



# NetIQ Advanced Authentication Framework

## **RADIUS Authentication Provider Configuration Guide**

Version 5.1.0

# Table of Contents

	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
About This Document .....	3
<b>RADIUS Authenticator Overview</b> .....	<b>4</b>
<b>Setting RADIUS Authenticator</b> .....	<b>5</b>
Microsoft Windows Server 2008 .....	5
Microsoft Windows Server 2012/Microsoft Windows Server 2012 R2 .....	9
<b>Configuration Procedure</b> .....	<b>13</b>
<b>RADIUS BSP Policies</b> .....	<b>15</b>
Auto Fill Domain .....	16
Enable Auto Enroll .....	18
<b>Troubleshooting</b> .....	<b>20</b>
Cannot Install RADIUS Authentication Provider after Configuration .....	20
Invalid Configuration Data Input Error .....	20
<b>Index</b> .....	<b>21</b>

# 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. authenticates users or devices before granting them access to a network;
- b. authorizes those users or devices for certain network services;
- c. accounts 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 insecure 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 protocol's implementations.

# Setting RADIUS Authenticator

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

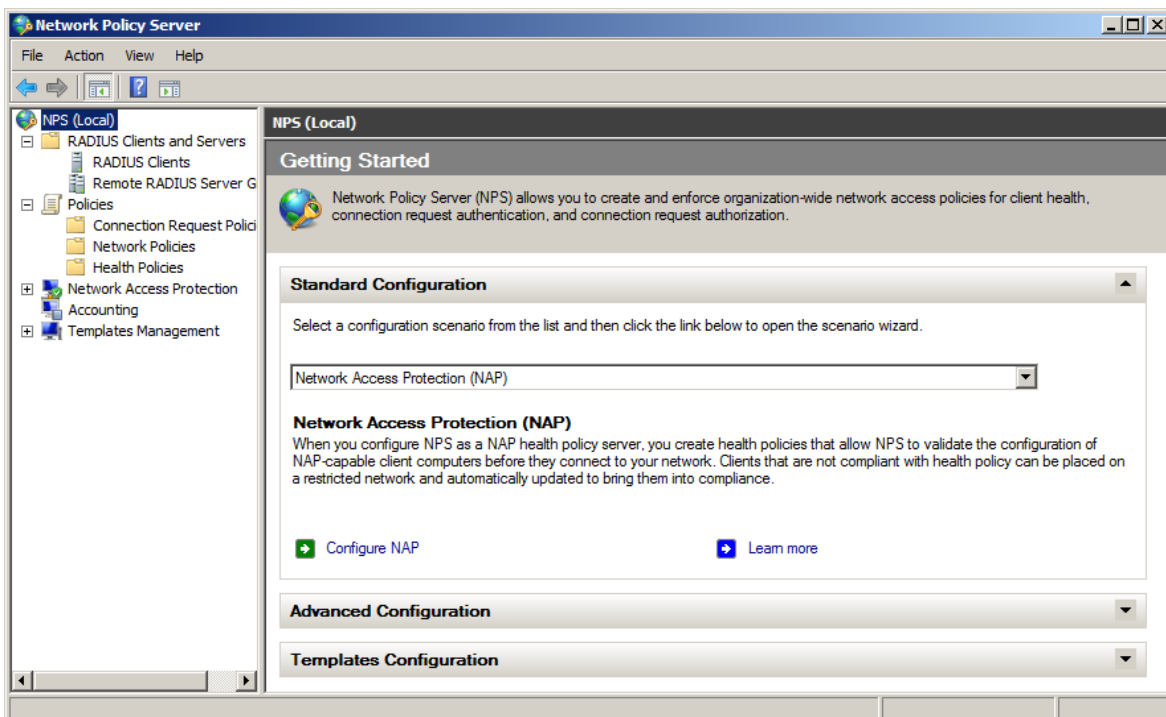
In this chapter:

- [Microsoft Windows Server 2008](#)
- [Microsoft Windows Server 2012/Microsoft Windows Server 2012 R2](#)

## Microsoft Windows Server 2008

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**. Click **Install**.
2. After the installation of **Network Policy Server**, open it through Administrative Tools. Configure **Network Access Protection (NAP)**.



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

**Server Properties** [X]

Settings | **Advanced**

Enable this RADIUS client

Select an existing template:

\_\_\_\_\_

**Name and Address**

Friendly name:  
Server

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

**Shared Secret**

Select an existing Shared Secrets template:  
None

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:  
●●●

Confirm shared secret:  
●●●

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

**Additional Options**

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

OK Cancel Apply

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

Copy of Connections to other access servers Properties

Overview | Conditions | Constraints | Settings

Policy name: Copy of Connections to other access servers

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 .

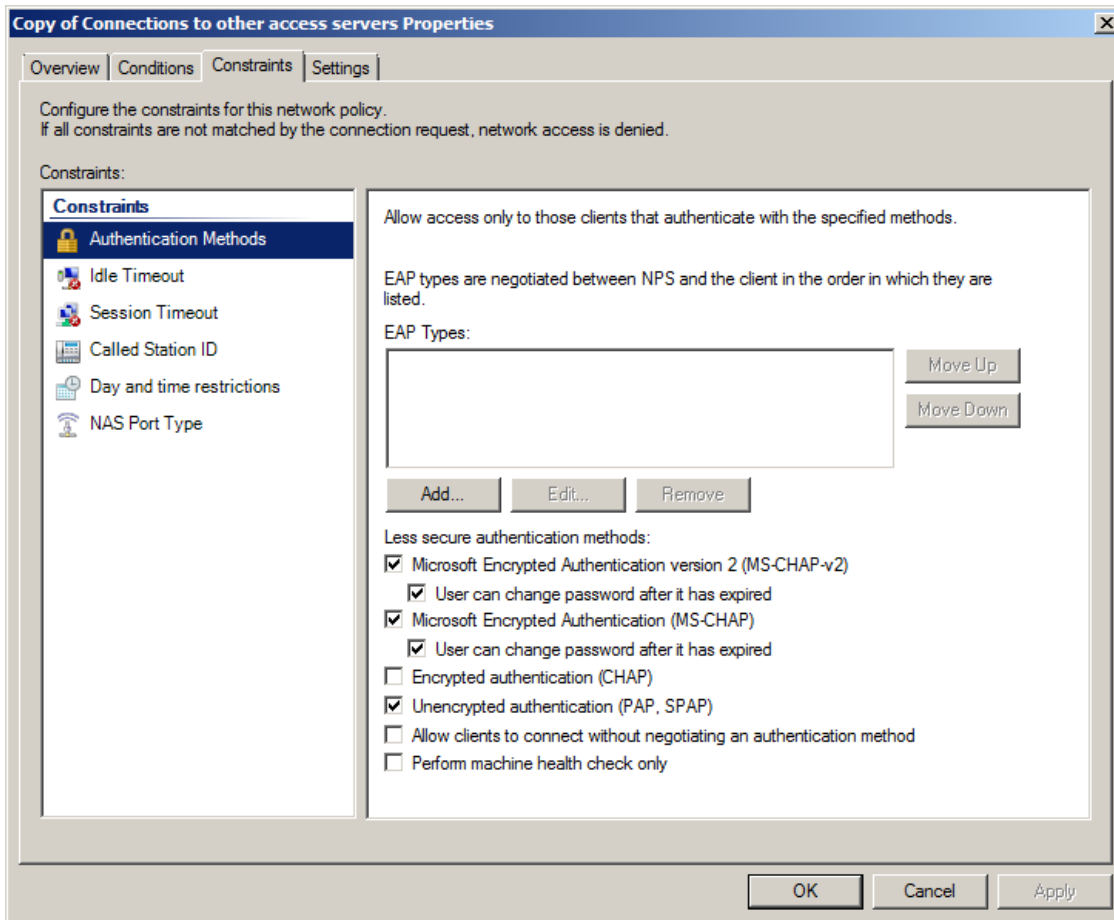
Network connection method  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select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

Type of network access server:  
Unspecified

Vendor specific:  
10

OK Cancel Apply

5. On the **Constraints** tab, select the **Unencrypted authentication (PAP, SPAP)** check box and click **OK**.



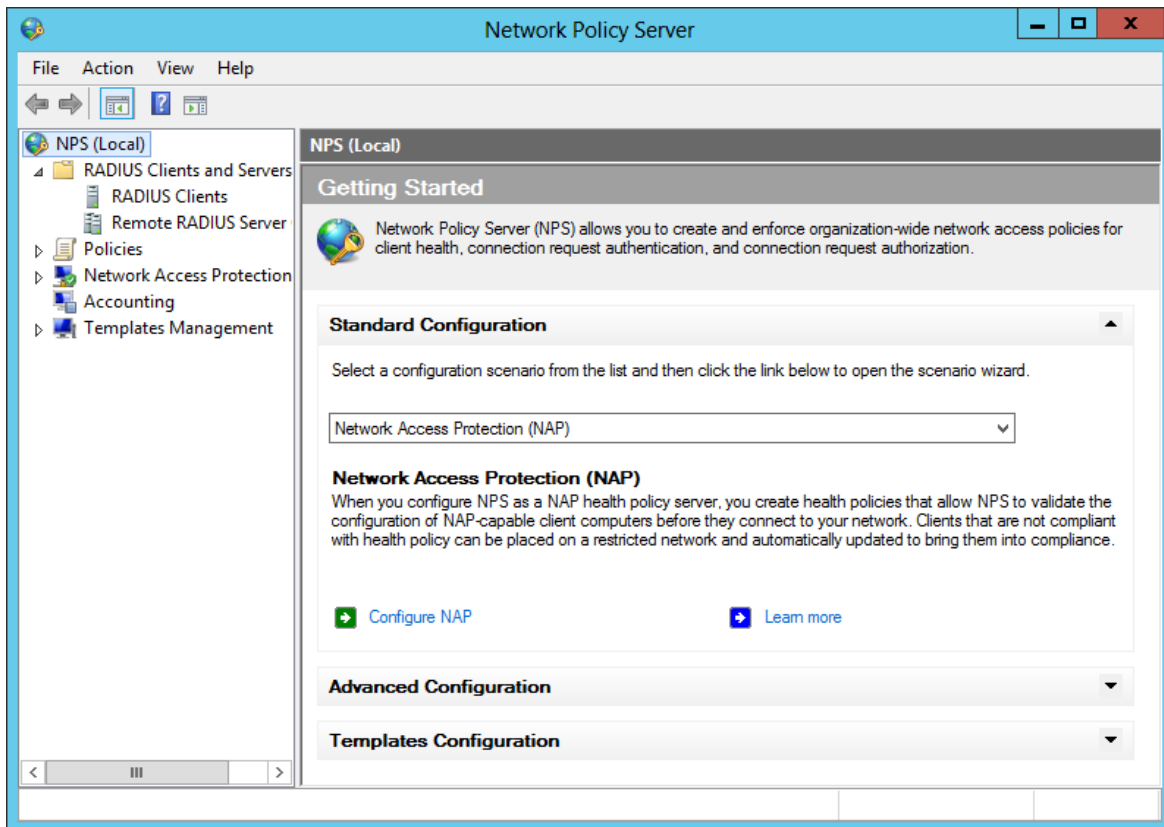
✖ Encrypted authentication (CHAP) is not supported.



## Microsoft Windows Server 2012/Microsoft Windows Server 2012 R2

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**. Click **Install**.
2. After the installation of **Network Policy Server**, open it through Administrative Tools. Configure **Network Access Protection (NAP)**.



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

Server Properties

Settings Advanced

Enable this RADIUS client

Select an existing template:

\_\_\_\_\_

Name and Address

Friendly name:  
Server

Address (IP or DNS):  
10.0.0.249 Verify...

Shared Secret

Select an existing Shared Secrets template:  
None

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:  
●●●

Confirm shared secret:  
●●●

OK Cancel Apply

Server Properties

Settings Advanced

Vendor

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

Vendor name:  
RADIUS Standard

Additional Options

Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

OK Cancel Apply

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

Copy of Connections to other access servers Properties

Overview Conditions Constraints Settings

Policy name: Copy of Connections to other access servers

**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 .

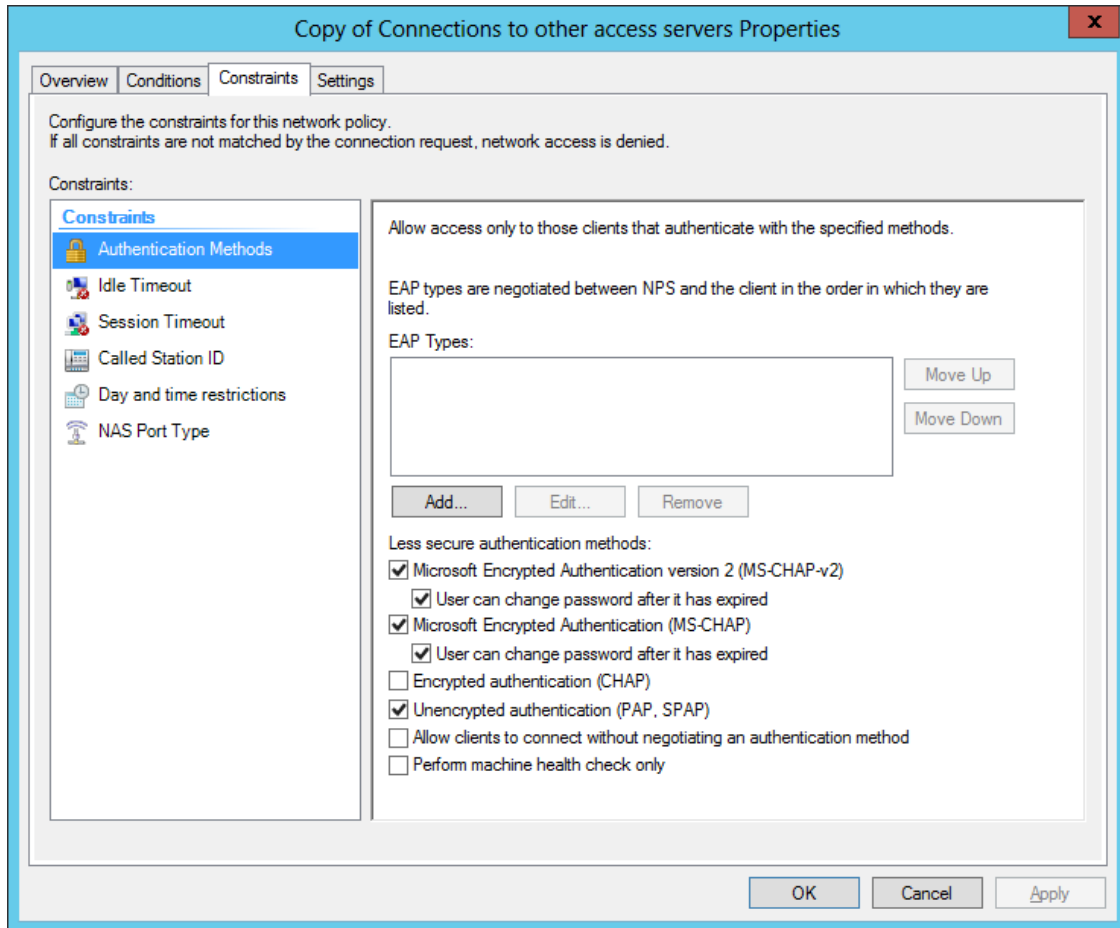
**Network connection method**  
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point,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


Type of network access server:  
Unspecified

Vendor specific:  
10

OK Cancel Apply


5. On the **Constraints** tab, select the **Unencrypted authentication (PAP, SPAP)** check box and click **OK**.




 Encrypted authentication (CHAP) is not supported.


# Configuration Procedure

Before running the installer, it is required to configure it first.

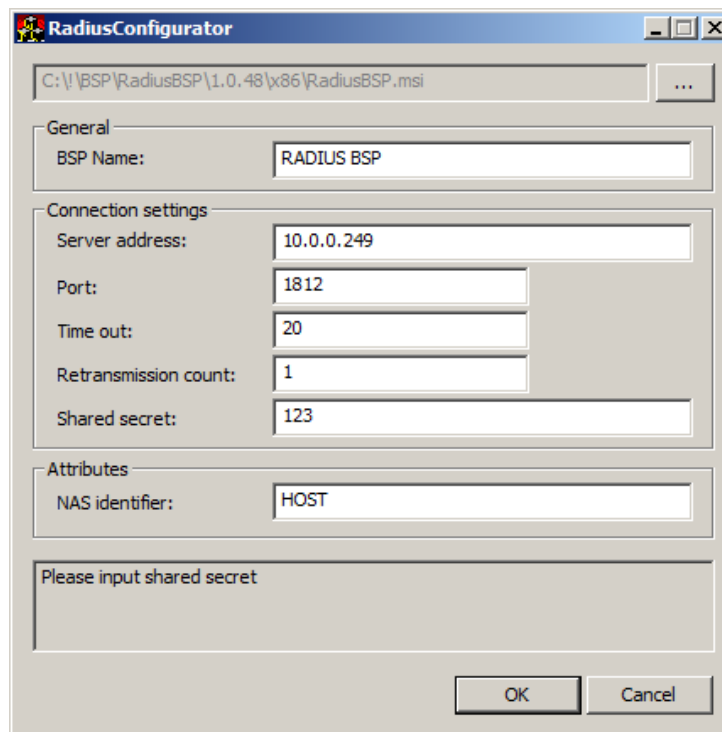
 Configuration of the installer requires the **Local Admins** privileges.

Please, follow the steps below:

1. Run the **RadiusConfigurator.exe** file.
2. Click the **Browse** button () and select the **RadiusBSP.msi** file.
3. Specify the RADIUS server address (either IP or DNS name) in the **Server address** text field.





 Please, do not use localhost or 127.0.0.1.

4. Enter the shared secret value into the **Shared secret** text field.
5. Optionally, specify the name of NAS identifier in the **NAS identifier** text field.
6. Click **OK**.



The screenshot shows the RadiusConfigurator dialog box with the following fields and values:

- File path: C:\BSP\RadiusBSP\1.0.48\x86\RadiusBSP.msi
- General section: BSP Name: RADIUS BSP
- Connection settings section: Server address: 10.0.0.249, Port: 1812, Time out: 20, Retransmission count: 1, Shared secret: 123
- Attributes section: NAS identifier: HOST
- Bottom section: Please input shared secret (empty text area)
- Buttons: OK, Cancel

-  The **Port** field indicates the port through which RADIUS authentication provider will connect to the RADIUS Server.
-  The **Retransmission count** field indicates the number of times the RADIUS authentication provider will try to connect to the RADIUS Server. It can be useful in case of network errors.
-  The **Shared Secret** field corresponds to the password that was configured on the server while creating RADIUS client.
-  The **BSP Name** (the name of the configured authentication provider) will be displayed automatically after you choose the **.msi** file.

After the configuration, it is required to proceed to installation.

## RADIUS BSP Policies

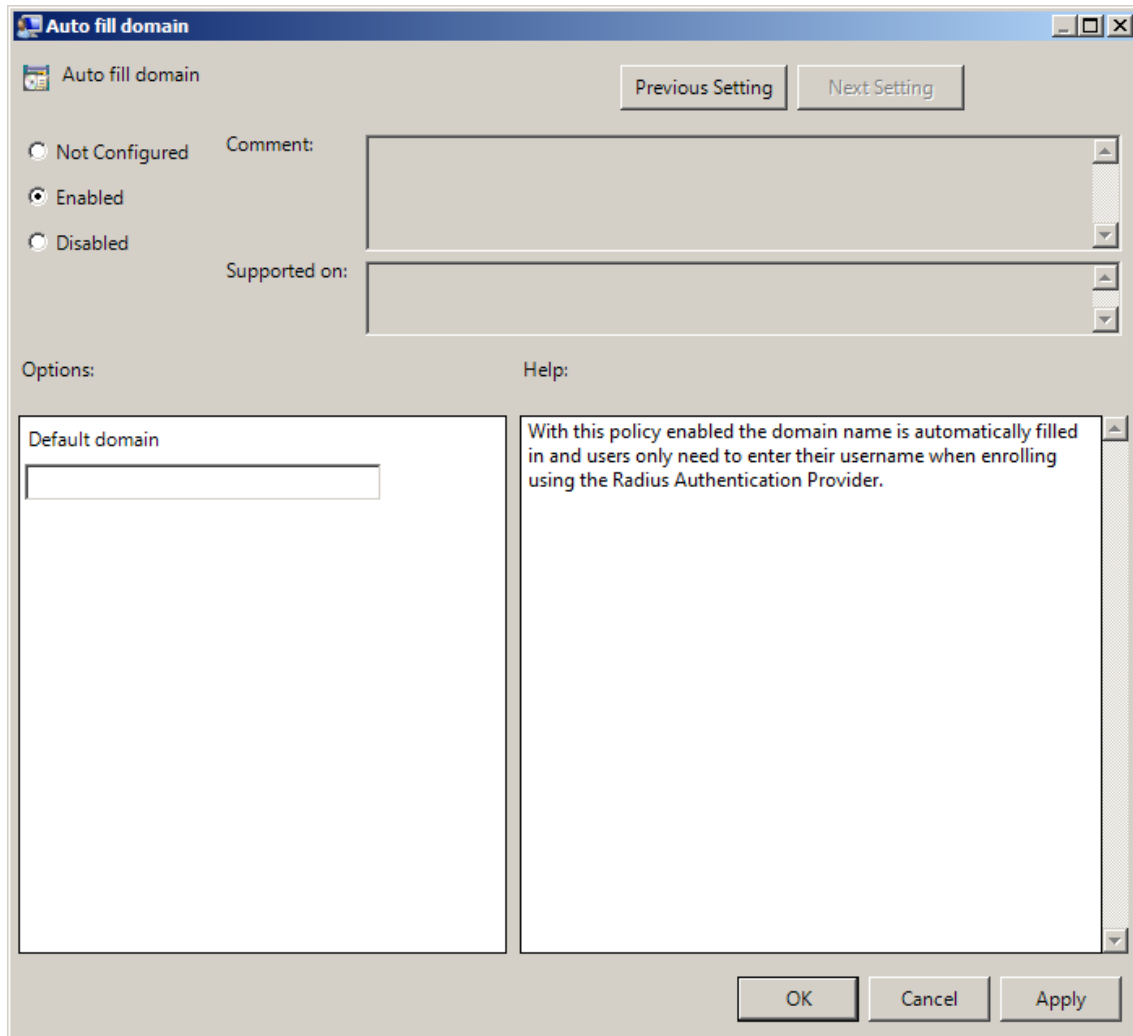
The **RADIUS BSP** section includes policies allowing you to edit RADIUS authentication settings.

It includes:

- [Auto fill domain](#)
- [Enable auto enroll](#)

## Auto Fill Domain

With the **Auto fill domain** policy enabled the domain name is automatically filled in and users only need to enter their username when enrolling using the RADIUS Authentication Provider.



To access the **Auto fill domain** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> Radius Authentication Provider**.

Registry settings:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\BioAPI\BSP\RadiusBSP

**AutoFillDomain:**

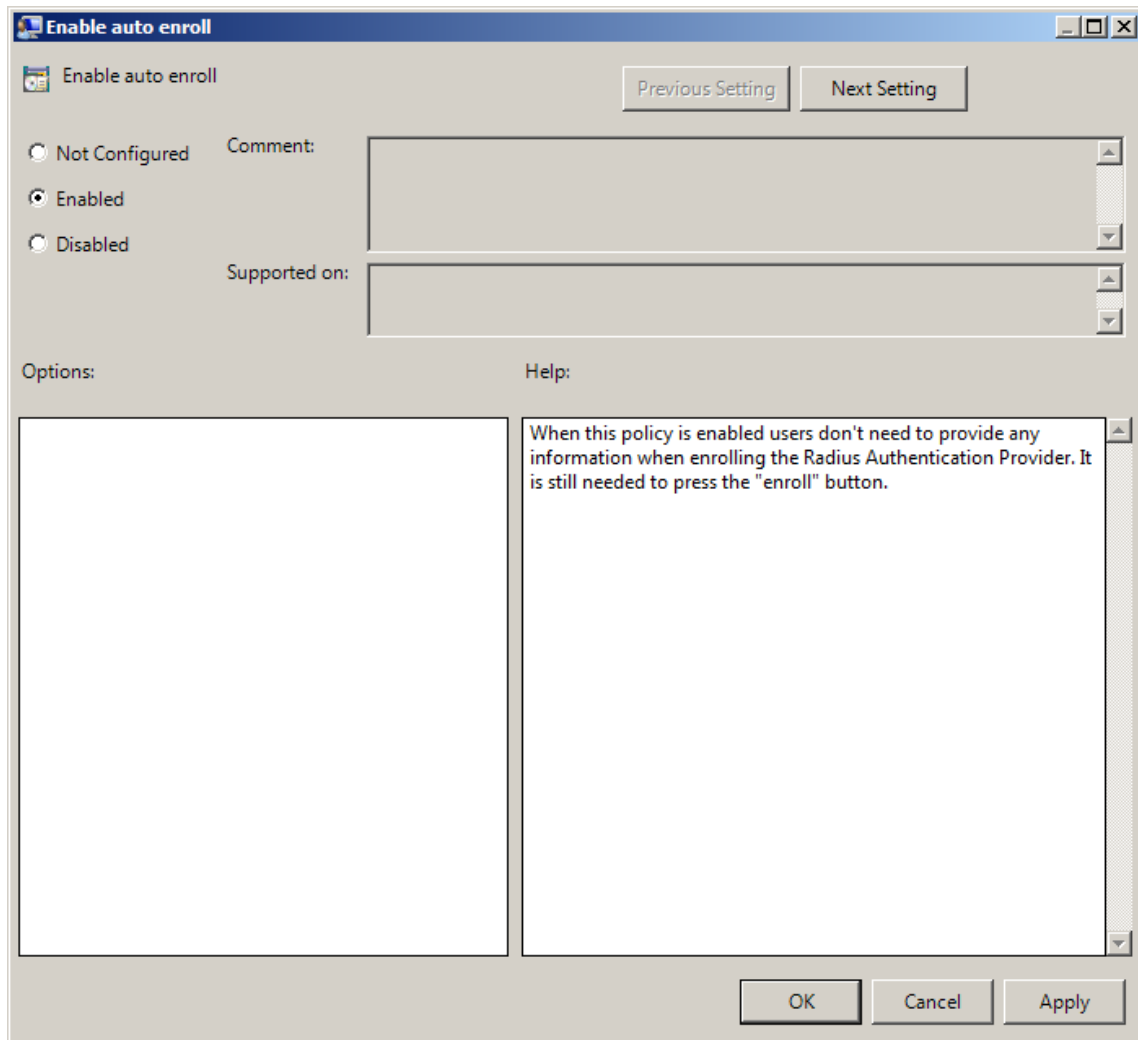
- value type: REG\_DWORD
- value data: netiq;



- description: netiq is the domain name that will be automatically filled in.

## Enable Auto Enroll

When the **Enable auto enroll** policy is enabled, users do not need to provide any information when enrolling the RADIUS authentication provider. It is still needed to click the **Enroll** button.



To access the **Enable auto enroll** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration - > Policies - > Administrative Templates -> Radius Authentication Provider**.

Registry settings:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\BioAPI\BSP\RadiusBSP

**EnableAutoEnroll:**

- type: REG\_DWORD
- value: 0x00000001 (1)

- description: 1 means that the policy is enabled

## 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 RADIUS Authentication Provider after Configuration

**Description:**

Error message (**File open error**) appears when opening RadiusBSP.msi file after having executed Radius Configurator 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, 16, 18  
Authenticator 3

## C

Client 3-4  
Create 5, 9

## D

Data 20  
Domain 16

## E

Enroll 18  
Error 20

## F

File 20

## K

Key 4

## L

Local 13  
Logon 3

## M

Microsoft Windows Server 2008 5  
Microsoft Windows Server 2012 5, 9

## N

Network 4-5, 9

## P

Policy 5, 9, 16, 18  
Protocol 4

---

**R**

RADIUS 1, 3-5, 9, 13, 15-16, 18, 20  
Remote 4

**S**

Security 4  
Server 5, 9, 13