Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.
# Contents

About NetIQ Corporation .......................... 5
About this Book ................................. 7

1 System Requirements .......................... 9

2 Configuring the Preliminary Settings ....... 11
   Setting DNS for Server Discovery .................. 11
   Using a Specific Advanced Authentication Server .................. 12

3 Installing and Uninstalling Windows Authentication Agent .................. 13
   Installing Windows Authentication Agent .................. 13
   Uninstalling Windows Authentication Agent .................. 13
      Using the Setup Wizard .................. 13
      Using Control Panel .................. 14

4 Troubleshooting .............................. 15
   Debugging Logs for Advanced Authentication .................. 15
   Agent Unable to Connect to the Server .................. 16
   Authentication Agent Does Not Prompt the Restricted Browser for Authentication .................. 16
About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new
In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster
We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software
In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion
We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management
Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide: www.netiq.com/about_netiq/officelocations.asp
United States and Canada: 1-888-323-6768
Email: info@netiq.com
Web Site: www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide: www.netiq.com/support/contactinfo.asp
North and South America: 1-713-418-5555
Europe, Middle East, and Africa: +353 (0) 91-782 677
Email: support@netiq.com
Web Site: www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click Add Comment at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.
About this Book


Intended Audience

This guide is intended for Advanced Authentication and Windows administrators.

About Windows Authentication Agent

Authentication Agent allows you to perform strong multi-factor authentication on one computer to get authorized access to another computer where it is not possible to display the user interface or connect any external authentication devices. You can install the Authentication Agent on a workstation or laptop. When an authentication is initiated from a computer using Authentication Agent chain, the Authentication Agent on another computer prompts a restricted browser where user must perform authentication.

IMPORTANT: If both the Windows Client and Authentication Agent are installed on the same workstation, the Authentication Agent is logged on automatically through the SSO feature. If the Windows Client is not installed, user must log in to the Authentication Agent manually.
You must have the administrator privileges to install and uninstall Windows authentication agent.

Ensure that you have installed one of the following operating systems:

- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows 8.1 (32-bit and 64-bit)
- Microsoft Windows 10 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
Configuring the Preliminary Settings

This chapter contains sections about the pre-configuration settings of Authentication Agent. You can perform one of the following to connect the Authentication Agent with the respective server:

- Setting DNS for Server Discovery
- Using a Specific Advanced Authentication Server

Setting DNS for Server Discovery

To allow the Authentication Agent to discover the daemon host, perform the following steps:

1. Click Start > Control Panel > Administrative Tools > DNS, to open the DNS manager.
2. Add Host A or AAAA record and PTR record:
   2a. In the console tree, right-click the forward lookup zone that includes your domain name and click New Host (A or AAAA).
   2b. Specify a DNS name for the Advanced Authentication Server with daemon host in Name.
   2c. Specify the IP address for the Advanced Authentication Server in IP address. You can specify 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).
   2d. Select Create associated pointer (PTR) record to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you provided in Name and IP address.
3. Add a SRV record:

   **NOTE:** Ensure that the LDAP SRV record exists at DNS server. If the record is not available, you must add it manually.

   3a. In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.
   3b. In the Select a resource record type list, click Service Location (SRV) and click Create Record.
   3c. Click Service and specify _oob.
   3d. Click Protocol and specify _tcp.
   3e. Click Port Number and specify 443.
   3f. In Host offering this service, specify the FQDN of the Advanced Authentication server with daemon host.
      For example, authsrv.mycompany.com.
   3g. Click OK.
Using a Specific Advanced Authentication Server

You can specify an Advanced Authentication server with daemon host on the Authentication Agent that can be used when a workstation is not joined to a domain. You can also use this option when the user wants to force a connection to a specific Advanced Authentication server with daemon host when a workstation with Authentication Agent is joined to a domain.

To discover a specific server, perform the following:

1. In the C:\ProgramData\NetIQ\Windows Client\config.properties file, configure discovery.host = <IP_address|domain_name>.
   For example, discovery.host = 192.168.20.40 or discovery.host = auth2.mycompany.local.
2. Restart the system.
Installing and Uninstalling Windows Authentication Agent

This chapter contains the following sections:

- Installing Windows Authentication Agent
- Uninstalling Windows Authentication Agent

Installing Windows Authentication Agent

To install Windows authentication agent on Windows, perform the following steps:

**NOTE:** Before installing Windows authentication agent, navigate to Control Panel > All Control Panel Items > System and identify your system type.

1. Run `naaf-authagent-x86-release-<version>.msi` for 32-bit operating system or `naaf-authagent-x64-release-<version>.msi` for 64-bit operating system.
2. Click Next.
3. Accept the License Agreement and click Next.
4. Click Next to install agent on the default folder or click Change to select a preferred folder.
5. Click Install.
6. Click Finish.

**NOTE:** If Windows Client and Authentication Agent are installed on a Windows workstation, the agent applies same approach as Windows client to discover the Advanced Authentication server.

If Authentication Agent is installed on a Windows workstation without Windows Client, then agent cannot discover the Advanced Authentication server.

Uninstalling Windows Authentication Agent

You can uninstall Windows authentication agent in the following ways:

- Using Setup Wizard
- Using Control Panel

Using the Setup Wizard

To uninstall Windows authentication agent using the setup wizard, perform the following steps:

1. Run `naaf-authagent-x86-release-<version>.msi` for 32-bit operating system or `naaf-authagent-x64-release-<version>.msi` for 64-bit operating system.
2. Click Next.
Select Remove.
4 Click Remove to confirm.

Using Control Panel
To uninstall Windows authentication agent using control panel, perform the following steps:

1 Click Start menu > Control Panel > Programs and Features.
2 Right click NetIQ Windows Authentication Agent and select Uninstall.
3 Click OK to confirm.
Troubleshooting

This chapter contains the following topics:

- "Debugging Logs for Advanced Authentication" on page 15
- "Agent Unable to Connect to the Server" on page 16
- "Authentication Agent Does Not Prompt the Restricted Browser for Authentication" on page 16

Debugging Logs for Advanced Authentication

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

1. Run DiagTool.exe (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click Clear All (if applicable) in the Debug logs tab.
3. Click Enable.
4. Restart the system.
5. Reproduce your problem.
7. Click Save logs in the Debug logs tab.
8. Specify a file name and path. Click Save to save the logs.
9. Click Disable to disable the logging.
10. Click Clear All.

If you don't have the Diagnostic Tool you can perform the actions manually:

1. Create a text file C:\ProgramData\NetIQ\Logging\config.properties.
2. Add a string to the file: logEnabled=True that ends by a line break.
3. Create a directory: C:\ProgramData\NetIQ\Logging\Logs\.
4. Restart the machine.
5. Reproduce your problem.
6. Pack the logs located in C:\ProgramData\NetIQ\Logging\Logs\ into a zip file.
7. Change logEnabled=True to logEnabled=False in the folder, C:\ProgramData\NetIQ\Logging\config.properties

With the Diagnostic Tool, you can check the network problems on a workstation, issues in connection between a workstation and DNS Server, and to get a list of the Advanced Authentication Servers that can be discovered. To identify Advanced Authentication server, perform the following steps:

NOTE: As a prerequisite, ensure that DiagTool.exe file is available with the following files in the same directory:

- DiagTool.exe.config
1. Run DiagTool.exe (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click Servers.
3. In the Search settings, specify the domain name in Domain to find a list of Advanced Authentication servers in the specified domain.
   If you want to find particular server then clear Use system DNS server and specify the IP address of the DNS server in DNS server.
4. Select Use v6 DNS lookup to allow the Diagnostic Tool to find the Advanced Authentication server using _aav6 records.
   If you want to find the Advanced Authentication server using _aaa records then clear Use v6 DNS lookup.
5. Click Search.

**NOTE:** If you configure IP address of the Advanced Authentication server in the DNS service record, the Diagnostic tool cannot find and retrieve the respective record. Ensure that you configure the DNS service record with Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

**Agent Unable to Connect to the Server**

After the installation of Authentication Agent on Windows machine, if you try to login to the agent, an error message Failed to connect to the server is displayed. This occurs because you have not configured Authentication Agent with the preliminary settings.

As a solution, ensure one of the following configuration is accomplished:

- Configure DNS in the Authentication Agent for server discovery. For more information, see Setting DNS for Server Discovery.
- Configure specific Advanced Authentication server in the file config.properties. For more information, see Using a Specific Advanced Authentication Server.

**Authentication Agent Does Not Prompt the Restricted Browser for Authentication**

When you initiate the authentication using Authentication Agent chain from one computer, the Authentication Agent on another computer does not prompt the restricted browser where you can pass the respective authentication chain.

As a solution to this issue, perform the following:

- Ensure that you have logged in to the computer, where the Authentication Agent is installed.
- Ensure that Authentication Agent icon is displayed in the System Tray.
- Place the mouse cursor on Authentication Agent icon in the System Tray and check whether the agent is logged in. If the agent is not logged in, double click the icon and authenticate. After successful log in to the agent, initiate the authentication from another computer using the Authentication Agent chain and try to authenticate with the agent.