NetIQ Advanced Authentication Framework

Deployment Guide

Version 5.1.0

Table of Contents

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

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 - 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 auhtentication servers to host plug-in modules for current and future authentication methods.

- **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 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.

3. Client

- **NetIQ Advanced Authentication Framework – Client**

<CD drive>_client\client.msi
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.

- **NetIQ Advanced Authentication Framework - VDA Shell**

<CD drive>_vdashell\vdashell.msi

This package contains NetIQ VDA Shell component.

VDA Shell allows to use pre-session and in-session authentication for the following terminal server connections: Microsoft RDP, Citrix XenApp, VMware View on thin clients.

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

6

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 direct ory 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.

❇ It is recommended to deploy the Authenticore Servers in Active Directory sites with at least one Domain Controller available, because the Authenticore Server connects random Domain Controller in the same Active Directory site and if Domain Controllers are not available in the same site, Authenticore Server will go to a random Domain Controller.

❇ 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

Architecture Examples

In this chapter:

- Basic architecture
- Remote access architecture
- 802.1x architecture
- VDI architecture
- Enterprise architecture

Basic Architecture

This diagram shows a basic architecture with NetIQ Advanced Authentication Framework. It provides strong authentication for desktops connected to an Active Directory domain with full fail-over for the NetIQ backend servers.

Domain Controller
NAA Password Filter

NAA Server(s)
NAA Authenticore Server
Authentication Providers

Client
NAA Client
Authentication Provdiers

NetIQ Password Filter is installed on the Domain Controller.

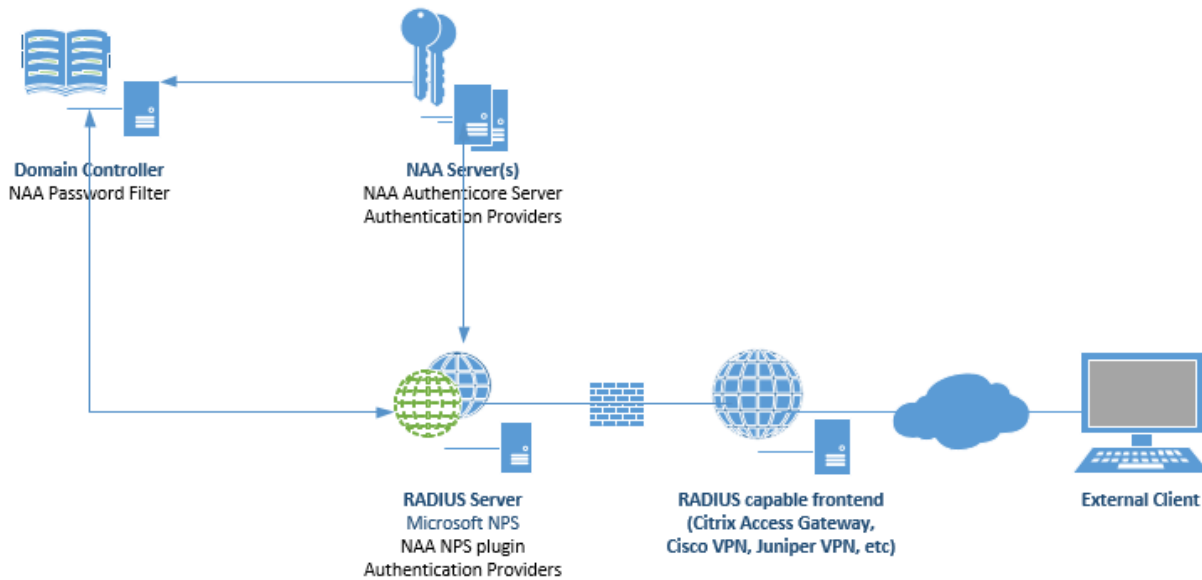The following components are installed on NetIQ Server(s):

- Authenticore Server;
- Authentication Providers.

The following components are installed on the Client:

- NetIQ Client;
- Authentication Providers.

Remote Access Architecture

In this section a Standard Installation example is shown with NetIQ being used for Remote access using RADIUS authentication. Whereas a possibility is to install all necessary NetIQ components on the RADIUS server itself, the example below illustrates another scenario where the RADIUS Protection component is installed on the RADIUS server and the remaining components are installed on a separate server.

NetIQ Password Filter is installed on the Domain Controller.

The following components are installed on Authenticore Server(s):
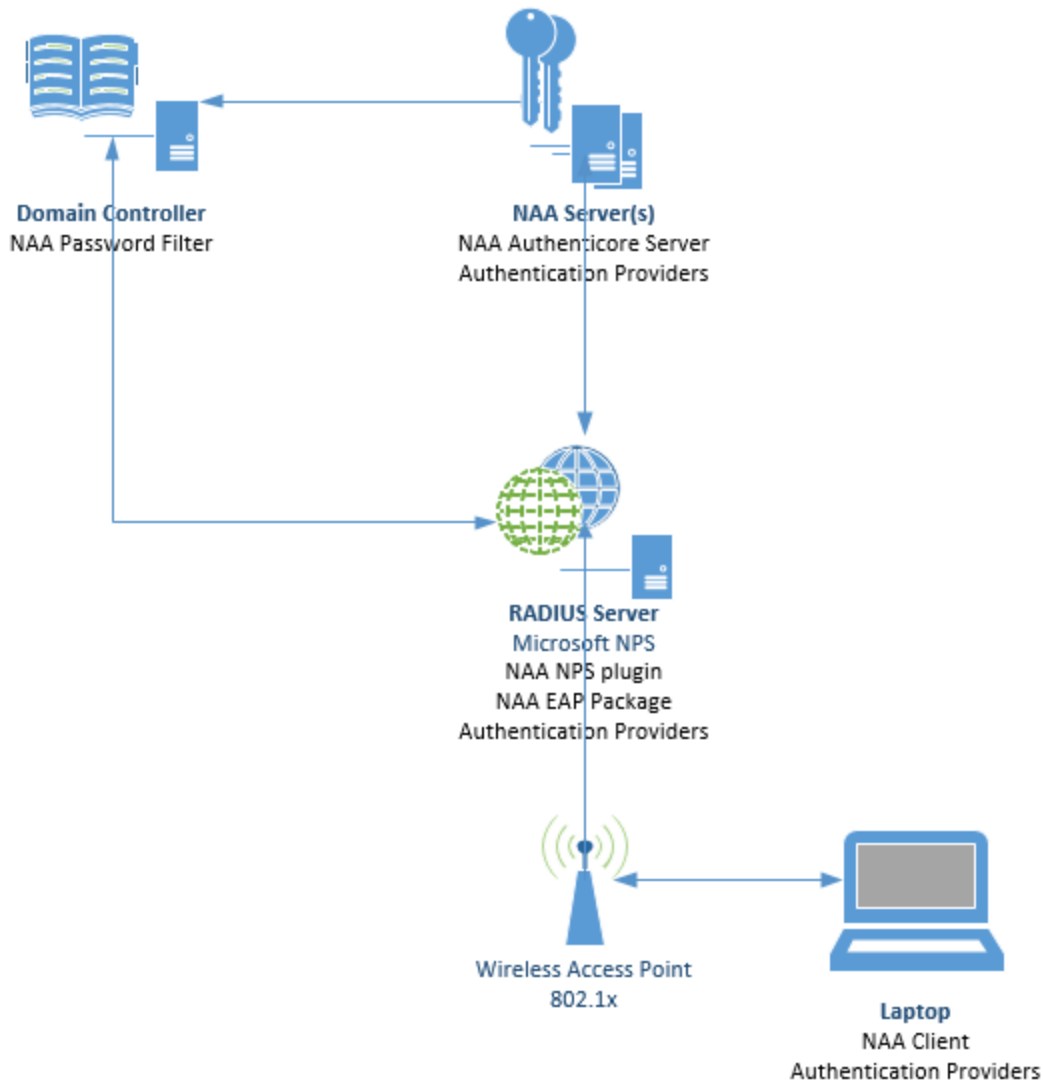
- Authenticore Server;
- Authenticore Providers.

The following components are installed on the RADIUS Server:

- NetIQ NPS plugin;
- Authentication Providers.

802.1x Architecture

NetIQ is suited to do 802.1x user authentication on supported access points. These can be wireless or wired. An end user device will need to do a user authentication to the network even before an IP-address is retrieved from the DHCP server. This results in very high security. After a successful authentication the end-user device will get an IP address and is automatically logged on into the domain. This way the 802.1x authentication is transparent for the user.

Domain Controller
NAA Password Filter

NAA Server(s)
NAA Authenticore Server
Authentication Providers

RADIUS Server
Microsoft NPS
NAA NPS plugin
NAA EAP Package
Authentication Providers

Wireless Access Point
802.1x

Laptop
NAA Client
Authentication Providers

NetIQ Password Filter is installed on the Domain Controller.

The following components are installed on NetIQ Server(s):

- Authenticore Server;
- Authentication Provider.

The following components are installed on the RADIUS NPS:
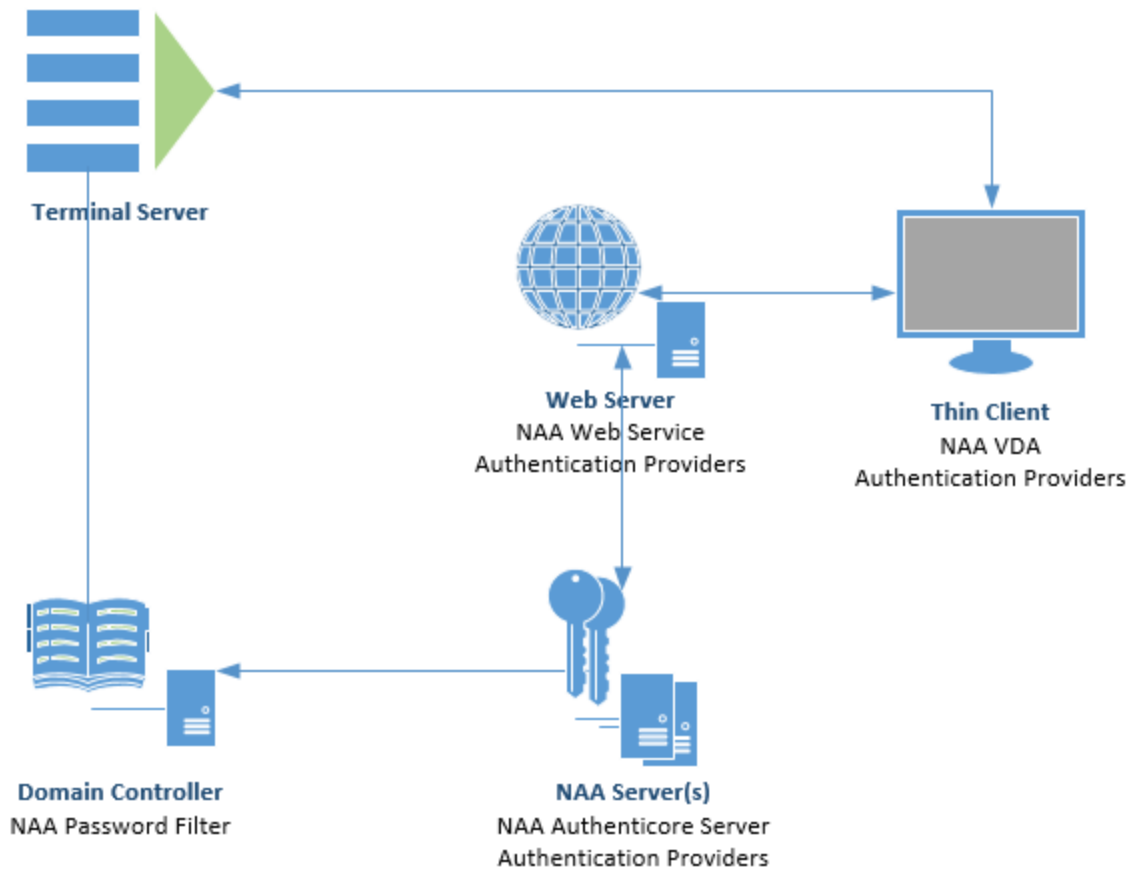
- NetIQ NPS plugin;
- EAP Package;
- Authentication Providers.

The following components are installed on the workstation:

- NetIQ Client;
- Authentication Providers.

VDI Architecture

In this section NetIQ is used to do pre-session authentication to a VDI infrastructure. This can be Microsoft RDS, Citrix XenApp, Citrix XenDesktop and VMware Horizon View. Thin clients which are not connected to the domain will communicate with NetIQ Authenticore through the NetIQ webservice and after a successful authentication will logon to the VDI infrastructure.

Terminal Server

Web Server
NAA Web Service
Authentication Providers

Thin Client
NAA VDA
Authentication Providers

Domain Controller
NAA Password Filter

NAA Server(s)
NAA Authenticore Server
Authentication Providers

NetIQ Password Filter is installed on the Domain Controller.

The following components are installed on the Web Server:

- NetIQ Web Service;
- Authentication Providers.

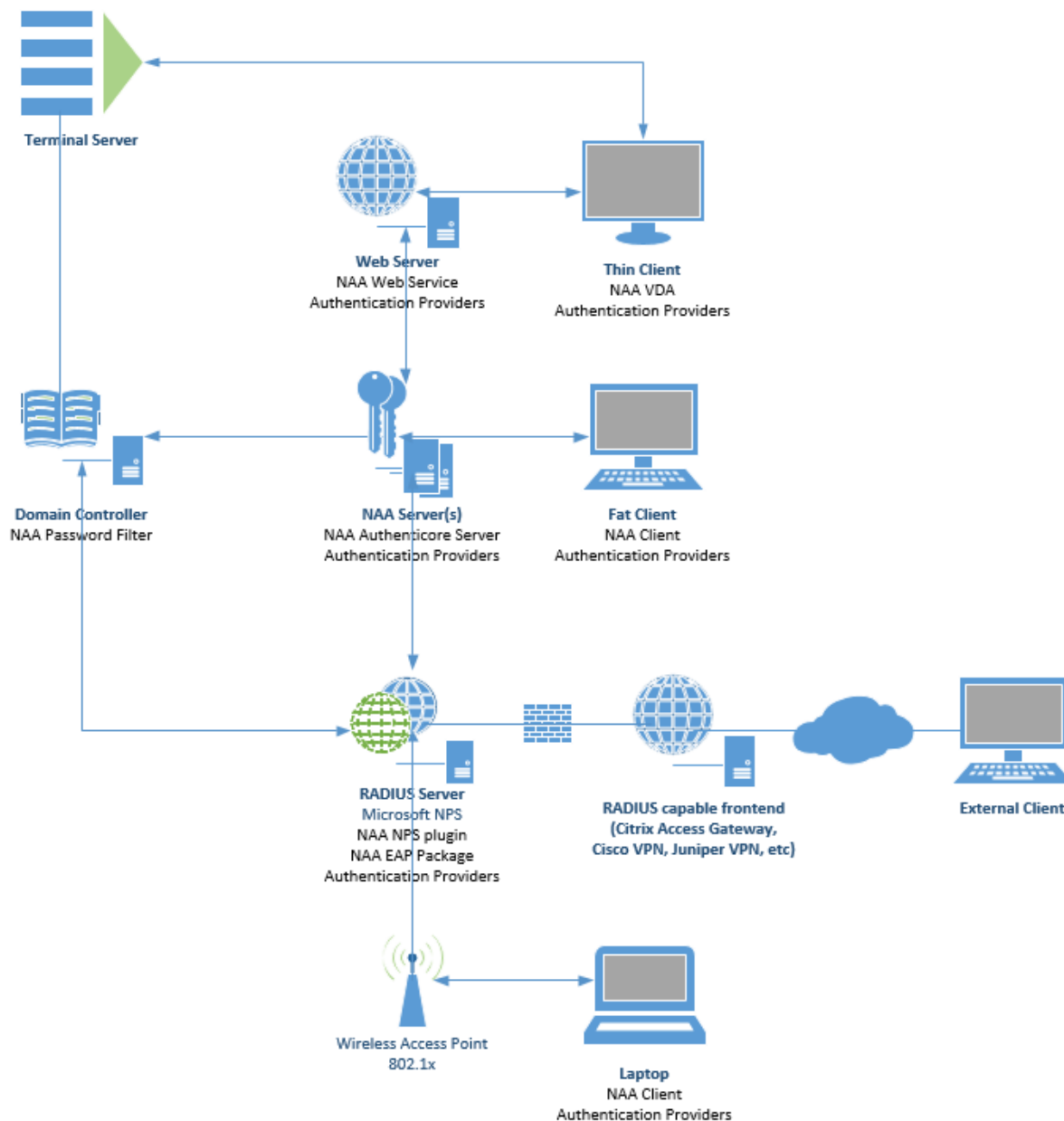The following components are installed on NetIQ Server(s):

- Authenticore Server;
- Authentication Providers.

The following components are installed on the Thin Client:

- NetIQ VDA;
- Authentication Providers.

Enterprise Architecture

In this section an example is given of a full featured enterprise architecture with all components of NetIQ Advanced Authentication Framework. In this scenario NetIQ is used for strong authentication on connected fat clients in the domain, 802.1x authentication on wireless hotspots, RADIUS authentication for remote access and VDA authentication for a VDI environment using thin clients not connected to the Active Directory Domain.

NetIQ Password Filter is installed on the Domain Controller.

The following components are installed on NetIQ Server(s):

- Authenticore Server;
- Authentication Providers.

The following components are installed on the Web Server:

- NetIQ Web Server;
- Authentication Providers.

The following components are installed on the Fat Client:

- NetIQ Client;
- Authentication Providers.

The following components are installed on the Thin Client:

- NetIQ VDA;
- Authentication Providers.

The following components are installed on the workstation:

- NetIQ Client;
- Authentication Providers.

NetIQ Solution Deployment

In this chapter:

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

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.
7. Install applicable authentication providers.
8. Restart the Authenticore Server.

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

9. Log on to the additional Member Server with **Local Admins + Authenticore Admins** privileges.
10. Install an additional Authenticore Server:

    1. Run **Autorun.exe.**
    2. Select **Authenticore Server** and click **Install**. Use default settings for Authenticore Server installation.

11. Verify whether an additional Authenticore Server is added to the **Authenticore Servers** group.
12. Use an existing Enterprise Key file to restore it through **Authenticore Tray Manager** manually.
13. Install applicable authentication providers.
14. Restart the Authenticore Server.

Active Directory Lightweight Domain Services

In this chapter:

- [Installing AD LDS With Minimum Privileges](#) - a number of steps of the installation should be preliminary performed by the user with Domain Admins privileges. E.g., creating service accounts and groups, installing NetIQ Group Policy Templates. All other steps can be performed by the user with minimum privileges.
- [Installing AD LDS With Domain Admins Privileges](#) - installation is performed easier and faster, and requires fewer steps.

Installing AD LDS With Minimum Privileges

⊗ 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.

   ⊗ If you deploy Advanced Authentication in parent domain and plan to use it for users in child domains, it's required to add AuthenticoreService account to members of Enterprise Admins group.

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**. Verify whether the **Change Password** and **Reset password** checkboxes are selected. Close the **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.

⊛ If you don't have sufficient privileges to install NetIQ Group Policy Templates, please edit local group policies on the Authenticore Server with **gpedit.msc**.

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 and the AuthenticoreServer account to the group of local administrators.
2. Log off and logon back to apply the permissions.
3. Add the Active Directory Lightweight Directory server role (For more information, see: 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 NAAFRS 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.
23. Install applicable authentication providers.
24. Restart the Authenticore Server.

✴ 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** page, 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 NAAFRS 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.
12. Install applicable authentication providers.
13. Restart the Authenticore Server.

Installing AD LDS With Domain Admins Privileges

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

The unique AD LDS should be configured in the following way:

1. Create Universal Security group named **NetIQ Advanced Authentication Framework Admins** in the **Users** container.
2. Log in to Member Server with NetIQ Admins or Domain Admins privileges.
3. Install **NetIQ Group Policy Templates**.
4. Install AD LDS server role (For more information, see: http://technet.microsoft.com/en-

© NetIQ

us/library/cc754486(v=ws.10).aspx).

5. Create an AD LDS instance:

   1. On the **Setup Options** page of wizard, select **A unique instance**. Click **Next**.
   2. On the **Instance Name** page, input an instance name: **NAAF** and description: **AD LDS NAAF instance**. Click **Next**.
   3. On the **Ports** page, input 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. Do not perform any actions on the **File Locations** and **Service Account Selection** pages. Click **Next**.
   6. On the AD LDS Administrator's page, select **This account**, click **Browse** and specify **NetIQ Advanced Authentication Framework Admins** group. Click **Next**.
   7. Do not perform any actions on the **Importing LDIF Files** and **Ready to Install** pages. Click **Next**.
   8. Finish the Active Directory Lightweight Directory Services configuration.

✪ At the end of AD LSD instance creation, it may be required to specify the account and password of the user who is the member of the **NetIQ Advanced Authentication Framework Admins** group.

   6. Open **Group Policy Management Console**.
   7. Create a new group policy object (GPO) **NAAF** and link it to the entire domain if you have not done that yet.
   8. Browse the following path: **Computer Configuration -> Policies -> Administrative Templates -> NetIQ Advanced Authentication Framework -> Repository**.
   9. Enable the **Repository** policy with the **ADAM instance** default value. Enable the **ADAM Settings** policy with the default settings: **CN=NAAF**, ADAM server port number: **50000**. If you use Novell DSfW, the **Enable Novell support** policy should be also enabled.
   10. Apply the policies on the Member Server.
   11. Extend the schema for AD LDS.

✪ Schema extension should be performed on the server with the configured AD LDS instance.

   12. Install Authenticore Server:

   1. Open **Autorun.exe**.

2. Select **Authenticore Server** and click **Install**. Use default settings for Authenticore Server installation. After the installation, restart your computer.

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

13. Verify whether Authenticore Server is added to the **Authenticore Servers** group.
14. Verify that Authenticore Server is added to the **NetIQ Advanced Authentication Framework ADAM Servers** group.
15. Verify that NetIQ administrator added to the **Authenticore Admins** group.
16. Log in to Member Server as user with LDS Admins privileges or Domain Admins privileges.
17. Generate the Enterprise Key and apply the license.
18. Save securely the copy of the Enterprise Key.
19. Install applicable authentication providers.
20. Restart the Authenticore Server.

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

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

1. Log in to the additional Member Server with NetIQ Admins or Domain Admins privileges (NetIQ administrator should be added to the **Local Admins** group).
2. Install AD LDS server role (For more information, see: http://technet.microsoft.com/enus/library/cc754486(v=ws.10).aspx).
3. Configure replica for 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 an instance name: **NAAF** and description: **AD LDS NAAF instance**. Click **Next**.
   3. On the **Ports** page, input LDAP port number: **50000** and SSL port number: **50001**. Click **Next**.
   4. On the **Joining a Configuration Set** page, click **Browse** and select the first server, then input 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** page, select the **CN=NAAF** checkbox. Click **Next**.

7. Do not perform any actions on the **File Locations** and **Service Account Selection** pages. Click **Next**.
8. On the **AD LDS Administrators** page, select **This account**, click **Browse** and specify **NetIQ Advanced Authentication Framework Admins** group. Click **Next**.
9. On the **Ready to Install** page, review your installation selections. Click **Next**.
10. Finish the Active Directory Lightweight Directory Services configuration.

4. Log in to the additional Member Server with Domain Admins privileges.
5. Install an additional Authenticore Server:

   1. Log in to server with Domain Admins/Local Admins+ Authenticore Admins privileges.
   2. Open **Autorun.exe**.
   3. Select **Authenticore Server** and click **Install**. Use default settings for Authenticore Server installation.

6. Verify whether an additional Authenticore Server is added to the Authenticore Servers group.
7. Verify that the Member Server added to the **NetIQ Advanced Authentication Framework ADAM Servers** group. Verify whether the **Trust this computer for delegation to any service** option is selected at the **Delegation** tab in ADUC (for Kerberos only).
8. Use an existing Enterprise Key file to restore it through **Authenticore Tray Manager** manually.
9. Install applicable authentication providers.
10. Restart the 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 EAP Server

⊗ NetIQ EAP Server is not related to obligatory components.

1. NetIQ EAP Server can be installed only on NPS server.
2. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
3. Install NetIQ EAP Server.
4. Restart the server.
5. Repeat the actions for each required server.

NetIQ NPS Plugin

NetIQ NPS Plugin is not related to obligatory components.

1. NetIQ NPS Plugin can be installed only on NPS Server. 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 NPS plugin.
4. Restart the server.
5. Repeat the actions for each required server.

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 RTE

1. NetIQ RTE can be installed on any workstation or server.
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.

NetIQ Client Installation

⊗ Please install NetIQ Client on several test workstations first. Proceed to mass installation only after internal testing.

Install NetIQ Client and all necessary NetIQ authentication providers on each workstation where needed. It is 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 Client - Installation Guide.

⊗ In order to permit client-server interaction, it is necessary to configure permissions for TCP port 135 and Dynamic RPC (for more information please check MSDN).

NetIQ VDA

1. NetIQ RTE can be installed on any workstation or server.
2. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
3. Install NetIQ VDA.
4. Restart your workstation.
5. Repeat the actions for each required workstation.

NetIQ Access Manager Advanced Authentication Plugin

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

1. Install NAMAAPluginSetup.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.

NetIQ SecureLogin Advanced Authentication Plugin

Before the installation of NSL AA Plugin make sure that **Client** or **RTE**, at least one **authentication provider** and **Novell SecureLogin** are already installed on your computer. Otherwise the installation of NSL AA Plugin will be impossible.

1. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.
2. Install NetIQ NSLPlugin.
3. Restart the workstation.
4. Repeat these 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