



NetIQ Advanced Authentication
Framework - Extensible Authentica-
tion Protocol Server

Administrator's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Support	4
Installing and Removing EAP Server Package	5
Integration in RRAS/NPS Server	5
Logon to VPN	9
Configuration of VPN Connection	11
Logon to 802.1x Protected Network	12
Simplified Scheme of NAAF EAP Server Principle of Work	13
Troubleshooting	14
Cannot Install EAP Server Package	14
Index	15

Introduction


About This Document


Purpose of the Document

This EAP Administrator's Guide is intended for system administrators and describes the integration of NetIQ Advanced Authentication Framework – Extensive Authentication Protocol Server.


Document Conventions

This document uses the following conventions:

 **Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

 **Important notes.** This sign indicates important information you need to know to use the product successfully.

 **Notes.** This sign indicates supplementary information you may need in some cases.

 **Tips.** This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

Support

EAP Server is a server and client component. It is included to NetIQ Client. EAP Server supports authentication only on Microsoft Windows 7.

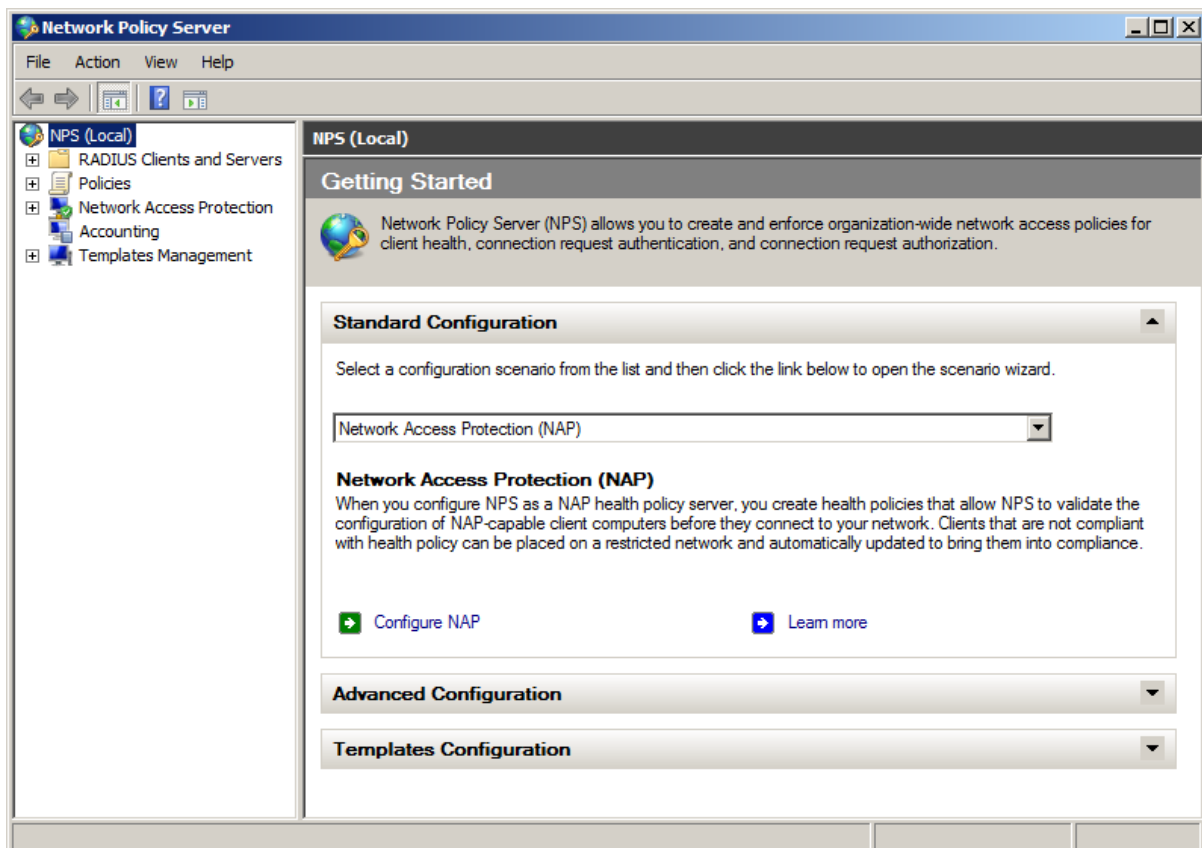
Installing and Removing EAP Server Package

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

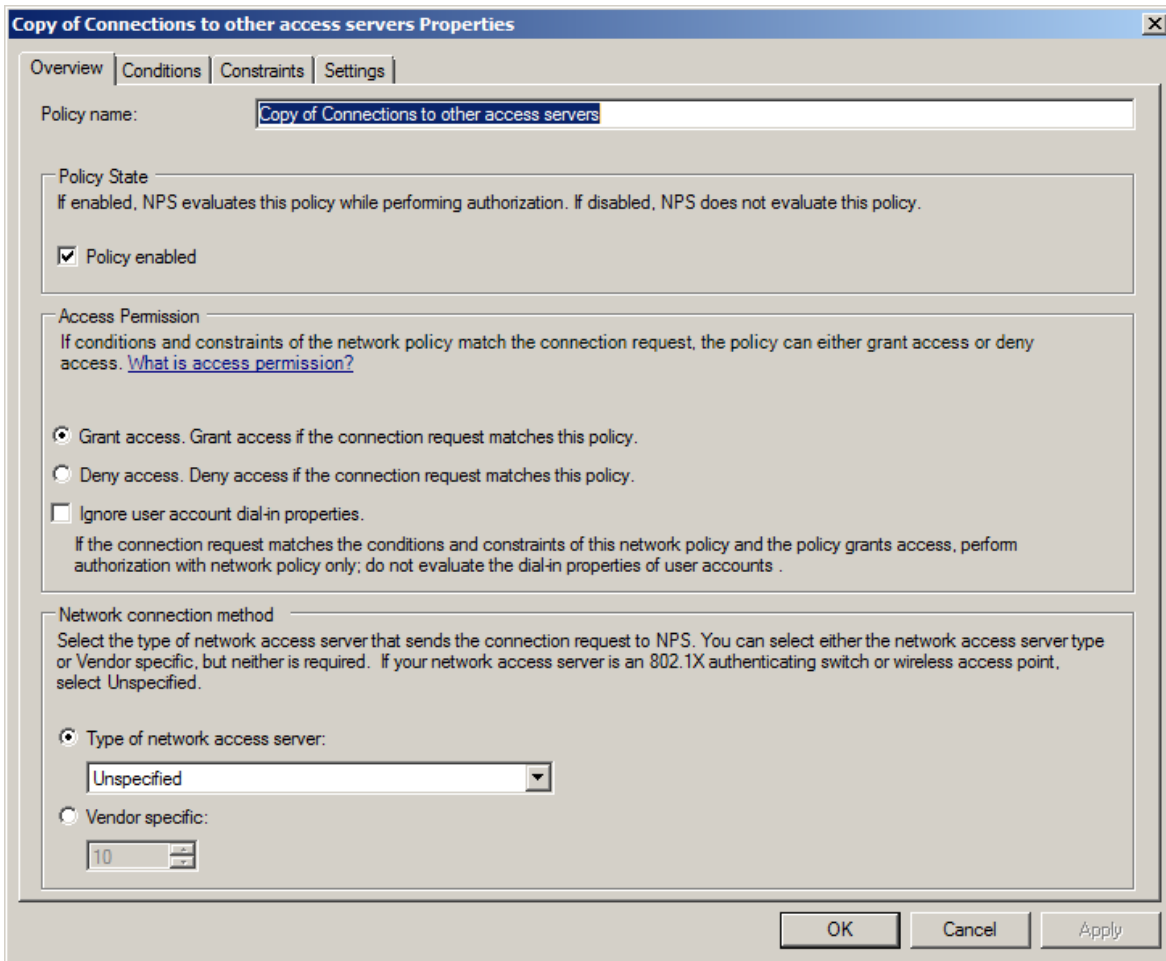
Integration in RRAS/NPS Server

EAP Server package should be installed on RRAS/NPS server to perform authentication of NetIQ Advanced Authentication Framework EAP Server clients. Administrator who is running the given package installation must be a member of **Local Admins** group.

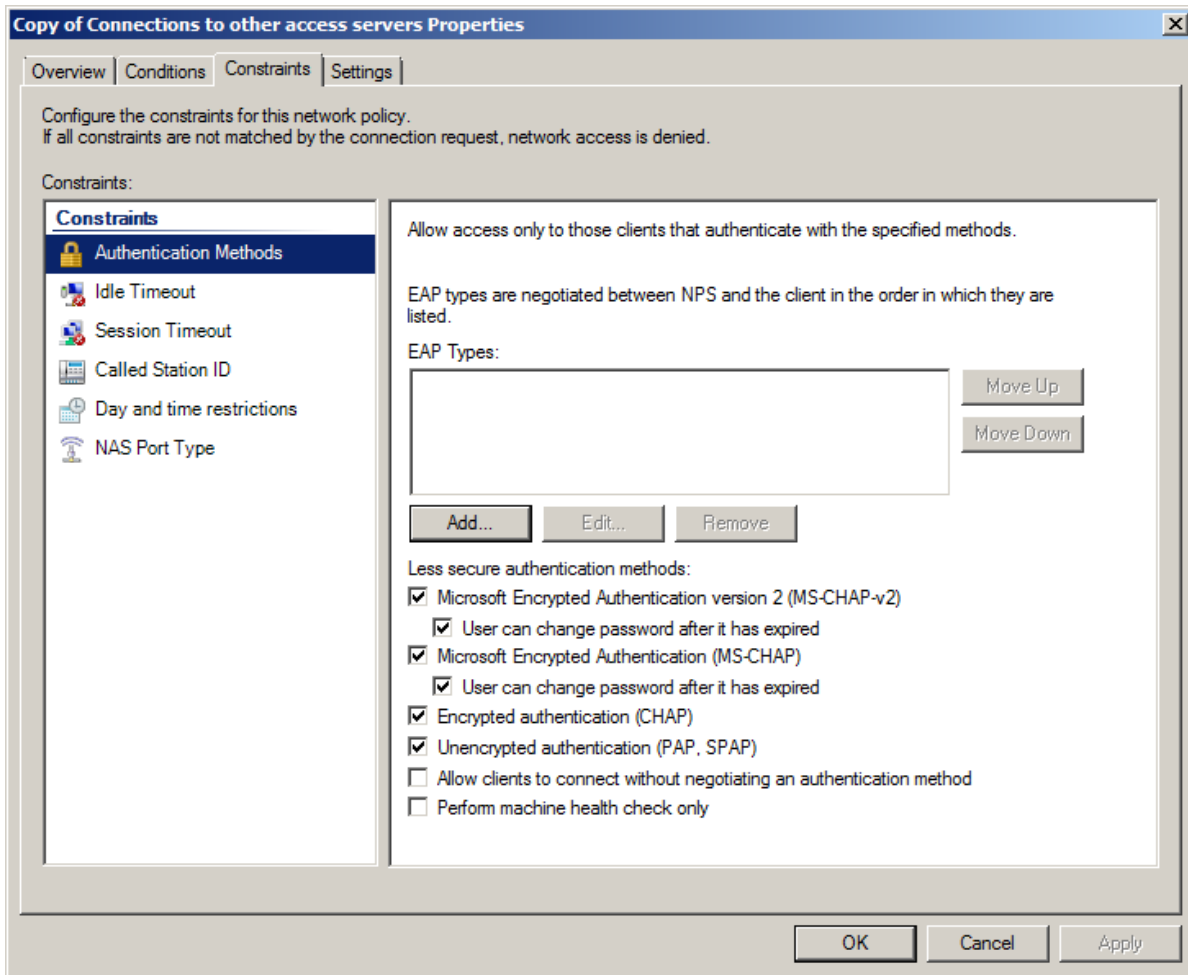
1. In **Server Manager**, add a new role: **Network Policy and Access Services**. Out of all the offered options, it is important that you keep **Network Policy Server**. Click **Install**.
2. After Network Policy Server is installed, open it through Administrative Tools. Configure **Network Access Protection (NAP)**.



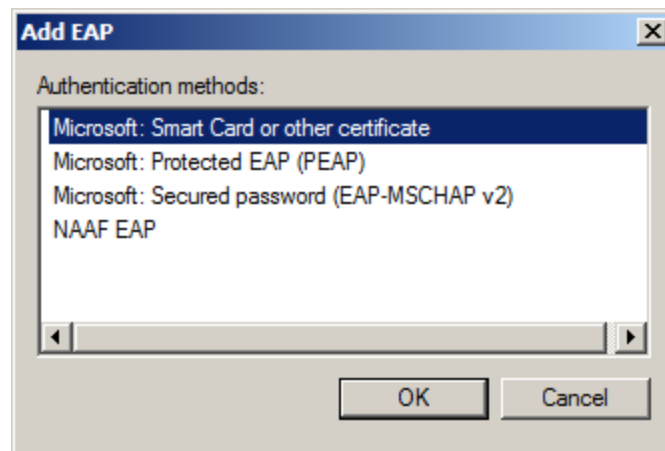
3. In **Network Policies**, disable all the policies. Duplicate the **Connections to Other Access Servers** policy and make it a granting one.



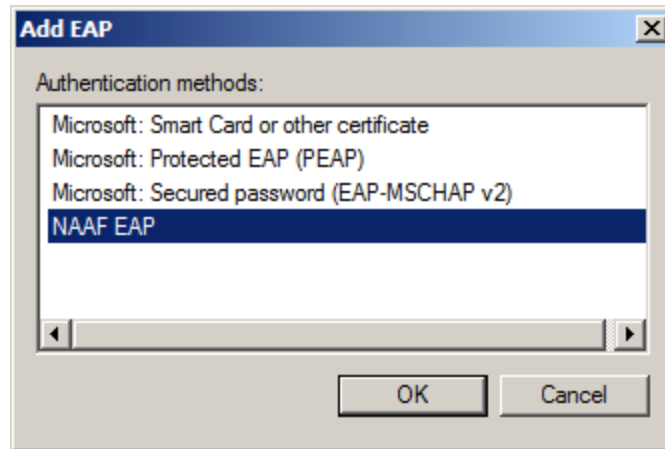
4. On the **Constraints** tab, select **Encrypted authentication (CHAP)** and **Unencrypted authentication (PAP, SPAP)**.



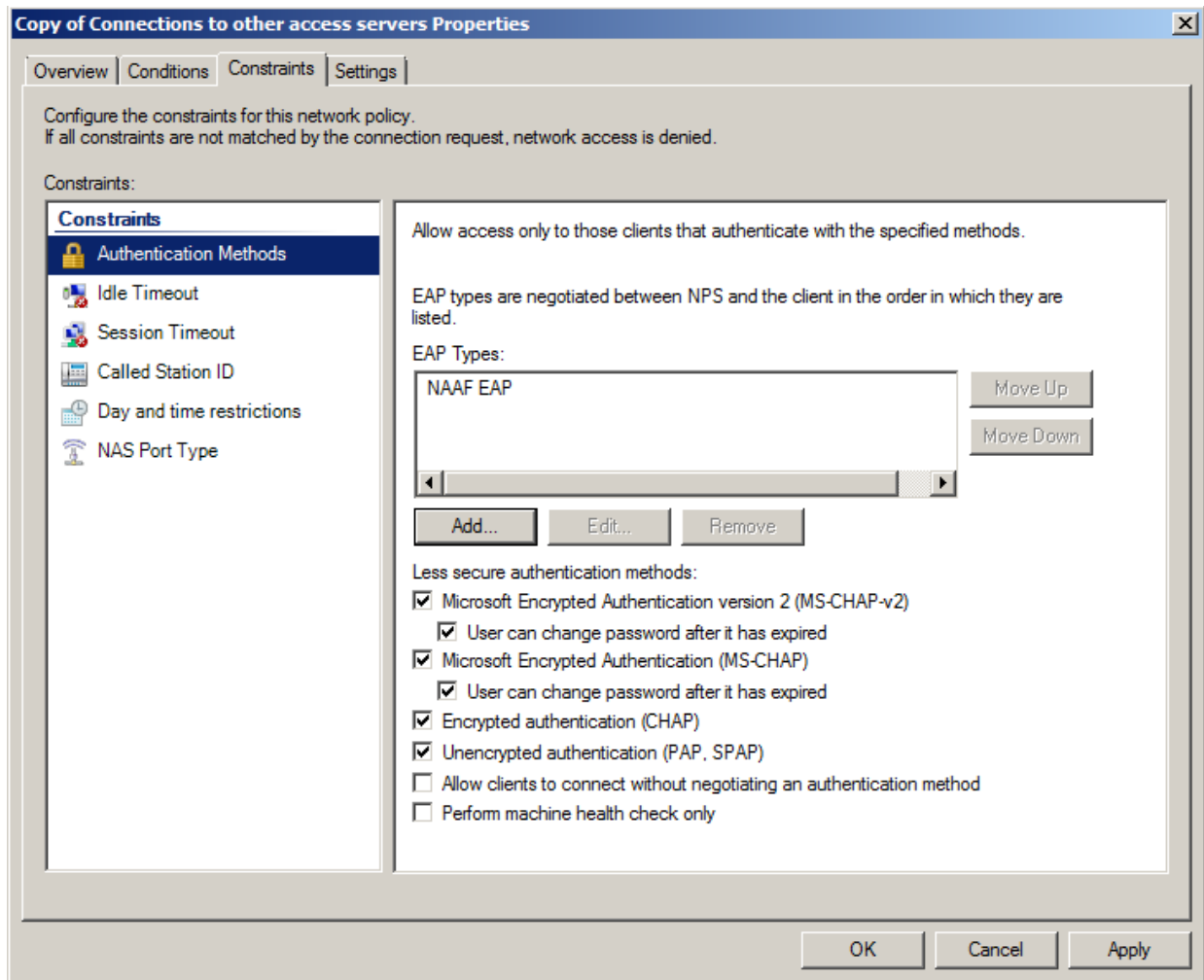
5. Then click the **Add** button to create the VPN connection. The following window will be displayed:




Select **NAAF EAP**:



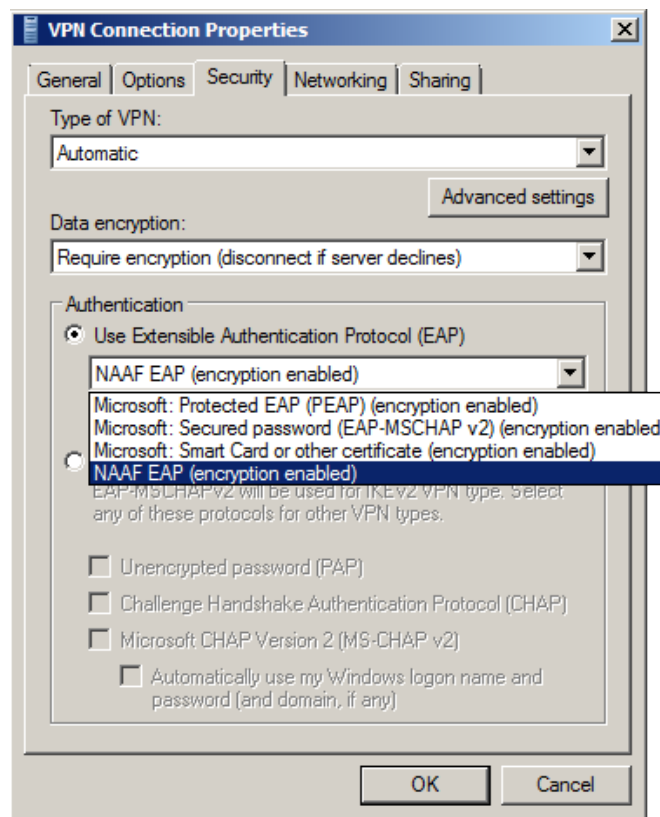
6. The **NAAF EAP** type is successfully added. Click **Apply** to create VPN connection.



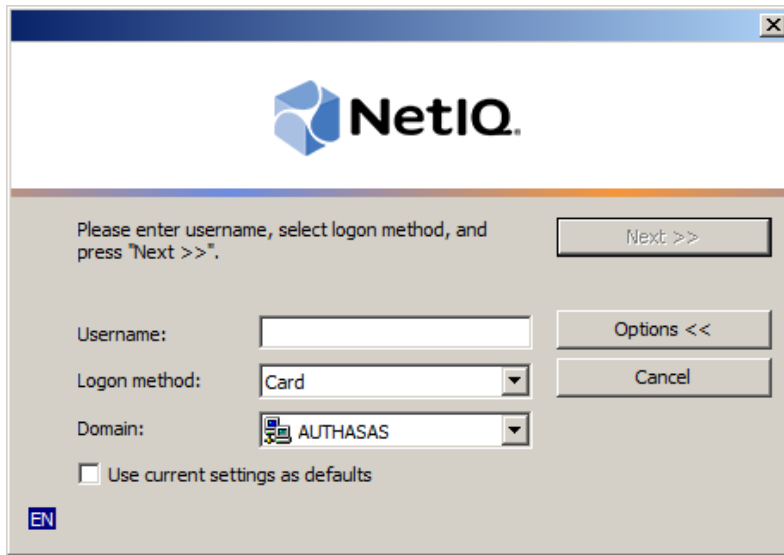
Logon to VPN

 Make sure that VPN connection is configured correctly. For more information, see the [Configuration of VPN Connection](#) chapter.

1. Click the **Network** icon in the system tray.
2. Right-click the established VPN connection.
3. Open **VPN Connection Properties** and select the **Security** inlay.
4. Select **Use Extensible Authentication Protocol (EAP)** and click **NAAF EAP (encryption enabled)**.



5. Click **OK**. The following window will be displayed in case of establishing VPN connection.



The image shows a NetIQ login dialog box. At the top, there is a blue header bar with the NetIQ logo and the text "NetIQ.". Below the header, the main area is light gray. It contains the following elements:

- A message: "Please enter username, select logon method, and press 'Next >>'." followed by a "Next >>" button.
- A "Username:" label followed by a text input field.
- A "Logon method:" label followed by a dropdown menu currently showing "Card".
- A "Domain:" label followed by a dropdown menu currently showing "AUTHASAS".
- A checkbox labeled "Use current settings as defaults" which is currently unchecked.
- Two additional buttons: "Options <<" and "Cancel".
- A small "EN" icon in the bottom left corner.

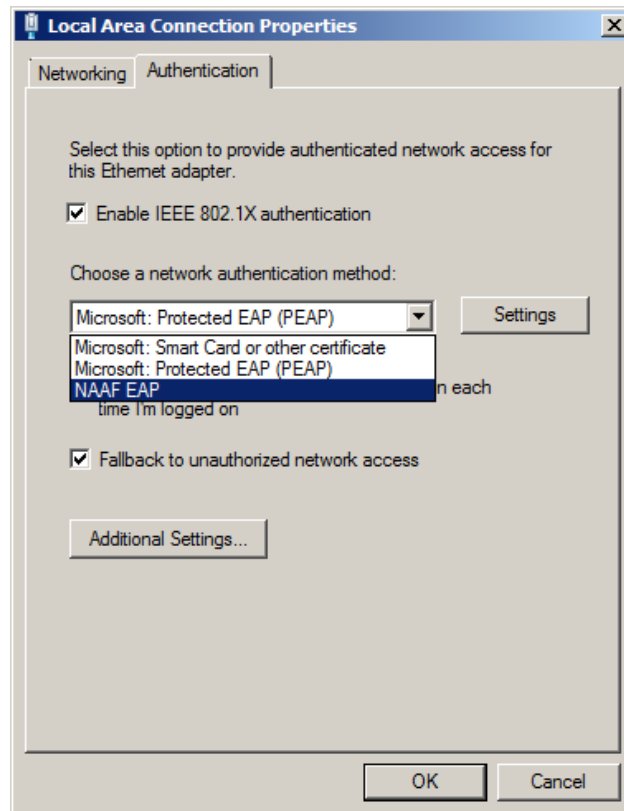
Configuration of VPN Connection


To configure a Virtual Private Network (VPN) Connection:

1. Click the **Start** button.
2. Select **Control Panel**.
3. Click **Network and Internet**.
4. Select **Network and Sharing Center**.
5. Click the **Set a new connection or network** link. The **Set Up a Connection or Network Wizard** will be opened.
6. In the wizard, select **Connect to a workplace** and click **Next**.
7. Select **Use my Internet Connection (VPN)** to connect to a workplace using VPN connection through the Internet. Select **Dial directly** to connect to a workplace using VPN connection with a modem by directly dialing a phone number to the workplace without going through the Internet.
8. In the **Internet address** text field, enter the IP address of the VPN server or the network's domain name.
9. In the **Destination name** text field, enter the name of the connection. The default name is **VPN Connection**.
10. Select the **Use as smart card** check box in case smart card will be used to authenticate to VPN connection.
11. Select the **Allow other people to use this connection** check box to provide anyone with access to the computer to use this connection.
12. Select the **Don't connect now; just set it up so I can connect later** check box to create the VPN connection but not connect to it.
13. Click **Next**.
14. Enter the domain username of the workplace in the **User name** text field.
15. Enter the password for the domain user account in the **Password** text field.
16. If necessary, select the **Show characters** check box to view the password.
17. Select the **Remember this password** check box to save the password.
18. If necessary, enter the domain name of the workplace in the **Domain** text field.
19. The connection is ready for use.

Logon to 802.1x Protected Network

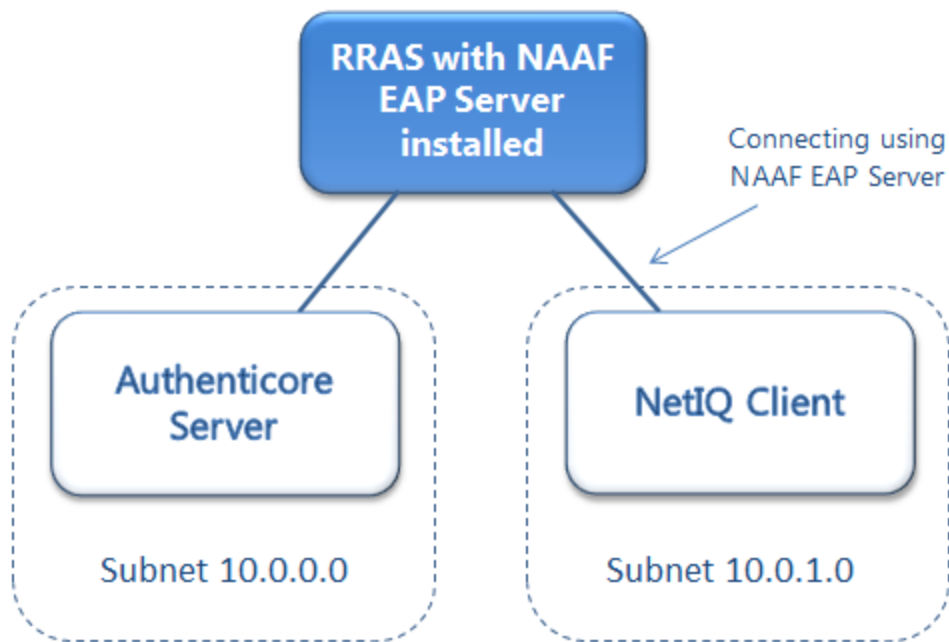
To use the 802.1x protocol, start the **Wired AutoConfig** service. When it is started, the **Authentication** tab appears. Go to the **Authentication** tab to select **NAAF EAP** from the list of network authentication methods.



 To detect network connections during logon, enable the **Enable 802.11 pre logon authentication** policy. For more information, see Group Policy Templates - Administrator's Guide.

Simplified Scheme of NAAF EAP Server Principle of Work

To logon using the NAAF EAP Server, client sends a request to logon using the authenticator. RRAS receives a request via NAAF EAP Server and in its turn sends a request to the authentication server, and then receives a response from the server and either logs on or rejects the entrance to the network.



Troubleshooting

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

Cannot Install EAP Server Package

Description:

Error appears when installing EAP Server Package on your computer.

Cause:

1. You are installing EAP Server Package on the network drive.
2. You have no space left on the disk.
3. You are installing EAP Server Package on the unsupported OS.
4. You are installing EAP Server Package on the OS with the wrong bitness.

Solution:

- a. Change the installation path.
- b. Free the amount of disk space needed for installation.
- c. Check the Support chapter.
- d. Check your OS's bitness (x64/x86) and run the corresponding installer (x64/x86).

Index

A

Administrator 1, 3, 5
Authentication 1, 3, 5, 9, 12
Authenticator 3

C

Client 4
Connection 9, 11
Control 11

D

Domain 11

E

Error 14

L

Local 5
Logon 3, 9, 12

N

Network 5, 9, 11

P

Package 14
Password 11
Policy 5, 12
Properties 9
Protocol 1, 3

S

Security 9
Server 4-5, 13-14
Support 4, 14

U

User 11