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.

ℹ️ **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**

© NetIQ

<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.

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.

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 failover 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):
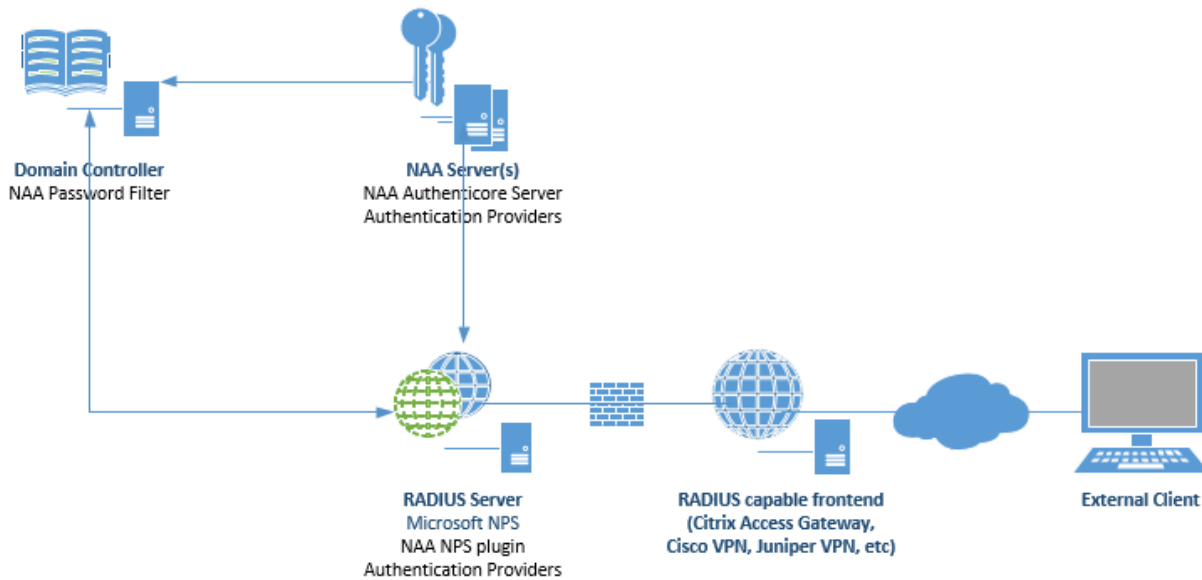
- Authenticore Server;
- Authentication Providers.

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.

Domain Controller
NAA Password Filter

NAA Server(s)
NAA Authenticore Server
Authentication Providers

RADIUS Server
Microsoft NPS
NAA NPS plugin
Authentication Providers

RADIUS capable frontend
(Citrix Access Gateway,
Cisco VPN, Juniper VPN, etc)

External Client

NetIQ Password Filter is installed on the Domain Controller.

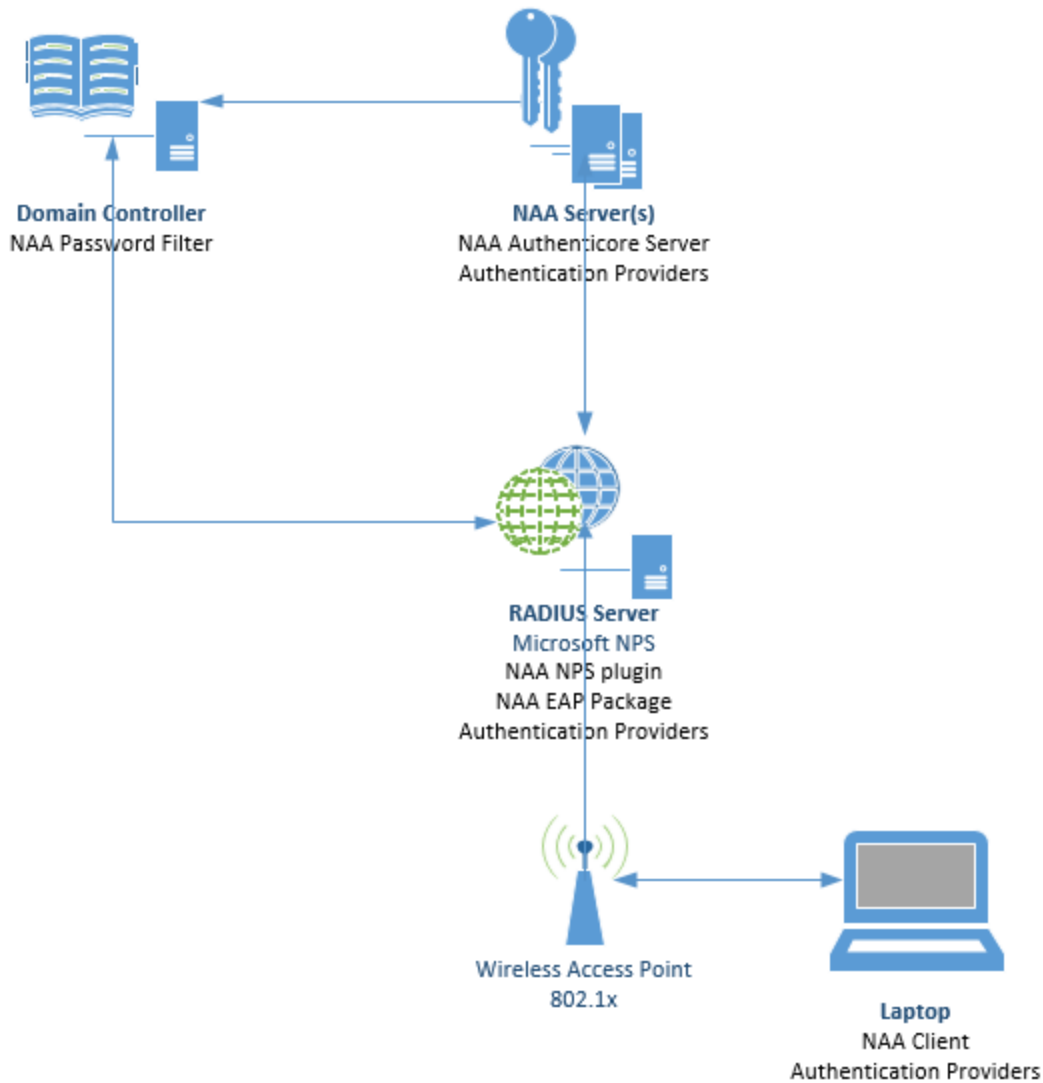The following components are installed on Authenticore Server(s):

- 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.

NetIQ Password Filter is installed on the Domain Controller.

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

- Authenticore Server;
- Authentication Provider.

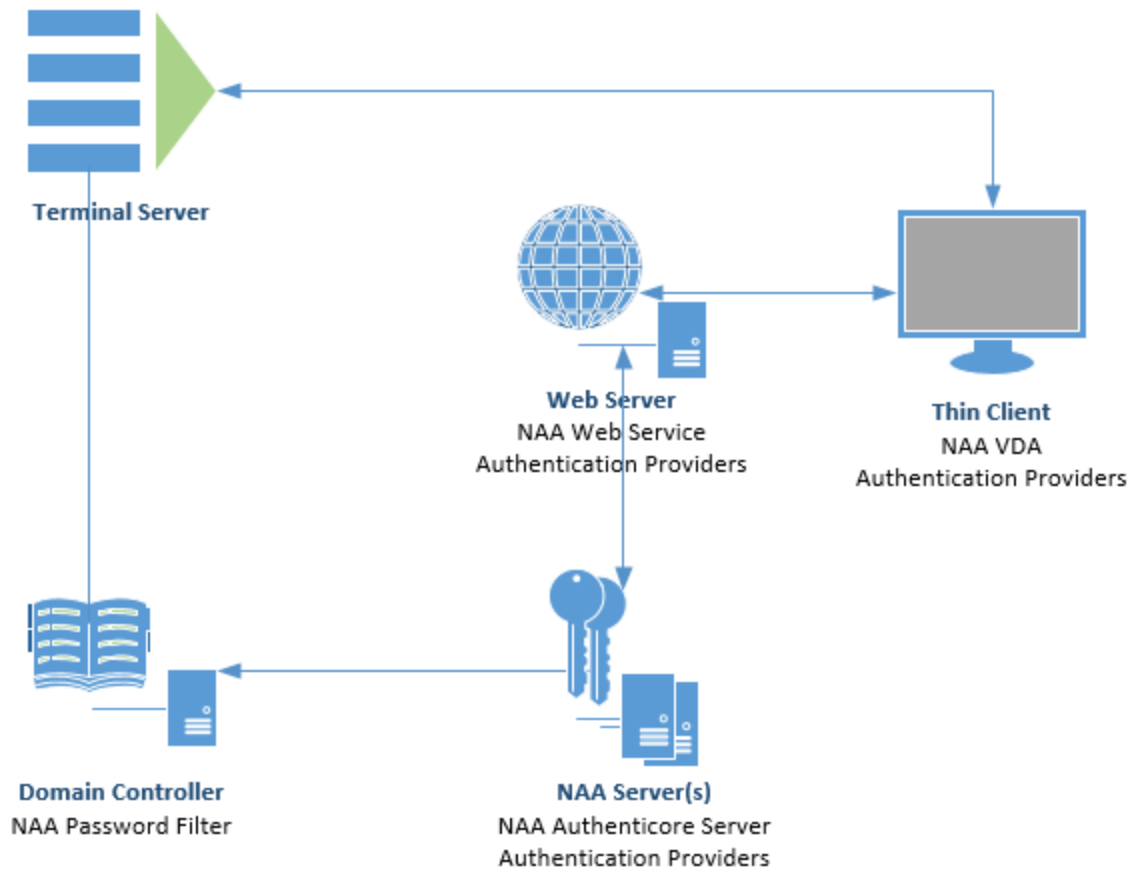The following components are installed on the RADIUS NPS:

- 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.

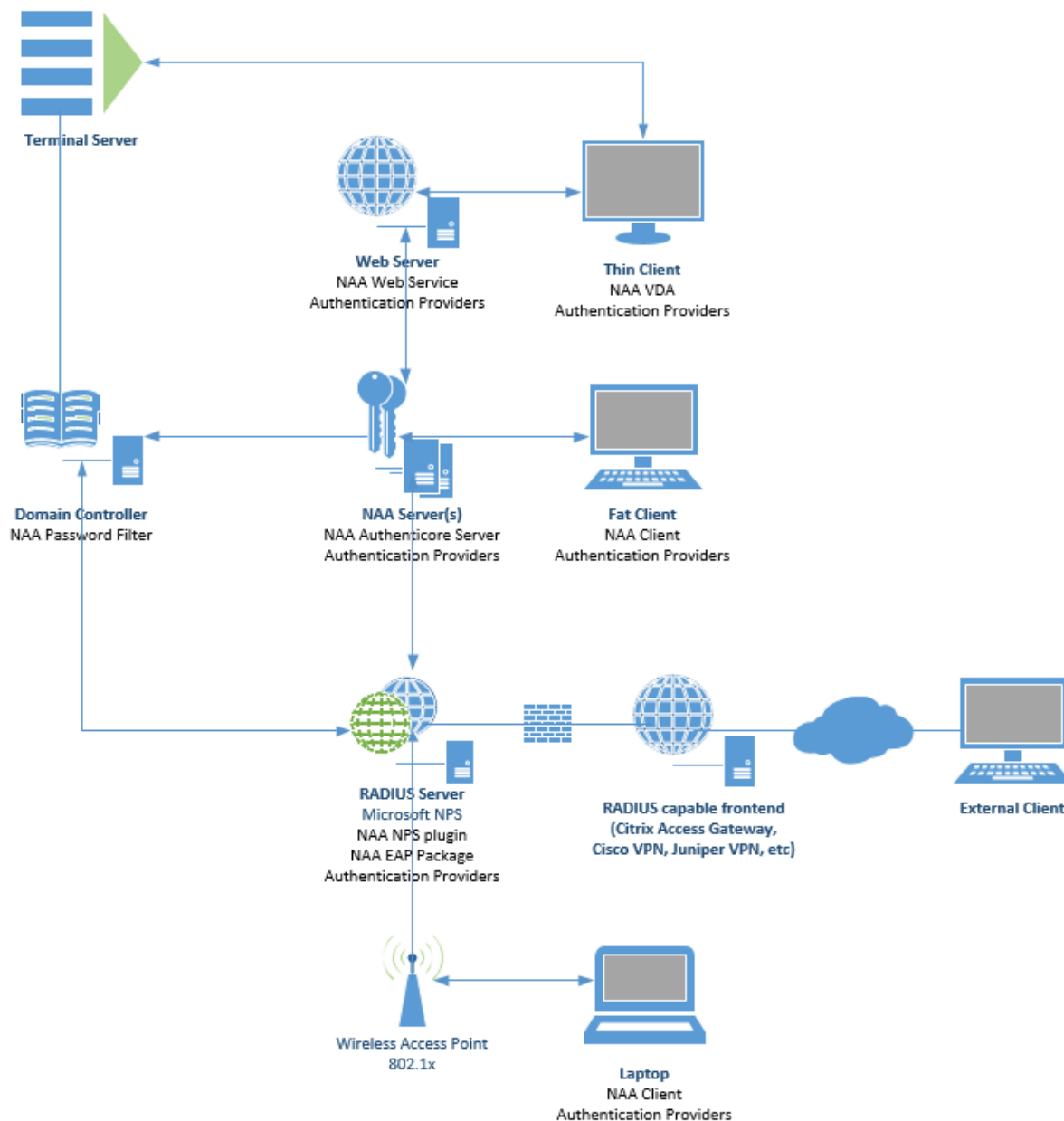The following components are installed on NetIQ Server(s):

- Authenticore Server;
- Authentication Providers.

15

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.

© NetIQ

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

Group Policy Templates should be installed on Domain Controller or Member Server with Group Policy Management Console already installed on it.

1. Open **Autorun.exe** from NetIQ Advanced Authentication Framework distribution kit.

2. Install NetIQ Group Policy Templates.

3. Restart the server.

4. Repeat these actions for each required 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.

ℹ 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. Open **Autorun.exe**.
> 2. 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.
> 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. 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.

5. Generate the Enterprise Key and save it securely.

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

6. Log on to the additional Member Server with **Local Admins + Authenticore Admins** privileges.

7. Install additional Authenticore Server:

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

8. Get the existing Enterprise Key from the first Authenticore Server through the **Authenticore Tray Manager** icon.

Active Directory Lightweight Domain Services

✱ 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 **NetIQ Advanced Authentication Framework Admins** in the **Users** container.

2. Add the user who will be the administrator of NetIQ Advanced Authentication Framework to the **NetIQ Advanced Authentication Framework Admins** group. It is also required to add this user to the **Local Admins** group of Member Server.

3. Log on to Member Server as NetIQ administrator.

4. Install **NetIQ Group Policy Templates**.

5. Install AD LDS server role (For more information, see: http://technet.microsoft.com/en-us/library/cc754486(v=ws.10).aspx).

6. Create AD LDS instance:

> 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 5-6.
> 6. At the 7th step **AD LDS Administrators** select **This account**, click **Browse...** and specify **NetIQ Advanced Authentication Framework Admins** group.
> 7. 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 **NetIQ Advanced Authentication Framework Admins** group.

7. Open **Group Policy Management Console**.

8. Create a new group policy object (GPO) NAAF and link it to entire domain if you have not done that yet.

9. Browse the following path: **Computer Configuration -> Policies -> Administrative Templates -> NetIQ Advanced Authentication Framework -> Repository**.

10. Enable **Repository** policy with **ADAM Instance** default value. Enable **ADAM Settings** policy with default settings: **CN=NAAF**, ADAM server port number: **50000**. If you use Novell DSfW you also need to enable a policy: **Enable Novell support**.

11. Apply the policies on the Member Server.

12. Extend the schema for AD LDS (errors with rights may occur at steps 4-6 while schema extension).

⊗ Schema extension should be performed on the server with the configured AD LDS instance. The user who performs schema extension should be the member of **Local Admins** and **AD LDS Admins** groups.

13. Log on to system as a user with **Domain Admins** privileges.

14. Install Authenticore Server:

    1. Open **Autorun.exe**.
    2. 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.

⊛ 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 install-ation 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.

⊛ If you try to generate Enterprise Key just after the installation of Authenticore server, the fol-lowing error will appear: "Could not register AuthenticoreService account. Could not get access to ADAM Servers".

15. Add Authenticore Server to the **NetIQ Advanced Authentication Framework ADAM Serv-ers** group.

16. Add NetIQ administrator to the **Authenticore Admins** group.

17. Log on to Member Server as NetIQ administrator.

18. Restart schema extension (now error doesn't occur at the 5th step).

19. Log on to Member Server as a user with **Domain Admins** privileges.

20. In the command line open `%ProgramFiles%\NetIQ\NetIQ Advanced Authentic-ation Framework`.

21. Enter `authtray /master` in the command line.

22. Generate the Enterprise Key and apply the license.

23. Save securely the copy of the Enterprise Key.

⊛ 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:

24. Add NetIQ administrator to the **Local Admins** group of the additional Member Server.

25. Log on to the additional Member Server as NetIQ administrator.

26. Install AD LDS server role (For more information, see: http://technet.microsoft.com/en-us/library/cc754486(v=ws.10).aspx).

27. Configure replica for AD LDS instance:

> 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 click **Browse...** and select the first server, then input LDAP port: 50000.
> 5. At the 5th step **Administrative Credentials for the Configuration Set** select **This account** and enter **User name** and **Password** for NetIQ administrator.
> 6. At the 6th step please check the box on **CN=NAAF**.
> 7. At the 10th step **AD LDS Administrators** select **This account**, click **Browse...** and specify **NetIQ Advanced Authentication Framework Admins** group.

28. Log on to the additional Member Server with **Domain Admins** privileges.
29. Install the additional Authenticore Server:

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

30. Add the Member Server to **NetIQ Advanced Authentication Framework ADAM Servers** group. Verify whether the **Trust this computer for delegation to any service** option is included at the **Delegation** tab in **ADUC** (for Kerberos only).

31. Get the existing Enterprise Key from the first Authenticore Server through the **Authenticore Tray Manager** icon.

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

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

Policy 5, 19, 21, 25, 27

R

RADIUS 12, 14, 17
Remote 10, 12, 25
RTE 5, 19, 27-29

S

Security 21
Server 4, 7-8, 11-13, 15, 18-21, 26
Settings 22
Software 6
System 4, 8

W

Windows 6, 8, 20