NetIQ Advanced Authentication Framework - Authenticore Server

Administrator's Guide

Version 5.1.0

© NetIQ

Table of Contents

1

Table of Contents **2**

Introduction **3**

About This Document 3

Authenticore Server Overview 4

Authenticore Tray Manager **5**

Managing Authenticore Server 5

Managing Enterprise Key 7

Generating New Enterprise Key 7

Selecting Cryptographic Algorithms 11

Obtaining Current Enterprise Key 12

Restoring Enterprise Key 13

Managing Licenses 16

Troubleshooting **19**

Enterprise Key Discrediting 20

Error Applying License 21

Error Obtaining Enterprise Key 22

Error Restoring Enterprise Key 23

Index **24**

© NetIQ

Introduction

About This Document

Purpose of the Document

This Authenticore Server Administrator's Guide is intended for system administrators and describes how to work with NetIQ Advanced Authentication Framework Authenticore Tray Manager.

Document Conventions

This document uses the following 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.

© NetIQ

Authenticore Server Overview

The **Authenticore server** is the central component in an Advanced Authentication Enterprise deployment. The server has many functions, most importantly matching authenticators and granting access when authenticators match. In this process, the Authenticore Server receives an authentication request from an Advanced Authentication Client, the stored credential is retrieved from the directory, decrypted, and then matched against the sample provided by the user. If the sample matches the stored template, then the Authenticore Server returns the success to the client and MSGINA or Credential provider can then authenticate the user to the domain.

The Authenticore server is also responsible for enforcing all policies that are configured for the user and the client. User and computer policies are retrieved from AD or AD LDS, while global security policies are retrieved as Group Policy Objects that have been applied to the domain, to an Organization Unit, or to a Security Group.

Authenticore Server themselves belong to a Global Security Group which allows for the Advanced Authentication Clients to locate the servers, which may be added or removed on the fly, or moved between sites for performance optimization.

One or more Authenticore Servers may also be designated as log servers to capture all authentication and credential management events. For organizations with dedicated log servers (aggregators), the log server may be deployed on a server that is not configured as an Authenticore Server.

© *NetIQ*

Authenticore Tray Manager

In this chapter:

• Managing Authenticore Server;
• Managing Enterprise Key;
• Managing Licenses.

Authenticore Tray Manager is an application that allows you to stop/start Authenticore server, manage Enterprise Key and licenses. This application is auto-started once the first Authenticore server in domain is installed. Later on Authenticore Tray Manager can be either auto-started when Windows is loading or started manually, if autostart is disabled (**Start > Programs > NetIQ Advanced Authentication Framework > Authenticore Tray Manager**).

Managing Authenticore Server

Authenticore Tray Manager allows you to stop and to start the Authenticore server.

The manual server start is used in cases, when the server hasn't been started automatically due to certain problems. For example, during server installation on ADAM you may face the following problem: if you haven't written the "sc config AAARS depend= ADAM_AAA" command before restarting the computer, the server will be stopped after it and you will have to start it manually.

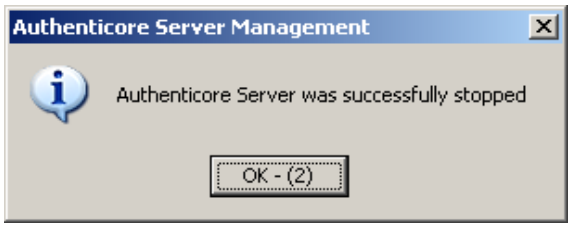
The current state of Authenticore server is shown by Authenticore Tray Manager icons:

indicates that the server is working;

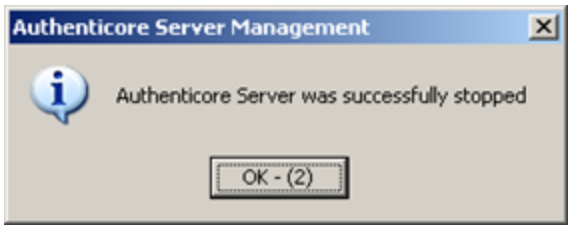
indicates that the server is stopped, unavailable or not found.

To stop an Authenticore server:

• Right-click the **Authenticore Tray Manager** icon on your system tray and select **Stop server**. The server is stopped with notification:

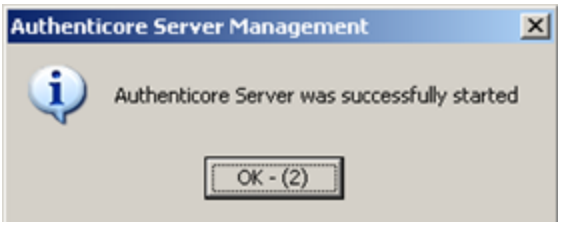


© NetIQ



To start an Authenticore server:

• Right-click the **Authenticore Tray Manager** icon on your system tray and select **Start server**. The server is started with notification:



© *NetIQ*

Managing Enterprise Key

In this chapter:

• Generating New Enterprise Key;
• Obtaining Current Enterprise Key;
• Restoring Enterprise Key.

Generating New Enterprise Key

Generating a new Enterprise Key is an emergency measure in case the current Enterprise Key has been discredited.

After a new Enterprise Key has been generated, all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the **NetIQ Advanced Authentication Framework** tab in a user/computer properties dialog.

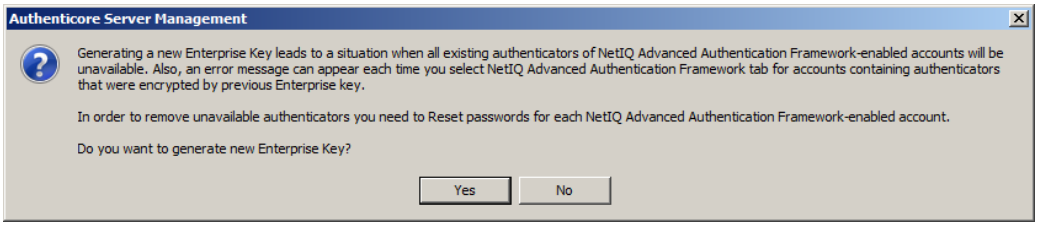
If new enterprise key is generated to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

Before generating a new Enterprise Key you must stop all Authenticore servers in domain.

To generate a new Enterprise Key:

1. Right-click the **Authenticore Tray Manager** icon and select **Enterprise Key > Generate new key**.

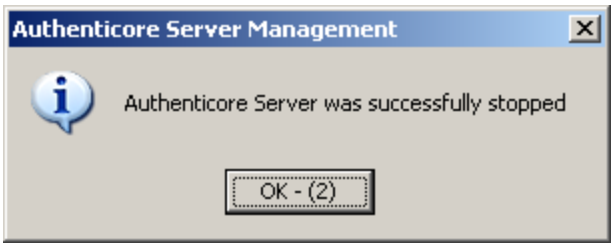
2. The following dialog opens:



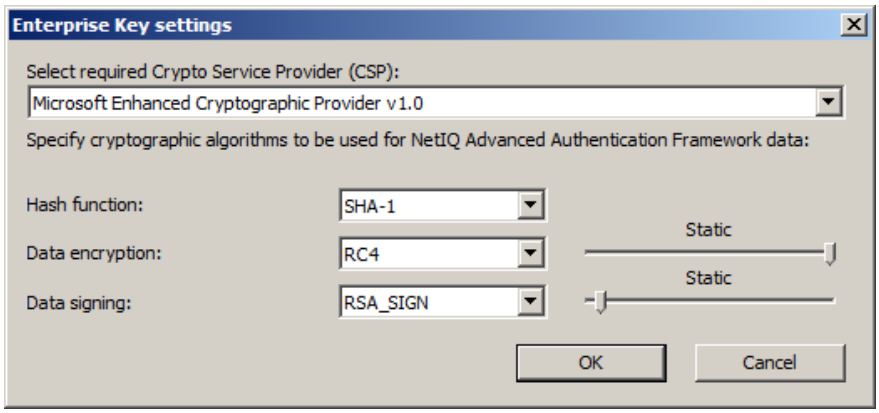
Click **Yes** to continue.

The current Authenticore server is stopped with notification:

© NetIQ



3. The **Enterprise Key settings** dialog is displayed.



To modify Enterprise Key settings:

1. Select **Crypto Service Provider (CSP)**. The main CSP types are:

- Microsoft Base Cryptographic Provider v 1.0 – basic cryptographic functionality that can be exported to other countries or regions.
- Microsoft Strong Cryptographic Provider – extension of the Microsoft Base Cryptographic Provider available with Windows 2000 and later.
- Microsoft Enhanced Cryptographic Provider v1.0 (default) – the Enhanced Provider supports stronger security through longer keys and additional algorithms. It can be used with all versions of CryptoAPI.

The list of available CSPs may vary depending on what CSPs are installed on the local PC.

The Microsoft Strong Provider and the Enhanced Provider are backward-compatible with the Base Provider except that the providers can only generate RC2 or RC4 keys of default key length. The default length for the Base Provider is 40 bits. The default length for the Enhanced Provider is 128 bits. Thus the Enhanced Provider cannot create keys with Base Provider-compatible key lengths. However, the Enhanced Provider can import RC2 and RC4 keys of up to 128 bits. Therefore, the Enhanced Provider can import and use 40 bit keys generated using the Base Provider.

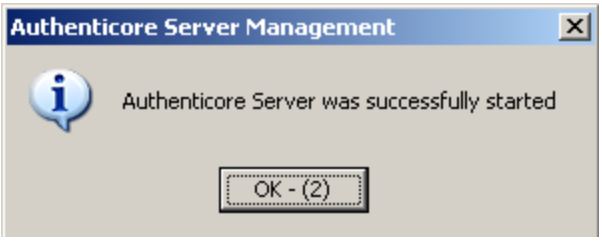
© NetIQ

2. Select encryption algorithms.

3. Set the key length (the upper slider) and the length of data signature (the lower slider). (See Selecting Cryptographic Algorithms)

4. Click **OK**.

The Authenticore server is started with notification:

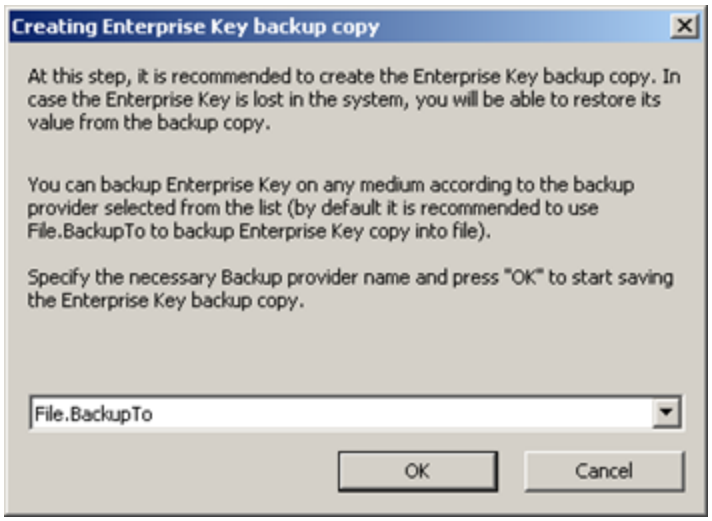


Once Enterprise Key parameters are defined and applied, you should create a backup copy, from which you can restore the Key, if it is lost or corrupted. Restoring the Enterprise Key from the backup copy is also helpful when the Authenticore server is re-installed. Re-installing the Authenticore server means generating a new Enterprise Key. The Enterprise Key is used to encrypt all data in Active Directory, that is why when a new Enterprise Key is generated, the Authenticore Server cannot decrypt the data encrypted with the previous Key. To avoid resetting users' passwords and re-enrolling their patterns after the Authenticore server has been re-installed, you should back up the Enterprise Key while installing the first Authenticore server and then restore it on the new Authenticore server.

5. After Enterprise Key parameters have been defined, you should create a backup copy of the Key so that you could restore the Key in case it is lost or corrupted.

It is highly recommended that you create a backup copy on Flash Drive and save it in the safe place.

© *NetIQ*



Choose **File. BackupTo** (default); Click **OK**.

6. The **Enterprise Key backing up** dialog is displayed:

- Enter the file name and specify the path in the **File name** box <u>or</u> use the **Browse** button to select the path to backup file.
- To set a password for the file, check the **Set password** for the file box, and then enter and confirm the password.
- Click **OK.**

Enterprise Key is exported and generated with notifications:

© *NetIQ*

Selecting Cryptographic Algorithms

The table below presents the accordance of algorithms' keys lengths, included into the standard Windows supply, to the selected CSP type:

Algorithm	Base CSP	Strong CSP	Enhanced CSP
Hash function			
MD2	128 bits	128 bits	128 bits
MD4	128 bits	128 bits	128 bits
MD5	128 bits	128 bits	128 bits
SHA1	160 bits	160 bits	160 bits
SHAMD 5 SSL3	288 bits	288 bits	288 bits
Data encryption			
DES	56 bits	56 bits	56 bits
RC2	40 bits	40 bits	128 bits
RC4	40 bits	40 bits	128 bits
3DES TWO KEYS	Not supported	112 bits	112 bits
3DES	Not supported	168 bits	168 bits
Data signing			
RSA	512 bits	512 bits	1024 bits

© *NetIQ*

Obtaining Current Enterprise Key

Currently this feature is temporarily unavailable under Microsoft Windows Server 2008 ™ due to bug in the operational system.

Obtaining current enterprise key is needed when you have more than one Authenticore Server and you are configuring an additional Authenticore Server or when you are rebuilding one of our Authenticore Servers).

To obtain a copy of the current Enterprise Key on additional Authenticore servers in a domain

- On a server, right-click the **Authenticore Tray Manager** icon and select **Enterprise Key > Obtain current key**.

As a result, the current server will address another working Authenticore server and request for the current Enterprise Key. The Enterprise Key is obtained with notification. The backup copy of the Key will be saved on the server.

© NetIQ

Restoring Enterprise Key

In the situation when you are configuring the new Authenticore Server or rebuilding Authenticore Server and you have Enterprise Key file, Authenticore Tray Manager will help you restore it.

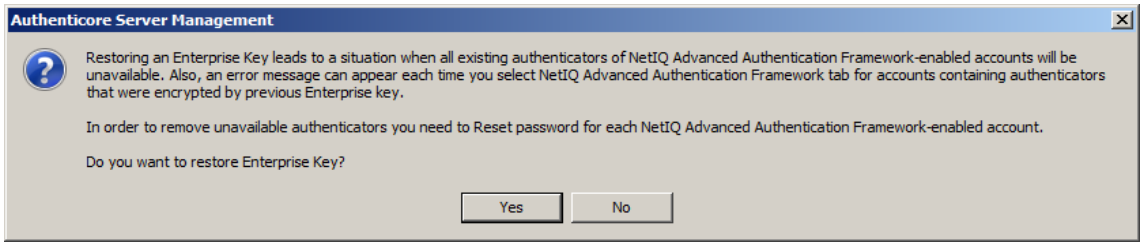
After the Enterprise Key has been restored from the backup copy and the restored key does not match the old one, then all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the NetIQ Advanced Authentication Framework tab in a user/computer properties dialog.

To restore Enterprise Key

If new enterprise key is used to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

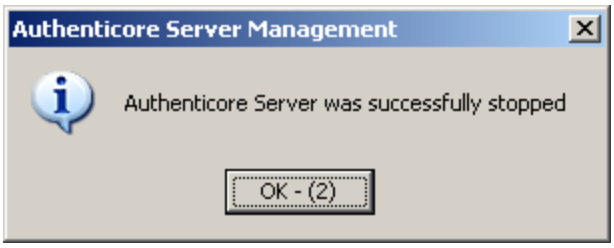
1. Right-click the Authenticore Tray Manager icon and select **Enterprise Key > Restore key**.

2. The following dialog opens:

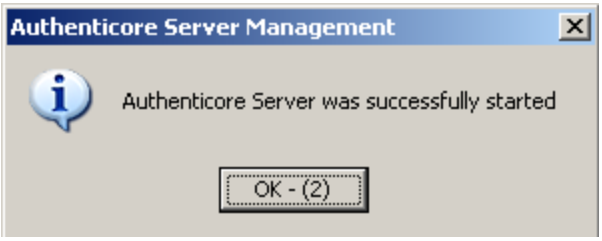


Click **Yes** to continue.

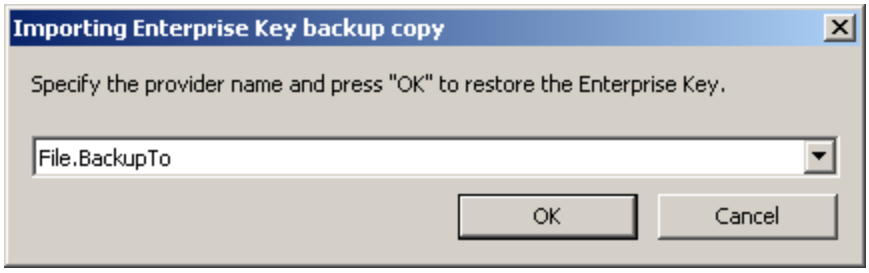
The server is stopped and then started again with notifications:



© NetIQ

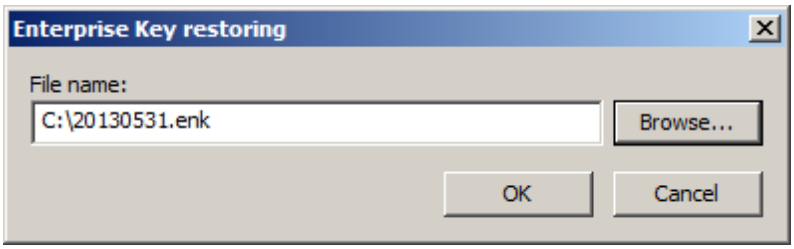


3. The **Importing Enterprise Key** backup copy dialog is displayed:

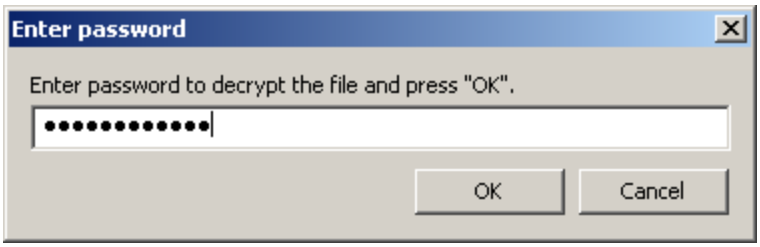


Select the backup provider and click **OK**.

4. Enter the file name and path or use the **Browse** button to locate the backup copy file. Click **OK**.



If you protected the file with a password while creating the backup copy, the following dialog is displayed:



Type your password and click **OK**.

The Enterprise Key is restored with notification:

© *NetIQ*

Authenticore Server Management
Enterprise Key was successfully restored.
OK - (4)

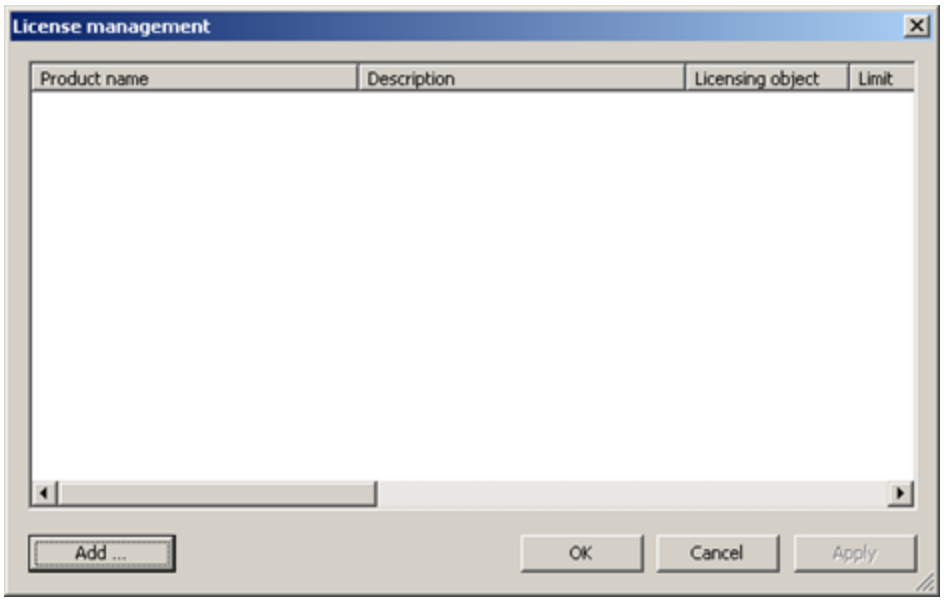
© NetIQ

Managing Licenses

To manage licenses:

1. Right-click the **Authenticore Tray Manager** icon and select **License Management**.

2. The License management dialog is displayed:



This dialog displays the list of applied licenses. You can:

- view the details of any applied license;
- add and apply a new license.

Adding and Applying a License

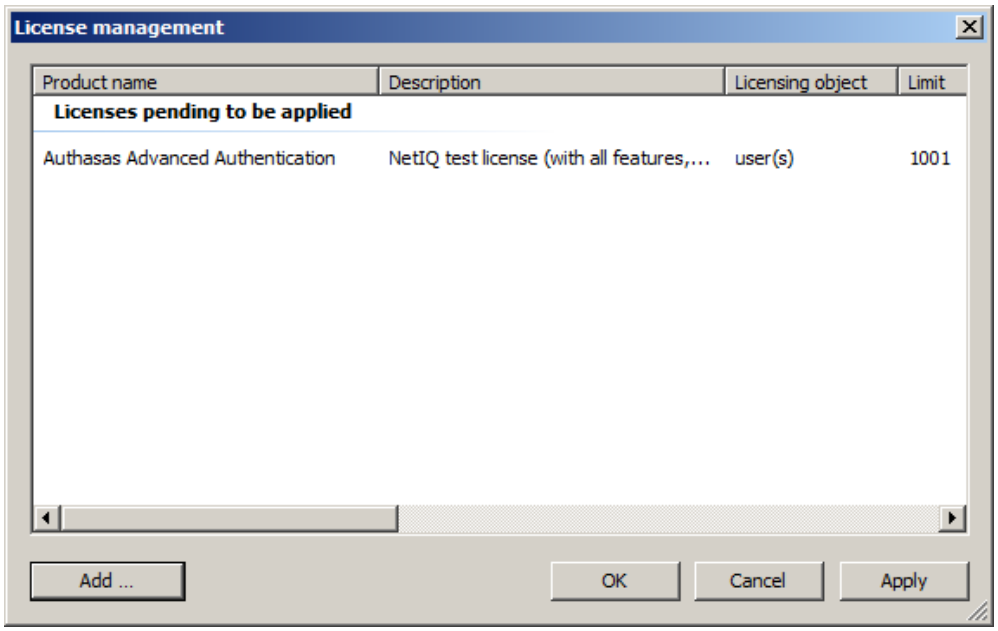
To add a new license

1. In the **License management** dialog, click **Add**.

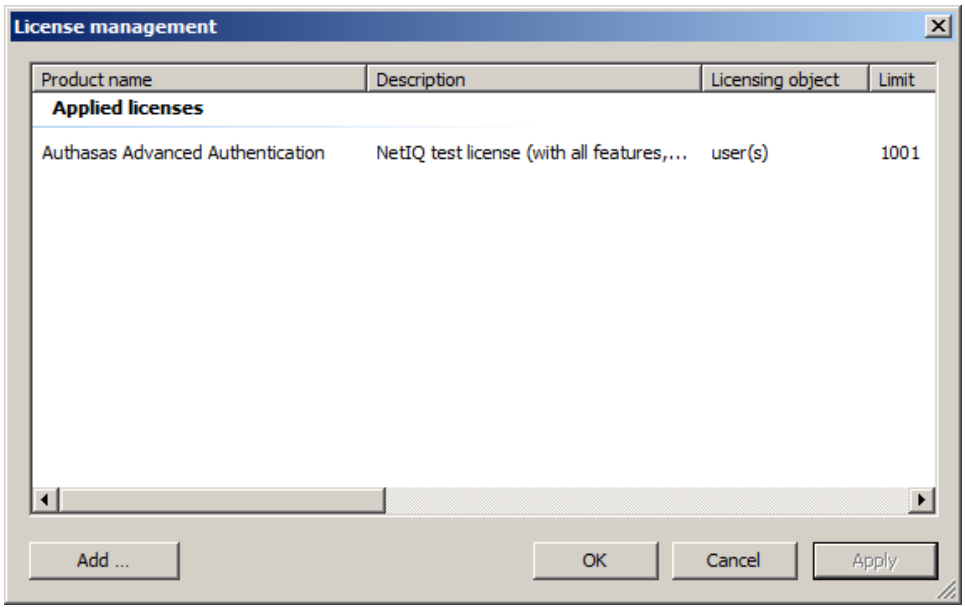
2. Select and open the license file.

3. The license you have added is displayed in the dialog as pending to be applied:

© *NetIQ*



4. To apply license, click **Apply**. The license is now displayed as applied:



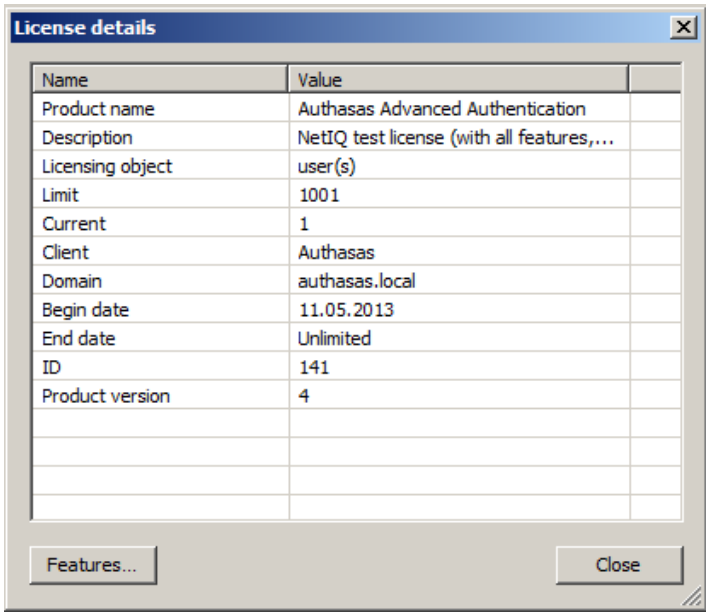
If a license of the given type already exists, you are prompted to overwrite the earlier license.

Viewing License Details

To view license details:

© *NetIQ*

- Double-click the license in the License management dialog. The License details page opens:



If you click the **Features** button, you will be provided with an opportunity to view the list of all licensed components of the solution.

© *NetIQ*

Troubleshooting

In this chapter:

• Enterprise Key Discrediting;

•Error Applying License;
•Error Obtaining Enterprise Key;

•Error Restoring Enterprise Key.

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

When you contact support service

Please when you turn to support service for help, describe the problem as precisely as you can and attach logs from the PC, on which the problem occurred. To create logs, use **LogCreator** tool that is located on the installation disk in **\Tools\LogCollector** folder.

To get logs

1. Copy **LogCreator.exe** file to C:\ drive of the faulty computer. Successful tool launch from a network drive cannot be guaranteed.
2. Run the tool.
3. In the opened dialog click **Enable all**. As a result, all components in **Debugged components** section are selected.
4. Close the dialog.
5. Repeat the steps that you performed before the problem occurred.
6. Run the tool again and click **Save** logs.
7. Save the logs in archive file.

© NetIQ

Enterprise Key Discrediting

Description:

The current Enterprise Key has been discredited.

Solution:

If Enterprise Key is discredited, follow the steps below:

1. Stop all Authenticore servers.

2. Use one of the servers to generate a new Enterprise Key. After the Key has been generated, start the server.

3. Start other Authenticore servers. Obtain the Enterprise Key on each of them.

⚠ After a new Enterprise Key has been generated, all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the **NetIQ Advanced Authentication Framework** tab in ADUC snap-in.

⚠ If new enterprise key is generated to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

© *NetIQ*

Error Applying License

Description:

The selected license is not applied, the error message is displayed.

Cause:

a) The term specified in the license has expired;

b) The domain name specified in the license does not match the current domain name;

c) The current number of licensing objects exceeds the limit specified in the license;

d) The license file is corrupted.

Solution:

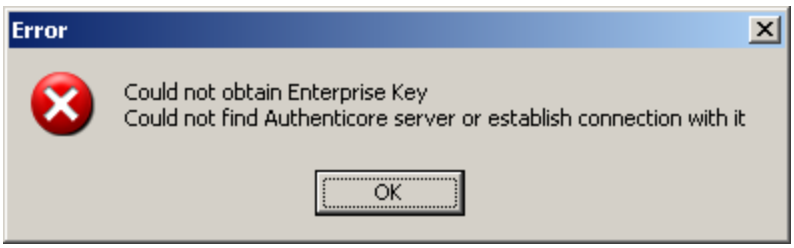
Check the license details and contact the support service.

© *NetIQ*

Error Obtaining Enterprise Key

Description:

The current Enterprise Key cannot be obtained. The error message is displayed:



Cause:

a) The Authenticore server is not connected to the network.

b) Additional Authenticore servers were being restarted or stopped while attempting to obtain the Key.

c) Attempting to obtain the current Enterprise Key on the only Authenticore server in domain. This is needless.

Solution:

a) Check that there is another working Authenticore server in the domain.

b) Check that all Authenticore servers are available in the network.

c) Check that the Domain Controller is available.

© *NetIQ*

Error Restoring Enterprise Key

Description:

The Enterprise Key is not restored from the backup copy. The error message is displayed:

Cause:

a) You have mistyped the password while importing the Key from the backup copy.

b) The backup copy file is corrupted.

Solution:

a) Retype the password and retry.

b) If the Enterprise Key was lost and cannot be restored, generate a new one.

After a new Enterprise Key has been generated, all data encrypted with the previous Key become unavailable, and you will receive the error message every time you open the **NetIQ Advanced Authentication Framework** tab in ADUC snap-in.

If new enterprise key is generated to replace an old one, then password reset is required for activating user accounts that worked with the previous enterprise key.

© *NetIQ*

Index

A

Active Directory 9
Administrator 1
ADUC 20, 23
Algorithms 9, 11
Authentication 1, 3-5, 7, 13, 20, 23
Authenticator 3
Authenticore server 4-5, 22
Authenticore Tray Manager 3, 5, 7, 12-13, 16

D

Domain 22

E

Enterprise Key 5, 7, 12-13, 19-20, 22-23
Error 19, 21-23

F

File 10

G

Generate 7

K

Key 7, 12-13, 20, 22-23

L

Logon 3

M

Microsoft Windows Server 2008 12

O

Obtain 20

R

Restore 13

© *NetIQ*

S

Security 4
Server 1, 3-5, 12-13
system 12

U

User 4

W

Windows 8, 11-12

© *NetIQ*