



NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
NetIQ Advanced Authentication Framework Deployment	4
System Solution	4
Service Accounts and Groups	6
System Planning	7
Choosing Directory Services	7
Authenticore Servers	7
Configuring an Environment that Includes AD LDS	9
NetIQ Solution Deployment	10
Extending Schema	10
Group Policy Configuring	10
Installing and Configuring of First Authenticore Server	11
Installing and Configuring of Additional Authenticore Server	12
NetIQ Password Filter Installation	13
NetIQ Log Server Installation	13
NetIQ Administrator Workplace Configuring	14
NetIQ Client Installation	14
NetIQ EAP Server	15
NetIQ NPS Plugin	15
NetIQ Web Service	15
NetIQ RTE Server	16
Troubleshooting	17
The AD LDS (ADAM) Replica Problem	17
Index	18

Introduction

About This Document

Purpose of the Document

This Deployment Guide is intended for advanced administrators and describes the procedure of NetIQ Advanced Authentication Framework solution deployment.

For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ components guides.

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.

NetIQ Advanced Authentication Framework Deployment

In this chapter:

- [System Solution](#);
- [System Planning](#);
- [Solution Deployment](#).

System Solution

NetIQ Advanced Authentication Framework installation package consists of 3 group of components stored on the installation CD:

1. Server Components

- **NetIQ Advanced Authentication Framework – Authenticore Server**

<CD drive>_authenticore\authenticore.msi

This package contains NetIQ Authenticore Server component.

An **Authenticore Server** is responsible for user data processing, particularly for the user authentication process.

- **NetIQ Advanced Authentication Framework - EAP Server**

<CD drive>_eapserver\eapserver.msi

This package contains NetIQ EAP Server component.

EAP Server is an Internet Engineering Task Force (IETF) standard that provides an infrastructure for network access clients and authentication servers to host plug-in modules for current and future authentication methods.

- **NetIQ Advanced Authentication Framework – Log Server**

<CD drive>_logserver\logserver.msi

This package contains NetIQ Log Server component.

Log Server collects and accumulates messages about events regarding on NetIQ from NetIQ Authenticore Servers.

- **NetIQ Advanced Authentication Framework - NPS Plugin**

<CD drive>_npsplugin\npsplugin.msi

This package contains NetIQ NPS Plugin component.

NPS Plugin adds Authentication to the Microsoft Network Policy Server. It allows authenticating with any RADIUS compliant client using OATH OTP authenticator to NetIQ.

- **NetIQ Advanced Authentication Framework – Password Filter**

<CD drive>_pwdfilter\passwordfilter.msi

This package contains NetIQ Password Filter component.

Password Filter is a service which notifies Authenticore Server about the instances of password change for domain users. It's necessary to synchronize passwords between domain services and NetIQ storage.

- **NetIQ Advanced Authentication Framework – Web Service**

<CD drive>_webservice\webservice.msi

This package contains NetIQ Web Service component.

Web Service allows users to authenticate in domain services using their own authenticators on non-domain joined clients.



Please do not execute webservice.msi directly, because you can have a problem with necessary permissions. Please use **Autorun.exe** to install NetIQ Web Service.

2. Administrative Tools

<CD drive>_admttools\admttools.msi

The package contains components that allow the administrator to control and monitor the NetIQ Advanced Authentication Framework system.

3. Client

- **NetIQ Advanced Authentication Framework – Client**

<CD drive>_client\client.msi

The NetIQ Client is a component that must be installed on every NetIQ-secured workstation. It allows users to enroll authenticators and to authenticate in their operating systems using enrolled authenticators.

- **NetIQ Advanced Authentication Framework – RTE**

<CD drive>_rte\rte.msi

This package contains RTE (Runtime Environment) component.

RTE allows to use SDK (Software Developer Kit) with no need to install NetIQ Advanced Authentication Framework Client component. It is useful when you would like to use NetIQ Advanced Authentication Framework to secure access to certain applications only, without changing the regular Windows logon procedure.



You also need to get and install necessary NetIQ authentication providers from NetIQ official website.

Service Accounts and Groups

When you install Authenticore Server for the first time, the following groups and accounts are created:

- **AuthenticoreService** – a mandatory domain account used by Authenticore Server. AuthenticoreService is a member of the Domain Users, Domain Admins and Enterprise Admins groups and is given a batch logon privilege on each Authenticore Server.
- **Authenticore Admins** – a domain group of users able to install and configure Authenticore Servers. By default, the group includes the following predefined system groups of the users: Domain Admins and Enterprise Admins. If the administrator is not a member of the Authenticore Admins group, he/she will not be able to install and set up Authenticore Server.
- **Authenticore Servers** – a domain group, which lists all Authenticore Servers installed in the domain. A new computer is automatically added to Authenticore Servers group when “NetIQ Advanced Authentication Framework – Authenticore Server” package is installed.
- **NetIQ Advanced Authentication Framework Admins** – a domain group of users, which can be given control over NetIQ Advanced Authentication Framework user and computer settings. In this case all you need to do to delegate control to a new user is add them to NetIQ Advanced Authentication Framework Admins group. By default, NetIQ Advanced Authentication Framework Admins group contains Domain Admins group, members of which have pre-given control over NetIQ Advanced Authentication Framework setting. For other users, which are not members of NetIQ Advanced Authentication Framework Admins or Domain Admins group, control over NetIQ Advanced Authentication Framework settings is given manually.
- **NetIQ Advanced Authentication Framework ADAM Servers** – a domain group that contains servers with installed Active Directory Lightweight Directory Services (AD LDS) or Active Directory Application Mode (ADAM) Servers. This group only exists in configurations with extended ADAM/AD LDS schema.

System Planning

Before installing the NetIQ Advanced Authentication Framework solution please check that your corporate environment satisfies the NetIQ System Requirements at the NetIQ System Requirements document.

Choosing Directory Services

Choose one of directory services for NetIQ data. The NetIQ solution can operate with:

- Microsoft **Active Directory (AD DS)**.
- Microsoft **Active Directory Lightweight Directory Services (AD LDS)** formerly known as Microsoft **Active Directory Application Mode (ADAM)**, is a light-weight implementation of Active Directory.
- Novell **Domain Services for Windows (DSfW)** is a solution that allows server to act like an Active Directory service. In this case we also need to join one or some member servers based on Microsoft Windows Server platform to Domain and then configure Active Directory Lightweight Directory Services. So we have small differences between how to install and configure NetIQ using AD DS+AD LDS and how to install and configure NetIQ using Novell DSfW+AD LDS.

The installation procedure differs depending on the selected type of directory services.

Authenticore Servers

The NetIQ 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.

Recommended hardware requirements

- CPU: Intel Core 2 Duo 2.0 GHz.
- RAM: 2 GB.
- Free space on system partition of hard drive: 30 GB (for events and logs).

Operating system requirements

- Microsoft Windows Server 2003 Service Pack 2 x86/x64.
- Microsoft Windows Server 2003 R2 Service Pack 2 x86/x64.
- Microsoft Windows Server 2008 R2 Service Pack 1.
- Microsoft Windows Server 2012.

 It's not recommended to install NetIQ Authenticore Server on Domain Controllers due to necessity of restarting after any updating of NetIQ Authenticore Server or authentication providers.

Estimate optimal number of Authenticore Servers

You'll need to prepare one or some Member servers to install NetIQ Authenticore Server component.

There are certain rules for estimating optimal number of Authenticore Servers:

- not less than two Authenticore Servers in the domain to provide the minimal level of fault tolerance;
- not less than one Authenticore Server on each site;
- the minimal number of Authenticore Servers within one site is estimated according to the Microsoft recommendation concerning minimal number of Domain Controllers on the site;
- the number of Authenticore Servers can exceed the minimal number to increase the fault tolerance of the biometric authentication service for critical subsections;
- for small subsections, presented as separated sites, it is recommended to install Authenticore Server on Domain Controller directly to minimize expenses of purchasing additional equipment;
- to attain the maximum performance of Authenticore Server, install it on Domain Controller directly. In this case the average coefficient of the performance increase in comparison with the case of installation on Member Server can be calculated by the formula:

$$C_{performance_increase} = V_{bus}/V_{network},$$

where **V_bus** – the average speed of data transfer via hardware bus of the Domain Controller server, **V_network** – the average speed of data transfer via the network between Authenticore and Domain Controller.

Configuring an Environment that Includes AD LDS

If you chose AD LDS in case of AD or DSfW we need to prepare AD LDS instance at first.

The unique AD LDS must be configured the following way:

1. At the 1st step of wizard choose **A unique instance**.
2. At the 2nd step input an Instance name: **NAAF** and description: **AD LDS NAAF instance**.
3. At the 3rd step input LDAP port number: **50000** and SSL port number: **50001**.
4. At the 4th step select **Yes, create an application directory partition**, and then input Partition name: **CN=NAAF**.
5. Skip steps 5-7.
6. Finish the Active Directory Lightweight Directory Services configuring.

The additional AD LDS servers must be configured using this instruction:

1. At the 1st step of wizard select **A replica of an existing instance**.
2. At the 2nd step input an Instance name: **NAAF** and description: **AD LDS NAAF instance**.
3. At the 3rd step input LDAP port number: **50000** and SSL port number: **50001**.
4. At the 4th step press **Browse** and select the first server, then input LDAP port: **50000**.
5. Skip the 5th step.
6. At the 6th step please check the box on **CN=NAAF**.
7. Skip final steps 7-10.



It's recommended to configure additional AD LDS servers to provide good level of fault tolerance and increase performance. Check Microsoft's recommendations regarding AD LDS.

NetIQ Solution Deployment

Extending Schema

 For Windows Server 2003 before extending schema domain functional level should be raised to Windows Server 2003.

 Before extending schema please ensure that you have Remote Server Administration Tools installed on the server. Otherwise you may have a problem with Idifde.exe

1. Logon to Domain Controller or Member server as Domain Administrator and open **Autorun.exe**.
2. Click **Extend AD Schema**.
3. Select **Active Directory** or **ADAM/AD – LDS** according with your choice.
4. If you chosen ADAM/AD – LDS you'll need to input server with unique AD LDS instance in the Server name field.
5. Check the Port number and Root partition according on how you configured AD LDS instance.
6. Press **OK**. Then you'll need to press Enter on several occasions when needed.

 You can get an error after the fourth pressing of **Enter** button during extending schema in case of using Novell DSfW. Disregard it.

Group Policy Configuring

1. Open Group Policy Management console.
2. Create a new group policy object (GPO) NAAF and link it to entire domain if you didn't do that yet.
3. Open AAA GPO in Group Policy Management Editor and add the following administrative templates: **NAAF_Repository**, **NAAF_Repository_ADAM** (you can find the appropriate adm-files in \Tools\Policies\ folder of NetIQ distributive).

4. Browse the following path: Computer Configuration -> Policies -> Administrative Templates -> Classic Administrative Templates -> NetIQ Advanced Authentication Framework -> Repository.
5. Enable **Repository** policy with ADAM Instance default value.
6. Enable **ADAM Settings** policy with default settings: **CN=NAAF**.
7. If you use Novell DSfW you also need to enable a policy: **Enable Novell support**.

Installing and Configuring of First Authenticore Server

1. Add the server in **NetIQ Advanced Authentication Framework ADAM Servers** group.
2. Logon to server with privileges of Local Administrator + Authenticore Admins.
3. Open **Autorun.exe**.
4. Select Authenticore server and click **Install**. Use default settings for Authenticore Server installation - after the installation you get warning that includes recommendation to configure Enterprise Key and apply License.
5. Press **OK** at the **Enterprise Key backup copy** window.
6. Press **OK** at the **Creating Enterprise Key backup copy** window;
7. Select a path to secure place (it maybe a USB Flash Drive that is stored in safe deposit) and input a name for Enterprise Key file (you can also optionally set a password).
8. Apply your licenses.
9. Install all necessary NetIQ authentication providers.
10. If you use ADAM, write **sc config AAARS depend= ADAM_NAAF** in the command line after the installation is complete.
11. Restart the server.
12. Check the server state by watching on the NetIQ Authenticore Server tray manager icon.

 License should be applied during the installation of NetIQ Advanced Authentication Framework Authenticore Server. Otherwise other components will not be installed.

Selecting Cryptographic Algorithms

When you install Authenticore Server for the first time in the domain, Setup Wizard will prompt you to specify the Crypto Service Provider (CSP) type and to select the algorithms to generate the unique Enterprise Key.

The table below presents the accordance of the 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

Installing and Configuring of Additional Authenticore Server

1. Add the new server in **NetIQ Advanced Authentication Framework ADAM Servers** group.
2. Logon to server with privileges of Local Administrator + Authenticore Admins.
3. Open **Autorun.exe**.
4. Select Authenticore server and click **Install**. Use default settings for Authenticore Server installation.

5. Right click on NetIQ Authenticore Server tray manager icon, select **Enterprise Key - > Restore key...**
6. Agree with a question on Enterprise Key restoring – you'll see that the server is starting.
7. Press **OK** at the **Importing Enterprise Key backup copy** dialog window.
8. Apply existing Enterprise Key file (enk) from secure storage device.
9. Install all necessary NetIQ authentication providers.
10. If you use ADAM, write **sc config AAARS depend= ADAM_NAAF** in the command line after the installation is complete.
11. Restart the server.
12. Check the server state by watching on the Authenticore Server tray manager icon.
13. Repeat these actions for each additional Authenticore Server.

NetIQ Password Filter Installation

1. Logon to first Domain Controller.
2. Open **Autorun.exe**.
3. Install NetIQ Password Filter.
4. Restart Domain Controller.
5. Repeat these actions for each Domain Controller.

NetIQ Log Server Installation

1. Logon to server which you want to use as NetIQ Log Server.
2. Open **Autorun.exe**.
3. Install NetIQ Log Server.

4. Open AAA GPO in Group Policy Management Editor and add the administrative template **NAAF** (you can find an appropriate adm-file in \Tools\Policies\ folder of NetIQ distributive).
5. Browse the following path: Computer Configuration -> Policies -> Administrative Templates -> Classic Administrative Templates -> NetIQ Advanced Authentication Framework -> Event Log
6. Enable **Log Servers** policy. Specify Log Server name.
7. Configure other policies when needed.

NetIQ Administrator Workplace Configuring

1. Logon to server which you want to use as NetIQ administrator workplace. You also need to have Remote Server Administration Tools (RSAT) installed at the same servers.
2. Open **Autorun.exe**.
3. Install NetIQ Administrative Tools.
4. Install all necessary NetIQ authentication providers.
5. Delegate necessary permissions to NetIQ administrators by adding them into the Authenticore Admins group.
6. Delegate necessary permissions to NetIQ security officers by adding them into the NetIQ Advanced Authentication Framework Admins group.
7. Open AAA GPO in Group Policy Management Editor and browse the following path: Computer Configuration -> Policies -> Administrative Templates -> Classic Administrative Templates -> NetIQ Advanced Authentication Framework.
8. Configure other policies when needed.

NetIQ Client Installation

Install NetIQ Client and all necessary NetIQ authentication providers on each workstation where needed. It's urged to use Group Policy for installation and updating of NetIQ components on workstations. You can find the detailed instruction on how to configure mass installation via Group Policy in NetIQ Client Installation Guide.

NetIQ EAP Server

1. NetIQ EAP Server can be installed only on Microsoft Windows 2008 Server R2 Server Pack 1 with the installed NPS server.
2. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
3. Install NetIQ RTE.
4. Restart your server operation system.
5. Repeat the actions for each required server operation system.

NetIQ NPS Plugin

1. NetIQ NPS Plugin can be installed only on Microsoft Windows 2008 Server R2 Server Pack 1 and Microsoft Windows Server 2012 with the installed NPS Server. You also need to have NetIQ Authenticore Server installed on your computer.
2. Logon to first Domain Controller.
3. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
4. Install NetIQ NPS plugin.
5. Restart Domain Controller.
6. Repeat these actions for each Domain Controller.

NetIQ Web Service

1. Logon to first Domain Controller. You also need to have NetIQ Authenticore Server installed on your computer.
2. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
3. Install NetIQ Web Service.
4. Restart Domain Controller.

5. Repeat these actions for each Domain Controller.

NetIQ RTE Server

Operating system requirements:

- Microsoft Windows XP (x86) SP3/ Microsoft Windows 7 (x64/x86) SP1/ Microsoft Windows 8 (x86/x64);
- Microsoft Windows Server 2008 R2 SP1/ Microsoft Windows Server 2003 (x64/x86) SP2/ Microsoft Windows Server 2003 R2 (x64/x86) SP2; Microsoft Windows Server 2012.

1. NetIQ RTE can be installed on any workstation where NetIQ Client is not needed.
2. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
3. Install NetIQ RTE.
4. Restart your workstation.
5. Repeat the actions for each required workstation.

Troubleshooting

The AD LDS (ADAM) Replica Problem

Question: NetIQ is working correctly, but we are having issues with AD LDS replica. The Event log on the Primary server is getting loaded with Warnings stating: "The attempt to establish a replication link for the following writable directory partition failed."

It is also getting another error: "The directory server has failed to create the AD LDS serviceConnectionPoint object in Active Directory Lightweight Directory Services. This operation will be retried."

Answer: Please check the [following link](#).

The information from this topic indicates that the Instance Service is using a local user instead of a Domain user. That is not accurate. However, it is using Network Service as the user, which seemed like it should have been correct.

This is the case on both the Primary and Replica server.

Please change this user to the <Domain>\Administrator and the error will go away.

If you then got other errors please add Generate Audit rights to that user and also add it to the Domain Administrators Group, and restart the service. Please do it on the all servers you are using.

Index

A

Active Directory 6-7, 9-10, 17
Administrator 14, 17
Algorithms 12
Application 7
Authentication 1, 3-4, 6-7, 11-12, 14-16
Authenticator 3
Authenticore server 7, 11-12

C

Client 5, 14, 16
Create 10

D

Domain 6-8, 13, 15, 17

E

Enterprise Key 11, 13
Event Log 14

G

Generate 17

L

License 12
Logon 3, 10-15

M

Microsoft Windows Server 2003 8
Microsoft Windows Server 2008 8, 16
Microsoft Windows Server 2012 8

N

Network 4

P

Password 5, 13
Policy 10, 14

R

Remote 10, 14
RTE 5, 15-16

S

Server 4, 6, 10-13, 15
Settings 11
Software 5
System 4, 7

W

Windows 5, 7, 10, 12, 15
Windows XP 16