NetIQ Advanced Authentication Framework

Maintenance Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

This Maintenance Guide is intended for *NetIQ Administrators* and *NetIQSecurity Officers* and describes how to maintain *Infrastructure* with NetIQ Advanced Authentication Framework solution.

Purposes of Maintenance

Maintenance is necessary for providing uninterrupted possibility to authenticate by various authentication methods and uninterrupted possibility to administrate NetIQ settings of users and computers using NetIQ Advanced Authentication Framework. This document describes maintenance remedies for *End Users*, because only end users are directly interacting with NetIQ.

Difficulties of Maintenance

Difficulties of maintenance depends on homogeneity of infrastructure. The uniform infrastructure contains workstations with the same or similar hardware and software configurations. The maintenance of such infrastructure is easier than the maintenance of infrastructure that contains workstations with various types of hardware and software configurations. End users must spend more time and engage more people for configuring of specific features (drivers, hardware compatibility, operating systems, third-party software). So these conclusions is right also for NetIQ maintenance. Check NetIQ system requirements for preliminary compatibility checking with your infrastructure.

Terms

NetIQ Administrator – user with delegated NetIQ privileges. NetIQ Administrator performs installation and configuring of NetIQ Advanced Authentication Framework. Check Administrator responsibility list.

NetIQ Helpdesk – a technical staff of NetIQ Support Center that assists *End Users* in case of any questions and problematic situations on NetIQ Advanced Authentication Framework.

NetIQ Knowledge Base – a section of NetIQ Support Center, which contains useful information with often asked questions and appropriate answers on NetIQ solution.

NetIQ Security Officer – user with delegated NetIQ privileges. NetIQ Security Officer assists user to enroll his/her own authenticator and monitor security during users' authentication. Check Security Officer responsibility list.

NetIQ Support Center – a department of NetIQ Company; also means NetIQ support website.

Defect - an error in the Software which is reproducible or repeatable and which causes the NetIQ solution to not function substantially in conformance with its specifications, the applicable End User documentation, or other related documentation, including without limitation, any other engineering documentation for the NetIQ solution, or commonly accepted operating principles as defined by industry standards.

End user – company that is using or plans to use NetIQ Advanced Authentication Framework.

Incident - a situation when *End User* or distributor is needed to contact *NetIQ Helpdesk* for assistance.

Infrastructure – object of *End User* that contains all servers, workstations and communication channels between them.

Responsibilities of Staff Working with NetIQ

NetIQ Administrator Responsibilities

1. Installation of server and administrative components.
2. Preliminary check of NetIQ system requirements and NetIQ upgrade in test environment or on the small selection in production domain to be sure that the upgrade will not cause any problems.
3. Upgrade of server and administrative components.
4. Deployment and upgrade of client components.
5. Configuration of Authenticore Servers.
6. Solution of any problem depending on inability to logon.
7. Regular inspection of events with system failures and warnings including NetIQ Authenticore server failures.
8. Assist NetIQ Security Officer with any NetIQ problems.
9. Ask *NetIQ Helpdesk* for extra technical help upon NetIQ solution.
10. Notify NetIQ Helpdesk about any *Defects* in NetIQ solution.
11. Communication with NetIQ Helpdesk about defects and *Incidents* (NetIQ Helpdesk can ask extra information for diagnostics of incident), including checking of workarounds and confirmation of closing an incident.

NetIQ Security Officer Responsibilities

1. Enrolling users' authenticators.
2. Assist users with enrolling and understanding of how NetIQ works and how users need to use it.
3. Regular inspection of NetIQ events with any failures and warnings.

Recommendation for Upgrading Procedure

It is recommended to upgrade NetIQ at the time of lowest user activity (evening after work, weekends).

1. Make a snapshot of virtual machine with Authenticore Server if you use virtual machines for NetIQ servers.
2. If you have only one Authenticore Server, we recommend you to install and configure additional server to provide fault tolerance.
3. Upgrade first Authenticore Server, restore the Enterprise Key, upgrade all authentication providers in case of there are changes in them; reboot server.
4. Make sure that the Authenticore Server was successfully started after reboot.
5. Stop other Authenticore Servers temporarily and try to authenticate by any user authenticator (this user should not have cached authenticators).
6. Start other Authenticore Servers.
7. If test authentication in step 5 was successful, you can upgrade other Authenticore Servers including all updated authentication providers one-by- one, else please check errors in Event Viewer and contact with NetIQ Helpdesk with detailed information. Please make sure that all Authenticore Servers were started after reboots.
8. Upgrade first Password Filter, reboot DC.
9. Check Event Viewer on DC to be sure that Password Filter was successfully loaded.
10. Upgrade other Password Filters one-by-one.
11. Upgrade Administrative tools on all NetIQ administrator servers and workstations.
12. Upgrade client components (NetIQ Client, authentication providers) on selection of 5-10 or 5% of workstations with different configurations.
13. Wait for 2-5 days: collect and analyze feedback from users.
14. Upgrade selection of 30% of workstations.
15. Wait for a week: collect and analyze feedback from users.
16. Upgrade remaining workstations.

What You Need To Do In Case Of Authenticore Server Is Unavailable

1. Check how many Authenticore Servers are unavailable. If all Authenticore Servers are unavailable, please provide users with temporary possibility to logon by classical password.
2. If you can start and logon to server, try to start Authenticore Server manually via Authenticore Server tray manager.
3. If you can't start server manually, try to re-install it.
4. Check Event Viewer for any errors, analyze errors.
5. Restore snapshot with working state, if you use virtual machines for servers.

   ℹ Restoring a state from snapshot may cause a situation when server drops off from domain. It may cause authentication failures. Please rejoin it to the domain and reinstall the Authenticore Server in such case.
6. Deploy new Authenticore Server(s) using existing Enterprise Key. Ask NetIQ administrator or responsible person for Enterprise Key. Enterprise Key should be stored in secure place.
7. If you have lost an Enterprise Key, you will need to generate new Enterprise Key. It also means that all NetIQ settings including enrolled authenticators will be lost and you will need to re-enroll them.
8. If your Authenticore Servers don't work after preparing new Authenticore Servers, please check schema extension, try to extend schema again.

Enhancing Reliability and Security of Infrastructure

In this chapter:

- Infrastructure
- NetIQ Authenticore Servers
- Servers and Workstations with NetIQ components installed
- Enhancing security

Infrastructure

1. Backup Active Directory monthly using any preferable utility. You need it, because all NetIQ settings are stored in AD/AD LDS.
2. Use two or more Domain Controllers for fault tolerance at first according to Microsoft's recommendations.
3. Availability of redundant communication channel between users' workstations and near Authenticore Servers for a case of any communication channel problems.

NetIQ Authenticore Servers

1. Use two or more NetIQ Authenticore Servers for each site. See Microsoft's recommendations for Domain Controllers.
2. Prevent situations when all Authenticore Servers are unavailable. Use Authenticore Servers in different locations.
3. Check Event Viewer for any system or NetIQ errors and warnings daily.
4. Use uninterruptible power supply for a case of electricity disconnection and disruption.
5. Availability of 30 GB free space on system partition of hard drive (for events and logs).
6. Save snapshot with working state after any upgrade in case of using virtual machines for NetIQ Authenticore Servers.

   ℹ Restoring a state from snapshot may cause a situation when server drops off from domain. It may cause authentication failures. Please rejoin it to the domain and reinstall the Authenticore Server in such case.
7. Every Authenticore Server must contain all used authentication providers installed.

Servers and Workstations with NetIQ Components Installed

1. Use recommended operating system updates.
2. Availability of 60 GB free space on system partition of hard drive.

3. Check preliminary whether NetIQ supports new version of client and server OS before migrating to them.
4. If you use DLP software, make sure that this software doesn’t block USB devices that are used for user authentication.
5. Use authenticators caching in the next situations:

    A. Slow communication channel;
    B. Planned works with communication channel;
    C. Migration of employees to the new office;
    D. Business trip with corporate laptop.

Enhancing Security

1. Use secure storage for Enterprise Key. Otherwise you can compromise it.
2. Delegate Authenticore Admins privileges to trusted administrators only. Administrators should have good knowledge of Active Directory.
3. Delegate NetIQ Advanced Authentication Framework Admins and NetIQ Advanced Authentication Framework User/Computer settings management privileges to trusted security officers only.

Index