Product Manual

Software

CSI Web Server

Revision: 09/2022

CSL I.D - 943

RELIABLE SINCE 1974 MONITORING

CAMPBELL SCIENTIFIC

Campbell Scientific, Inc. Software End User License Agreement (EULA)

COPYRIGHT: This software is protected by United States copyright law and international copyright treaty provisions. This software may not be sold, included or redistributed in any other software, or altered in any way without prior written permission from Campbell Scientific. All copyright notices and labeling must be left intact.

NOTICE OF AGREEMENT: Please carefully read this EULA. By installing or using this software, you are agreeing to comply with the following terms and conditions. If you do not want to be bound by this EULA, you must promptly return the software, any copies, and accompanying documentation in its original packaging to Campbell Scientific or its representative.

This software can be installed as a trial version or as a fully licensed copy. All terms and conditions contained herein apply to both versions of software unless explicitly stated.

TRIAL VERSION: Campbell Scientific distributes a trial version of this software free of charge to enable users to work with Campbell Scientific data acquisition equipment. You may use the trial version of this software for 30 days on a single computer. After that period has ended, to continue using this product you must purchase a fully licensed version.

This trial may be freely copied. However, you are prohibited from charging in any way for any such copies and from distributing the software and/or the documentation with any other products (commercial or otherwise) without prior written permission from Campbell Scientific.

LICENSE FOR USE: Campbell Scientific grants you a non-exclusive license to use this software in accordance with the following:

1. The purchase of this software allows you to install and use a single instance of the software on one physical computer or one virtual machine only.
2. This software cannot be loaded on a network server for the purposes of distribution or for access to the software by multiple operators. If the software can be used from any computer other than the computer on which it is installed, you must license a copy of the software for each additional computer from which the software may be accessed.

3. If this copy of the software is an upgrade from a previous version, you must possess a valid license for the earlier version of software. You may continue to use the earlier copy of software only if the upgrade copy and earlier version are installed and used on the same computer. The earlier version of software may not be installed and used on a separate computer or transferred to another party.
4. This software package is licensed as a single product. Its component parts may not be separated for use on more than one computer.
5. You may make one (1) backup copy of this software onto media similar to the original distribution, to protect your investment in the software in case of damage or loss. This backup copy can be used only to replace an unusable copy of the original installation media.

Limited warranty

The following warranties are in effect for ninety (90) days from the date of shipment of the original purchase. These warranties are not extended by the installation of upgrades or patches offered free of charge:

Campbell Scientific warrants that the installation media on which the software is recorded and the documentation provided with it are free from physical defects in materials and workmanship under normal use. The warranty does not cover any installation media that has been damaged, lost, or abused. You are urged to make a backup copy (as set forth above) to protect your investment. Damaged or lost media is the sole responsibility of the licensee and will not be replaced by Campbell Scientific.

Campbell Scientific warrants that the software itself will perform substantially in accordance with the specifications set forth in the instruction manual when properly installed and used in a manner consistent with the published recommendations, including recommended system requirements. Campbell Scientific does not warrant that the software will meet licensee's requirements for use, or that the software or documentation are error free, or that the operation of the software will be uninterrupted.

Campbell Scientific will either replace or correct any software that does not perform substantially according to the specifications set forth in the instruction manual with a corrected copy of the software or corrective code. In the case of significant error in the installation media or documentation, Campbell Scientific will correct errors without charge by providing new media, addenda, or substitute pages. If Campbell Scientific is unable to replace defective media or documentation, or if it is unable to provide corrected software or corrected documentation within a reasonable time, it will either replace the software with a functionally similar program or refund the purchase price paid for the software.

All warranties of merchantability and fitness for a particular purpose are disclaimed and excluded. Campbell Scientific shall not in any case be liable for special, incidental, consequential, indirect, or other similar damages even if Campbell Scientific has been advised of the possibility of such damages. Campbell Scientific is not responsible for any costs incurred as a result of lost profits or revenue, loss of use of the software, loss of data, cost of re-creating lost data, the cost of any substitute program, telecommunication access costs, claims by any party other than licensee, or for other similar costs.

This warranty does not cover any software that has been altered or changed in any way by anyone other than Campbell Scientific. Campbell Scientific is not responsible for problems caused by computer hardware, computer operating systems, or the use of Campbell Scientific's software with non-Campbell Scientific software.

Licensee's sole and exclusive remedy is set forth in this limited warranty. Campbell Scientific's aggregate liability arising from or relating to this agreement or the software or documentation (regardless of the form of action; e.g., contract, tort, computer malpractice, fraud and/or otherwise) is limited to the purchase price paid by the licensee.

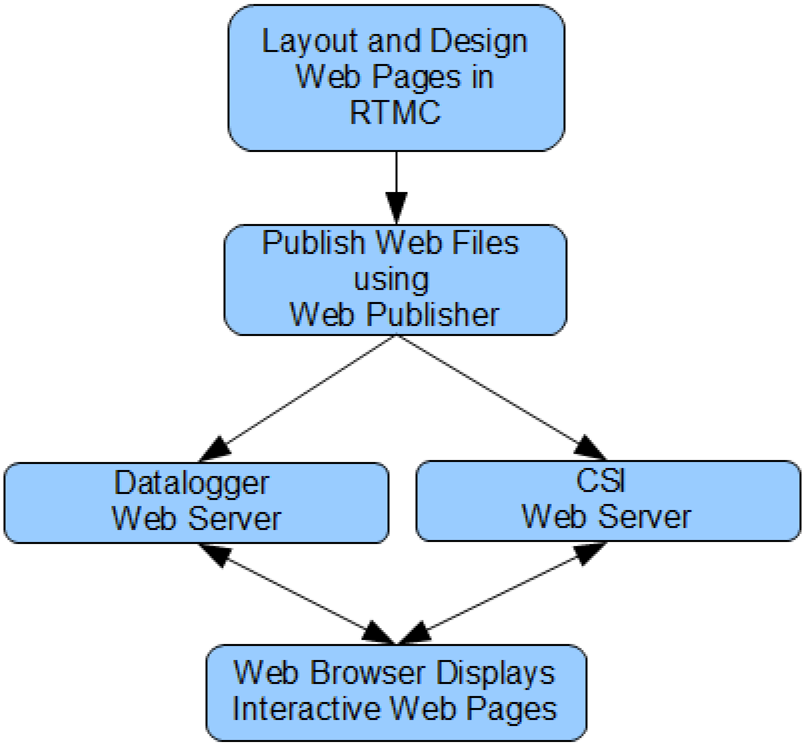
Table of contents

1. CSI Web Server

The CSI Web Server allows you to view your RTMC projects using a web browser. Included with the CSI Web Server are the CSI Web Server Administrator and the Web Publisher. The CSI Web Server Administrator allows you to configure the web server, check the status of the web server, set up user accounts and passwords, and easily browse to sites running on the web server. The Web Publisher allows you to publish your RTMC project to either a PC website using the CSI Web Server or to an HTTP-enabled datalogger.

2. Getting Started

The diagram below shows the basic steps in creating your web content:


Layout and Design Web Pages in RTMC
Publish Web Files using Web Publisher
Datalogger Web Server
CSI Web Server
Web Browser Displays Interactive Web Pages

You first use RTMC Development or RTMC Pro Development to create a project containing the display and/or control components that you want to be available from your website. Next, the Web Publisher is used to publish the web files. From RTMC Pro, you can press the Publish to Web button (🌐) to bring up the Web Publisher and publish your project. The Web Publisher can also be opened from the Windows Start Menu by selecting **All Apps | Campbell Scientific | Web Publisher**. From the Web Publisher, you can choose to add a PC Websites (p. 8) or a Datalogger Websites (p. 11) (a datalogger website requires an RTMC Pro project). After filling in the desired settings, press the **Publish Website** button to publish the content.

> Note: If firewalls exist between your web server (i.e., a PC running CSI Web Server or a web-enabled datalogger) and the target audience of your website(s), the firewalls will need to be configured to allow incoming traffic on the port being used by the web server. (The port used by the CSI Web Server is configured through the CSI Web Server Administrator. The port used by a web-enabled datalogger is configured through DevConfig. The default port is 80 for both the CSI Web Server and a web-enabled datalogger.) See your Network Administrator for help in configuring the firewalls.

For an explanation of setting up the CSI Web Server, watch a video at www.campbellsci.com/videos/rtmc-pro-software-publishing-data ▶. Information on the CSI Web Server begins at the 6-minute mark.

2.1 Supported Web Browsers

CSI Web Server supports the following target browsers:

- Chrome
- Firefox

3. CSI Web Server Administrator

The CSI Web Server Administrator allows you to configure the web server, check the status of the web server, set up user accounts and passwords, and easily browse to sites running on the web server. It can be opened from the Windows Start Menu by selecting **Campbell Scientific | CsiWebAdmin**

3.1 Status

The **Status** tab shows the status of the web server and allows you to browse to sites running on the web server.

If the web server is not running, click on the image to start the web server.

When the web server is running, the version of the web server running will be displayed. The protocol, port, and status (e.g., Protocol HTTP, port 80, status Listening) will also be displayed.

A list of sites provided by the web server will be shown. You can click on any site to browse to that site.

The keys icon (🔑) next to each site can be used to create or edit the .csipasswd file for that site. See Web Security (p. 14) for more information about .csipasswd files and how they control users and their website access rights.

The plus icon (➕) next to "Root" creates a new remote folder. You can then use the keys icon next to the new remote folder to create the .csipasswd file for that remote folder before publishing a website to the folder. See Web Publisher (p. 8) for information on publishing a website to the remote folder.

The trash can icon next to each website can be used to remove the website.

> Note: Only sites published to the web server’s root directory and immediate subdirectories of the root directory will be shown. Sites cannot be published to deeper subdirectories.

3.2 Configuration

3.2.1 Edit Root Permissions

The **Edit Root Permissions** button is used to create or edit the root .csipasswd file. It performs the same function as the keys icon next to Root on the **Status** tab, but can be used to edit the root permissions even when the CSI Web Server is not running. See Web Security (p. 14) for more information on the function of the root .csipasswd file.

3.2.2 HTTP

The **HTTP** tab controls the root directory and HTTP server port that will be used by the CSI Web Server.

HTML Root Directory – The directory that the web server will use to store/serve web pages, scripts, password files, and source description files

HTTP Server Port – The TCP Port on which the HTTP server will listen for unencrypted connections. You may need to change this port if there is already a web server running on this machine or if your firewall does not allow service on TCP port 80.

3.2.3 HTTPS

The **HTTPS** tab can be used to set up the CSI Web Server for encrypted service. This requires a Private Key File and Certificate File obtained from a third party Certificate Authority.

HTTPS Enabled – Specifies whether the web server will attempt to offer an HTTPS (encrypted) service.

Server Name – Specifies the domain name that the server will report when it redirects requests from an unsecure link to a secure one. This will only happen if the HTTPS protocol is enabled and the private key and certificate have valid content. This value should be the Fully Qualified Domain Name (FQDN) for your web server and, depending upon firewalls, proxies, and port-forwarding configurations, may be different from the host machine name.

HTTPS Server Port – Specifies the TCP port on which the HTTPS server will listen for unencrypted connections. You may need to change this port if there is already a web server running on this machine or if your network or personal firewall do not allow service on TCP port 443.

Private Key File – Specifies the name of the PEM encoded file that contains the HTTPS private key. The TLS/SSL stack used by the web server supports only AES128 or AES256 encryption for the private key file.

The private key file should be placed in your C:\CampbellSci\CsiWebServer folder to ensure appropriate user rights.

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

1. The file extension you received it in 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.

Private Key Password – Specifies the password used to decrypt the TLS/SSL private key. It will be ignored if a private key is specified that is not encrypted.

Certificate File – Specifies the name of the PEM-encoded file that contains the x509 HTTPS certificate.

The certificate file should be placed in your C:\CampbellSci\CsiWebServer folder to ensure appropriate user rights.

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

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

   -----BEGIN CERTIFICATE-----

   [*Unreadable Content goes here*]

   -----END CERTIFICATE-----

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

3.2.4 Log Control

The **Log Control** tab allows you to configure how log files are maintained by the CSI Web Server.

Log File Mode – Controls the way that the web server will write its log files. Select **Disabled** to disable log files, **New Log on Time Intervals** to specify that a new log file will be started on the time interval specified by the Baling Interval, or **New Log after Max Size** to specify that a new log file will be started after the current log file exceeds the size specified by the Maximum Log File Size.

Log Files Directory – Specifies the directory in which the web server will write its log files.

Baling Interval – Specifies the maximum time interval that will be recorded in any one log file when the Log File Mode is set to New Log on Time Intervals.

Maximum Log File Size – Specifies the maximum size (in bytes) that will be recorded in any one log file when the Log File Mode is set to New Log after Max Size.

Maximum Log Files Count – Specifies the maximum number of log files that will be kept by the web server before the oldest is overwritten.

Log HTTP Headers – Controls whether the web server will write the headers of HTTP requests and HTTP responses in its log file.

4. Web Publisher

The Web Publisher is a website management tool that lets you customize web content for use with the CSI Web Server or a web-enabled datalogger like the CR1000. Most of the content for each website comes from an RTMC project file (*.RTMC2). In addition, the Web Publisher has display settings that allow you to show other tabs such as data browsing and network status.

4.1 Websites

The Web Publisher supports two different kinds of websites: PC websites and Datalogger websites.

PC Website - PC websites run on the CSI Web Server. The CSI Web Server supports any number of websites and lets you control user access rights for each website. PC websites support all of the different data sources supported by RTMC (LoggerNet, Data File, Database, HTTP Datalogger, and Virtual Data Sources).

Datalogger Website - Datalogger websites run on a compatible HTTP-enabled datalogger such as the CR6 or a CR1000 with an NL121 attached. Datalogger websites must be designed by RTMC Pro and can only have one data source. The data source must be an HTTP Datalogger Source.

Press the **Add** button to add a new website. From the pop-up menu, choose whether you wish to add a PC Website or a Datalogger Website.

4.1.1 PC Websites

PC websites run on the CSI Web Server. The CSI Web Server supports any number of websites and lets you control user access rights for each website. PC websites support all of the different data sources supported by RTMC (LoggerNet, Data File, Database, HTTP Datalogger, and Virtual Data Sources).

Press the **Add** button and select **Add PC Website** to add a PC Website.

You can press the **Rename** button to rename the website. This will be the name shown in the title bar, when the website is accessed.

4.1.1.1 PC Web Server Settings

Host Address - Specifies the address where you will be publishing your website. The address can be localhost (that is, the computer running Web Publisher), a domain name, or an IP address in the form XXX.XXX.XXX.XXX for an IPv4 address or

[XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX] for an IPv6 address. If you are using a port other than the default port (80 for http, 443 for https), you need to specify it using a colon followed by the port. For example, campbellsci.com:8080, 192.168.1.1:1234, or [2620:24:8080:8600:85a1:fcf2:2172:11bf]:8080.

> Note: If the web server has HTTPS enabled (through the CSI Web Server Administrator), it must be specified by adding https:// in front of the IP address or domain name.

User ID - In order to publish a website to the CSI Web Server, a user account must be created with an access level of "all". The CSI Web Server Administrator is used to do this with the CSI Web Server. A .csipasswd file is created that controls user accounts and passwords that will be able to publish projects to the web server and/or access websites on the CSI Web Server. (See Web Security (p. 14) for more information.)

Password - The password associated with the user ID that has been given "all" access to publish websites to the web server.

Remote Folder - The remote folder controls where a website will be published relative to the web server's root directory. (By default, the web server's root directory is C:\Campbellsci\CsiWebServer. It can be changed from the CSI Web Server Administrator.) On the CSI Web Server, you can create as many websites and folders as you want. Each remote folder must be directly below the web server's root directory (i.e., you cannot publish to *remote_folder\subdirectory*). Clicking on the **Remote Folder** drop down list will show you which folders are currently available.

4.1.1.2 Website Settings

Send new password file - If a website has been previously created and user rights set up, you may or may not want to overwrite the existing password file for that website.

Edit Password File - Brings up the website .csipasswd file editor. This file is used by the web server to manage user access to the website.

Edit Tracker Code - Tracker codes can optionally be inserted to track website access. All tracker codes are inserted into a <script> </script> block and are automatically inserted in each page of your website. Google Analytics™ web analytics service and many other tracking services are available for free. The available services range from simple hit counters to enterprise-class web analytic solutions.

Disable Web Sockets - By default, web sockets are used to push data from the web server or datalogger as soon as it becomes available. This is the preferred method. However, some networks do not allow web sockets. Selecting this check box will disable web sockets causing data to be polled by the web browser.

4.1.1.3 RTMC Settings

Project File - The RTMC project file (*.RTMC2) that will be used to generate the website. PC websites support all of the available data sources. When publishing a website, all of the screens, images, and required files are compiled together and automatically copied to the web server.

Default Poll Interval – This setting determines the rate at which data is polled by a web browser on older systems. This setting is somewhat deprecated because of more modern web technologies that have been implemented across many of our products. If you have the latest version of our software, data is now pushed from the web server or datalogger as soon as it becomes available instead of needing to be continually polled.

This functionality is available in:

- CSI Web Server 1.4 or later
- CR1000/CR3000/CR800 Series OS 29 or later
- CR6 Series OS 4 or later

If this functionality is not supported on your system, data will revert to being polled at the **Default Poll Interval**. This means that the browser must ask the web server if it has any new data to be displayed. This setting determines how often new data will be requested. The default poll interval is set to 10 seconds. This setting should be adjusted to provide data at a rate that is suitable for your application. There are many factors that affect how fast data will be able to be polled including the number of users viewing the page, the number of dataloggers being polled, the size of data tables in the dataloggers, the resources available to the web server, the internet browser resources, connection bandwidth, etc.

4.1.1.4 Display Settings

Hide Navigation Tabs - By default, websites will be displayed with navigation tabs at the top of the web page. These tabs allow users to navigate your website. You can disable these tabs and implement your own navigation system using "Hot Spots" in RTMC Pro.

Show data browse tab - The show data browse tab option will display a **Browse Data** tab on your website. This tab allows you to view data from all of your data sources.

It also provides a mechanism to do custom data queries. Custom data queries let you download data files or view data directly in the browser. Each table in the Browse Data tab will have a **Custom** link next to the table name. Click on the link to open the Custom Data Query window and perform a custom data query.

Show network status tab - The show network status tab option will display a **Network Status** tab on your website. When viewing network status on a CSI Web Server, you will see all of your data sources used by the current website. Databases and Data File sources don't currently display any status information. LoggerNet data sources and HTTP Datalogger Sources display a link. When LoggerNet data sources are clicked, all of the stations in the LoggerNet network are displayed with their collection statistics. When an HTTP Datalogger Source is clicked, you see the datalogger status information.

4.1.2 Datalogger Websites

Datalogger websites run on a compatible HTTP-enabled datalogger such as the CR6 or a CR1000 with an NL121 attached. Datalogger websites must be designed by RTMC Pro and can only have one data source. The data source must be an HTTP Datalogger Source.

Press the **Add** button and select **Add Datalogger Website** to add a Datalogger Website.

You can press the **Rename** button to rename the website. This will be the name shown in the title bar, when the website is accessed.

4.1.2.1 Datalogger Web Server Settings

Host Address - Specifies the address where you will be publishing your website. The address can be a domain name or IP address in the form XXX.XXX.XXX.XXX for an IPv4 address or [XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX] for an IPv6 address. If you are using a port other than the default port (80 for http, 443 for https), you need to specify it using a colon followed by the port. For example, campbellsci.com:8080, 192.168.1.1:1234, or [2620:24:8080:8600:85a1:fcf2:2172:11bf]:8080.

> Notes: If the datalogger has only HTTPS enabled with HTTP disabled, it must be specified by adding https:// in front of the IP address or domain name.
>
> CR1000/CR3000/CR800 series dataloggers require OS 28 or later to support IPv6 addresses.

User ID - In order to publish a website to a datalogger web server, a root level user must be created. Device Configuration Utility (DevConfig) is used to do this for a datalogger web server. The .csipasswd file controls user accounts and passwords that will be able to publish projects to the web server. In order to publish, a user account needs to be assigned an access level of "all". This user account with "all" access is called the Root User ID. (See Web Security (p. 14) for more information.)

Password - The root password is the password associated with the root user ID that has been given "all" access to publish websites to the web server.

Remote Folder - The remote folder controls where a website will be published relative to the web server's root directory. On the datalogger web server, you are limited on which folders you have available. Currently you can specify /CPU/, /USR/, or /CRD/, if these directories are available.

Clicking on the "Remote Folder" drop down list will show you which folders are currently available.

4.1.2.2 Website Settings

Send new password file - If a website has been previously created and user rights set up, you may or may not want to overwrite the existing password file for that website.

Edit Password File - Brings up the website .csipasswd file editor. This file is used by the web server to manage user access to the website. On datalogger websites, the .csipasswd file is always placed in the /CPU/ drive automatically.

Hide the password file - The .csipasswd file can optionally be hidden on datalogger web servers. Hiding the .csipasswd file is a security measure that will help protect access to user names and passwords. Once the .csipasswd file is hidden, it will no longer show up in the file system. Republishing the website with this option disabled will cause the .csipasswd file to show up again.

Edit Tracker Code - Tracker codes can optionally be inserted to track website access. All tracker codes are inserted into a <script> </script> block and are automatically inserted in each page of your website. Google Analytics™ web analytics service and many other tracking services are available for free. The available services range from simple hit counters to enterprise-class web analytic solutions.

Disable Web Sockets - By default, web sockets are used to push data from the web server or datalogger as soon as it becomes available. This is the preferred method. However, some networks do not allow web sockets. Selecting this check box will disable web sockets causing data to be polled by the web browser.

4.1.2.3 RTMC Settings

Project File - The RTMC project file (*.RTMC2) that will be used to generate the website. Datalogger websites require an RTMC Pro project that only contains one data source. The data source must be an HTTP Datalogger Source. When publishing a website, all of the screens, images, and required files are compiled together and automatically copied to the web server.

> Note: The HTTP datalogger source in your RTMC project does not need to be specific to the datalogger that the website is published to (e.g., an RTMC project with an HTTP datalogger source at 192.168.4.14 can be published to a datalogger with an IP address of 192.168.9.99). This allows you to create one RTMC project that can be published to multiple datalogger websites.

Default Poll Interval – This setting determines the rate at which data is polled by a web browser on older systems. This setting is somewhat deprecated because of more modern web technologies that have been implemented across many of our products. If you have the latest version of our software, data is now pushed from the web server or datalogger as soon as it becomes available instead of needing to be continually polled.

This functionality is available in:

- CSI Web Server 1.4 or later
- CR1000/CR3000/CR800 Series OS 29 or later
- CR6 Series OS 4 or later

If this functionality is not supported on your system, data will revert to being polled at the **Default Poll Interval**. This means that the browser must ask the web server if it has any new data to be displayed. This setting determines how often new data will be requested. The default poll interval is set to 10 seconds. This setting should be adjusted to provide data at a rate that is suitable for your application. There are many factors that affect how fast data will be able to be polled including the number of users viewing the page, the number of dataloggers being polled, the size of data tables in the dataloggers, the resources available to the web server, the internet browser resources, connection bandwidth, etc.

4.1.2.4 Display Settings

Hide Navigation Tabs - By default, websites will be displayed with navigation tabs at the top of the web page. These tabs allow users to navigate your website. You can disable these tabs and implement your own navigation system using Hot Spots in RTMC Pro.

Show data browse tab - The show data browse tab option will display a **Browse Dat**a tab on your website. This tab allows you to view data from HTTP data source.

It also provides a mechanism to do custom data queries. Custom data queries let you download data files or view data directly in the browser. Each table in the Browse Data tab will have a **Custom** link next to the table name. Click on the link to open the Custom Data Query window and perform a custom data query.

Show file browse tab - The show file browse tab option will display a **Browse Files** tab on a datalogger web server. The file browser allows you to traverse the file system of the datalogger. Each folder is displayed with a link as well as some information about the size of the folder and when the folder was last written to. When clicking on a folder, you will see a list of all the visible files in the directory. Each file is a link, so you can click on the file and view it or download it. The size of the file and last write time are also displayed. Clicking on the [..] link will take you back to the root directory list of the datalogger file system.

Show datalogger status tab - The show datalogger status tab option will display a **Datalogger Status** tab on your website. If you are viewing the website on a datalogger web server, you will see the datalogger status. This includes datalogger information, program information, battery information, and card information.

5. Web Security

Users and their website access rights are controlled through .csipasswd files. Note that .csipasswd files control access to websites as well as direct access to data sources and dataloggers using the API commands described in the manual.

Each user can be given one of the following access levels:

- **None** – No access is allowed. The account is disabled.
- **Read Only** – Allowed to view data. No values can be changed.
- **Read/Write** – Allowed to view data, make changes to writeable values in a datalogger's Public or Status table or a virtual data source, and set a datalogger's clock.
- **All** – Allowed to view data, make changes to writeable values in a datalogger's Public or Status table or a virtual data source, set a datalogger's clock, use the API FileControl command, and publish websites.

5.1 PC Websites

In order to publish a website to the CSI Web Server, a .csipasswd file must be created. The root directory and each remote folder under the root directory can have its own .csipasswd file. This .csipasswd file controls the user accounts and passwords that will be able to publish projects to that directory and controls user access to websites in that directory. In order to publish, a user account needs to be assigned an access level of "all".

If a remote folder does not have its own .csipasswd file, the root .csipasswd file will be used.

For PC Websites, there is a default .csipasswd file which includes two users:

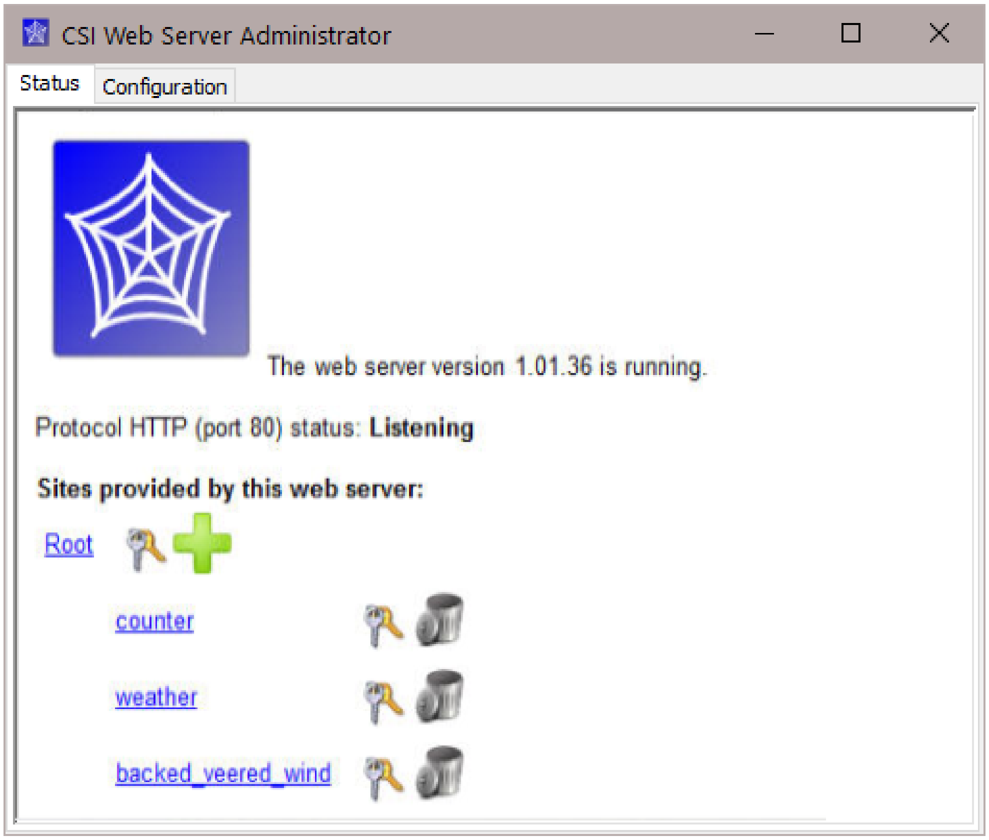
Username: admin
Password: admin
Access Level: All

Username: anonymous
Password:
Access Level: Read Only

If a root .csipasswd file has not been created, this default .csipasswd file will be used for the root directory and any remote folder that does not include its own .csipasswd file, The CSI Web Server Administrator is the preferred method of creating and editing .csipasswd files. They can also be created and edited from the Web Publisher. Both methods are described below.

5.1.1 Using the CSI Web Server Administrator

To create the .csipasswd file in the root directory, press the keys icon next to "Root". To create a .csipasswd file for a new remote folder press the + icon next to "Root", enter a name for the site, and press Add Subdirectory. Once the new subdirectory appears under "Root", press the keys icon next to the subdirectory to create the .csipasswd file for that subdirectory. The key icons can also be used later to edit the .csipasswd files.



The web server version 1.01.36 is running.

Protocol HTTP (port 80) status: **Listening**

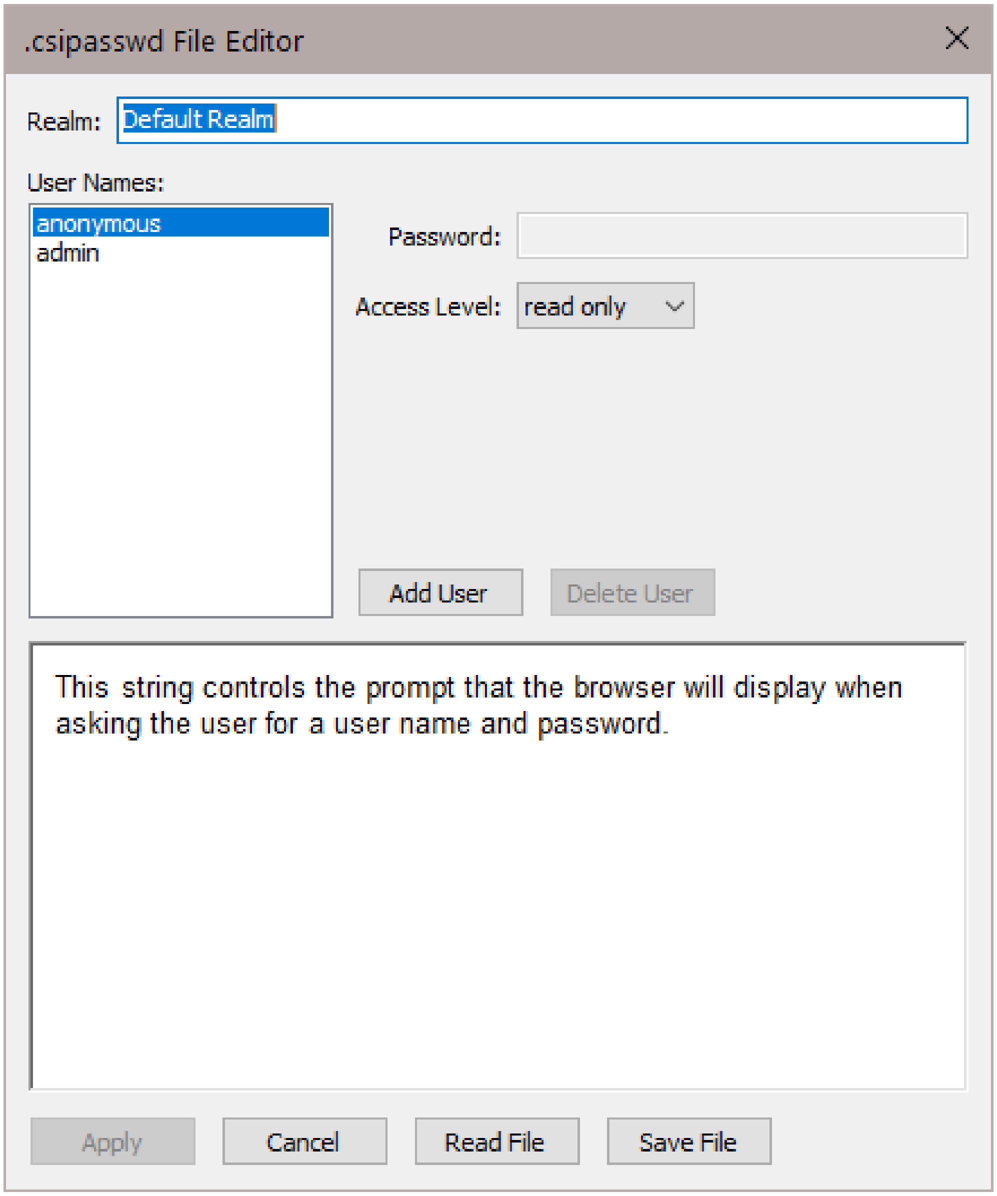
Sites provided by this web server:

Root

counter

weather

backed_veered_wind



.csipasswd File Editor

Realm: Default Realm

User Names:
anonymous
admin

Password:

Access Level: read only

This string controls the prompt that the browser will display when asking the user for a user name and password.

The .csipasswd File Editor dialogue box that is opened when the keys icon is pressed has the following fields:

- **Realm** - The name given to this realm. (A realm is a collection of user names and their access levels.) The name will be used in the prompt the browser displays when asking the user for a user name and password.
- **User Names** - Shows the users that are currently defined in this realm. Press **Add User** to add a new user. Select a user name in the list and press **Delete User** to remove that user.
- **Password** – The password for the selected user.

- **Access Level** – Sets the access level for the selected user.
    - **None** – No access is allowed. The account is disabled.
    - **Read Only** – Allowed to view data. No values can be changed.
    - **Read/Write** – Allowed to view data, make changes to writeable values in a datalogger's Public or Status table or a virtual data source, and set a dataloggers clock.
    - **All** – Allowed to view data, make changes to writeable values in a dataloggers Public or Status table or a virtual data source, set a dataloggers clock, use the API FileControl command, and publish websites.

After defining the desired user names and access levels, click **Apply** to apply the changes. You can also click **Cancel** to discard the changes. Click **Read file** to read a .csipasswd file into the **Website .csipasswd File Editor**. Click **Save File** to save the contents of the **Website .csipasswd File Editor** to a .csipasswd file.

5.1.2 Using the Web Publisher

To create or edit a .csipasswd file from the Web Publisher, select a website from the **Websites** list. You will be creating or editing the .csipasswd file for the subdirectory shown in Remote Folder. If the Remote Folder field is blank, the website is being published to the root directory and you will be editing or creating the root .csipasswd file. Select the **Send new password file** check box and then press the **Edit Password File** button to bring up the **Website .csipasswd File Editor**. Define the user names and access levels you want to be available for this website and press the **OK** button. Press the **Publish Website** button to publish the website and send the new password file.

> Notes: If you are creating a root .csipasswd file from the Web Publisher, you will need to enter the default admin user ID and password described above in the User ID and Password field to publish the website and send the new password file. When the website is published again in the future, you will use an "all" access level user ID and password from the root .csipasswd file to publish to the root directory.
>
> If you are creating a .csipasswd file for a remote folder from the Web Publisher, you will need to enter an "all" access level user ID and password from the root .csipasswd file (or the default admin user ID and password described above if there is no root .csipasswd file) to publish the website and send the new password file. When the website is published again in the future, you will use an "all" access level user ID and password from the remote folder's .csipasswd file to publish to the remote folder.

5.2 Datalogger Websites

Device Configuration Utility (DevConfig) must be used to create the initial .csipasswd file for a datalogger. The .csipasswd file is created by connecting to the datalogger in DevConfig and then pressing the **Edit .csipasswd File** button on the **Net Services** tab. Define the user names and access levels you want to be available and press the **Apply** button. Pressing the **Apply** button sends the file to the datalogger.

Once a .csipasswd file resides on the datalogger, it can be overwritten from the Web Publisher. Select the datalogger website from the **Websites** list. Select the **Send new password file** check box and then press the **Edit Password File** button to bring up the **Website .csipasswd File Editor**. Define the user names and access levels you want to be available and press the OK button. Press the **Publish Website** button to publish the website and send the new password file.

When you press the OK button on the **Website .csipasswd File Editor** dialogue box in Web Publisher, this file is stored to your computer. When you press the **Publish Website** button, this file will be sent to the datalogger and will overwrite the current .csipasswd file. Note that when you press the **Edit Password File** button, you are editing the file stored on your computer, not the one stored on the datalogger. This file does not contain any changes made using DevConfig. Therefore, if you have made changes to the .csipasswd file from DevConfig, they will be overwritten when you press the **Publish Website** button.

6. API Commands

The CSI Web Server supports an HTTP API interface for accessing data from data sources defined in the RTMC projects running on the web server. These commands can also be used to access data directly from dataloggers.

See Web Server/API Commands in the CRBasic Editor help for more information.

INFO

CAMPBELL SCIENTIFIC®
WHEN MEASUREMENTS MATTER

Global Sales & Support Network

A worldwide network to help meet your needs

CANADA
USA
COSTA RICA
UK
GERMANY
FRANCE
SPAIN
CHINA
INDIA
THAILAND
BRAZIL
SOUTH AFRICA
AUSTRALIA
● Campbell Scientific Regional Offices

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: Vincennes, 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

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: Shepshed, 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