



NetIQ Advanced Authentication Framework - Windows Client

Installation Guide

Version 5.2.0

Table of Contents

	1
Table of Contents	2
Introduction	3
About This Document	3
About Windows Client	4
System Requirements	5
Preliminary configuration	6
How to set DNS for server discovery	7
Installing and Removing Windows Client	10
Installing Windows Client	10
Removing Windows Client	15
Microsoft Windows 7	16
Microsoft Windows 8.1	16
Microsoft Windows 10	16
Troubleshooting for Windows	17
Chain icons can't be updated	18
Long boot	19
Index	20

Introduction

About This Document

Purpose of the Document

This Windows Client Installation Guide is intended for all user categories and describes system requirements that should be fulfilled before the installation of NetIQ Advanced Authentication Framework Windows Client.

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.

About Windows Client

Windows Client replaces standard way of log on to Microsoft Windows by a more secure using the authentication chains configured in NetIQ Advanced Authentication.



In Windows Client 5.2 the users are able to use only Password for logon in the following cases:

1. When Authentication Server is not available (e.g. offline logon).
2. When local account was used to log on.



To log on with Microsoft account enter <WorkstationName>\<MicrosoftAccount> in the user name field, e.g. win81x64\pjones@live.com.

System Requirements

 Installing and removing Windows Client requires **Local Admins** privileges.

The following system requirements should be fulfilled:

- Microsoft Windows 7 (x64/x86) SP1/Microsoft Windows 8.1 (x64/x86)/Microsoft Windows 10 (x64/x86).
- The machine must be joined to a domain.
- DNS is properly configured for NetIQ Advanced Authentication Server discovery. [Check the related article.](#)
- Users of Active Directory repository or eDirectory repository (if [Domain Services for Windows](#) technology is used) may be used for logon. Users from AD LDS repository can't be used for logon.

Preliminary configuration

The chapter contains articles about required pre-configuration.

- [How to set DNS for server discovery.](#)

How to set DNS for server discovery

Question:

I would like to set DNS for server discovery. How can I do it and what is its workflow?

Answer:

To set DNS for server discovery:

1. Open DNS Manager. To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. Set **Reverse Zone Lookup**:
 - a. Go to the **Reverse Zone Lookup** folder icon, right click it and select **New Zone**.
 - b. After **New Zone Wizard** opens, click **Next**.
 - c. Select **Primary Zone** as the **Zone Type**. Click **Next**.
 - d. Type the first three octets of your network IPV4 address range like 192.168.1. Click **Next**.
3. Add Host A or AAAA record and PTR record:
 - a. In the console tree, right-click the forward lookup zone which includes your domain name, and click **New Host (A or AAAA)**.
 - b. In the **Name** text field, type a DNS name of the NetIQ Advanced Authentication Server.
 - c. In the **IP address** text field, type the IP address for the NetIQ Advanced Authentication Server. You can type the address in IP version 4 (IPv4) format (to add a host (A) resource record) or IP version 6 (IPv6) format (to add a host (AAAA) resource record).
 - d. Select the **Create associated pointer (PTR) record** check box to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you entered in Name and IP address
4. Add SRV record:
 - a. In the console tree, right-click the forward lookup zone which includes your domain name, and click **Other New Records**.
 - b. In the **Select a resource record type** list, click **Service Location (SRV)**, and then click **Create Record**.
 - c. Click **Service**, and then type **_aaa**.
 - d. Click **Protocol**, and then type **_tcp**.
 - e. Click **Port Number**, and then type **443**.
 - f. In **Host offering this service**, type the FQDN of the server that is added (e.g., authsrv.mycompany.com).
 - g. Click **OK**.

Repeat the actions described in points 3-4 for DB Slave and Member servers. You may vary the Priority and Weight values for different servers to prioritize them.

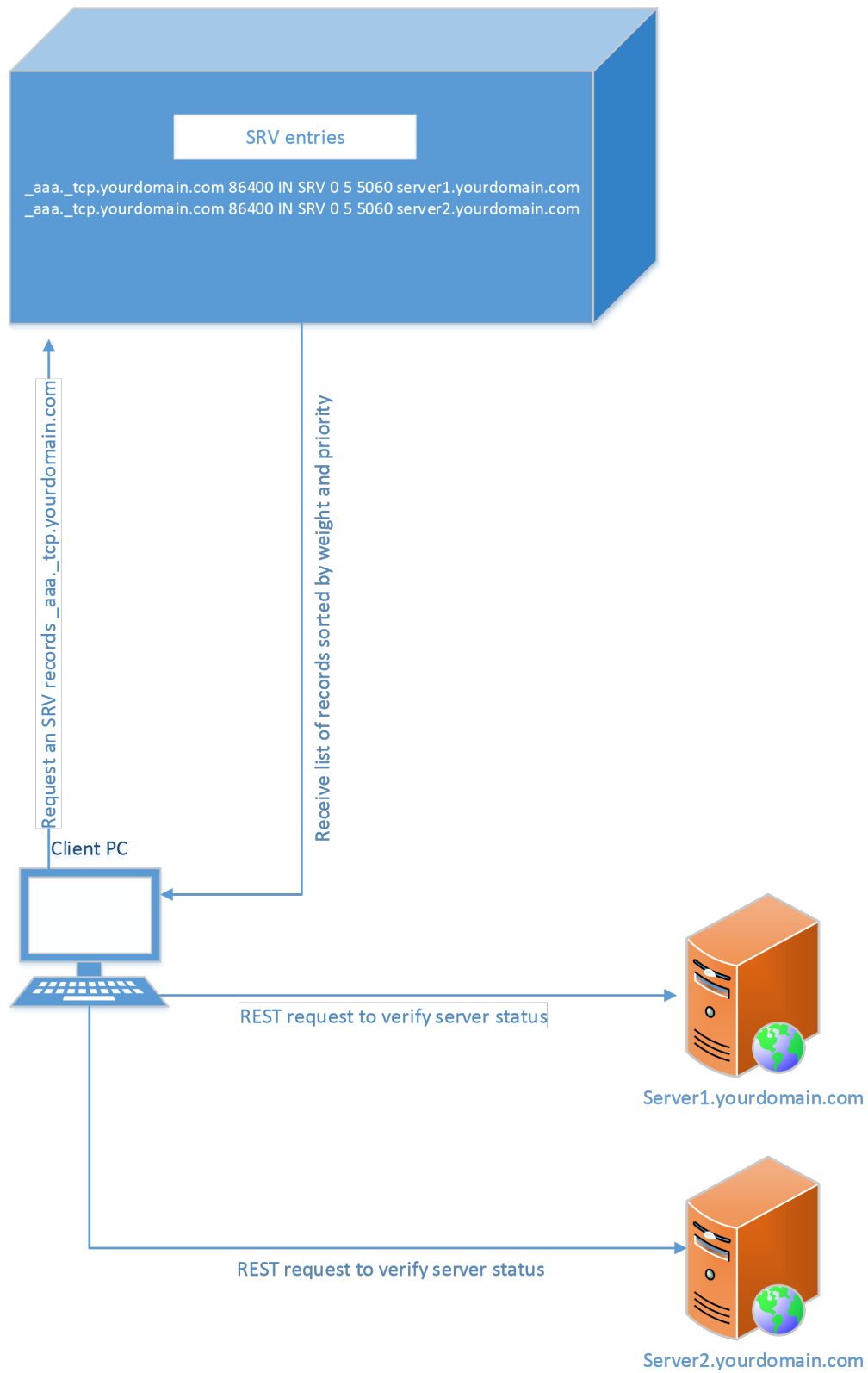
DNS server contains SRV entries `_service._proto.name` TTL class SRV priority weight port target, where:

- **Service** - symbolic name of an applicable service.
- **Proto** - transport protocol of an applicable service; usually either TCP or UDP.
- **Name** - domain name for which this record is valid; ends with dot.
- **TTL** - standard DNS time to live field.
- **Class** - standard DNS class field (this is always IN).
- **Priority** - priority of the target host; lower value means more preferred.
- **Weight** - a relative weight for records with the same priority; higher value means more preferred.
- **Port** - TCP or UDP port on which the service is located.
- **Target** - canonical hostname of the machine providing the service; ends with dot.

Server discovery workflow is the following:

1. Client sends request through TCP protocol (port 443) to get the list of all entries `_aaa._tcp.yourdomain.com`.
2. Client receives the sorted list by weight and priority.
3. Since the priority field determines the precedence of use of the record's data, client always uses SRV record with the lowest-numbered priority value first.
4. Client sends https request to check server availability status. If the first connection to the server fails, then client will fall back to other records of equal or higher value. If service has multiple SRV records with the same priority value, client will use the weight field to determine which server to use.

The diagram below shows server discovery workflow graphically.



Installing and Removing Windows Client

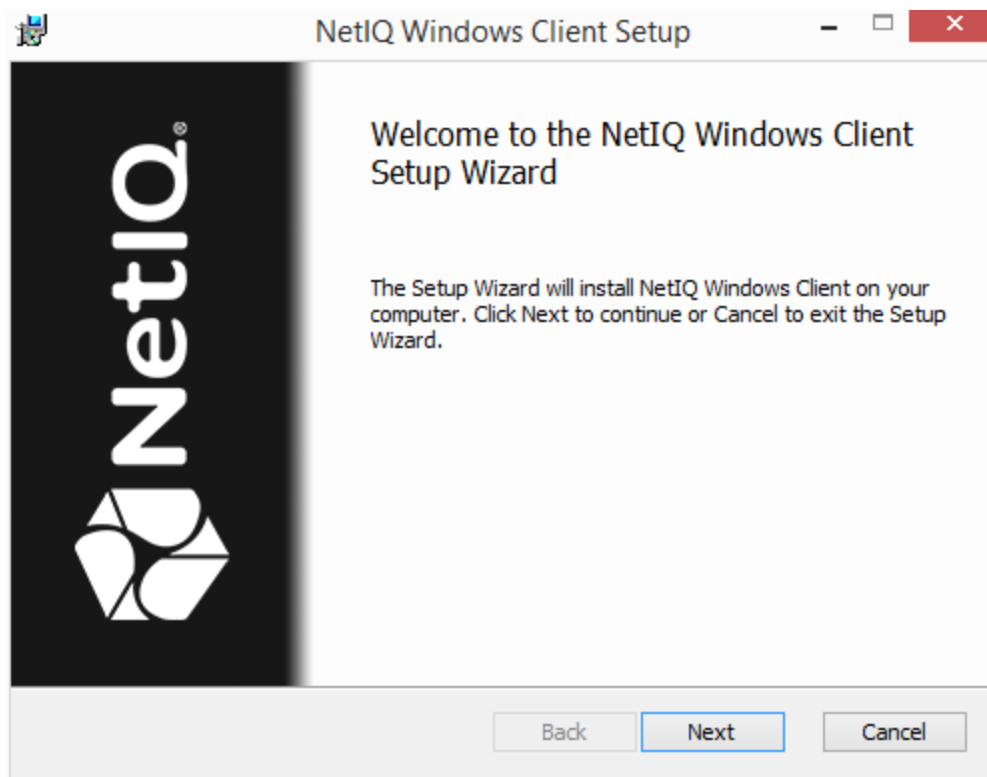
In this chapter:

- [Installing Windows Client](#)
- [Removing Windows Client](#)

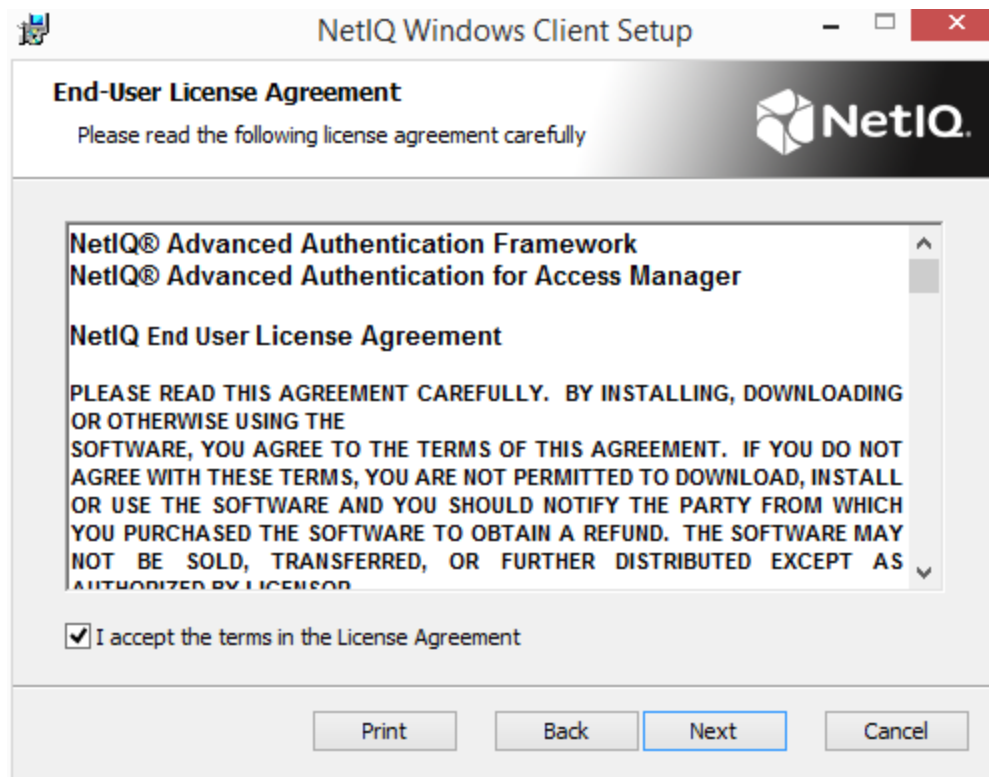
Installing Windows Client

To install Windows Client via Setup Wizard:

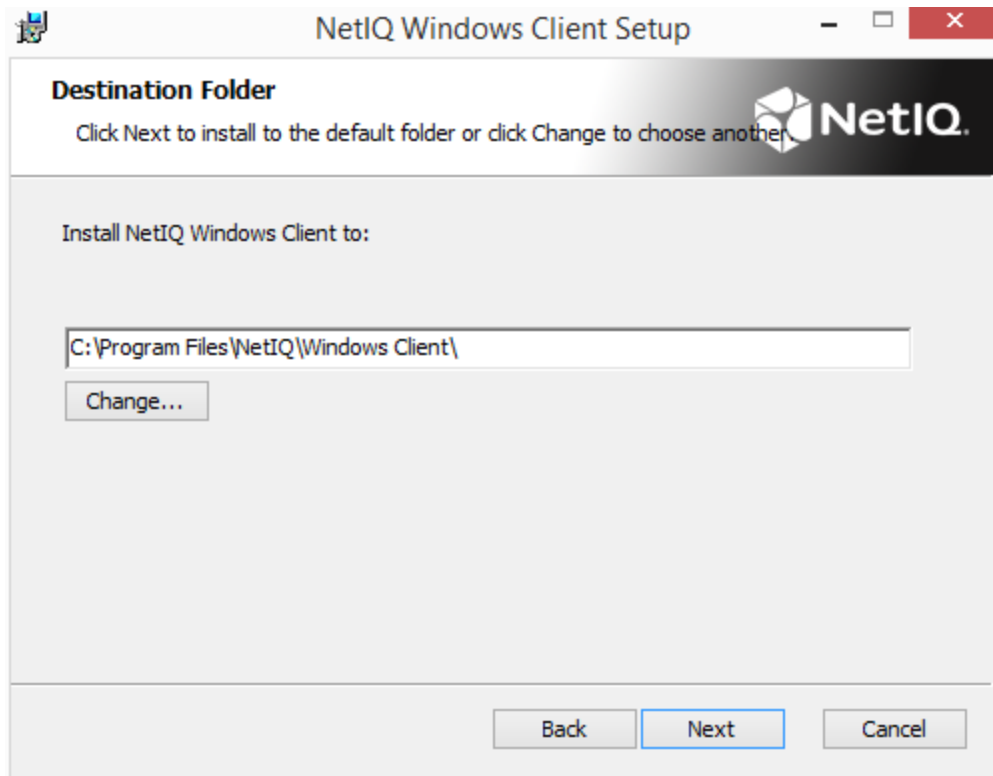
1. Check **System** properties (Control Panel\All Control Panel Items\System) to detect your **System type**.
2. Run **NAAF - WinClientInstaller- Win32- <version>.msi** in case of 32-bit Operating System, **NAAF - WinClientInstaller- x64- <version>.msi** in case of 64-bit Operating System.
3. Click **Next** to continue.



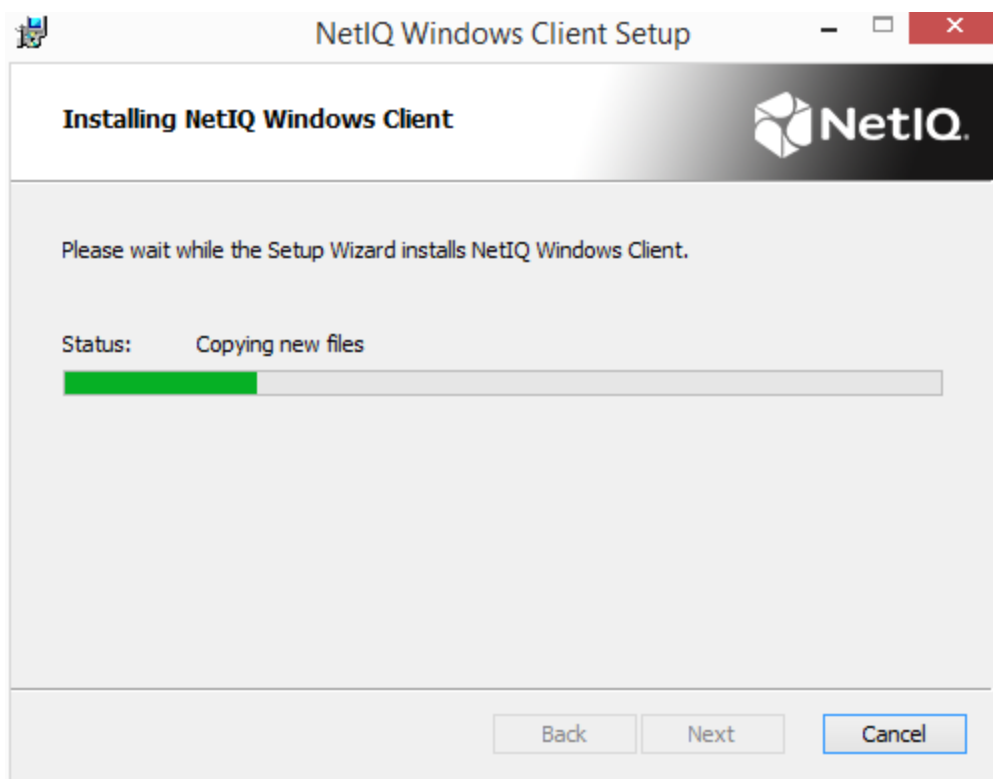
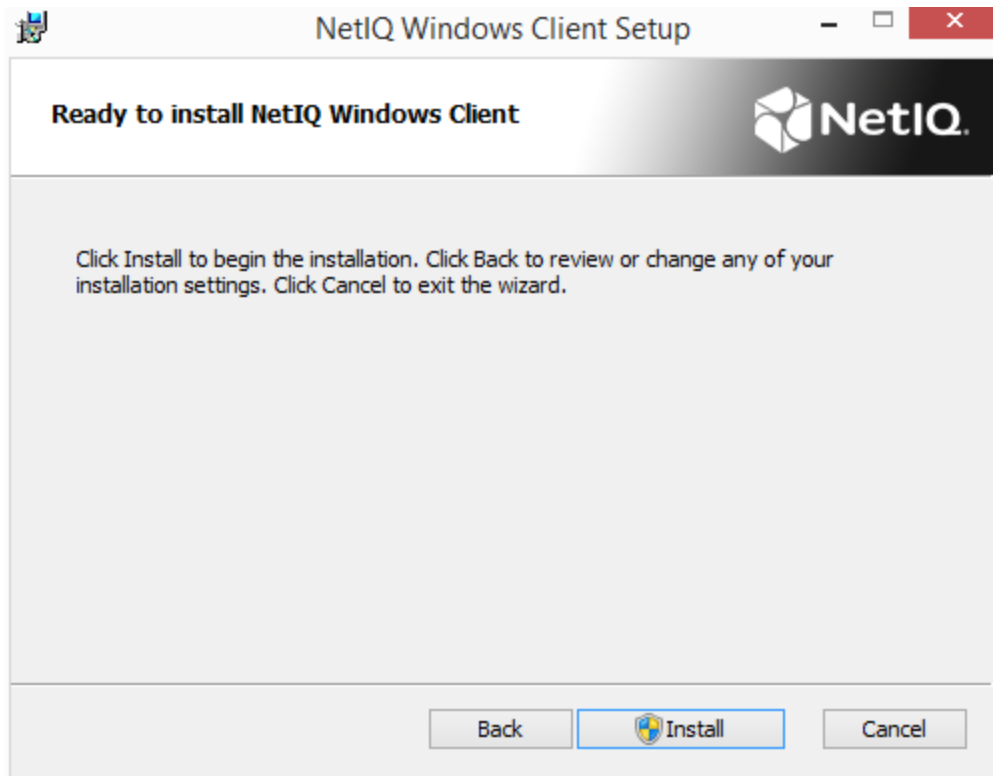
4. Read the **License Agreement**. Select the **I accept the terms in the license agreement** checkbox and click **Next**.



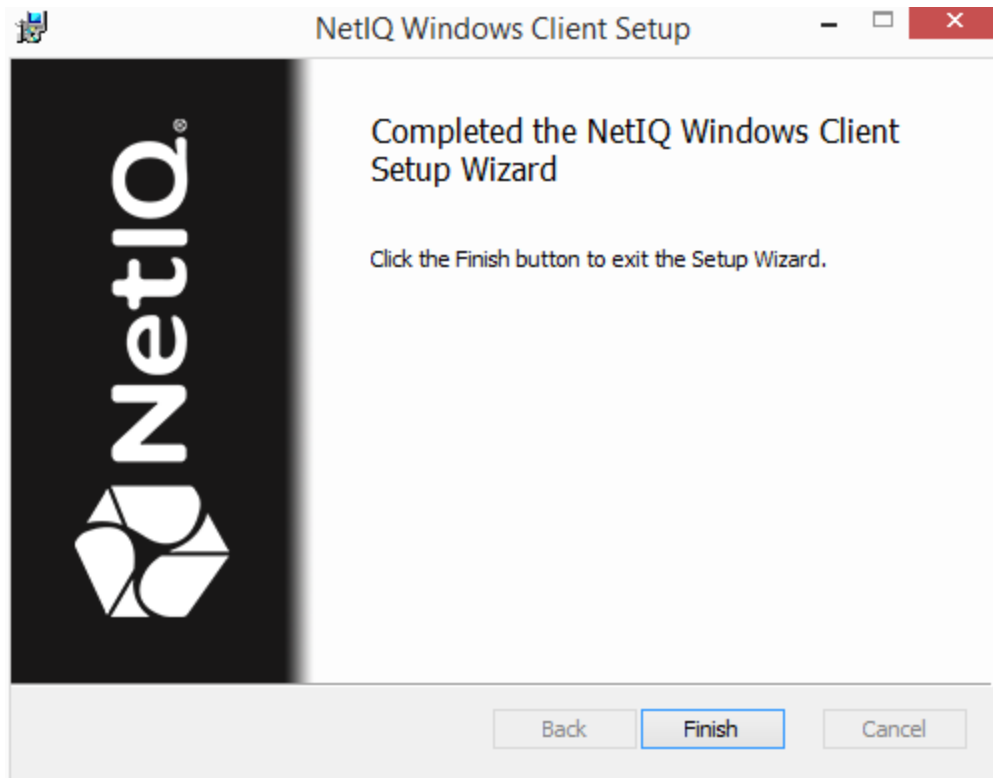
5. Click **Next** to install to the default folder or click **Browse** to choose another.



- To change the destination folder, click the **Change** button and select an applicable destination.
 - To continue, click **Next**.
5. Click **Install** and wait until the component is installed.

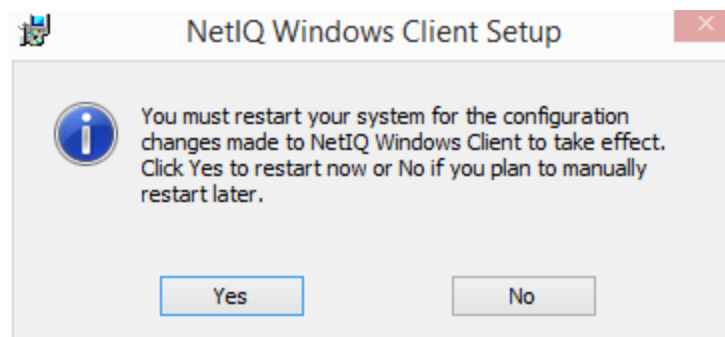


6. Click **Finish** to close the Wizard.



 It is required to set **Require admin password to register endpoint/workstation** to **OFF** in **Endpoint management options** on NetIQ Advanced Authentication Administrative Portal. Otherwise the required endpoint won't be created.

7. Click **Yes** to restart the operating system.



Removing Windows Client

Windows Client can be removed via Setup Wizard or Control Panel.

To remove Windows Client via Setup Wizard, follow the steps:

1. Run **NAAF - WinClientInstaller- Win32- <version>.msi** in case of 32-bit Operating System, **NAAF - WinClientInstaller- x64- <version>.msi** in case of 64-bit Operating System.
2. Click **Next** to continue.
3. Select **Remove** as an applicable operation and click **Next** to remove Windows Client from your computer.
4. Click **Remove** to confirm removal.

To remove Windows Client via Control Panel, select one of the links that corresponds to your operating system:

- [Microsoft Windows 7](#)
- [Microsoft Windows 8.1](#)
- [Microsoft Windows 10](#)

Microsoft Windows 7

1. In the **Start** menu, select **Control panel** and then double-click **Programs and Features**.
2. Select **NetIQ Windows Client** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Microsoft Windows 8.1

1. In the **Search** menu, select **Apps > Control Panel > Programs > Programs and Features**.
2. Select **NetIQ Windows Client** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Microsoft Windows 10

1. Right-click the **Start** button and select **Control Panel > Programs > Programs and Features**.
2. Select **NetIQ Windows Client** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

Troubleshooting for Windows

To investigate the possible issues you may be asked to collect the debug logs.

To enable debug logging for all Client components, follow the steps:

- Create a text file *C:\ProgramData\NetIQ\Logging\config.properties*
- Add a string to the file: *logEnabled=True* which ends by line break
- Create directory: *C:\ProgramData\NetIQ\Logging\Logs*
- Restart the workstation

Reproduce the problem. Logs will be located in *C:\ProgramData\NetIQ\Logging\Logs*.

Chain icons can't be updated

Issue

System administrator applied the new icons for the used authentication chains, but they were not updated on the Windows Client.

Solution

Windows Client does not update the icons to reduce the traffic. Please remove the folder `C:\ProgramData\NetIQ\Windows Client\logocache` to clear the icons cache.

Long boot

Question:

With the Windows Client installed I experience longer *Please wait* screen during OS boot?

Answer:

It happens because NetIQ Advanced Authentication has to wait for network to get and show a list of available authentication chains.

Index

A

Active Directory 5
Authentication 1, 3-5, 7, 14, 19
Authenticator 3

C

Client 3-4, 8, 10, 15-18
Control 10, 15-16
Control panel 16
Create 7, 17

D

Domain 5

L

License 11
Local 5
Logon 3

P

Password 4
Protocol 7

R

Remove 15

S

Server 4, 7
System 5, 10, 15, 18

W

Windows 1, 3-5, 10, 15-19
Windows 7 5, 15-16
Windows 8 15-16