NetIQ Advanced Authentication Framework - Network Policy Server (NPS) Plugin

Administrator's Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This NPS Administrator Guide is intended for system administrators and describes the work of NetIQ Advanced Authentication Framework – Network Policy Server Plugin.

Document Conventions

This document uses the following 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.

ℹ **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.

NPS Logon Method Selection

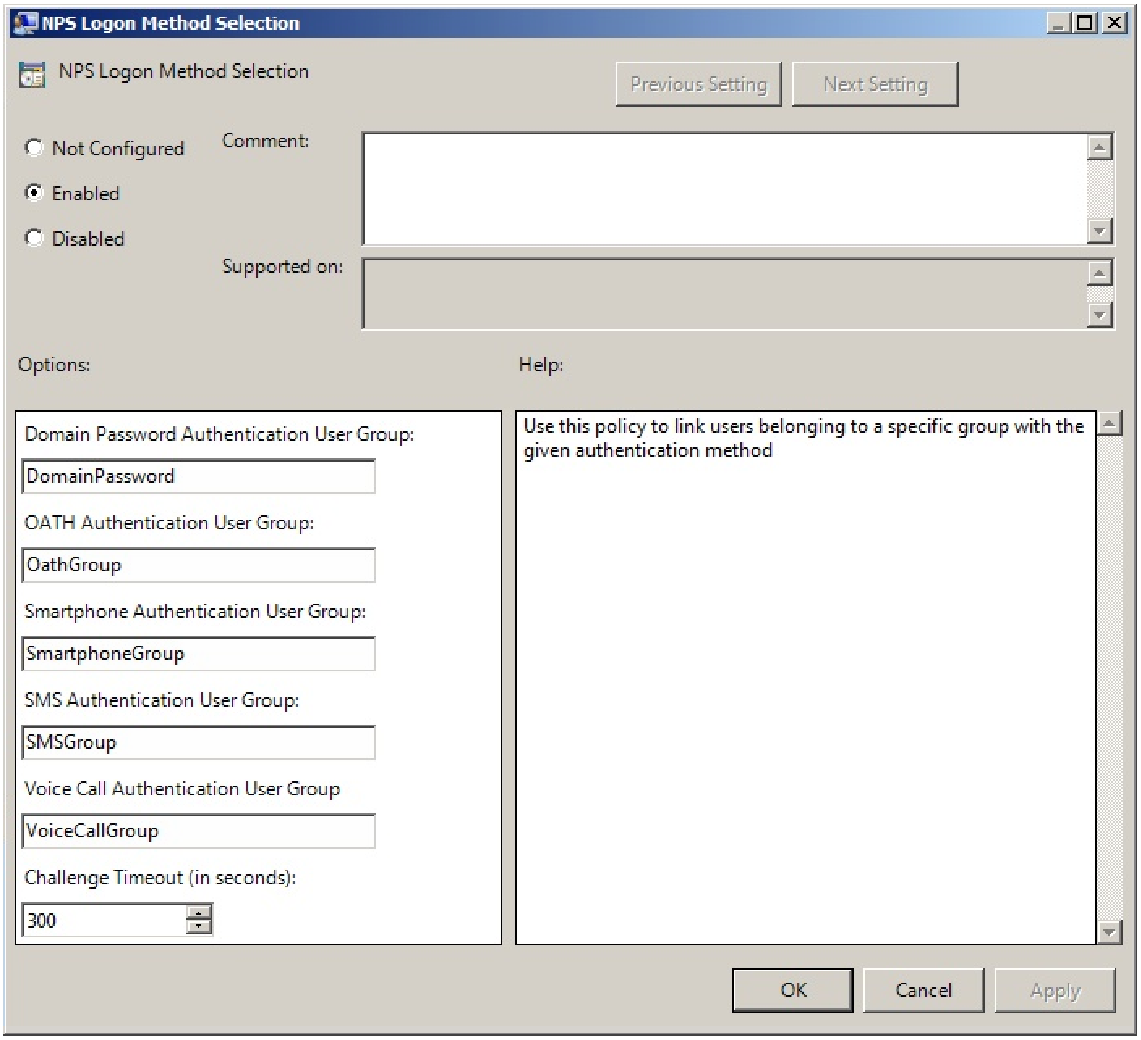
The **NPS Logon Method Selection** policy allows you to link users belonging to a specific group with the given authentication method. AD group names should be specified in the fields. Users should be included in these groups directly (group inheritance doesn't work). If the user is the member of several groups, the first group from the list will be used and the corresponding authentication method will be selected. If the user is not a member of any group, it will be required to enter the domain password during authentication.

The policy is included in the **NPS** subfolder of the **Security** section which is located in **Group Policy Management Editor** under **Computer Configuration -> Policies -> Administrative Templates: Policy definitions -> NetIQ Advanced Authentication Framework**.

✱ MSCHAPv2 protocol is supported by all authentication providers except for SMS AP. SMS AP requires PAP protocol.

✱ To access policy sections, NetIQ Administrative Tools or NetIQ Group Policy Templates should be preliminary installed.

✱ The **Challenge Timeout** option is available starting from NetIQ Advanced Authentication Framework v4.11. It provides with a capability to specify time during which authentication with an applicable authentication provider should be confirmed.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Domain Password Authentication User Group: DomainPassword

OATH Authentication User Group: OathGroup

Smartphone Authentication User Group: SmartphoneGroup

SMS Authentication User Group: SMSGroup

Voice Call Authentication User Group: VoiceCallGroup

Challenge Timeout (in seconds): 300

Help:

Use this policy to link users belonging to a specific group with the given authentication method

To access the **NPS Logon Method Selection** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates - > Authasas Advanced AuthenticationNetIQ Advanced Authentication Framework -> Security -> NPS**.

Registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework

NPSLogonMethodSelection:

- value type: REG_DWORD
- value data: 0x00000001 (1)
- description: 1 means that the policy is enabled

ChallengeTimeout:

- value type: REG_DWORD
- value data: 0x0000012c (300)
- description: 300 displays duration of NPS logon timeout (in seconds)

DomainPasswordUserGroup:

- value type: REG_SZ
- value data: DomainPassword
- description: DomainPassword displays the name of the group for which authentication with domain password will be selected

OathUserGroup:

- value type: REG_SZ
- value data: OathGroup
- description: OathGroup displays the name of the group for which OATH OTP authentication method will be selected

OobUserGroup:

- value type: REG_SZ
- value data: SmartphoneGroup
- description: SmartphoneGroup displays the name of the group for which Smartphone authentication method will be selected

SmsUserGroup:

- value type: REG_SZ
- value data: SMSGroup
- description: SMSGroup displays the name of the group for which SMS authentication method will be selected

VoiceUserGroup:

- value type: REG_SZ
- value data: VoiceCallGroup
- description: VoiceCallGroup displays the name of the group for which Voice Call authentication method will be selected

Return Password

It may be required for NPS to return a user's password. E.g. this may be required for Citrix NetScaler Gateway (check the article Configuring Password Return with RADIUS for details). To enable the **Return Password** feature open the HKEY_ LOCAL_ MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework registry key on NPS and create the following parameter:

ReturnPassword:

- value type: REG_DWORD
- value data: 0x00000001 (1)

These are the required Citrix Netscaler Gateway settings:

Password Vendor Identifier must be set to 1094795552.

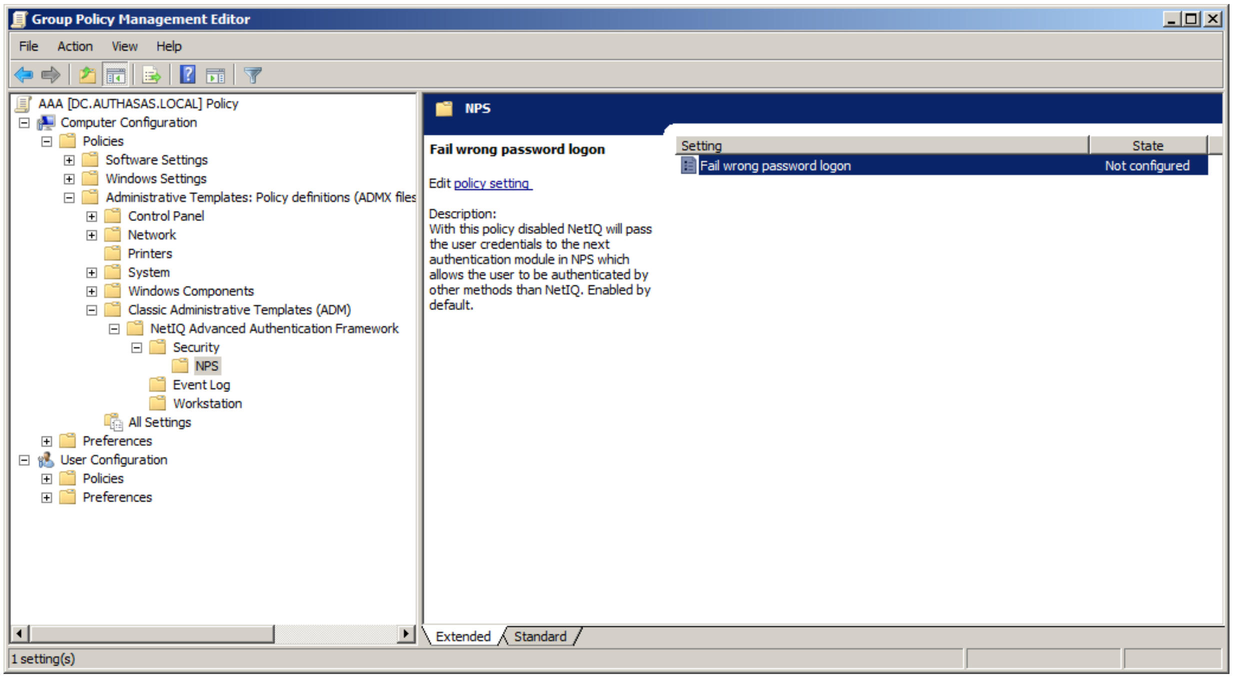
Password Attribute Type must be set to 2.

The **Return Password** feature is presented from version 4.12 and currently only PAP protocol is supported.

Fail Wrong Password Logon Policy

The **Fail wrong password logon** policy is used in version 4.10.212 and earlier.

With the **Fail wrong password logon**policy disabled NetIQ will pass the user credentials to the next authentication module in NPS which allows the user to be authenticated by other methods than NetIQ. The policy is enabled by default.



Fail wrong password logon

Edit policy setting

Description:
With this policy disabled NetIQ will pass the user credentials to the next authentication module in NPS which allows the user to be authenticated by other methods than NetIQ. Enabled by default.

Setting	State
Fail wrong password logon	Not configured

If NPS plugin is installed, OATH OTP or Smartphone authentication provider are used in RADIUS authentication instead of usual domain password. If the **Fail wrong password logon**policy is enabled, NPS plugin is installed and the user has inputted domain password instead of OTP, the authentication should be successful. Both OTP and domain password will cause successful authentication.

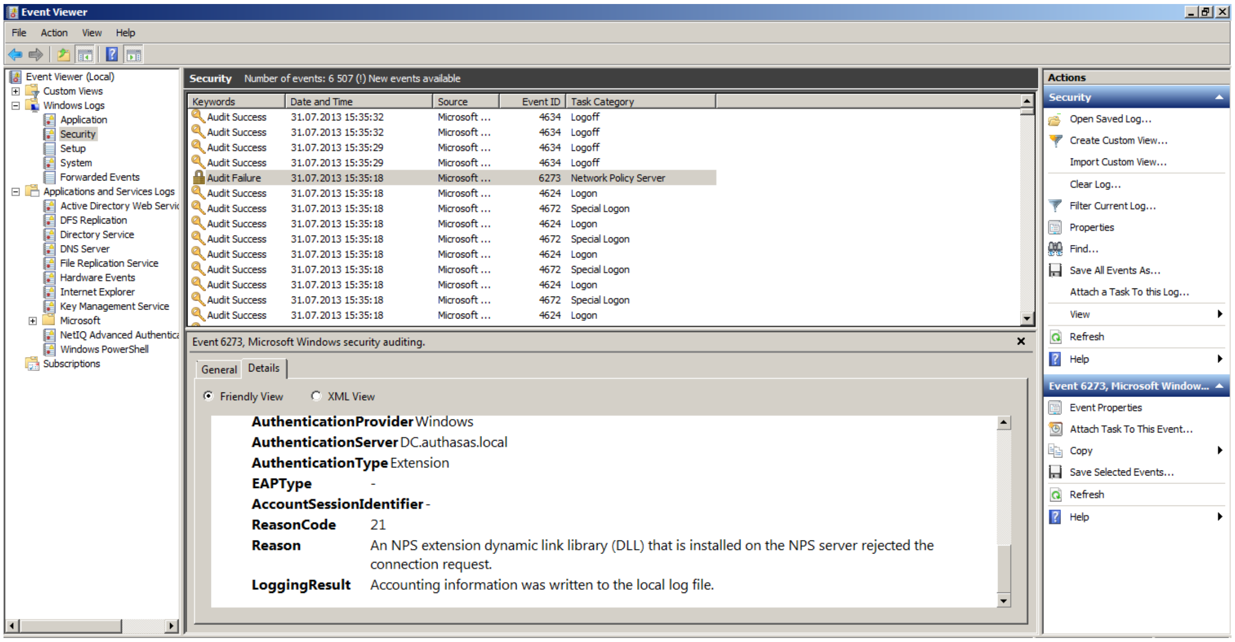
Troubleshooting

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

Impossible To Authenticate Using One of Methods of Authentication

Description:

Authentication using one of methods of authentication has failed.



Security Number of events: 6 507 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	31.07.2013 15:35:32	Microsoft ...	4634	Logoff
Audit Success	31.07.2013 15:35:32	Microsoft ...	4634	Logoff
Audit Success	31.07.2013 15:35:29	Microsoft ...	4634	Logoff
Audit Success	31.07.2013 15:35:29	Microsoft ...	4634	Logoff
Audit Failure	31.07.2013 15:35:18	Microsoft ...	6273	Network Policy Server
Audit Success	31.07.2013 15:35:18	Microsoft ...	4624	Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4672	Special Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4624	Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4672	Special Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4624	Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4672	Special Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4624	Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4672	Special Logon
Audit Success	31.07.2013 15:35:18	Microsoft ...	4624	Logon

Event 6273, Microsoft Windows security auditing.

AuthenticationProvider	Windows
AuthenticationServer	DC.authasas.local
AuthenticationType	Extension
EAPType	-
AccountSessionIdentifier	-
ReasonCode	21
Reason	An NPS extension dynamic link library (DLL) that is installed on the NPS server rejected the connection request.
LoggingResult	Accounting information was written to the local log file.

Cause:

An NPS extension dynamic link library (DLL) that is installed on the NPS server rejected the connection request.

Solution:

Please, try to authenticate using the correct method of authentication. If the reason of the failed authentication is another, then open **Event Viewer** > **Windows logs> Security** to find out the reason of the failed authentication.

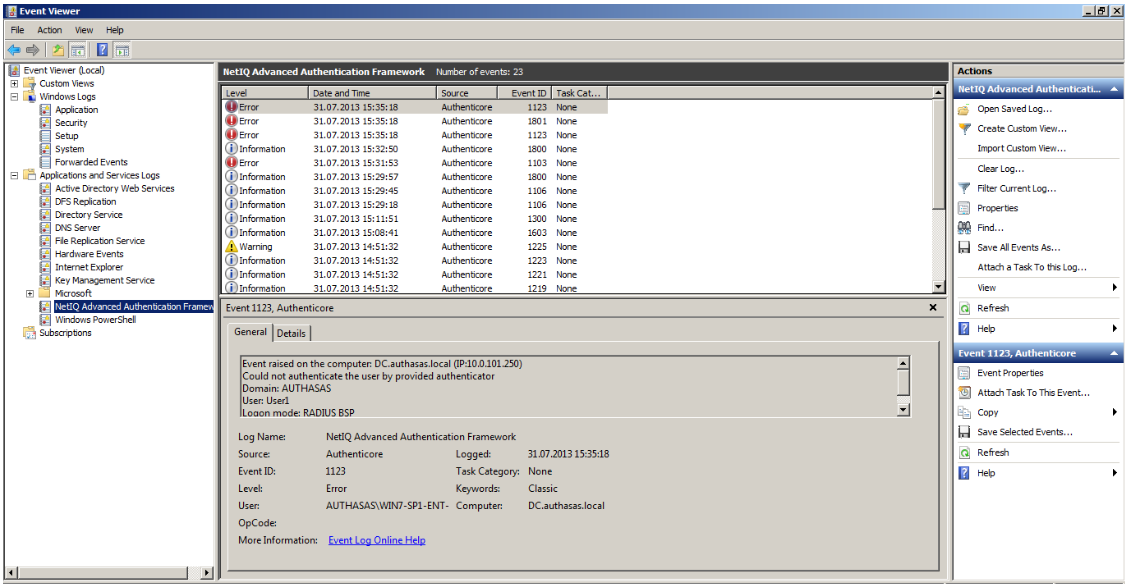
Authentication Using OTP Has Failed

Description:

Authentication using OTP has failed.

Cause:

NPS plugin is not installed.



NetIQ Advanced Authentication Framework Number of events: 23

Level	Date and Time	Source	Event ID	Task Cat...
Error	31.07.2013 15:35:18	Authenticore	1123	None
Error	31.07.2013 15:35:18	Authenticore	1801	None
Error	31.07.2013 15:35:18	Authenticore	1123	None
Information	31.07.2013 15:32:50	Authenticore	1800	None
Error	31.07.2013 15:31:53	Authenticore	1103	None
Information	31.07.2013 15:29:57	Authenticore	1800	None
Information	31.07.2013 15:29:45	Authenticore	1106	None
Information	31.07.2013 15:29:18	Authenticore	1106	None
Information	31.07.2013 15:11:51	Authenticore	1300	None
Information	31.07.2013 15:08:41	Authenticore	1603	None
Warning	31.07.2013 14:51:32	Authenticore	1225	None
Information	31.07.2013 14:51:32	Authenticore	1223	None
Information	31.07.2013 14:51:32	Authenticore	1221	None
Information	31.07.2013 14:51:32	Authenticore	1219	None

Event 1123, Authenticore

General | Details

```
Event raised on the computer: DC.authasas.local (IP:10.0.101.250)
Could not authenticate the user by provided authenticator
Domain: AUTHASAS
User: User1
Logon mode: RADIUS BSP
```

Log Name:	NetIQ Advanced Authentication Framework		
Source:	Authenticore	Logged:	31.07.2013 15:35:18
Event ID:	1123	Task Category:	None
Level:	Error	Keywords:	Classic
User:	AUTHASAS\WIN7-SP1-ENT-	Computer:	DC.authasas.local
OpCode:			
More Information:	Event Log Online Help		

Solution:

Please, install NPS plugin to authenticate using OTP.

Index