



NetIQ Advanced Authentication Framework - Log Server

Administrator's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Log Server Overview	4
Log Server Settings	4
Log Servers Policy	5
Troubleshooting	6
Cannot Get Access to Log Server	7
Index	8

Introduction

About This Document

Purpose of the Document

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

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.

Log Server Overview

Log Server is a separate computer/server which is intended for storing data on events occurred on Authenticore servers. It is an optional component.

Log Server is used for the simplification of log collection for debugging or troubleshooting. When Log Server interacts with Log Client all client events information is duplicated on the Log Server, which is actually the storage place of all the server and client events.

When Log Client is not installed, the event information is collected only from Authenticore Server.

Every product component has its event log copy. Every event is written locally. Besides, in the **Log Server** policy you can list computers that will duplicate all the events. In default configuration with two installed Authenticore servers, each of them will have its own event log copy.

Log Server Settings

To configure log server parameters, use the following group policies:

- The **Log Servers** policy (allows you to specify the names of log servers).
- The group policies that allow you to determine the accuracy with which the log is kept, i.e., whether successful events are tracked or not:
 - **Register all authentication events;**
 - **Register all password management events.**
- The **Freeze communication if log server is unavailable** policy determines the rules for resolving conflicts in case the remote log server was unavailable at the moment of writing an event onto it.

It has 4 setting components:

1. MaxTimeoutPeriod;
2. TimeoutPeriod;
3. ReconnectPause;

4. ReconnectPauseIncrement.

The operation algorithm is as follows:

- 1) The messages are delivered to the server with ReconnectPause period.
- 2) If the server was unavailable during the TimeoutPeriod time, ReconnectPause is increased to ReconnectPauseIncrement time. At the same time, TimeoutPeriod is increased to the TimeoutPeriod time stated in the policy.
- 3) During the previous step, ReconnectPause is increased only by the time $\text{TimeoutPeriod} < \text{MaxTimeoutPeriod}$.

In case the information is sent to an unavailable Log Server, the events are not processed.

For the detailed information about the stated policies, see NetIQ Advanced Authentication Framework Administrative Tools Administrator's Guide.

Log Servers Policy

The policy determines the list of event log servers.

The policy allows you to specify the list of domain computers that serve to collect and store events coming from NetIQ Advanced Authentication Framework system components.

To compile the list, type computer names in the "Log servers" field in DNS or NetBIOS format, close, separated by semicolon, e.g. Computer1;Computer2.domainname.com;Computer3.

In case the policy is not configured or disabled, NetIQ Advanced Authentication Framework events are recorded only in the local computer log.

In case the policy is enabled, NetIQ Advanced Authentication Framework events are recorded both in the local computer log and on the remote event log server.

 Computers with names included into "Log servers" list must have the installed NetIQ Advanced Authentication Framework – Log Server package.

Troubleshooting

In case you face any problem with your Log Server, try to reboot it at first. In case it didn't help, 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 logs

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.

Cannot Get Access to Log Server

Description:

You cannot get access to the Log Server.

Cause:

- a) There is no Log Server installed;
- b) Log server was turned off;
- c) Log Server is being reloaded.

Solution:

- a) Install Log Server;
- b),c) Check Firewall settings and the correctness of the domain names permission.

Index

A

Administrator 1, 5
Authentication 1, 3, 5
Authenticator 3

C

Client 4

L

Logon 3

P

Policy 5

S

Server 1, 3-4, 6-7