Legal Notices

Copyright 2014 - 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.
Contents

About this Book ................................................. 5

1 System Requirements ......................................... 7

2 Configuring the Preliminary Settings ......................... 9
   Setting DNS for Server Discovery .................................. 9
   Using a Specific Advanced Authentication Server ................. 10
   Configuring Time to Close the Restricted Browser ................ 11

3 Installing and Uninstalling Windows Authentication Agent .......... 13
   Installing Windows Authentication Agent ......................... 13
   Uninstalling Windows Authentication Agent ........................ 13
      Using the Setup Wizard ........................................ 14
      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
      Authentication Agent Does Not Respond During the Login Process .......................... 17
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.
1 System Requirements

You must have the administrator privileges to install and uninstall Windows authentication agent.

For system requirements of Windows Authentication Agent, see Windows Authentication Agent.
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:
   - In the console tree, right-click the forward lookup zone that includes your domain name and click New Host (A or AAAA).
   - Specify a DNS name for the Advanced Authentication Server in Name.
   - 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).
   - 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:
   - In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.
   - In the Select a resource record type list, click Service Location (SRV) and click Create Record.
   - Click Service and specify _oob.
   - Click Protocol and specify _tcp.
   - Click Port Number and specify 443.
In Host offering this service, specify the FQDN of the Advanced Authentication Server with Daemon host [link](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/configuring_policy.html#t45mod4edeg8).

For example, authsrv.mycompany.com.

Click OK.

_aav6 records:

In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.

In the Select a resource record type list, click Service Location (SRV) and click Create Record.

Click Service and specify _aav6.

Click Protocol and specify _tcp.

Click Port Number and specify 443.

In Host offering this service, specify the FQDN of the server that is added.

For example, authsrv.mycompany.com.

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\AdvancedAuthenticationAgent`.
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:

**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, 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.
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
- 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.