

August 2023

**Keywords or phrases:**

Biobrain® Supervise, Software, SCADA, OPC UA, Products Powered by Biobrain®

# Connecting Biobrain® Supervise to Products Powered by Biobrain® via OPC Unified Architecture (UA)

Cyril Mak\*, Dr. Christian Endres, Alexander Skrypzinski

Sartorius Stedim Biotech GmbH, August-Spindler-Strasse 11, 37079 Goettingen

\* Correspondence

Email: [bioprocess.support@sartorius.com](mailto:bioprocess.support@sartorius.com)

## Abstract

Since version 4.9, Biobrain® Supervise has provided a simple way to connect Biobrain® powered devices via the built-in OPC UA client, which enables different instruments or systems that provide OPC Unified Architecture (UA) servers to be connected securely.

This application note provides step-by-step guidance for establishing a secure connection between Biobrain® Supervise and products powered by Biobrain® using OPC UA to allow supervisory control and data acquisition.

## Introduction

Biobrain® Supervise is a Supervisory Control and Data Acquisition (SCADA) system. An OPC Unified Architecture (UA) client was introduced in Biobrain® Supervise 4.9, allowing the software to easily connect to the OPC UA server of Biobrain® devices.

Products powered by the Biobrain® automation platform are engineered to allow rapid adaption of a biomanufacturing facility to address ever-changing requirements. Among its several practical features, it provides an OPC UA server to enable connections to other SCADA, Distributed Control System (DCS), or historian systems.

OPC Unified Architecture (OPC UA) is an open standard communication protocol for industrial automation developed by the OPC Foundation. It is manufacturer-independent and can be used for different kinds of data exchange (machine to machine, machine to PC, PC to PC).

The following instructions are exemplary for Biostat® STR Generation 3 and they are applicable for all products powered by Biobrain®.

## Prerequisites

Ensure that the Biobrain® Supervise system running version 4.9 or newer with a licensed OPC UA client module and the Biobrain® device is connected to the same network. In the context of this application note, it is required that the Biobrain® device is configured for local user management and use a static IP address. It is assumed that both systems use self-signed OPC UA application certificates default configuration for both systems. Traffic via TCP port 4840, as used by the OPC UA server, must be permitted by the respective firewalls.

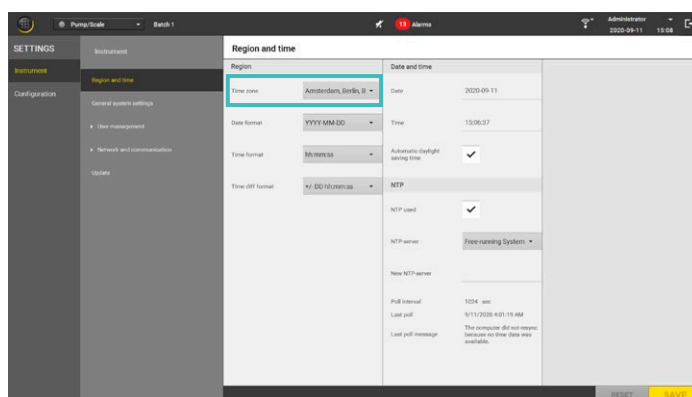
## Biobrain® Device Configuration

### Step 1: Verify the Time Zone Is Correct

Log in to the Biobrain® device using an account with administrative privileges. Open the “Region and time” section located in the Instrument settings of the device administration interface.

Verify that the currently selected “Time zone” (figure 1) matches the actual time zone of the instrument’s installation location. If the time zone is not set correctly, change it to the appropriate setting and click SAVE.

After changing the instrument’s time zone, create a new self-signed X.509 application certificate for the OPC UA server using the built-in function of the Biobrain® device. Open the “OPC settings” located under “Network and communication” in the Instrument settings. Click the “UPDATE CERTIFICATE” button to create an updated certificate (figure 3).



**Figure 1:** Time Zone Configuration in the “Region and Time” Settings of the Biobrain® Device (Here Biostat STR® Generation 3)

Step 2: Determine the OPC UA Server Endpoint URL

To determine the Biobrain® device OPC UA server’s endpoint URL, open the “Network settings” in the “Network and communication” section of the Instrument settings (figure 2).

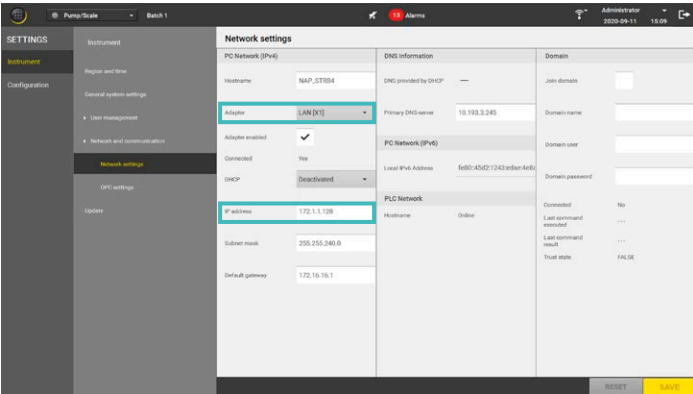


Figure 2: Determination of the IP Address of the Biobrain® Device (Here Biostat STR® Generation 3)

Identify and take note of the IP address of the adapter “LAN [X1]” See Table 1 for the server address.

OPC UA server address	<IP address>:4840 e.g., 172.1.1.128:4840
-----------------------	---

Table 1: Format of the Biobrain® Device’ IP Address and Port

Step 3: Configure the OPC UA Server

The configuration of the bioreactors OPC UA server can be modified in the “OPC settings” located in the “Network and communication” section of the linstrument settings (figure 3).

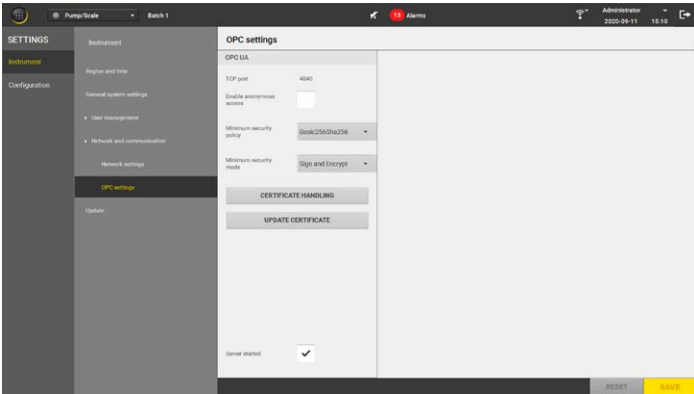


Figure 3: Default Configuration of the OPC UA Server

It is recommended to only allow secure client connections to the OPC UA server by applying the most secure profile. “Anonymous access” should be disabled to prevent unauthorized access to the OPC UA server.

The “Minimum security mode” should be set to “Sign and Encrypt,” enforcing authentication at the application level. Digital signatures ensure the integrity and authenticity of communication messages exchanged and encryption prevents eavesdropping. The security policy defines the algorithm and key length used to sign and/or encrypt messages exchanged. We suggest that you set the “Minimum security policy” to “Basic256Sha256.”

Ensure that the server is started by activating the checkbox next to “Server started.”

Save any changes made by clicking the SAVE button. Table 2 summarizes the default settings of the OPC UA server that coincide with the recommendations made above.

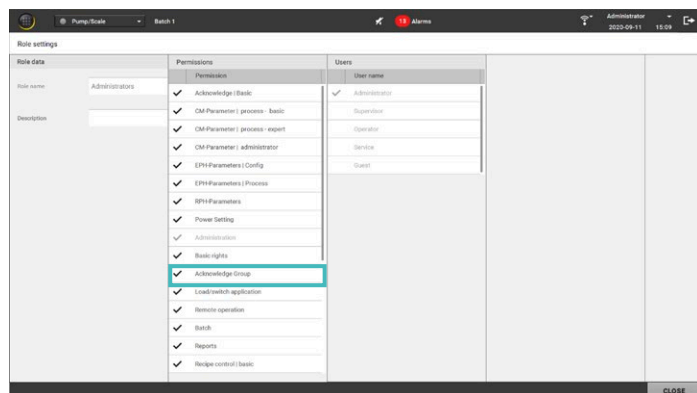
Function	Setting
Enable anonymous access	Deactivated
Minimum security policy	Basic256Sha256
Minimum security mode	Sign and Encrypt
Server started	Activated

Table 2: Default Configuration Settings of the OPC UA Server

# Biobrain® Supervise Configuration

## Step 4: Grant Access Permissions for the OPC UA Server

The Biobrain® device OPC UA server of products powered by Biobrain® supports user authentication with built-in user management. Any user assigned to a security role for which “Remote operation” permission is granted can establish a client session to the OPC UA server. Permissions for security roles can be granted or revoked under “Roles” located in the “User management” section of the Instrument settings (figure 4).



**Figure 4:** “Remote Operation” Permission Granted for the “Administrators” Security Role

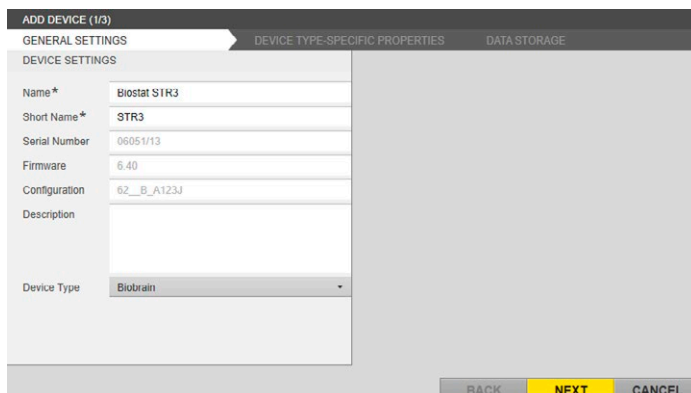
By default, this permission is granted to the security roles and users listed in Table 3.

Security Role	User
Administrators	Administrator
Supervisors	Supervisor

**Table 3:** Security Roles and Users With the “Remote Operation” Permission Set as Default

## Step 1: Configure a Device to Connect to Products Powered by Biobrain®

Open Biobrain® Supervise and create a new device by activating the “Add device” functionality located under “Devices” in the administration interface. In the GENERAL SETTINGS tab of the opened ADD DEVICE dialog, enter a “Name” (e.g., “Biostat STR3”) and a “Short Name” (e.g., “STR3”) for the new device. For the “Device Type,” select “Biobrain” (figure 5). Continue by clicking NEXT.



**Figure 5:** General Configuration Settings of an OPC UA Device in Biobrain® Supervise

In the DEVICE TYPE-SPECIFIC PROPERTIES tab (figure 6), configure the appropriate TIMING SETTINGS (e.g., “Polling rate:” “5000 ms;,” “Max. retries:” “3;,” “Reconnect rate” “15 s).

Under CONNECTION SETTINGS enter the IP address and port of the OPC UA server determined earlier (e.g., 172.1.1.128:4840). Select “Sign and Encrypt” as the “Security mode” and “Basic256Sha256” as the “Security policy.”

Select “Username” as the “Authentication mode” and enter the username and password for the Biobrain® device user who has “Remote operation” permissions such as an administrator by default, the administrator account has no password).

Under SECURITY CHECK OVERRIDES leave “Accept expired certificates” deactivated and ensure that the “Disable hostname check” checkbox is activated.

**Figure 6:** *DEVICE TYPE-SPECIFIC PROPERTIES* During the Configuration of an OPC UA Device in Biobrain® Supervise With “Test Connection” Highlighted

Table 4 lists all necessary settings to connect Biobrain® Supervise to the default configuration of a OPC UA server.

Remain on this configuration tab to initiate the exchange of OPC UA certificates as described in the following sections of this technical note.

Parameter	Setting
CONNECTION SETTINGS	
Device address (OPC UA server)	<IP address of Biobrain® device OPC UA server>:4840
Security mode	Sign and Encrypt
Security policy	Basic256Sha256
AUTHENTICATION	
Authentication mode	Username
Username	administrator
Password	<no password>
SECURITY CHECK OVERRIDES	
Accept expired certificates	Deactivated
Disable hostname check	Activated

**Table 4:** *Connection and Authentication Settings for a Biobrain® Supervise Device to Connect to Biobrain® Device Using the Default Configuration*

## Step 2: Exchange Certificates And Establish the OPC UA Connection

When a connection between Biobrain® Supervise and the Biobrain® device is first established, an application certificate will be sent from the OPC UA server of the Biobrain® devices to the Biobrain® Supervise OPC UA client, and vice versa. Both certificates need to be trusted on either side to allow a secure connection.

### Step 2.1: Trust the Server Certificate

To initiate the certificate exchange, activate the “Test connection” button in the CONNECTION SETTINGS configuration dialog (figure 6) of Biobrain® Supervise. The Biobrain® device OPC UA server will send its application certificate to Biobrain® Supervise. The connection test will fail as Biobrain® Supervise does not yet trust the application certificate of the OPC UA server. Acknowledge the connection test result.

Open the Windows Explorer of the Biobrain® Supervise system and navigate to the folder location shown in Table 5. Cut and paste the certificate file of the Biobrain® device OPC UA server from the “rejected” folder into the “trusted” folder (Table 5).

<b>Rejected Certificates</b>
%ProgramData%\Sartorius\Biobrain® Supervise\Services\OpcUa\Client\pki\rejected\certs
<b>Trusted Certificates</b>
%ProgramData%\Sartorius\Biobrain® Supervise\Services\OpcUa\Client\pki\trusted\certs
<b>Certificate File of the Biobrain® Device OPC UA Server</b>
Sartorius BIOBRAIN OPC Server [<Thumbprint>].der

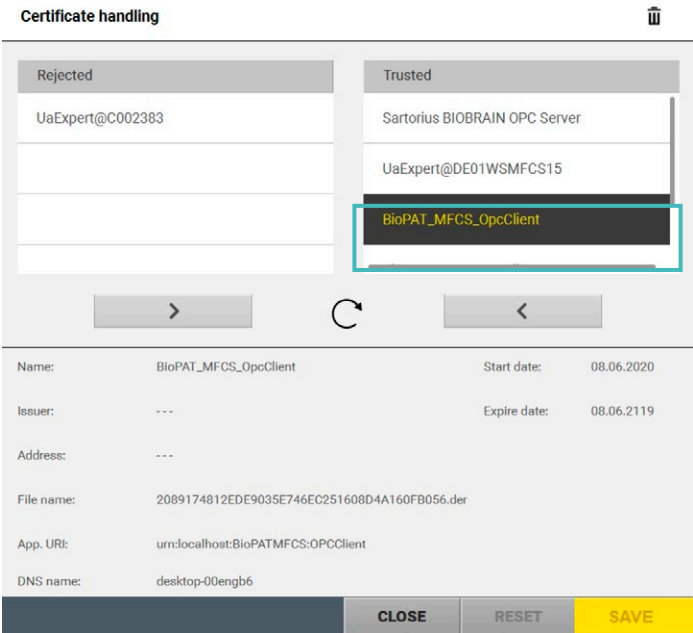
**Table 5:** *Folder Locations for Rejected and Trusted Biobrain® Supervise Certificates and File Name Structure of OPC UA Server Application Certificates*

**Step 2.2: Trust the Biobrain® Supervise Client Certificate**

Return to Biobrain® Supervise and execute “Test connection” again (figure 6). The connection test will fail again as the OPC UA server does not yet trust the application certificate of the Biobrain® Supervise client. Acknowledge the connection test result.

In the Human Machine Interface (HMI) of the Biobrain® device, go to the “OPC settings” located in the “Network and communication” section of the Instrument settings (figure 3). Open “Certificate handling” (figure 7).

Trust the Biobrain® Supervise client certificate “BioPAT\_MFCS\_OpcClient” by moving it from the “Rejected” column to the “Trusted” column and click SAVE.



**Figure 7:** Certificate Handling for the OPC UA Server of a Biobrain® Device

**Step 2.3: Verify the Correct Connection Settings**

Return to Biobrain® Supervise and execute “Test connection” once more (figure 6).

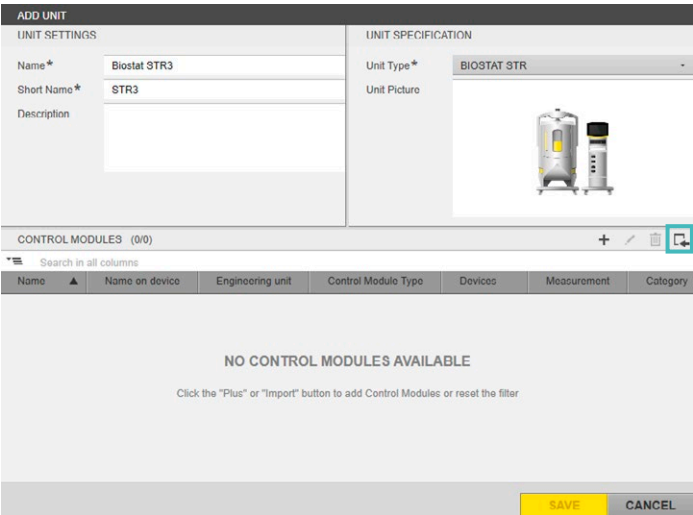
The connection test will now pass as all necessary application certificates are trusted on both the client and server sides (figure 8). Acknowledge the connection test result and continue configuring the device. Finally, add the newly created device by clicking SAVE.



**Figure 8:** Successful Connection Test in Biobrain® Supervise After Trusting All Necessary Application Certificates

**Step 3: Configure a Biobrain® Device Unit in Biobrain® Supervise**

Create a new unit by activating the “Add unit” functionality located under “Units” in the administration section. In the ADD UNIT dialog, enter a “Name” (e.g., “Biostat STR3”) and a “Short Name” (e.g., “STR3”) for the new unit. Click on the “Import Control Modules” button (figure 9).



**Figure 9:** ADD UNIT Dialog in Biobrain® Supervise With “Import Control Modules” Functionality Highlighted

In the following “Import Control Modules” dialog, select the newly created device for the Biobrain® device (e.g., “Biostat STR3”) and click NEXT.

Load the XML configuration file provided with the product powered by Biobrain® and click NEXT to continue.

Select the appropriate instrument configuration specified in the configuration file (e.g., “STR3\_010008\_B1\_BI010000”) and click NEXT to continue.

In the control module selection, select all control modules and finish the import by clicking OK. Save the new unit by clicking SAVE in the “Add unit” dialog.

## Results

By completion of this step-by-step guide, a secure connection between Biobrain® Supervise and the Biobrain® device was successfully configured and established. Biobrain® Supervise is ready to be used for supervisory control and data acquisition of the connected products powered by Biobrain®.

## Conclusion

This application note outlines how to successfully connect products powered by Biobrain® with Biobrain® Supervise software via OPC UA so it can be conveniently used for supervisory control and data acquisition.

The OPC client functionality of Biobrain® Supervise, leveraging the UA protocol and advanced setting options, offers a flexible and secure way of integrating products powered by Biobrain® into Biobrain® Supervise systems using a standardized communication protocol.


Consequently, users can extend the capabilities of a Biobrain® device with the complete set of functionalities offered by Biobrain® Supervise.

## Germany

Sartorius Stedim Biotech GmbH  
August-Spindler-Strasse 11  
37079 Goettingen  
Phone +49 551 308 0

## USA

Sartorius Stedim North America Inc.  
565 Johnson Avenue  
Bohemia, NY 11716  
Toll-Free +1 800 368 7178

 For further contacts, visit  
[www.sartorius.com](http://www.sartorius.com)