

NetIQ Advanced Authentication Framework - Extensible Authentication Protocol Server

Administrator's Guide

Version 5.1.0

Table of Contents

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

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.

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, 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 and Microsoft Windows 8.

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**. Press **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 **Connections to Other Access Servers** policy and make it a granting one.

erview Conditions	Constraints Settings	1			
blicy name:	Copy of Connect	ions to other access se	rvers		
Policy State	uates this policy while r	performing authorization	. If disabled, NPS does	not evaluate this policy	
Policy enabled					
Access Permission					
If conditions and co access. <u>What is ac</u>	nstraints of the networ cess permission?	k policy match the cor	nnection request, the p	olicy can either grant a	iccess or deny
Grant access. Gr	int access if the conne	ction request matches t	his policy.		
🖱 Deny access. De	ny access if the conne	ction request matches th	nis policy.		
Ignore user acco	int dial-in properties.				
If the connection authorization with	equest matches the co network policy only; do	nditions and constraints not evaluate the dial-in	of this network policy a properties of user accord	nd the policy grants ac unts .	cess, perform
Network connection	method				
Select the type of ne or Vendor specific, b select Unspecified.	work access server th ut neither is required. I	at sends the connectior your network access s	n request to NPS. You c erver is an 802.1X auth	an select either the net enticating switch or win	work access server type eless access point,
Type of network	access server:				
Unspecified		•			
C Vendor specific:					
10 📫					

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

Copy of Connections to other access ser	vers Properties	X
Overview Conditions Constraints Setting	35	
Overview Conditions Constraints Setting Configure the constraints for this network point all constraints are not matched by the constraints: Constraints Constraints: Constraints Constraints Image: Authentication Methods Image: Authentication Methods Image: Constraint and the constraint and t	Is licy. nection request, network access is denied. 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	

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

A	dd EAP
	Authentication methods:
	Microsoft: Smart Card or other certificate
	Microsoft: Protected EAP (PEAP)
	MICROSOFT: Secured password (EAP-MISCHAP v2)
	OK Cancel

Choose **NAAF EAP**:

Add EAP	×
Authentication methods:	
Microsoft: Smart Card or other certificate	
Microsoft: Protected EAP (PEAP)	
Microsoft: Secured password (EAP-MSCHAP v2)	
NAAF EAP	
OK Cancel	1
	,

6. The **NAAF EAP** type is successfully added and to create VPN connection the **Apply** button should be pressed:

Copy of Connections to other access ser	vers Properties	X
Overview Conditions Constraints Setting	s	
Overview Conditions Constraints Setting Configure the constraints for this network polifial constraints are not matched by the control Constraints Constraints: Constraints Constraints Image: Constraints of this network polification Methods Constraints Image: Constraints Image: Constraints Constraints Image: Constraints Constraintex Const	s icy. nection request, network access is denied. 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: NAAF EAP Move Up Move Down Add Edit Remove Less secure authentication methods: Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Microsoft Encrypted authentication (PAP, SPAP) Allow clients to connect without neootiating an authentication method	
	Perform machine health check only	
	,	
	OK Cancel Apply	

Logon to VPN

Make sure that VPN connection is configured correctly. For more information, see <u>Configuration of VPN Connection</u> 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).

VPN Connection Properties	×
General Options Security Networking Sh	aring
Type of VPN:	
Automatic	•
	Advanced settings
Data encryption:	
Require encryption (disconnect if server decli	nes)
Authentication	
Use Extensible Authentication Protocol (EAP)
NAAF EAP (encryption enabled)	<u> </u>
Microsoft: Protected EAP (PEAP) (encryp Microsoft: Secured password (EAP-MSC	ition enabled) HAP v2) (encryption enabl
Microsoft: Smart Card or other certificate	(encryption enabled)
EAP-MSUHAPV2 will be used for IKEV2	/PN type. Select
any of these protocols for other VPN type	·S.
Unencrypted password (PAP)	
🗖 Challenge Handshake Authentication	Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP	v2)
Automatically use my Windows lo	gon name and
password (and domain, if any)	
0	K Cancel

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

	NetIQ.	X
Please enter usern press "Next >>".	ame, select logon method, and	Next >>
Username: Logon method: Domain: Use current set	Card	Options << Cancel

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**.
- 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. Check the **Use as smart card** box in case if smart card will be used to authenticate to VPN connection.
- 11. Check the **Allow other people to use this connection** box to provide anyone with access to the computer to use this connection.
- 12. Check the **Don't connect now; just set it up so I can connect later** 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, check the **Show characters** box to view the password.
- 17. Check the **Remember this password** 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. After clicking on the **Authentication** tab, it is possible to select from the list of network authentication methods **NAAF EAP**.

Networking Authentication	
Select this option to provide authenticated network access for this Ethemet adapter.	
Time I'm logged on Fallback to unauthorized network access Additional Settings	
OK Cancel	

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 logons 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

	Α
Administrator 1, 3, 5 Authentication 1, 3, 5, 9, 12 Authenticator 3	
	С
Client 4 Connection 9, 11 Control 11	
	D
Domain 11	
	E
Error 14	
	L
Local 5	
Logon 5, 9, 12	N
Network 5.9.11	
Network 5, 5, 11	Р
Package 14 Password 11 Policy 5	
Properties 9	
Protocol 1, 3	
	S
Security 9 Server 4-5, 13-14 Support 4, 14	
	U

User 11