How to Resolve Users Receiving Authentication Prompts when Using Windows Authentication for AOneSearch Website

This article applies to Barracuda ArchiveOne version 6.5 or later.

The Archive search website (AOneSearch) can be configured with either forms-based or Windows integrated authentication. Windows integrated authentication may be preferable for users as they do not have to enter their credentials to log in to the Archive search website. If Windows integrated authentication is configured, but the user still receives a Windows dialog from the server prompting them to authenticate, confirm the configuration is correct.

Step 1. Ensure the AOneSearch URL is in the Local Intranet Zone

If you are logged in to 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 are not challenged for a username/password. However, if you use the Fully Qualified Domain Name (FQDN) or IP address, you are challenged to authenticate. By adding the AOneSearch URL to the Local Intranet Zone in IE, the FQDN is considered part of the intranet, and therefore trusted, so your domain login is honored as authentication to the website. The addition of the FQDN or IP address for a server to the list of intranet servers can be centralized so that it automatically applies to all users who log in to 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 click **Sites**.
3. Click **Advanced**, and enter the required URL, for example, https://mail.barracuda.com, and click **Add**.
4. Click **Close**, and **OK** in the remaining dialog boxes to save the configuration.

Step 2. Ensure Kernel Mode Authentication is Enabled on the Website

As the ArchiveOne Search & Retrieval websites component is commonly installed on web servers which host other applications (e.g. OWA), enabling Kernel mode authentication allows for multiple application pools which run under different identities to use Windows integrated authentication (for more information see the MSDN blog IIS 7 and Kernel mode authentication). To check Kernel mode is enabled:

1. On each web server, open **IIS Manager**.
2. Browse to the **AOneSearch** website under **Default Web Site**.
3. Double-click **Authentication** in the **Features View**.
4. Select **Windows Authentication**, and click **Advanced Settings** in the far right pane.
5. Ensure **Enable Kernel-mode authentication** is selected, and click **OK**.