



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

Administrator's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Fail Wrong Password Logon Policy	4
NPS Logon Method Selection	5
Troubleshooting	8
Impossible To Authenticate Using One of Methods of Authentication	8
Authentication Using OTP Has Failed	9
Index	10

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.



Notes. This sign indicates supplementary information you may need in some cases.



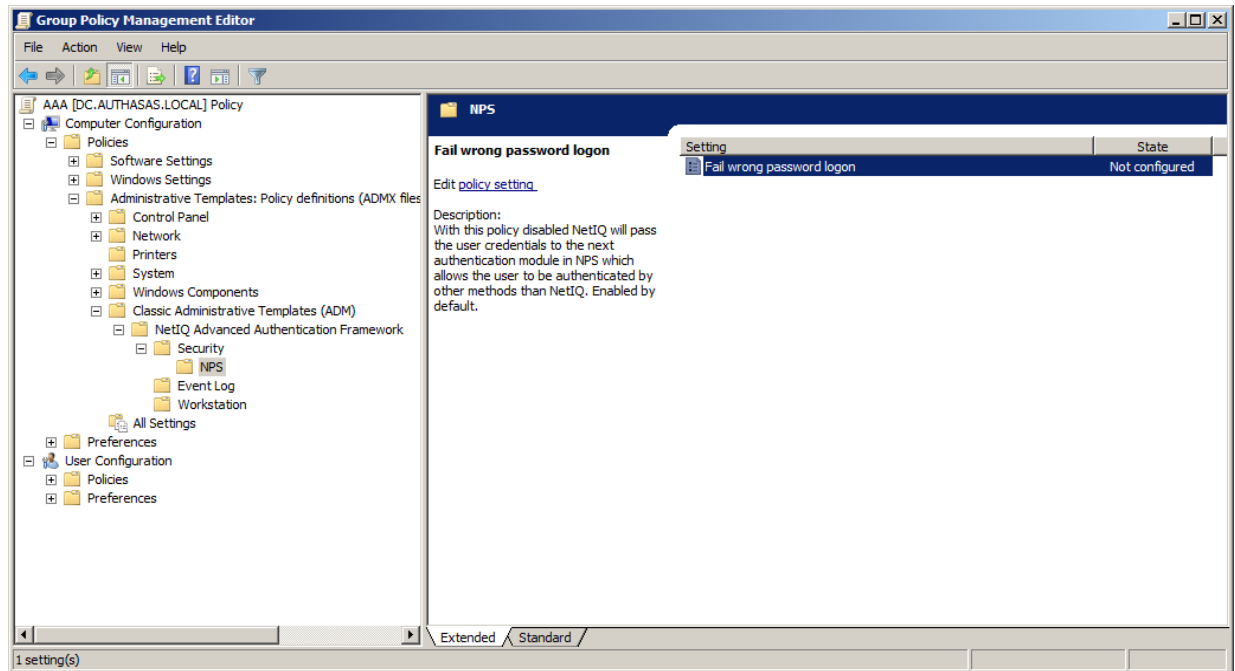
Tips. This sign indicates recommendations.

- 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.

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.






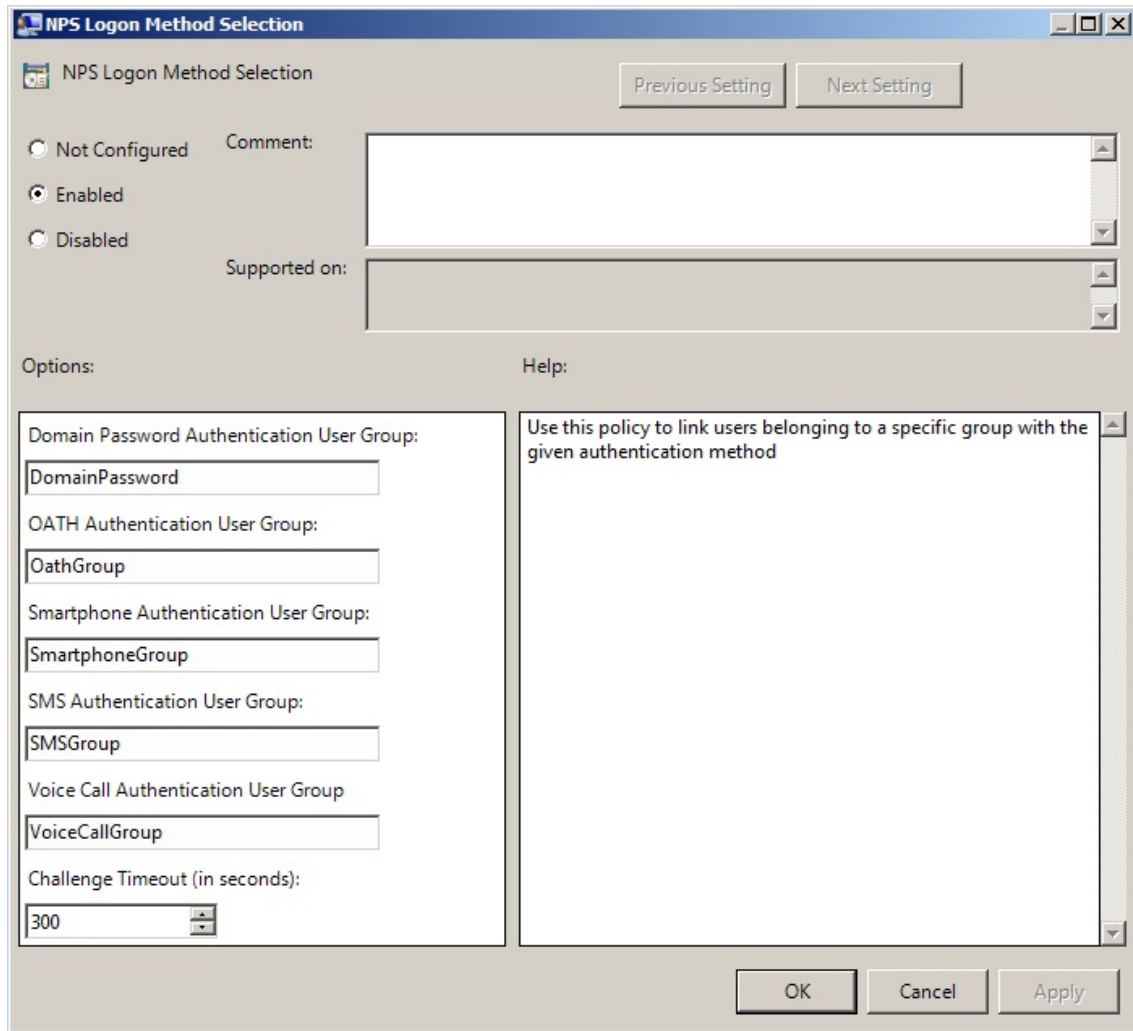
If NPS plugin is installed, OATH OTP or Smartphone authentication provider are used in RADIUS authentication instead of usual domain password. If the **Fail wrong password logon** policy is enabled, NPS plugin is installed and the user has inputted domain password instead of OTP, the authentication should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

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.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework

NPSLogonMethodSelection:

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

ChallengeTimeout:

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

DomainPasswordUserGroup:

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

OathUserGroup:

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

OobUserGroup:

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

SmsUserGroup:

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

VoiceUserGroup:

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

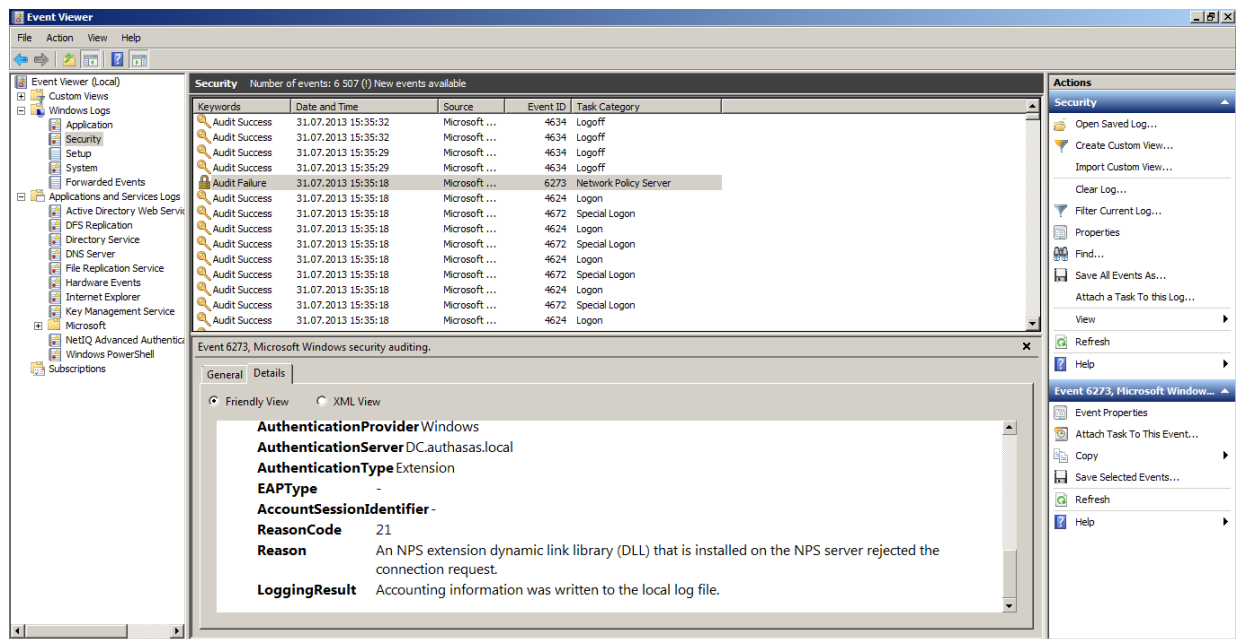
Troubleshooting

i 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.



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.

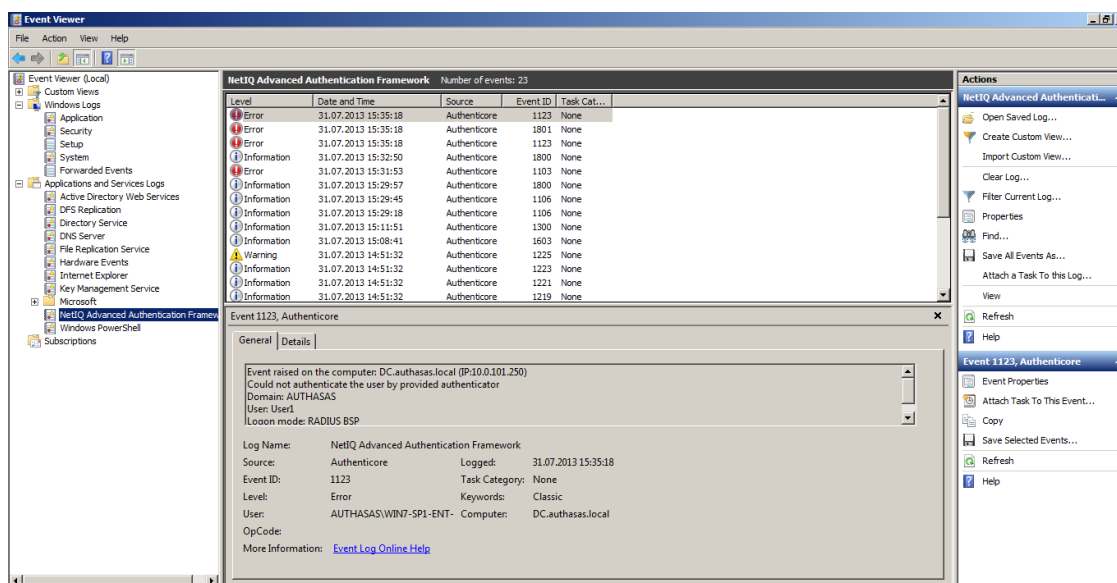
Authentication Using OTP Has Failed

Description:

Authentication using OTP has failed.

Cause:

NPS plugin is not installed.



Solution:

Please, install NPS plugin to authenticate using OTP.

Index

A

Administrator 1, 3
Authentication 1, 3, 5, 8-9
Authenticator 3

E

Event Viewer 8

L

Logon 3, 5

N

Network 1, 3

O

OATH 4, 7
OTP 4, 9

P

Password 4
Policy 5

S

Security 5