NetIQ Advanced Authentication Framework - Password Filter

Administrator's Guide

Version 5.1.0

Table of Contents

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 is installed on all 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.

Password Filter has the following operational algorithm:

1. In case of password reset, NetIQ user personal data should be cleared. The information about the date of password reset should be stored in settings (user authenticators are not deleted).
2. Change user password.
3. A new record should be added to the event log informing about password change or reset.

Steps 1 and 2 are done with the help of Authenticore Server. Step 3 is realized through Log 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:

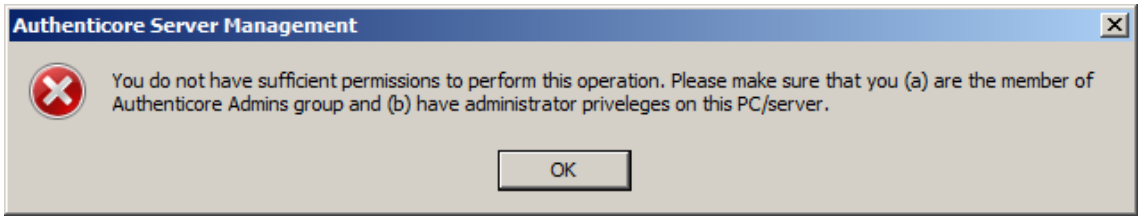
Please when you turn to support service for help, describe the problem as precisely as you can and attach logs from the PC, on which the problem occurred. To create logs, use LogCreator tool that is located on the installation disk in \Tools\LogCollector folder.

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