
Advanced Authentication 6.2

IIS Authentication Plug-in 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 this Book	5
About NetIQ Corporation	7
1 System Requirements	9
2 Configuring the Preliminary Settings	11
Modifying Identity for an Application Pool	11
Enabling Windows Authentication for RDWeb	11
Enabling Windows Authentication for Outlook Web Access	12
Configuring the Advanced Authentication Server	12
3 Installing and Uninstalling the IIS Authentication Plug-in	13
Installing the IIS Authentication Plug-in	13
Uninstalling the IIS Authentication Plug-in	13
Using the Setup Wizard	13
Using Control Panel	13
4 Configuring the IIS Authentication Plug-in	15
5 Troubleshooting	17
Debugging Logs	17
Using Diagnostic Tool	17
Manual	18

About this Book

The IIS Authentication Plug-in guide provides information about system requirements and how to install and configure the IIS Authentication plug-in on Windows.

Intended Audience

This guide is intended for the Advanced Authentication domain administrators.

About IIS Authentication Plug-in

The Advanced Authentication IIS Authentication plug-in facilitates you to configure multi-factor authentication for the websites that are hosted and managed on the Microsoft IIS server. So the users who want to access the websites must perform multi-factor authentication on the IIS server.

For example, Bob, who is an end-user wants to access his mails on the Outlook Web Access (OWA) or the shared applications through Remote Desktop Web (RDWeb) that are hosted on the IIS server. He must perform multi-factor authentication using the IIS Authentication plug-in and get a secured access to OWA or RDWeb.

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.

1 System Requirements

Ensure that the following softwares are installed:

- ◆ Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2016
- ◆ Microsoft IIS Manager
- ◆ Microsoft .NET Framework 4.5

You must have the administrator privileges to install and uninstall the IIS Authentication plug-in.

2 Configuring the Preliminary Settings

You must complete the following tasks before using the IIS Authentication plug-in for multi-factor authentication on the Microsoft Internet Information Services (IIS) server:

- ♦ Change identity for an application pool, see [Modifying Identity for an Application Pool](#).
- ♦ Configure Windows authentication for RDWeb, see [Enabling Windows Authentication for RDWeb](#).
- ♦ Configure Windows authentication for OWA, see [Enabling Windows Authentication for Outlook Web Access](#).
- ♦ Create an OAuth 2.0 event, see [Configuring the Advanced Authentication Server](#).

Modifying Identity for an Application Pool

Perform the following steps to change the identity for any application that is running on IIS server to make the application secure and reliable:

- 1 Open the IIS Manager Console.
- 2 Click **Application Pools**.
- 3 Select a preferred application pool from the list.
For example, RDWeb Access.
- 4 Click **Advanced Settings** from the **Actions** menu on the right pane.
- 5 Set **Identity** to **LocalSystem** in **Process Model**.
- 6 Click **OK**.
- 7 Restart the IIS server.

Enabling Windows Authentication for RDWeb

Windows authentication is required for the IIS Authentication plug-in to send the encrypted password in a cryptographic exchange to the web server. To enable Windows authentication for RDWeb, perform the following steps:

- 1 Navigate to `C:\Windows\Web\RDWeb\Pages` and open the `web.config` file on Remote Desktop Web Access server.
- 2 Follow the instructions in the comment that begins with **To turn on Windows Authentication** and make relevant changes.
- 3 Save the changes.

Enabling Windows Authentication for Outlook Web Access

Windows authentication is required for the IIS Authentication plug-in to send the encrypted password in a cryptographic exchange to the web server. To enable Windows authentication for OWA, refer to the instructions available on the [Forum \(https://social.technet.microsoft.com/Forums/en-US/04211f65-0177-4df6-9d4f-5817caef2538/exchange-2013-owa-allow-integrated-windows-authentication-for-internal-network-user-?forum=exchangesvrclients\)](https://social.technet.microsoft.com/Forums/en-US/04211f65-0177-4df6-9d4f-5817caef2538/exchange-2013-owa-allow-integrated-windows-authentication-for-internal-network-user-?forum=exchangesvrclients).

Configuring the Advanced Authentication Server

Before configuring the IIS Authentication plug-in, you must create an **OAuth 2.0** event to enable the multi-factor authentication for the websites that are hosted on the Microsoft IIS server.

To obtain the Client ID and Client secret to configure the IIS Authentication plug-in, perform the following steps:

- 1 Log in to the Advanced Authentication Administration portal.
- 2 Create a chain with the preferred authentication methods.
- 3 Create an **OAuth 2.0** event and assign the preferred chain from the **Available** list to the event.

Make a note of the **Client ID** and **Client secret** for further use.

- 4 Specify any one URL in the **Redirect URIs. One URI per line**.
 - ♦ For Remote Desktop Web (RDWeb), specify `https://<rdwebaccess>/rdweb`
 - ♦ For Outlook Web Access (OWA), specify `https://<outlookwebaccess>/owa`

NOTE: The **Redirect URIs. One URI per line** is case insensitive. Therefore, ensure to specify the URL is lower case.

NOTE: You must specify single URL in **Redirect URIs. One URI per line** for integrating with IIS Authentication plug-in. If you have provided more than one URL, an error message `No client redirect URI was supplied in the request` is displayed when users try to authenticate to the URL using the plug-in.

- 5 Click **Save**.

3 Installing and Uninstalling the IIS Authentication Plug-in

This chapter contains the following sections:

- ♦ [Installing the IIS Authentication Plug-in](#)
- ♦ [Uninstalling the IIS Authentication Plug-in](#)

Installing the IIS Authentication Plug-in

- 1 Run the file `naaf-aafiisplugin-x64-release-<version>.msi` file.
- 2 Click **Next**.
- 3 Read and accept the **License Agreement** and click **Next**.
- 4 Click **Next** to install the plug-in in the default folder or click **Change** to select a preferred folder.
- 5 Click **Install**.
- 6 Click **Finish**.
- 7 Restart your machine.

Uninstalling the IIS Authentication Plug-in

You can uninstall the IIS Authentication plug-in in one of the following ways:

- ♦ [Using Setup Wizard](#)
- ♦ [Using Control Panel](#)

Using the Setup Wizard

- 1 Run the file `naaf-aafiisplugin-x64-release-<version>.msi` file.
- 2 Click **Next**.
- 3 Select **Remove**.
- 4 Click **Remove** to confirm.

Using Control Panel

- 1 Click **Start > Control Panel > Programs and Features**.
- 2 Right click **NetIQ AAF IIS Module** and select **Uninstall**.
- 3 Click **OK**.

4 Configuring the IIS Authentication Plug-in

You can configure the IIS Authentication plug-in with the Advanced Authentication server, OAuth 2.0 event details and then integrate the plug-in with IIS Manager to implement multi-factor authentication for the websites hosted on the IIS server.

To configure the IIS Authentication plug-in perform the following steps:

- 1 Click **Start > Administration Tool** on Windows system where you have installed the IIS Authentication plug-in.
- 2 Specify the following details:

Table 4-1 IIS Authentication plug-in parameters

Parameter	Description
Server URL	The DNS name or IP address of the Advanced Authentication server without <code>https://</code> .
Client ID	ID that is obtained from the OAuth 2.0 event.
Client secret	Secret that is obtained from the OAuth 2.0 event.
Tenant name	If the Multitenancy mode is enabled, specify the preferred tenant name. If the Multitenancy mode is not enabled then specify TOP by default.

- 3 Click **Save**.

- 4 Click **Registrations**.

The **Manage IIS registrations** window is displayed. All the websites that are hosted on the IIS Manager are populated in this window.

- 5 Select the preferred website and click **Enable**.

The users must pass the authentication methods in the IIS Authentication plug-in to access these websites that are enabled in the **Manage IIS registrations** window.

To disable a website, select the website and click **Disable**. The users can access the disabled websites without authenticating through the IIS Authentication plug-in.

To update the websites list, click **Refresh**.

To integrate the IIS Manager with the IIS Authentication plug-in, perform the following steps:

- 1 Open the IIS Manager console.
- 2 In **Features View** of IIS Manager, double-click **Authentication**.
- 3 On the Authentication page, select **Anonymous Authentication**.
Click **Edit** to set the anonymous authentication for users who will connect to the site.
- 4 In the **Edit Anonymous Authentication Credentials** dialog box, select **Application pool identity** and set this identity to `LocalSystem`.

5 Troubleshooting

This chapter contains the following section on troubleshooting:

- ♦ [“Debugging Logs” on page 17](#)

Debugging Logs

You can obtain the logs for IIS Authentication plug-in in the following ways:

- ♦ [“Using Diagnostic Tool” on page 17](#)
- ♦ [“Manual” on page 18](#)

Using Diagnostic Tool

To collect 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**.

With the Diagnostic Tool, you can also 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 specify 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 specify the IP address of your DNS server in **DNS server** and click **Search** again.

Manual

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

- 1 Create a text file `C:\ProgramData\NetIQ\Logging\config.properties`.
- 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 system.
- 5 Repeat the scenario.
- 6 Compress the logs located in `/Library/Logs/NetIQ/Logs/` into a zip file.
- 7 Change `logEnabled=True` to `logEnabled=False` in the file.