NetIQ Advanced Authentication Framework

RADIUS Authentication Provider Configuration Guide

Version 5.1.0

Table of Contents

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.

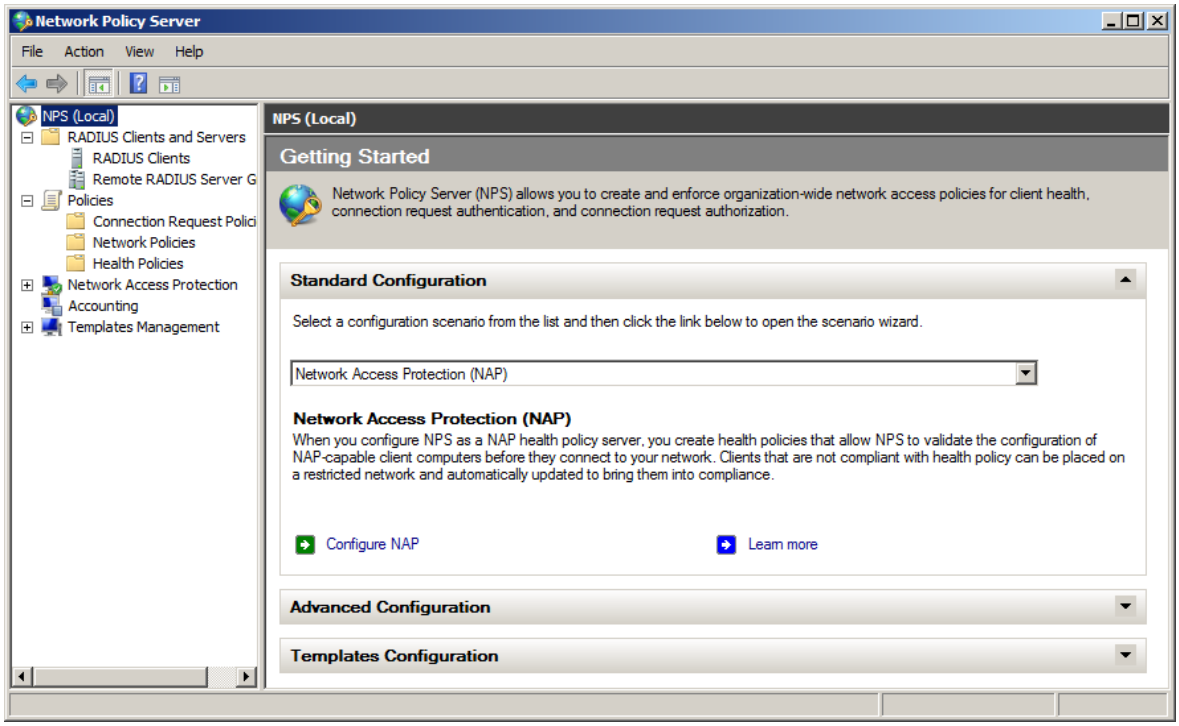
In this chapter:

Microsoft Windows Server 2008

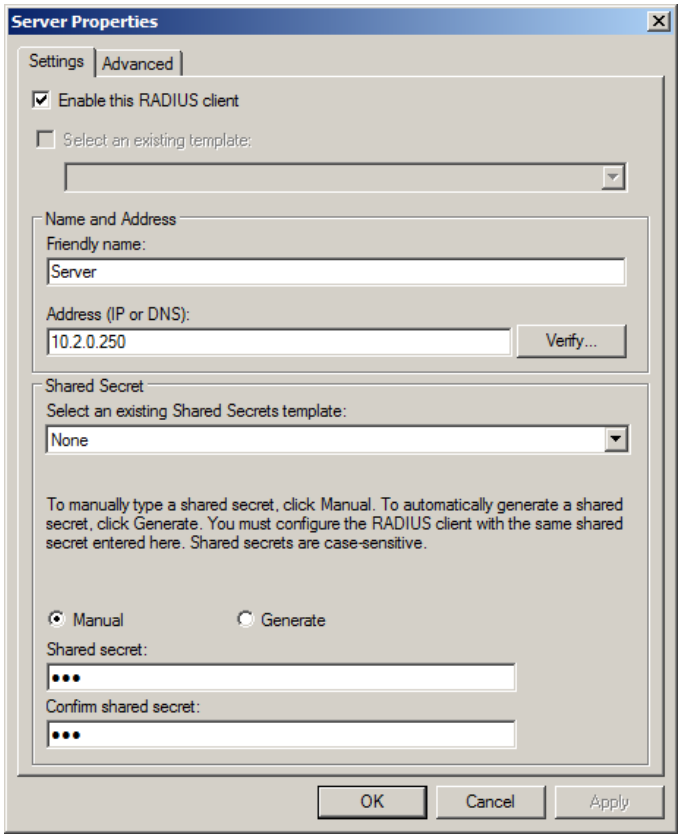
In order to set RADIUS manually:

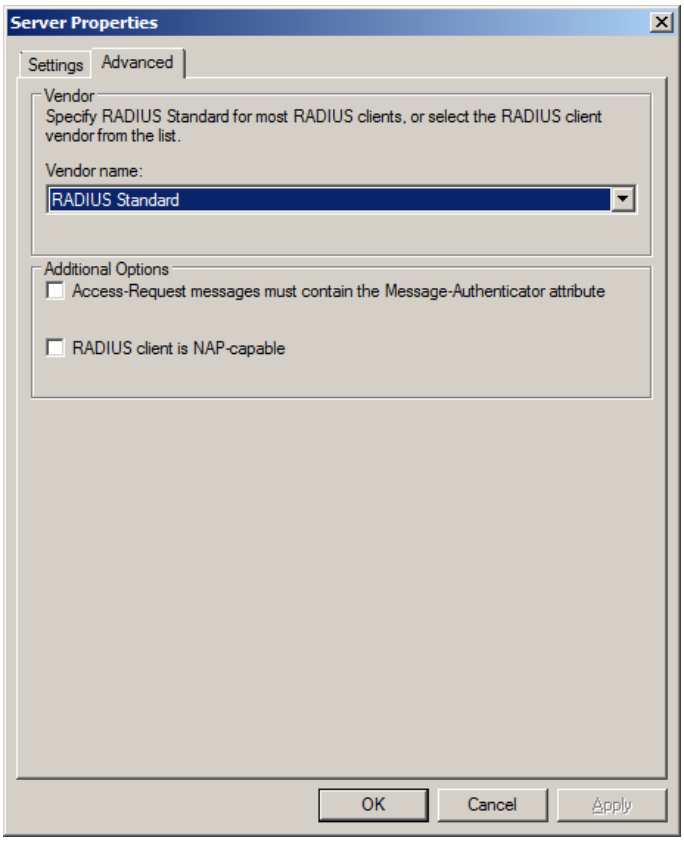
1. In **Server Manager**, add a new role: **Network Policy and Access Services**. Out of all the offered options, it is important that you keep **Network Policy Server**. Press **Install**.

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

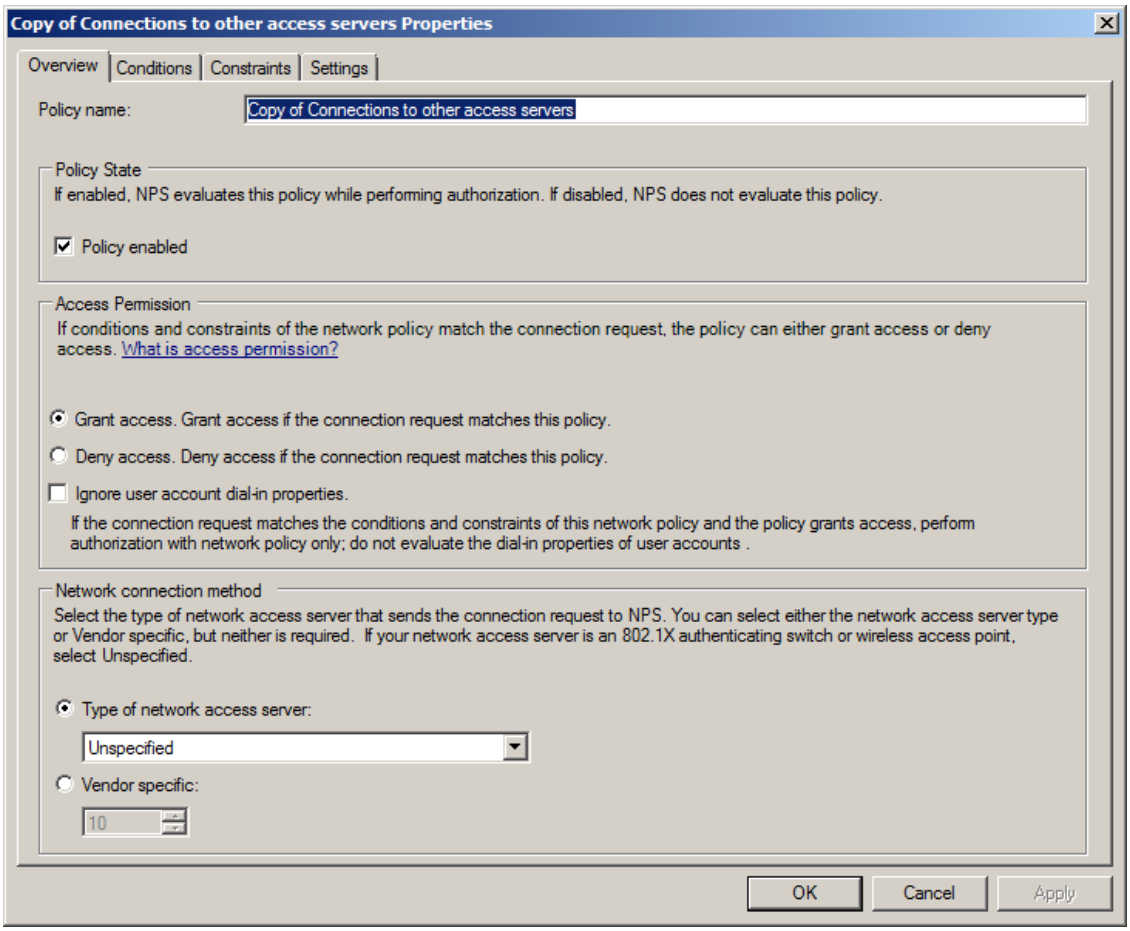


3. Create clients by manually inputting their IPs and **Shared Secret** (any symbol line).

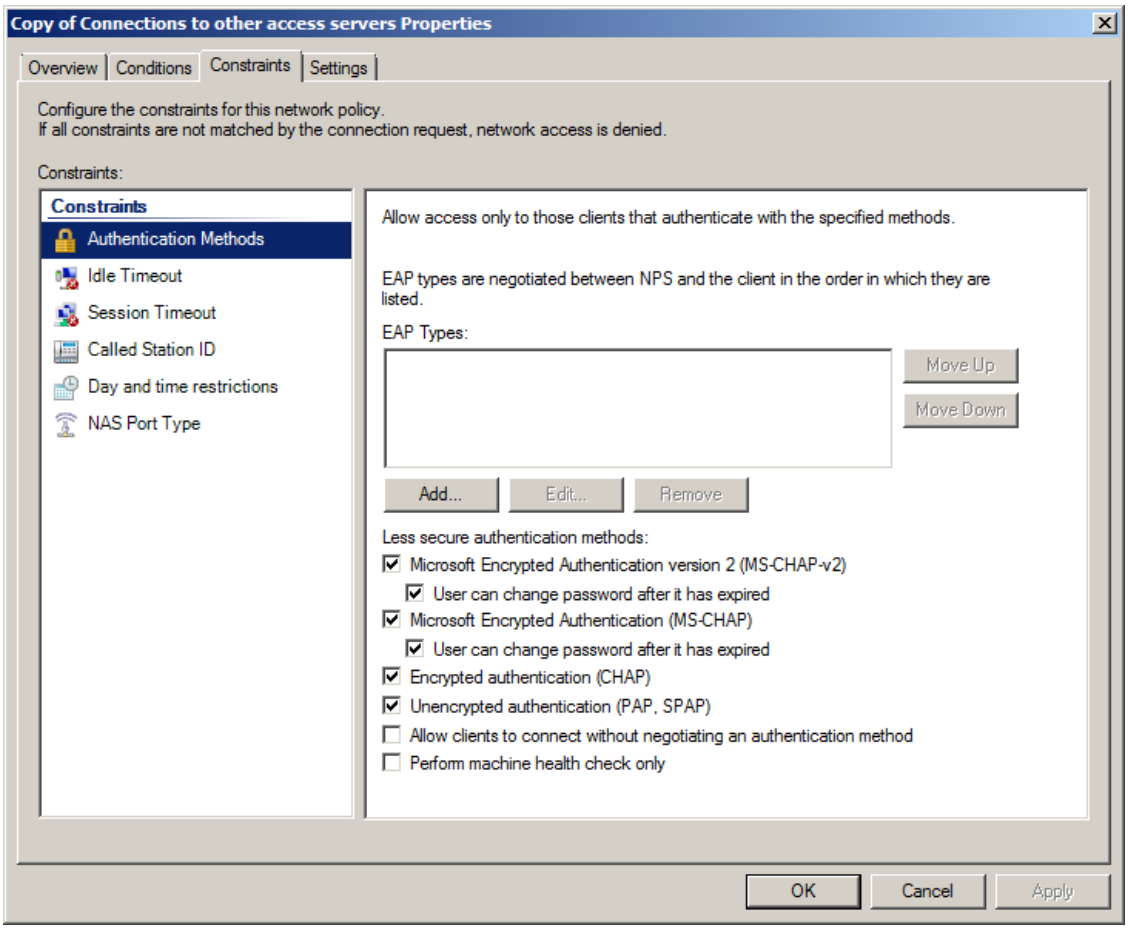

Server Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Server
Address (IP or DNS):
10.2.0.250
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate 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



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



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


Copy of Connections to other access servers Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
Perform machine health check only
OK
Cancel
Apply

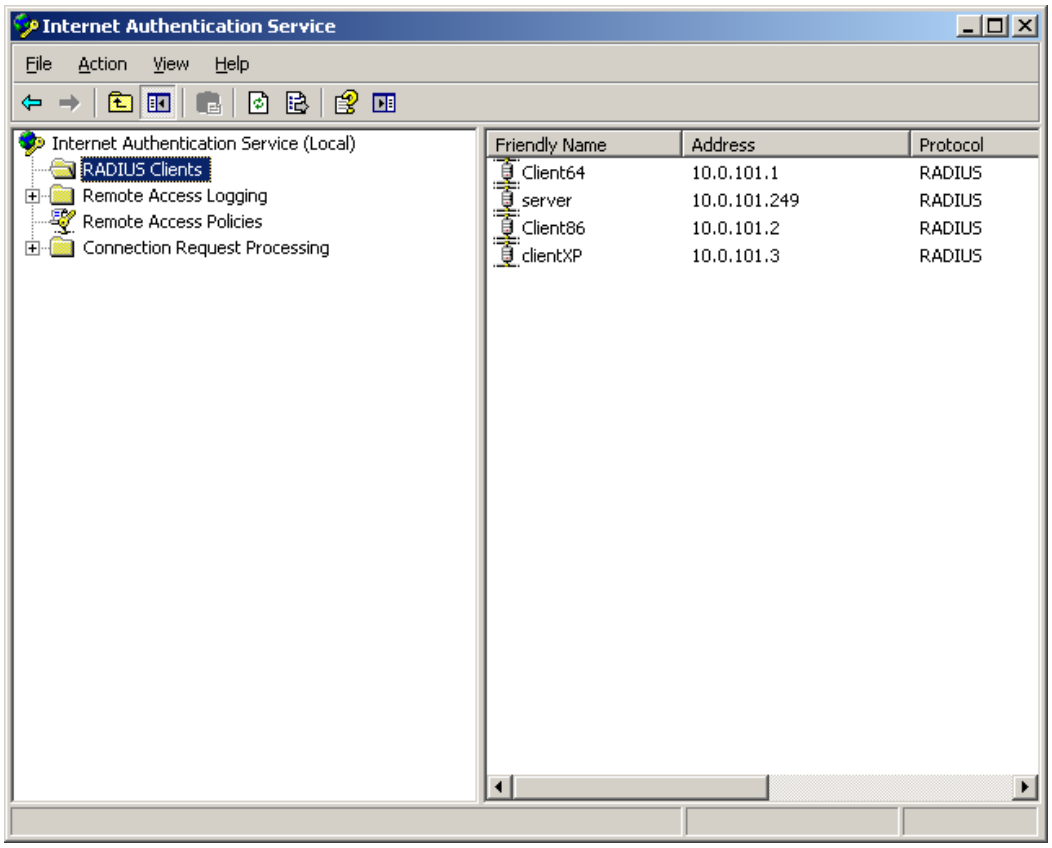
Microsoft Windows Server 2003

In order to set RADIUS manually:

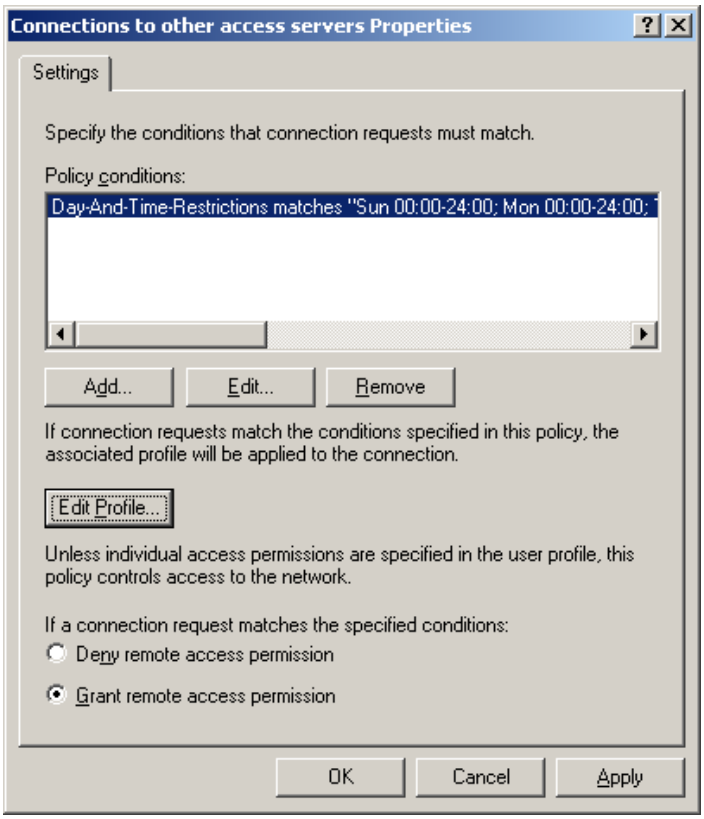
1. In **Windows Component Wizard**, add a new component: **Networking Services**. Out of all the offered options, it is important that you keep **Internet Authentication Services**.

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.

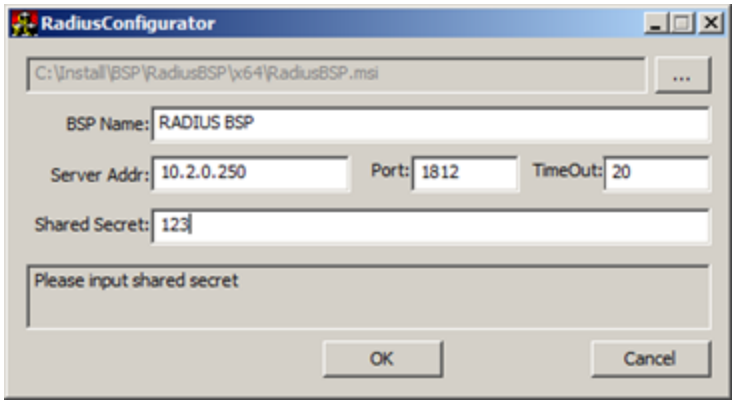
In order to use the configurator tool the user has to have **Local Administrator** privileges.

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**.



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

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

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.

RADIUS BSP Policies

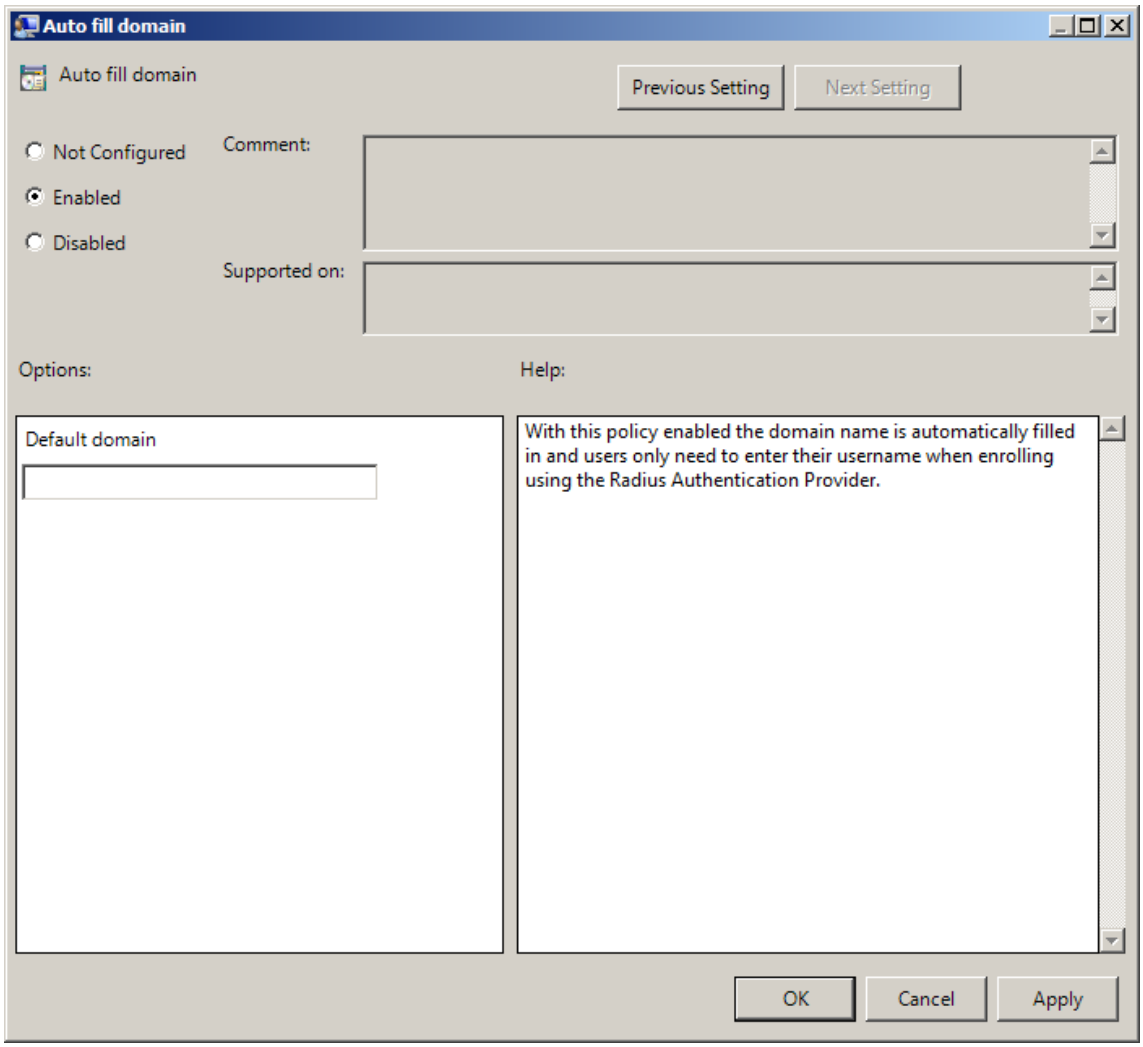
The **RADIUS BSP** section includes policies allowing you to edit RADIUS authentication settings.

It includes:

- Auto fill domain
- Enable auto enroll

Auto Fill Domain

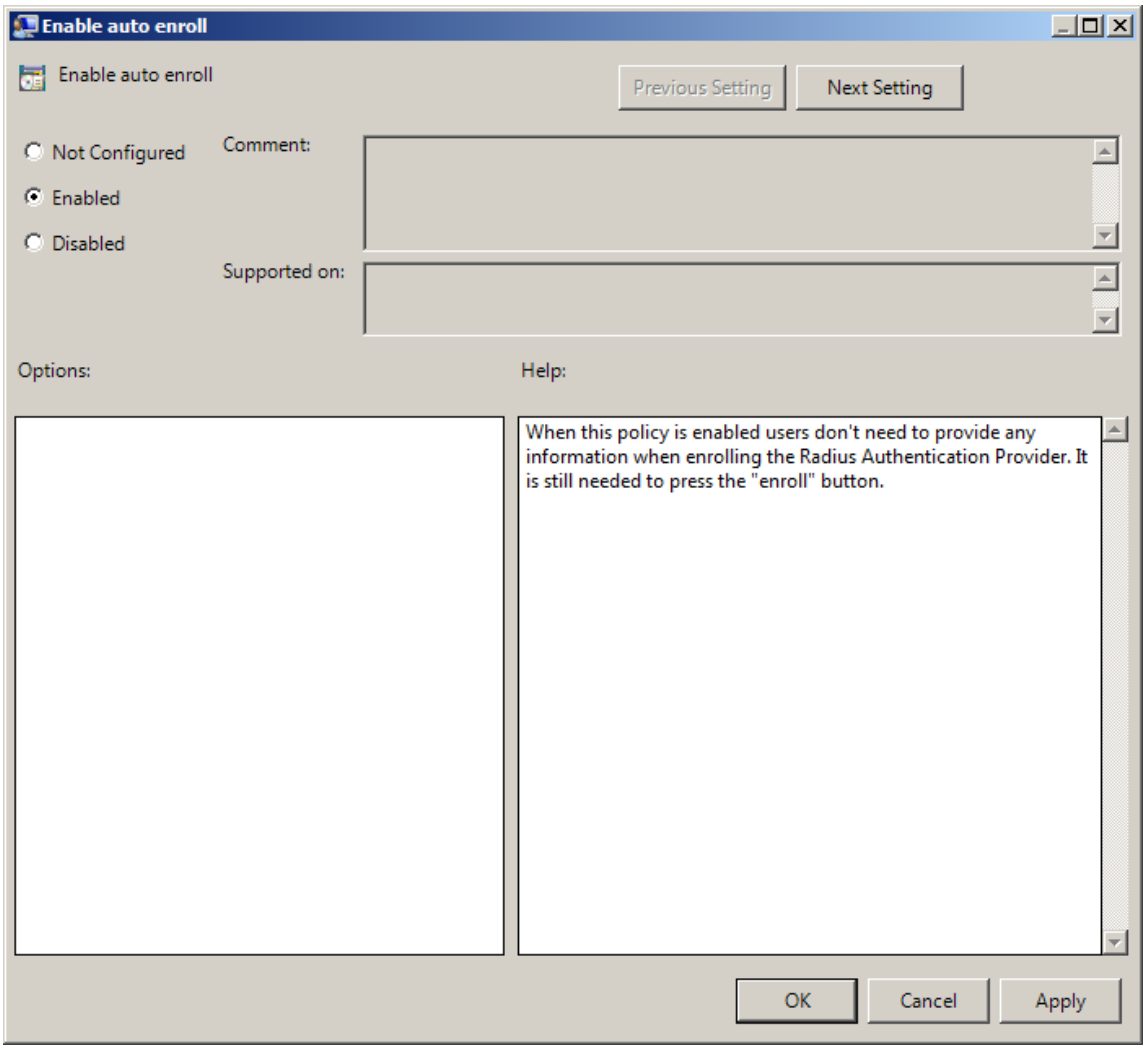
With the **Auto fill domain** policy enabled the domain name is automatically filled in and users only need to enter their username when enrolling using the RADIUS Authentication Provider.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BioAPI\BSP\OathBSP
parameter: AutoFillDomain (REG_DWORD)
value: netiq
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 press the **Enroll** button.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BioAPI\BSP\RadiusBSP
parameter: EnableAutoEnroll (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

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 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

R

S

W