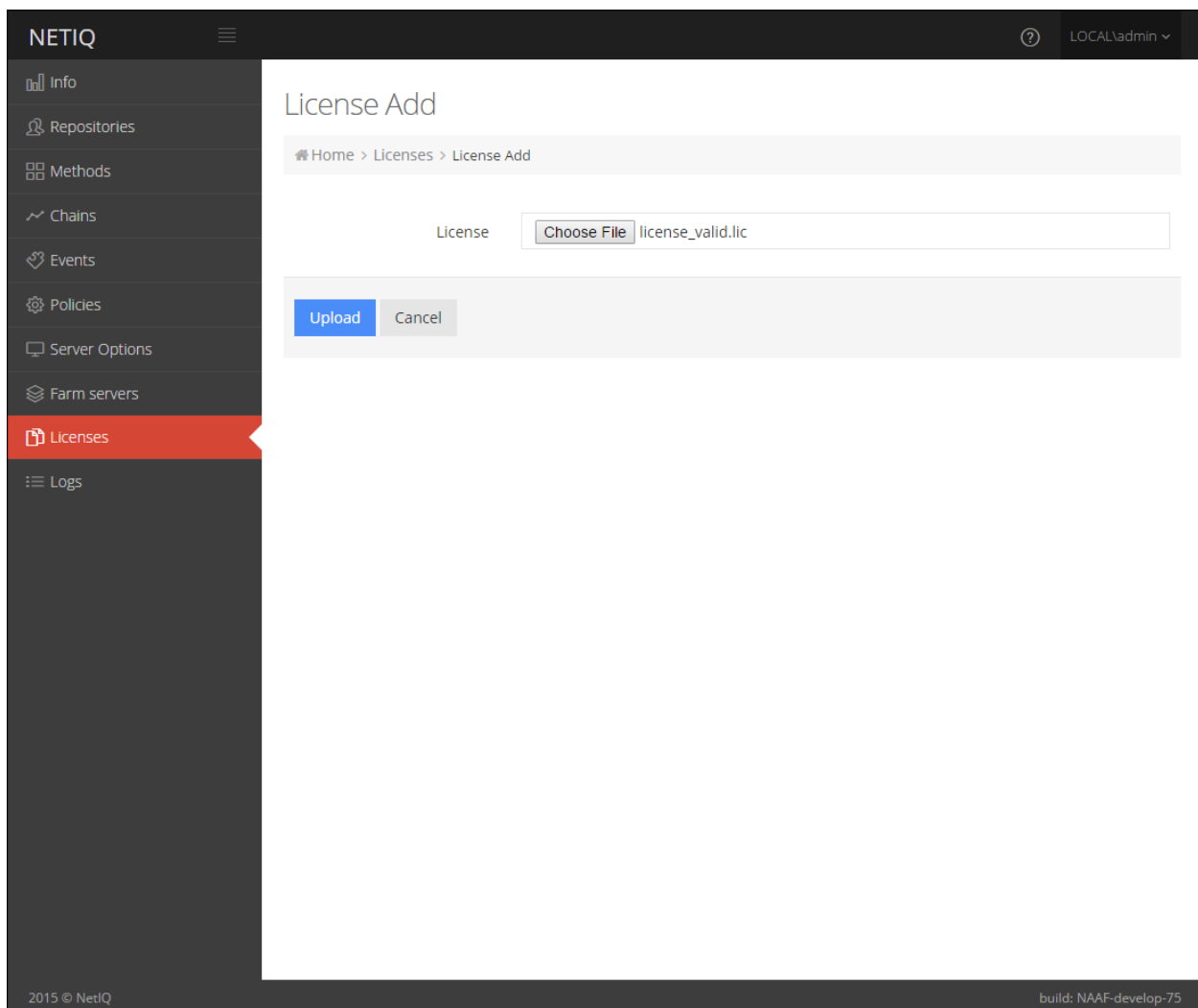
The screenshot shows the NetIQ web interface. On the left is a dark sidebar with a menu containing: Info, Repositories, Methods, Chains, Events, Policies, **Server Options** (highlighted in red), Farm servers, Licenses, and Logs. The main content area is titled "Server Options" with a subtitle "server specific configuration". Below this is a breadcrumb "Home > Server Options". The first section is "Web server SSL certificate for HTTPS". It contains a light blue box with instructions: "Upload certificate file (*.pem, *.crt). The file must contain **both** certificate and private key." followed by an "Example:" and a code block showing a PEM format certificate and private key. Below this is a form with a label "New SSL certificate", a "Choose File" button, and the text "No file chosen". At the bottom of this section is a blue "Upload" button. The second section is "Login page background". It contains a light blue box with instructions: "Upload login page background image in JPEG or PNG format." Below this is a form with a label "New background", a "Choose File" button, and the text "No file chosen". At the bottom of this section is a blue "Upload" button. The footer of the page shows "2015 © NetIQ" on the left and "build: NAAF-develop-75" on the right.

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.



The screenshot shows the NetIQ web interface for adding a license. The left sidebar contains a navigation menu with the following items: Info, Repositories, Methods, Chains, Events, Policies, Server Options, Farm servers, Licenses (highlighted in red), and Logs. The main content area is titled "License Add" and shows a breadcrumb trail: Home > Licenses > License Add. Below the breadcrumb, there is a "License" label and a file input field. The file input field has a "Choose File" button and the text "license_valid.lic". Below the file input field, there are two buttons: "Upload" (in blue) and "Cancel" (in gray). At the bottom of the interface, the footer shows "2015 © NetIQ" on the left and "build: NAAF-develop-75" on the right.

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 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	443	HTTPS	All Communications
Admin UI	443	HTTPS	All Communications
Enroll UI	443	HTTPS	All Communications

- * 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.

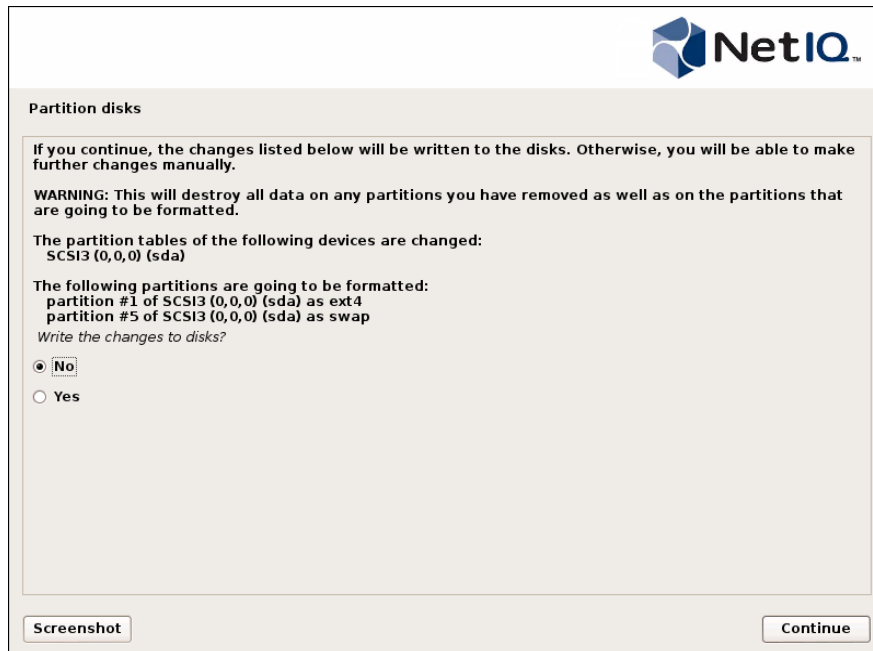
In this chapter:

- Partition Disks
- Networking Is Not Configured

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.

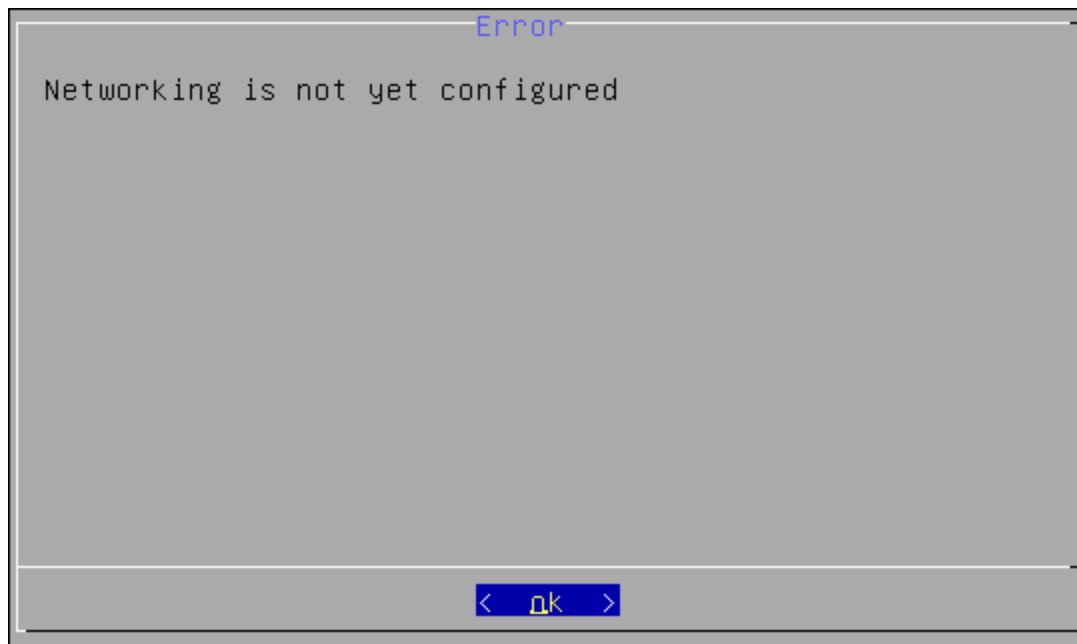
Solution:

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

A

Authentication 1, 3-6, 9-10, 48
Authenticator 3

C

Console 4, 11, 13, 16-18, 21, 24-25, 51
Create 28, 39

D

Default 48

E

Edit 42-45
Enroll 48
Export 34

F

File 46-47

L

License 47
Logon 3

M

Menu 17-18, 21, 24-25

P

Password 37, 40
PIN 9
Policy 45
Protocol 48

R

RADIUS 5, 10, 44, 48

S

Server 3, 5, 11-12, 14, 17-18, 24-27, 30, 34, 39, 46, 48, 50-51

System 4

U

User 9, 17, 40