Installation Guide

Advanced Authentication- ADFS Plug-in

Version 5.4

MICRO FOCUS

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/.

Contents

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

The ADFS Plug-in Installation Guide provides users with system requirements that must be fulfilled before the installation of Advanced Authentication ADFS plug-in.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

About ADFS Plug-in

ADFS plug-in provides you with the ability to integrate Advanced Authentication with Active Directory Federation Services 3.0 (ADFS 3.0) that helps to perform strong authentication to access the secured systems and applications.

1 System Requirements

IMPORTANT: You must have Local Admin rights to install and uninstall the ADFS plug-in.

Ensure that the system meets the following requirements:

- Microsoft Windows Server 2012 R2
- Microsoft .NET Framework 4.5
- Active Directory Federation Services 3 (ADFS 3.0)
- Microsoft SQL Server 2014 (can be installed on a separate server)
- You must have at least a self-signed certificate configured on Advanced Authentication. For more information, see “Configuring Server Options” in the *Advanced Authentication - Administration* guide.

You must install the ADFS plug-in on each ADFS server in an ADFS farm. After installation, ensure that you configure each ADFS plug-in to work together with the same Microsoft SQL database. This configuration enables sharing the internal state between different servers in the farm.

2 Installing and Uninstalling the ADFS Plug-in

2.1 Installing the ADFS Plug-in

1. Run `NAAF-ADFSv3Support-x64-Release-<version>.msi`.
2. Click **Next**.
3. Read and accept the Licence Agreement, then click **Next**.
4. Click **Next** to install the ADFS plug-in to the default folder (`%ProgramFiles%\NetIQ\ADFSv3`) or click **Browse** to choose another folder.
   - Click **Change** to change the destination folder.
   - Click **Next**.
5. Click **Install**.
6. Select **Lauch ADFSv3 Configurer** and click **Finish**.

2.2 Updating the ADFS Plug-in

To update the ADFS plug-in, perform the steps in section Installing the ADFS Plug-in.

After you update the ADFS plug-in, run the ADFS Configurer tool to reconfigure the plug-in. For more information, see Configuring the ADFS Plug-in.

2.3 Uninstalling the ADFS Plug-in

IMPORTANT: Before uninstalling the last ADFS plug-in in the ADFS farm, run Configuring the ADFS Plug-in and click **Switch ADFS 3.0** to **normal mode**, run **PowerShell** with the following commands:

```
Set-AdfsWebConfig -ActiveThemeName default
Remove-AdfsWebTheme –TargetName v5plugin
```

You can uninstall the ADFS plug-in through the Setup Wizard or Control Panel.

To uninstall the ADFS plug-in through the Setup Wizard, perform the following steps:

1. Run `NAAF-ADFSv3Support-x64-Release-<version>.msi`.
2. Click **Next**.
3. Select **Remove** and click **Next**.
4. Click **Remove** to confirm the uninstallation.

To uninstall the ADFS plug-in through the Control Panel, perform the following steps:

1. In the **Start** menu, select **Control Panel** and then double-click **Programs and Features**.
2. Select **NetIQ ADFS Plugin** and click **Uninstall**.
3. Confirm the uninstallation.

3 Configuring the ADFS Plug-in

You can start the ADFS 3.0 Configurer manually or automatically after installation of the ADFS plug-in.

To run the ADFS 3.0 Configurer manually, perform the following steps:

1. Click **Start** and specify **ADFSv3 Support Configurer** in **Search**.
2. Select the appropriate option from the search results.

To configure the Advanced Authentication ADFS plug-in, perform the following steps:

1. Specify a database connection in **DB connection string** or click **Database**.
2. Specify a **Server name** of Microsoft SQL Server in **Connection Properties**.
3. The **Use Windows Authentication** option is selected by default. Select the **Use SQL Server Authentication** for SQL authentication and specify the SQL Server credentials.
4. Select or specify a database name.
5. Click **Test Connection**.

   NOTE: A user account, in which the ADFS 3.0 Configurer is started must have the db_owner rights to access the database.

   ---

6. Click **OK**.
7. Click **Check DB** to validate access to the selected database.
8. You might receive the following error that indicates the specified database does not exist:

   ```
   Cannot open database "<DatabaseName>" requested by the login. The login failed.Login failed for user '<Username>'.
   ```

   a. Click **Init (create) DB** to create a new database.

   NOTE: The **Init (create) DB** option for existing database is equivalent to **Check DB** option. The required tables and indices are not overwritten, if they have been already created.

   IMPORTANT: You must click the **Check DB** option or **Init (create) DB** option each time you want to reconfigure the ADFS 3.0 plug-in.

   ---

9. Click **Next**.
10. Copy the specified value from **Service GUID (read only)** under the **Configure URL** to a text file.
11. Specify the following URL in **V5 server API URL**:

    http://<NAAFServer>/adfs/. Replace <NAAFServer> to an Advanced Authentication hostname (recommended) or IP address.

    WARNING: Ensure that the URL ends with a backslash`'/'`.

    ---

12. Click **Next**.
13. Select **SSL certificate** in the **ADFS 3.0 HTTPS (SSL) certificate for browser endpoint** list.
14. Copy the text from **Public key for V5 server** to any text file.

TIP: You can click **Regenerate key** if a currently used key was compromised. This is required only on one ADFS server in ADFS farm.

15. Click **Next**.
16. Click **Switch ADFS 3.0 to work with V5.**
17. Click **Save**.

IMPORTANT: You can click **Switch ADFS 3.0 to normal mode** if you want to disable the ADFS plug-in. You need to do this on only one ADFS server in ADFS farm.

4 Configuring SQL Server Database Permissions

The following procedure describes how to configure the required access permissions of the ADFS plug-in to a Microsoft SQL Server database. If you have selected **Windows authentication** on step 3 of Configuring the ADFS Plug-in, perform the following steps:

1. Open Microsoft SQL Server Management Studio on an SQL server.
2. Browse the database and go to the **Security - Users** section.
3. Add a new user with the following details:
   - **User type**: `SQL user with login`
   - **User name:** `LocalSystem`
   - **Login name**: `NT AUTHORITY\SYSTEM`
   - **Default schema**: `dbo`
4. Go to the **Membership** section and select `db_owner`.
5. Click **OK**.

5 Configuring Advanced Authentication Server

1. Open the Advanced Authentication Administrative Portal.
2. Open the properties of ADFS event in the **Events** section.
3. Specify chains that can be used for the ADFS Event.
4. Click **ADFS Partners.**
5. Enter a **Description** for ADFS partner.
6. In **Partner ID**, paste the copied GUID from **Service GUID (read only)** (step 10 of Configuring the ADFS Plug-in).
7. In **Public key (PEM)**, paste the copied public key from **Public key for V5 server** (step 14 of Configuring the ADFS Plug-in).
8. Click **OK**.
9. Click **Back** on the **ADFS partners** page.
10. Click **Save** on the **ADFS** event page.

NOTE: You must add only one ADFS partner for an ADFS farm.

6 Troubleshooting

To obtain the debug logs for ADFS plug-in, 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 problem.
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**.

If you do not have the Diagnostic Tool, you can perform the actions manually:

1. Create a text file `config.properties in the folder C:\ProgramData\NetIQ\Logging\`.
2. Add a string to the file: `logEnabled=True` that ends with 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 the folder `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 do this, perform the following steps:

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Switch to the **Servers** tab.
3. In the **Search settings** you must enter FQDN in **Domain** and click **Search**. A list of Advanced Authentication Servers is displayed.
4. If the list is not displayed, clear **Use system DNS server** and enter the IP address of your DNS server in **DNS server** and click **Search** again.