Advanced Authentication 6.4

NPS Plug-in Installation Guide

July 2022

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.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/legal (https://www.microfocus.com/en-us/legal).

Contents

About this Book 5

1 Network Protocol Service (NPS) Plug-in 7

2 System Requirements for Installing NetIQ NPS Plug-in 9

3 Installing and Uninstalling the NetIQ NPS Plug-in 11

Installing the NetIQ NPS Plug-in. 11
Uninstalling the NetIQ NPS Plug-in 11

4 Configuring the NetIQ NPS Plug-in 13

5 Troubleshooting 15

Debugging Logs for NetIQ NPS Plug-in 15
Using the Diagnostic Tool 15
Manual 15
Logging for Windows Specific NetIQ NPS Plug-in Events. 16

About this Book

The NetIQ NPS Plug-in guide provides information about system requirements and how to install and configure the NetIQ NPS Plug-in on Windows.

Intended Audience

This guide is intended for the Advanced Authentication administrators.

1 Network Protocol Service (NPS) Plug-in

The NetIQ NPS Plug-in enables you to configure multi-factor authentication for RADIUS clients. The NetIQ NPS Plug-in uses the existing RADIUS events and RADIUS rules.

Figure 1-1 *NetIQ NPS Plug-in in Advanced Authentication as a Service*

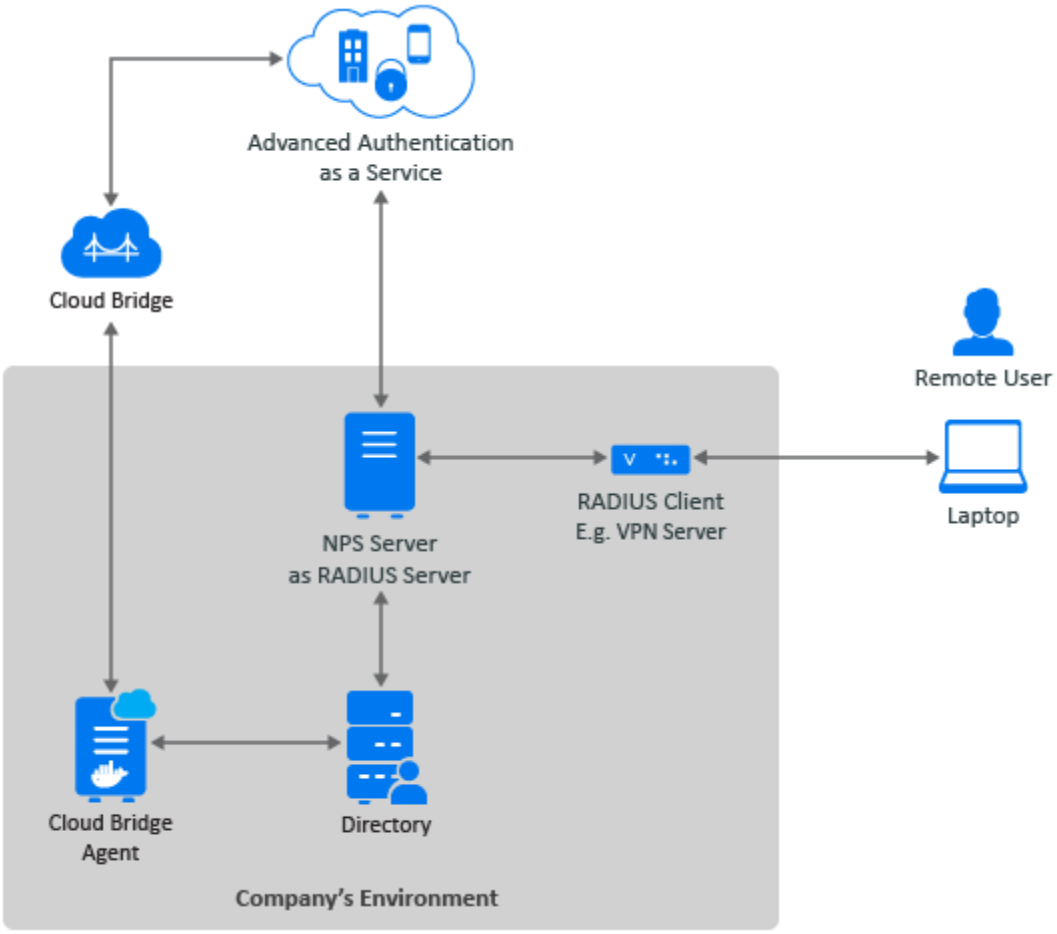
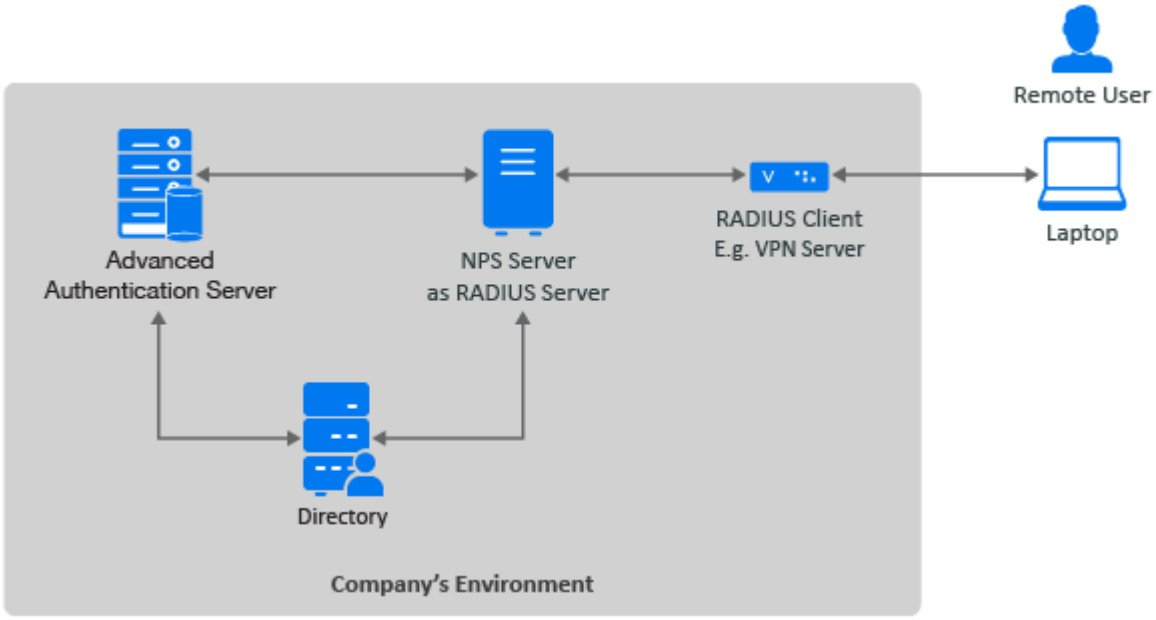


Figure 1-2 *NetIQ NPS Plug-in in Advanced Authentication On-premise Deployment*



2 System Requirements for Installing NetIQ NPS Plug-in

Before installing the NetIQ NPS Plug-in, ensure that the following requirements are met:

- Microsoft Windows Server 2012 R2, 2016, or 2019 is installed.
- Microsoft Network Policy Server (NPS) is configured. For more information, see Manage NPS (https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-top).

You must have the administrator privileges to install and uninstall the NetIQ NPS Plug-in.

Before configuring the NetIQ NPS plug-in, ensure to comply with the following pre-requisites:

- Third-party RADIUS client to work with Microsoft NPS server is configured.
- The required chains are assigned to the RADIUS Server event.
- The required RADIUS Clients are added in the RADIUS Options policy. For more information, see Adding Clients.

3 Installing and Uninstalling the NetIQ NPS Plug-in

This chapter contains the following sections:

- Installing the NetIQ NPS Plug-in
- Uninstalling the NetIQ NPS Plug-in

Installing the NetIQ NPS Plug-in

Perform the following steps to install NetIQ NPS Plug-in.

1. You can download the `naaf-npsplugin-x64-release-<version>.msi` file from Software Licenses and Downloads (https://sld.microfocus.com) portal.
2. Run the `naaf-npsplugin-x64-release-<version>.msi` file.
3. Click **Next**.
4. Read and accept the **License Agreement**, and click **Next**.
5. Click **Next** to install the plug-in in the default folder or click **Change** to select a preferred folder.
6. Click **Install**.
7. Click **Finish**.
8. Restart your machine.

Uninstalling the NetIQ NPS Plug-in

Perform the following steps to uninstall NetIQ NPS Plug-in.

1. Click **Start > Control Panel > Programs and Features**.
2. Right-click **NetIQ NPS Plugin** and select **Uninstall**.
3. Click **OK**.
4. Restart your machine.

4 Configuring the NetIQ NPS Plug-in

To configure the NetIQ NPS Plug-in, perform the following steps:

1. Create a NPS endpoint in Advanced Authentication server and keep the endpoint ID and secret. For more details, see Managing Endpoints.
2. Navigate to `C:\ProgramData\NetIQ\NPSPlugin`.
3. Open `config.properties` file.
4. Specify the following details:
   - Specify the domain name or IP address in `discovery.host`.

     For example, `discovery.host: 192.168.20.40` or `discovery.host: auth2.mycompany.local`.
   - Specify a port number (optional parameter) for the client-server interaction in `discovery.port`.

     For example, `discovery.port: 443`.
   - Specify the ID from the NPS endpoint in `endpoint_id`.

     For example, `endpoint_id: 6e1a79cee82311ea9e300242ac110003`.
   - Specify the Secret from the NPS endpoint in `endpoint_secret`.

     For example, `endpoint_secret: 3WcDvM9ddwQUF7pqARvfZqyMEGOqF022`
   - (Only in case of multitenancy) Specify the tenant in tenant

     For example, `tenant: Company`

     This parameter is not required since Advanced Authentication 6.3 Service Pack 5.
5. Click **Save**.
6. Restart NPS Service.

You can configure RADIUS rules in the RADIUS Options to set up the required behavior.

NOTE: Because of keeping the authentication state in memory, the NPS Plug-in does not support load balancing. Most RADIUS Clients can be configured to use multiple RADIUS Servers and the RADIUS Clients can switch to another RADIUS Server if the first RADIUS Server does not operate.

---

5 Troubleshooting

This chapter contains the following section:

- "Debugging Logs for NetIQ NPS Plug-in" on page 15
- "Logging for Windows Specific NetIQ NPS Plug-in Events" on page 16

Debugging Logs for NetIQ NPS Plug-in

This section contains the following topics:

- "Using the Diagnostic Tool" on page 15
- "Manual" on page 15

Using the Diagnostic Tool

To view the debug logs using the Diagnostic Tool, perform the following steps:

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click **Clear All** in the **Debug logs** tab.
3. Click **Enable**.
4. Restart the system.
5. Reproduce your issue.
6. Run `DiagTool.exe`.
7. Click **Save logs** in the **Debug logs** tab.
8. Specify a file name and path.
9. Click **Save**.
10. Click **Disable**.
11. Click **Clear All**.

Manual

If you do not have the Diagnostic Tool, you can view the debug logs manually. To view the debug logs manually, perform the following steps:

1. Navigate to `C:\ProgramData\NetIQ\Logging\`.
2. Create a text file `config.properties`.
3. Add a string to the file: `logEnabled=True` that ends with a line break.
4. Create a directory `C:\ProgramData\NetIQ\Logging\Logs\`.
5. Restart the system.

6 Repeat the issue.

7 Compress the logs located in `C:\ProgramData\NetIQ\Logging\Logs\` into a ZIP file.

Logging for Windows Specific NetIQ NPS Plug-in Events

To view the logs for Windows specific NetIQ NPS Plug-in events, perform the following steps:

1 Click **Start > Event Viewer**.

2 Click **Windows Logs > Application**.

3 Check the logs that are specific for NetIQ NPS plug-in.

The following table describes list of events:

Event Id	Severity	Description
1	Error	Failed to establish connection with server. Message: Connection refused, code: 10061.
2	Information	User XXX successfully completed method and started new one: TOTP:1 (from ZZZ.ZZ.Z.ZZZ:ZZZ, https:YES).
3	Error	User XXX was not found (from ZZZ.ZZ.Z.ZZZ:ZZZ, https:YES).
4	Information	Message from AAF server in case of multi stage logon.
5	Success	Connecting to server ZZZ.ZZ.ZZ.ZZZ:ZZZ, using ssl:YES.