



NetIQ Advanced Authentication Framework

RADIUS Authentication Provider Configuration Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
RADIUS Authenticator Overview	4
Setting RADIUS Authenticator	6
Microsoft Windows Server 2008	6
Microsoft Windows Server 2003	9
Configuration Procedure	12
Troubleshooting	13
Cannot Install RADIUS Authentication Provider after Configuration	13
Invalid Configuration Data Input Error	13
Index	14

Introduction

About This Document

Purpose of the Document

This RADIUS Authentication Provider Configuration Guide is intended for all user categories and describes how to use the client part of NetIQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to configure RADIUS type of authentication.

For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ Advanced Authentication Framework – Client User's Guide.

Information on managing other types of authenticators is given in separate 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, buttons are put in bold type, e.g.: the **Logon** window.

RADIUS Authenticator Overview

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting management for computers to connect and use a network service.

RADIUS serves three functions:

- a. to authenticate users or devices before granting them access to a network;
- b. to authorize those users or devices for certain network services;
- c. to account for usage of those services.

Key features of RADIUS are:

1. Client/Server Model

- A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.
- RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.
- RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

2. Network Security

- Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

3. Flexible Authentication Mechanisms

- The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms.

4. Extensible Protocol

- All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the

protocol.

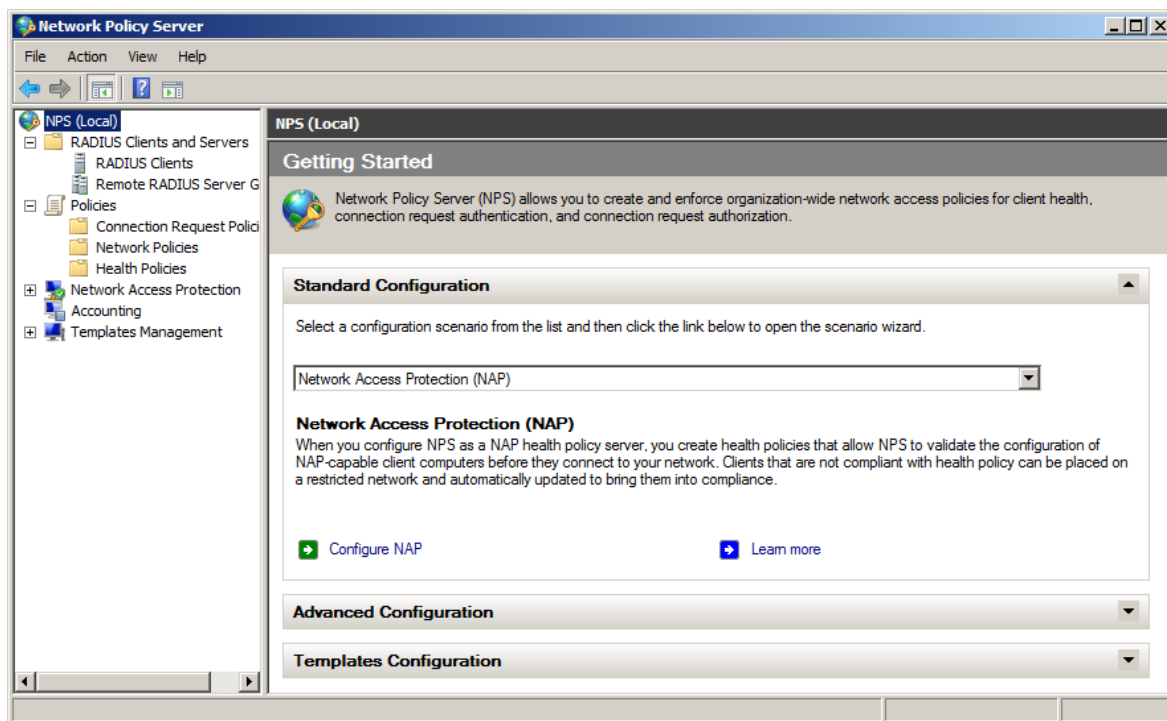
Setting RADIUS Authenticator

- ✱ RADIUS authentication provider should be installed both on the Server and the Client.

Microsoft Windows Server 2008

In order to set RADIUS manually

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**. Press **Install**.
2. After Network Policy Server is installed, open it through Administrative Tools. Configure **Network Access Protection (NAP)**.



3. Create clients by manually inputting their IPs and **Shared Secret** (any symbol line).

Server Properties [X]

Settings | **Advanced**

☒ Enable this RADIUS client

☐ Select an existing template:

[Dropdown]

Name and Address

Friendly name:
Server

Address (IP or DNS):
10.2.0.250 [Verify...]

Shared Secret

Select an existing Shared Secrets template:
None [Dropdown]

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:
[Masked]

Confirm shared secret:
[Masked]

[OK] [Cancel] [Apply]

Server Properties [X]

Settings | **Advanced**

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard [Dropdown]

Additional Options

☐ Access-Request messages must contain the Message-Authenticator attribute

☐ RADIUS client is NAP-capable

[OK] [Cancel] [Apply]

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

The screenshot shows the 'Copy of Connections to other access servers Properties' dialog box with the 'Overview' tab selected. The 'Policy name' field contains 'Copy of Connections to other access servers'. The 'Policy State' section has 'Policy enabled' checked. The 'Access Permission' section has 'Grant access. Grant access if the connection request matches this policy.' selected. The 'Network connection method' section has 'Type of network access server:' selected, with a dropdown menu showing 'Unspecified'.

Copy of Connections to other access servers Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.
☐ Deny access. Deny access if the connection request matches this policy.
☐ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

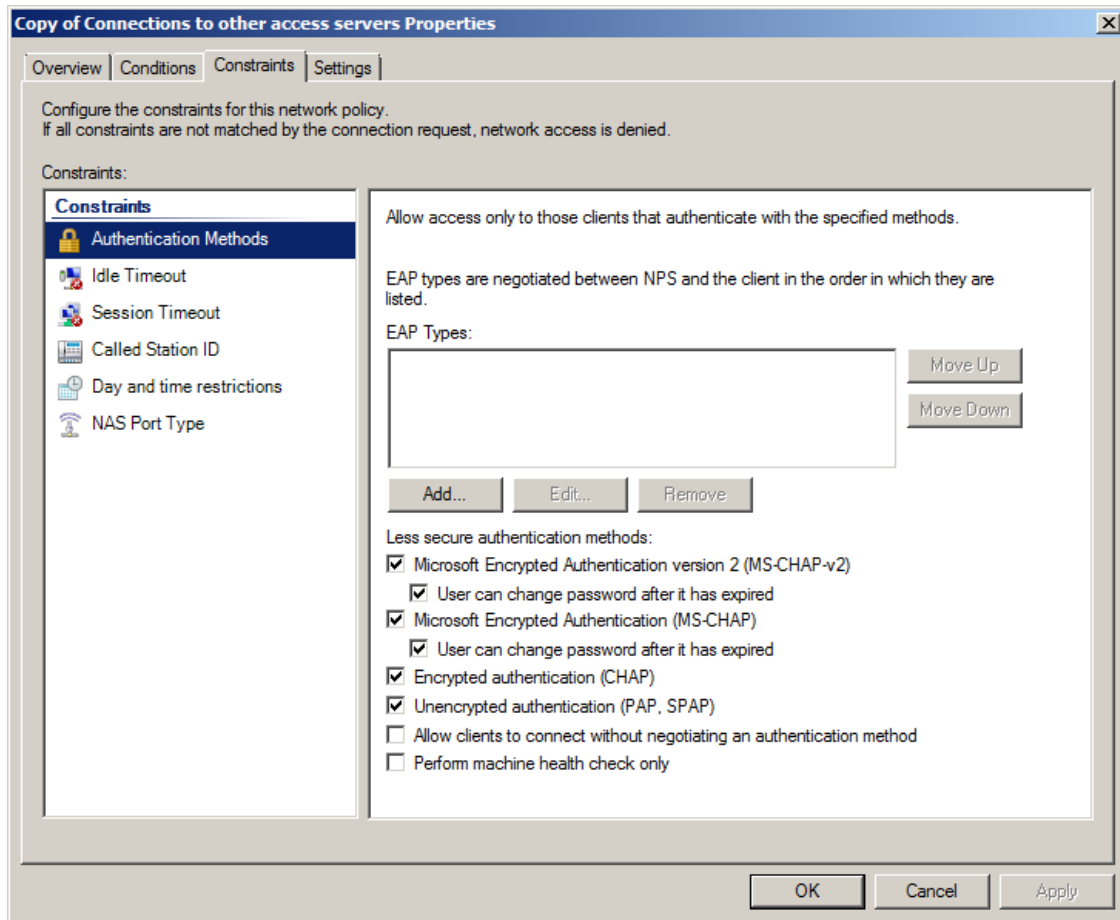
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

☐ Vendor specific:

OK Cancel Apply

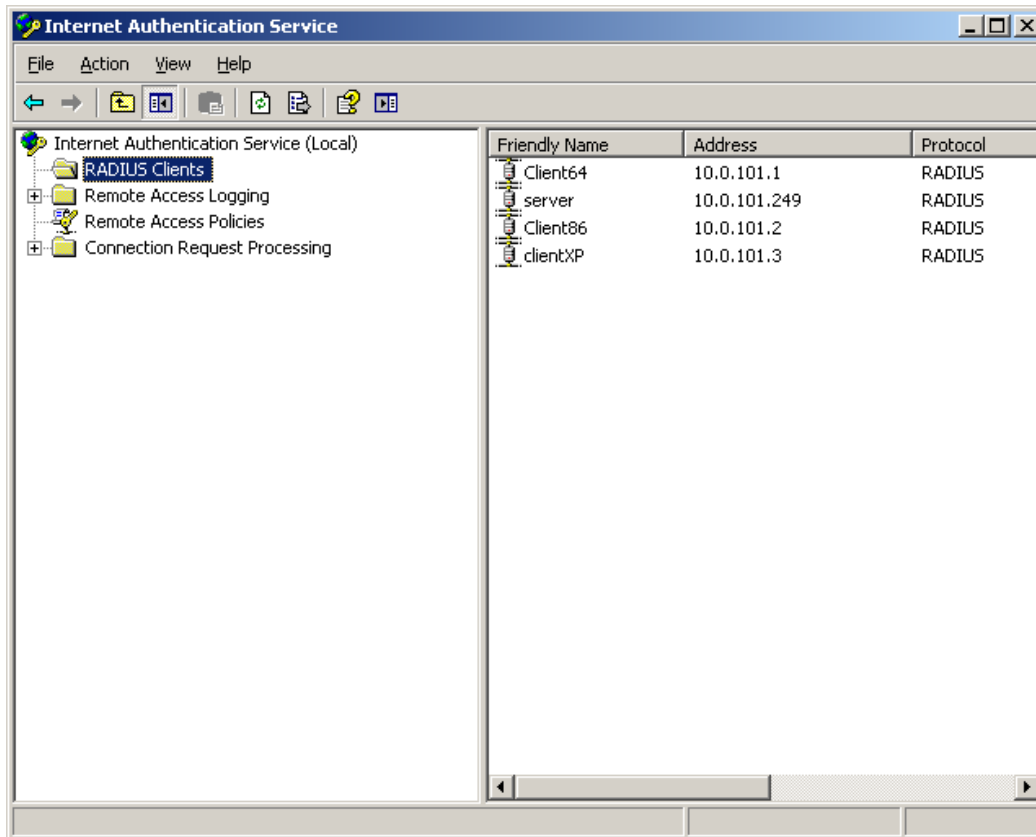
5. On Constraints tab, select **Encrypted authentication (CHAP)** and **Unencrypted authentication (PAP, SPAP)**.



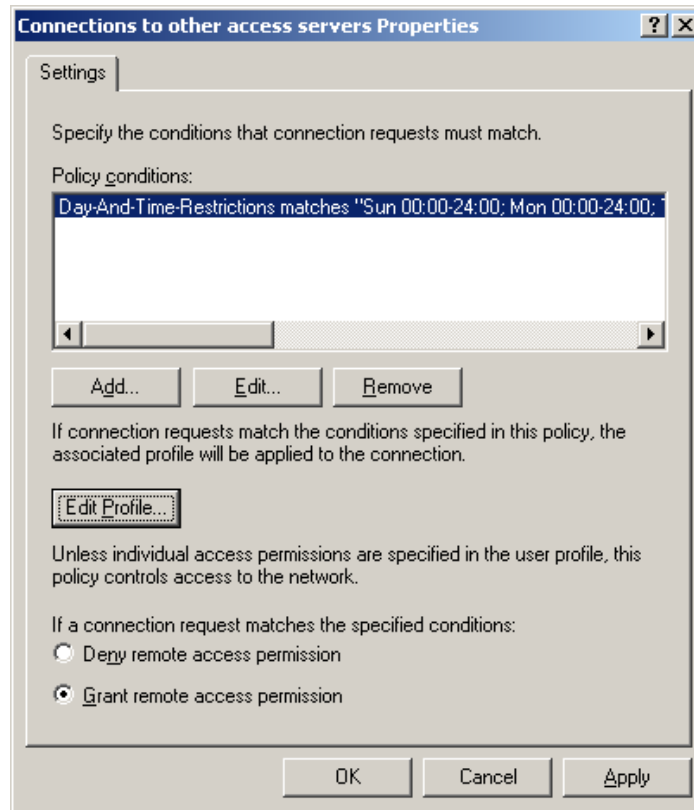
Microsoft Windows Server 2003

In order to set RADIUS manually

1. In Windows Component Wizard, add a new component: **Networking Services**. Out of all the offered options, it is important that you keep **Internet Authentication Services**.
2. After **Internet Authentication Services** is installed, open it.
3. Create clients by manually inputting their IPs and **Shared Secret** (any symbol line).



4. Move the **Connections to Other Access Servers** policy. Open the policy's **Properties**, click the **Edit Profiles** button.



5. On Authentication tab, select **Encrypted authentication (CHAP)** and **Unencrypted authentication (PAP, SPAP)**.

Configuration Procedure

Before running the installer you should first configure it. Please follow the steps below:

1. Run **RadiusConfigurator.exe** file.

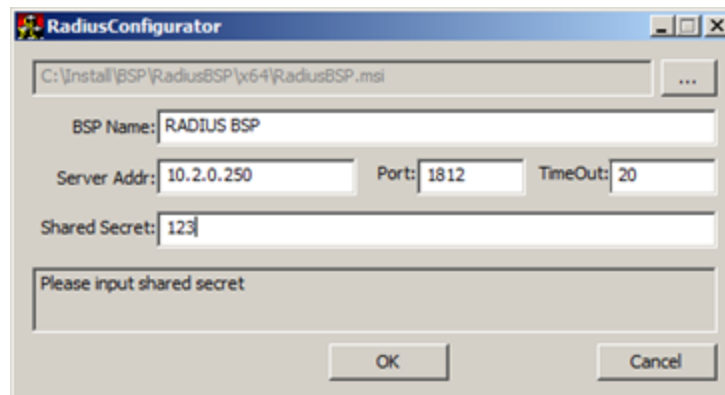
✖ In order to use the configurator tool the user has to have **Local Administrator** privileges.

2. Use the **Browse** button () and choose the **RadiusBSP.msi** file.

3. In the **Server Address** field type in RADIUS server address (either IP or DNS name).

✖ Please do not use localhost or 127.0.0.1.

4. Type in the shared secret and press **OK**.



i The **Port** field indicates the port through which RADIUS authentication provider will connect to the RADIUS Server.

i The **Shared Secret** field corresponds to the password that we configure on the server when creating RADIUS client.

i The **BSP Name** (which is the name of the authentication provider being configured) will be displayed automatically after you choose the .msi file.

Now you can proceed with installation.

Troubleshooting

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

Cannot Install RADIUS Authentication Provider after Configuration

Description:

Error message (**File open error**) appears when opening RadiusBSP.msi file after having executed RadiusConfigurator on the host PC.

Cause:

Your installer is broken.

Solution:

Download the installer once again.

Invalid Configuration Data Input Error

Description:

You receive **Authenticators don't match** notification when testing your authenticator on either a client part (before saving the authenticator) or server part (after having saved it) or both of them. Your authenticator is not working properly.

Cause:

You have input the wrong data in Radius Configurator. The configurator will not indicate it.

Solution:

Run the Configurator and type in the correct data.

Index

A

Authentication 1, 3-4, 9
Authenticator 3-4, 6

C

Client 3-4
Create 6, 9

D

Data 13

E

Edit 10
Error 13

F

File 13

K

Key 4

L

Local 12
Logon 3

M

Microsoft Windows Server 2003 9
Microsoft Windows Server 2008 6

N

Network 4, 6

P

Policy 6
Properties 10
Protocol 4

R

RADIUS 1, 3-4, 6, 9, 12-13

Remote 4

S

Security 4

Server 6, 12

W

Windows 9