



# HTTP Authorization Module Application Guide






## Description

This module allows a Crestron 2-series processor with Ethernet to authenticate user credentials against a web server using the BASIC Authentication schema. When multiple instances of the module are cascaded, as shown in the demonstration program, this module can be used to provide multiple levels of access to a system.

Although this module is expected to work with any HTTP server that supports BASIC Authentication, ControlWorks Consulting is only able to support this module when used in conjunction with Microsoft Windows 2003 R2 server with Internet Information Server. ControlWorks does not provide support for configuration or troubleshooting of any server-side software or software including, but not limited to the operating system or server software.

## Supported Processors

This module will work with all 2-series processors that are equipped with Ethernet

Compatibility			Processor Requirements	
 2-Series Compatible	 NOT CNMSX Compatible	 NOT System Builder Compatible	 Ethernet REQUIRED	 Compact Flash NOT NEEDED

## Processor Ethernet Configuration Information

This module requires one TCP/IP client object to be inserted in the SIMPL Windows Program. This client should be configured with the DNS name or IP address of the server that will be processing the authentication as well as the port number that the server is running on (Typically this would be port 80). This information can be obtained from your network administrator.

Device Settings: Crestron TCP/IP Client

Device Name | IP Net Address | Connection Sheet | Device Info

IP ID: 03

IP ID  
 Remap this IP ID at program upload

Default Address:

.  .  .   Use IP Address  
  Use Host Name

Port:

TCP  
 UDP

OK Cancel Apply

or

Device Settings: Crestron TCP/IP Client

Device Name | IP Net Address | Connection Sheet | Device Info

IP ID: 03

IP ID  
 Remap this IP ID at program upload

Default Address:

10 . 2 . 0 . 231  Use IP Address  
  Use Host Name

Port:

TCP  
 UDP

OK Cancel Apply

The connection to the server is managed by the module; if it is held open, the module will not function properly. Refer to the demonstration program for an example of managing the connection when multiple instances of the module are used.

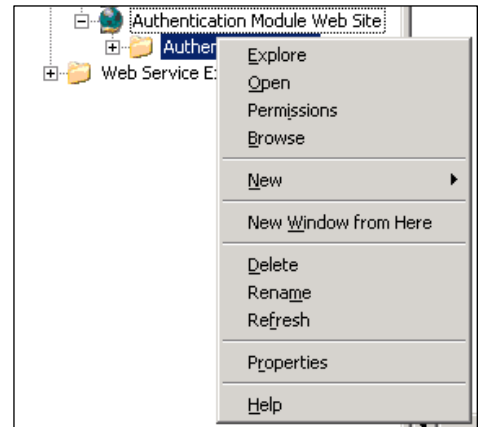
## Server-Side Configuration

This section assumes that Internet Information Server (IIS) on a Windows 2003 R2 Server is being utilized. This document also assumes that you have already set up a website container, directory, or virtual directory for the files containing the authorizations and that you are versed in configuring an IIS Website and file permissions. Should this not be the case, contact your network administrator for additional information on how to execute the server-side configuration for your application.

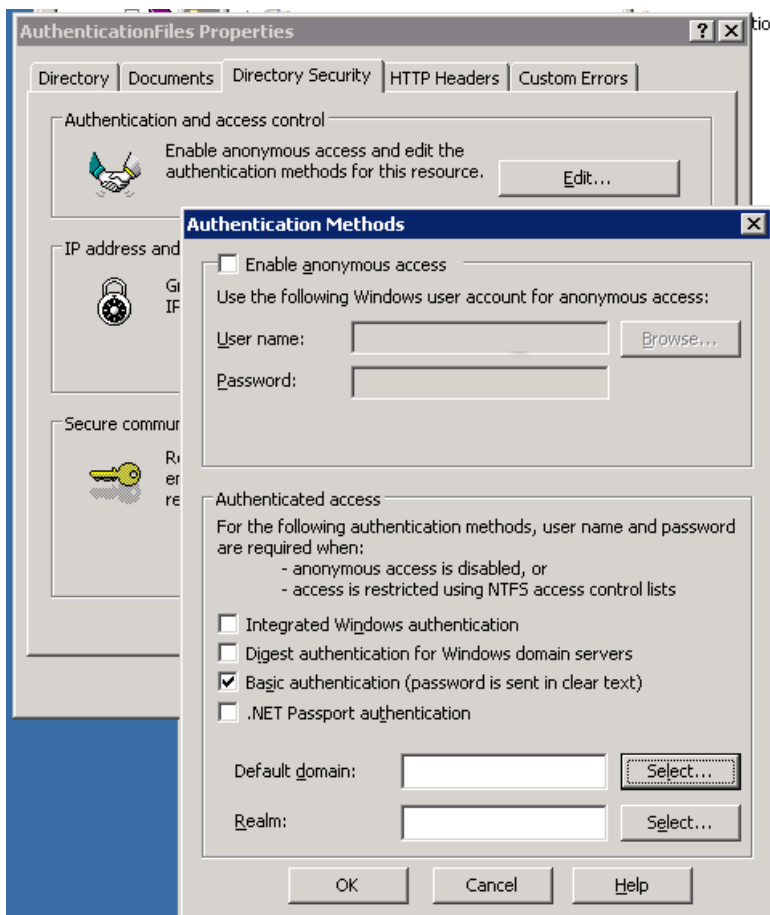
**SECURITY NOTE:** This module uses the HTTP/1.1 BASIC Authentication schema. This schema uses Base64 to encode but not encrypt the username and password for transmission, meaning that the user's password may be discovered using certain network monitoring techniques. The implications of this should be carefully considered if this module is to be utilized across the Internet or another untrusted network. The risk posed can be minimized by placing the Crestron processor(s) and the server performing the authentication on the same network, and/or by employing a switched network topology, VLANs, and/or 802.1x access control. Contact your network administrator or security consultant for additional information.

## Configuring IIS Directory Security

Open the Internet Information Services Manager, then locate the Web Site (or folder within the web site) that will contain the authorization files. Right click this object then choose properties. (**Note:** It is recommended that these file be located in a separate directory than other files hosted on the same server).



Once the Properties dialog is open, choose the Directory Security Tab then click the "Edit..." button under Authentication and Access Control header. Ensure that the "Enable Anonymous Access", "Integrated Windows Authentication", "Digest Authentication for Windows domain servers", and ".NET Passport authentication" checkboxes are not checked, and that the "Basic authentication (password is sent in clear text)" checkbox is checked.



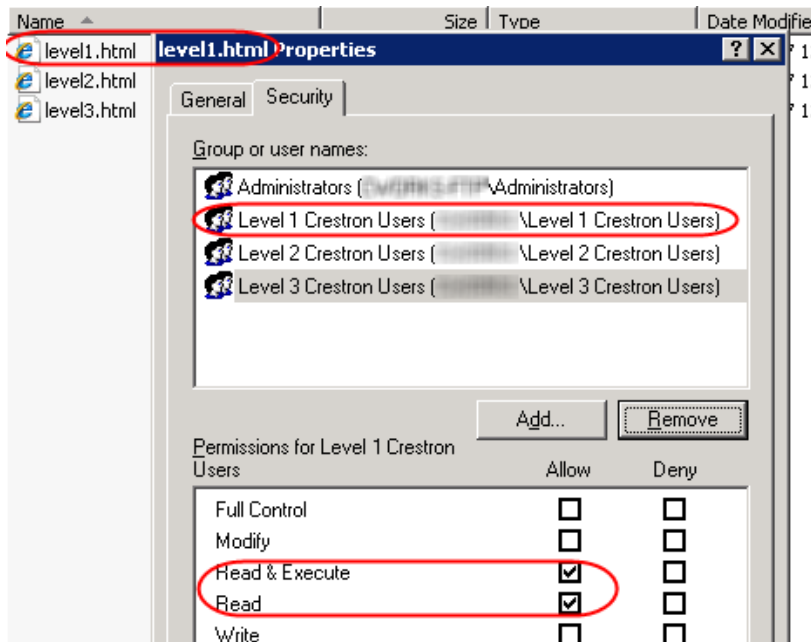
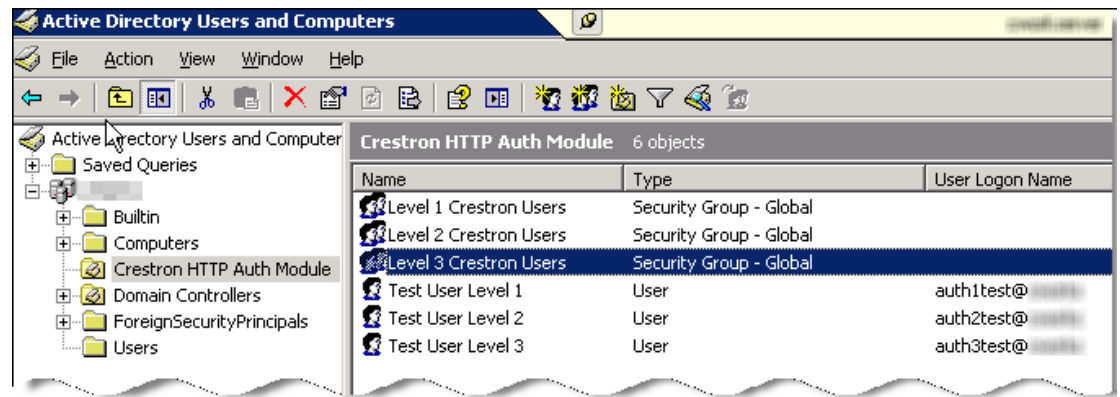
The name of the Windows domain that the majority of users will be authenticating against should be entered in the "Default Domain" text box, while the "Realm" text box may be left empty.

Once these settings have been verified, click "OK" to close the Authentication Methods dialog box then click "OK" to close the properties dialog box.

## Configuring File Permission

The next step will be to assign permissions to the files that will be authorized. ControlWorks suggests that a security group be created for each level of access desired. Then, simply grant each group permissions to access the file with the corresponding authorization level and ensure that other users (for example 'Everyone') do not have permission to access the files.

For example, if you have three authorization levels, as shown in the demonstration program included with the module, you would typically have three files (for example, level1.html, level2.html, and level3.html). You would also have three security groups (for example, Level 1 Crestron Users, Level 2 Crestron Users, and Level 3 Crestron users).



In this scenario, "Level 1 Crestron Users" would be granted Read access to the "level1.html" file, "Level 2 Crestron Users" would be granted Read access to the "level2.html" file (plus, potentially, the "level1.html" file if desired as a failsafe), and so on.

### Testing the Configuration

Finally, make sure that users are assigned to the proper groups, then test the configuration by attempting to open the URL in Internet Explorer. If the configuration is correct, you will receive a username and password prompt. Only after

entering the username and password of a user who has been assigned permissions should the text of the file be displayed.

If the text of the file is displayed *without* being prompted for a username and password, check to ensure that the "Integrated Windows Authentication" and "Enable Anonymous Access" checkboxes on the Authentication Methods dialog are unchecked (see previous page).

If the text of file is displayed after being prompted for a username and password, or if the file is not displayed after entering a correct username and password, then ensure that the file permissions and group memberships (if applicable) are correct. The module will not function properly until you can verify that the file will be loaded by a standard Internet Browser. ControlWorks will be unable to support the module until this level of functionality can be verified.

## HTML File Creation and Formatting

---

This module determines access level by reading a specially tagged HTML file. Unless otherwise specified, there is a limit of 254 characters within a tag and text will be output exactly as entered (that is, HTML tags will not be processed). All fields are optional and do not need to be specified if not used. The tags recognized by the module are:

<code>&lt;html&gt;...&lt;/html&gt;</code>	Used to define the beginning and end of the HTML file. The <code>&lt;/html&gt;</code> tag must be present in the file to be properly processed. There is a limit of 65,500 characters between these tags.
<code>&lt;auth_name&gt;...&lt;/auth_name&gt;</code>	The name of the authorization represented by the file. The module will represent text exactly as entered on the [authorization_name\$] serial output
<code>&lt;auth_detail&gt;...&lt;/auth_detail&gt;</code>	Typically a brief description of the type of access represented. The module will represent this text exactly as entered on the [authorization_detal\$] serial output.
<code>&lt;auth_params&gt;...&lt;/auth_params&gt;</code>	Used to define the parameters of the authorization; typically a string formatted as needed to be processed by external logic . Refer to the demonstration program for one example. The module will represent this text exactly as entered on the [authorization_string1\$] serial output.
<code>&lt;auth_params1&gt;...&lt;/auth_params1&gt;</code>	This field is identical in function to the <code>&lt;auth_params&gt;</code> tag. If both tags are present in the file, only the <code>&lt;auth_params&gt;</code> tag will be processed.
<code>&lt;auth_params2&gt;...&lt;/auth_params2&gt;</code>	This field provides an additional 254 characters, if needed, for the authorization string. The module will represent this text exactly as entered on the [authorization_string2\$] serial output.
<code>&lt;auth_params3&gt;...&lt;/auth_params2&gt;</code>	This field provides an additional 254 characters, if needed, for the authorization string. The module will represent this text exactly as entered on the [authorization_string3\$] serial output.
<code>&lt;auth_valid&gt;...&lt;/auth_valid&gt;</code>	A number between 0 and 65535 (without commas or other punctuation) specifying the period of time that the authorization is valid for. Depending on the programming, this may be number of seconds, minutes, hours, or even days. Typically this would be used to drive logic to automatically log a user out after a period of time.

While these tags may be used within an HTML file containing other tags, ControlWorks recommends that when possible these tags be used in a HTML file free from other tags, as larger files will reduce the performance of the module and may have an impact on the performance of the entire Crestron program. A sample file, in its entirety is shown below for reference:

```
<html>
<auth_name>Level 1 Authorization</auth_name>
<auth_detail>For higher level access, contact classroom support at x. 1234</auth_detail>
<auth_params>DVD=YES,VCR=YES,VTC=NO,PROJ=YES,ATC=NO,AUX=NO,SCREEN=YES,DOC=NO</auth_params>
<auth_valid>60</auth_valid>
</html>
```

## Module Application

---

This module can be applied in several ways depending on the desired results

### Basic Access Control

For basic access control, for example, simply granting or denying access to the entire system one instance of the module may be used. In this case, connect the tcp\_rx\$, tcp\_tx\$, tcp\_connected\_fb, and tcp\_connect signals on the module directly to the TCP/IP client used to establish the connection. Pulsing the "login\_now" digital input after entering a username, password, and optionally a domain will attempt to log the user in.

### Tiered Access Control

For tiered access control, for example if there is a "Beginner", "Intermediate" and "Advanced" level of access to the system, use one instance of the module for each module and connect the tcp\_rx\$, tcp\_tx\$, tcp\_connected\_fb, and tcp\_connect signals to the TCP/IP client as described for "Basic Access Control"; these signals are internally buffered and may be jammed.

This example is illustrated in the demonstration program included with the module.

In this case, the same username, password, and domain serials would be connected to all modules; the "Login" button on the touchpanel would be connected to the highest level of access, in this example "Advanced", and the "authorization\_failure\_fb" output would be connected to the login\_now input on the next highest level of access and so forth.

Note that because logins are attempted sequentially the more levels of access there are, the longer the potential delay before a login attempt completes.

### Parallel Access Control

For parallel access control, for example, if separate files will control access to various aspects of the system you may either use multiple TCP/IP clients with each instance of the module connected to its own TCP/IP client or you may sequence login attempts using one TCP/IP client.

In this case, the specific implementation will largely on the specific needs present in your application, but can often be thought of as simply multiple uses of the "Basic Access Control" scheme within the same program.

# Signal And Parameter Descriptions

Bracketed signals such as "[signal\_name]" are optional signals

## DIGITAL INPUTS

tcp\_connect\_fb..... Connect this signal to the "Connect\_F" output of the TCP/IP client symbol.

http\_login\_now ..... Pulse this input after entering a username and password to begin a login attempt.

## ANALOG INPUTS

This module does not utilize any analog inputs.

## SERIAL INPUTS

tcp\_rx\$ ..... Connect this signal to the RX\$ output of the TCP/IP client symbol

username\$ ..... Connect this signal to the username keyboard logic

password\$ ..... Connect this signal to the password keyboard logic

[domain\$] ..... Optional. Connect this signal to the domain keyboard logic.

## DIGITAL OUTPUTS

tcp\_connect..... Connect this signal to the "Connect" input on the TCP/IP client symbol. This signal is jamable.

authorization\_success\_fb..... This output is pulsed when the authorization attempt is successful, and indicates that the authorization data on the serial outputs is valid.

authorization\_failure\_fb..... This output is pulsed when the authorization attempt fails (typically as a result of a 403 error response).

[authorization\_undetermined\_fb] ..... This output is pulsed when the module is unable to determine if the authorization attempt has succeeded or failed. Typically, this is generated when the connection is successful but the module receives a status response other than 200 or 403.

[timeout\_expired\_fb] ..... This output is pulsed when the timeout has expired without either establishing a connection or receiving a response

## ANALOG OUTPUTS

[authorization\_duration] ..... Value of the <auth\_valid> parameter in the loaded file.

## SERIAL OUTPUTS

[authorization\_name\$] ..... Value of the <auth\_name> parameter in the loaded file.

[authorization\_details\$] ..... Value of the <auth\_detail> parameter in the loaded file

[authorization\_string1\$...3\$] ..... Value of the <auth\_params1> through <auth\_params3> parameters in the loaded file.

## **PARAMETERS**

Path.....	The URL of the file to load without the host name (for example, to load <a href="http://www.whatever.com/folder/file.html">http://www.whatever.com/folder/file.html</a> enter /folder/file.html)
Host .....	Host name header, used if multiple virtual hosts are on the same server usually similar to <a href="http://www.whatever.com">www.whatever.com</a>
Timeout .....	Amount of time, in seconds, that the module will wait to establish a connection and process a file before pulsing the timeout_expired_fb output.

# Support

---

This module is supported by ControlWorks Consulting, LLC. Should you need support for this module please email [support@controlworks.com](mailto:support@controlworks.com) or call us at 440-449-1100. ControlWorks normal office hours are 9 AM to 5 PM Eastern, Monday through Friday, excluding holidays.

Before calling for support, please ensure that you have loaded and tested operation using the included demonstration program and touchpanel(s) to ensure that you understand the correct operation of the module. It may be difficult for ControlWorks to provide support until the demonstration program is loaded.

Updates, when available, are automatically distributed via Email notification to the address entered when the module was purchased. In addition, updates may be obtained using your username and password at <http://www.thecontrolworks.com/customerlogin.aspx>.

## Distribution Package Contents

---

The distribution package for this module should include:

HTTP_Authorization_v1.umc.....	Crestron User Module
Base64 Encode Engine V1.usp .....	SIMPL+ file used within the module\
Base64 Encode Engine V1.ush .....	SIMPL+ header file
HTTP_authorization_engine_v1.usp .....	SIMPL+ file used within the module
HTTP_authorization_engine_v1.ush .....	SIMPL+ header file
Serial_To_Star_String.usp .....	SIMPL+ file used in demonstration program
Serial_To_Star_String.ush .....	SIMPL+ header file
http_authorization_demo_v1.smw .....	Demonstration program
http_authorization_help_v1.smw .....	This help file

## Revision History

---

V1 lincoln@controlworks.com 2007.06.16

Initial release

## Development Environment

---

Version 1 of this module was developed on the following hardware and software. Different versions of hardware or software may or may not operate properly. If you have questions, please contact us.

### Hardware

Crestron PRO2 Processor	v3.155.1243
-------------------------	-------------

### Software

Crestron SIMPL Windows	Version 2.08.38
Crestron Vision Tools Pro-e	Version 3.5.0.7
Crestron Database Version	18.7.8
Crestron Symbol Library	Version 472
Crestron Device Library	Version 472

# ControlWorks Consulting, LLC Software License Agreement

---

## Definitions:

*ControlWorks*, *We*, and *Us* refer to ControlWorks Consulting, LLC, with headquarters located at 701 Beta Drive, Suite 22 Mayfield Village, Ohio 44143-2330. *You* and *Dealer* refer to the entity purchasing the module. *Client* and *End User* refer to the person or entity for whom the Crestron hardware is being installed and/or will utilize the installed system. *System* refers to all components described herein as well as other components, services, or utilities required to achieve the functionality described herein. *Module* refers to files required to implement the functionality provided by the module and may include source files with extensions such as UMC, USP, SMW and VTP. *Demo Program* refers to a group of files used to demonstrate the capabilities of the Module, for example a SIMPL Windows program and VisionTools Touchpanel file(s) illustrating the use of the Module but not including the Module. *Software* refers to the Module and the Demo Program.

## Disclaimer of Warranties

ControlWorks Consulting, LLC software is licensed to You as is. You, the consumer, bear the entire risk relating to the quality and performance of the Software. In no event will ControlWorks Consulting, LLC be liable for direct, indirect, incidental or consequential damages resulting from any defect in the Software, even if ControlWorks Consulting, LLC had reason to know of the possibility of such damage. If the Software proves to have defects, You and not Us must assume the cost of any necessary service or repair resulting from such defects.

## Provision of Support

We provide limited levels of technical support only for the most recent version of the Module as determined by Us. We do not provide support for previous version of the module, modifications to the module not made by Us, to persons who have not purchased the module from Us. In addition, we may decline to provide support if the Demo Program has not been utilized. We may withdraw a module from sale and discontinue providing support at any time and for any reason, including, for example, if the equipment for which the Module is written is discontinued or substantially modified. The remainder of your rights and obligations pursuant to this license will not be affected should ControlWorks discontinue support for a module.

## Modification of Software

You may not decrypt (if encrypted), reverse engineer, modify, translate, disassemble, or de-compile the Module in whole or part. You may modify the Demo Program. In no event will ControlWorks Consulting, LLC be liable for direct, indirect, incidental or consequential damages resulting from You modifying the Software in any manner.

## Indemnification/Hold Harmless

ControlWorks, in its sole and absolute discretion may refuse to provide support for the application of the Module in such a manner that We feel has the potential for property damage, or physical injury to any person. Dealer shall indemnify and hold harmless ControlWorks Consulting LLC, its employees, agents, and owners from any and all liability, including direct, indirect, and consequential damages, including but not limited to personal injury, property damage, or lost profits which may result from the operation of a program containing a ControlWorks Consulting, LLC Module or any component thereof.

## License Grant

Software authored by ControlWorks remains the property of ControlWorks. ControlWorks grants You the non-exclusive, non-transferable, perpetual license to use the Software authored by ControlWorks as a component of Systems programmed by You. This Software is the intellectual property of ControlWorks Consulting, LLC and is protected by law, including United States and International copyright laws. This Software and the accompanying license may not be transferred, resold, or assigned to other persons, organizations or other Crestron Dealers via any means.

**The use of this software indicates acceptance of the terms of this agreement.**

Copyright (C) 2009 ControlWorks Consulting, LLC All Rights Reserved – Use Subject to License.  
US Government Restricted Rights. Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraphs (a)-(d) of FAR 52.227-19.