NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

© NetIQ

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.

ℹ 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.

NetIQ Advanced Authentication Framework Overview

In this chapter:

About NetIQ Advanced Authentication Framework

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

Why choose NetIQ Advanced Authentication Framework™?

NetIQ Advanced Authentication Framework™...

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

NetIQ Server Appliance Functionality

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

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

Terms

In this chapter:

Authenticator

Authenticator is data submitted by a user for the purpose of his/her personality validation. Both common character strings (e.g. symbolic password) and data received from a hardware authentication device (e.g. digital fingerprint model, memory card ID) can appear as an authenticator. Two authenticator types are usually distinguished: reference authenticator and current authenticator.

Reference authenticator is data submitted by a user to the system as a part of registration procedure, while current authenticator - a part of authentication procedure. Particular characteristics of these data depend on the authentication method selected by the user, such as password, or digital fingerprint model, or memory card ID, etc. A successful logon is performed only when the reference and current authenticators match.

Authentication Chain

Authentication Chain is a configured authentication process in which a user must pass credentials to all module instances defined in it. It means that authentication chain processes requests and applies several authentication methods. Authentication chains are configured only when a single set of credentials is not sufficient.

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.

Event

Event is the authentication moment or application where the framework should authenticate to.

NetIQ Server Appliance Deployment

ⓘ To increase performance, it is recommended to install several NetIQ Servers in the domain. In this case, the servers will automatically join in a cluster and function as an integral authentication service. It will increase not only the speed of the requests processing, but also the safety of the whole system. Installing several NetIQ Servers also increases fault tolerance. If for some reason one of the servers stops, the user still has a possibility to logon by authenticator.

In this chapter:

- Installing NetIQ Server Appliance
- First Login to NetIQ Admin Interface
- Configuring NetIQ Server Appliance

Installing NetIQ Server Appliance

NetIQ Server appliance can be installed in graphic or text mode. For more information, see the Installing Server chapter of the Server - Installation Guide.

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:

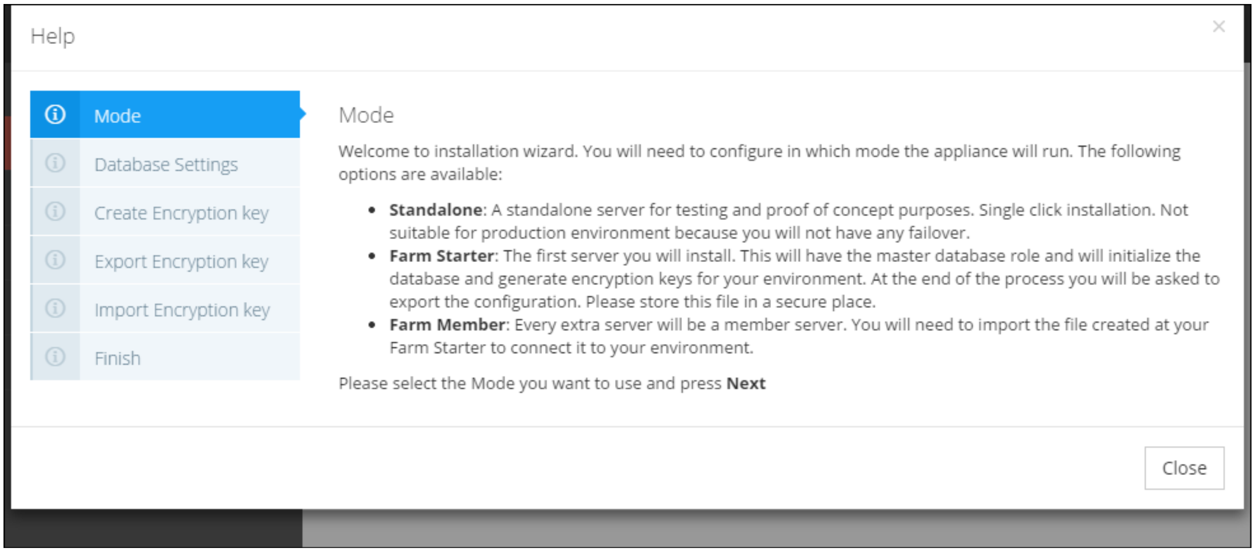
- Standalone is used for demo. It is an all-sufficient server that is not suitable for production environment.
- Farm Starter is the first installed server. It will have the master role and will initialize the database and generate encryption keys for your environment.
- Farm Member is every extra server. The file created at your Farm Starter should be imported and connected to your environment.

© NetIQ

Standalone

To configure the Standalone 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). Read the Help wizard. Click Close after reading it.



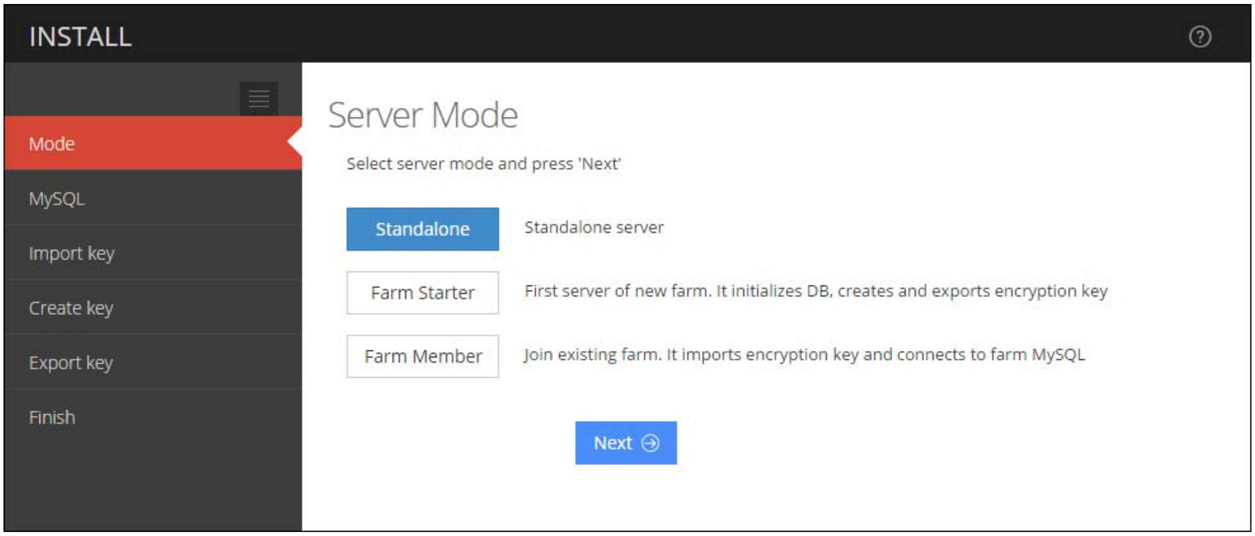
Mode

Welcome to installation wizard. You will need to configure in which mode the appliance will run. The following options are available:

- **Standalone**: A standalone server for testing and proof of concept purposes. Single click installation. Not suitable for production environment because you will not have any failover.
- **Farm Starter**: The first server you will install. This will have the master database role and will initialize the database and generate encryption keys for your environment. At the end of the process you will be asked to export the configuration. Please store this file in a secure place.
- **Farm Member**: Every extra server will be a member server. You will need to import the file created at your Farm Starter to connect it to your environment.

Please select the Mode you want to use and press **Next**

2. Select the Standalone server mode and click Next.

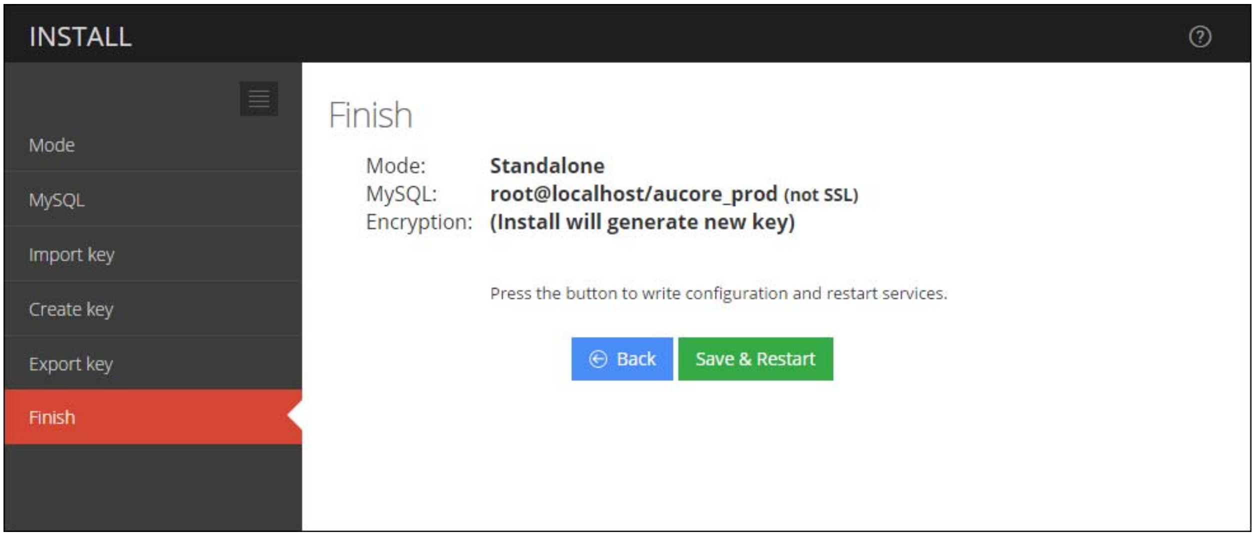


Server Mode

Select server mode and press 'Next'

Standalone	Standalone server
Farm Starter	First server of new farm. It initializes DB, creates and exports encryption key
Farm Member	Join existing farm. It imports encryption key and connects to farm MySQL

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



Finish

Mode: **Standalone**
MySQL: **root@localhost/aucore_prod (not SSL)**
Encryption: **(Install will generate new key)**

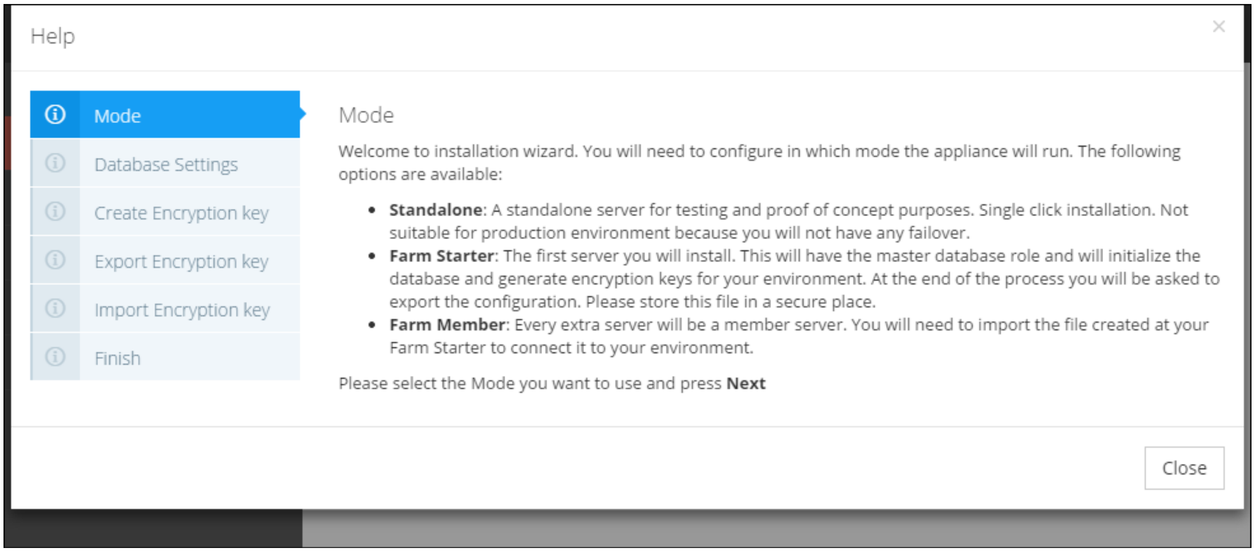
Press the button to write configuration and restart services.

© NetIQ

Farm Starter

To configure the Farm Starter 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). Read the Help wizard. Click Close after reading.



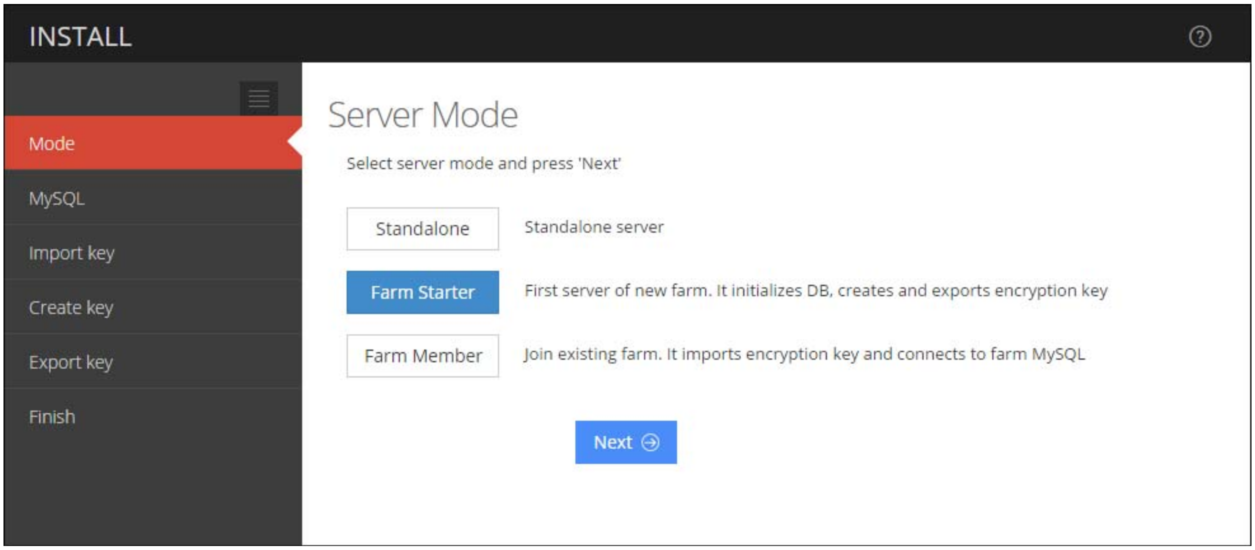
Mode

Welcome to installation wizard. You will need to configure in which mode the appliance will run. The following options are available:

- **Standalone**: A standalone server for testing and proof of concept purposes. Single click installation. Not suitable for production environment because you will not have any failover.
- **Farm Starter**: The first server you will install. This will have the master database role and will initialize the database and generate encryption keys for your environment. At the end of the process you will be asked to export the configuration. Please store this file in a secure place.
- **Farm Member**: Every extra server will be a member server. You will need to import the file created at your Farm Starter to connect it to your environment.

Please select the Mode you want to use and press **Next**

2. Select the Farm Starter server mode and click Next.



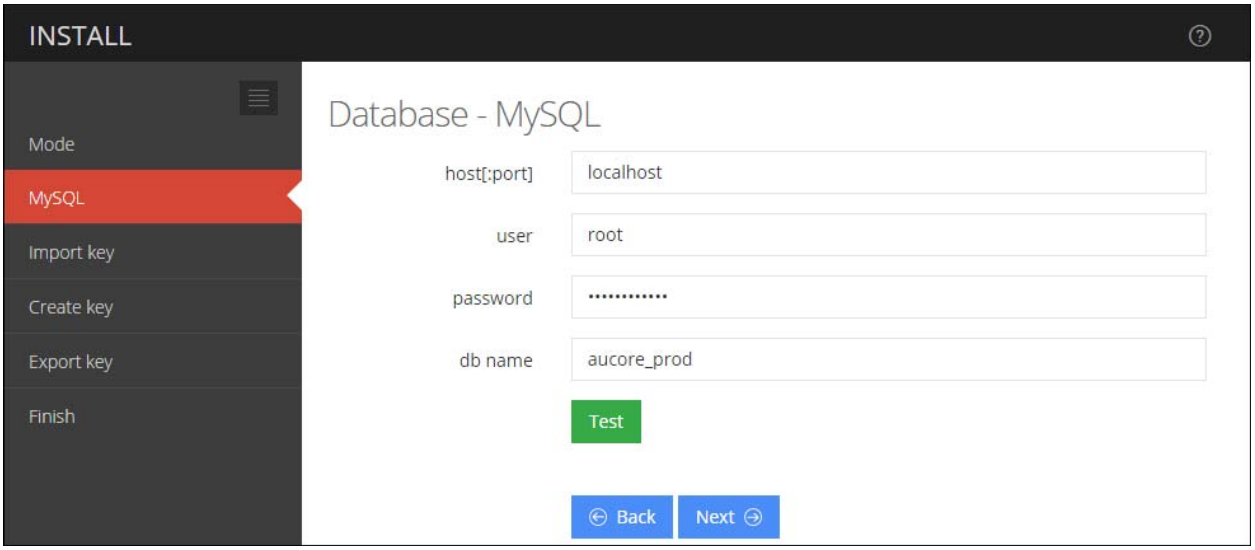
Server Mode

Select server mode and press 'Next'

Standalone	Standalone server
Farm Starter	First server of new farm. It initializes DB, creates and exports encryption key
Farm Member	Join existing farm. It imports encryption key and connects to farm MySQL

3. Enter the password to the Password text field. Click the Test button to verify the connection. If connection is established successfully, click Next to continue.

© NetIQ



INSTALL

Database - MySQL

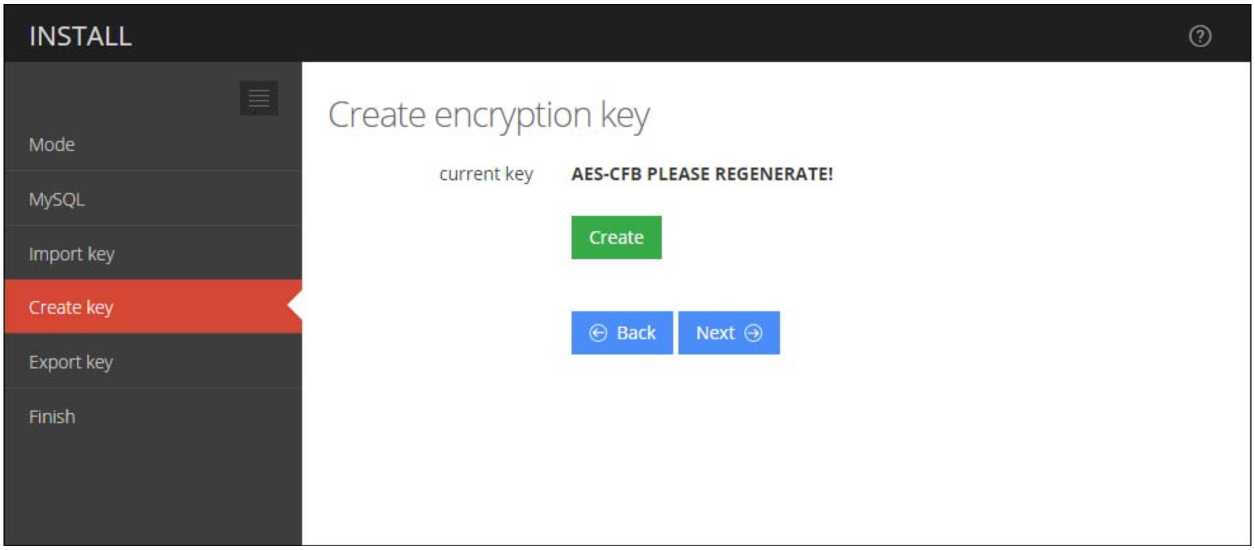
host[:port] localhost

user root

password ••••••••••••

db name aucore_prod

4. Click the Create button to generate encryption key file.

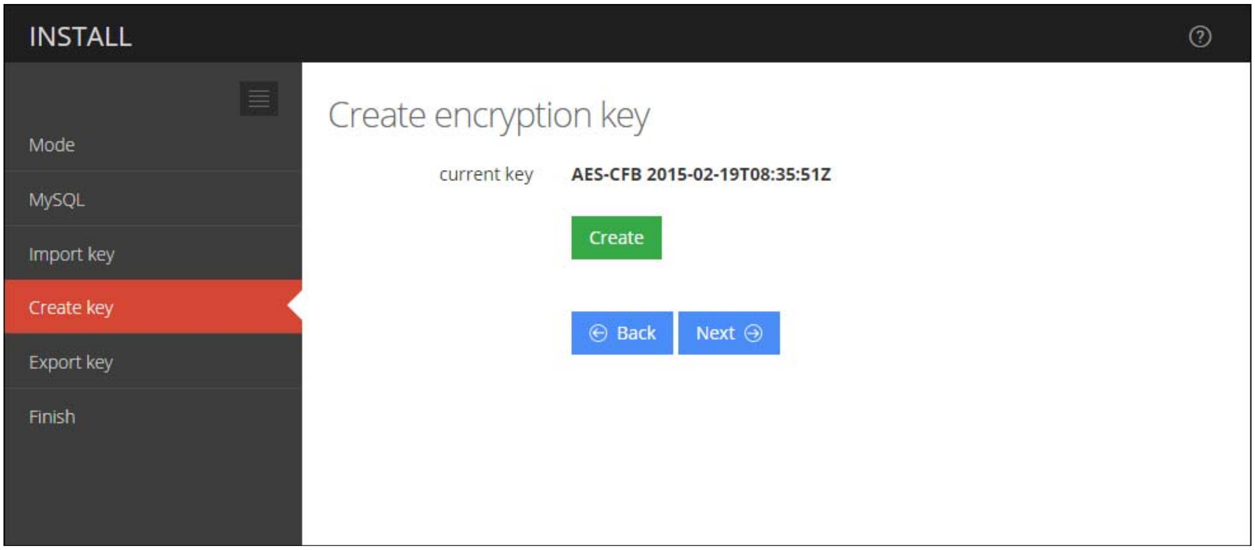


INSTALL

Create encryption key

current key **AES-CFB PLEASE REGENERATE!**

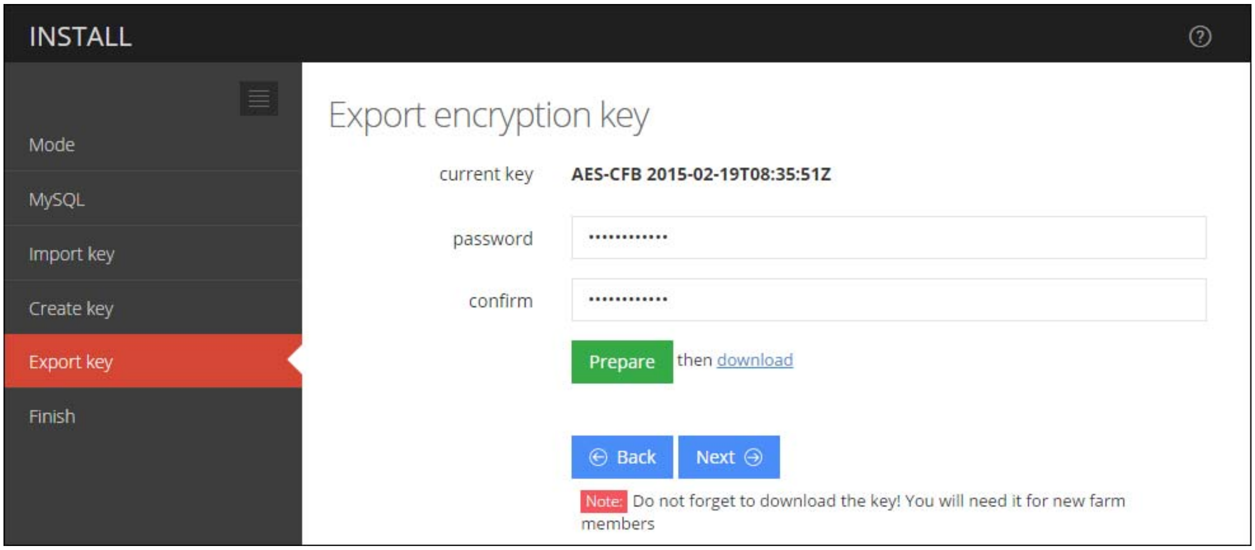
5. After generating encryption key file, click the Next button to continue.



Create encryption key

current key AES-CFB 2015-02-19T08:35:51Z

6. Enter the password and confirm it. Click the Prepare button to prepare encryption key file.



Export encryption key

current key AES-CFB 2015-02-19T08:35:51Z

password ••••••••••••

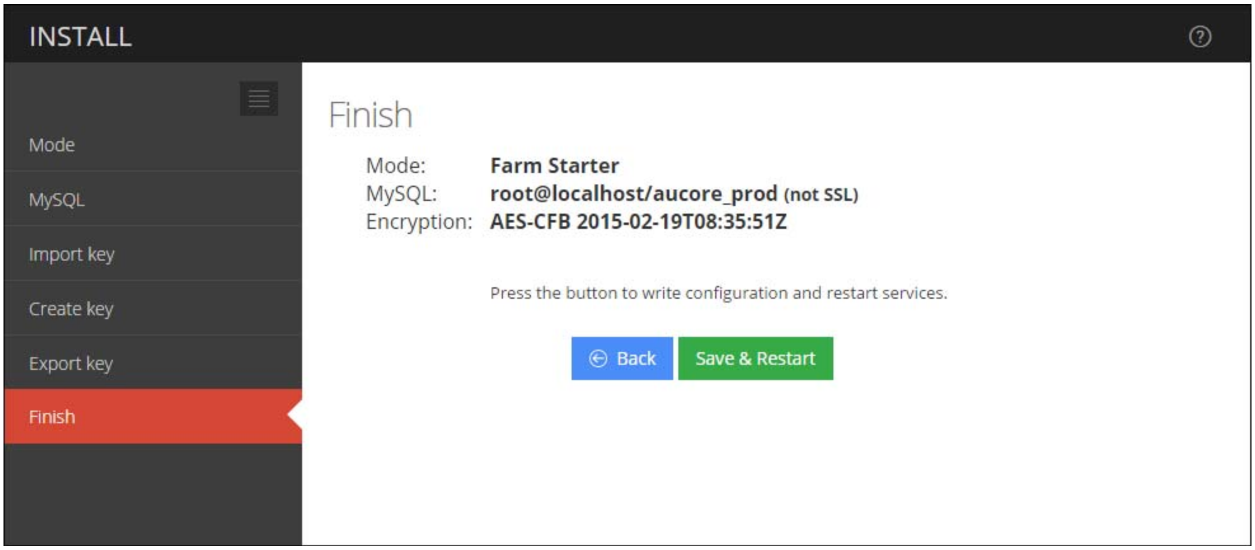
confirm ••••••••••••

then download

Note: Do not forget to download the key! You will need it for new farm members

After preparing it, click the Download link to download the encryption file. Save it in a secure place. You will need it for new Farm Member servers configuration. Click Next to continue.

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



Finish

Mode: **Farm Starter**
MySQL: **root@localhost/aucore_prod (not SSL)**
Encryption: **AES-CFB 2015-02-19T08:35:51Z**

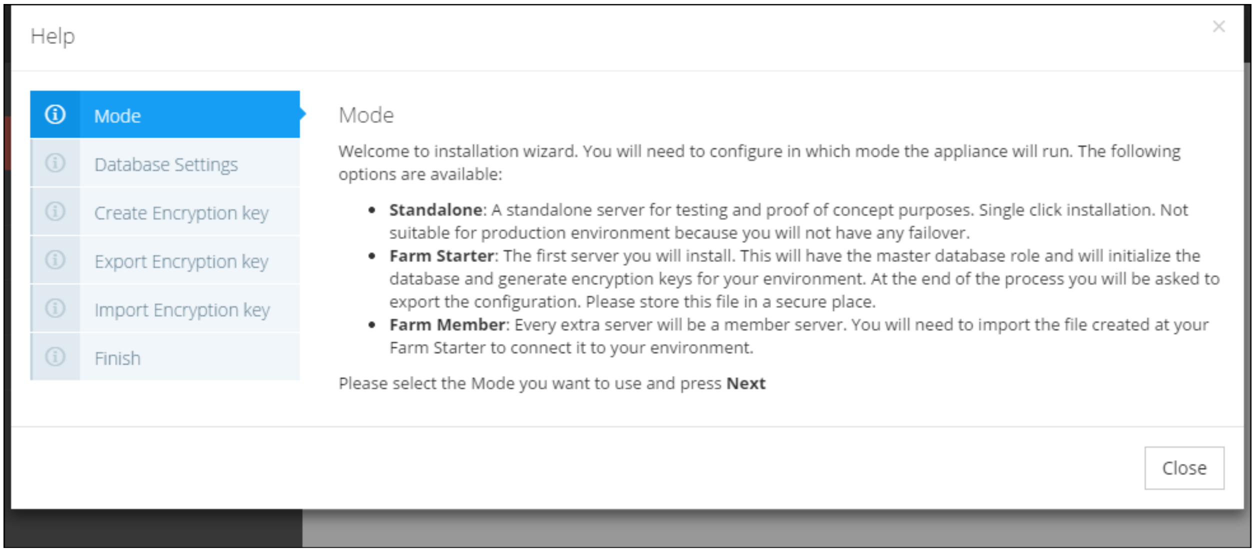
Press the button to write configuration and restart services.

© NetIQ

Farm Member

To configure the Farm 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). Read the Help wizard. Click Close after reading it.



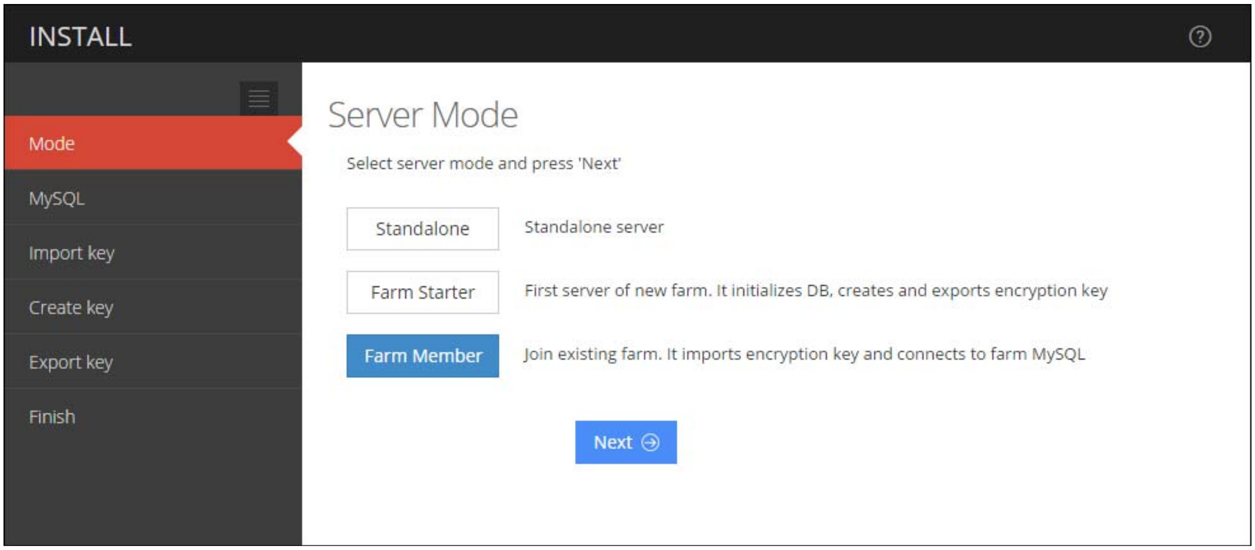
Mode

Welcome to installation wizard. You will need to configure in which mode the appliance will run. The following options are available:

- **Standalone**: A standalone server for testing and proof of concept purposes. Single click installation. Not suitable for production environment because you will not have any failover.
- **Farm Starter**: The first server you will install. This will have the master database role and will initialize the database and generate encryption keys for your environment. At the end of the process you will be asked to export the configuration. Please store this file in a secure place.
- **Farm Member**: Every extra server will be a member server. You will need to import the file created at your Farm Starter to connect it to your environment.

Please select the Mode you want to use and press **Next**

2. Select the Farm Member server mode and click Next.



Server Mode

Select server mode and press 'Next'

Standalone — Standalone server

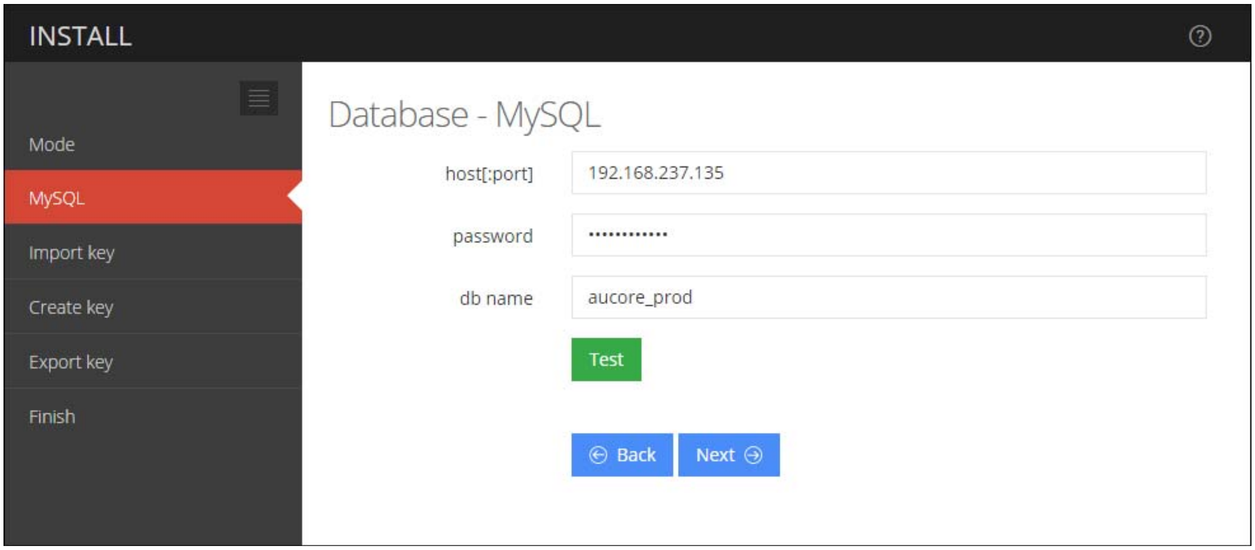
Farm Starter — First server of new farm. It initializes DB, creates and exports encryption key

Farm Member — Join existing farm. It imports encryption key and connects to farm MySQL

3. Enter your Farm Starter server IP address to the host[:port] text field and your password to the Password text field. Click the Test button to verify the connection. If connection is

© NetIQ

established successfully, click Next to continue.



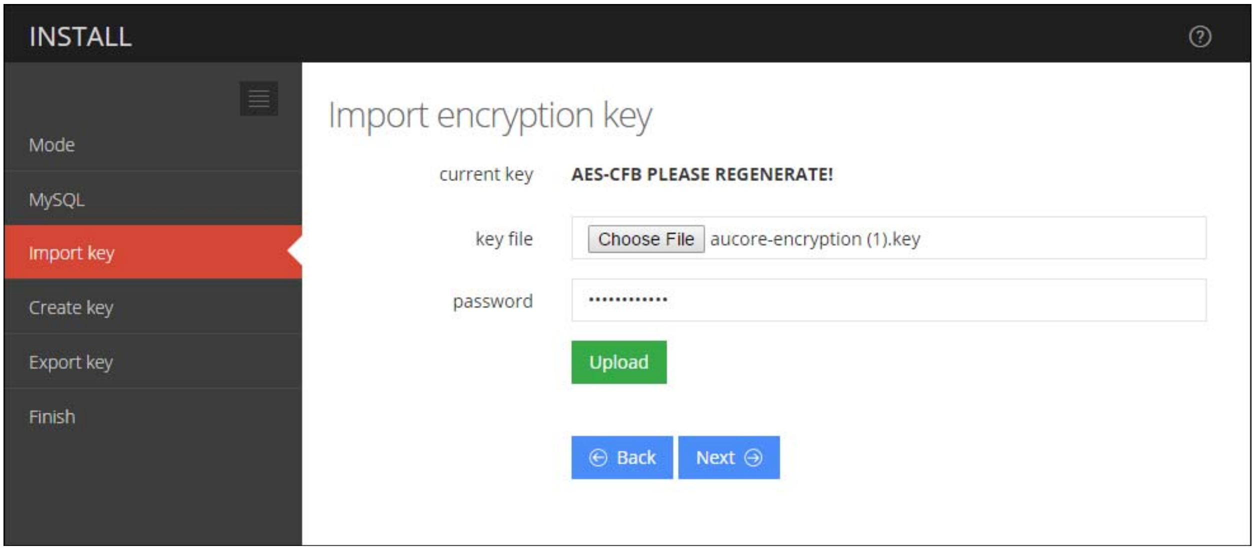
Database - MySQL

host[:port] 192.168.237.135

password ••••••••••••

db name aucore_prod

4. Upload the encryption key file that was generated by your Farm Starter server. Click the Choose File button and add an applicable file. Enter the your password to the Password text field and click Upload. Click Next to continue.



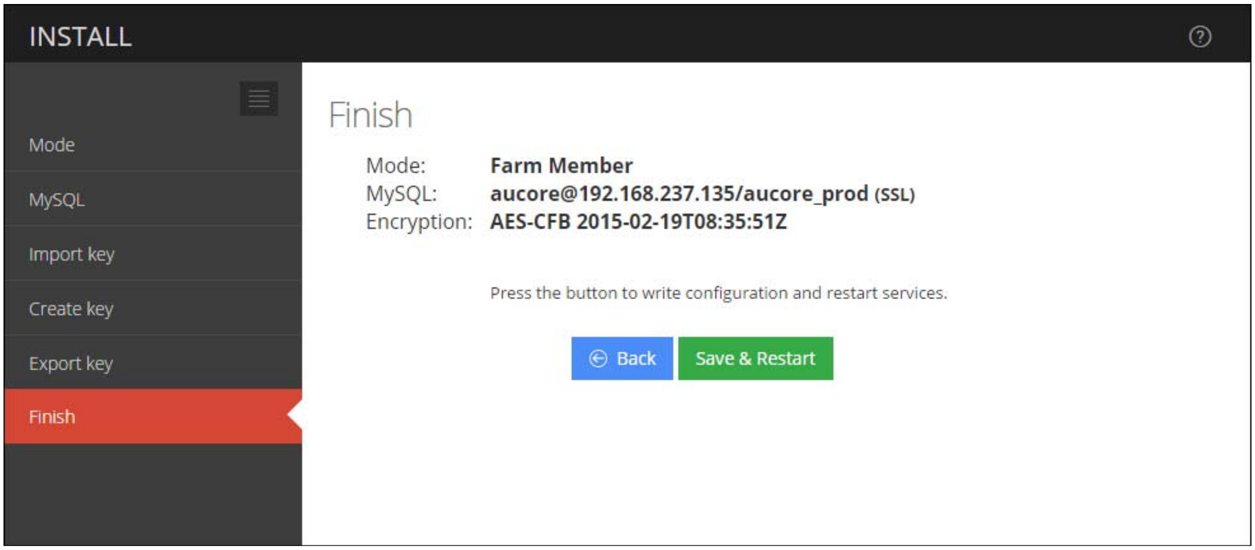
Import encryption key

current key AES-CFB PLEASE REGENERATE!

key file aucore-encryption (1).key

password ••••••••••••

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



Finish

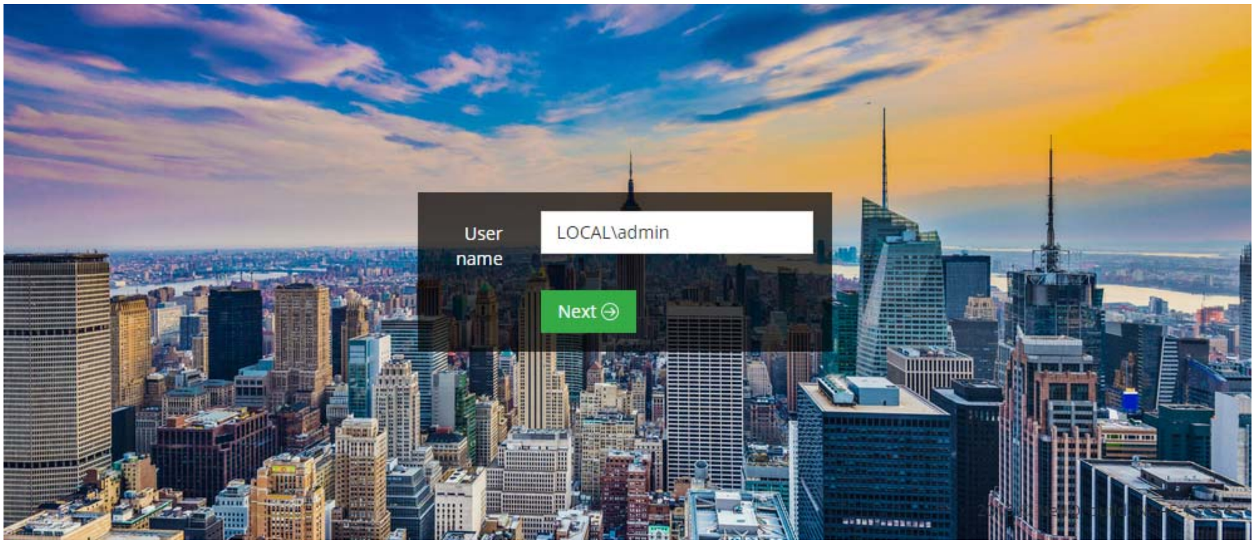
Mode: Farm Member
MySQL: aucore@192.168.237.135/aucore_prod (SSL)
Encryption: AES-CFB 2015-02-19T08:35:51Z

Press the button to write configuration and restart services.

First Login To NetIQ Admin Interface

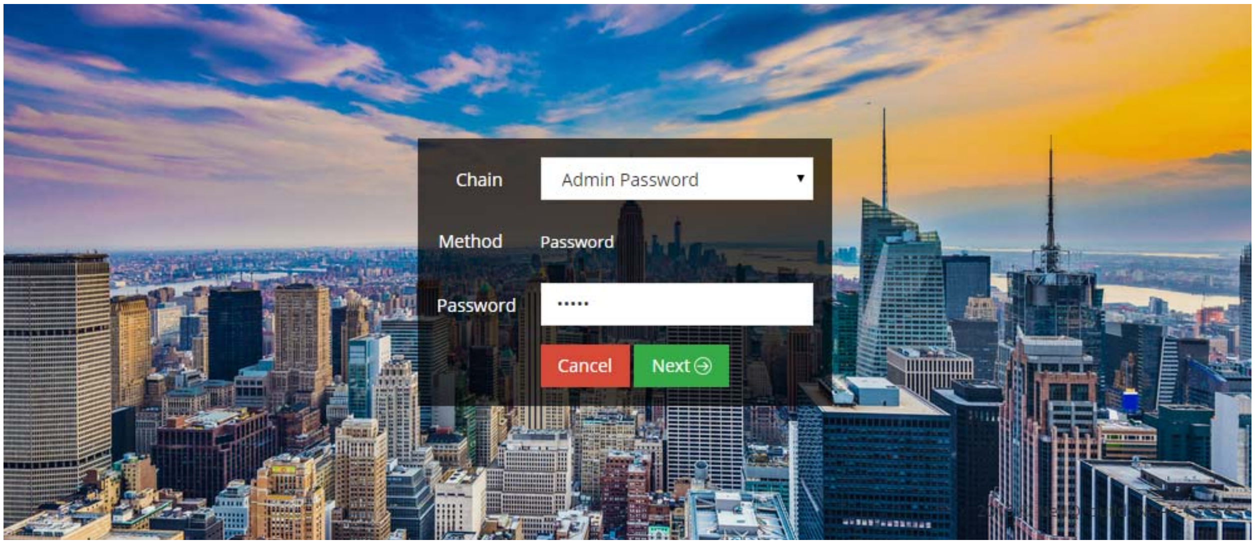
After setting up an applicable server mode, the NetIQ Admin Interface will be displayed. To log in to NetIQ Admin Interface, follow the steps:

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



User name: LOCAL\admin

2. The Admin Password chain is automatically pre-selected by the system as the only available method. Enter the password to the Password text field (admin by default) and click Next to log in.



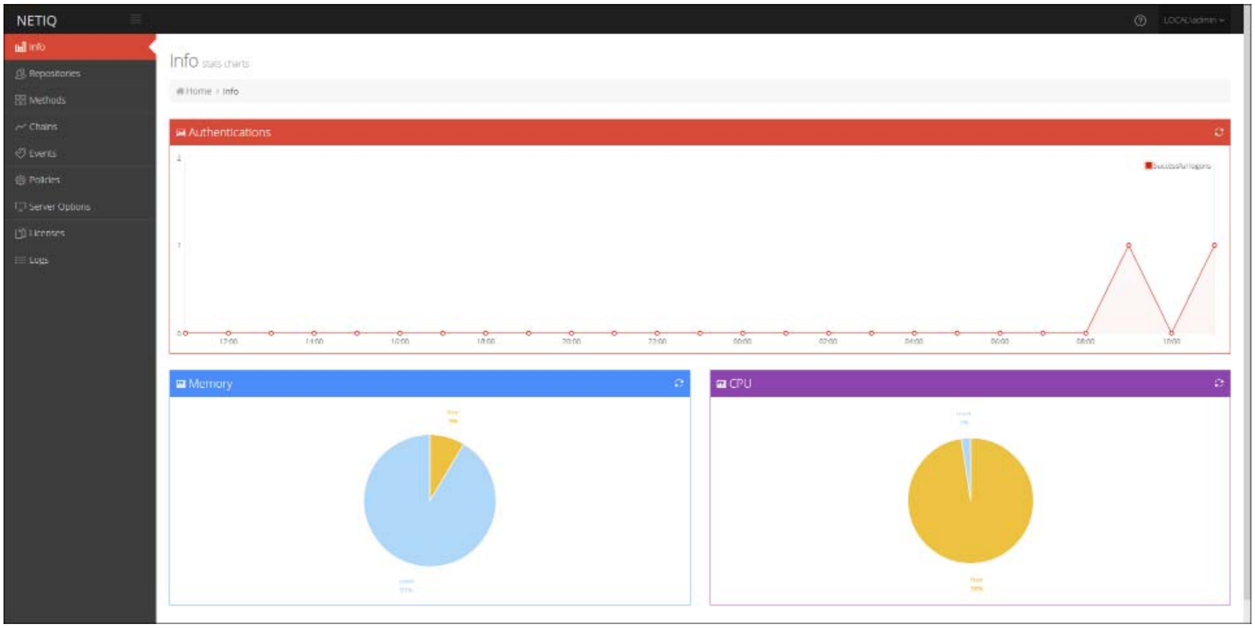
Chain: Admin Password

Method: Password

Password: •••••

© NetIQ

3. The main page of NetIQ Admin Interface will be displayed.

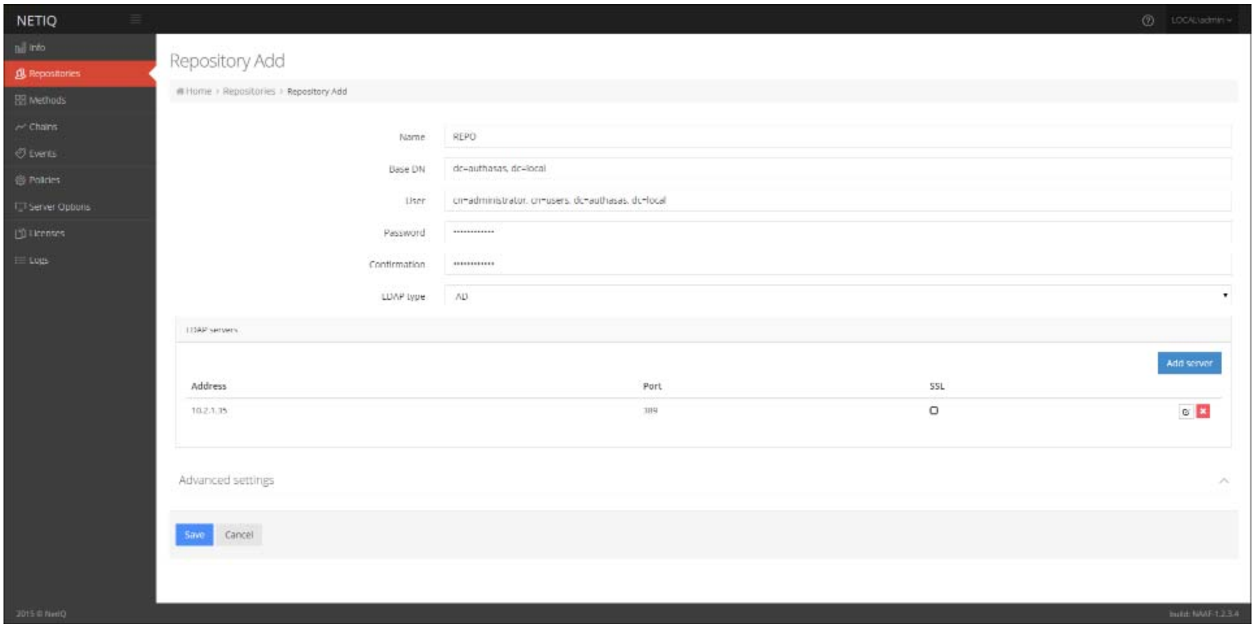


Configuring NetIQ Server Appliance

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, follow the steps:

1. Log in to NetIQ Admin Interface.
2. Add repository that will be used for NetIQ authentication framework.



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

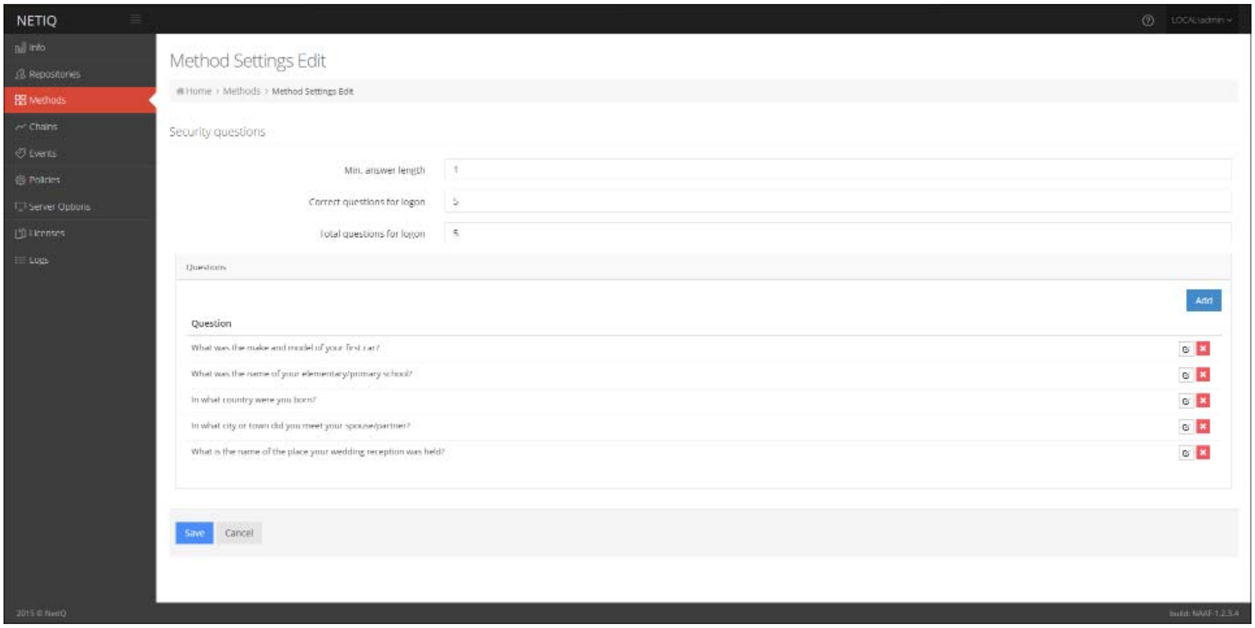
Address	Port	SSL
10.2.1.35	389	☐

Advanced settings

   a. Open the Repositories section.
   b. Click the Add button.
   c. Fill in the Name, Base DN, User, Password, Confirmation text fields. Select an applicable repository type from the LDAP type dropdown.
   d. Click the Add server button.
   e. 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).

f. Click Save at the bottom of the Repositories view to verify and save the specified credentials.

3. Configure applicable authentication methods for NetIQ authentication framework.



Method Settings Edit

Security questions

Min. answer length: 1

Correct questions for logon: 5

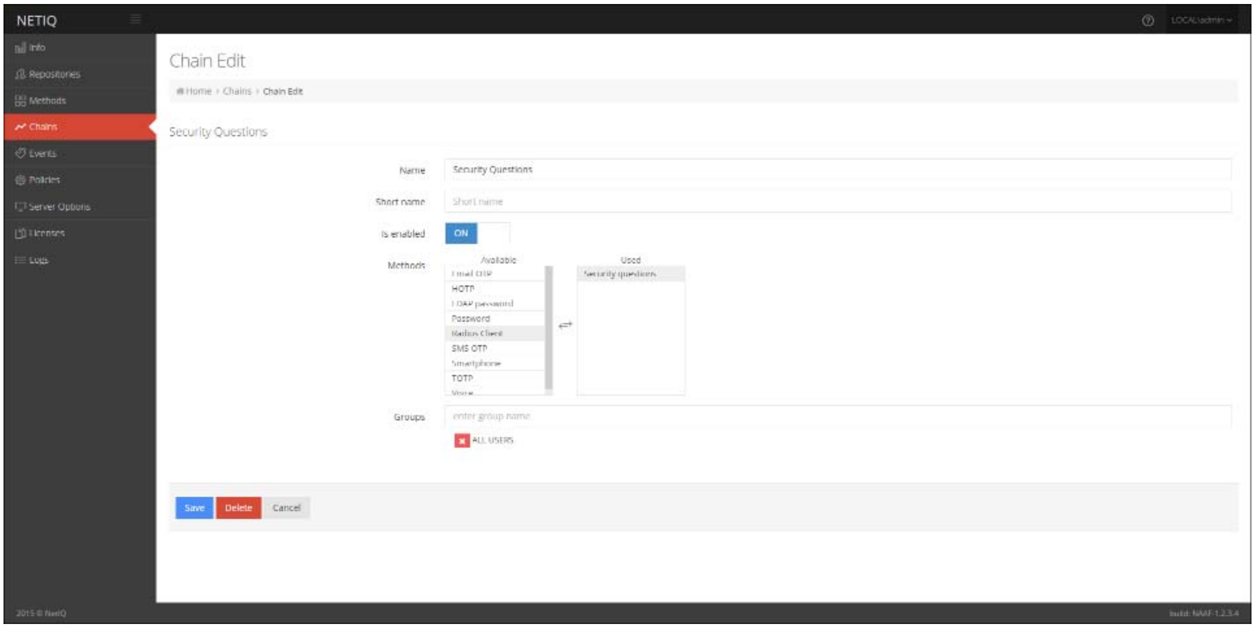
Total questions for logon: 5

Questions

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 reception was held?

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

4. Create new chains or edit existing ones that NetIQ authentication framework will work with. The specified chains will connect to events.



Chain Edit

Home › Chains › Chain Edit

Security Questions

Name: Security Questions

Short name: Short name

Is enabled: ON

Methods:

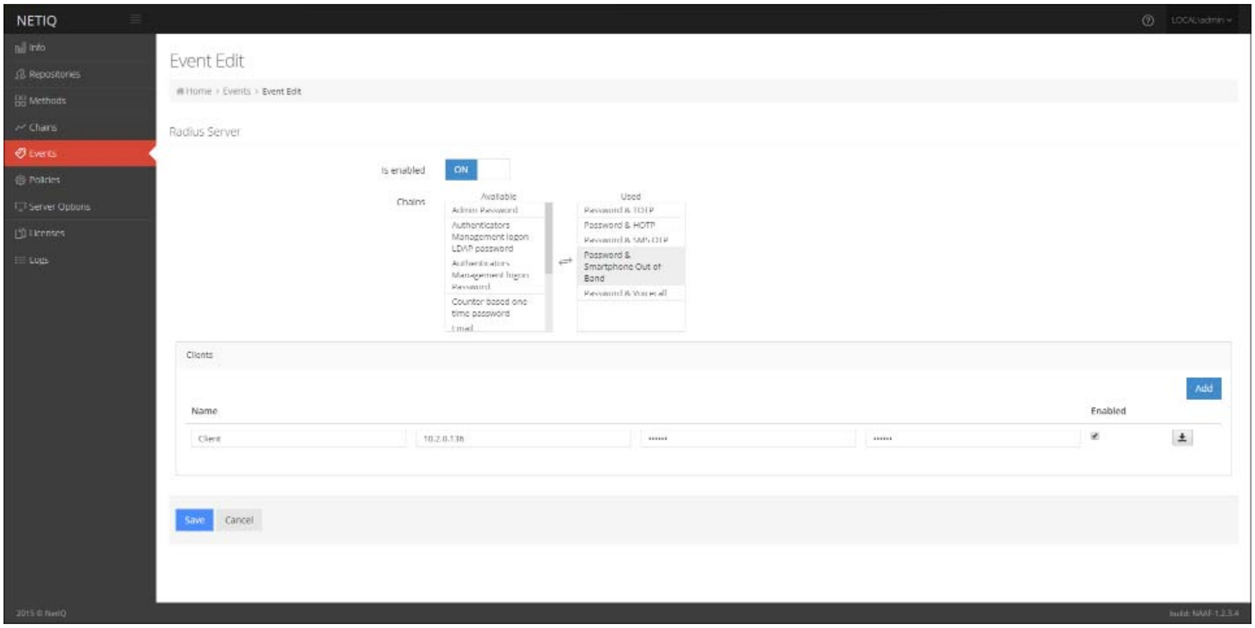
Available	Used
Email OTP	Security questions
HOTP	
LDAP password	
Password	
Radius Client	
SMS OTP	
Smartphone	
TOTP	
Voice	

Groups: enter group name

☒ ALL USERS

a. Open the Chains section.
b. 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).
c. Fill in the Name and Short name text fields.
d. Select whether the current authentication chain is enabled or disabled by clicking the Is enabled toggle button.
e. Select methods that will be assigned to the chain.
f. Specify groups that will be allowed to use the current authentication chain in the Groups text field.
g. Click Save at the bottom of the Chains view to save the configuration.

5. Configure and enable authentication events for NetIQ authentication framework. Currently the supported events are RADIUS Server, NAM and NCA.



Event Edit

Radius Server

Is enabled: ON

Chains

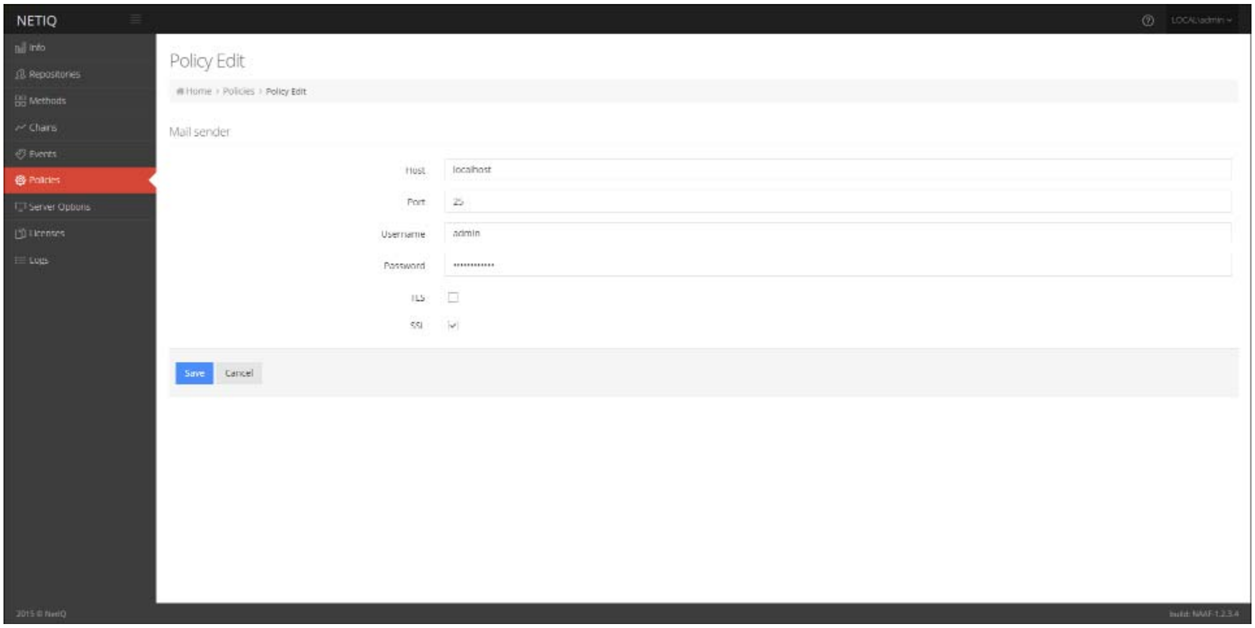
Available	Used
Admin Password	Password & TOTP
Authenticators Management logon LDAP password	Password & HOTP
Authenticators Management logon Password	Password & SMS OTP
Counter based one time password	Password & Smartphone Out of Band
Email	Password & Voice call

Clients

Name				Enabled
Client	10.2.0.136	••••••	••••••	☑

a. Open the Events section.
b. Click the Edit button next to an applicable event.
c. Select whether the current event is enabled or disabled by clicking the Is enabled toggle button.
d. Select methods that will be assigned to the current event.
e. If available, add clients assigned to the current event.
f. Click Save at the bottom of the Events view to save configuration.

6. Configure the policies for NetIQ authentication framework. The configured policies will be applied for all servers.



Policy Edit

Mail sender

Host: localhost

Port: 25

Username: admin

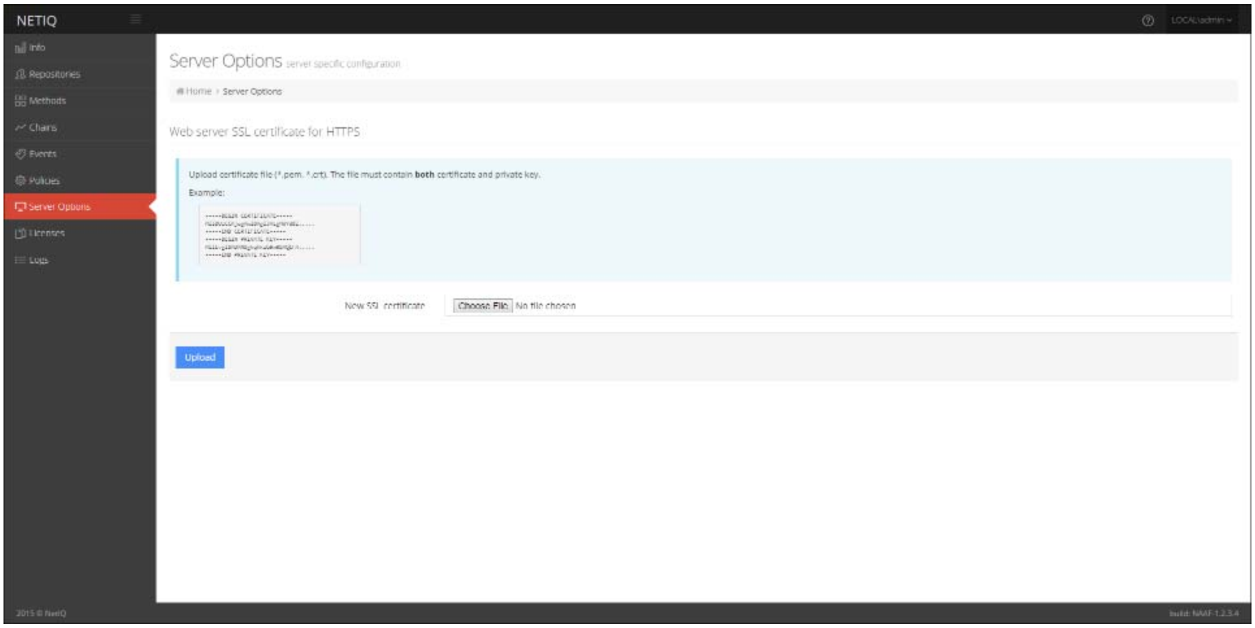
Password: ••••••••••••

TLS ☐

SSL ☑

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

7. Specify the protocol that will be used by NetIQ Server. 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.



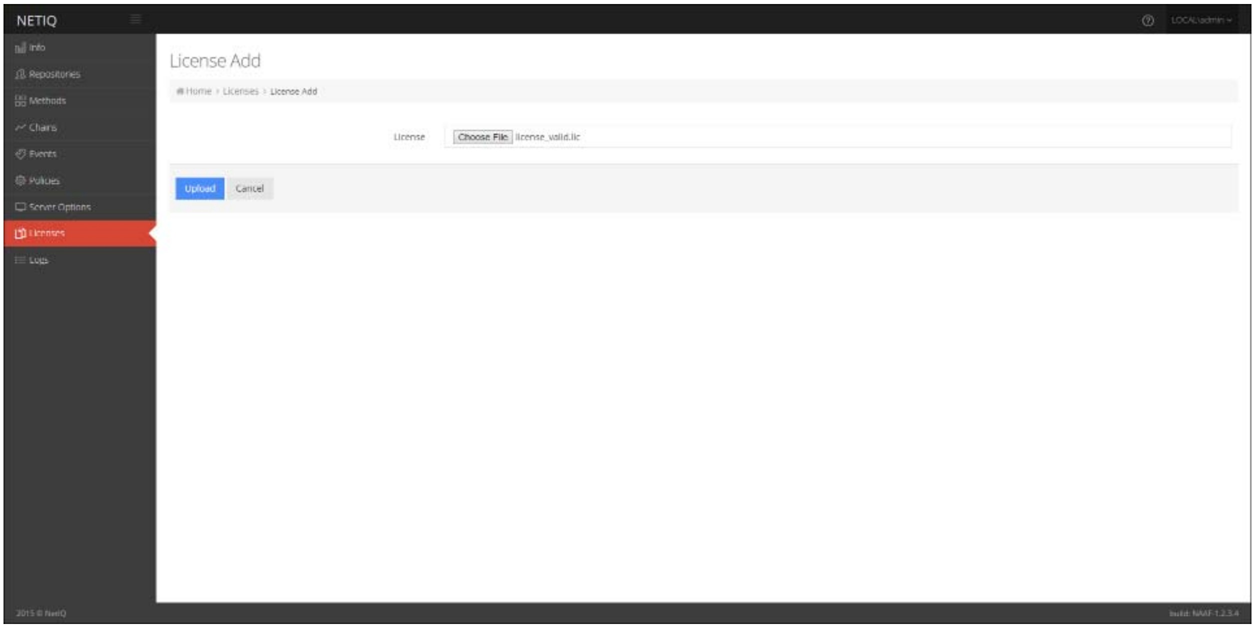
Upload certificate file (*.pem, *.crt). The file must contain **both** certificate and private key.

Example:

```
-----BEGIN CERTIFICATE-----
[illegible]
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
[illegible]
-----END PRIVATE KEY-----
```

a. Open the Server Options section.
b. Click the Choose File button and select the new SSL certificate.
c. Click Upload to upload the selected SSL certificate.

8. Add the license for NetIQ authentication framework. The temporary license is active for 30 days and will expire at the specified date.



License Add

Home › Licenses › License Add

License: Choose File license_valid.lic

a. Open the Licenses section.
b. Click the Choose File button and select the valid license.
c. Click Upload to upload the license.

© NetIQ

Index

© NetIQ