# Aras Innovator 32

## Windows Authentication Setup

***Document #: D-008153***

***Last Modified:*** *5/9/2024*

# Copyright Information

Copyright © 2024 Aras Corporation. All Rights Reserved.

Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
**Phone:** 978-691-8900

**E-mail:** support@aras.com

**Website:** https://www.aras.com/

**Notice of Rights**

Copyright © 2024 by Aras Corporation and/or its affiliates. All rights reserved.

This document is protected by U.S. and international copyright laws and conventions. No copyright may be obscured or removed from this document. This document may not be modified or altered, or reproduced or transmitted in any form, without the explicit permission of the copyright holder.

Aras Innovator, Aras, and the Aras Corp "A" logo are registered trademarks of Aras Corporation in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

**Notice of Liability**

THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY, AND THE CONTENTS HEREOF ARE SUBJECT TO CHANGE WITHOUT NOTICE. THE INFORMATION CONTAINED IN THIS DOCUMENT IS DISTRIBUTED ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR A WARRANTY OF NON-INFRINGEMENT. ARAS SHALL HAVE NO LIABILITY TO ANY PERSON OR ENTITY WITH RESPECT TO ANY LOSS OR DAMAGE CAUSED OR ALLEGED TO BE CAUSED DIRECTLY OR INDIRECTLY BY THE INFORMATION CONTAINED IN THIS DOCUMENT OR BY THE SOFTWARE OR HARDWARE PRODUCTS DESCRIBED HEREIN.

# Table of Contents



©2024 Aras Corporation All Copyrights Reserved.

# Send Us Your Comments

Aras Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for future revisions.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where and what level of detail?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, indicate the document title, and the chapter, section, and page number (if available).

You can send comments to us in the following ways:

**Email:**
TechDocs@aras.com
Subject: Aras Product Documentation

Or,

**Postal service:**
Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Attention: Aras Technical Documentation

If you would like a reply, provide your name, email address, address, and telephone number.

If you have usage issues with the software, visit https://www.aras.com/support/

©2024 Aras Corporation All Copyrights Reserved.

# 1 Overview

Aras Innovator provides the flexibility to give administrators many options when controlling the maintenance of user logins to Aras Innovator. One method is the use of the Windows Authentication Plugin. This plugin provides a way to implement specialized requirements for single-sign-on, authorization control, and auditing. These configurations can include standard Aras Innovator connections, leverage Web Server authentication, or use client portals for authentication. This document concentrates on the use of the Windows Authentication plugin for Active Directory authentication but is not the only the possible configuration. Many implementations are possible, but this document should help with one of the most common deployments using Windows Authentication.

**Note:** Changes described in this document should not be made to a production instance of Aras Innovator while it is running. Plan to implement these features only when users are not connected to the system, in a controlled deployment.

©2024 Aras Corporation All Copyrights Reserved.

# 2 Aras Innovator Windows Authentication Plugin for External Authentication

You can customize the Aras Innovator client logon using the Windows Authentication Plugin described in this section. This plugin enables you to implement specialized requirements for single-sign-on, authorization control, and auditing. The customization is pre-installed in the OAuth server installation and is enabled by modifications to the installed features on the OAuth server as well as configuration changes in the OAuth server Installation. In reading this section it helps to keep in mind that this is only one possible implementation of this feature; this section represents what Aras has had the most requests for and can be set up without programming knowledge.

## 2.1 Administrative Setup

This section describes the options that the administrator can enable in an Aras Innovator instance.

### 2.1.1 Enabling Windows Authentication

In order to enable the Windows Authentication Plugin, you must first enable the Windows Authentication feature on the OAuth server. A server administrator needs to enable the following feature in the roles and services section.

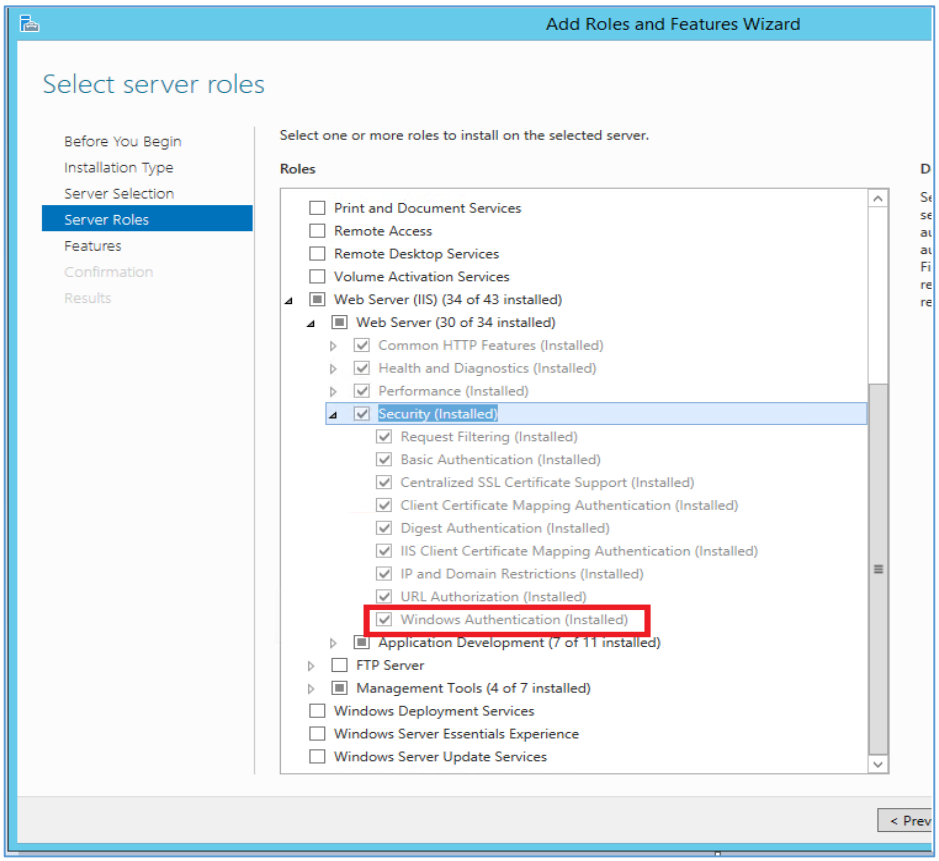



Figure 1.

©2024 Aras Corporation All Copyrights Reserved.

If you do not have Windows Authentication setup, the following URL takes you to the login selection page so you can select the login type:

```
?prompt=select_account
```

If you have Windows Authentication set up, the following code forces the user to log in to the specified database:

```
?auth=Windows&db=InnovatorSolution
```

### 2.1.2 Manual Configuring of Windows Sign-In Endpoint

In the general case the Aras Innovator installer sets up this endpoint automatically and no additional steps are required.

In case the Aras Innovator installer was not used for OAuth server 11.0 SP15 or 12.0 SPX deployment, the `/OAuthServer/signin-windows` endpoint must be configured manually. This endpoint must have Windows Authentication enabled and should have Anonymous Authentication disabled. It could be done using the `appcmd.exe` tool located in `%WINDIR%\System32\inetsrv` folder.

Run the following command to see if the `signin-windows` endpoint is protected by Windows Authentication:

```
appcmd list config "Default Web Site/<web_alias>/OAuthServer/signin-
windows" -section:system.webServer/security/authentication/
windowsAuthentication /text:enabled
>
true
```

The command should return `true`.

If `false` is returned, run the following command to enable Windows Authentication:

```
appcmd set config "Default Web Site/<web_alias>/OAuthServer/signin-
windows" /section:windowsAuthentication /enabled:true /commit:appHost
```

It is further recommended to disable Anonymous Authentication:

```
appcmd set config "Default Web Site/<web_alias>/OAuthServer/signin-
windows" /section:anonymousAuthentication /enabled:false /commit:appHost
```

### 2.1.3 Configuring the Windows Authentication Plugin (Optional)

After enabling Windows Authentication, you must configure the OAuth server to use the Windows Authentication Plugin. This section describes how to configure the plugin for use when Microsoft Active Directory single sign-on is desired. This plugin is used to receive the Windows Identity from the authentication module with a trusted value of Windows user account name in the `DomainName\UserName` form. This method of authentication is described in section 4.

#### *2.1.3.1 Enabling the Windows Authentication Plugin*

Use the following procedure to enable the OAuth Windows Authentication Plugin in the OAuth server Installation Directory.

1. Go to the `<Installation Directory>\OAuthServer\` folder.
2. Open the `OAuthServer.Plugins.json` file.
3. Enable the `Aras.OAuth.Server.Plugins.WindowsAuthentication` plugin:

©2024 Aras Corporation All Copyrights Reserved.

```
{
   "Name": "Aras.OAuth.Server.Plugins.WindowsAuthentication",
   "Enabled": true,
   "Options": {
      "AuthenticationType": "WindowsRemote",
      "DisplayName": "Windows"
   }
}
```

**Warning** Do not change the `AuthenticationType` because it is used internally in the OAuth server.

Do not use the `Windows` value for `AuthenticationType` because it is already reserved by the IIS Integration module.

#### *2.1.3.2 Enabling the WindowsUserByNameClaimMapper Plugin*

1. Go to the `<Installation Directory>\OAuthServer\` Folder.
2. Open the `OAuthServer.Plugins.json` file.
3. Enable the `Aras.OAuth.Server.Plugins.WindowsUserByNameClaimMapper` plugin:

```
{
   "Name": "Aras.OAuth.Server.Plugins.WindowsUserByNameClaimMapper",
   "Enabled": true,
   "Options": {
      "AuthenticationType": "WindowsRemote",
      "AllowedDomainNames": ".*",
      "AllowedDomainUsers": ".+",
      "DeniedDomainUsers":
         "^admin$|^root$|^vadmin$|^authadmin$|^esadmin$"
   }
}
```

Use this plugin to specify the following parameters:

- `AuthenticationType`: the authentication type to be used with the current mapper.
- `AllowedDomainNames`: a regular expression. The domain portion of the Windows user account name must match this expression in order to be used in Aras Innovator. If there is a finite list of domains to recognize then it is best to use a fixed list with the or `"|"` operator, for example, `'^europe$|^usa$|^fareast$'`. The `'^'` character in this context means matching the start of a string. The `'$'` character matches the end of the string. A string without these, e.g. `'east'` would match `'FarEast'` and also `'EasterIsland'` and any string containing the sequence `'east'`. Matches are case insensitive.
- `AllowedDomainUsers`: a regular expression. Usually it is best to keep it at `'.+'` which means to match one or more characters. This expression must match in order for the logon to Aras Innovator to be allowed. The username portion of the Windows user account name is matched against this. If it matches then it becomes the login_name used to log into Aras Innovator.

©2024 Aras Corporation All Copyrights Reserved.

- `DeniedDomainUsers`: it is matched against the username if it passes the `allowed_domain_users` test. If the match is true, then access to Aras Innovator is denied. This prevents domain users from logging in as Aras Innovator users with the same username. This option should be set to a list of special purpose Aras Innovator users. The 'Innovator Admin' (username=admin) user for example is often used when batch loading data or managing AML upgrades. The **Super User** (`username=root`) user must be used when applying database upgrade patches to the Aras Innovator database. The **Vault Admin** (username=vadmin) user is used only by the Vault server in order to access the mime type database. Other `denied_domain_users` might include the user used by the Aras Innovator Scheduler Service, or a test user used to review upgrades in functionality.

**Warning** `AuthenticationType` must be equal to the authentication type specified in the appropriate authentication plugin.

#### *2.1.3.3 Enabling the CustomProtocol Plugin*

If you want to use full windows authentication for all servers you will need to enable the `Aras.OAuth.Server.Plugins.CustomProtocol` plugin. Use the following procedure:

1. Go to the `<Installation Directory>\OAuthServer\` Folder.
2. Open `OAuthServer.Plugins.json` file.
3. Enable the `Aras.OAuth.Server.Plugins.CustomProtocol` plugin:

```
{
   // Enables Custom protocol type for OAuthServer
   "Name": "Aras.OAuth.Server.Plugins.CustomProtocol",
   "Enabled": true
}
```

### 2.1.4 Aras Innovator User Setup

In order to use authentication plugin with mapper plugin, a user Item with the required `login_name` must exist in the Aras Innovator database, with `logon_enabled = true`. The user's `login_name` must match the Windows Account Name. If no such user exists, the Login Form appears, but upon pressing the Login button the error message 'Authentication failed for *X*' is seen.

**Warning** Users must have a non-null password. Users with a null password will not be able to log in; however, the actual password is not used and can be set to anything.

©2024 Aras Corporation All Copyrights Reserved.

### 2.1.5 Logging in as an Authenticated User

To log in as a Windows Authenticated user, you must select **Windows** in the **Login with** drop down:


Figure 2.

### 2.1.6 Logging in as a Standard User

To log in as a standard user, you must select **Aras Innovator** in the **Login with** drop down:


Figure 3.

### 2.1.7 Switching Between Logon Types

For end user convenience, the Aras Innovator Login Screen caches your logon method (Windows/Standard). To return to the logon mode selection dialog, you will need to add the `prompt` query parameter with the `select_account` value. The full URL is:
`http://<host_name>/<application_alias>/?prompt=select_account`

©2024 Aras Corporation All Copyrights Reserved.

Another option is to clear `Aras.OAuth.Preferences.AuthenticationType` and `Aras.OAuth.Preferences.Database` cookies.

## 2.2 Configuring Single Sign On

Aras Innovator uses your browser configuration to reuse your Active Directory credentials for Single Sign On. The following section describes how to configure Single Sign on for Chrome and Edge.

**Note:** Single Sign On for Firefox is not supported due to browser limitations.

### 2.2.1 Configuring Single Sign On

1. In the start menu, search for **Internet Options** to open Internet Options.
2. Go to the **Security** tab.

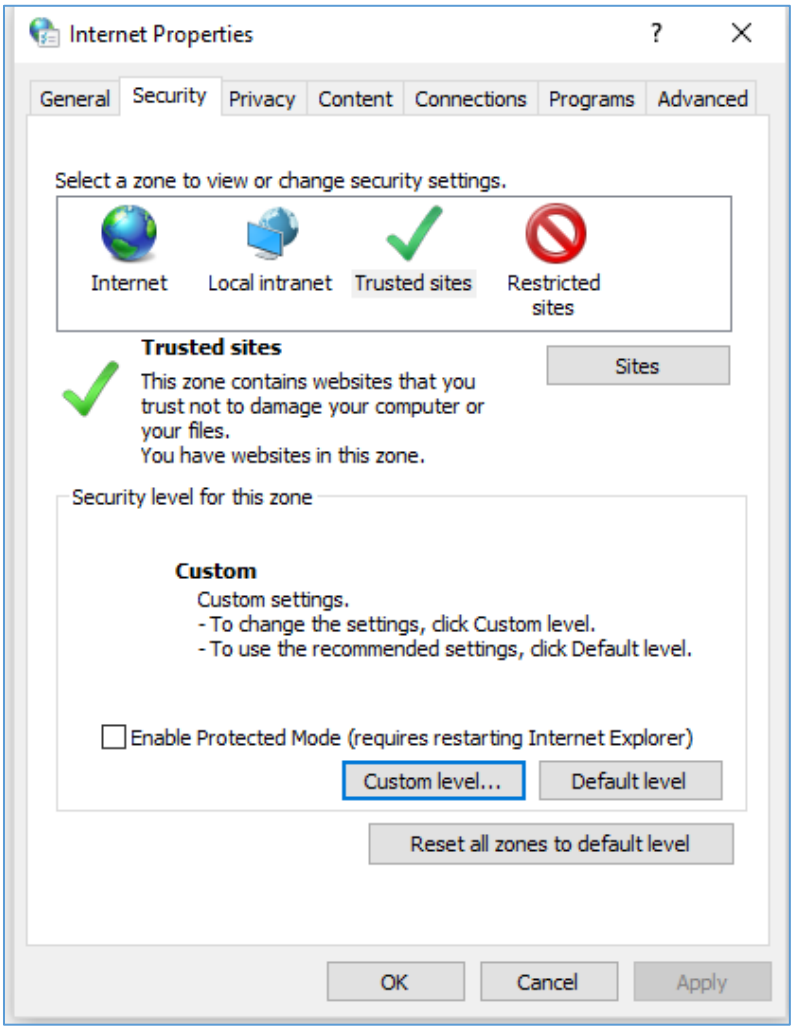



Figure 4.

Your URL should already be in the Trusted Sites zone if you have used the appropriate Client Settings Guide.

©2024 Aras Corporation All Copyrights Reserved.

3. Select **Custom Level**. The **Security Settings** dialog box appears.

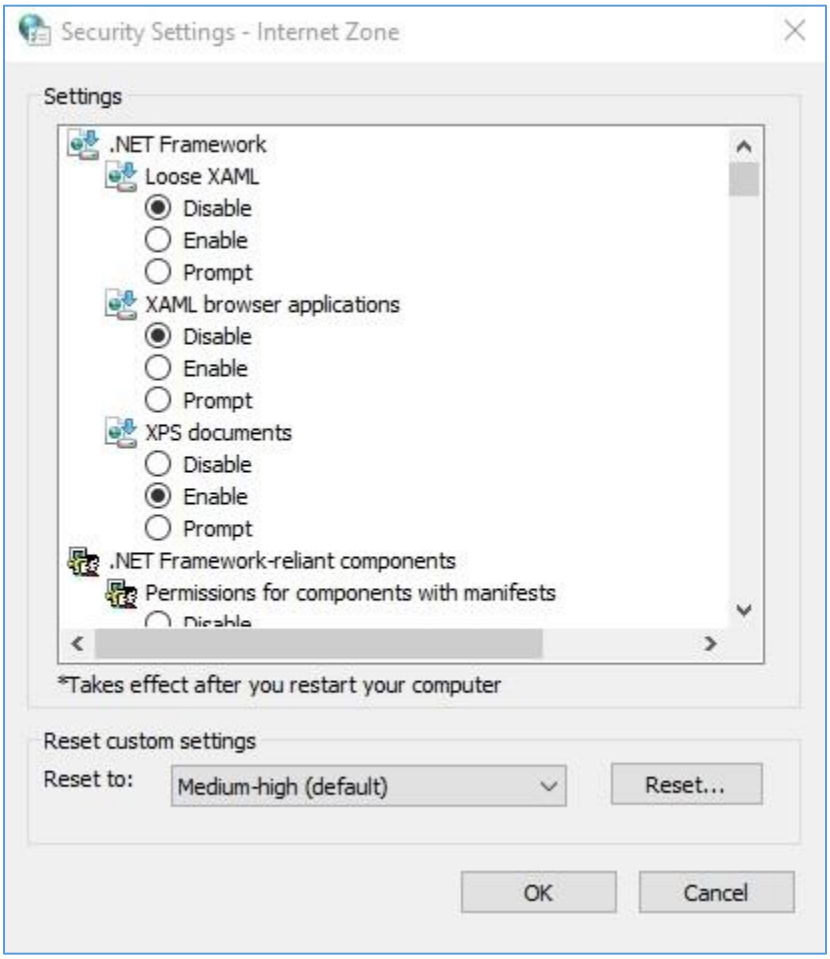



Figure 5.

©2024 Aras Corporation All Copyrights Reserved.

4. Scroll down to **User Authentication** and select **Automatic Logon with current user name and password**.

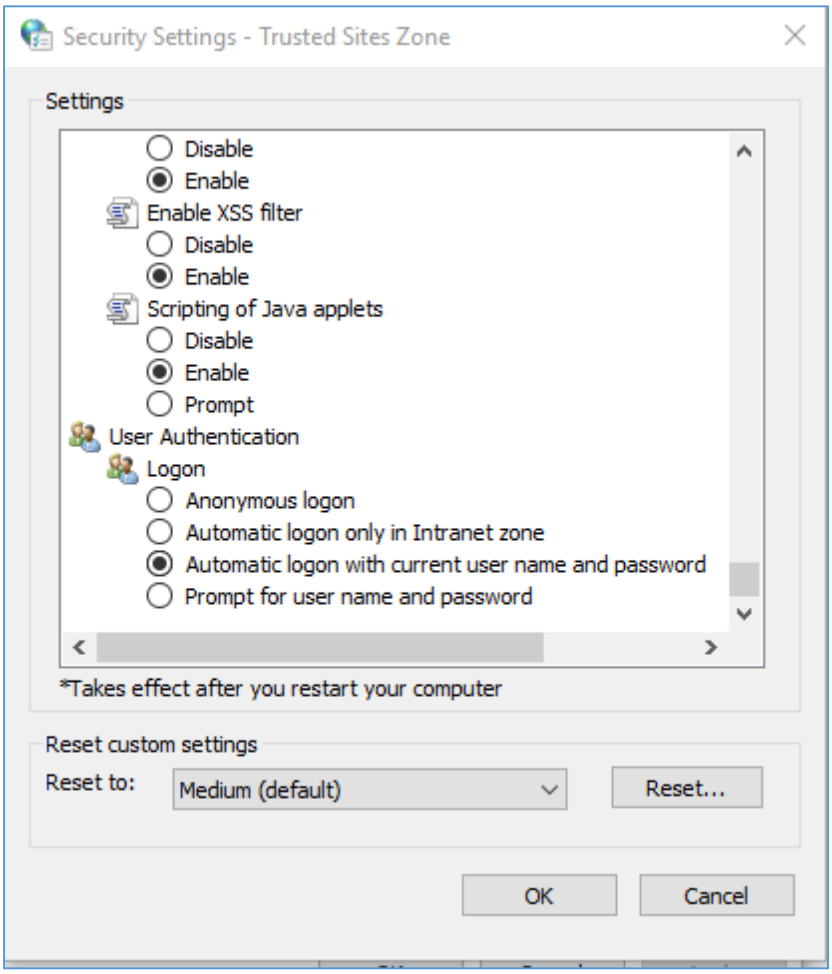



Figure 6.

5. Double click **OK**.

©2024 Aras Corporation All Copyrights Reserved.

# 3 Securing built-in Aras Innovator Accounts

It should be noted that the core Aras Innovator database comes with the following five built-in accounts:

- **Innovator Admin**—the **admin** username
- **Super User**—the **root** username
- **Vault Admin**—the **vadmin** username
- **Authentication Admin**—the **authadmin** username
- **ES Admin**—the **esadmin** username

The **Innovator Admin** and **Super User** accounts should be changed to prevent them being used by persons who know something about the default values of these passwords by disabling these accounts and only enabling logon during periods controlled by strict configuration management principals. Users should be made members of the **Administrators** Identity to have administrative privileges assigned to their own account, rather than using the Innovator **Admin** or **Super User** accounts.

The **Vault Admin** user cannot be disabled if the VaultServer feature of Aras Innovator is being used. The best way to restrict access to this account is to generate a random, sufficiently long password that is difficult to guess, and to store this password in encrypted form in the `VaultServerConfig.xml` file.

The **Authentication Admin** account is used to run Aras Innovator server methods that are necessary for authentication. The best way to restrict access to this account is to generate a random, sufficiently long password that is difficult to guess.

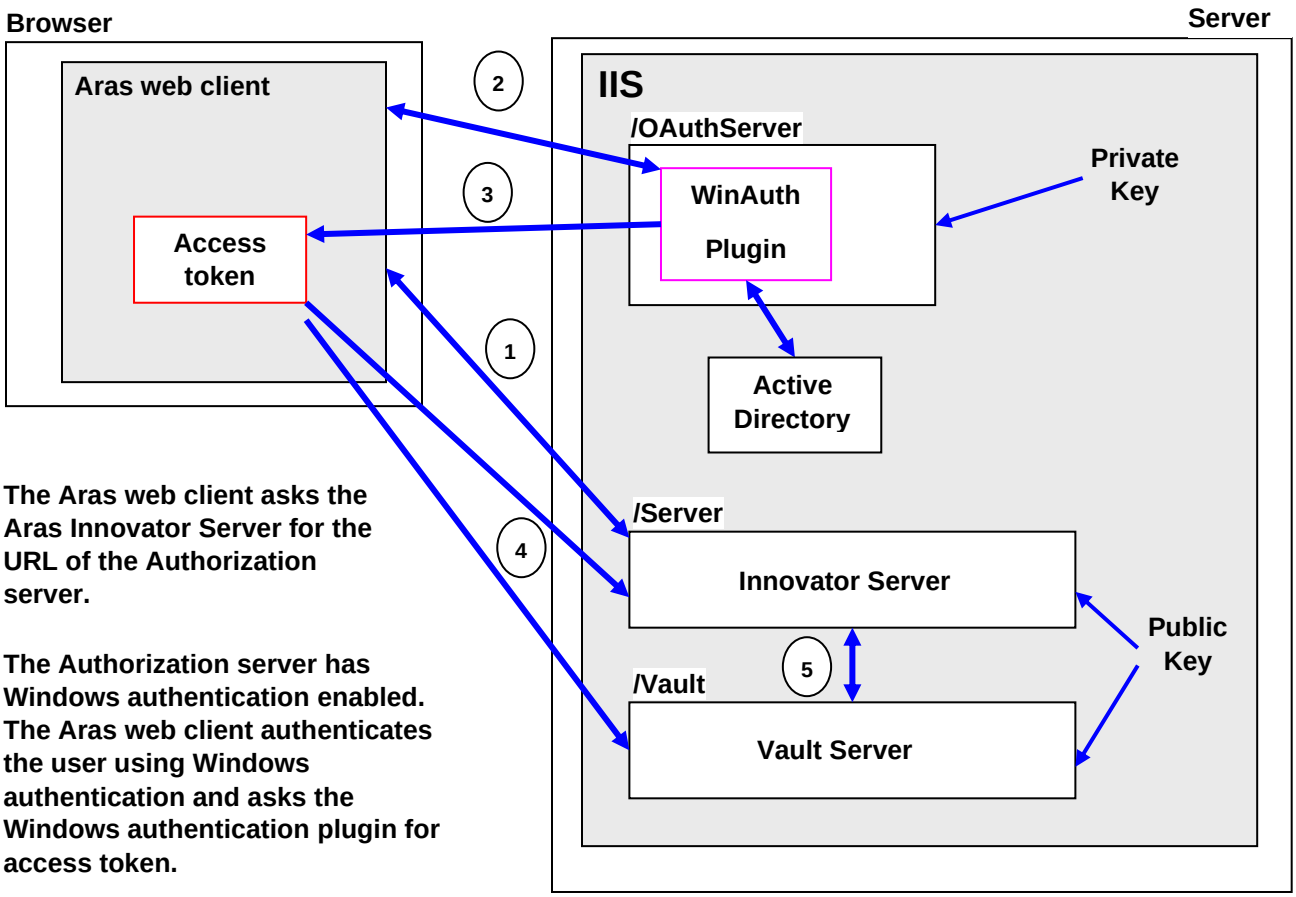
The **ES Admin** user cannot be disabled if Enterprise Search functionality is used. The best way to restrict access to this account is to generate a random, sufficiently long password that is difficult to guess, and to store this password in encrypted form in the `service.config` file.

The Aras Visual Collaboration solution also uses a designated user called `pdftron_user`. This user should be accommodated in the Windows Authentication setup as well.

©2024 Aras Corporation All Copyrights Reserved.

# 4 Reference Diagrams

## Client OAuth Authentication Sequence, Web Server Mode




1. The Aras web client asks the Aras Innovator Server for the URL of the Authorization server.
2. The Authorization server has Windows authentication enabled. The Aras web client authenticates the user using Windows authentication and asks the Windows authentication plugin for access token.
3. The Authorization server issues a user access token signed by its private key.
4. The Aras web client uses a received access token in requests to server applications. Server applications validate the access token using the public key of the Authorization server.
5. The Vault server proxies access token to Innovator server and may ask the Authorization server to re-issue the token in case it's expired in transit.

©2024 Aras Corporation All Copyrights Reserved.