



# NetIQ Advanced Authentication Framework - Password Filter

## **Administrator's Guide**

Version 5.1.0

# Table of Contents

---

	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>3</b>
About This Document .....	3
<b>Password Filter Overview</b> .....	<b>4</b>
<b>Troubleshooting</b> .....	<b>6</b>
List of Problems a User May Encounter .....	6
<b>Index</b> .....	<b>7</b>

# Introduction


## About This Document


### Purpose of the Document

This Password Filter Administrator's Guide is intended for system administrators and describes the work of NetIQ Advanced Authentication Framework Password Filter.


### 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.

# Password Filter Overview

Password Filter is a part of NetIQ Advanced Authentication Framework kit. This component is obligatory for:

- OATH OTP Authentication Provider
- Smartphone Authentication Provider
- NPS Plugin
- NetIQ Access Manager Advanced Authentication Plugin
- NetIQ Cloud Access

**Password Filter** guarantees passwords synchronization independently of the methods and means used for their change.

Password Filter should be installed on every Domain Controllers in the domain. Without it, NetIQ Advanced Authentication Framework will not work properly. The aim of password synchronization is to help users and admins to work with various passwords. Password Filter coordinates user passwords stored in different repositories. Remembering one synchronized password is more convenient than several passwords, so users face problems not so often and rarely contact the support service for help. Moreover, users scarcely write down synchronized passwords on paper.

Password Filter is loaded by LSASS process and it is notified of all the password change and reset events.

## How the password is changing

1. The request to change a password is sending to Domain Controller (DC).
2. DC checks if the password can be changed (e.g. the Minimum password age policy etc.).
3. DC asks its filters if the password can be changed. NetIQ Advanced Authentication Framework Password Filter always allows it.
4. DC changes the password in Active Directory.
5. DC notifies all filters about successful password change.
  - a. In case of password change: NetIQ Advanced Authentication Framework Password Filter asynchronously connects to the Authenticore Server (RPC) and writes the new password (encrypted by Enterprise Key).
  - b. In case of password reset: NetIQ Advanced Authentication Framework Password Filter synchronously connects to the Authenticore Server (RPC). DC waits until the new password will be written (encrypted by Enterprise Key) by the Authenticore Server.

For additional information, see NetIQ Advanced Authentication Framework Administrative Tools Administrator's Guide.



## Troubleshooting

If you encounter any problems with Password Filter, please contact the support service.

When you contact support service:

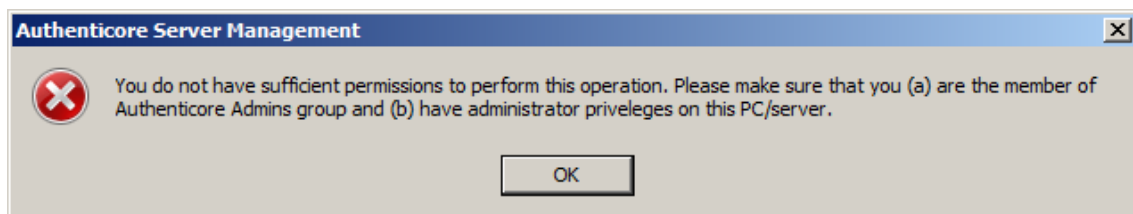
Please when you turn to support service for help, describe the problem as precisely as you can and attach logs from the PC, on which the problem occurred. To create logs, use LogCreator tool that is located on the installation disk in \Tools\LogCollector folder.

To get log:

1. Copy **LogCreator.exe** file to C:\ drive of the faulty computer. Successful tool launch from a network drive cannot be guaranteed.
2. Run the tool.
3. In the opened dialog click **Enable all**. As a result, all components in **Debugged components** section are selected.
4. Close the dialog.
5. Repeat the steps that you performed before the problem occurred.
6. Run the tool again and click **Save logs**.
7. Save the logs in archive file.

## List of Problems a User May Encounter

In case all Domain Controller are unavailable, Authenticore Server will be stopped. If you try to start it, you will receive an error notification:



In case Password Filter is not installed, you will not be able to configure Authenticore Server settings and start it.

# Index

---

## A

Active Directory 4  
Administrator 1, 4  
Authentication 1, 3-4  
Authenticator 3

## D

Domain 4, 6

## E

Enterprise Key 4

## L

List 6  
Logon 3

## O

OATH 4

## P

Password 1, 3-4, 6

## S

Server 4