



Advanced Authentication 6.4

IIS Authentication 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 System Requirements	7
2 Configuring the Preliminary Settings	9
Modifying Identity for an Application Pool	9
Configuring the Application Pool for Domain User Account	9
Enabling Windows Authentication for RDWeb	11
Enabling Windows Authentication for Outlook Web Access	11
Configuring the Advanced Authentication Server	11
Configuring the Web Authentication Policy	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 the Diagnostic Tool for Debugging Logs	17
Manually Debugging Logs	18
Outlook Web App Is Not Logged out Until the Browser Is Closed	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.

IIS Authentication plug-in leverages the Service for User (S4U) impersonation feature to obtain the user token to interact with and secure the Windows resources hosted on the IIS server. Advanced Authentication performs the primary authentication and then Windows authentication is required to acquire the access token for an identified user through S4U.

If the resources to be accessed are available on the local host, then set the IIS Pool as LocalSystem. This applies for applications with resources on single host, including small scale implementations of OWA, RDWeb, or similar applications.

When resources to be accessed are available on different hosts, then S4U requires the following:

- ♦ A domain user to manage the IIS Pool with the required privileges and groups.
- ♦ Configure Kerberos constrained resource delegation.

An example of this usage is multi-host services like Sharepoint with SQL hosted separately.

1 System Requirements

For system requirements of IIS Authentication plug-in, see [Plug-Ins Requirements](#).

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](#).
- ♦ Configure Web Authentication event, see [Configuring the Web Authentication Policy](#)

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 the **Identity** in the **Process Model** to one of the below values:
 - ♦ LocalSystem when working with only local resources.
This is the last step while configuring the application pool for local resources.
 - ♦ Specific username of the domain user with an appropriate privileges and delegations.
For Domain user account, continue with [Configuring the Application Pool for Domain User Account](#).
- 6 Click **OK**.

Configuring the Application Pool for Domain User Account

It is required to configure the following settings for running the pool using a domain user account:

- ♦ Add the Security policy on the IIS host where Advanced Authentication IIS Authentication Plug-in is installed and grant required permissions. For more information, see [Configuring IIS Hosts](#).
- ♦ Provide necessary permission for domain users on the domain. For more information, see [Domain Access to Authorization of User Accounts](#).
- ♦ Grant constrained delegation. For more information, see [Configuring Constrained Delegation](#).

Configuring IIS Hosts

The IIS hosts where the Advanced Authentication IIS Authentication Plug-in is installed, perform the following:

- 1 Add the preferred domain user to the local administrators group.
- 2 Navigate to one of the following paths to grant user privileges through the following permissions:
 - ♦ For local policy: **Start > Administrative Tools > Local Security Policy** navigate to **Local Policies > User Rights Assignment**.
 - ♦ For domain policy: Open relevant GPO in gpedit then navigate to **Local Policies > User Rights Assignment**.

Grant the following permissions:

- ♦ Act as part of the operating system
- ♦ Impersonate a client after authentication
- ♦ Log on as a service
- ♦ Log on as a batch job

Domain Access to Authorization of User Accounts

Accounts that perform Service for User Impersonation (S4U) need to be granted **Read tokenGroupsGlobalAndUniversal**. This gets assigned when the user accounts are included in the inbuilt domain group, Windows Authorization Access Group.

Launch **Active Directory Users and Computers**, click **Domain/builtin in tree > Windows Authorization Access Group Properties > Members** then search and select one or more users.

NOTE: When there are multiple domains, the pool user must be added to the group in each domain from where users will login.

Configuring Constrained Delegation

- 1 Launch **Active Directory Users and Computers** and select the preferred IIS host.
- 2 Click **Delegation** tab.
- 3 Select **Trust this computer for delegation to specified services only** and select **Use any authentication protocol**.
- 4 Configure each target resources by service type and host.

For example,

- ♦ **CIFS** service for file share.
- ♦ **SQLSvc** service for SQL 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.

NOTE: The Client ID and Client secret are required to be set in IIS server through the admin tool. Client secret is hidden after the initial setup and requires regeneration if the secret is not consumed by the IIS server.

- 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, URL can have mixed case and ensure the URL match the exact case.

NOTE: You must specify multiple URL in **Redirect URIs**. **One URI per line** for integrating with IIS Authentication plug-in.

- 5 Click **Save**.

Configuring the Web Authentication Policy

Perform the following steps to configure Web Authentication policy:

- 1 Log in to the Advanced Authentication Administration portal.
- 2 Navigate to **Policies > Web Authentication**.
- 3 Specify the DNS name of the Advanced Authentication server in **Identity Provider URL** field.

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	DNS name of the Advanced Authentication server without <code>https://</code> . NOTE: You cannot specify IP address of Advance Authentication server in Server URL.
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.
Logout URL	To handle logout in another application, set this field with URL related to that application. For example, to allow Outlook Web Access (OWA) to manage logout, set Logout URL with <code>/owa/logoff.owa</code> . This field can be empty. For example, in case of RDWeb. However, if the Logout URL is empty, IIS plug-in cannot manage the logout process.

- 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**.

5 Troubleshooting

This chapter contains the following section on troubleshooting:

- ♦ [“Debugging Logs” on page 17](#)
- ♦ [“Outlook Web App Is Not Logged out Until the Browser Is Closed” on page 18](#)

Debugging Logs

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

- ♦ [“Using the Diagnostic Tool for Debugging Logs” on page 17](#)
- ♦ [“Manually Debugging Logs” on page 18](#)

Using the Diagnostic Tool for Debugging Logs

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.

Manually Debugging Logs

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 issue.
- 6 Compress the logs located in C:\ProgramData\NetIQ\Logging\Logs\ into a ZIP file.

Outlook Web App Is Not Logged out Until the Browser Is Closed

If you have configured the exchange server to use the Windows Authentication and a prompt stating to close the browser to terminate the browser session is displayed then you can switch to the Form-based authentication.

Run the following command in the Exchange Management shell to use Form-based authentication:

```
Set-OwaVirtualDirectory -FormsAuthentication $true -WindowsAuthentication  
$false -Identity "IDENTITY_NAME"
```

Replace the IDENTITY_NAME with valid hostname\owa (web site name)