



NetIQ Access Manager - Advanced Authentication Plugin

User's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
Environment	4
Flash Drive Authentication Support Configuration for Linux	5
Index	7

Introduction

About This Document

Purpose of the Document

This NetIQ Access Manager Advanced Authentication Plugin Installation Guide is intended for all user categories and describes how to use NetIQ Access Manager Advanced Authentication Plugin.

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.

Environment

Components that are required:

- NetIQ Access Manager 3.2 SP1/SP2 server/appliance.
- NetIQ Web Service 4.8 and higher.

 [Java Runtime Environment](#) should be installed on the **Client** side.

Flash Drive Authentication Support Configuration for Linux

To enable flash drive authentication method for Linux, two requirements must be accomplished:

- Make sure that the **libblkid** library is installed (it is installed on most Linux versions by default). Check it with the `blkid` command that makes a call to the library mentioned above.

On Fedora it is possible to install it using `yum`. To do it, write down in the terminal window [root permissions required]:

yum install libblkid

- Add udev rules, so that a user could gain access to flash drives. Otherwise only root can gain access to them.

a. Create a new user group that will have permissions to access flash drives:

groupadd [your_group]

b. Add a user to the group from the previous stage:

useradd -G [your_group] [your_user]

To change a user group:

usermod -G [your_group1],[your_group2] [your_user]

c. Create a new udev file in **/etc/udev/rules.d**, udev rule files applies in alphabetical order that numbers in names are for **[10-my-usb.rules]**. E.g., the file containing number 10 in the name applies earlier than the file with the number 50 in its name.

d. Run **udevadm info /dev/sdb1** to get attributes of the required flash drive. E.g., it contains the attribute **DEVTYPE=partition**.

e. Write your udev rule to the previously created file!

ENV{DEVTYPE}=="partition", MODE="0666", GROUP=[your_group]

E.g.:

ENV{DEVTYPE}=="partition", MODE="0666", GROUP="users"

This will grant permission to the users from the group "**users**" to access USB devices of the type "**partition**".

 If you use the Konqueror browser, then it is necessary to enable Java Runtime Environment. If you use the Firefox browser, then Java Runtime Environment will be enabled by default and Sun Java Plugin will be used automatically.

 Flash drive is set automatically in openSUSE Linux when it is opened through Dolphin for the first time. It is also possible to set automount or to set flash drive manually.

Index

A

Authentication 1, 3, 5
Authenticator 3

C

Client 4
Create 5

L

Logon 3

U

User 1