Advanced Authentication 6.2
Windows Authentication Agent Installation Guide

February 2019
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 © 2019 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
   Configuring Time to Close the Restricted Browser .................. 13

3 Installing and Uninstalling Windows Authentication Agent 15
   Installing Windows Authentication Agent .......................... 15
   Uninstalling Windows Authentication Agent .......................... 15
      Using the Setup Wizard ........................................ 16
      Using Control Panel ........................................ 16

4 Troubleshooting 17
   Debugging Logs for Advanced Authentication .......................... 17
   Agent Unable to Connect to the Server ............................ 18
   Authentication Agent Does Not Prompt the Restricted Browser for Authentication .......................... 18
      Authentication Agent Does Not Respond During the Login Process ........................................ 19
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](http://www.netiq.com/about_netiq/officelocations.asp)

United States and Canada: 1-888-323-6768

Email: info@netiq.com

Web Site: [www.netiq.com](http://www.netiq.com)

Contacting Technical Support

For specific product issues, contact our Technical Support team.


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](http://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](http://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 (v1709, v1803, v1809 or v1903 32-bit or 64-bit)
- 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
- Configuring Time to Close the Restricted Browser

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 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 the following SRV records:

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

   For best load balancing, you need to perform the following actions only for Advanced Authentication web servers. You need not create the records for Global Master, DB Master, and DB servers.

   3a. _oob record:
      3a1. In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.
      3a2. In the Select a resource record type list, click Service Location (SRV) and click Create Record.
      3a3. Click Service and specify _oob.
      3a4. Click Protocol and specify _tcp.
      3a5. Click Port Number and specify 443.
For example, authsrv.mycompany.com.

3a7 Click OK.

3b _aav6 records:
3b1 In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.
3b2 In the Select a resource record type list, click Service Location (SRV) and click Create Record.
3b3 Click Service and specify _aav6.
3b4 Click Protocol and specify _tcp.
3b5 Click Port Number and specify 443.
3b6 In Host offering this service, specify the FQDN of the server that is added.
    For example, authsrv.mycompany.com.
3b7 Click OK.

NOTE: The Authentication Agent requires both the _oob and _aav6 records. The _aav6 to discover the Advanced Authentication server and _oob to map with the relevant Daemon Host.

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 when a workstation with Authentication Agent is joined to a domain.

When the Authentication Agent is installed on a Windows workstation without Windows Client, the agent uses the parameters configured in its own config.properties file to discover a specific server.

To enable the Authentication Agent to discover a specific server, perform the following steps:

1 Navigate to the path C:\ProgramData\NetIQ\Advanced Authentication Agent.
2 Open the file config.properties.
   The file contains the following parameters with preset values by default:
   • discovery.host: aafserver.local
   • discovery.port: 443
   • oobAgent.daemonHost: oobserver.local
   • oobAgent.daemonPort: 443
   The above parameters are prefixed with the comment syntax (#) by default.
3 Remove the comment syntax and set a valid host address and port number for each parameter.
   For example, discovery.host = 192.168.20.40 or discovery.host = auth2.mycompany.local
   The parameters discovery.host: aafserver.local and discovery.port: 443 allows the Authentication Agent to discover the server and register the user for logging in to the agent.
The parameters `oobAgent.daemonHost`: `oobserver.local` and `oobAgent.daemonPort`: 443 are designed to make the agent wait for the new authentication requests on the Daemon host then examine and accept these authentication request initiated using the Authentication Agent chain from another computer.

**NOTE:** If the parameters `oobAgent.daemonHost` and `oobAgent.daemonPort` are not configured, then the agent applies the same host address and port that been set for the parameter `discovery.host` and `discovery.port` automatically to examine and accept any authentication request initiated using the Authentication Agent chain.

4. Save the configuration.
5. Restart the system.

**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.

### Configuring Time to Close the Restricted Browser

You can configure the duration until when the restricted browser is displayed after the user is authenticated using the Authentication Agent. When a user selects the Authentication Agent chain from the Chains list in one Client system, the Authentication Agent prompts a restricted browser on the Windows Client where the user authenticates. Once the authentication is done, the browser displays a message `Authentication is successful`. This browser does not close till the user closes it manually. You can configure the time to close the browser automatically. The default value for closing the browser is 5 seconds.

To configure the time to close the browser, perform the following steps:

1. Navigate to `C:\ProgramData\NetIQ\Advanced Authentication Agent` and open `config.properties` file.

   If the configuration file does not exist, create a new file.

2. Specify `agentSuccessClose=n` where `n` is time in seconds.

3. Save the changes.

4. 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:

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

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, the agent can discover the Advanced Authentication server in one of the following ways:

- Setting DNS for Server Discovery
- Using a Specific 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.
3. 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.
4 Troubleshooting

This chapter contains the following topics:

- “Debugging Logs for Advanced Authentication” on page 17
- “Agent Unable to Connect to the Server” on page 18
- “Authentication Agent Does Not Prompt the Restricted Browser for Authentication” on page 18

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
- Ionic.Zip.dll
- JHSoftware.DNSClient.dll

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**

**Issue:** 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.

**Workaround:** 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**

**Issue:** 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.

**Workaround:** 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.
Authentication Agent Does Not Respond During the Login Process

**Issue:** Sometimes, it is not possible to log in to the Authentication Agent because the agent does not respond during the login process. When you place the cursor over the Authentication Agent icon in the System Tray, a message *Logon in progress* is displayed.

**Workaround:** As a solution to this issue, perform the following:

- When you boot your workstation, log in to Windows, and Windows Client is not installed, ensure that a restricted browser is prompted to authenticate to the Authentication Agent. You must not close the restricted browser without completing the authentication.
- Double click the Authentication Agent icon in the System tray and pass the respective authentication chain to log in to the Authentication Agent.
- If the restricted browser window is not prompted, ensure you have the appropriate configuration to discover the Advanced Authentication server and Daemon host.

For more information on the preliminary settings of the authentication agent, see Configuring the Preliminary Settings.