



NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	4
About This Document	4
System Requirements	5
NetIQ Advanced Authentication Framework Overview	6
About NetIQ Advanced Authentication Framework	6
NetIQ Server Appliance Functionality	6
Architecture	7
Basic Architecture	7
Enterprise Architecture	8
Enterprise Architecture with Load Balancer	9
Terms	10
Authentication Method	10
Authentication Chain	10
Authentication Event	11
NetIQ Server Appliance Deployment	12
Installing NetIQ Server Appliance	13
Graphic Mode	13
Text Mode	15
Configuration Console	18
Configuring Appliance Networking	19
Configuring Time and NTP Servers	22
Rebooting Appliance	25
Shutting Down Appliance	26
Setting up NetIQ Server Appliance Mode	27
DB Master	28
DB Slave	32
Member	36
First Login To NetIQ Admin Interface	39
Configuring NetIQ Server Appliance	41
Adding Repository	42
Configuring Method	43
Creating Chain	44
Configuring Event	45
Configuring Policy	46
Configuring Log Forwarding	47
Configuring Server Options	50
Adding License	51
Default Ports for NetIQ Server Appliance	52
Troubleshooting	53
Partition Disks	54
Networking Is Not Configured	55

Index	56
--------------------	-----------

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
- 2 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](#)

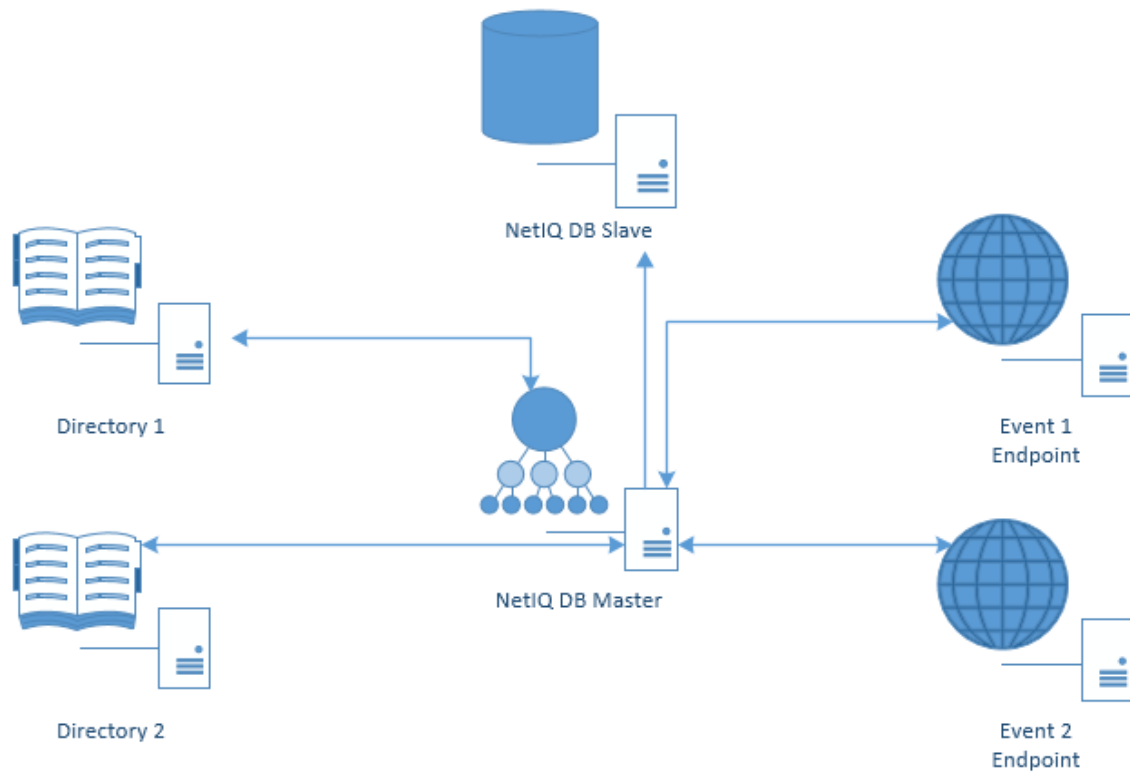
Basic Architecture

This diagram shows the basic architecture with 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.



Enterprise Architecture

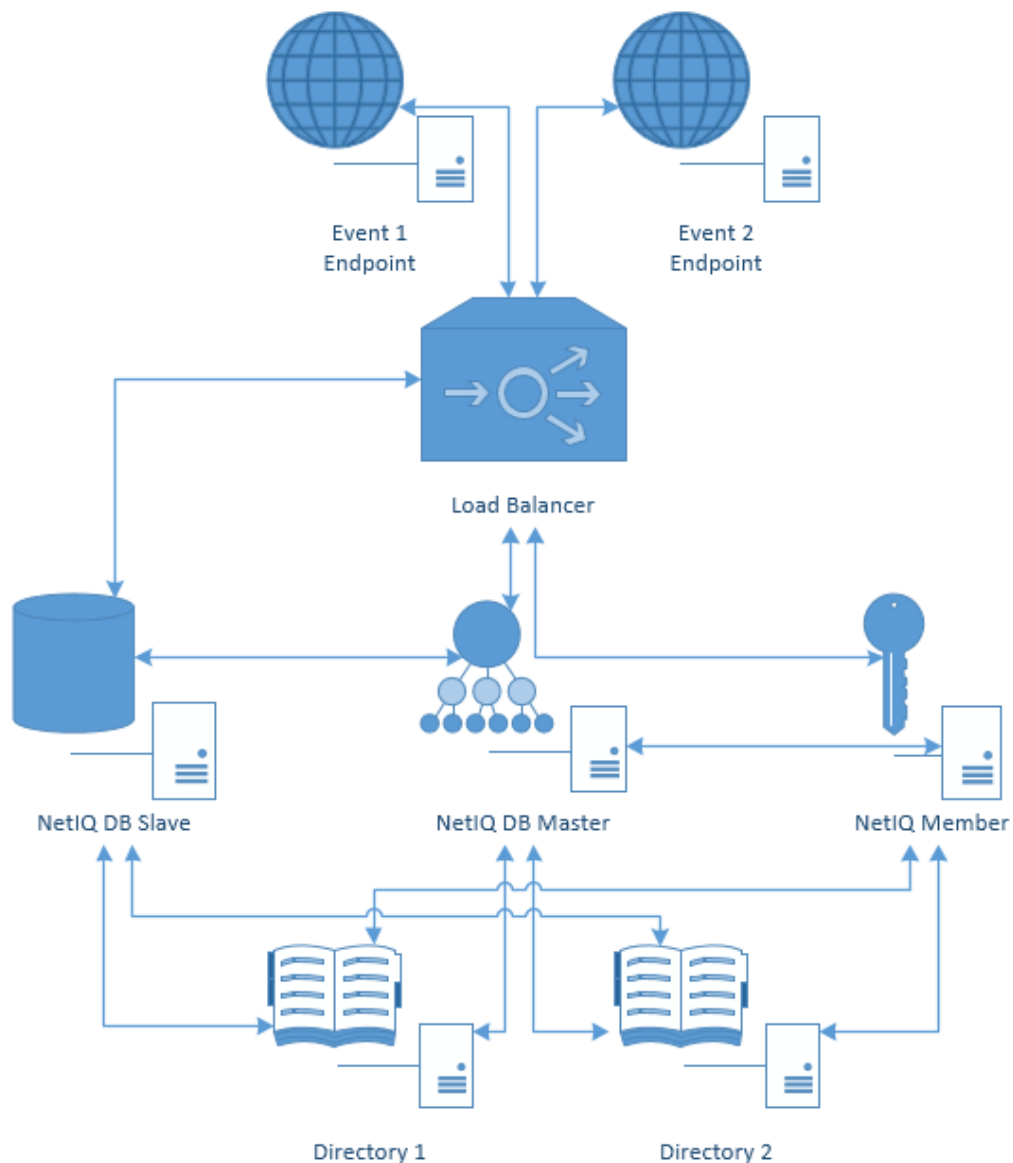
The following diagram shows interaction between DB Master, several directories and events. DB Master interacts at the same time with DB Slave, which contains the copy of the DB Master database. If DB Master dies, DB Slave will take over (hot slave).



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](#)

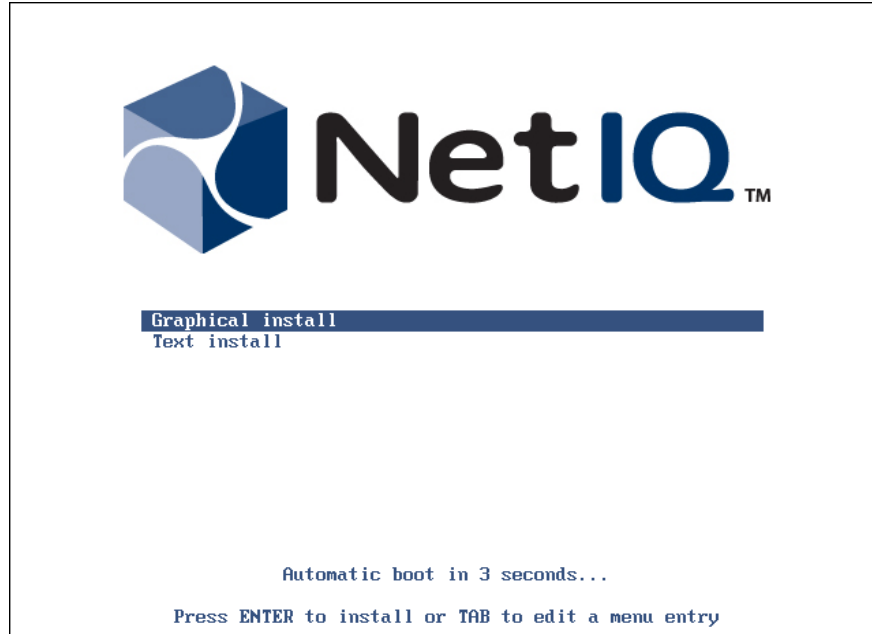
Graphic Mode

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

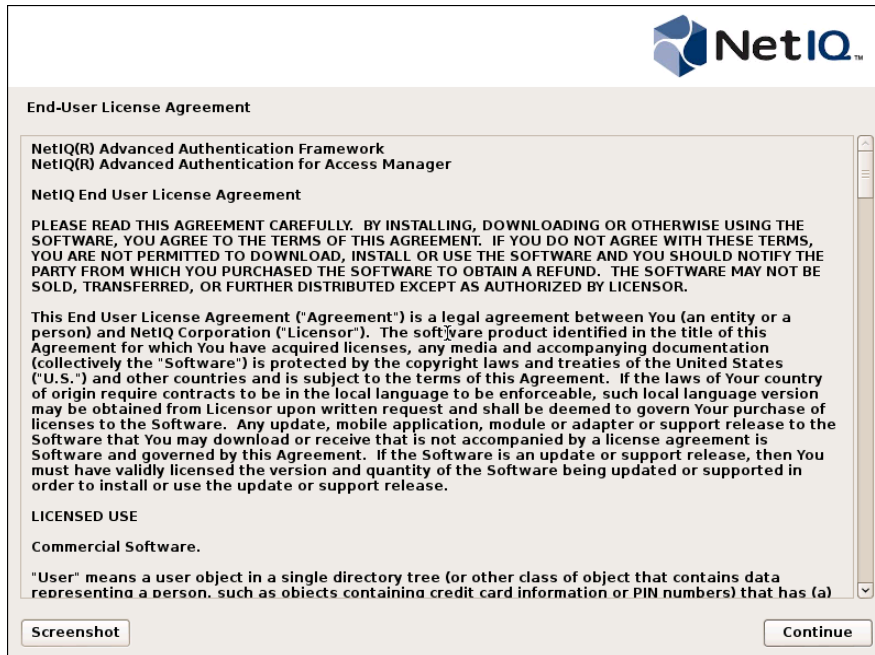
 To cancel the installation, click the **Cancel** button. The button is available only for certain processes of installation.

To install NetIQ Server appliance in the graphic mode:

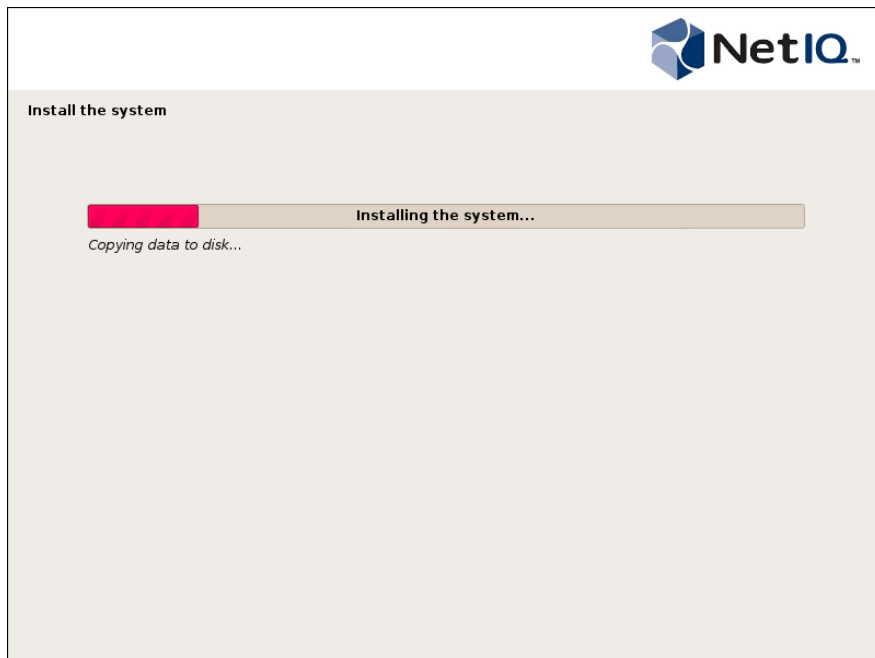
1. Select the **Graphical install** menu entry in the Setup Wizard and press **ENTER**.



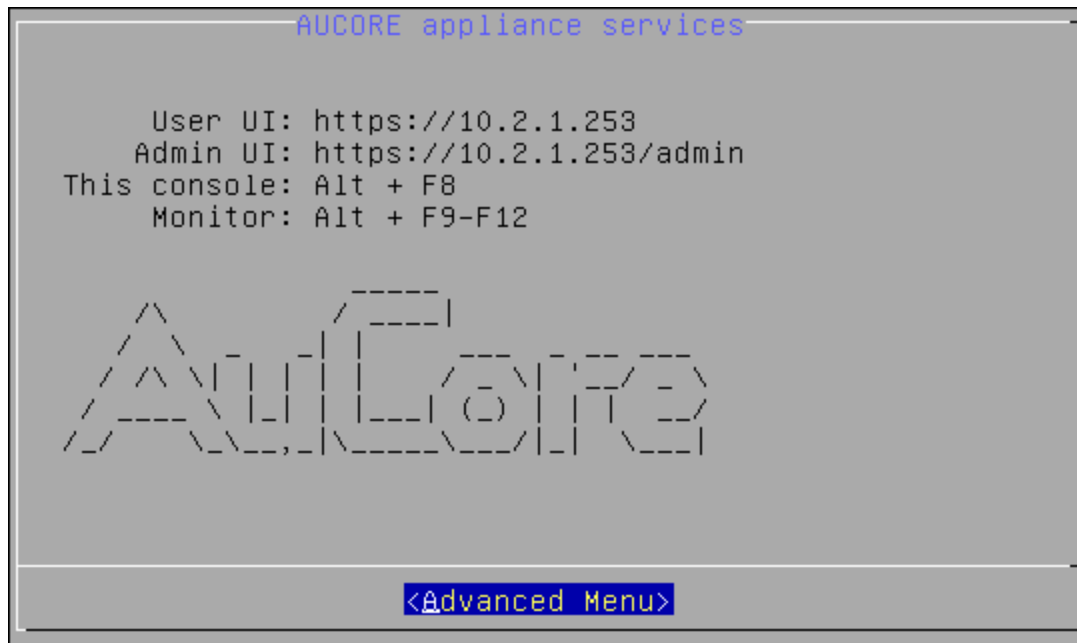
2. Read the license agreement. Select **I agree** at the bottom and click **Continue**.




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.

<Continue>

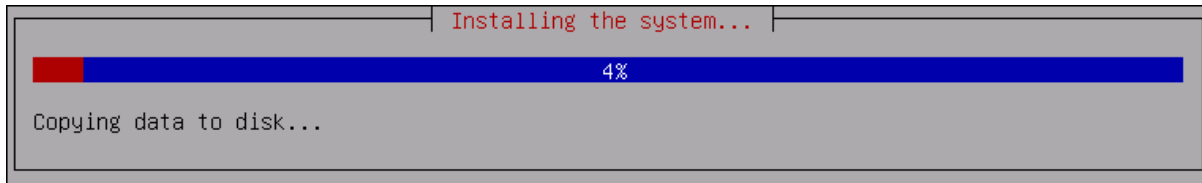
2. Select **I agree** to continue installation.

[!!] End-User License Agreement

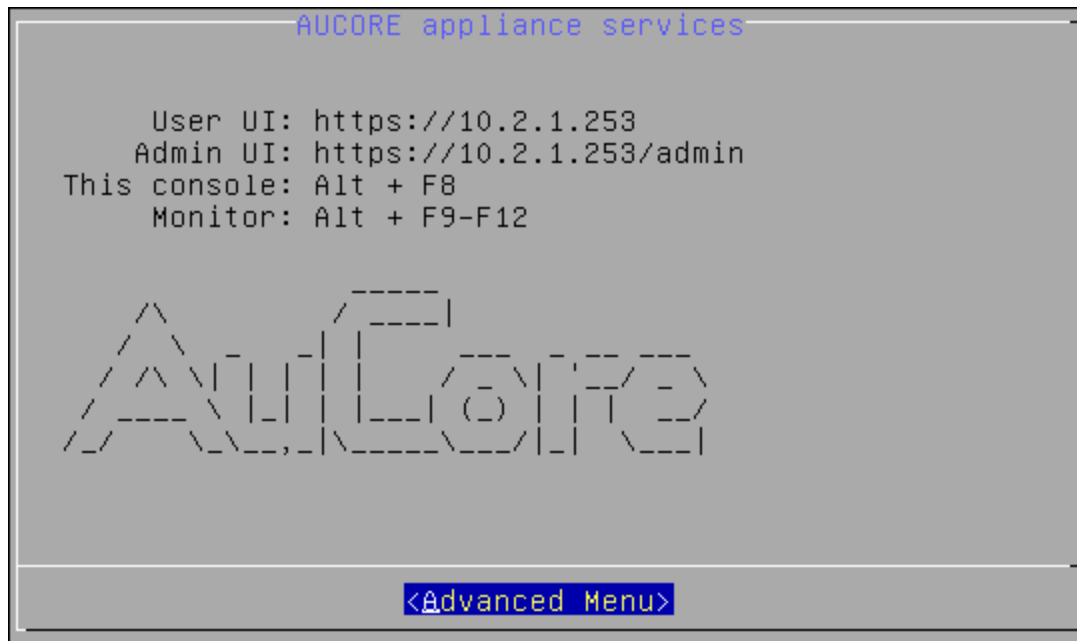
I agree
I don't agree

<Go Back>

3. The installation will be automatically started.



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

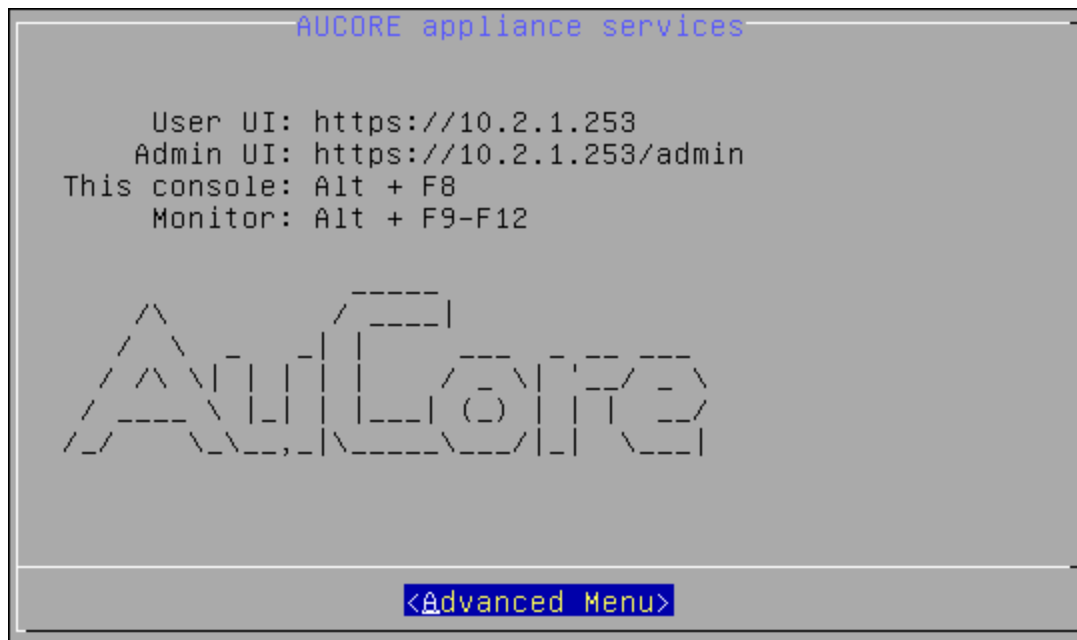


Configuration Console

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.

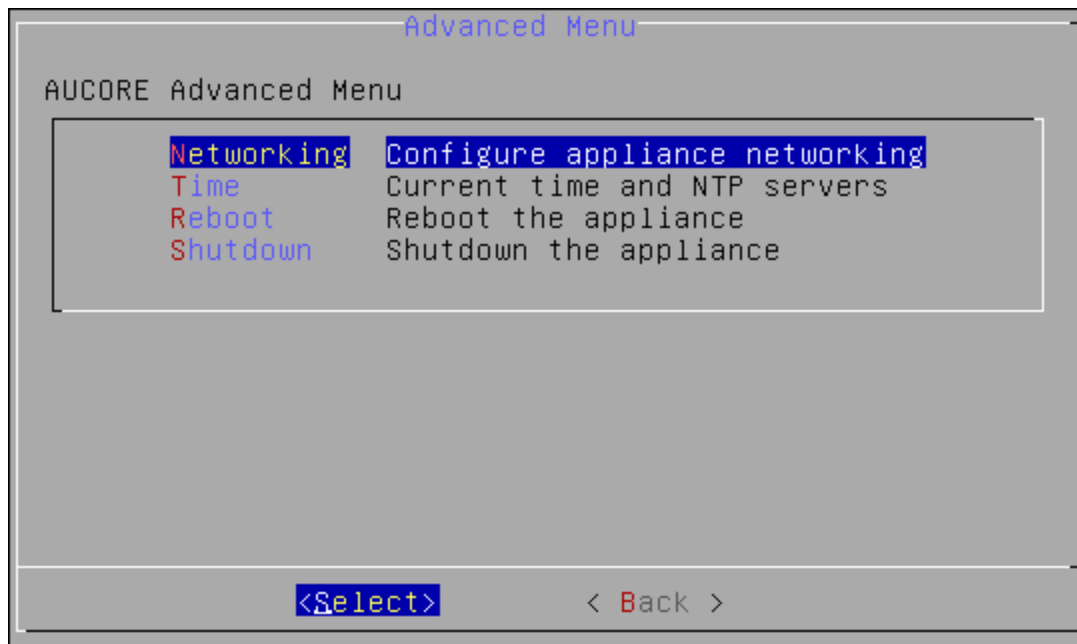


To proceed to NetIQ Server appliance management, select **Advanced Menu**.

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)

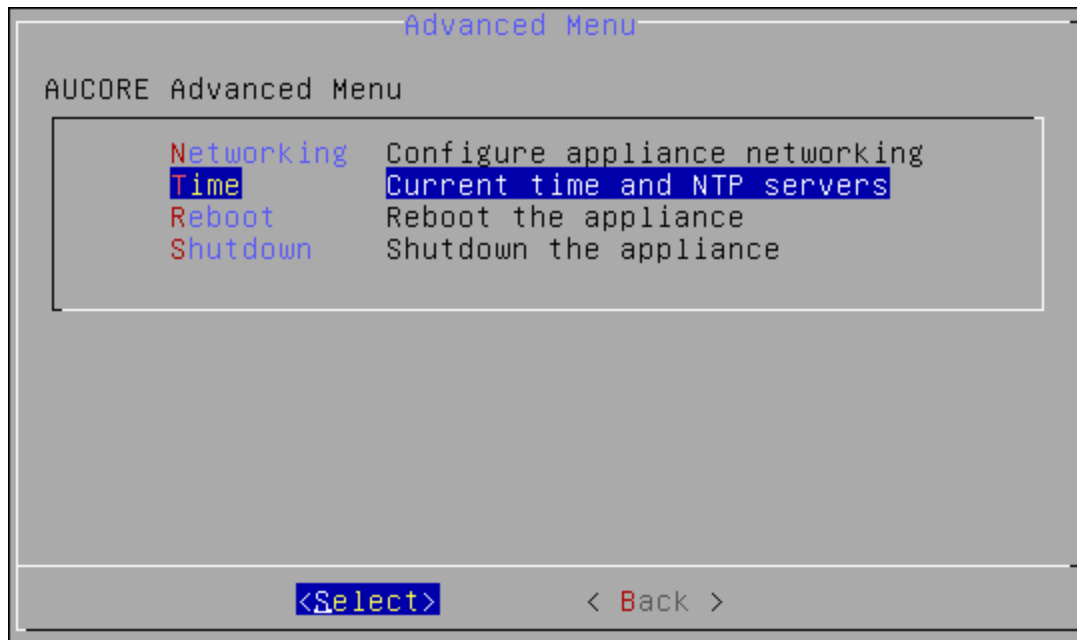
IP Address	10.2.0.208
Netmask	255.255.254.0
Default Gateway	10.2.0.100
Name Server	10.2.0.254
Name Server	10.2.0.4
Name Server	

<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:

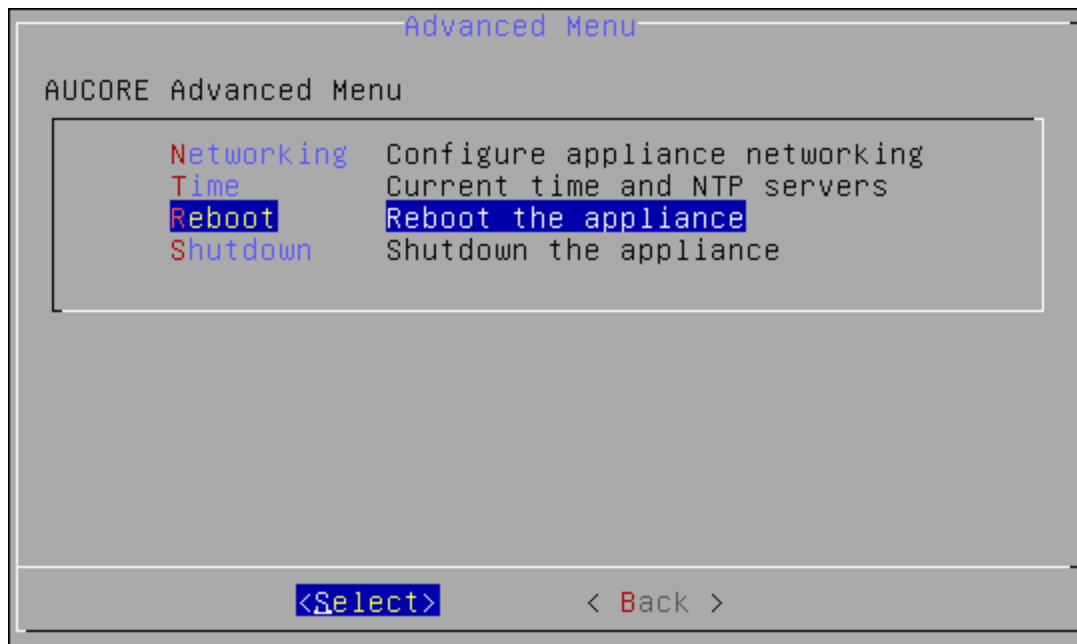
Server 1:	0.debian.pool.ntp.org	iburst
Server 2:	1.debian.pool.ntp.org	iburst
Server 3:	2.debian.pool.ntp.org	iburst
Server 4:	3.debian.pool.ntp.org	iburst

<Apply > <Cancel>

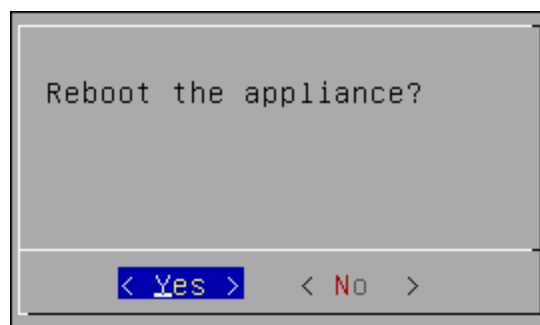
Rebooting Appliance

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

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



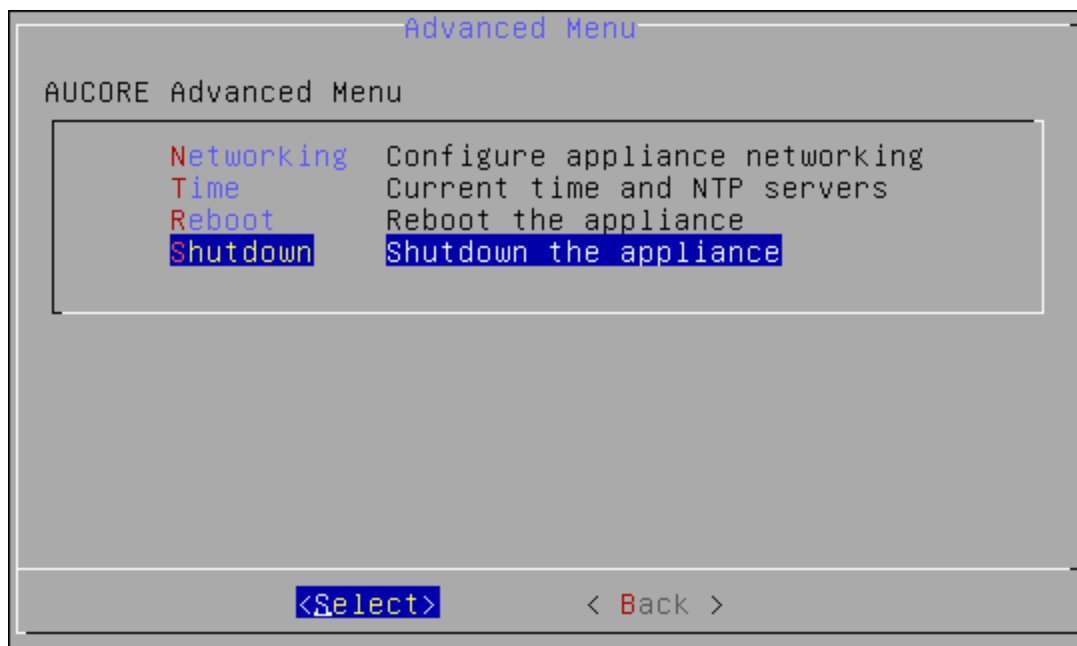
3. The confirmation message will be displayed. Select **Yes** to continue.



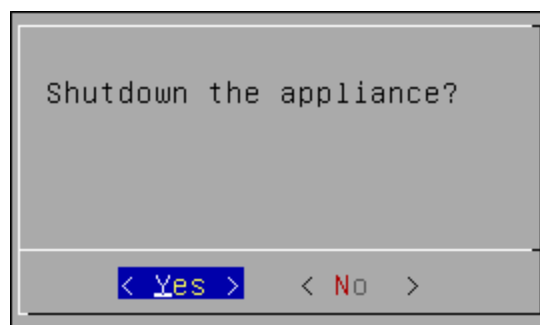
Shutting Down Appliance

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 of the NetIQ Admin Interface. On the left is a dark sidebar with a menu containing: 'Mode' (selected), 'DNS hostname', 'Password', 'Import DB Info', 'Create key', 'Copy DB', and 'Finish'. The main content area is titled 'Server Mode' and contains the following text:

Welcome to the NetIQ Advanced Authentication Framework. Before you can start using strong authentication, you must first configure this appliance.

The NetIQ Advanced Authentication Framework supports three types of database configurations on each server in the Authentication farm:

1. DB Master: The database to which all other servers connect. Only one master database is allowed within the farm.
2. DB Slave: The database used for backup and failover. Only one slave database is allowed within the farm. When the DB Master is unavailable, the DB Slave node responds to database-requests. When the DB Master becomes available again, the DB Slave node synchronizes with the DB Master and the DB Master becomes the primary point of contact for database requests again.
3. Member: Servers without database. A member server responds to authentication requests and connects to the master database service.

A server is also called an Authenticore server. Please select which type of server you want to install.

If this is your first Authenticore server, use DB Master. If this is your second Authenticore server, use DB Slave. If you already have a DB-Master and DB-Slave installed, use the Member server configuration.

Below the text are three selectable options, each with a button and a description:

- DB Master** (blue button): Server with master DB. All other servers will connect to this DB
- DB Slave** (light blue button): If master dies, this DB will take over (hot slave)
- Member** (light blue button): Server with no DB. There can be many farm members but 1 pair of master-slave only

A 'Next' button with a right arrow is located below these options.

At the bottom of the screen, the footer contains: 'Copyright © 2015 NetIQ. All rights reserved.' on the left and 'build: NAAF-5.1.3-187' on the right.

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

Install

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

DNS hostname

This configuration parameter provides the hostname of this server, as configured in DNS.

The hostname configured here is published to all Authenticore servers as the point of contact for this server. Ensure that all other Authenticore servers in this farm have the appropriate name configured in their respective DNS servers so that they can resolve this name.

It is recommended you provide both an address record (A) for this server, and a reverse lookup record (PTR).

Use the FQDN (Fully Qualified Domain Name) of this server in the client configuration of the clients of the radius server; therefore, it is important to have a properly functioning DNS infrastructure.

The FQDN you enter here is checked by doing a reverse lookup at the DNS server.

My DNS hostname

10.2.0.171

Back

Next

Copyright © 2015 NetIQ. All rights reserved.

build: NAAF-5.1.3-187

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

Install

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Password of LOCAL\admin user

Please set the password for the local admin account. This account is used to access to the Admin console of the NetIQ Advanced Authentication Framework. It can be entered at the admin login to administer this server.

It is possible to configure administrative access based on external repositories, such as a corporate Active Directory. In this case the local admin user can be removed from the global admin group once this is correctly configured.

Please note the username syntax for logging on to the admin interface is LOCAL\admin.

Password

Confirmation

Back

Next

Copyright © 2015 NetIQ. All rights reserved.

build: NAAF-5.1.3-187

© NetIQ

29

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

The screenshot shows the 'Install' window of the NetIQ Authenticore installation wizard. The left sidebar contains a list of steps: Mode, DNS hostname, Password, Import DB Info, **Create key** (highlighted), Copy DB, and Finish. The main content area is titled 'Create encryption key' and contains the following text:

The Authenticore server uses a shared key to encrypt the database and inter-server transactions. This shared key is created during the installation of the first (Master-DB) server. When installing an extra server it will receive the key from the first server so all encryption is the same.

Here you must generate an encryption key which will be used to encrypt sensitive data in the local database.

To generate the key, click Create before you click Next.

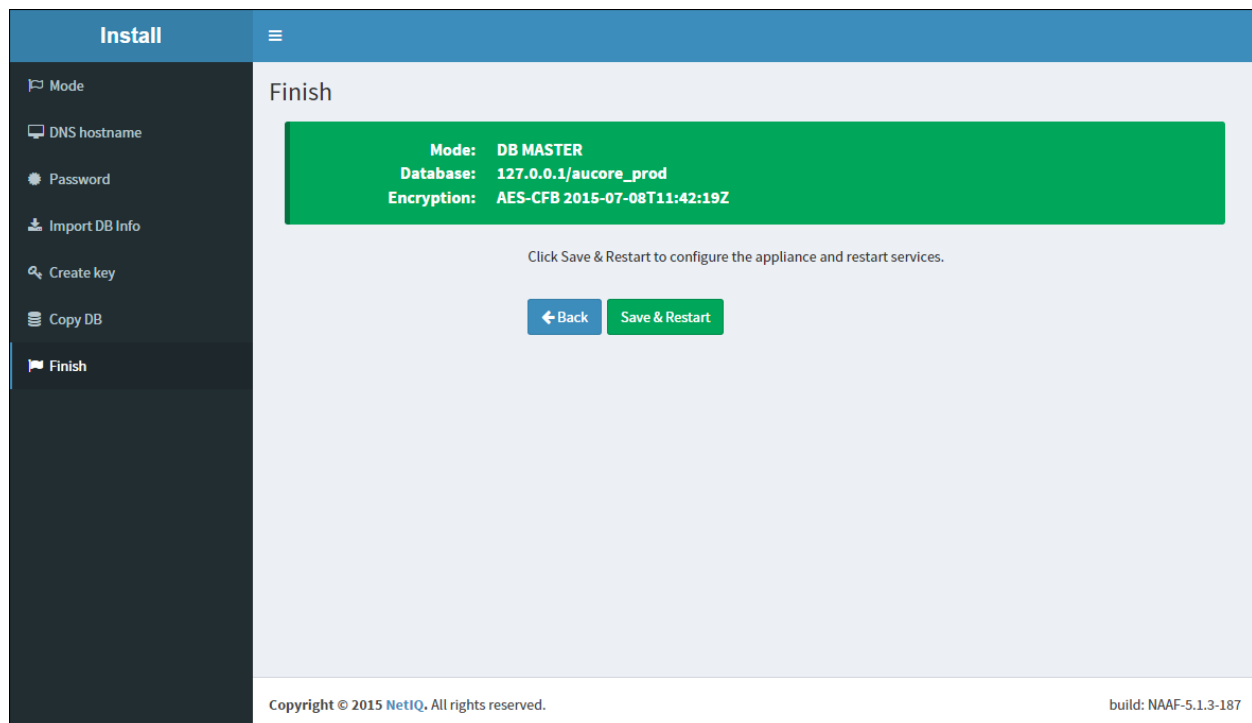
Below the text, the 'Current key' is displayed as 'AES-CFB 2015-07-08T11:36:40Z'. There are three buttons: a green 'Create' button, a blue '← Back' button, and a blue 'Next →' button.

At the bottom of the window, the copyright notice 'Copyright © 2015 NetIQ. All rights reserved.' and the build number 'build: NAAF-5.1.3-187' are visible.

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

This screenshot is identical to the previous one, showing the 'Create encryption key' step. The only difference is the 'Current key' value, which is now 'AES-CFB 2015-07-08T11:42:19Z', indicating that the key has been successfully generated. The 'Create' button remains visible, and the 'Next →' button is now the primary action for the user to proceed.

- 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.

Install

Mode

- DNS hostname
- Password
- Import DB Info
- Create key
- Copy DB
- Finish

Server Mode

Welcome to the NetIQ Advanced Authentication Framework. Before you can start using strong authentication, you must first configure this appliance.

The NetIQ Advanced Authentication Framework supports three types of database configurations on each server in the Authentication farm:

1. DB Master: The database to which all other servers connect. Only one master database is allowed within the farm.
2. DB Slave: The database used for backup and failover. Only one slave database is allowed within the farm. When the DB Master is unavailable, the DB Slave node responds to database-requests. When the DB Master becomes available again, the DB Slave node synchronizes with the DB Master and the DB Master becomes the primary point of contact for database requests again.
3. Member: Servers without database. A member server responds to authentication requests and connects to the master database service.

A server is also called an Authenticore server. Please select which type of server you want to install.

If this is your first Authenticore server, use DB Master. If this is your second Authenticore server, use DB Slave. If you already have a DB-Master and DB-Slave installed, use the Member server configuration.

DB Master	Server with master DB. All other servers will connect to this DB
DB Slave	If master dies, this DB will take over (hot slave)
Member	Server with no DB. There can be many farm members but 1 pair of master-slave only

Next →

Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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

Install

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

DNS hostname

This configuration parameter provides the hostname of this server, as configured in DNS.

The hostname configured here is published to all Authenticore servers as the point of contact for this server. Ensure that all other Authenticore servers in this farm have the appropriate name configured in their respective DNS servers so that they can resolve this name.

It is recommended you provide both an address record (A) for this server, and a reverse lookup record (PTR).

Use the FQDN (Fully Qualified Domain Name) of this server in the client configuration of the clients of the radius server; therefore, it is important to have a properly functioning DNS infrastructure.

The FQDN you enter here is checked by doing a reverse lookup at the DNS server.

My DNS hostname

10.2.0.190

Back

Next

Copyright © 2015 NetIQ. All rights reserved.

build: NAAF-5.1.3-187

- 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.

NetIQ

Info

Repositories

Methods

Chains

Events

Policies

Server Options

Farm servers

Licenses

Updates

Logs

Farm servers

Home > Farm servers

Replication

Server mode: DB MASTER

Replication: stopped

Not configured

Install DB SLAVE

Use this tool to add slave server as follows:

- Run installation of slave
- When you are on "Import database information" step, go here, enter slave hostname and press the button

Slave host

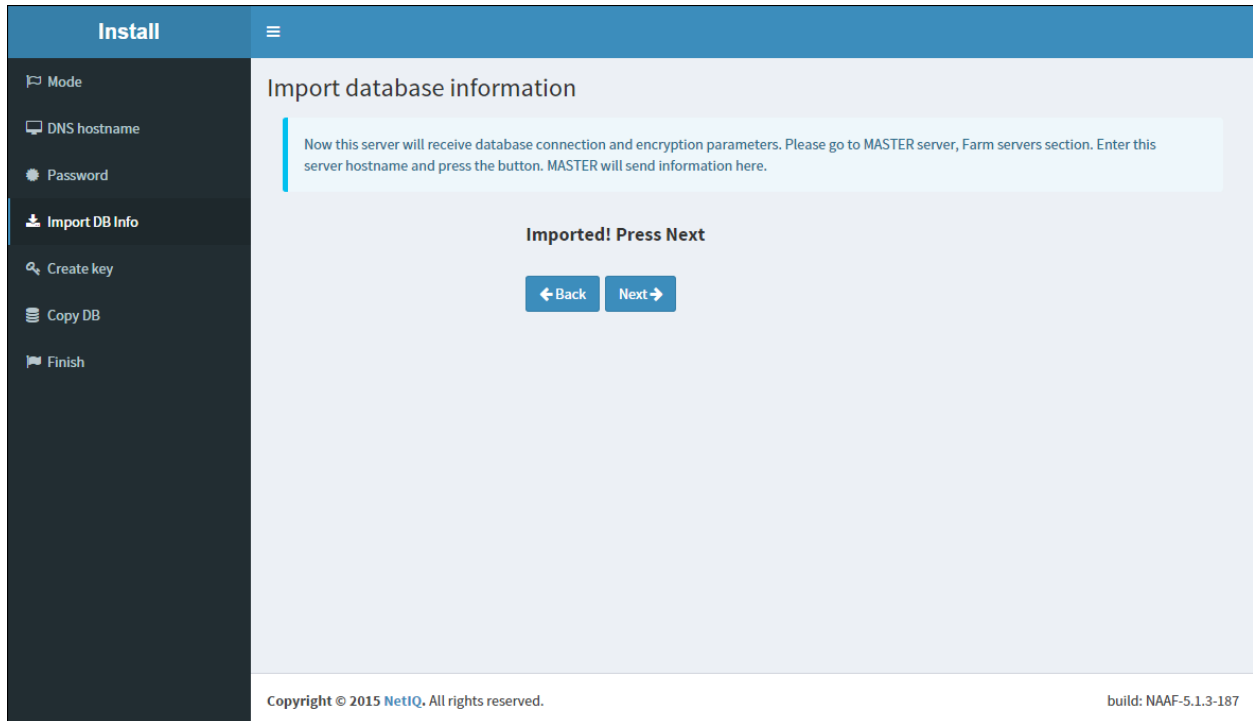
10.2.0.190

Register slave

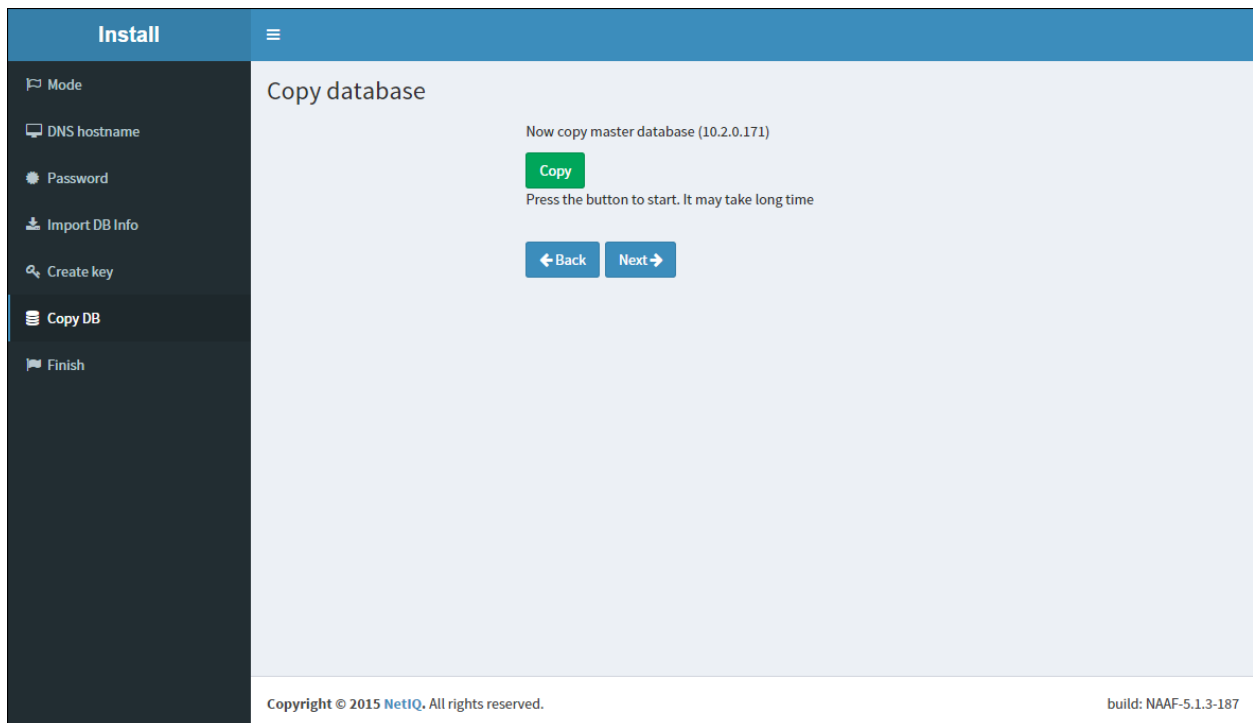
Install new MEMBER server

Use this tool to add new member server as follows:

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

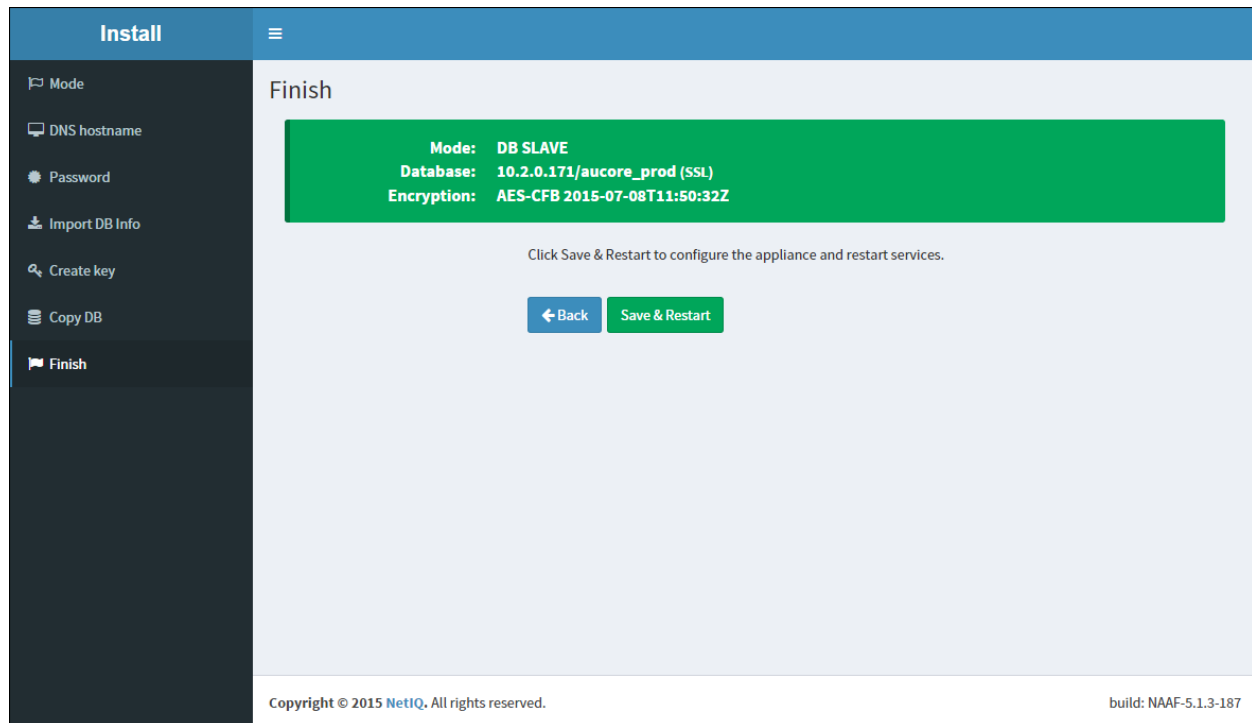





5. Click the **Copy** button to copy master database.



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.

Install

Mode

DNS hostname

Password

Import DB Info

Create key

Copy DB

Finish

Server Mode

Welcome to the NetIQ Advanced Authentication Framework. Before you can start using strong authentication, you must first configure this appliance.

The NetIQ Advanced Authentication Framework supports three types of database configurations on each server in the Authentication farm:

1. DB Master: The database to which all other servers connect. Only one master database is allowed within the farm.
2. DB Slave: The database used for backup and failover. Only one slave database is allowed within the farm. When the DB Master is unavailable, the DB Slave node responds to database-requests. When the DB Master becomes available again, the DB Slave node synchronizes with the DB Master and the DB Master becomes the primary point of contact for database requests again.
3. Member: Servers without database. A member server responds to authentication requests and connects to the master database service.

A server is also called an Authenticore server. Please select which type of server you want to install.

If this is your first Authenticore server, use DB Master. If this is your second Authenticore server, use DB Slave. If you already have a DB-Master and DB-Slave installed, use the Member server configuration.

DB Master	Server with master DB. All other servers will connect to this DB
DB Slave	If master dies, this DB will take over (hot slave)
Member	Server with no DB. There can be many farm members but 1 pair of master-slave only

Next →

Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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.

NetIQ

Info

Repositories

Methods

Chains

Events

Policies

Server Options

Farm servers

Licenses

Updates

Logs

Farm servers

Replication

Server mode:

DB MASTER paired with 10.2.0.190

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 host

10.2.1.248

Export database info

This server uses DB at 127.0.0.1

DB Master connects to localhost always. DB Slave and MEMBERS connect to DB Master under normal conditions. They connect to DB Slave when MASTER is not accessible.

MASTER

10.2.0.171

SLAVE

10.2.0.190

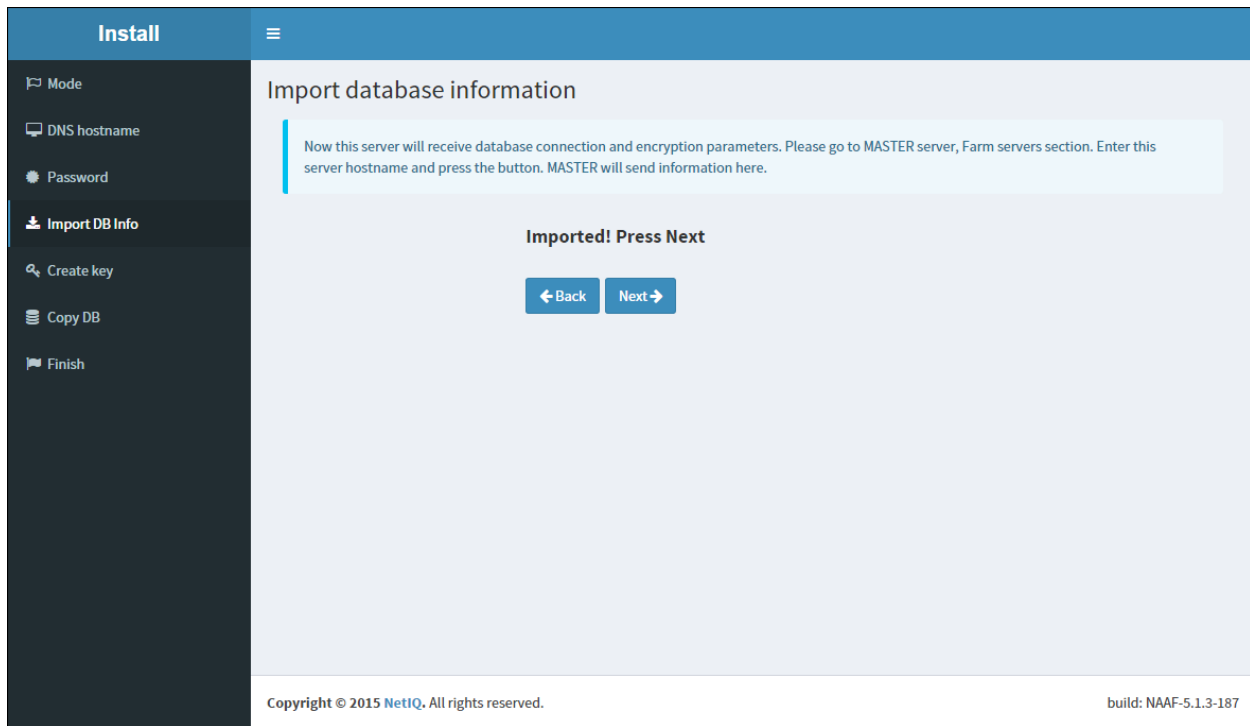
Copyright © 2015 NetIQ. All rights reserved.

build: NAAF-5.1.3-187

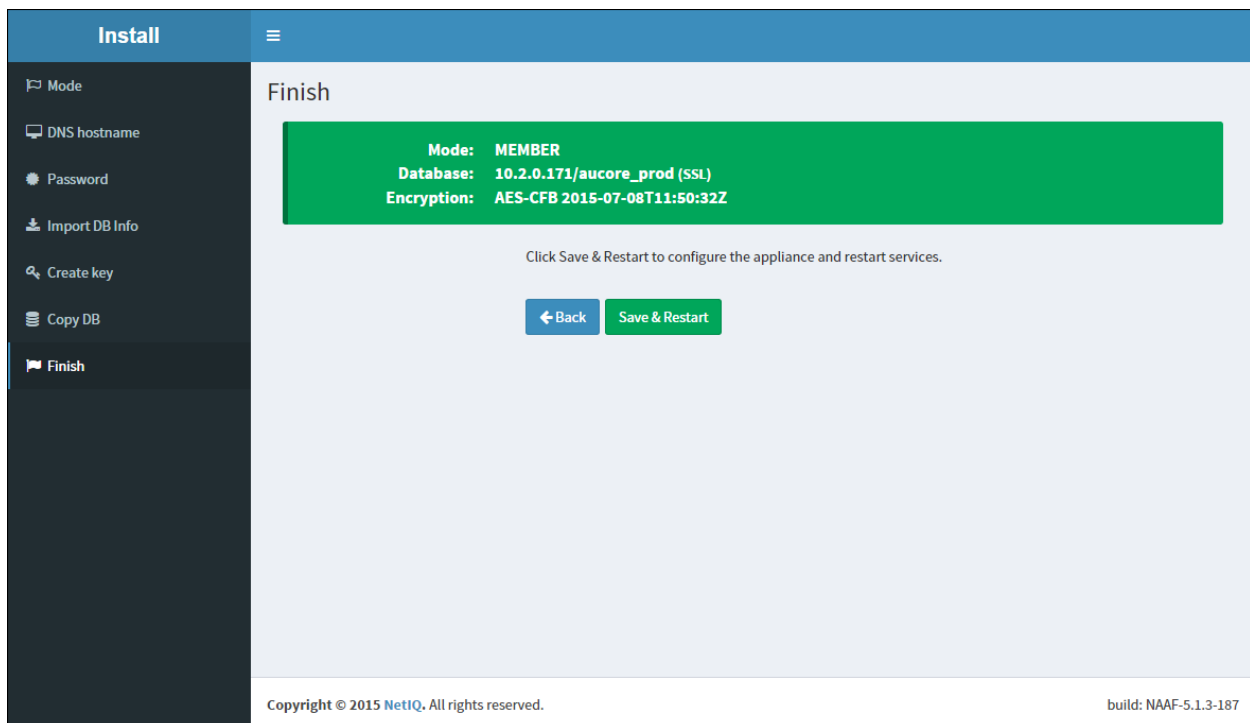
The Member server starts copying database information from the DB Master server. Once the database information is imported, click **Next** to continue.

© NetIQ

37



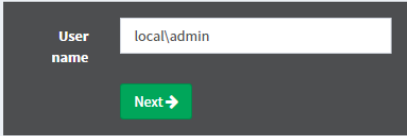
4. Click the **Save & Restart** button to write configuration and restart services. Services will be restarted within 30 seconds.



First Login To NetIQ Admin Interface

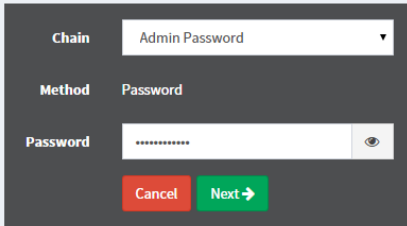
After setting up an applicable server mode, the NetIQ Admin Interface is displayed. To log in to NetIQ Admin Interface, follow the steps:

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



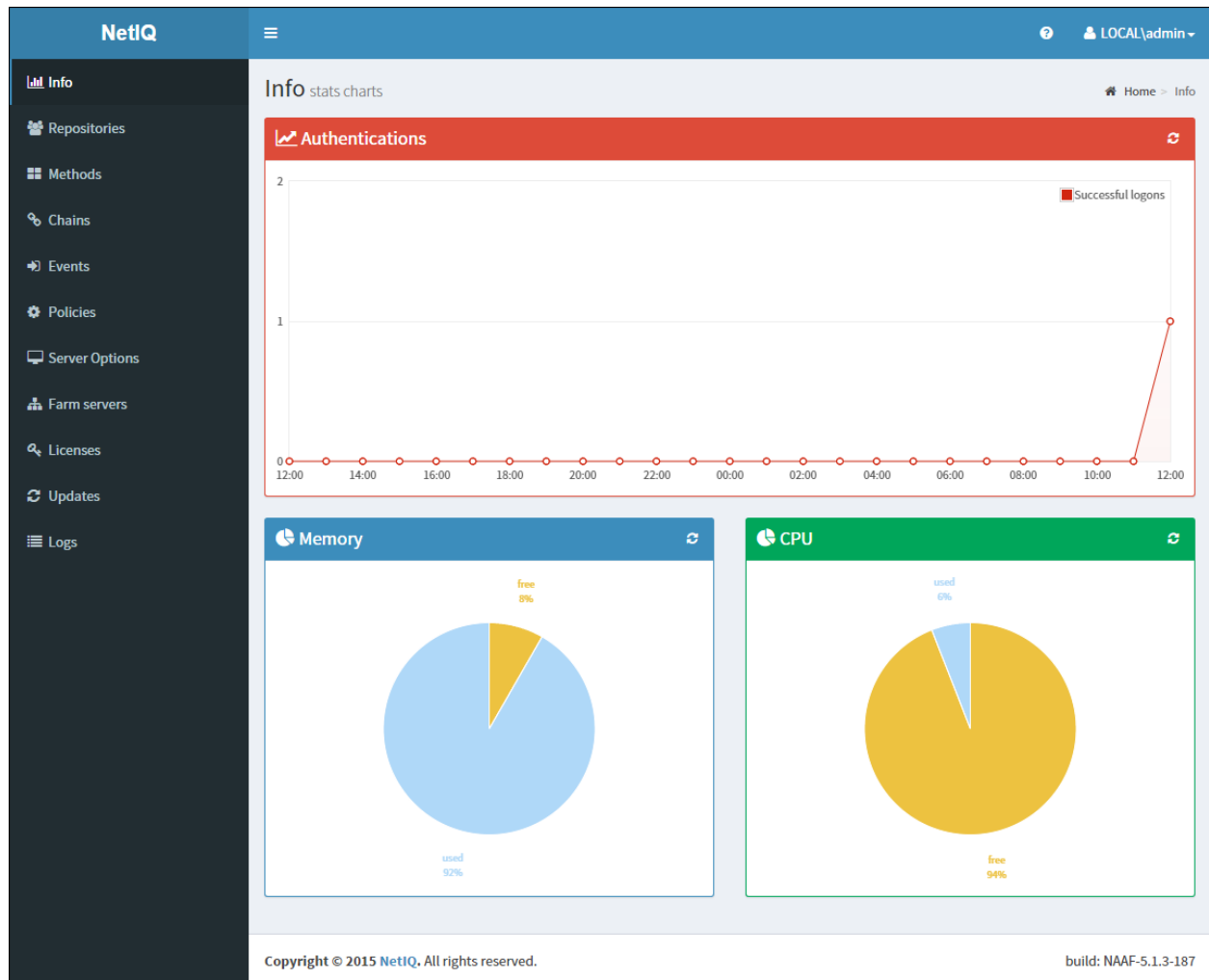
The screenshot shows a login dialog box with a dark gray background. On the left, the text "User name" is displayed. To its right is a white text input field containing the text "local\admin". Below the input field is a green button with the text "Next" and a right-pointing arrow.

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.



The screenshot shows a login dialog box with a dark gray background. It contains three labeled fields: "Chain" with a dropdown menu showing "Admin Password", "Method" with a dropdown menu showing "Password", and "Password" with a white text input field containing eight asterisks. To the right of the password field is an eye icon. At the bottom of the dialog are two buttons: a red "Cancel" button and a green "Next" button with a right-pointing arrow.

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. [Configure log forwarding](#)
7. [Specify an applicable protocol](#)
8. [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 Repository Add

Home > Repositories > Repository Add

Name: REPO

Base DN: dc=authasas, dc=local

User: cn=administrator, cn=users, dc=authasas, dc=local

Password: [masked]

Confirmation: [masked]

LDAP type: AD

LDAP servers

Address	Port	SSL
10.2.1.35	389	<input checked="" type="checkbox"/>

Advanced settings

Save Cancel

Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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.

The screenshot shows the NetIQ web interface for editing method settings. The left sidebar contains navigation links: Info, Repositories, Methods (selected), Chains, Events, Policies, Server Options, Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Method Settings Edit' and includes a breadcrumb trail: Home > Methods > Method Settings Edit. The settings are organized into sections: 'Security questions' with input fields for 'Min. answer length' (1), 'Correct questions for login' (5), and 'Total questions for login' (5); and 'Questions' which lists five sample questions, each with an edit icon and a delete icon. An 'Add' button is located at the top right of the questions list. At the bottom of the settings area are 'Save' and 'Cancel' buttons. The footer contains the copyright notice 'Copyright © 2015 NetIQ. All rights reserved.' and the build number 'build: NAAF-5.1.3-187'.

NetIQ

Method Settings Edit

Home > Methods > Method Settings Edit

Security questions

Min. answer length: 1

Correct questions for login: 5

Total questions for login: 5

Questions

Add

Question

What was the make and model of your first car?

What was the name of your elementary/primary school?

In what country were you born?


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

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

Save Cancel

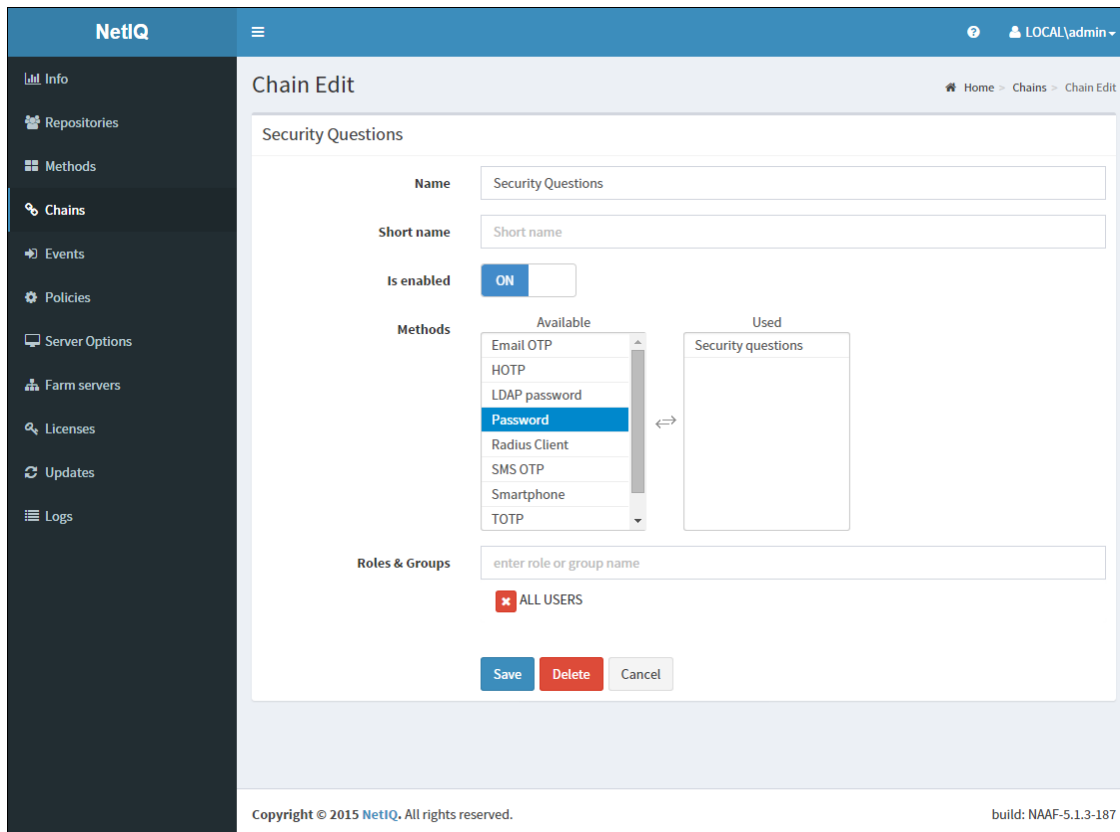
Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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 NetIQ Chain Edit interface. The left sidebar contains a navigation menu with options: Info, Repositories, Methods, Chains (selected), Events, Policies, Server Options, Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Chain Edit' and shows the configuration for a chain named 'Security Questions'. The 'Name' field is 'Security Questions' and the 'Short name' field is 'Short name'. The 'Is enabled' toggle is set to 'ON'. The 'Methods' section shows a list of available methods: Email OTP, HOTP, LDAP password, Password (selected), Radius Client, SMS OTP, Smartphone, and TOTP. A double-headed arrow indicates the selection of 'Password' for the 'Used' section, which currently contains 'Security questions'. The 'Roles & Groups' section has a text input field with 'enter role or group name' and a red asterisk icon next to 'ALL USERS'. At the bottom, there are 'Save', 'Delete', and 'Cancel' buttons. The footer shows 'Copyright © 2015 NetIQ. All rights reserved.' and 'build: NAAF-5.1.3-187'.

Configuring Event

- * The supported events are RADIUS Server, NAM and NCA.
- * Currently the built-in RADIUS Server supports only PAP.

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 interface for the Radius Server event. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation links: Info, Repositories, Methods, Chains, Events (selected), Policies, Server Options, Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Event Edit' and shows the 'Radius Server' event configuration. It includes an 'Is enabled' toggle set to 'ON', a 'Chains' section with 'Available' and 'Used' lists, and a 'Clients' section with a table for adding clients. The 'Available' list includes Admin Password, Authenticators, Management logon, LDAP password, Authenticators, Management logon, Password, and Counter based one time password. The 'Used' list includes Password & TOTP, Password & HOTP, Password & SMS OTP, Password & Smartphone Out-of-Band, and Password & Voicecall. The 'Clients' table has columns for Name, IP address, Username, Password, and Enabled status. A 'Save' button is at the bottom.

NetIQ

Event Edit

Home > Events > Event Edit

Radius Server

Is enabled ☒

Chains

Available

- Admin Password
- Authenticators
- Management logon
- LDAP password
- Authenticators
- Management logon
- Password
- Counter based one time password

Used

- Password & TOTP
- Password & HOTP
- Password & SMS OTP
- Password & Smartphone Out-of-Band
- Password & Voicecall

Clients


Add

Name	Enabled
Client	10.2.0.136

Save Revert to defaults Cancel

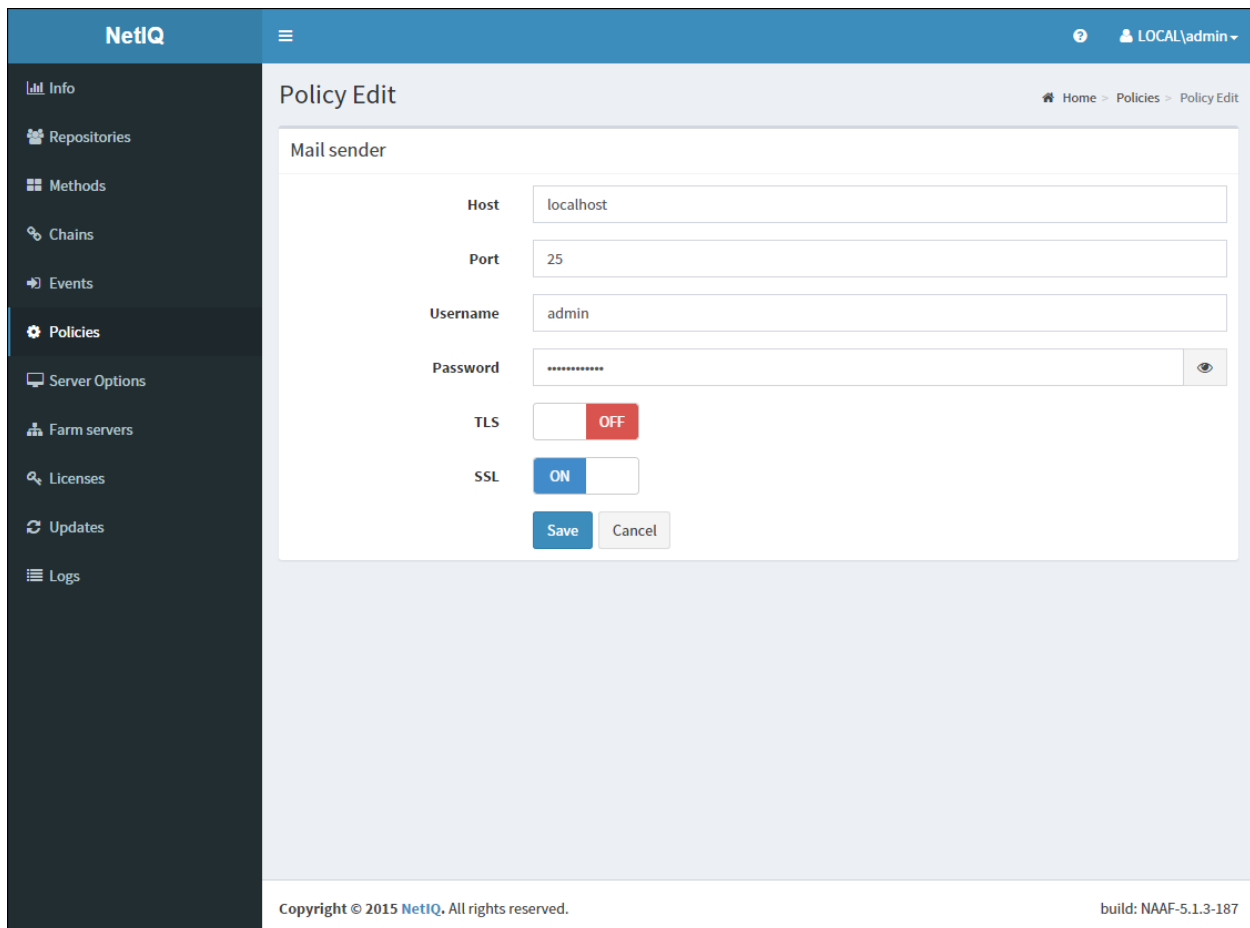
Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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 for editing a policy. The left sidebar contains a navigation menu with items: Info, Repositories, Methods, Chains, Events, Policies (highlighted), Server Options, Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Policy Edit' and includes a breadcrumb trail: Home > Policies > Policy Edit. Below the title is a 'Mail sender' section with the following fields and controls:

- Host:** Text input field containing 'localhost'.
- Port:** Text input field containing '25'.
- Username:** Text input field containing 'admin'.
- Password:** Password input field with masked characters '*****' and a toggle icon to show/hide the password.
- TLS:** A toggle switch currently set to 'OFF'.
- SSL:** A toggle switch currently set to 'ON'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom of the form.

At the bottom of the interface, the footer contains the text: 'Copyright © 2015 NetIQ. All rights reserved.' on the left and 'build: NAAF-5.1.3-187' on the right.

Configuring Log Forwarding

- ✖ Events from all facilities are recorded to syslog. E.g., aucore, kernel, daemon, etc.
- ✖ The same rsyslog configuration is used for each server type. Each server type in the appliance records its own log file.

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 screenshot shows the NetIQ web interface for editing a policy. The left sidebar contains a navigation menu with options: Info, Repositories, Methods, Chains, Events, Policies (selected), Server Options, Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Policy Edit' and shows the configuration for the 'CEF log forward' policy. The configuration includes an 'Enable' toggle set to 'ON', a 'Syslog server' text field containing 'syslog.server.ip', a 'Port' text field containing '514', and a 'Transport' dropdown menu set to 'UDP'. At the bottom of the configuration section are 'Save' and 'Cancel' buttons. The footer of the interface displays 'Copyright © 2015 NetIQ. All rights reserved.' and 'build: NAAF-5.1.3-187'.

Field	Value
Enable	ON
Syslog server	syslog.server.ip
Port	514
Transport	UDP

The following aucore 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

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), Farm servers, Licenses, Updates, and Logs. The main content area is titled 'Server Options' with a subtitle 'server specific configuration'. It contains two sections: 'Web server SSL certificate for HTTPS' and 'Login page background'. The first section has a text box with instructions to upload a certificate file (*.pem, *.cert) and an example of a PEM-formatted certificate and private key. Below this is a 'New SSL certificate' label, a 'Choose File' button (which shows 'No file chosen'), and an 'Upload' button. The second section, 'Login page background', has a text box instructing to upload a background image in JPEG or PNG format. It also features a 'New background' label, a 'Choose File' button (showing 'No file chosen'), and an 'Upload' button. At the bottom of the page, there is a copyright notice 'Copyright © 2015 NetIQ. All rights reserved.' and a build number 'build: NAAF-5.1.3-187'.

NetIQ

LOCAL\admin

Server Options server specific configuration

Home > Server Options

Web server SSL certificate for HTTPS

Upload certificate file (*.pem, *.cert). The file must contain **both** certificate and private key.

Example:

```
-----BEGIN CERTIFICATE-----
MIIDUzCCAgugAwIBAgIJAALgWVY4Sz.....
-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----
MIIEgIBADIANBgqehL09wRBAQFA.....
-----END PRIVATE KEY-----
```

New SSL certificate Choose File No file chosen

Upload

Login page background


Upload login page background image in JPEG or PNG format.

New background Choose File No file chosen

Upload

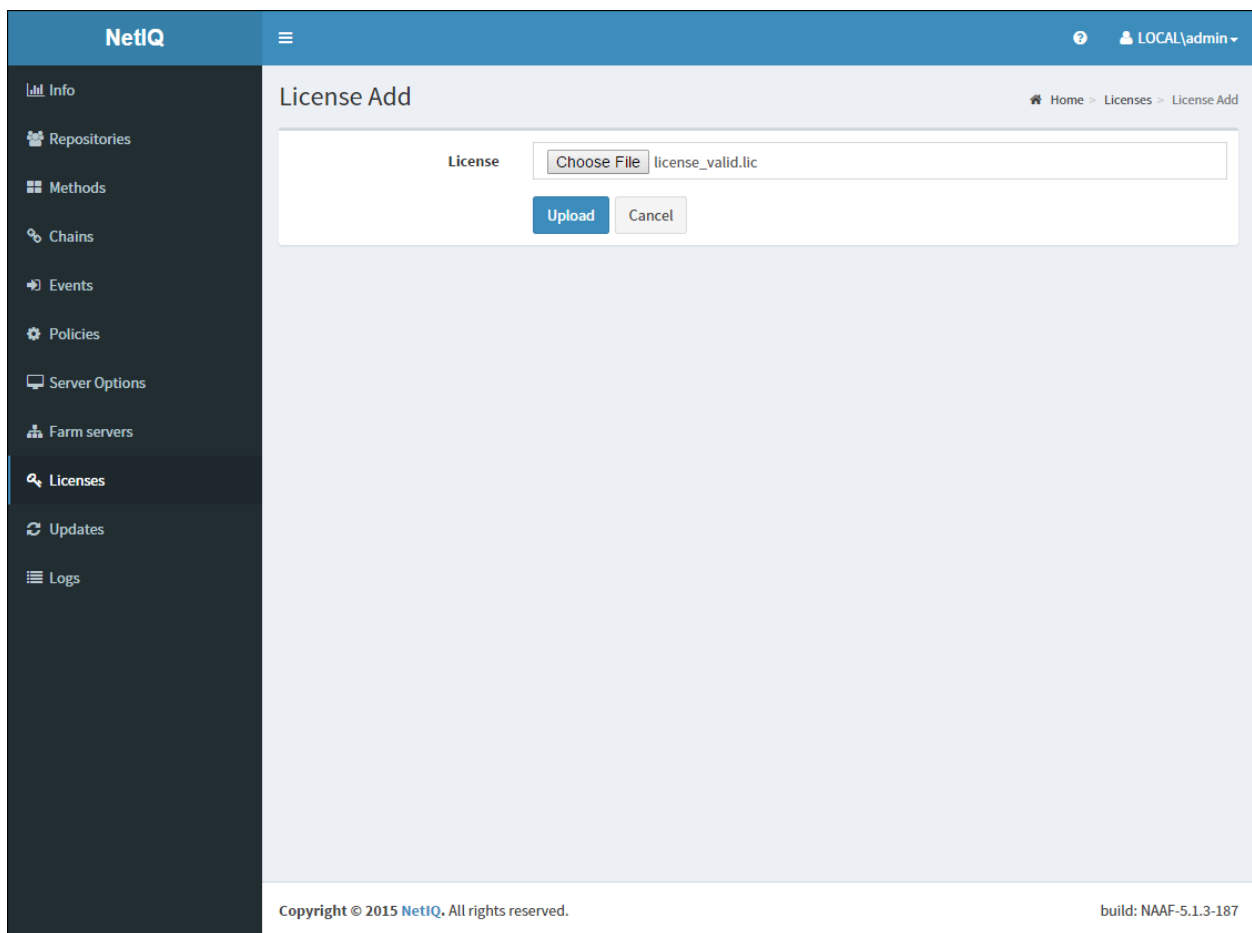
Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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.



NetIQ

LOCAL\admin

License Add

Home > Licenses > License Add

License

Choose File license_valid.lic

Upload Cancel

Copyright © 2015 NetIQ. All rights reserved. build: NAAF-5.1.3-187

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

- * 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.

Troubleshooting

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

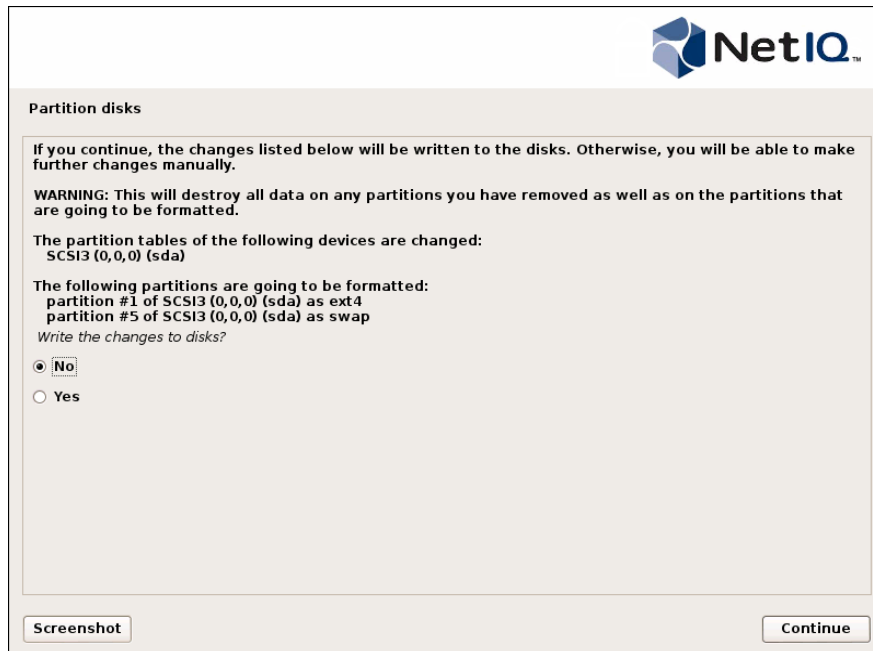
In this chapter:

- [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.

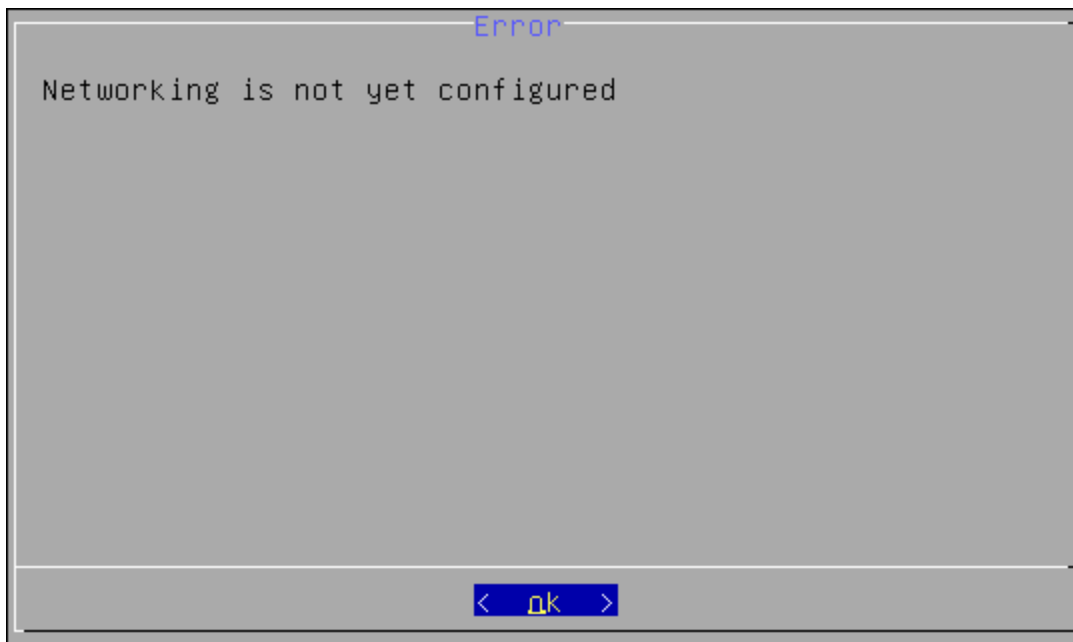
Solution:

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, 4-7, 10-11, 52
Authenticator 4

C

Console 5, 12, 14, 17-19, 22, 25-26, 55
Create 30, 41

D

Default 52

E

Edit 43-47
Enroll 52
Export 36

F

File 50-51

L

License 51
Local 48
Logon 4

M

Menu 18-19, 22, 25-26

P

Password 39, 42
PIN 10
Policy 46
Protocol 52

R

RADIUS 6-7, 11, 45, 52

S

Server 4, 6, 12-13, 15, 18-19, 25-28, 32, 36, 41, 45, 48, 50, 52, 54-55

System 5

T

Template 48

U

User 10, 18, 42, 48