NetIQ Advanced Authentication Framework

OATH Authentication Provider Configuration Guide

Version 5.1.0

Table of Contents

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.

ℹ️ **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:

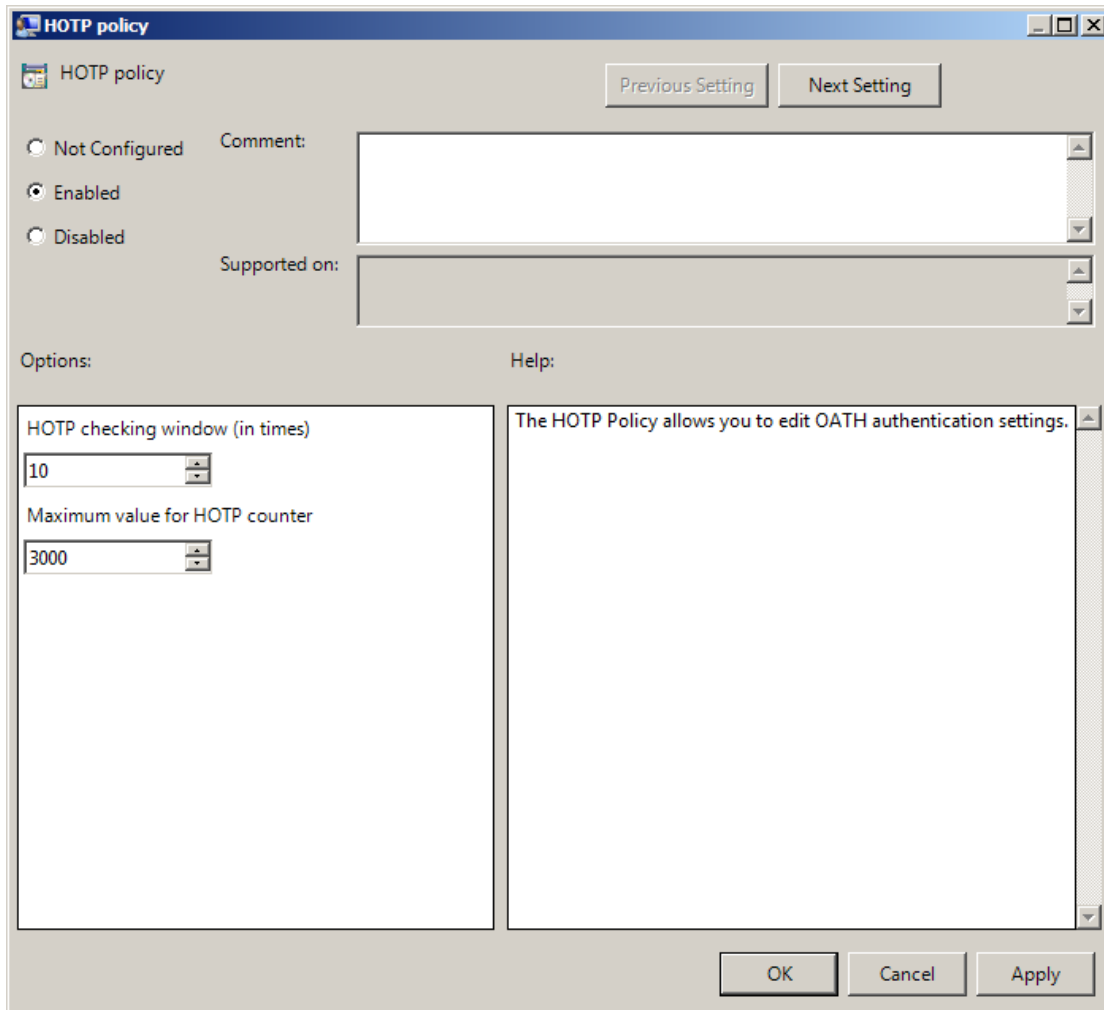- HOTP policy
- PIN required
- TOTP policy

HOTP Policy

The **HOTP policy** allows you to edit OATH authentication settings, in particular, to specify the number of generated OTPs to verify the match with the entered OTP during the enrollment and the maximum value for HOTP counter. The policy should be applied on both Authenticore Server and Client sides.

NetIQ increments an internal counter for an enrolled OATH HOTP authenticator every time a user authenticates using a YubiKey token. But if the user presses the YubiKey button not for authentication, the counter will be unsynchronized, because NetIQ will be waiting for the OTP which was already entered to a different place. If the user has pressed the YubiKey button the number of times which is greater than the specified **HOTP checking window** value, the authentication will fail. The **HOTP checking window** value equals to 10 by default.

The HOTP counter synchronization is performed automatically during re-enrollment.

If the **HOTP policy** is not configured and a token counter and a counter on NetIQ side are unsynchronized, it will be required just to re-enroll an OATH OTP authenticator.

The **Maximum value for HOTP counter** specifies a number of OTPs which NetIQ will enumerate starting from the stored on its side counter until the enumeration will reach the match with the entered OTPs during the enrollment. By default the parameter equals to 3000.

To access the **HOTP policy** in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> OATH Authentication Provider**.

Registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)Policies\BioAPI\BSP\OathBSP
HOTPWindow:
- value type: REG_DWORD
- value data: 0x0000000a (10)
- description: 10 displays the number of generated OTPs to verify the match with the entered OTP during the enrollment. 10 is the recommended value. The increase of the value may affect the Authenticore Server performance.
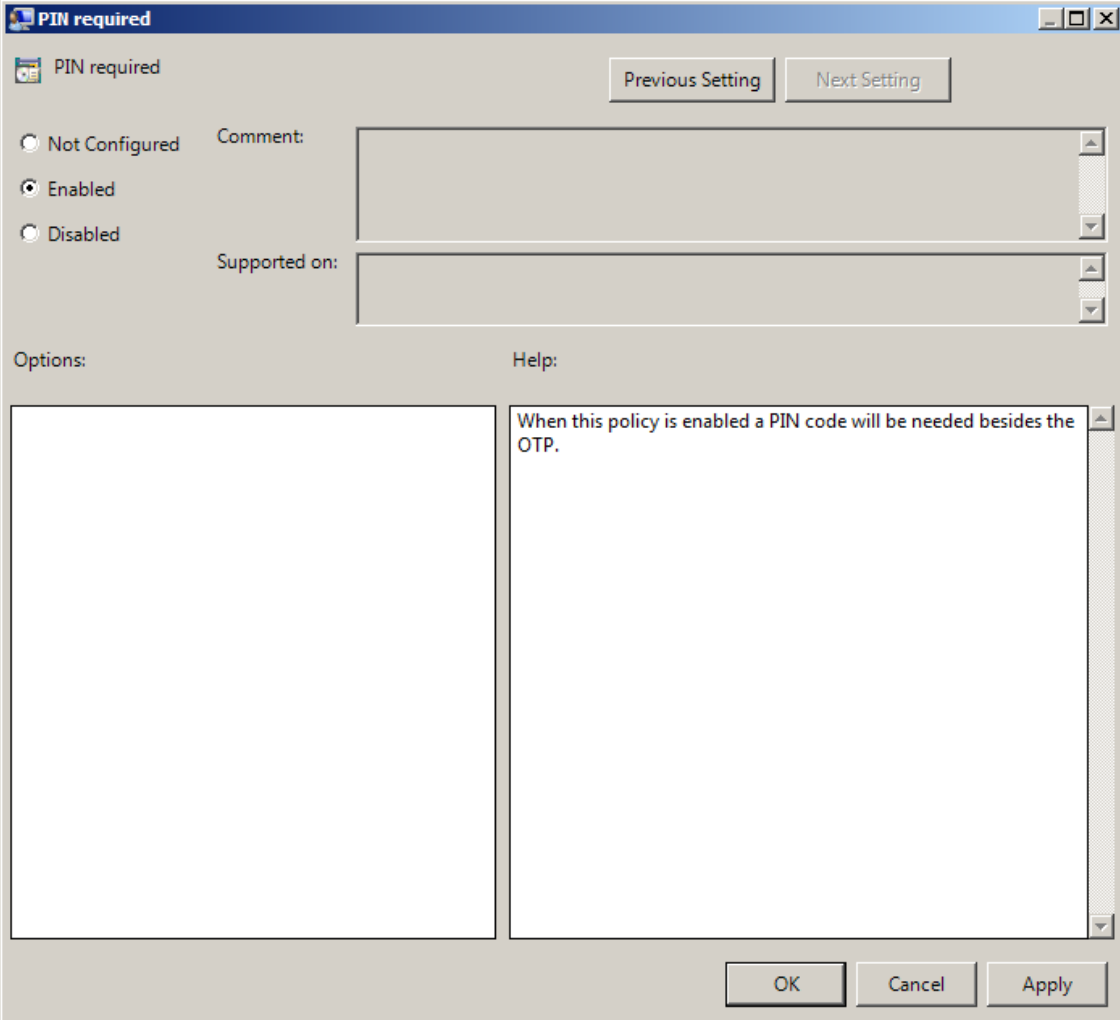
HotpSyncMaxCounter:
- value type: REG_DWORD
- value data: 0x00000bb8 (3000)

- description: 3000 displays the number of OTPs that are enumerated during the enrollment to synchronize HOTP counter. 3000 is the recommended value. The increase of the value may affect the Authenticore Server performance.

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.

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.

© *NetIQ*

To access the **PIN required** policy in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> OATH Authentication Provider**.

Registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BioAPI\BSP\OathBSP
PinRequired:
- value type: REG_DWORD
- value data: 0x00000001 (1)
- description: 1 means that the policy is enabled

TOTP Policy

The **TOTP policy** allows you to edit OATH authentication settings. In particular, it provides with a capability to specify TOTP generation step and the number of generated testing passwords.

To access the **TOTP policy** in the **Group Policy Management Editor** console, expand the following path: **Computer Configuration -> Policies -> Administrative Templates -> OATH Authentication Provider**.

Registry settings:
HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node\)Policies\BioAPI\BSP\OathBSP
TOTPStep:
- type: REG_DWORD
- value: 0x0000001e (30)
- description: 30 displays TOTP generation Step (in sec.)

TOTPWindow:
- type: REG_DWORD
- value: 0x00000004 (4)
- description: 4 displays TOTP checking window (in steps)

The maximum value of TOTP Window is:

- 16 - for OATH OTP AP v1.0.81 and earlier
- 64 - for OATH OTP AP v1.0.82 and later

YubiKey Configuration

To configure YubiKey Standard or NEO tokens to work as OATH HOTP compliant token:

1. Install [YubiKey Personalization Tool](#).
2. Plug-in a YubiKey Token.
3. Run the **YubiKey Personalization Tool**, go to the **OATH- HOTP** tab and click the **Advanced** button.
4. Select the configuration slot.
5. Select the **OATH Token Identifier** box in the **OATH-HOTH Parameters** section. Click the **Generate MUI** button.
6. Click the **Generate** button to generate the **Secret Key**.
7. Click the **Write Configuration** button. Confirm writing the configuration. Save the **.csv** file.
8. Copy the **.csv** file to **%ProgramFiles%\ NetIQ Advanced Authentication Framework\WEW** on the server with the installed NetIQ Web Enrollment Wizard.
9. Open the **WEW** folder and open the **web.config** file with Notepad.
10. Specify the name of the **.csv** file in the string
    <add key="yubikeyConfig" value="~/<filename>.csv"/>.
11. Save the **web.config** file.

Index

A

Authentication 1, 3-4, 7, 11, 13
Authenticator 3

C

Client 3

G

Generate 13

L

Logon 3

O

OATH 1, 3-6, 10-11, 13
One-time Password 4
OTP 4, 9, 12

P

Password 4, 9
PIN 5, 9
Policy 6, 10-11

S

Server 7

T

Token 13
Tool 13
TOTP 4-5, 11