Advanced Authentication 6.2

ADFS Multi-Factor Authentication Plug-in

February 2019

Legal Notices

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 Multi Factor Authentication (MFA) Plug-in Installation Guide provides users with system requirements that must be fulfilled before the installation of Advanced Authentication ADFS MFA plug-in.

Intended Audience

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

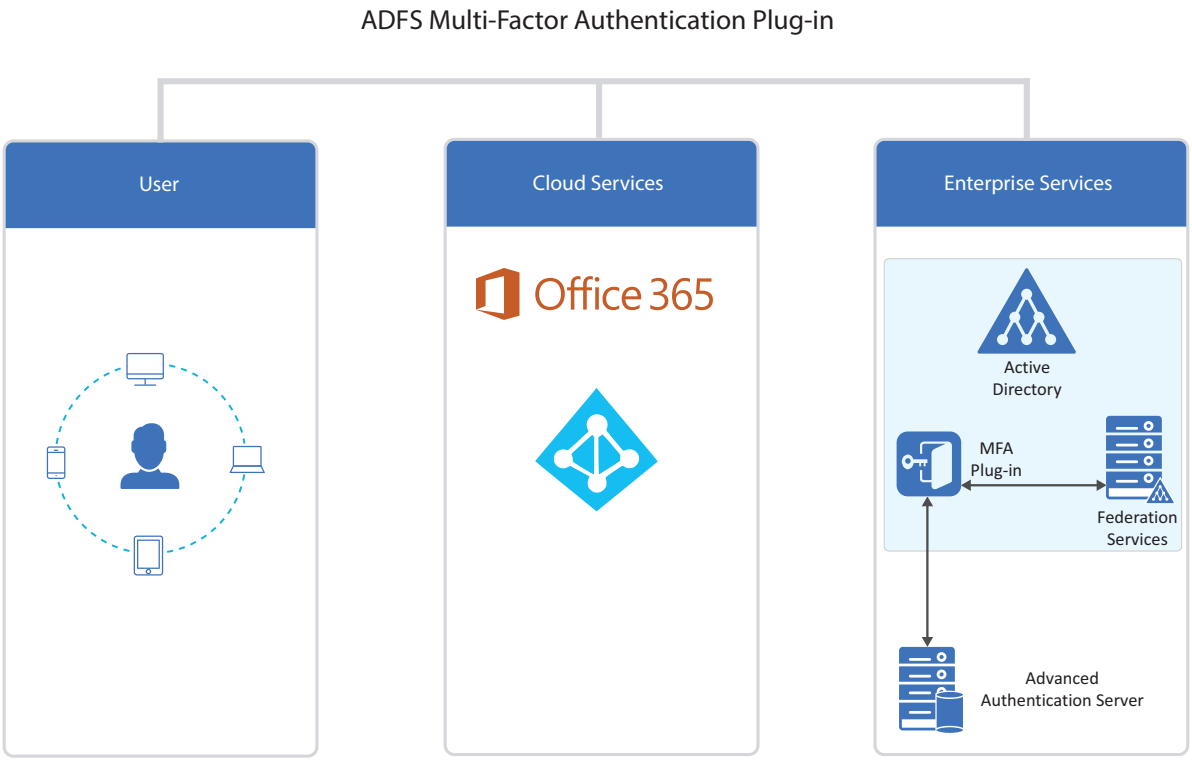
About ADFS Multi-Factor Authentication Plug-in

ADFS MFA plug-in provides you with the ability to integrate Advanced Authentication with Active Directory Federation Services 3.0 (Windows Server 2012 R2) or Active Directory Federation Services 4.0 (Windows Server 2016). This helps you to perform strong authentication to access the secured systems and applications.

NOTE: The ADFS MFA plug-in supports the following methods: Email OTP, Emergency password, HOTP, LDAP password, Password, RADIUS, SMS OTP, TOTP, and Voice OTP. To use the other authentication methods of Advanced Authentication, you need not install and configure the ADFS MFA plug-in. You can integrate with ADFS - using SAML. For more information, see“ Configuring Integration with ADFS (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/config_intrgtn_salesforce_adfs.html)” in the *Advanced Authentication - Administration* guide.

The following diagram illustrates the common deployment of ADFS Multi-Factor plug-in.

Figure 1 *ADFS Multi-Factor Authentication Plug-in*



1 System Requirements

IMPORTANT: You must have the local administrator privileges to install and uninstall the ADFS MFA plug-in.

Ensure that the system meets the following requirements:

- Microsoft Windows Server 2012 R2, 2016, or 2019[GUI].
- Microsoft .NET Framework 4.5
- ADFS role installed and configured. It must work correctly without the ADFS MFA plug-in

NOTE: It is recommended to have at least a self-signed certificate configured on Advanced Authentication. For more information, see "Configuring Server Options" in the *Advanced Authentication - Administration* guide.

2 Installing and Uninstalling the ADFS Multi-Factor Authentication Plug-in

Installing the ADFS MFA Plug-in

1. Run the file `NAAF-ADFSMFAPlugin-x64-Release-<version>.msi`.
2. Click **Next**.
3. Read and accept the License Agreement and click **Next**.
4. Click **Next** to install the ADFS MFA plug-in to the default folder (`%ProgramFiles%\NetIQ\AAF ADFS MFA Plugin\`).

   or

   Click **Change** to choose another folder.
5. Click **Next**.
6. Click **Install**.
7. Click **Finish**.

After you install the ADFS MFA plug-in, the **Administration Tool** is installed.

NOTE: You can find the ADFS MFA plug-in component in the Advanced Authentication Enterprise Edition or the Remote Access Edition distributive package.

You can install the plug-in on the other ADFS servers in the ADFS farm after installing and configuring the plug-in.

Uninstalling the ADFS MFA Plug-in

IMPORTANT: Before uninstalling the last ADFS MFA plug-in the ADFS farm, perform the following steps:

Microsoft Windows Server 2012 R2

1. Click **Authentication Policies**.
2. Click **Edit** in **Primary Authentication**.
3. Click the **Multi-factor** tab in **Edit Global Authentication Policy**.
4. Clear **AAF ADFS MFA Plugin**.

5 Click **Apply**.

6 Click **OK**.

Microsoft Windows Server 2016

1 Click **Authentication Methods.**

2 Click **Edit** in **Primary Authentication Methods**.

3 Click the **Multi-factor** tab in **Edit Authentication Methods**.

4 Clear **AAF ADFS MFA Plugin**.

5 Click **Apply**.

6 Click **OK**.

To uninstall the ADFS MFA plug-in, perform the following steps:

1 In the **Administration Tool**, click **Disable**.

2 Click **Start** > **Control Panel** > **Programs and Features**.

3 Select **NetIQ AAF ADFS MFA Plugin** and click **Uninstall**.

4 Confirm the uninstallation.

3 Configuring the ADFS Multi-Factor Authentication Plug-in

This chapter contains the following sections.

Configuring the Advanced Authentication ADFS MFA Plug-in

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

1. Launch the **Administration Tool**.
2. Specify a DNS name or IP address of an Advanced Authentication server without `https://` in **Server URL**.
3. Select **Ignore SSL errors** if the server has an invalid certificate (self-signed or expired).
4. The **Event name**, **Tenant name**, and **Templates path** are auto populated. You can edit them as per your requirement.

   NOTE: The **Tenant name** is ignored when multitenancy is disabled. Administrators need not edit the value of this field.

   ---
5. Specify a secret. The secret must contain a minimum of eight characters that include numbers and uppercase characters.
6. Click **Save**.
7. Click **Enable** only if it is a first (primary) server in the ADFS farm. For the other servers, you must click **Restart ADFS**.

   An endpoint will be created in the **Endpoints** section of the Advanced Authentication Administration portal.

After an endpoint is created in the Advanced Authentication server, the `config.properties` and `ep.properties` files are automatically created with the set configurations in the path `C:\ProgramData\NetIQ\AAF ADFS MFA Plugin`.

In the ADFS farm, all the plug-ins must have the same version of ADFS. If the versions are different, the synchronization will not happen and this affects the functionality of the plug-in.

IMPORTANT: During upgrading an ADFS MFA plug-in, it is recommended to upgrade all the other ADFS MFA plug-ins in the ADFS Farm.

For example, if you upgrade AAF ADFS MFA Plugin 6.0 to AAF ADFS MFA Plugin 6.1, then you must ensure that all the other plug-ins in the farm are also upgraded to ADFS 6.1.

Customizing the Branding of Advanced Authentication ADFS MFA Plug-in

This section contains the information on how to customize the branding of the Advanced Authentication ADFS MFA plug-in. Perform the following steps to customize the ADFS MFA plug-in templates:

1. Launch the **Administration Tool**.
2. Obtain the **Templates Path** from **Administration Tool**. The default path is following:

   `%ProgramFiles%\NetIQ\AAF ADFS MFA Plugin\templates`
3. The following table contains the files present in Templates Path and describes the customization options.

IMPORTANT: The information specified in {} is returned by Advanced Authentication server and displayed to the users. You can change the textual information outside {} to add custom branding or preferred descriptions.

Filename	Customization Options
`SelectChain.txt`	This file contains the following customization options for the chain selection: **{0}:** Contains the list of chains **{1}:** Contains the text for the **Next** button.
`ChainInfo.txt`	This file contains the following customization options for the chain information: **{0}:** Contains the chains identifier **{1}:** Contains a default value for individual chains **{2}:** Contains a text description for chains.
`LogonForm_<METHOD>_1.txt`	This file contains the following customization options for the login form: **{0}:** Contains the message returned from the server. For example, `Invalid Password` **{1}:** Contains a message that is displayed to the user that prompts user to input a value. For example, `Specify One Time Password` **{2}:** Contains the text for the **Next** button.
`FatalError.txt`	This file contains the error message text.

4 Configuring the Advanced Authentication Server for ADFS Plug-in

After you configure the ADFS MFA plug-in, you must create a customized ADFS event to enable multi factor authentication to ADFS.

To configure Advanced Authentication, perform the following steps:

1. Open the Advanced Authentication Administration portal.
2. Click **Events > Add**.
3. Create a customized event with the following parameters:
   - **Name**: Specify the name that you have specified in the Administration Tool. The default name is **MFA ADFS**.
   - **Event type**: Select **Generic**.
   - Select the required chains.

     You need not add the LDAP Password method in the chains because the multi-factor authentication with Advanced Authentication is done after the standard authentication with the Password method.
4. Click **Save**.
5. Open the ADFS console.
6. Click **Authentication Policies**.
7. In the **Actions** pane, click **Edit Global Primary Authentication Policies**.
8. Click the **Multi-factor** tab.
9. In **Select additional authentication method**, select **AAF ADFS MFA Plugin** and click **Apply**.

NOTE: ADFS MFA plug-in supports the following methods: Email OTP, Emergency password, HOTP, LDAP password, Password, RADIUS, SMS OTP, TOTP, and Voice OTP.

To use the other authentication methods of Advanced Authentication, you need not install and configure the ADFS MFA plug-in. You can integrate with ADFS - using SAML. For more information, see“ Configuring Integration with ADFS (https://www.netiq.com/documentation/advanced-authentication-63/server-administrator-guide/data/config_intrgtn_salesforce_adfs.html)” in the *Advanced Authentication - Administration* guide.

---

5 Configuring Multi-Factor Authentication on the ADFS Server for Testing Purpose

After you have installed and configured ADFS and configured the appliance with LDAP, you must configure MFA on the ADFS server.

To configure MFA on the ADFS server, perform the following steps:

1. Enable the Test page ADFS.

   NOTE: ADFS 2016 disables the `idpinitiatedsignon` page by default. You must manually enable it using the following command in Windows PowerShell:

   ```
   Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
   ```

2. Verify the URL in your browser: `https://<ADFSServer>/adfs/ls/idpinitiatedsignon.htm`.
3. Open the ADFS console.
4. Click **Trust Relationships > Relying Party Trusts > Action > Add Relying Party Trust**.
5. Select **Claim Aware** and click **Start**.
6. Select **Import data about the relying party published online or on a local network**.
7. Specify `https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml`
8. Click **Next**.
9. Specify the **Display name** and description (optional).
10. Select an **access control policy** as **Permit everyone and require MFA**.
11. Click **Next**.
12. Verify the configuration in the **Ready to Add Trust** tab.
13. Click **Next**.
14. Verify: `https://<ADFSServer>/adfs/ls/idpinitiatedsignon.htm`.

6 Troubleshooting

To obtain the debug logs for ADFS MFA 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.