



NetIQ Advanced Authentication Framework

OATH Authentication Provider Configuration Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
OATH Authenticator Overview	4
Setting OATH Authenticator via Group Policy	5
HOTP Policy	6
PIN required	7
TOTP Policy	9
Index	10

Introduction

About This Document

Purpose of the Document


This OATH Authentication Provider Configuration Guide is intended for administrators and describes how to set the group policy of NetIQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to manage OATH 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

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.

OATH Authenticator Overview

The **OATH** (open authentication) authentication type takes its name from the Initiative for Open Authentication (OATH), which is a collaborative effort of IT industry leaders aimed at providing reference architecture for universal strong authentication across all users and all devices over all networks.

Open authentication addresses One Time Password (OTP) – based authentication method.

OTP-based authentication is intended to act as a bridge between legacy and modern applications. OTP credentials will facilitate integration with applications that rely solely on user passwords. Because end users are already familiar with static passwords, a device-generated password can greatly facilitate the transition to stronger authentication.

In OTP-based authentication method, login is performed using an essentially random password each time. The passwords are generated by a device, most commonly a hardware token associated with the user, and so the password is not based on the user's memory. This greatly increases security.

TOTP (Time-based One-time Password algorithm) is a variant of the OTP authentication, where the one-time password changes at frequent intervals (say, every two minutes). Each one-time password is generated by applying a random-looking cryptographic function to a unique series value. In the time-based case, the value is the current time.

HOTP (Hmac-based One-Time Password algorithm) is a variant of OTP authentication, where one-time password is valid for an unknown period of time. HOTP authentication relies on a shared secret and a moving factor. Every time a new OTP is generated, the moving factor will be incremented and as a result generated one-time passwords should be different every time.

Setting OATH Authenticator via Group Policy


After the installation of OATH BSP, **OATH BSP** policies will be successfully added.

The **OATH BSP** section includes the following policies allowing you to edit OATH authentication settings.

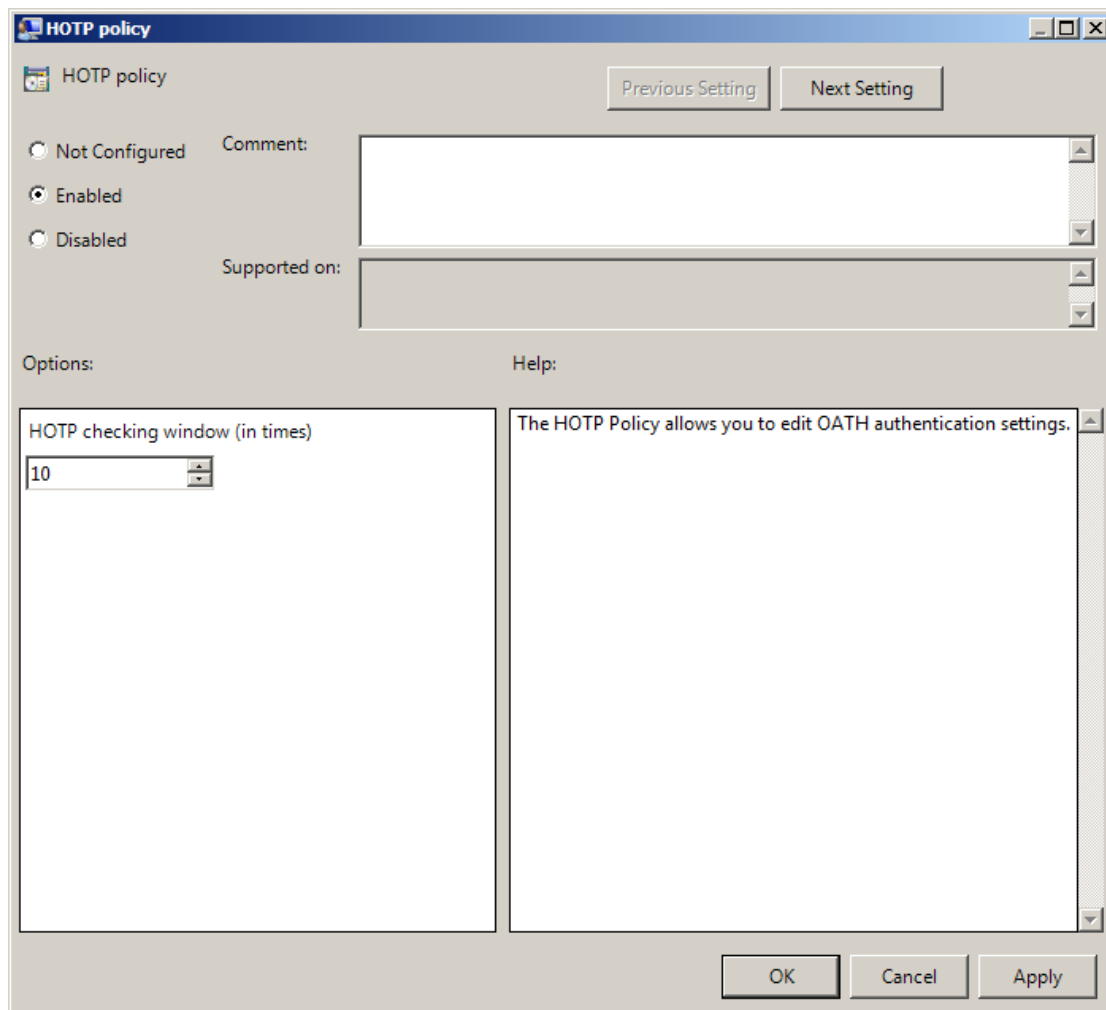
It includes:

- [HOTP policy](#)
- [PIN required](#)
- [TOTP policy](#)

HOTP Policy

 Please, take into consideration that schema should be extended by bioHotpCounter.cmd script for HOTP support.

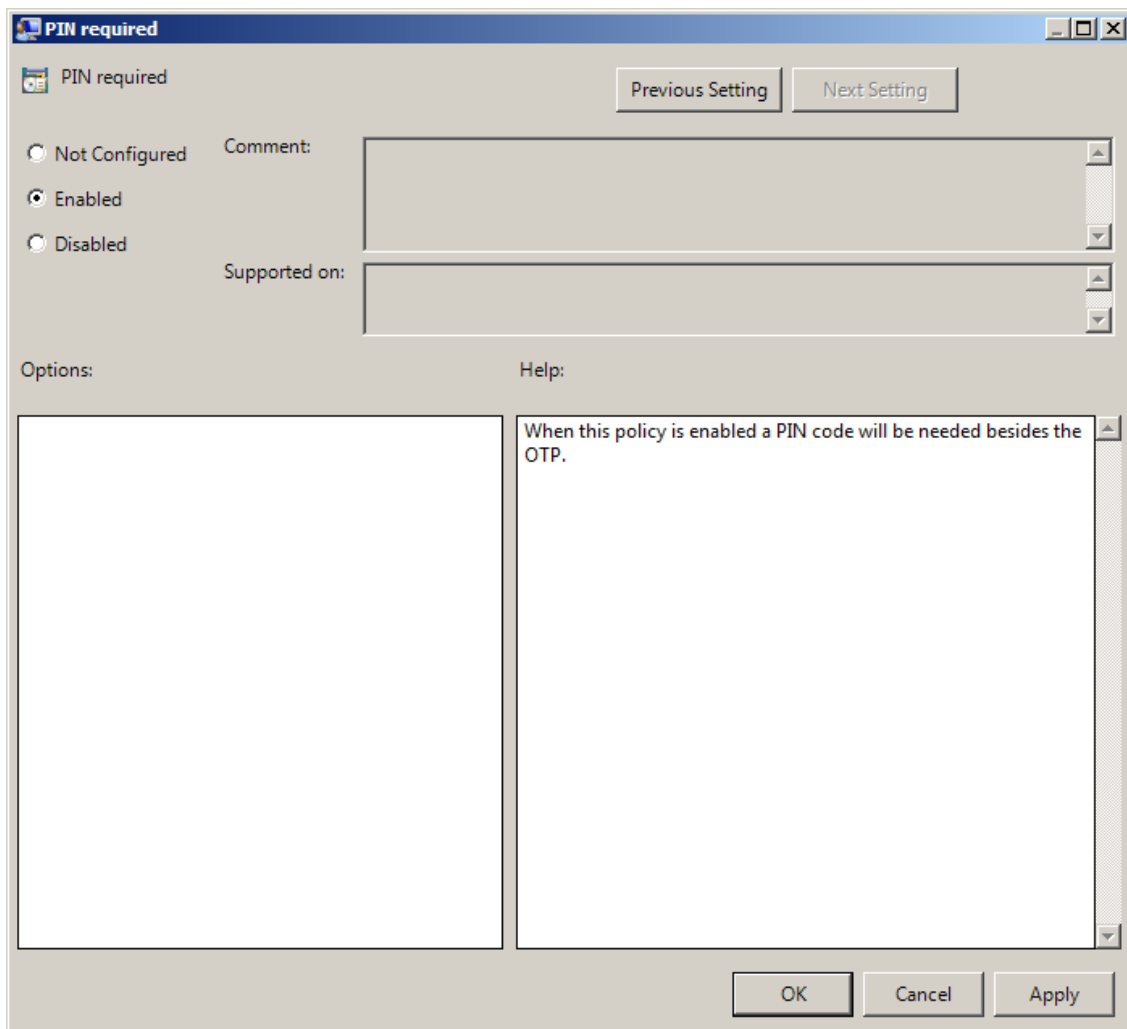
The **HOTP Policy** allows you to edit OATH authentication settings.




HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\BioAPI\BSP\OathBSP
parameter: HOTPWindow (REG_DWORD)
value: 0x0000000a (10)
10 displays the number of generated testing passwords.

PIN required

When the **PIN required** policy is enabled, a PIN code will be needed for authentication besides OTP. OTP and PIN should be inputted in one field. If you use the policy with the aim to use domain password instead of PIN, you should input OTP and domain password together in one field.



The screenshot shows a Windows-style dialog box titled "PIN required". At the top, there are two buttons: "Previous Setting" and "Next Setting". Below these, there are three radio buttons for configuration status: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with two empty text boxes. At the bottom left, there is an "Options:" section with an empty text box. At the bottom right, there is a "Help:" section with a text box containing the text: "When this policy is enabled a PIN code will be needed besides the OTP." At the very bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

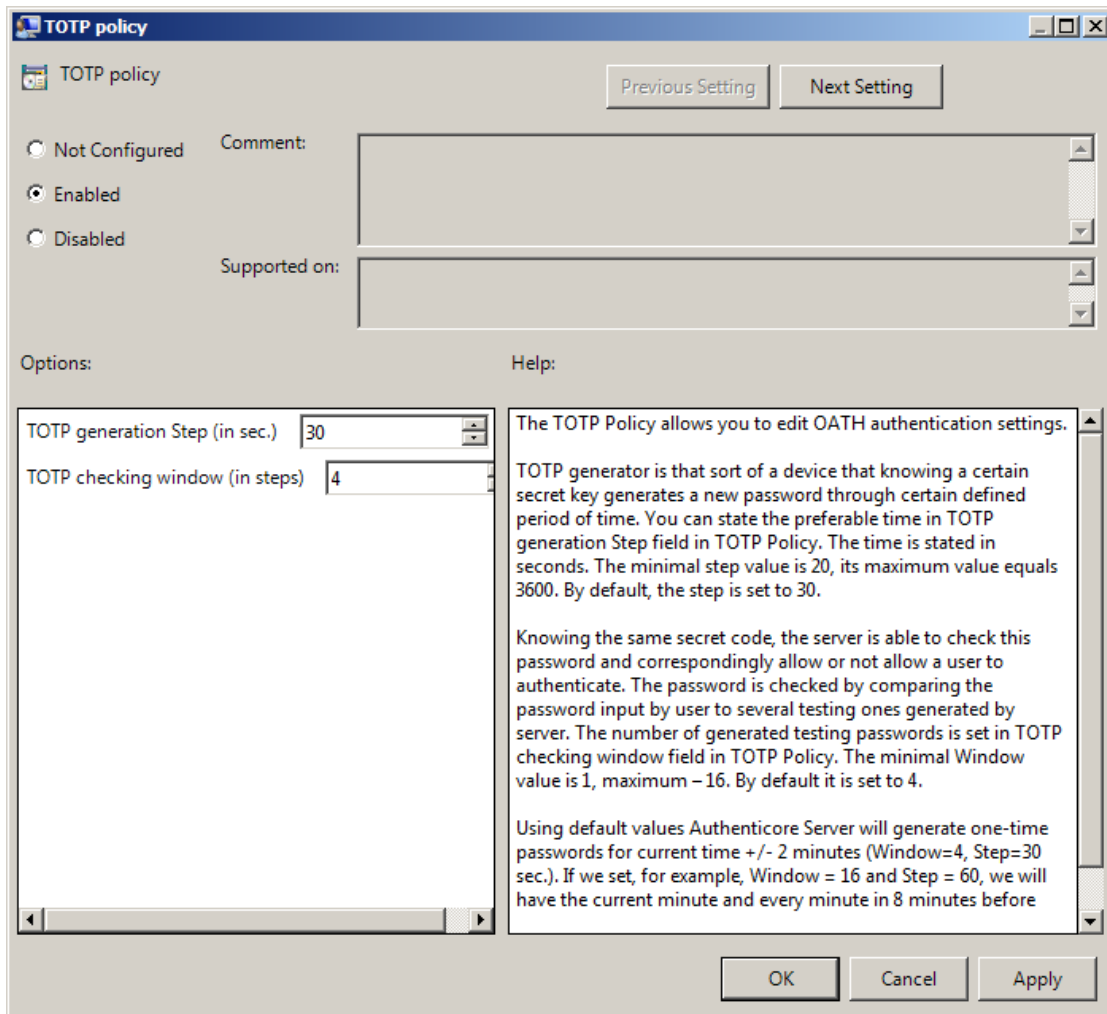
 To enable the **PIN Required** policy together with the **Use domain password as PIN** policy, it is necessary to install Password Filter on all Domain Controllers. Otherwise if the password is reset, changed or generated automatically, the password will be desynchronized and it will be required to re-enroll authenticators.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BioAPI\BSP\OathBSP
parameter: PinRequired (REG_DWORD)

value: 0x00000001 (1)
1 means that the policy is enabled

TOTP Policy

The **TOTP policy** allows you to edit OATH authentication settings.



HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\BioAPI\BSP\OathBSP

parameter: TOTPStep (REG_DWORD)

TOTPWindow (REG_DWORD)

value: 0x0000001e (30), 0x00000004 (4)

30 displays TOTP generation Step (in sec.)

4 displays TOTP checking window (in steps)

Index

A

Authentication 1, 3-4
Authenticator 3

C

Client 3

L

Logon 3

O

OATH 1, 3-6, 9
One-time Password 4
OTP 4, 7

P

Password 4, 7
PIN 5, 7
Policy 6

T

TOTP 4-5, 9