Waters Knowledge Base

How to configure PMI BYOS on a workstation with waters connect 3.2.0 or later - wkb279493

OBJECTIVE or GOAL

Configure a API client on a waters_connect 3.2.0 (or later) workstation to allow Protein Metrics BYOS software on the same workstation to access files in the waters_connect database

ENVIRONMENT

- waters_connect 3.2.0
- waters_connect 3.3.0
- waters_connect 3.5.0
- waters_connect 3.6.0
- waters_connect 3.7.0
- Protein Metrics BYOS v4.0 or later

PROCEDURE

1. **A - Before you start**
2. Install waters_connect (Services, waters_connect Hub server etc.) as described in the relevant installation or migration guide. Installing the base kit automatically installs the API alongside the other platform services, and enables TLS for the API.
3. Ask customer's IT dept to confirm that the following ports on the waters_connect Workstation PC are not blocked : 44312, 48505, 48333,
4. Ensure that the waters_connect UNIFI API service is running.
5. Ensure that the PC user account used to configure the client has the following user rights
    - Windows Administrator privileges
    - waters_connect user account contains the "Administrator" role

B - Configure an API Client for BYOS using waters_connect API Application Client Registration Tool

When you install waters_connect base kit the **ApplicationRegistrationTool.app.exe is** installed in this folder: *<install drive>*:\Program Files\Waters\waters_connect\ApplicationRegistrationTool\. This command line application is used to configure the API client that allows the BYOS file browser to see the contents of the Oracle database.

NOTE : Some other versions of UNIFI or waters_connect use a graphical user interface (GUI) to configure the API

client. Command line looks less user friendly, but if you follow the steps precisely it is no more complicated than the GUI procedure

1. On the waters_connect workstation navigate to C:\Program Files\Waters\waters_connect\ ApplicationRegistrationTool\
2. Right-click **ApplicationRegistrationTool.app** executable (ApplicationRegistrationTool.App.exe) and select **Run as administrator :**
   - **Result:** A console window opens.
   - If no console window opens see wkb202576
3. Type your *waters_connect username* and press ENTER.
4. Type your *waters_connect password* and press ENTER
   - **Result:** A summary page displays any previously registered third party applications, and asking you what you want to do next
5. Type R to register a client, and press Enter.
6. At “Please provide a name for the application client in Identity Server 4”, type a **Client name** and press ENTER.
   - IMPORTANT : Make a note of this, you will need it in Step 4 of ‘Configure BYOS’. For example, if you type *ByosClient* this sets **ClientName** and **ClientId** to *ByosClient*.
7. At "Please provide a flow for the application” type ***A*** and press ENTER. This specifies “Authorization code”.
8. It will ask you to "Provide a requiredPKCE value for the application (false or true):" Type *false* and press ENTER
9. It will the ask you to provide an access token. Type R for reference token and press return.

10. At “Please provide the RedirectUri(s) for the application. How many URIs do you need to define?:” type ***1*** and press ENTER
11. At “Please provide the RedirectUri with the index 0” type *http://localhost:44312/callback* and press ENTER
    - TIP : See Addition Information section for further details of redirectUri port settings..
12. At “Please provide the PostLogoutRedirectUri(s) for the application. How many URIs do you need to define?:” Type *1* and press ENTER.
13. At “Please provide the PostLogoutRedirectUri with the index 0” Type *http://localhost:44312/callback* and press ENTER.
    - NOTE : This is the same entry as for step 9. This is not an error. You must enter this same information a second time for the postlogoutredirecturi.
14. At “Please provide a secret for the application” type the secret **(f**or example "ByosSecret") and press ENTER. Make a note of this as what you set in the public API command line interface will later have to be entered in step ‘3 – Advanced’ of ‘Configure BYOS’.
    - TIP : It is recommended, but not required, to set this entry per customer’s security standards.
15. Default timeout values are as shown below. The numbers are time in seconds.
    - AbsoluteRefreshTokenLifetime is: 2592000
    - SlidingRefreshTokenLifetime is: 1296000
    - AccessTokenLifetime is: 3600
    - AuthorizationCodeLifetime is: 300
    - IdentityTokenLifetime is : 360

The AccessTokenLifetime should be increased from 3600s (1 hour) to 86400s (24 hours) as follows

1. Navigate to the default installation folder c:\Program Files\Waters\waters_connect\ApplicationRegistrationTool\
2. Right click on the config file file called *app.config* and select Open With > Notepad
3. For the "AccessTokenLifetime" replace 3600 with 86400
4. Save the edited file

C - Configure Byos v4.0 and later

NOTE : Where the Protein Metrics interface says “server” it means the waters_connect identity server software, i.e. the part of waters_connect that controls user log in. In the version below ‘identity server’ has been specified in places

1. On the processing PC open BYOS
2. In the menu bar select **Server** and from the drop down select **Configure**
   - **RESULT:** The Basic settings for BYOS server open
3. In Servers Configuration>UNIFI
   - Ensure that **Enabled** is ticked
   - In the Server field enter the address for the waters_connect identity server. By default this will be *https://localhost:48505/v1/unifi*
   - In the Download Path field type *C:\Protein Metrics\UNIFI*
   - For waters_connect 3.2.0 or later do not enter the waters_connect Username and Password. Instead these will be entered in the BYOS file browser when the user prompted to do so
4. Click on the Advanced option
   - In both the Client id and Client secret fields enter the name chosen at step 6 of **Configure a Client for BYOS using waters_connect API 2.0 Application Client Registration Tool**
   - In the Authorization Endpoint field type : *https://localhost:48333/connect/authorize*
   - In the Token Endpoint field type *https://localhost:48333/connect/token*
   - In the Scope field type *webapi*
5. Click **OK** to complete the configuration

D - Access the waters_connect UNIFI database from Byos

This section is completed by the customer.

1. In BYOS, select the workflow appropriate for the type of analysis to be completed. This could be from either the default “System Workflows” or customized “My Workflows” sets. In the **Samples** tab of the Project Creation dialog, the **Add UNIFI sample(s)** button is available:
2. Click **Add UNIFI sample(s)**. Note that because the Username and Password for the Waters UNIFI user account were not added during the **Configure UNIFI in Byos** section, the user will be prompted to enter these in a browser that will open. Once entered, the **Select UNIFI sample** dialog opens:
3. Navigate to and select the folder of interest in the left panel. The data associated with that folder then opens in the right panel. Two types of data can be loaded into Byos: **SampleResult** and **Analysis**. Only records that are applicable to Byos are displayed. If an Analysis record is selected, all the associated SampleResult records are