



RTMC Pro and CSI Web Server

Troubleshooting Guide

Table of contents

1. Introduction	1
2. Symptoms	2
2.1 Data in published project does not display	2
2.2 Variable font sizes on RTMC components	3
2.3 Publishing issues	4
2.3.1 The publish button has no effect	4
2.3.2 Publish failure: Authorization required	5
2.4 My published webpage cannot be reached	6
2.5 RTMC Run-time crashes frequently	6
2.6 RTMC webpage shows blank screen(s) and/or only tabs	7
2.7 Web service keeps crashing	7
2.8 Web service does not start	7
2.9 Microsoft IIS comes up instead of published webpage	8
2.10 TLS certificates and key errors	8
3. Troubleshooting steps	12
3.1 Checking RTMC data sources	13
3.1.1 Verifying the data source	13
3.1.2 Checking individual data source links	19
3.1.3 Verifying LoggerNet scheduled collection is turned on	23
3.2 Checking for broken formulas	26
3.3 Updating RTMC Pro	27
3.3.1 Updating RTMC Development or Run-time without RTMC Pro	27
3.4 Verifying the project was published as a PC website	28
3.5 Disabling or removing IIS	29
3.6 Assigning the CSI Web Server to run on a different port	32
3.7 Restarting the CSI Web Server service in Windows	34
3.8 Adjusting restart and recovery properties in Windows	35
3.9 Adjusting CSI Web Server permissions	37
3.10 Verifying CSI Web Server and data logger permissions	39
3.11 Finding CSI Web Server log files	43
3.12 Verifying TLS certificate and key location	44
3.13 Verifying TLS certificate and key format	45

1. Introduction

This troubleshooting guide is designed to help users diagnose and resolve common issues encountered when working with RTMC Pro and the CSI Web Server. It covers symptoms, potential causes, and step-by-step corrective actions for data display, publishing, connectivity, and web service problems. Each section provides clear guidance to restore proper operation and improve system reliability.


For best results, begin by identifying the symptom that matches your issue, then follow the linked troubleshooting steps. If problems persist after completing these procedures, contact Campbell Scientific Support for further assistance.

2. Symptoms

This section describes the symptoms or issues you may see while working with RTMC Pro and the CSI Web Server. Each symptom links you to steps you may take to resolve the issue.

2.1 Data in published project does not display	2
2.2 Variable font sizes on RTMC components	3
2.3 Publishing issues	4
2.3.1 The publish button has no effect	4
2.3.2 Publish failure: Authorization required	5
2.4 My published webpage cannot be reached	6
2.5 RTMC Run-time crashes frequently	6
2.6 RTMC webpage shows blank screen(s) and/or only tabs	7
2.7 Web service keeps crashing	7
2.8 Web service does not start	7
2.9 Microsoft IIS comes up instead of published webpage	8
2.10 TLS certificates and key errors	8

2.1 Data in published project does not display

If your RTMC screens show the  in the upper right of all or some of the components in the project, there is a problem pulling the data to display in the project. If you see this on all objects in your project, perform the steps in [Verifying the data source](#) (p. 13), [Verifying LoggerNet scheduled collection is turned on](#) (p. 23), and [Verifying the project was published as a PC website](#) (p. 28).

If you see this only on some objects and not others, start by verifying the individual data source links in [Checking individual data source links](#) (p. 19), then perform the steps in [Verifying the data source](#) (p. 13), [Verifying LoggerNet scheduled collection is turned on](#) (p. 23), and [Verifying the project was published as a PC website](#) (p. 28).

When verifying the data source, keep in mind the location of the webpage you are publishing and the source of data. Can the two talk to one another?

If you are publishing the webpage on a computer using LoggerNet as a data source, but the two computers are on separate networks, expect that the data will be unavailable to be populated. If the data source is from a data logger, via its built in HTTP server, and the data logger IP address isn't reachable from the computer hosting the published page on the CSI Web Server, data will be unable to display. If you are publishing a project on a data logger that uses LoggerNet as a data source, the data will never display. A project published to a data logger can only use the data logger itself as a data source.

2.2 Variable font sizes on RTMC components

If you notice inconsistencies in the font sizes of different RTMC components, the first thing to do is ensure you are running the latest version of RTMC. Start by performing the steps in [Updating RTMC Pro](#) (p. 27) or [Updating RTMC Development or Run-time without RTMC Pro](#) (p. 27).

Running the latest version of RTMC reduces these issues significantly.

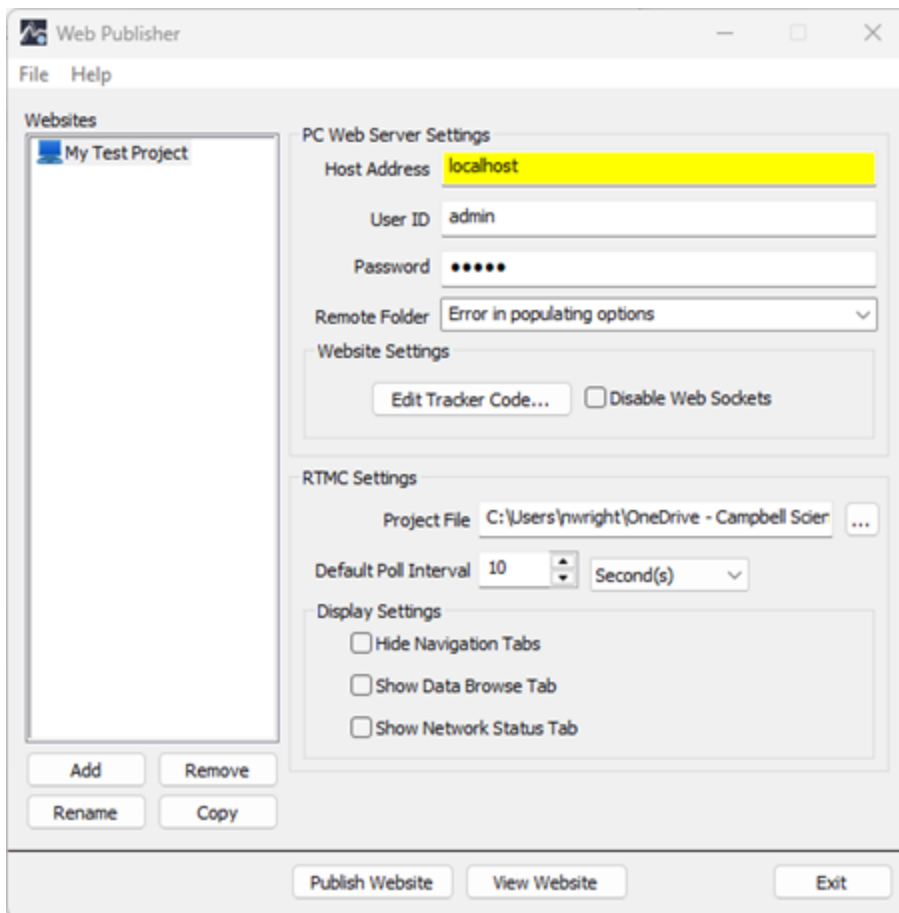
Further variances in font size can be due to the size of the individual components they belong to. When the size of an RTMC component is smaller than normal, RTMC will attempt to scale the font in order to avoid cutting parts off. To address the sizing issue, adjust the size of the component to unscale the font.

2.3 Publishing issues

2.3.1 The publish button has no effect

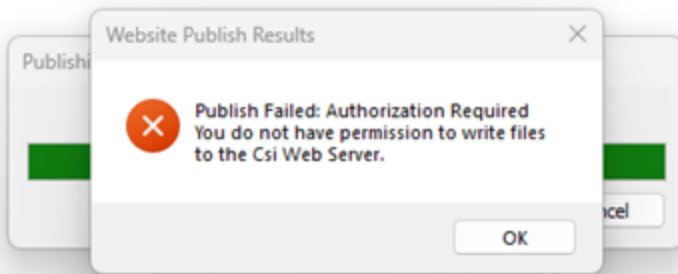
If clicking the **Publish Website** button for your RTMC project in the Web Publisher doesn't do anything, first verify the **Host Address** of the web server you are publishing to is correct.

Ensure the CSI Web Server is running and restart it, if necessary. See [Restarting the CSI Web Server service in Windows](#) (p. 34) for instructions on restarting the CSI Web Server service.



2.3.2 Publish failure: Authorization required

Sometimes you may get the error message "Publish Failed: Authorization Required" when you attempt to publish the RTMC project with the Web Publisher to the CSI Web Server or a data logger.

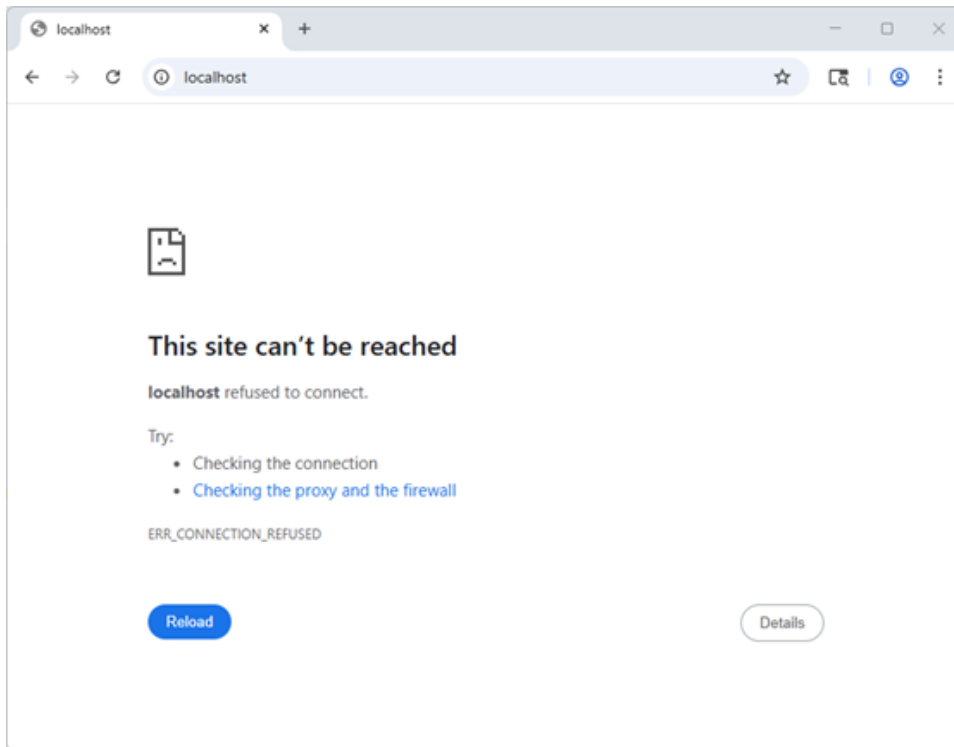


This issue is occurring because the username and/or password you are using on the web server isn't valid, or the username doesn't have permissions set correctly to enable access. To address this issue when publishing on the CSI Web Server, follow [Adjusting CSI Web Server permissions](#) (p. 37). To address this issue when publishing to a data logger, follow [Verifying CSI Web Server and data logger permissions](#) (p. 39).

2.4 My published webpage cannot be reached

If you attempt to visit the webpage hosted by the CSI Web Server and get an error like "This site can't be reached" or "Refused to connect," the web server may no longer be running.

Check to ensure the CSI Web Server is running and restart it, if necessary. See [Restarting the CSI Web Server service in Windows](#) (p. 34) for instructions on restarting the CSI Web Server service.



2.5 RTMC Run-time crashes frequently

If RTMC Run-time is crashing frequently, the first step is to update RTMC. Many crashing issues have been addressed in RTMC 5.02 and newer. Follow [Updating RTMC Pro](#) (p. 27) or [Updating RTMC Development or Run-time without RTMC Pro](#) (p. 27). Some crashes can also be due to issues with running RTMC Run-time in low memory environments. Some components can also crash RTMC. If you continue to experience frequent crashes after updating, report them to Campbell Scientific Support along with a copy of your RTMC project.

2.6 RTMC webpage shows blank screen(s) and/or only tabs

Blank page and tab issues have been addressed in RTMC 5.01 and newer. Update RTMC following [Updating RTMC Pro](#) (p. 27) or [Updating RTMC Development or Run-time without RTMC Pro](#) (p. 27). Then republish your RTMC project.

Some blank page or blank tab issues can be caused by webpage errors triggered by broken formulas in the expression builder. If you have already updated your RTMC to the most recent version and screens or tabs are still blank, look for formula issues in your RTMC project components using the expression builder, as described in [Checking for broken formulas](#) (p. 26).

2.7 Web service keeps crashing

If your CSI Web Server service keeps crashing repeatedly, first ensure you are running the latest version of RTMC Pro and CSI Web Server. If needed, follow [Updating RTMC Pro](#) (p. 27). Updating to the latest version can resolve many crashing issues.

Some crashing problems can be caused by an invalid TLS certificate or key failures. Refer to [Verifying TLS certificate and key location](#) (p. 44) and [Verifying TLS certificate and key format](#) (p. 45) to address TLS-related problems. If crashes persist, follow [Finding CSI Web Server log files](#) (p. 43) and contact Campbell Scientific Support to report the issue if necessary.

NOTE: AntiVirus Scans and some backup utilities can shut down the CSI Web Server. Create exceptions in those applications to ignore CSI Web Server directories as necessary.

2.8 Web service does not start

If publishing to the CSI Web Server fails or the CSI Web Server doesn't start, you may be experiencing a permissions issue. Permission issues might also present as an error message that indicates the service couldn't start because the associated account's credentials are incorrect, the password has expired, the account is locked, or it lacks necessary permissions like "Log on as a service." This typically means the CSI Web Server is not running under an account with the required user permissions.

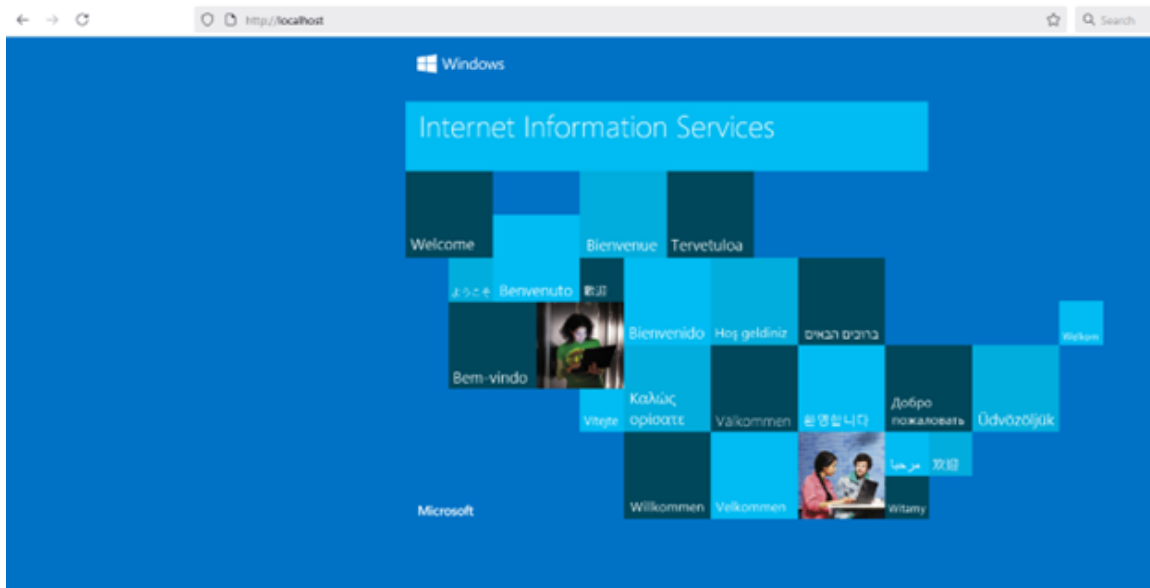
To address these issues see [Adjusting restart and recovery properties in Windows](#) (p. 35) and [Adjusting CSI Web Server permissions](#) (p. 37) and work with your local IT department as necessary.

2.9 Microsoft IIS comes up instead of published webpage

If your Web Publisher isn't working, displays a strange error, or a webpage hosted by the CSI Web Server encounters an error (like the one shown in the following image), it may be helpful to check whether your computer is experiencing a conflict with Microsoft's web server IIS (Internet Information Services).

To check if IIS is running on your computer, open a web browser and type either localhost or 127.0.0.1 into the address bar and press Enter. If a webpage similar to the following image appears, your computer or server is running Microsoft IIS.

To resolve this error and remove IIS, follow the instructions in [Disabling or removing IIS](#) (p. 29). If you are required to run IIS on your system, refer to the instructions in [Assigning the CSI Web Server to run on a different port](#) (p. 32) instead.



2.10 TLS certificates and key errors

a. Expired certificate

If the webpage being hosted by the CSI Web Server, or your data logger is secured with TLS and begins displaying a message like `NET::ERR_CERT_DATE_INVALID`, your TLS certificate is expired.

To resolve this issue, work with your IT department and/or your Certificate Authority to renew and update your certificate. Instructions for updating your certificate can be found in the CSI Web Server manual, Section 3.4 "Applying keys and certificates to CSI Web Server."



Your connection is not private

Attackers might be trying to steal your information from **yourwebsite.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_DATE_INVALID

Help improve security on the web for everyone by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

Similar browser errors may appear when viewing a webpage with a TLS certificate via localhost on the server where the project is published. This behavior is normal because the certificate for *www.yourwebsite.com* does not match the URL of the certificate.

b. NET::ERR_CERT_AUTHORITY_INVALID

This error may indicate you are using a self-signed certificate that does not reference a valid Certificate Authority. This is a certificate problem and can either be addressed by accepting the certificate in each browser that accesses the website on the computer or by working with your IT department to correct the certificate error.



Your connection isn't private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_AUTHORITY_INVALID

Advanced

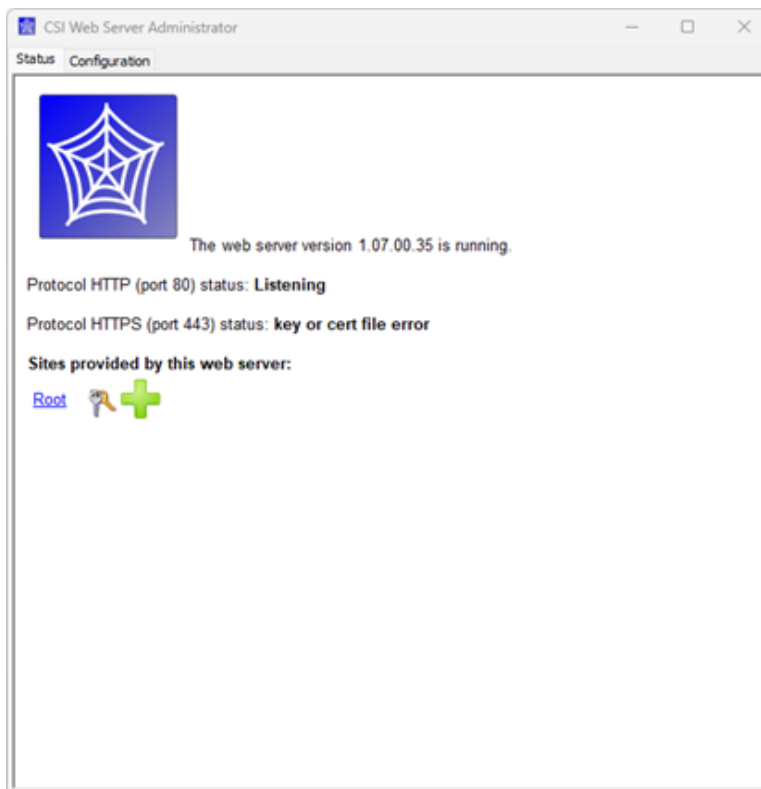
Go back

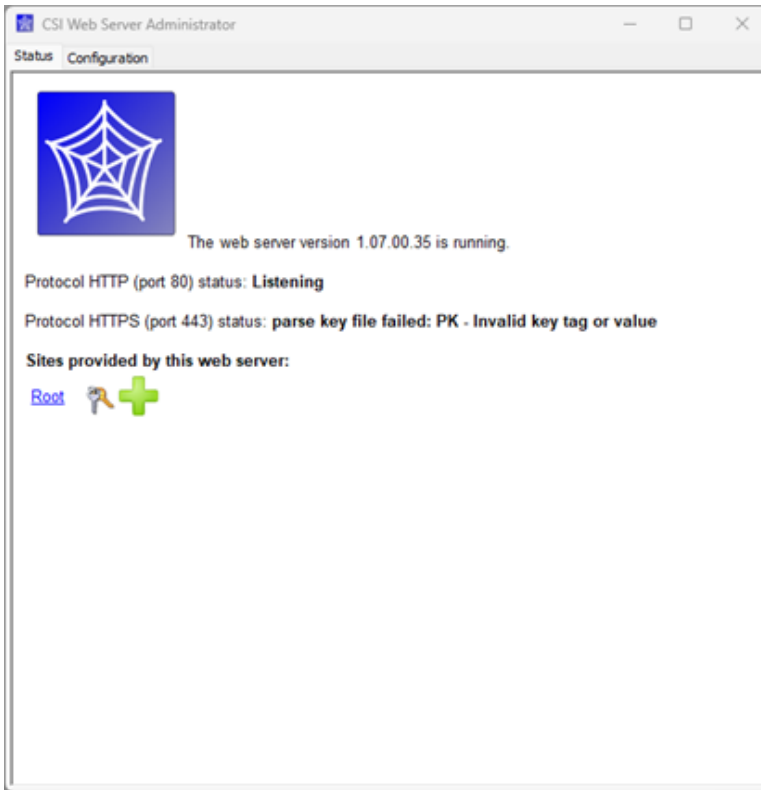
c. "Key or cert file error" or "Parse key file failed: PK – Invalid key tag or value"

When applying a TLS certificate and key in the CSI Web Server Administrator and restarting the web service, you may encounter error messages such as "Key or cert file error" or "Parse key file failed: PK – Invalid key tag or value." These errors typically indicate a problem with your certificate, the private key, or their file locations.

First, if your private key is password-protected, ensure the correct password has been entered in the CSI Web Server Administrator under the **Configuration** tab on the **HTTP** sub-tab. Then follow [Verifying TLS certificate and key location](#) (p. 44) and [Verifying TLS certificate and key format](#) (p. 45) to troubleshoot the issue.

You may have to work with your local IT department and/or the Certificate Authority that issued your certificate to resolve the problem.






3. Troubleshooting steps

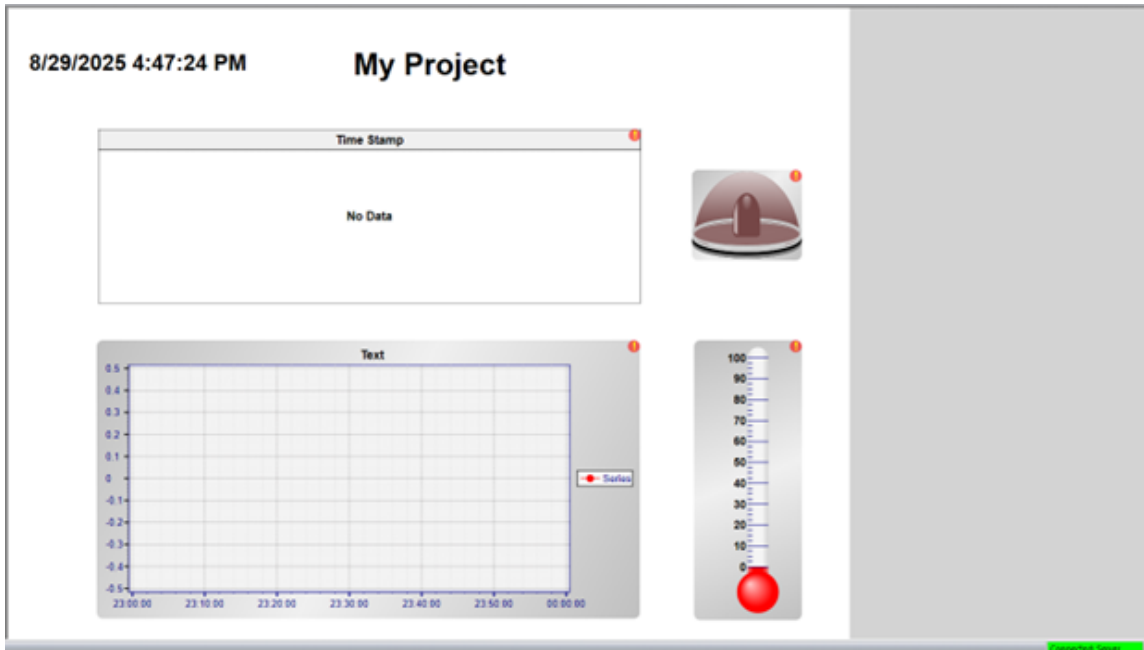
This section outlines the steps you may take to resolve the issues described in the previous section. That section includes links to the appropriate steps for each issue.

3.1 Checking RTMC data sources	13
3.1.1 Verifying the data source	13
3.1.2 Checking individual data source links	19
3.1.3 Verifying LoggerNet scheduled collection is turned on	23
3.2 Checking for broken formulas	26
3.3 Updating RTMC Pro	27
3.3.1 Updating RTMC Development or Run-time without RTMC Pro	27
3.4 Verifying the project was published as a PC website	28
3.5 Disabling or removing IIS	29
3.6 Assigning the CSI Web Server to run on a different port	32
3.7 Restarting the CSI Web Server service in Windows	34
3.8 Adjusting restart and recovery properties in Windows	35
3.9 Adjusting CSI Web Server permissions	37
3.10 Verifying CSI Web Server and data logger permissions	39
3.11 Finding CSI Web Server log files	43
3.12 Verifying TLS certificate and key location	44
3.13 Verifying TLS certificate and key format	45

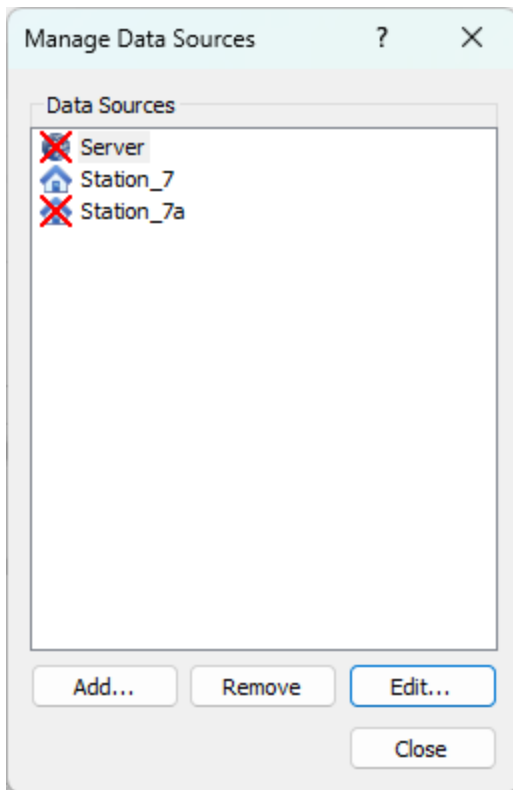
3.1 Checking RTMC data sources

3.1.1 Verifying the data source

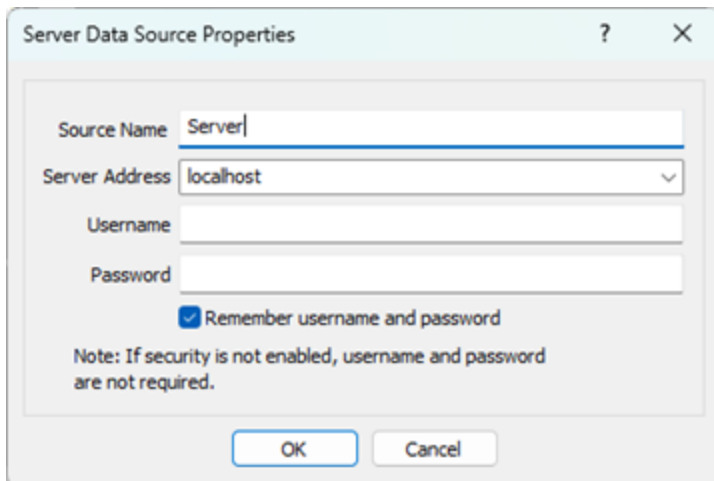
If your RTMC screens show the  in the upper right of the components in the project, there is a problem pulling the data to display in the project.



1. To verify the data source, open the project in RTMC Pro. On the **File** menu, navigate to **Project > Manage Data Sources**. Data sources unreachable from the computer running RTMC Pro are marked with a red X.



2. To correct the broken link, click **Edit** and update the connection information for the data source. The two most common data source types are 1) Server for a LoggerNet Server and 2) HTTP Datalogger Source. The **Edit** screen for a LoggerNet Data Source is below:

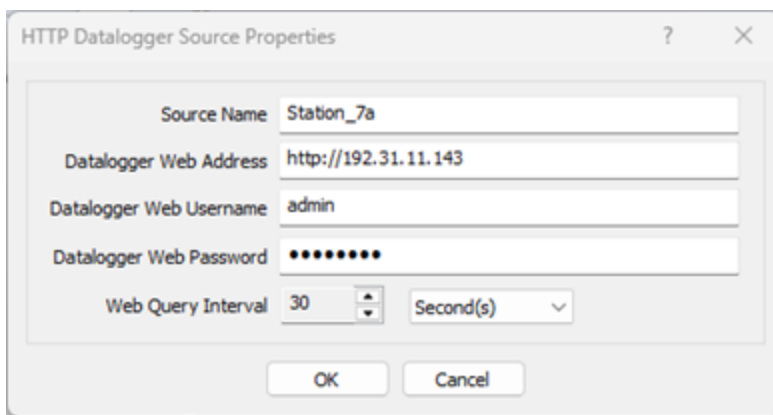


- a. Verify the **Server Address** is correct.
- b. If the project is being published as a webpage on the CSI Web Server running on a different computer than LoggerNet, you will need to use the IP address of the computer running LoggerNet instead of "localhost" for the **Server Address**.

If LoggerNet Security is enabled, you will also need to specify the **Username** and **Password** configured in the LoggerNet Security Manager. If you enter the username and password you use to log onto the computer, you are likely entering the wrong credentials. Since most users are not setting up a username and password in LoggerNet Security manager, it is common for both the **Username** and **Password** fields to be left blank.

- c. If the connection continues to fail, it can be helpful to work with your local IT department to verify a software or hardware firewall isn't blocking port 6789 to or on the computer running LoggerNet.

3. Here is the **Edit** screen for an HTTP Datalogger Source:



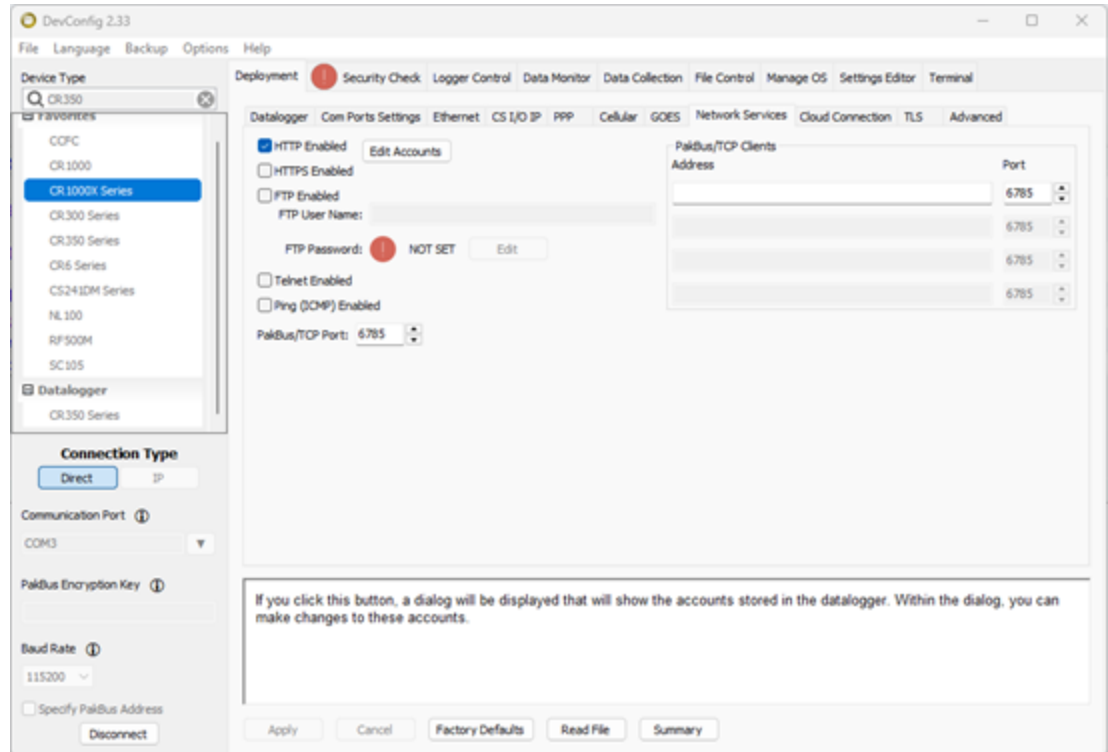
- a. Verify the IP address of the data logger is correct. If Ping is enabled in the data logger configuration, it can be useful to perform a Ping test from the computer running the RTMC project to verify the data logger is reachable. This is done from the command prompt of the Windows operating system by typing ping X.X.X.X, where the Xs are the IP address of the data logger.

NOTE: Another way to test is to open a web browser on the computer and enter the IP address of the data logger followed by :80. If you see the data logger internal webpage display, the connection is working.

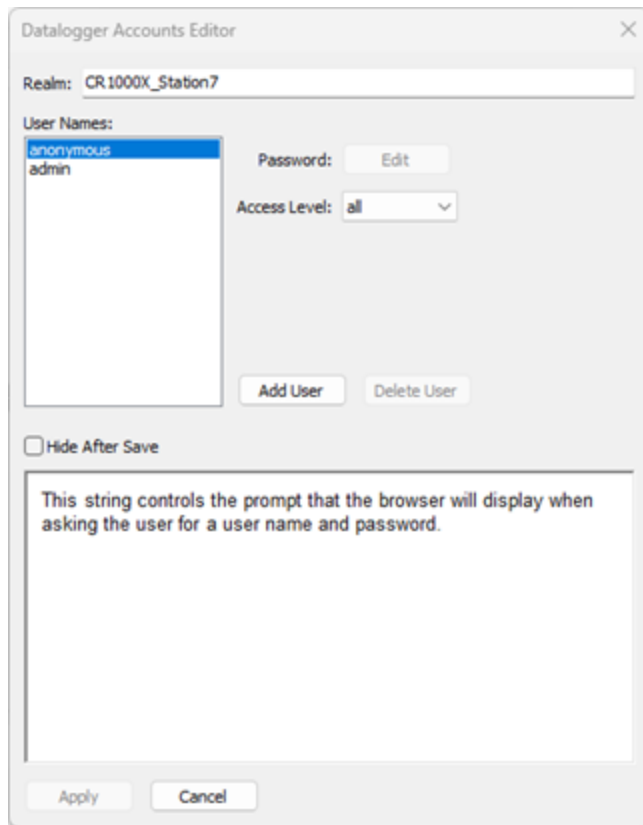
If the connection information appears accurate, you may need to work with your IT department to make sure you can reach the device over the network. Be sure to

verify the IP address, Subnet Mask, and Gateway Address of the data logger match the network connection indicated by your IT department.

- b. Ensure the **Username** and **Password** entered are the current username and password of the data logger HTTP service.
 - i. Connect to the data logger directly over USB or RS-232 using the Device Configuration Utility.
 - ii. Click the **Network Services** tab.

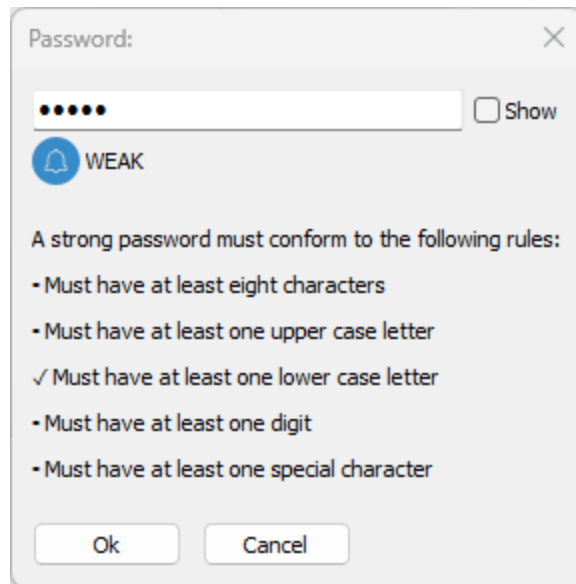


- iii. Verify the **HTTP Enabled** check box is selected (this enables the data logger HTTP data source) and click **Edit Accounts**.




- iv. From the **Datalogger Accounts Editor** window, verify the username being specified in your RTMC Pro data source is correct.

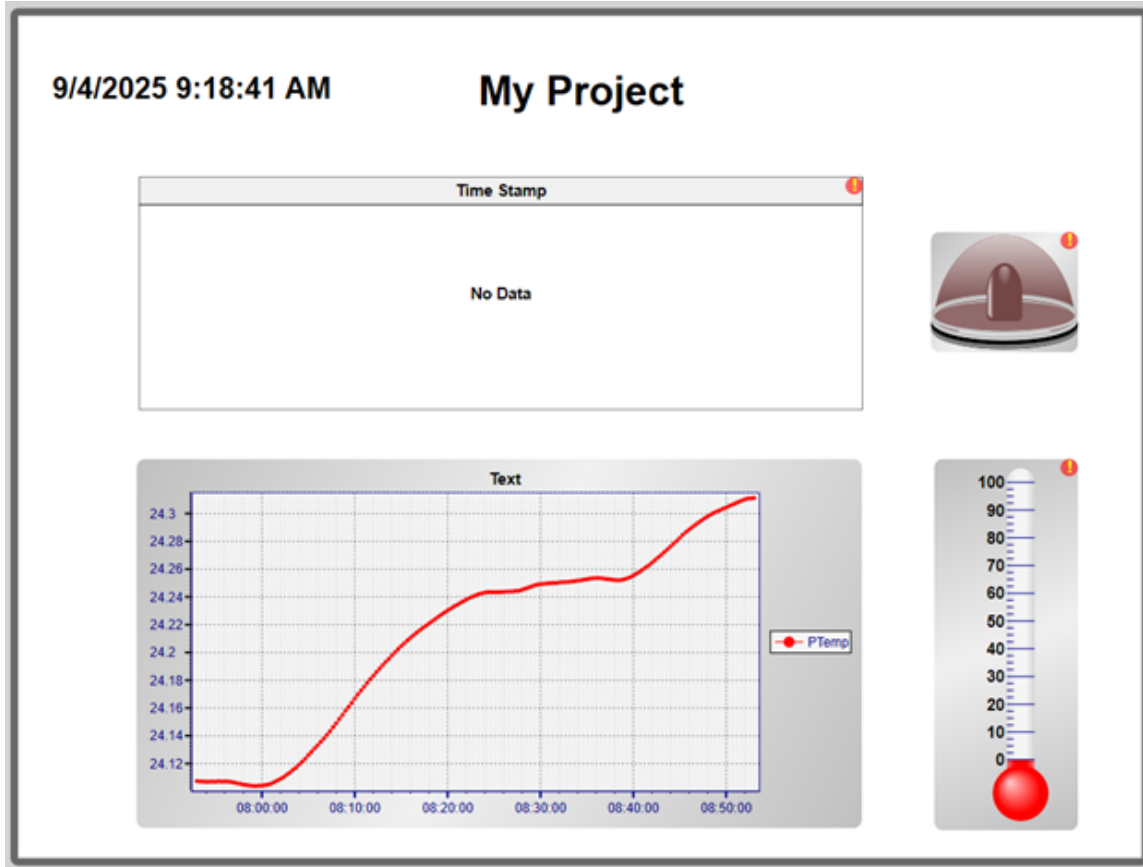
- v. Highlight the username and click **Edit** to verify the password is correct. (Click **Show** to make the password visible.)



- vi. If necessary, make changes and click **OK**.
- vii. If available, click **Apply** on the **Datalogger Accounts Editor** window.
- viii. If available, click **Apply** on the Device Configuration Utility **Network Services** tab screen.

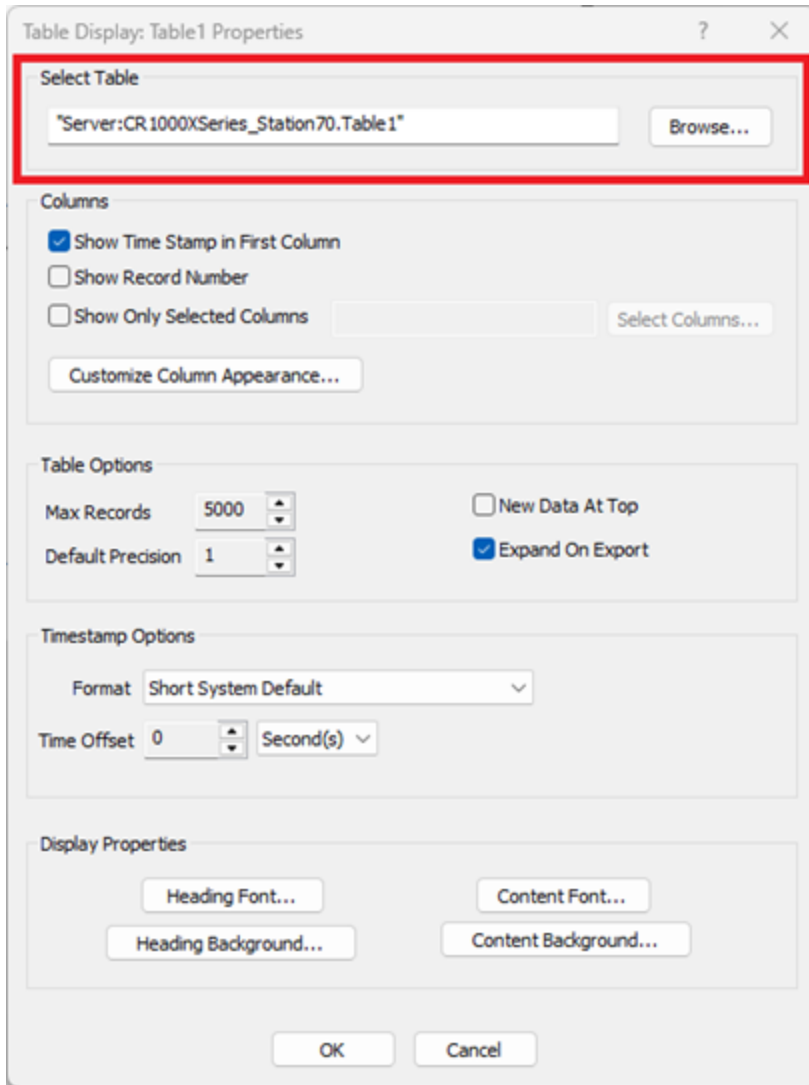
3.1.2 Checking individual data source links

After verifying your data source connections, verify the individual data source links of the components in your RTMC project are correct. This is particularly applicable when only some of the objects in your RTMC project are showing the  mark. Below is an image of a simple RTMC project with both working and broken data source links:

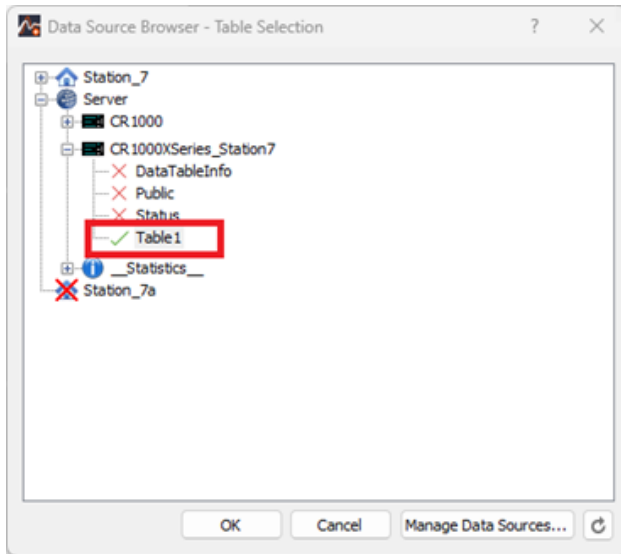


To fix the table component link in the top left:

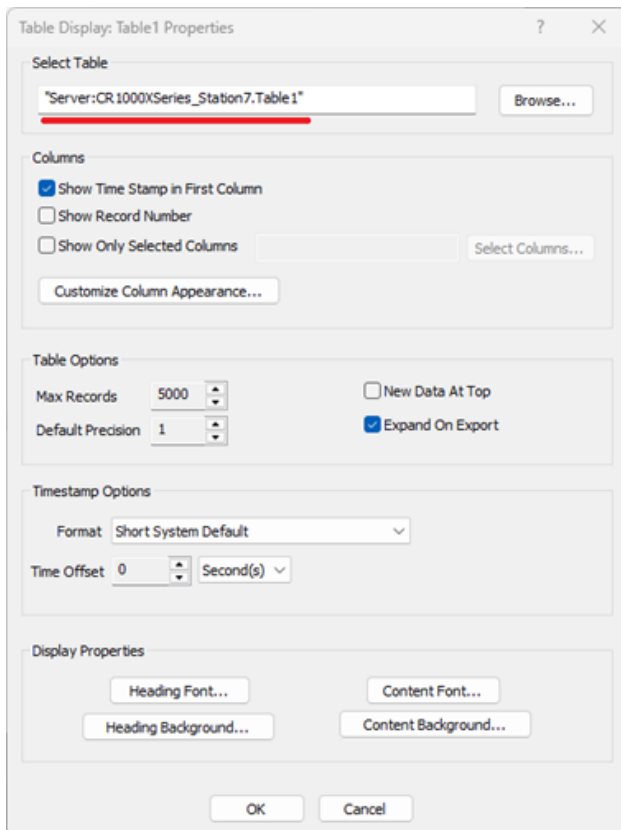
1. Right click the object and choose **Properties**.
2. Note the incorrect data source link. It has an extra 0 after the 7. To fix it click **Browse**.



3. On the **Data Source Browser – Table Selection** screen, select the correct data source and click **OK**.



4. Note the corrected data source link on the **Table Display: Table1 Properties** screen.

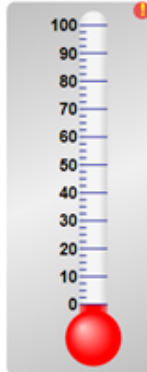
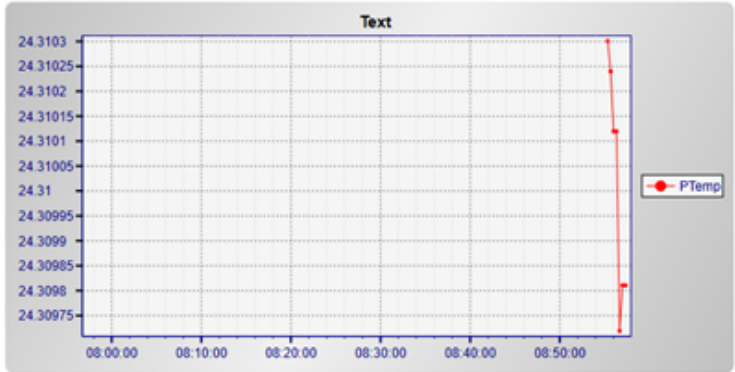



5. Click **OK**.

6. Note the object correctly displays data from the data source now.

9/4/2025 9:23:13 AM **My Project**

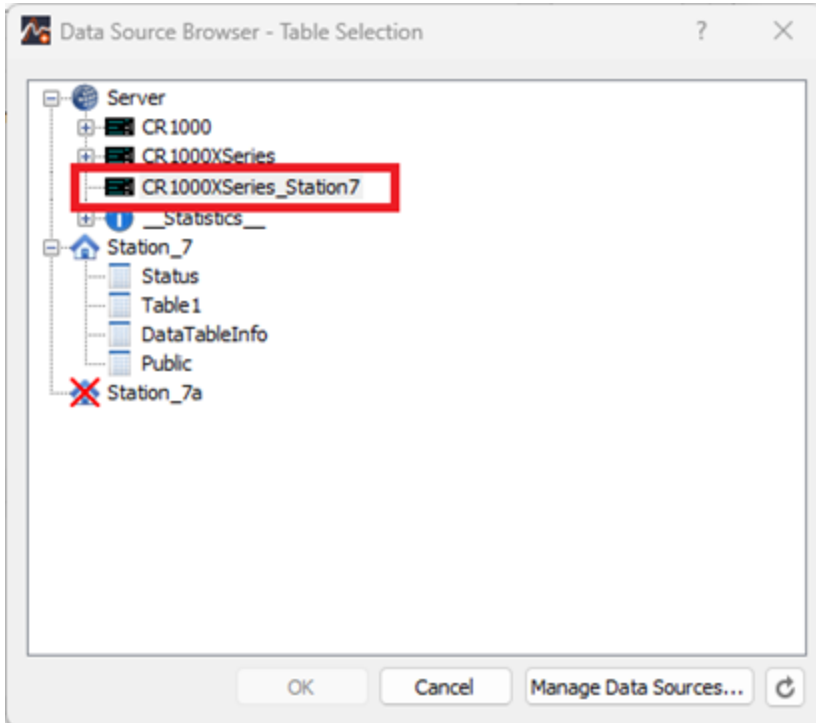
Time Stamp	CR1000XData(1)	CR1000XData(2)	CR1000XData(3)	CR1000XData(4)
4/2/2017 8:54:40 AM	0.0	0.0	0.0	0.0
4/2/2017 8:55:00 AM	0.0	0.0	0.0	0.0
4/2/2017 8:55:20 AM	0.0	0.0	0.0	0.0
4/2/2017 8:55:40 AM	0.0	0.0	0.0	0.0
4/2/2017 8:56:00 AM	0.0	0.0	0.0	0.0
4/2/2017 8:56:20 AM	0.0	0.0	0.0	0.0
4/2/2017 8:56:40 AM	0.0	0.0	0.0	0.0
4/2/2017 8:57:00 AM	0.0	0.0	0.0	0.0



7. Repeat this process for all broken data sources in your project.

3.1.3 Verifying LoggerNet scheduled collection is turned on

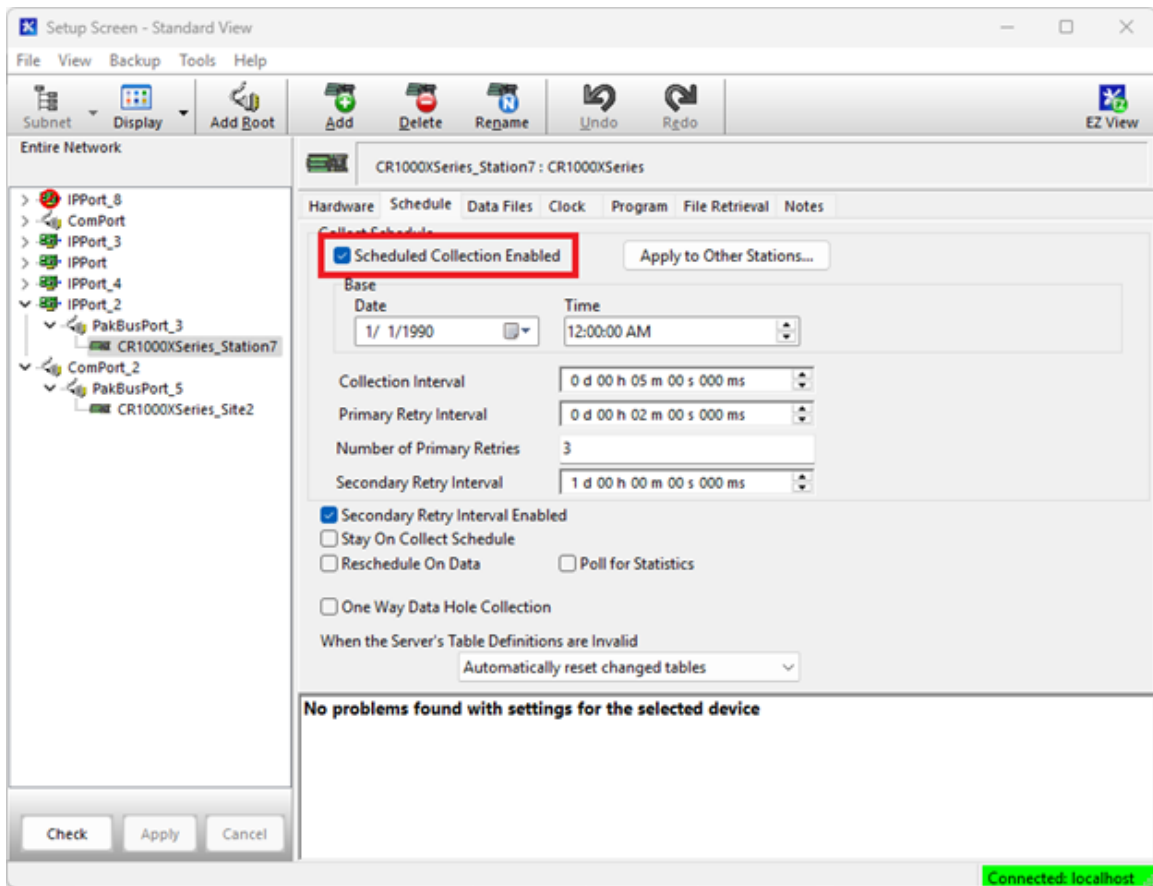
If your data source is a LoggerNet Server Data Source but doesn't display, or you notice new data no longer displays, check LoggerNet to verify new data is being collected from your station(s). In the following image, you can see a data logger in RTMC that doesn't have scheduled collection enabled. Note the + symbol is missing from the left side of the data logger. With scheduled collection not enabled, there are no data tables to select.



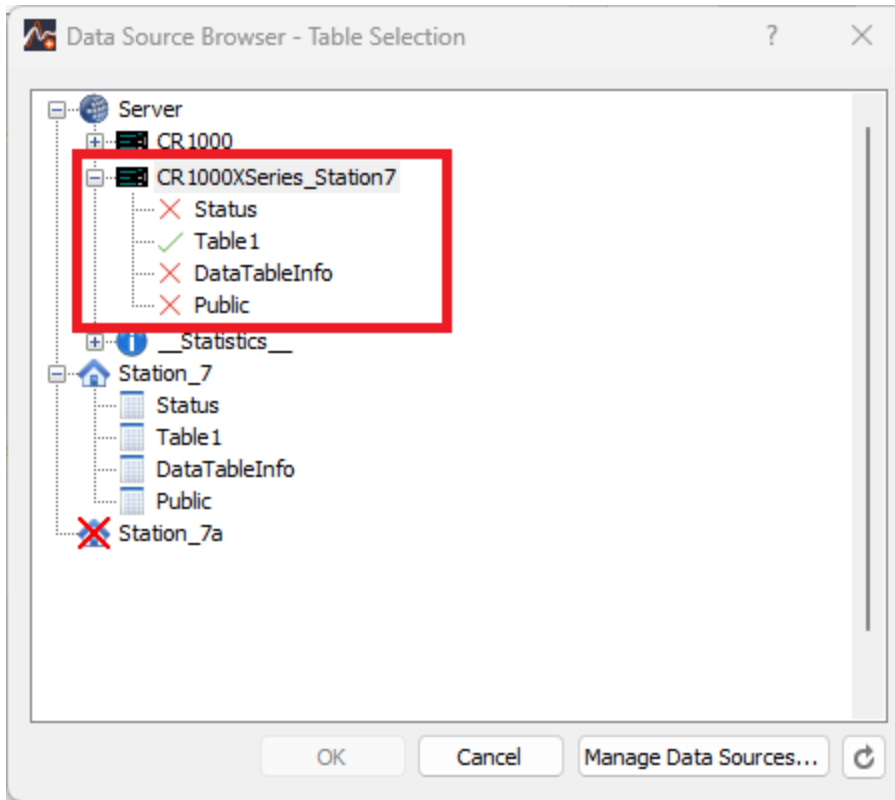
To verify scheduled collection is enabled:

1. Open LoggerNet **Setup** screen.
2. Select the data logger you are using as a data source.
3. Click the **Schedule** tab on the right side.

4. Ensure the **Scheduled Collection Enabled** check box is selected.

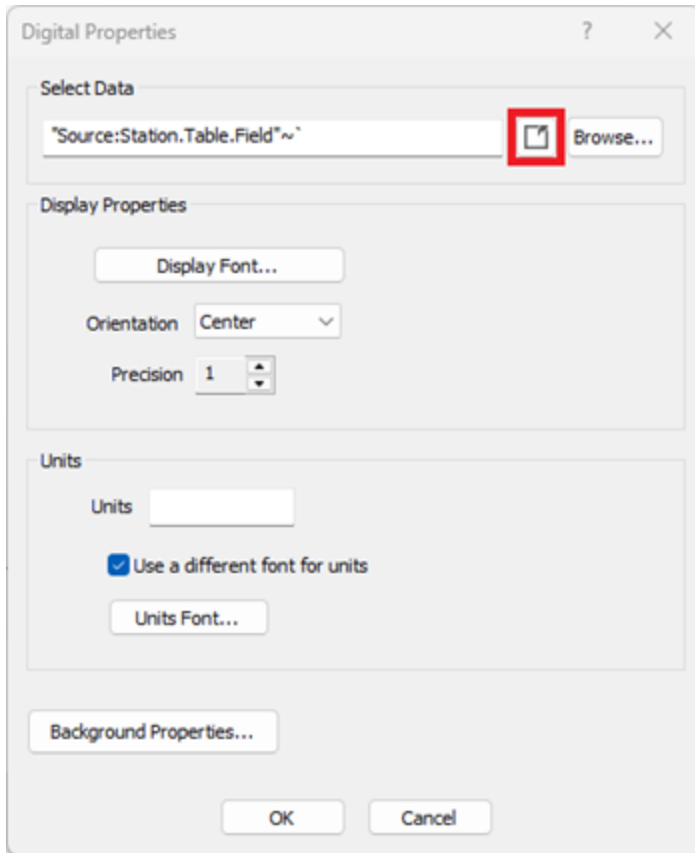


5. Once data has been collected in LoggerNet, note the availability of the tables in the **Data Source Browser – Table Selection** screen.

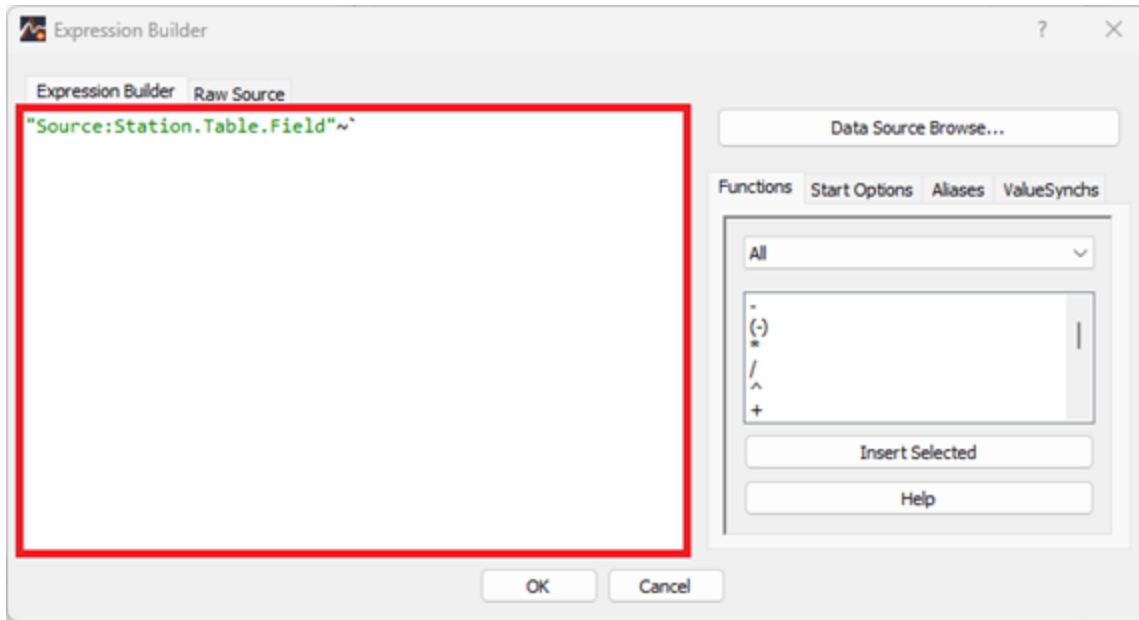


3.2 Checking for broken formulas

To check for broken formulas in your RTMC project components, right click the component and click **Properties**. This displays the **Properties** window. Click the **Expression Builder** button highlighted below:



This opens the **Expression Builder** window. In the **Expression Builder** window, verify the formula doesn't have any errors. Make any needed corrections and click **OK**. Click **OK** on the **Properties** window.



3.3 Updating RTMC Pro

To update RTMC Pro:

1. Visit www.campbellsci.com/rtrmcpro.
2. Under **Downloads**, download the latest patch for RTMC Pro and run it on your computer.
3. Once the patch is complete, reboot the computer.

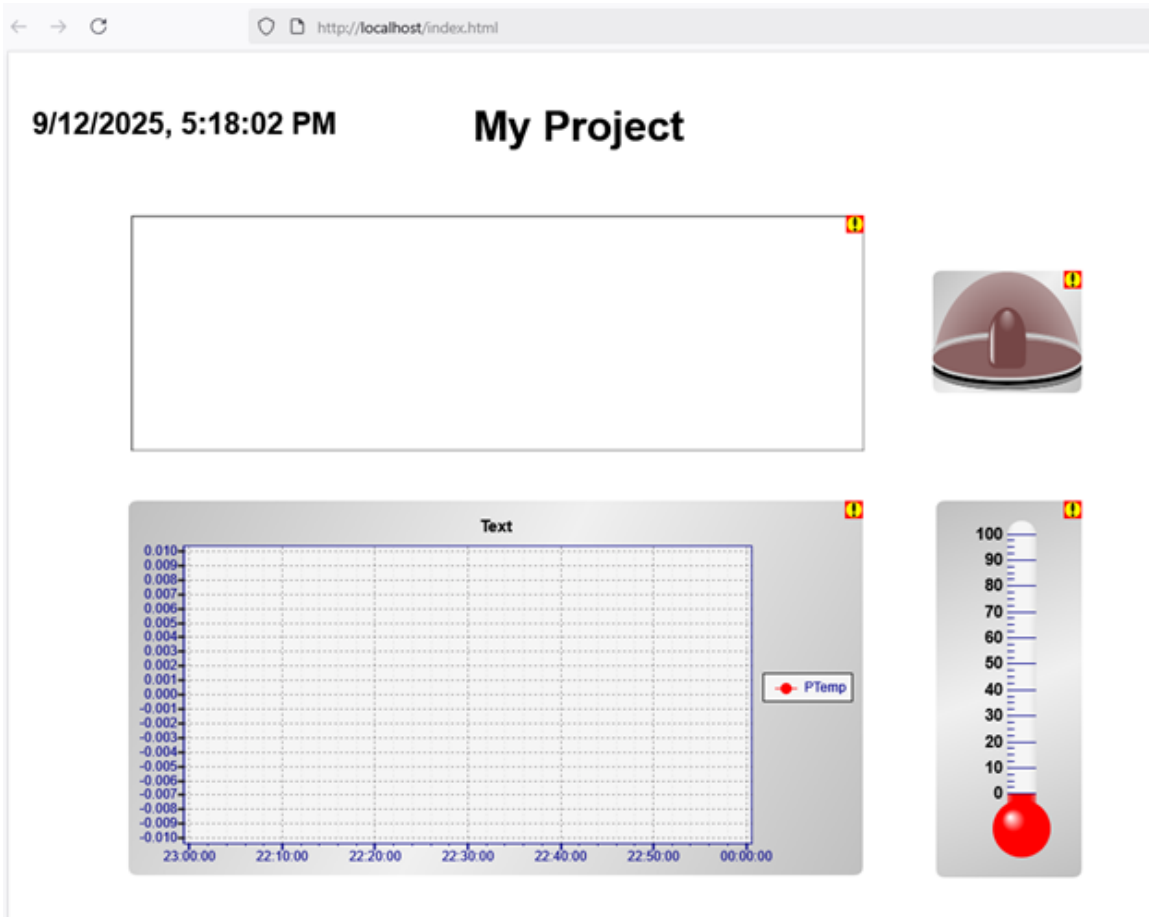
3.3.1 Updating RTMC Development or Run-time without RTMC Pro

NOTE: RTMC Development and RTMC Run-time are included with LoggerNet. Updating LoggerNet should also update to the latest version of these applications. If you encounter an issue, contact Campbell Scientific Support.

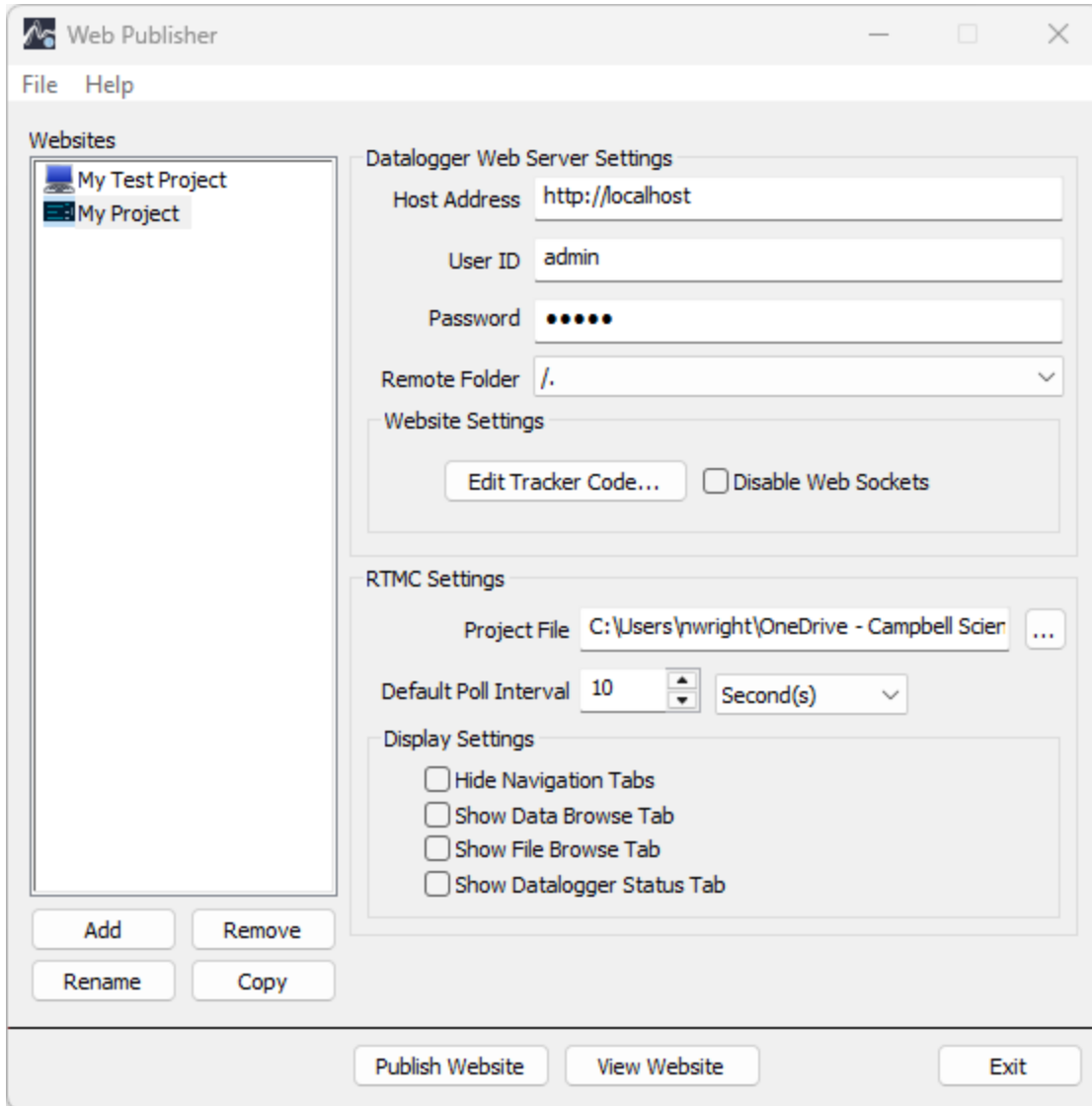
1. Visit <https://www.campbellsci.com/loggernet>.
2. Under **Downloads**, download the latest patch for LoggerNet and run it on your computer.
3. Once the patch is complete, reboot the computer.

3.4 Verifying the project was published as a PC website

If your PC or CSI Web Server project is published and doesn't display any data sources, and you have verified the data sources and their links are correct, verify your project has been published as the correct type.



The Web Publisher application will allow you to publish the project as one of two types: a PC Website or a Data logger Website. Check the icon to the left of your website name in the **Websites** field of the Web Publisher to verify the website has been published as the correct type. Note the icon of a computer indicates a computer website and the icon of a data logger indicates a data logger website.

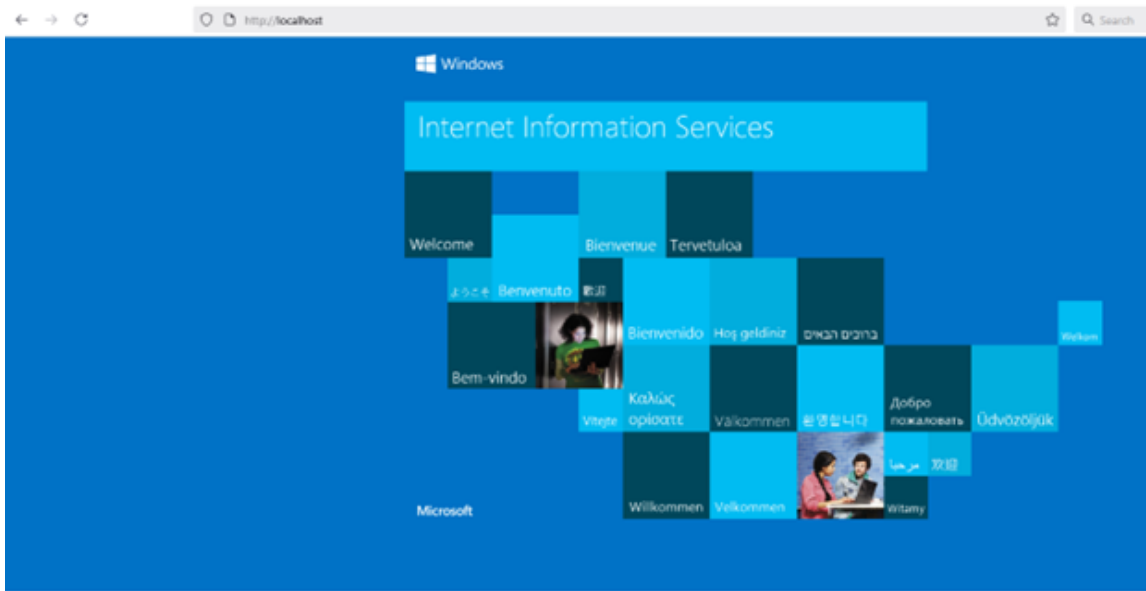


If the project has been published as the incorrect type, click **Add** to add the page as the correct type. Once the correct option has been selected, republish the webpage.

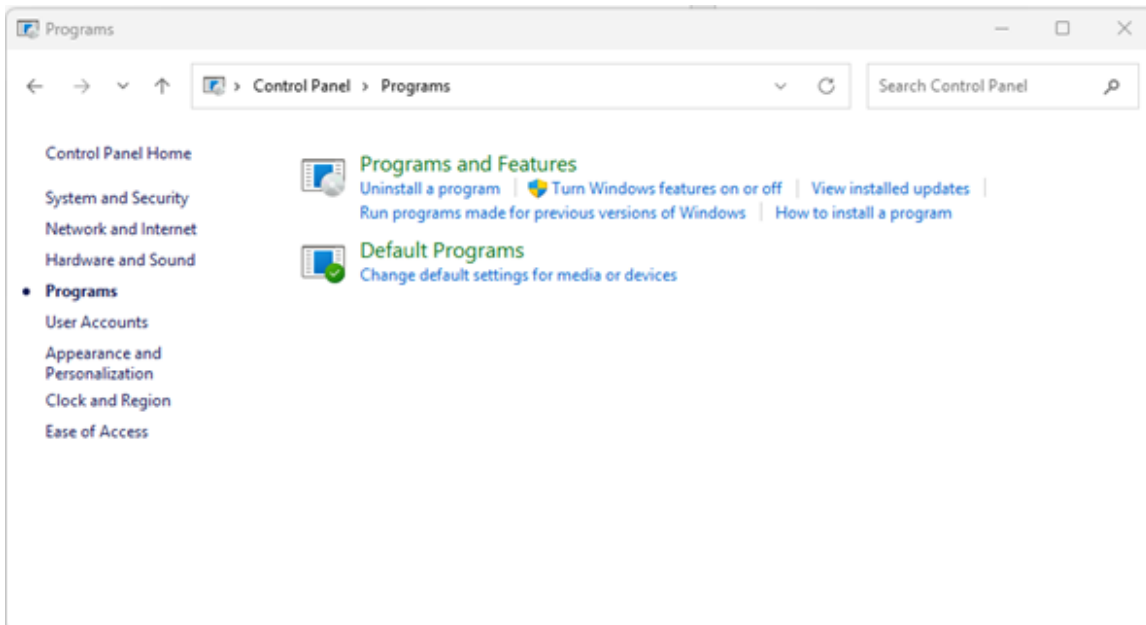
3.5 Disabling or removing IIS

If your Web Publisher isn't working or gives strange errors, verify your computer isn't running into a conflict with the Microsoft web server called IIS (or Internet Information Services).

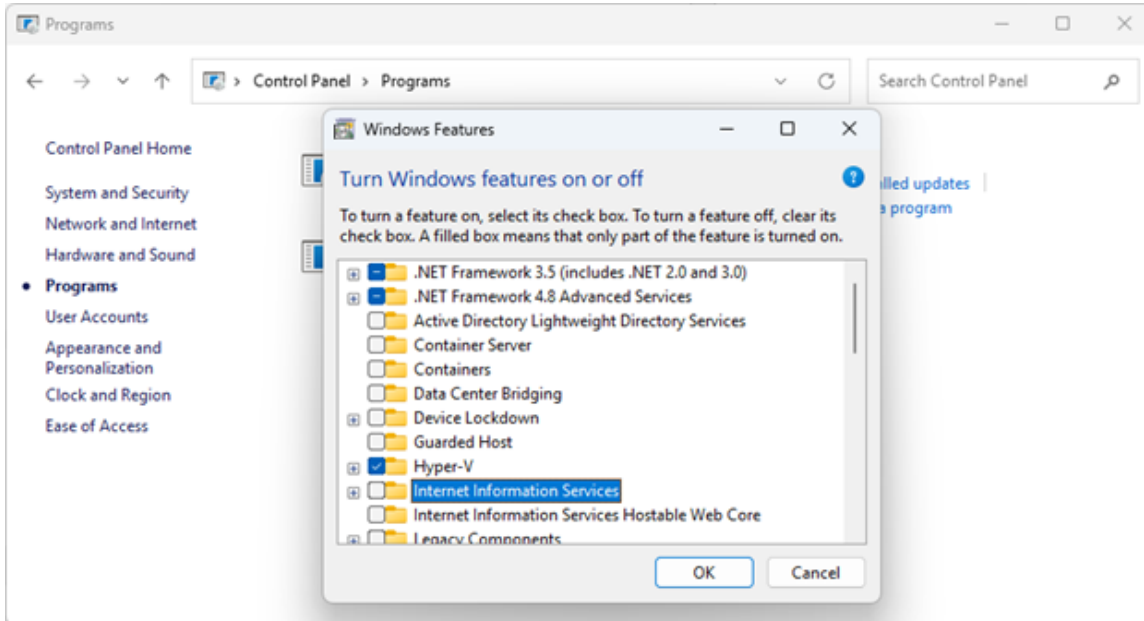
To check if IIS is running on your computer, open a web browser, type localhost or 127.0.0.1 into the address bar, and press Enter. If a webpage similar to the one below appears, your computer or server is running Microsoft IIS.



If you are not using the Microsoft web Server, remove IIS from your computer. To remove IIS from a client machine, open the **Control Panel** and go to **Programs** or **Programs and Features**. There is an option to **Turn Windows features on or off**.



On the list of **Windows Features**, unselect **Internet Information Services** and click **OK**.



Once the process is complete, reboot your computer and IIS will be removed thereby removing the conflict between the CSI Web Server and IIS.

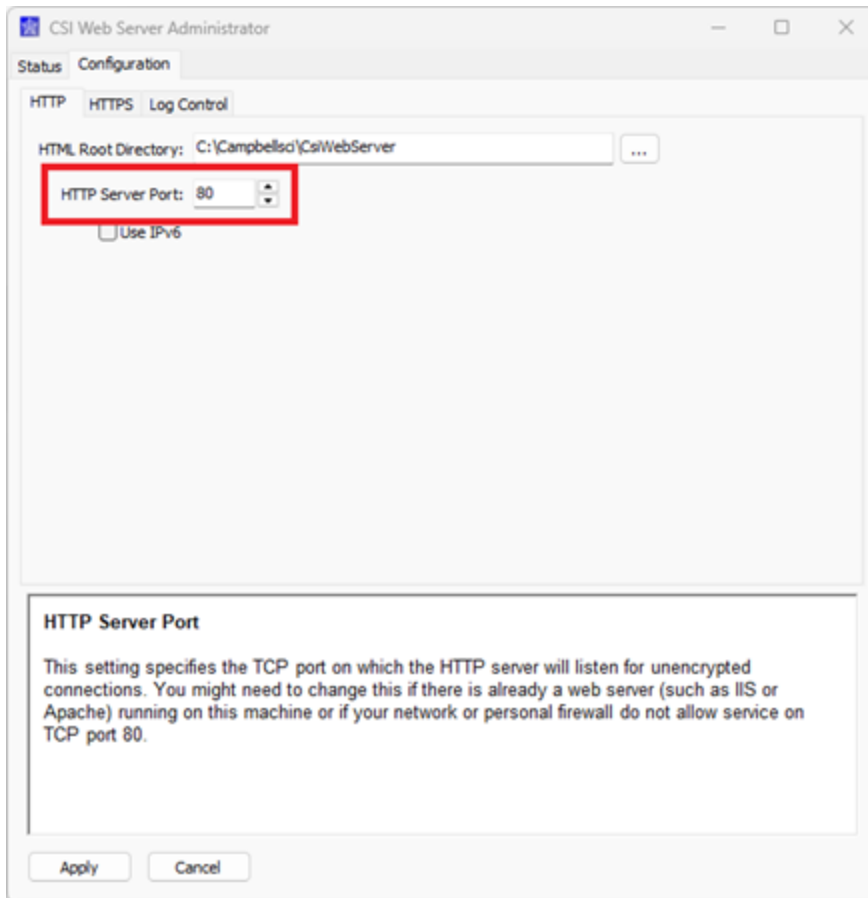
To remove IIS from a Windows server, go to **Server Manager and Server Roles**. Using the wizard, deselect the IIS or Internet Information Services role and click **OK**.

If you have a webpage hosted by IIS on the same computer as the CSI Web Server, you can change the port number the CSI Web Server operates on. See [Assigning the CSI Web Server to run on a different port](#) (p. 32) for instructions.

3.6 Assigning the CSI Web Server to run on a different port

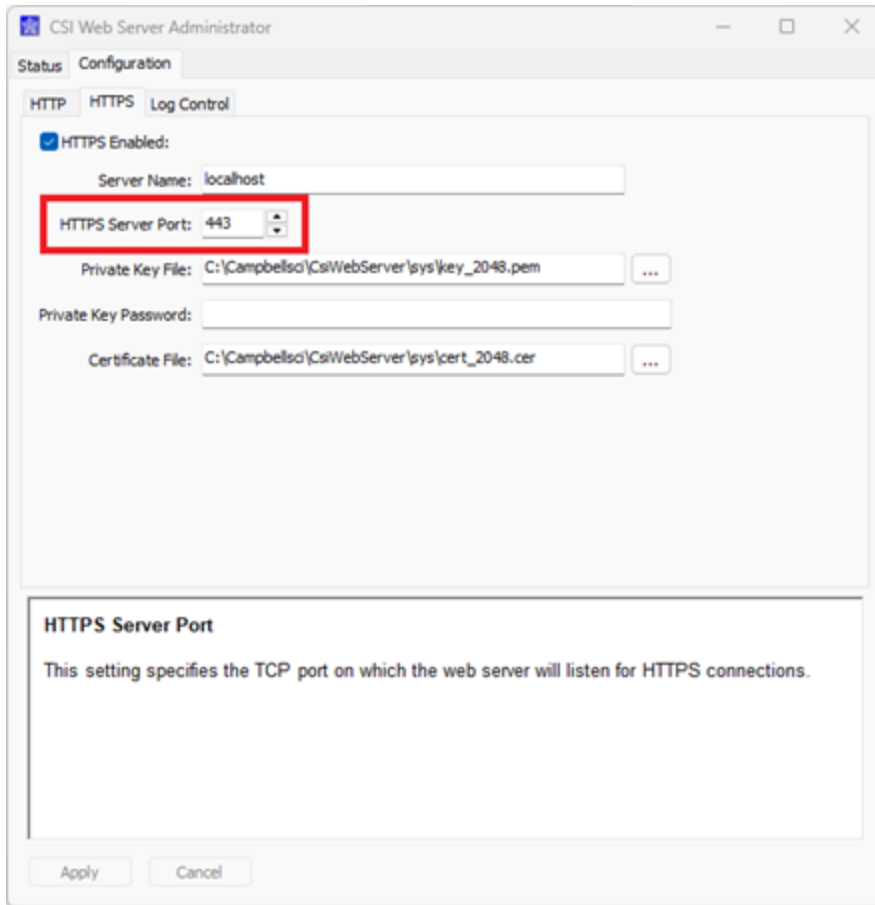
If your computer needs to run IIS to support an unrelated webpage, or you are unable to uninstall IIS, you can configure the CSI Web Server to run on a different port.

To change the port, navigate to the "C:\Program Files (x86)\Campbellsci\CsiWebServer\CsiWebAdmin.exe" application and launch the CSI Web Server Administrator. Inside the CSI Web Server Administrator, click the **Configuration** tab. The **HTTP Server Port** will be displayed by default on the **HTTP** sub tab. The default port is 80 for HTTP. To change the port number, enter a new port number between 1 and 49151 and click **OK**. A common alternative port to 80 for HTTP is 8080.



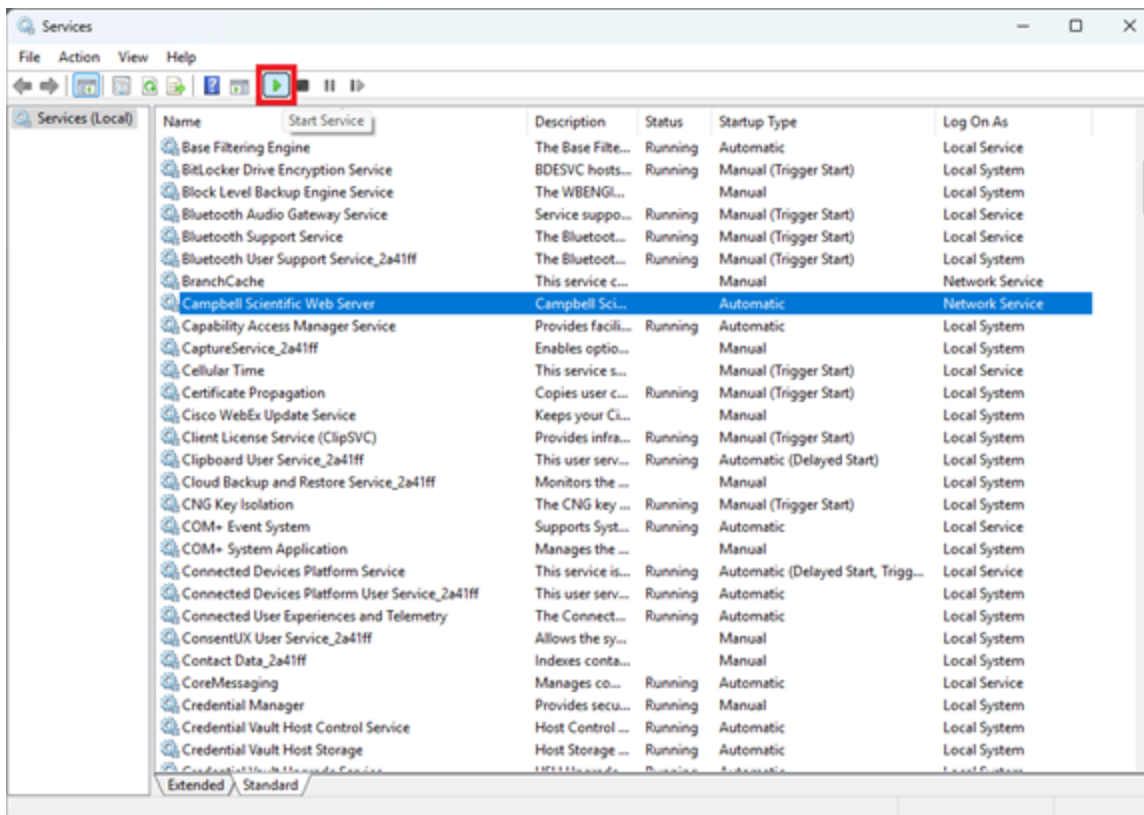
Once the new port has been applied, append a colon followed by the port number to the end of the address to access the webpage via a browser. For example: 192.168.1.21:8080 or localhost:8080.

To change the port for HTTPS, click the **Configuration** tab in the CSI Web Server Administrator. Click the **HTTPS** sub tab and enter the new port number for HTTPS. Click **OK**.



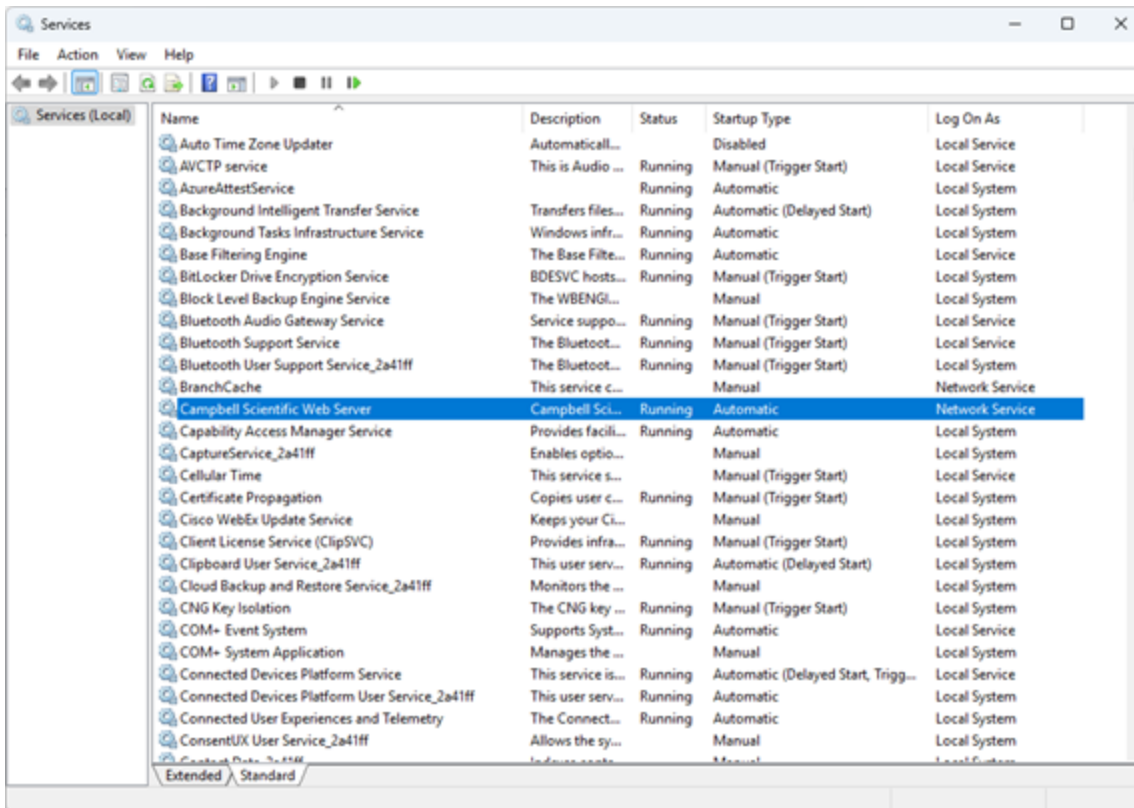
3.7 Restarting the CSI Web Server service in Windows

To restart the Campbell Scientific Web Server Service in Windows, launch **Services** from Windows as an Administrator. Navigate to the **Campbell Scientific Web Server** service (depending on the version of CSI Web Server you originally installed the service may be called CSI Web Server instead). Click on the service to highlight it, then click the green play button at the top of the window to restart the service.

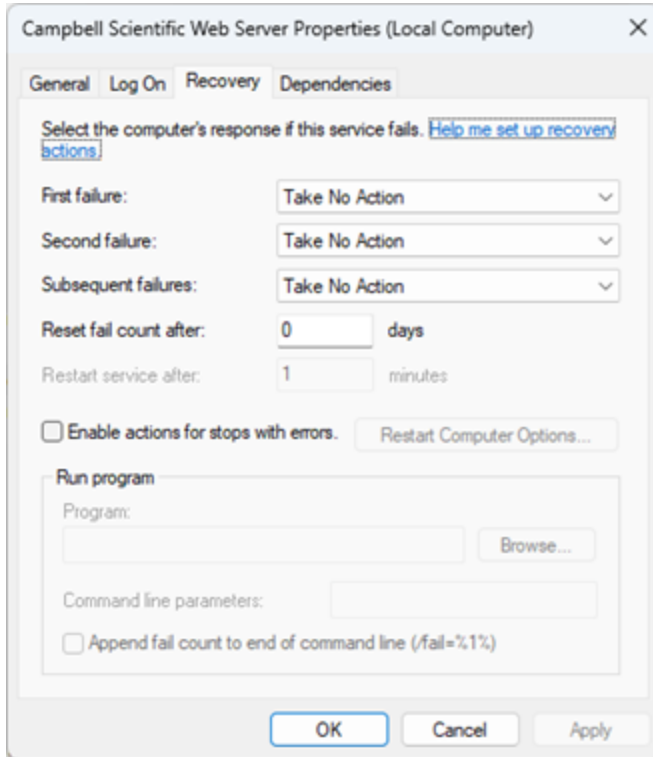


3.8 Adjusting restart and recovery properties in Windows

In instances where the CSI Web Server service is being forcefully closed or crashing due to security software, a backup application, or other factors, setting the Service Recovery options can improve recovery. To set the Recovery options, launch **Services** from Windows as an Administrator. Navigate to the **Campbell Scientific Web Server** service (depending on the version of CSI Web Server you originally installed, the service may be called CSI Web Server instead). Double click on the service to open its properties.



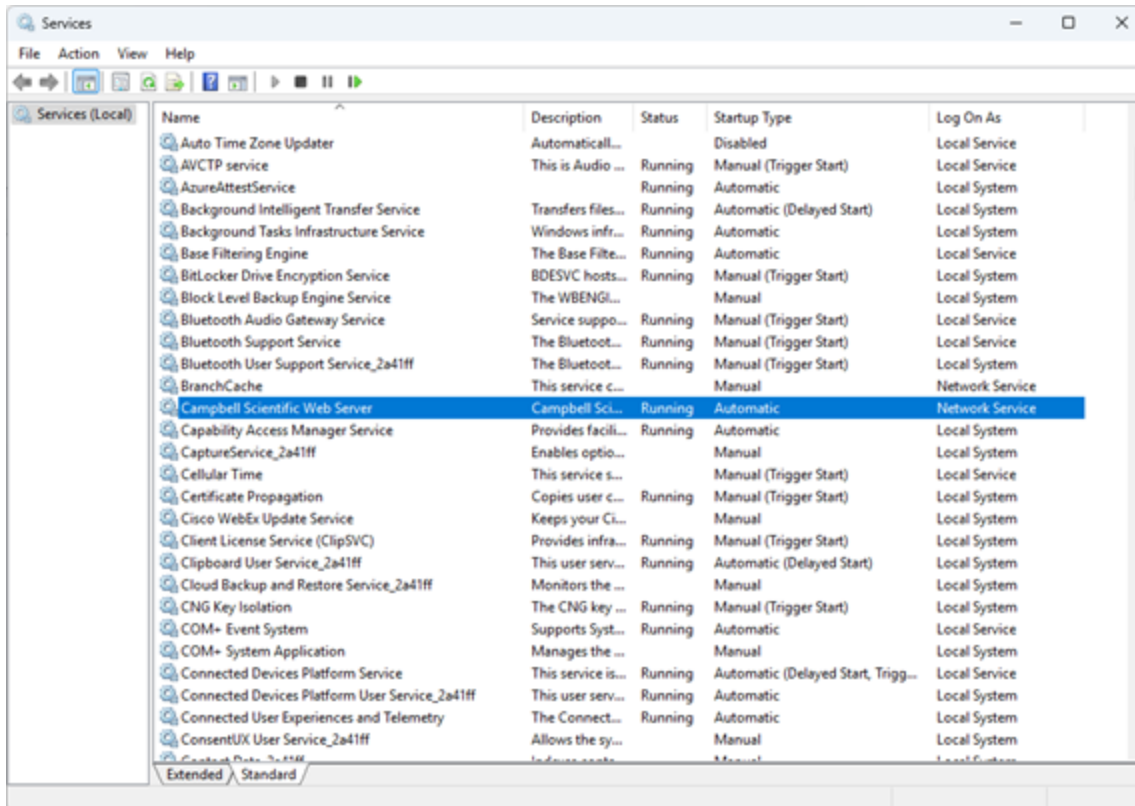
From the **Properties** screen, click the **Recovery** tab.



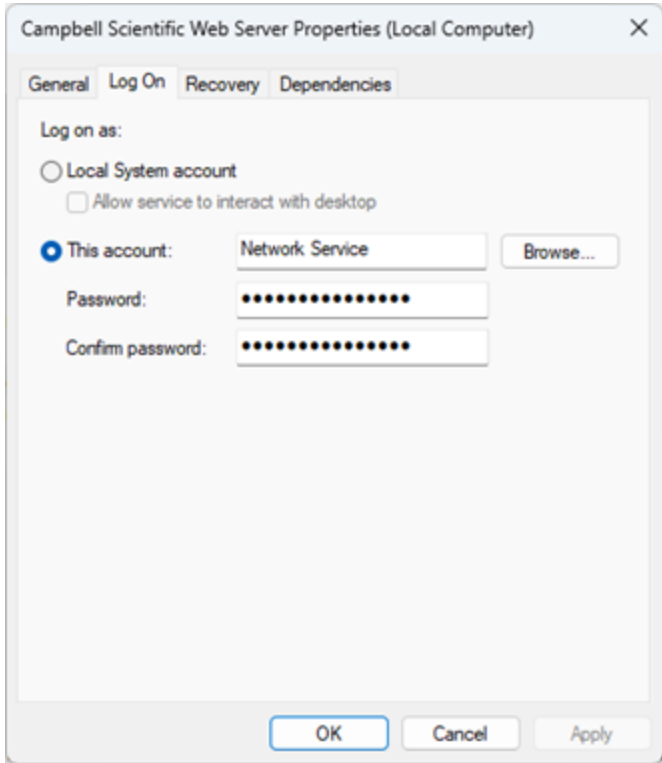
On the **Recovery** tab, change the **First failure**, **Second failure**, and **Subsequent failures** settings all to **Restart the Service**. Click **OK**. The service should now recover better after being forcefully closed or crashing.

3.9 Adjusting CSI Web Server permissions

To verify or change the service **Log On** permissions, launch **Services** from Windows as an Administrator. Navigate to the Campbell Scientific Web Server service (depending on the version of CSI Web Server you originally installed, the service may be called CSI Web Server instead). Double click on the service to see its properties.



From the **Properties** screen, click the **Log On** tab.

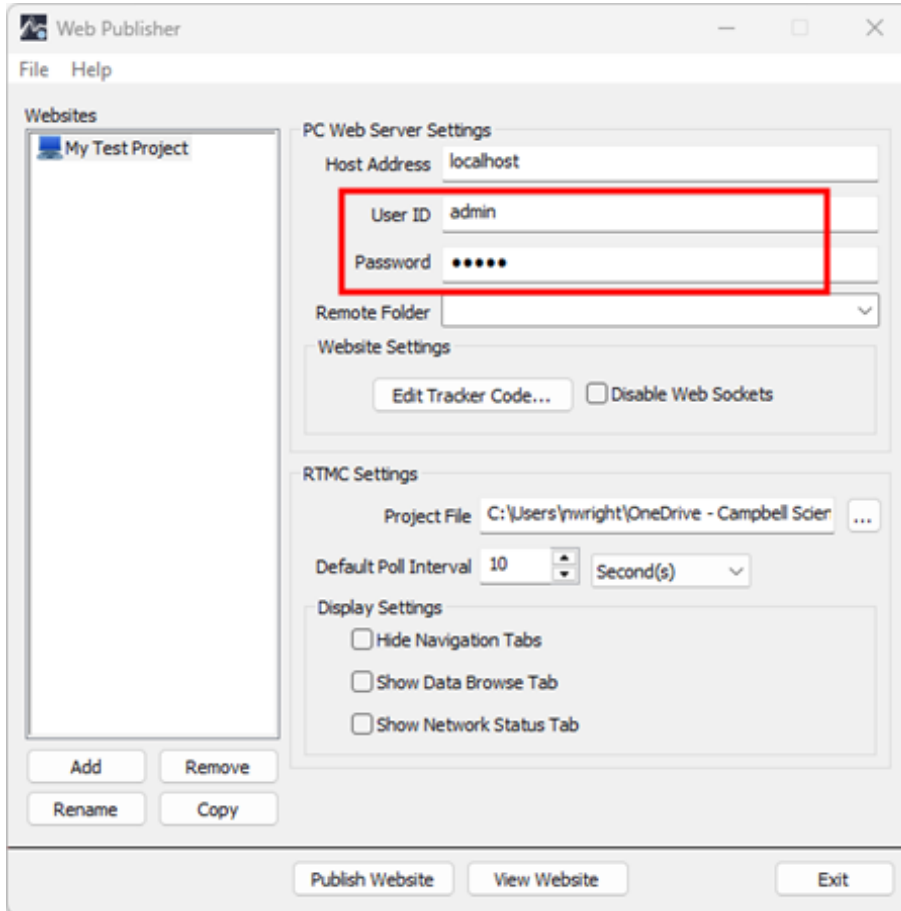


On the **Log On** tab you'll notice the **This account:** field that specifies the username, **Password**, and **Confirm Password** fields.

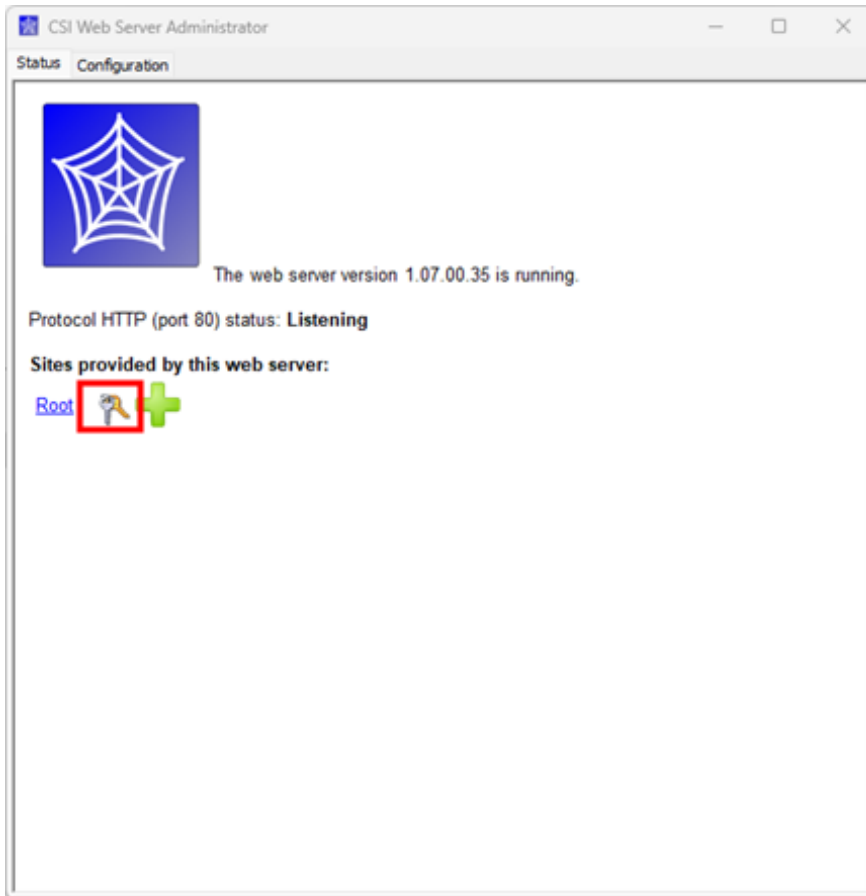
Consult with your IT department on the permissions needed for the service based on the network environment you are operating in. Setting the account to a local administrator may not always be the right configuration. In many cases, if the service is running as the Network Service account, the service will operate correctly. Alternatively, a local administrative account can generally run the service with the permissions it requires. In some cases, a local administrator account may need to be a member of a domain group to have rights to run the service. It all depends on how Local Network and Local Computer Security policy are enforced.

3.10 Verifying CSI Web Server and data logger permissions

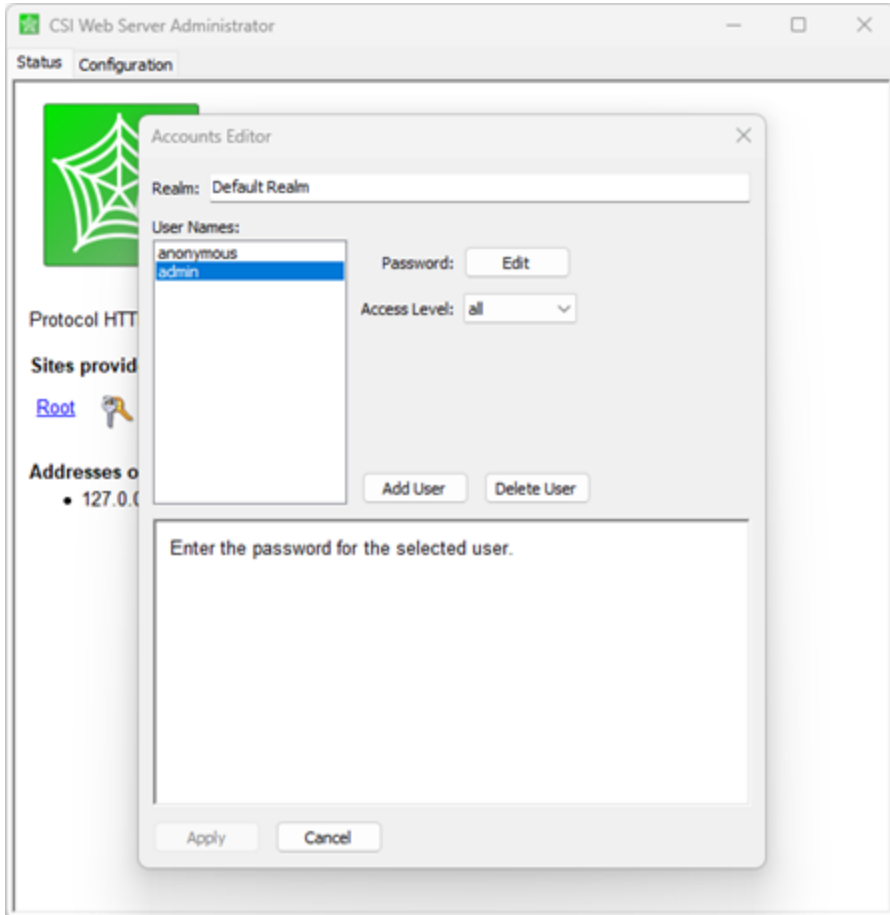
To verify the permissions of the CSI Web Server, first note the user ID and password you are using in the Web Publisher.



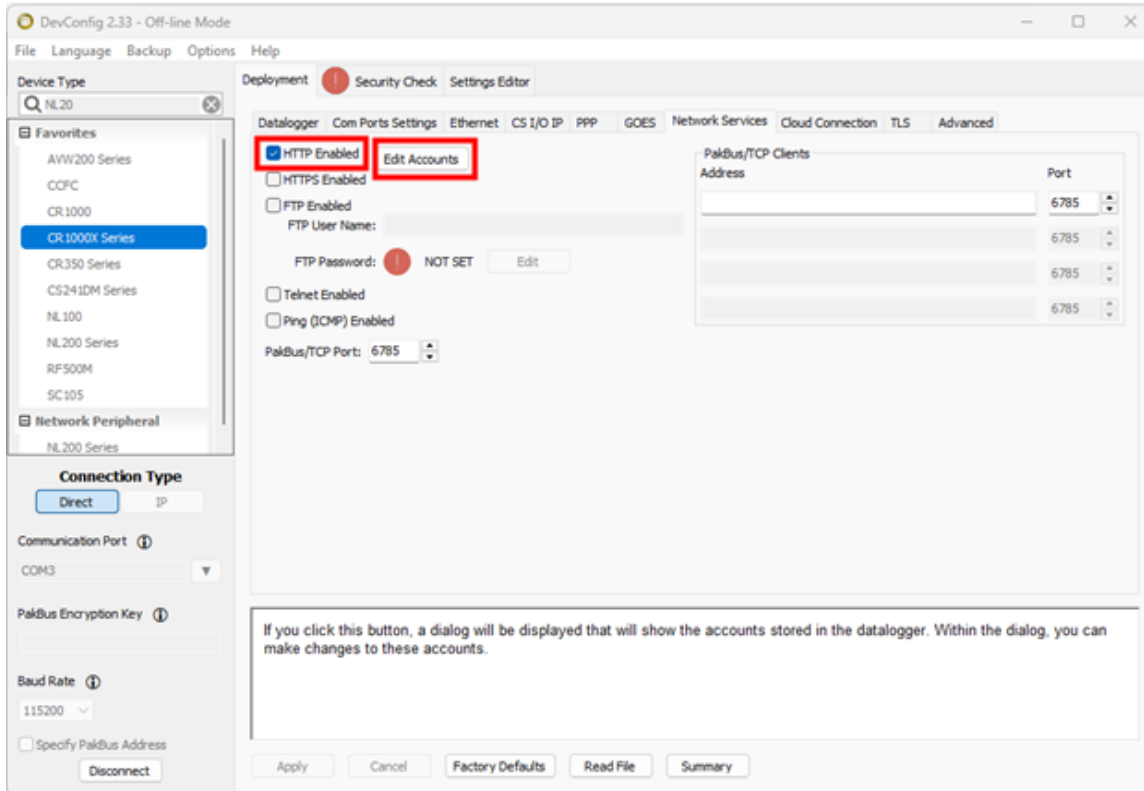
Launch the CSI Web Server Administrator. Click the keys icon next to the website or directory where you want to check or adjust the permissions.



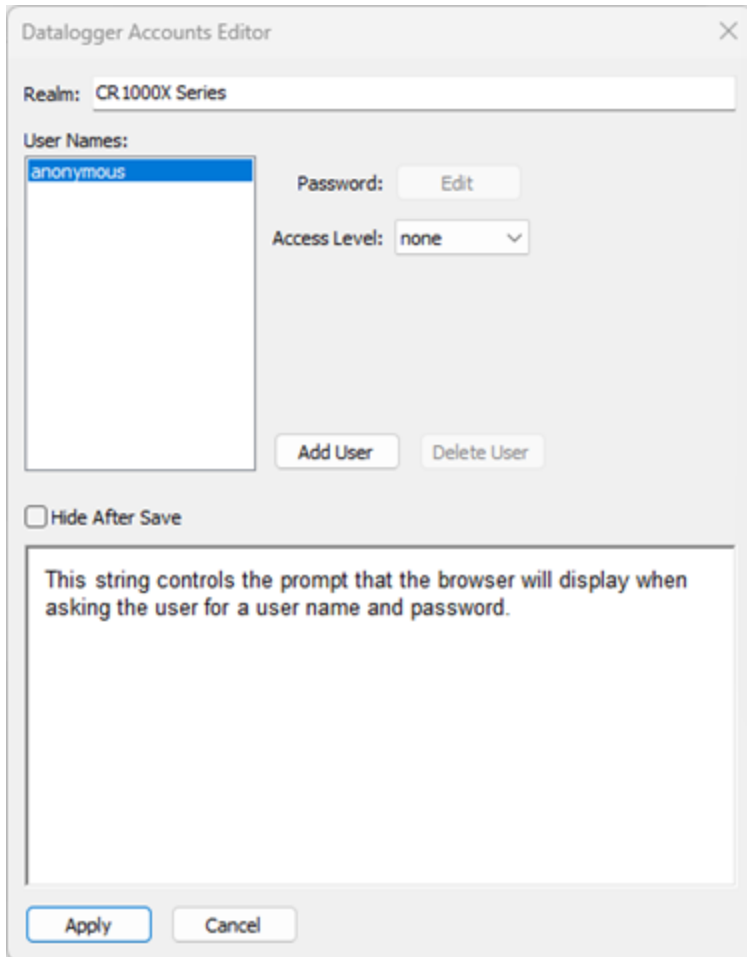
This will open the **Accounts Editor**. On the **Accounts Editor** screen, review the account you are using to publish the webpage from the Web Publisher. Verify the account is present, **the Access Level** is set to Write or All, and the password is set correctly.



If you are publishing to the built-in web server of a data logger, use the Device Configuration Utility to verify the permissions of the data logger. Once you are connected to your data logger with the Device Configuration Utility, click the **Network Services** tab. On the **Network Services** tab, verify the **HTTP Enabled** checkbox has been selected. This setting enables the web server in the data logger, allowing you to both host and publish the webpage to the data logger.



Once you have verified the service is enabled, click **Edit Accounts** on the **Network Services** tab to bring up the **Datalogger Accounts Editor** window.



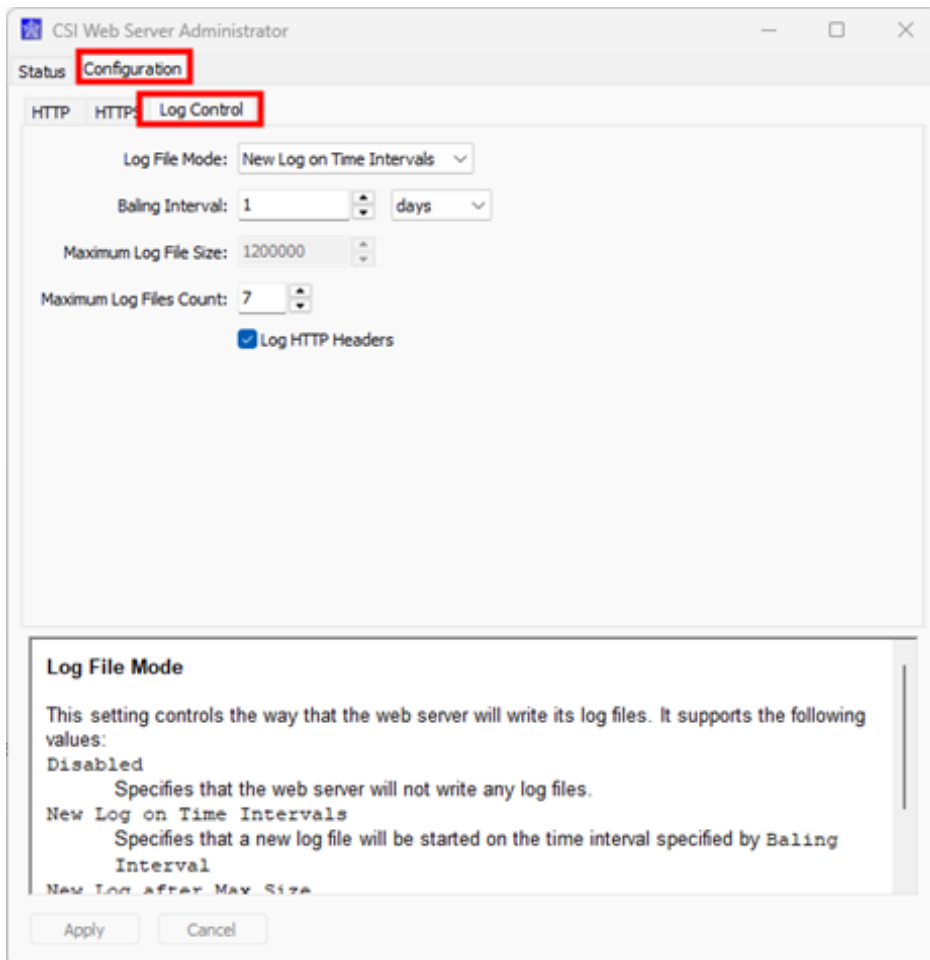
Verify the username and password you are using in the Web Publisher matches a username set up in the data logger. Also, verify the username's **Access Level** is set to Write or All, and the password is set correctly. If you make changes, click **Apply**.

3.11 Finding CSI Web Server log files

If you are experiencing issues with the CSI Web Server, like crashes, it may be helpful to examine the CSI Web Server logs. To get the logs, you first need to ensure logging is enabled in the CSI Web Server Administrator.

Launch the CSI Web Server Administrator application and click on the **Configuration** tab. Click the **Log Control** tab. On the **Log Control** tab, ensure **Log File Mode** setting is set to **New Log on Time Intervals** (you can also use **New Log After Max Size**).

Set the length of each log file based on a time period by setting the **Baling Interval**. Hours and days are usually the best time intervals. Then set the **Maximum Log Files Count**. You can also include the HTTP Headers with the **Log HTTP Headers** setting. Once your log settings are entered, click **Apply**.



Once enough time has passed, you should have a series of logs detailing what has been happening with the web server. The log files can be found in the following directory with filenames like `csiwebd1.log`:

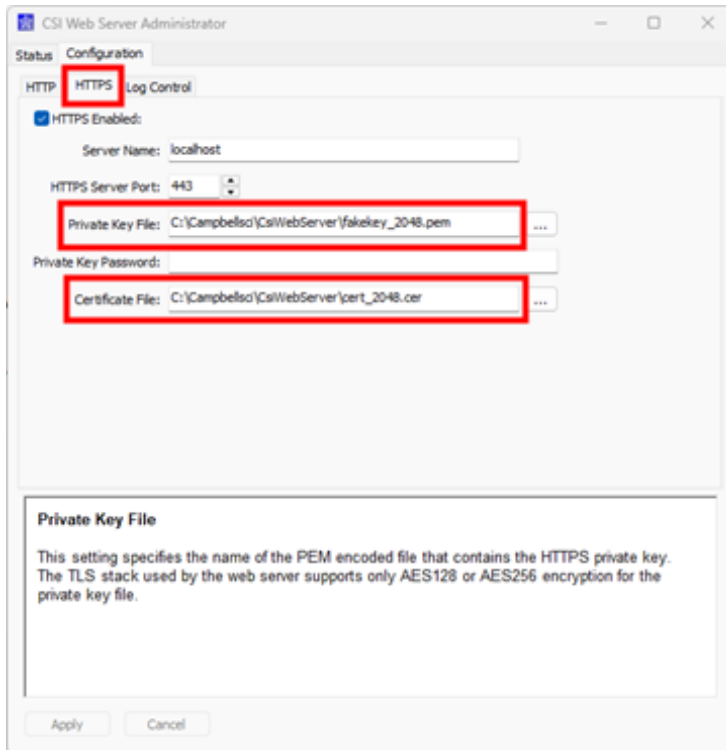
```
C:\Campbellsci\CsiWebServer\sys\log
```

These logs can be extremely helpful when working with a Campbell Scientific Support Engineer.

3.12 Verifying TLS certificate and key location

To verify your TLS key and certificate are stored in the right location, launch the CSI Web Server Administrator. Click the **Configuration** tab. Click the **HTTPS** sub tab. Note the path of the **Private Key File** and the **Certificate File**.

Both of these need to be stored in a directory the CSI Web Server Service can reach. If the path is not in C:\Campbellsci\CsiWebServer or a sub directory of that folder, it is likely not going to work. For security reasons, the recommended path to store the file in is C:\Campbellsci\CsiWebServer\Sys\. If the files are not in one of these directories, move them and then update the path in the CSI Web Server Administrator.



3.13 Verifying TLS certificate and key format

Verify the TLS key and/or certificate are valid. Navigate to the directory where the files are stored and open the files as a text document. Look at the headers of the files to verify they are correct.

Two clear signs that your private key file is in the correct format are:

1. The file extension is .pem.
2. When opening a copy of the key file in Notepad or other ASCII text editor, it has header and footer information similar to the following:

```
-----BEGIN RSA PRIVATE KEY-----
```

```
[Unreadable Content goes here]
```

```
-----END RSA PRIVATE KEY
```

If this information does not match your key file, it is in the wrong format.

An example of an incorrect key file is below. Notice the header reads "Begin Certificate." In this case, a user was sent a certificate in both a .cer and .pem format, and because they had not saved a copy of their private key file, they assumed the .pem formatted certificate was a key.

```
-----BEGIN CERTIFICATE-----
MIIEDzCCAvegAwIBAgIJANW2Fdyr28GdMA0GCSqGSIb3DQEBBQUAMIGdMQswCQYD
VQQGEwJVUzENMAsGAlUECAwEVXRhaDEOMAwwGAlUEBwwFTG9nYW4xIjAgBgNVBAoM
GUNhbXBiZWxsIFNjaWVudG1maWMsIEluYy4xJzAlBgNVBAMHmpvbi10cmFlbnR2
ZWluLmNhbXBiZWxsc2NpLmNvbTEiMCAGCSqGSIb3DQEJARYTAm9uQGNhbXBiZWxs
c2NpLmNvbTAEFw0xNDA4MDQxNzE3MzRaFw00NzA2MTIxNzE3MzRaMIGdMQswCQYD
VQQGEwJVUzENMAsGAlUECAwEVXRhaDEOMAwwGAlUEBwwFTG9nYW4xIjAgBgNVBAoM
GUNhbXBiZWxsIFNjaWVudG1maWMsIEluYy4xJzAlBgNVBAMHmpvbi10cmFlbnR2
ZWluLmNhbXBiZWxsc2NpLmNvbTEiMCAGCSqGSIb3DQEJARYTAm9uQGNhbXBiZWxs
c2NpLmNvbTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPBkUySlvoK
5UX7r1Da5agnOGqHamkZzXfi/vlo6cwF142z3Php+nz5WRcGY6GjvADapJPB94ed
HOBJ7RZSzbCAx6NLb86RcZOYwTeCNeIZQlc6mNfWDazo4vCvu000BKlduq47L2t+
mAEVvx7GjaqxoEGGuGGy74KTziPeXZRltr3fNAMYQWuqNZSjBPFv91zMa3GiAd4
cb7cfnQHaiBJ2ur/AuAyGZxbaXOknCfgNd/MyE566/F7sy1IsPbuxsqWet8lAxZt
kjoRsQIzaHbZdV2QkQ0sE5140skiElhFCoCrt5kQCUunKaxrrRlKMiAe/7CxOnYX
SbMQys76J7sCAwEAAANQME4wHQYDVR0OBBYEFwLwhtoLc6u2+NulWAZQ0SKOpYyLf
MB8GAlUdIwQYMBaAFLwhtoLc6u2+NulWAZQ0SKOpYyLFAwGAlUdEwQFMAMBAf8w
DQYJKoZIhvcNAQEFBQADggEBAA6hlXluCj6n+lCMbbF+oi7jihku8UILM29oGiZI
PMrZ0Nu66rTKqykY/1+g9VffzMW5nhCuuxznU4yUbcEHBglesW2wG/DOTFQRTsoV
gU16jfZiN9oPtrW6VfizgvYuZvUoQPvYY9dmPeY9I3onaGIfEAKLI40M8M9kly+h
PCheZDEsa6l2zpYW4OrduxRfx08QuzGKdEiKmkWAZXocXux9IC10XaFrnEap00ck
ivnWZKc81s2kcZRN3QBkw/vMF9ZoJC+AZzDqY2+qZvjAuaEZZzoGxy4QBXDsgMLn
lMApiGQogKpi8Z0kV7u4ipyW4+algaWDbvSmeVvk7Y5V3Pxs=
-----END CERTIFICATE-----
```

The same applies to certificates. Generally, for help on certificates, contact your IT department.

Global Sales and Support Network

A worldwide network to help meet your needs



Campbell Scientific Regional Offices

Australia

Location: Garbutt, QLD Australia
Phone: 61.7.4401.7700
Email: info@campbellsci.com.au
Website: www.campbellsci.com.au

Brazil

Location: São Paulo, SP Brazil
Phone: 11.3732.3399
Email: vendas@campbellsci.com.br
Website: www.campbellsci.com.br

Canada

Location: Edmonton, AB Canada
Phone: 780.454.2505
Email: dataloggers@campbellsci.ca
Website: www.campbellsci.ca

China

Location: Beijing, P. R. China
Phone: 86.10.6561.0080
Email: info@campbellsci.com.cn
Website: www.campbellsci.com.cn

Costa Rica

Location: San Pedro, Costa Rica
Phone: 506.2280.1564
Email: info@campbellsci.cc
Website: www.campbellsci.cc

France

Location: Montrouge, France
Phone: 0033.0.1.56.45.15.20
Email: info@campbellsci.fr
Website: www.campbellsci.fr

Germany

Location: Bremen, Germany
Phone: 49.0.421.460974.0
Email: info@campbellsci.de
Website: www.campbellsci.de

India

Location: New Delhi, DL India
Phone: 91.11.46500481.482
Email: info@campbellsci.in
Website: www.campbellsci.in

Japan

Location: Kawagishi, Toda City, Japan
Phone: 048.400.5001
Email: jp-info@campbellsci.com
Website: www.campbellsci.co.jp

South Africa

Location: Stellenbosch, South Africa
Phone: 27.21.8809960
Email: sales@campbellsci.co.za
Website: www.campbellsci.co.za

Spain

Location: Barcelona, Spain
Phone: 34.93.2323938
Email: info@campbellsci.es
Website: www.campbellsci.es

Thailand

Location: Bangkok, Thailand
Phone: 66.2.719.3399
Email: info@campbellsci.asia
Website: www.campbellsci.asia

UK

Location: Shephed, Loughborough, UK
Phone: 44.0.1509.601141
Email: sales@campbellsci.co.uk
Website: www.campbellsci.co.uk

USA

Location: Logan, UT USA
Phone: 435.227.9120
Email: info@campbellsci.com
Website: www.campbellsci.com