



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
TOTP Policy	5
PIN Required Policy	5
Index	6

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.

Setting OATH Authenticator via Group Policy

TOTP Policy

The TOTP Policy allows you to edit OATH authentication settings.

TOTP generator is that sort of a device that knowing a certain secret key generates a new password through certain defined period of time. You can state the preferable time in **TOTP generation Step** field in **TOTP Policy**. The time is stated in seconds. The minimal step value is 20, its maximum value equals 3600. By default, the step is set to 60.

Knowing the same secret code, the server is able to check this password and correspondingly allow or not allow a user to authenticate. The password is checked by comparing the password input by user to several testing ones generated by server. The number of generated testing passwords is set in **TOTP checking window** field in **TOTP Policy**. The minimal Window value is 1, maximum – 16. By default it is set to 4.

Using default values NetIQ Server will generate one-time passwords for current time +/- 2 minutes (Window=4, Step=60 sec.). If we set, for example, Window = 16 and Step = 60, we will have the current minute and every minute in 8 minutes before and later that time (-8:00, -7:00, ... 0, 1:00, ... 8:00). If we set Window=4 and Step = 30, we will have -1:00, -0:30, 0, 0:30, 1:00.

PIN Required Policy

When this 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.

Index

A

Authentication 1, 3-4
Authenticator 3

C

Client 3

L

Logon 3

O

OATH 1, 3-5
One-time Password 4
OTP 4-5

P

Password 4
PIN 5
Policy 5

S

Server 5

T

TOTP 4-5

W

Window 5