



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
NetIQ Solution Deployment	9
NetIQ Group Policy Templates	9
NetIQ Authenticore Server Configuration	10
Active Directory Domain Services	10
Active Directory Lightweight Domain Services	11
NetIQ Password Filter Installation	16
NetIQ Administrator Workplace Configuration	16
NetIQ Web Enrollment Wizard	16
NetIQ Web Service	17
NetIQ Access Manager Advanced Authentication Plugin	17
Troubleshooting	18
The AD LDS (ADAM) Replica Problem	18
Index	19

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 groups 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.

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

- **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 is necessary to synchronize passwords between domain services and NetIQ storage.

- **NetIQ Advanced Authentication Framework – Web Enrollment Wizard**

<CD drive>_webservice\wew.msi

This package contains NetIQ Web Enrollment Wizard component.


Web Enrollment Wizard allows users to enroll or manage authenticators from any place (workstation, laptop, tablet PC or smartphone) in the web browser, without necessity to install any software.

- **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. Administration Components

- **NetIQ Advanced Authentication Framework – Administrative Tools**

`<CD drive>_admtools\admtools.msi`


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

- **NetIQ Advanced Authentication Framework – Group Policy Templates**

`<CD drive>_admtools\grouppolicies.msi`

This package contains NetIQ Group Policy Templates components.

Group Policy Templates is a component that allows administrators to control the working environment of user accounts and computer accounts.

 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 is only exists in configurations with extended ADAM/AD LDS schema.

System Planning

Before installing the NetIQ Advanced Authentication Framework solution, please check whether 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)** which 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.



NetIQ supports SUSE Linux Enterprise Server 11 SP1 as Novell DSfW directory service.

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

Information on securing Microsoft Server 2003 Domain Controllers can be found here:

<http://technet.microsoft.com/en-us/library/cc875836.aspx>

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.



Authenticore Servers can be installed only on member servers, not on Domain Controllers. Installation of Authenticore Servers on Domain Controllers is not supported. In case of installation of Authenticore Servers on Domain Controllers, you can get the following issues:

1. Domain Controller has long startup (several minutes).
2. Authenticore Server and Log Server services cannot be started automatically.

Estimate optimal number of Authenticore Servers

You will 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.


NetIQ Solution Deployment

In this chapter:

- [NetIQ Group Policy Templates](#)
- [NetIQ Authenticore Server configuration](#)
- [NetIQ Password Filter installation](#)
- [NetIQ Administrator Workplace Configuration](#)
- [NetIQ Web Enrollment Wizard](#)
- [NetIQ Web Service](#)
- [NetIQ Access Manager Advanced Authentication Plugin](#)

NetIQ Group Policy Templates

 In case Active Domain Lightweight Domain Services (AD LDS) is selected as an applicable directory service, it is required to install NetIQ Group Policy Templates on the server with the installed AD LDS instance.


 NetIQ Group Policy Templates should be installed only on the server that will be used for administration and editing group policies.

Before installing NetIQ Group Policy Templates, please check whether Group Policy Management Console is installed on an applicable Domain Controller or Member Server.

To install NetIQ Group Policy Templates:

1. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
2. Install NetIQ Group Policy Templates.
3. Restart the server.

NetIQ Authenticore Server Configuration

 For Windows Server 2003: before Authenticore Server configuration, domain functional level should be raised to Windows Server 2003.


In this chapter:


- [Active Directory Domain Services](#)
- [Active Directory Lightweight Domain Services](#)

Active Directory Domain Services


The AD DS should be configured in the following way:

1. Log on to Domain Controller with **Domain Admins + Schema Admins** privileges.
2. Extend the schema for AD DS.

 The schema extension utility should be run from the local drive. There may occur problems in case of running it from the network drive.

 Necessary privileges are being delegated and attributes are being created in AD DS during the schema extension. The list of attributes is represented in the [List of attributes added for NetIQ Advanced Authentication Framework](#) chapter of the Knowledge Base.

3. Log on to Member Server with **Domain Admins** privileges.
4. Install Authenticore Server:
 1. Run **Autorun.exe**.
 2. Select **Authenticore Server** and click **Install**. Use default settings for Authenticore Server installation. After the installation, restart your computer.
 3. The service account and service groups are being created during the installation of Authenticore Server. For more information, see the [Service Accounts and Groups](#) chapter.

 Authenticore Servers can be installed only on Member Servers, not on Domain Controllers.

5. Verify whether Authenticore Server is added to the **Authenticore Servers** group.
6. Generate the Enterprise Key through **Authenticore Tray Manager** manually and save it securely.

In case of additional Authenticore Servers, AD DS should be configured in the following way:

7. Log on to the additional Member Server with **Local Admins + Authenticore Admins** privileges.
8. Install an additional Authenticore Server:
 1. Run **Autorun.exe**.
 2. Select **Authenticore Server** and click **Install**. Use default settings for Authenticore Server installation.
9. Verify whether an additional Authenticore Server is added to the **Authenticore Servers** group.
10. Get the existing Enterprise Key from the first Authenticore Server through **Authenticore Tray Manager** manually.

Active Directory Lightweight Domain Services



Before Authenticore Server configuration, please ensure that you have Remote Server Administration Tools installed on the server. Otherwise there may occur problems with **ldifde.exe**.

Please follow the instructions to prepare your environment for the NetIQ deployment (privileged admins permissions required).

1. Open Active Directory Users and Computers. Click **View** and select **Advanced Features**.
2. Browse to the **Users** container.
3. Create a Global Security Group named **Authenticore Admins**.
4. Assign users and groups to manage the NetIQ Authenticore Servers. Add a user account which will perform deployment of Authenticore Servers.
5. Create a Global Security Group named **NetIQ Advanced Authentication Framework Admins**.
6. Assign users and groups to manage/enroll NetIQ users, ensure that your user account is a member of this group.
7. Create a Global Security Group named **Authenticore Servers**.
8. Create a Global Security Group named **NetIQ Advanced Authentication Framework ADAM Servers**.
9. Create an account named **AuthenticoreService**, set the **Password never expires** option.
10. Right-click the account. Select **Properties**. The **Properties** window will be displayed.
11. Click the **Security** tab.
12. Click the **Advanced** button.
13. Click the **Add** button in the **Permissions** tab of the **Advanced Security Settings** window.

14. Select principal object type.
15. In object name field, enter username of an account which will perform Authenticore Servers deployment. Click **OK**.
16. In the **Permissions** list, please check the options **Change password** and **Reset password**. Click **OK**.
17. In the **Advanced Security Settings** window, click **OK**. Close properties window.
18. Choose servers on which you will install the Authenticore Servers. Open properties of the servers, switch to the **Delegation** tab.
19. Enable the **Trust this computer for delegation to any service (Kerberos only)** option. Apply changes.
20. Add the servers to the **Authenticore Servers** and **NetIQ Advanced Authentication Framework ADAM Servers** groups.
21. Configure NetIQ policies:
 1. Run **Autorun.exe** from NetIQ Advanced Authentication Framework distributives folder.
 2. Install the **Group policy templates**.
 3. Create a new Group Policy Object which will be applied on all servers and workstations with NetIQ components installed. Edit the GPO.
 4. Browse the following path: **Computer Configuration -> Policies -> Administrative Templates -> NetIQ Advanced Authentication Framework Repository -> Repository**.
 5. Enable the **Repository** policy with the **ADAM Instance** default value.
 6. Switch to: **Computer Configuration -> Policies -> Administrative Templates -> NetIQ Advanced Authentication Framework ADAM -> Repository**.
 7. Enable **ADAM Settings** policy with default settings: **CN=NAAF**, ADAM server port number: **50000**. If you use Novell Domain Services for Windows, you also need to enable the **Enable Novell support** policy.

On the server on which you will install the first Authenticore Server, please perform the following actions:


1. Add a user account which will perform the deployment of Authenticore Servers to the group of local administrators.
2. Log off and logon back to apply the permissions.
3. Add the Active Directory Lightweight Directory Services role (For more information, see: [http://technet.microsoft.com/en-us/library/cc754486\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754486(v=ws.10).aspx)).
4. Create an AD LDS instance:
 1. On the **Setup Options** page of the wizard, select **A unique instance**. Click **Next**.

2. On the **Instance Name** page, input the instance name: **NAAF** and description: **AD LDS NAAF instance**. Click **Next**.
 3. On the **Ports** page, input the LDAP port number: **50000** and SSL port number: **50001**. Click **Next**.
 4. On the **Application Directory Partition** page, select **Yes, create an application directory partition**, and then input partition name: **CN=NAAF**. Click **Next**.
 5. On the **File Locations** page, view the installation directories. Do not change them. Click **Next**.
 6. On the **Service Account Selection** page, the **Network Service** account value will be selected by default. Do not change it. Click **Next**.
 7. On the **AD LDS Administrators** page, select **This account**, click **Browse** and specify **NetIQ Advanced Authentication Framework Admins** group. Click **Next**.
 8. On the **Importing LDIF Files** page, do not import any LDIF file. Click **Next**.
 9. On the **Ready to Install** page, review your installation selections. Click **Next**.
 10. Finish the Active Directory Lightweight Directory Services configuration.
5. Run **Autorun.exe** from NetIQ Advanced Authentication Framework distributives folder, click **Extend AD Schema**.
 6. Switch to **ADAM/AD – LDS**. Check the configuration settings and click **OK**.
 7. Follow the schema extension.
 8. Log off and logon back to apply the permissions.
 9. Run **Autorun.exe** from NetIQ Advanced Authentication Framework distributives folder.
 10. Install the Authenticore Server.
 11. To make Authenticore Server start only when AD LDS is loaded, run the following command:

```
sc config NAAFERS depend=
RpcSS/NetLogon/SamSS/RpcLocator/NAAFKeystorage/NAAFLogBroker/ADAM_NAAF
```
 12. Restart the server in order to finish the installation of the Authenticore Server.
 13. Log on. Click **Start** button. Find and run the **Authenticore Tray Manager**.
 14. Right-click the Authenticore Tray Manager tray icon. Select **Enterprise Key -> Generate new key**.
 15. Click **Yes** to confirm the Enterprise Key generation.
 16. Click **OK** in **Enterprise Key settings** window to apply cryptography settings.
 17. Create a backup copy of the Enterprise Key.
 18. Save securely the copy of the Enterprise Key.
 19. Right-click the **Authenticore Tray Manager** tray icon. Select **License management**.
 20. In the **License management** window, click **Add**. Browse for a license file. Apply the license.
 21. Delegate rights to the **NetIQ Advanced Authentication Framework Admins** group in the following way: DSACLs \\<LDSServerAddress>:<LDSPortNumber>\<InstanceName>

/G "<DomainName>\NetIQ Advanced Authentication Framework:GA" /I:T
E.g., DSACLs \\localhost:50000\cn=NAAF /G "TestDomain\NetIQ Advanced Authentication Framework Admins:GA" /I:T

22. Ask your privileged administrator to apply the NetIQ policy (done in point 5) to all servers and workstations with NetIQ components installed.


 It is recommended to configure at least one additional Authenticore Server to provide a good level of fault tolerance, load balancing and increase performance. To decide how many Authenticore Servers you need please follow the Microsoft's recommendations regarding number of Domain Controllers.

On the server on which you will install an additional Authenticore Server please do the following:

1. Add a user account which will perform the deployment of Authenticore Servers to the group of local administrators.
2. Log off and logon back to apply the permissions.
3. Add the Active Directory Lightweight Directory Services role.
4. Create a replica of AD LDS instance:
 1. On the **Setup Options** page of the wizard, select **A replica of an existing instance**. Click **Next**.
 2. On the **Instance Name** page, input the instance name: **NAAF** and description: **AD LDS NAAF instance**. Click **Next**.
 3. On the **Ports** page, input the LDAP port number: **50000** and the SSL port number: **50001**. Click **Next**.
 4. On the **Joining a Configuration Set** page, click Browse... and select the first server, then input the LDAP port: 50000. Click **Next**.
 5. On the **Administrative Credentials for the Configuration Set** page, select **This account** and enter **Username** and **Password** for NetIQ administrator. Click **Next**.
 6. On the **Copying Application Directory Partitions**, select the **CN=NAAF** checkbox. Click **Next**.
 7. On the **File Locations** page, view the installation directories. Do not change them. Click **Next**.
 8. On the **Service Account Selection** page, the **Network Service** account value will be selected by default. Do not change it. Click **Next**.
 9. On the **AD LDS Administrators** page, select **This account**, click **Browse** and specify **NetIQ Advanced Authentication Framework Admins** group. Click **Next**.
 10. On the **Ready to Install** page, review your installation selections. Click **Next**.

11. Finish the Active Directory Lightweight Directory Services configuration.
5. Run **Autorun.exe** from NetIQ Advanced Authentication Framework distributives folder.
6. Install the Authenticore Server.
7. To make Authenticore Server start only when AD LDS is loaded, run the following command:
sc config NAAFERS depend=
RpcSS/NetLogon/SamSS/RpcLocator/NAAFKeystorage/NAAFLogBroker/ADAM_NAAF
8. Restart the server in order to finish the installation of the Authenticore Server.
9. Log on. Click **Start** button. Find and run **Authenticore Tray Manager**.
10. Right-click the **Authenticore Tray Manager** tray icon. Select **Enterprise Key -> Restore key**.
11. Apply an existing Enterprise Key from a first Authenticore Server.

NetIQ Password Filter Installation

 NetIQ Password Filter is an obligatory component for:


- OATH OTP Authentication Provider
- Smartphone Authentication Provider
- NPS Plugin
- NetIQ Access Manager Advanced Authentication Plugin
- NetIQ Cloud Access

1. Log on to first Domain Controller.
2. Open **Autorun.exe**.
3. Install NetIQ Password Filter.
4. Restart the server.
5. Repeat these actions for each required Domain Controller of a domain in which you are deploying NetIQ.

NetIQ Administrator Workplace Configuration

1. Log on 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 to 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 NAAF GPO in **Group Policy Management Editor** and browse the following path: **Computer Configuration -> Policies -> Administrative Templates -> NetIQ Advanced Authentication Framework**.
8. Configure other policies when needed.

NetIQ Web Enrollment Wizard

 NetIQ Web Enrollment Wizard is not related to obligatory components.


1. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
2. Install NetIQ Web Enrollment Wizard.
3. Restart the server.
4. Repeat these actions for each required server.

NetIQ Web Service

 NetIQ Web Service is not related to obligatory components.

1. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
2. Install NetIQ Web Service.
3. Restart the server.
4. Repeat these actions for each required server.

NetIQ Access Manager Advanced Authentication Plugin

 Root permissions are required for the installation of NetIQ Access Manager Advanced Authentication Plugin.

1. Install NAMAAPPluginSetup.jar to the `/opt/novell` folder on NetIQ Access Manager.
2. After the installation is started and the *"Welcome to the installation of NetIQ Access Manager – Advanced Authentication Plugin"* text is displayed, press 1 to continue.
3. After the *"Consider it as a license..."* text, press 1 to accept.
4. When you are suggested to select target path, enter `opt/novell`.
5. If the directory already exists and is not empty, press 1 to continue, if you confirm the installation and deleting all existing files.
6. Select the packs you want to install. Input 1 to select the required pack, 0 – to deselect the pack.
7. After the pack selection is done, press 1 to continue.
8. NetIQ Access Manager Advanced Authentication Plugin was installed successfully on `/opt/novell`.
9. Required authentication methods should be configured in accordance with NAM AA Plugin - Installation Guide.

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

Account 13
Active Directory 6-7, 10-11, 18
Administrator 9, 16, 18
Application 7, 13
Authentication 1, 3-4, 6-7, 9, 11, 16-17
Authenticator 3
Authenticore server 8
Authenticore Tray Manager 10, 13

C

Console 9
Create 11

D

Domain 6-10, 12, 16, 18

E

Edit 12
Enterprise Key 11, 13

F

File 13

G

Generate 10, 18

L

License 13
List 10
Local 11
Logon 3

N

Network 13

O

OATH 16

P

Password 4, 9, 11, 16
Policy 5, 9, 12, 16
Properties 11

R

Remote 16
Reset 12
Restore 15

S

Security 11
Server 4, 6-7, 9-11
Settings 11
System 4, 7

U

Username 14

W

Windows 7, 10