

NetIQ Advanced Authentication Framework

RADIUS Authentication Provider Configuration Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	
Introduction	
About This Document	
RADIUS Authenticator Overview	4
Setting RADIUS Authenticator	6
Microsoft Windows Server 2008	6
Microsoft Windows Server 2003	
Configuration Procedure	
RADIUS BSP Policies	14
Auto Fill Domain	15
Enable Auto Enroll	
Troubleshooting	17
Cannot Install RADIUS Authentication Provider after Configuration	
Invalid Configuration Data Input Error	
Index	

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.

Simportant 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
- <u>Microsoft Windows Server 2003</u>

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).

Advanced an existing template: and Address y name: r ss (IP or DNS): 0.250		¥
ole this RADIUS client ect an existing template: and Address y name: r ss (IP or DNS): 0.250		y
ect an existing template: and Address y name: r ss (IP or DNS): 1.250		V
and Address ly name: r ss (IP or DNS): 1.250		Y
and Address ly name: r ss (IP or DNS):).250		
and Address ly name: r ss (IP or DNS):).250		
ss (IP or DNS): 1.250		
ss (IP or DNS):).250		
ss (IP or DNS):).250		
J.25U		Verifie
		veniy
d Secret		
an existing Shared Secrets template	e:	
		•
nually type a shared secret, click Ma , click Generate. You must configure entered here. Shared secrets are ca	anual. To automatically g the RADIUS client with ase-sensitive.	enerate a shared the same shared
anual O Generate		
d secret:		_
n shared secret:		_
		a 1

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

y of Connections	to other access se	ervers Properties		
verview Condition	s Constraints Settin	ngs		
olicy name:	Copy of Conn	iections to other access serv	ers	
Policy State	valuates this policy wh	ile performing authorization. I	lf disabled, NPS does no	ot evaluate this policy.
Policy enabled				
Access Permissio	1			
If conditions and access. What is	constraints of the net access permission?	work policy match the conn	ection request, the poli	cy can either grant access or deny
Grant access.	Grant access if the cor	nnection request matches thi	s policy.	
C Deny access.)eny access if the cor	nnection request matches this	s policy.	
Ignore user ac	ount dial-in properties			
If the connection authorization wi	n request matches the h network policy only;	conditions and constraints o do not evaluate the dial-in p	of this network policy and roperties of user account	d the policy grants access, perform its .
Network connect	on method			
Select the type of or Vendor specific select Unspecified	network access serve , but neither is required	r that sends the connection r d. If your network access ser	request to NPS. You car rver is an 802.1X authen	n select either the network access server type nticating switch or wireless access point,
• Type of netwo	rk access server:			
Unspecified		•		
C Vendor specif	D :			
10 *				

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

opy of Connections to other access se	vers Properties	×
Overview Conditions Constraints Setting	js	
Configure the constraints for this network po If all constraints are not matched by the con Constraints: Constraints	licy. nection request, network access is denied.	
Authentication Methods	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.	
Called Station ID	EAP Types: Move Up	
NAS Port Type	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 	
	 User can change password alter 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 Ap	ylc

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.

Connections to other access servers Properties	'×
Settings	
Specify the conditions that connection requests must match.	
Policy <u>c</u> onditions:	
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;	
A <u>d</u> d <u>E</u> dit <u>R</u> emove	
If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.	
[Edit Profile]	
Unless individual access permissions are specified in the user profile, this policy controls access to the network.	
If a connection request matches the specified conditions: O De <u>n</u> y remote access permission	
<u>G</u> rant remote access permission	
OK Cancel <u>A</u> pply	

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**.

RadiusConfigurator		
C:\Install\BSP\RadiusBSP\x64\Rad	iusBSP.msi	
BSP Name: RADIUS BSP		
Server Addr: 10.2.0.250	Port: 1812	TimeOut: 20
Shared Secret: 123		
Please input shared secret		
	ОК	Cancel

D 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.

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.

🔙 Auto fill domain		-02	×
Auto fill domain		Previous Setting Next Setting	
 Not Configured Enabled Disabled 	Comment: Supported on:	×	
Options:		Help:	
Default domain		With this policy enabled the domain name is automatically filled in and users only need to enter their username when enrolling using the Radius Authentication Provider.	
		OK Cancel Apply	

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.

💭 Enable auto enroll				_ _ ×
Enable auto enrol	I	Previous Settin	g Next Setting	
O Not Configured	Comment:			<u> </u>
Enabled				
C Disabled	Supported on:			
Options:		Help:		
		When this policy is enabled information when enrolling is still needed to press the "	users don't need to provid the Radius Authentication enroll" button.	e any Provider. It
			OK Cancel	Apply

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

Troubleshooting

1 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

	Α	
Authentication 1, 3-4, 11		
Authenticator 3		
	С	
Client 3-4		
Create 6, 11		
	D	
Data 17		
Domain 15		
	E	
Edit 11		
Enroll 16 Error 17		
	-	
	F	
File 17		
	Κ	
Key 4		
	L	
Local 13		
Logon 3		
	М	
Microsoft Windows Server 2003 6, 11		
Microsoft Windows Server 2008 6		
	Ν	
Network 4, 6		
	Ρ	
Policy 6		
Properties 11		

Protocol 4

R RADIUS 1, 3-4, 6, 11, 13-17 Remote 4 Security 4 Server 6, 13 W

Windows 11