How to Set Windows Integrated Authentication for the ArchiveOne Search and Retrieval Website

https://campus.barracuda.com/doc/46206772/

This article refers to the Barracuda ArchiveOne versions 5.8.1 and higher, except where noted

Use the steps in this article to change the authentication method for the ArchiveOne Search website to Windows integrated authentication. For example, this method is useful if you do not want to prompt end-users to log in to the ArchiveOne Search website.

Step 1. Determine the Web Servers Hosting the Search and Retrieval Website

Use the following steps to determine the web server(s) hosting the Search and Retrieval website:

1. On the Archive server, open the ArchiveOne console.
2. Right-click the Status Node, and click **Run System Configuration Wizard**.
3. In the wizard, click **Next** until you reach the **Search URL** page.
4. The address on the Search URL page indicates where the ArchiveOne Search and Retrieval website is hosted. This may be an individual hostname or a DNS alias which represents a number of load balanced web servers.

Step 2. Modify the Web Server Configuration

For ArchiveOne version 7.3 and higher:

1. Browse to the local configuration store in **C:\ProgramData\Barracuda\ArchiveOne\LocalConfigurationStore**.
2. Open the **Web_AOneSearch.ini** in a text editor such as Notepad.
3. Find the line: **AuthenticationMode=Forms**
4. Edit the line to: **AuthenticationMode=Windows**
5. Save and close the file.
6. Open **IIS Manager** and expand ***Servername* > Application Pools.**
7. Right-click the application pool **Archive One 4.0** and select **Recycle**.

For ArchiveOne version 7.2 and earlier:

On each web server identified in the previous set of steps, make the following configuration changes:

1. Browse to the **AOneSearch** folder, by default **C:\Program Files**

(x86)\Barracuda\ArchiveOne\Web\AOneSearch

1. Version 6 and earlier default location: **C:\inetpub\wwwroot\AOneSearch**
2. If you have installed the Search and Retrieval websites in a non-default location, you can browse to the **AOneSearch** content directory from IIS Manager:
    1. In IIS Manager, expand the ***Servername*** **> Sites > Default Web Site**, and click **AOneSearch**.
    2. In the central pane, click the **Content View** and then in the right-hand pane, click **Explore** from the **Actions** menu. This will open the directory in Explorer.

2. Make a copy of the **web.config** file; you can revert to the backup if required.
3. Open the **web.config** file in Notepad.
4. Locate the lines:
   <authentication mode=”Forms”>
   <forms loginUrl=”Login.aspx” name=”.C2CFORMSAUTH” timeout=”12345678″ protection=”All”></forms>
   </authentication>
   <authorization>
   <deny users=”?”></deny>
   </authorization>
   <identity impersonate=”false”></identity>
5. Replace the lines with:
   <authentication mode="Windows"/>
   <authorization>
   <deny users="?"></deny>
   <allow users="*"/>
   </authorization>
   <identity impersonate="false"></identity>
6. Save and close the file.

Step 3. Change the Authentication Method

Complete the following on each identified web server:

1. In **IIS) Manager**, expand the **server name > Sites > Default Web Site**, and click **AOneSearch**.
2. If using *IIS version 7*, complete the following steps:
    1. In the center pane, double-click the **Authentication** icon.
    2. Right-click **Anonymous Authentication**, and click **Disable**.
    3. Right-click **Forms Authentication**, and click **Disable**.
    4. Right-click **Windows Authentication**, and click **Enable**.
    5. In the right pane, click **Advanced Settings**.
    6. Select **Enable Kernel-mode authentication**, and click **OK**.
    7. In the left pane, click **Application Pools**.
    8. In the center pane, right-click the **Archive One** application pool, and select **Recycle**.

3. If using *IIS version 6*, complete the following steps:
    1. Right-click **AOneSearch**, and click **Properties**.
    2. Click the **Directory Security** tab, and click **Edit**.
    3. Clear **Anonymous authentication**.
    4. Select **Windows Integrated Authentication**.
    5. In the left pane, expand **Application Pools**.
    6. Right-click the **Archive One** application pool, and click **Recycle**.

Step 4. Add the AOneSearch URL to the Local Intranet Zone in Internet Explorer

If you're logged into a domain, Microsoft Internet Explorer (IE) only allows integrated authentication to a website in the domain if the site name is not deemed to be external. If you connect to a web server using the machine name, you won't be challenged for a username/password. However if you use the Fully Qualified Domain Name (FQDN) or IP address, you will be challenged to authenticate. By adding the AOneSearch URL to the Local Intranet Zone in IE the FQDN will be considered part of the intranet, therefore trusted, and so your domain login will be honoured as authentication to the website. The addition of the FQDN or IP address for a server to the list of 'intranet' servers can be centralised so that it automatically applies to all users who log into a domain, using Group Policy. To apply the setting manually:

1. From the **Tools** menu, select **Internet options**.
2. On the **Security** tab, select **Local intranet** and then click **Sites**.
3. Click **Advanced**, then enter the required URL (for example, https://mail.barracuda.com) and click **Add**.
4. Click **Close** and click **OK** in all dialogs to save the configuration.