

BB4-8422 System - Settings

Network

Default Settings

When the device is initially booted, eth0 will default to a static IPv4 address of 10.0.0.101. Eth1 will be set dynamically by your DHCP server on your network.

Interface	Default IP
eth0	10.0.0.101
eth1	DHCP/Dynamic

Network Settings

Dashboard / System / Network

⚙️ eth0

Mode	static
IPv4 Address	192.168.1.60
Netmask	255.255.255.0
Gateway	192.168.1.1
Nameservers: Comma separated	8.8.8.8
<input type="submit" value="Submit"/>	

Mode	static
IPv6 Address	2603:b050:4723:0:d25f:b8ff:fe89:1
Netmask	64
Gateway	2603:b050:ffff:ff4:7fff:ffff:ffff:ff89
Nameservers: Comma separated	2001:4860:4860::8888,2001:4860:
<input type="submit" value="Submit"/>	

Transmit
Bytes: 86928099
Packets: 308136

Receive
Bytes: 34492928
Packets: 390781

Current status:
(Changes applied on reboot)



IPv4 Address: 192.168.1.60
IPv6: 2603:b050:4723:0:d25f:b8ff:fe89:11db
MAC Address: D0:5F:B8:9C:AB:B0

Each device has two Ethernet ports called "eth0" and "eth1" on the device (eth0 illustrated above, both are available on the Networks page). The Ethernet ports support both IPv4 and IPV6. To change port settings, select Mode from the list. If static is selected, enter the IP address, netmask, and gateway. Then click Submit. Changes apply upon reboot of the IoTServer.



IMPORTANT: You cannot put both Ethernet ports on the same subnet. When there are 2 interfaces on the same subnet there is no assurance as to which interface will be used to transmit traffic and the machine will accept traffic for either IP on either interface. This is because in Linux the IP address belongs to the host and is not associated with the interface.

User List

Dashboard / System / Users

 Users
Add a user 

Show entries Search:

Username ↑↓	↑↓
admin	
joe.smith	
Username	

Showing 1 to 2 of 2 entries

User information table

Local user credentials are stored on the device. Each local user will be listed in the "System->Users" page. On this page, existing users can be deleted and created. By clicking on a user, you can further edit the properties of the local user. Note that for SNMPv3, the term "user" may apply to another machine wishing to query the IoTServer or send traps to the IoTServer.

Add User

① Add new user

Username:

Password:

Local users can be added on the User List page. To add a user, supply the required username and password. The user will be added to the user list upon completion.

IMPORTANT: Users can have different roles. After creating a new user, you must edit these roles (i.e. Access web interface) before the user can be utilized in the intended fashion. This can be done by clicking on the username.

Editing New and Existing Users

Once a user has been created, the user parameters can be edited by clicking on the username in the user list. Further instructions are provided for editing users on the [User Settings](#) page.

RADIUS Settings

① Radius Authentication for Web Users (optional)

Radius server:

Shared secret:

Radius authorization type:

RADIUS (Remote Authentication Dial in User System) is a commonly used method of maintaining large lists of users that change frequently. Our devices support utilizing RADIUS servers for authentication.

To enable RADIUS logins, go to System->Users and fill in the Radius Server, Shared secret, and Radius authorization type for your server. Once those have been created, users will be able to check "Login via RADIUS" on the login screen. They will then be authenticated by your own RADIUS server.

We support all major types of RADIUS servers including FreeRadius and Microsoft Server with Active Directory.

Radius Server	Address or domain name of your RADIUS server
Shared secret	This is the shared secret password established by your RADIUS server. This device will use the shared secret as a means of logging in to the server.
RADIUS Authorization Type	All major protocols for RADIUS authorization are supported, these include: <ul style="list-style-type: none"> • PAP • CHAP • MSCHAP • MSCHAPv2

User Settings

[Dashboard](#) / [System](#) / [Users](#) / [Edit user](#)

 [Edit User](#)

Local users can be edited by choosing their name from the list found in System->Users, or they can edit themselves by clicking on "User Settings" in the top right corner of any web page.

Username:	joe.smith
Optional for password changes:	
Password:	****password***
Repeat:	*****repeat*****
Access permissions:	<input checked="" type="checkbox"/> Web <input type="checkbox"/> SNMP MIB (Agent) <input type="checkbox"/> SNMP Trap Receiver

A password and username can be set on this page. Users will be assigned access permissions, or "roles," as well. A user that logs into the local web interface would be required to have "Web" permissions.

Modbus User Settings

Modbus Settings	
Modbus register number display format:	modicon ▼

Every local user has the option of setting the display settings for Modbus registers. The user can select:

- Address
- Number
- Modicon

Once a local user selects a format, all Modbus registers will be formatted as such throughout the web UI.

SNMP Settings

Access permissions: Web SNMP MIB (Agent) SNMP Trap Receiver

SNMP Settings

Authentication type: MD5 ▾ Authentication Passphrase: MyAuthPhrase

Privacy type: DES ▾ Privacy Passphrase: MyPrivPhrase

Trap receiver only

Engine ID:

Any user that will be accessing the IoTServer using SNMPv3 will require additional settings for authentication and privacy. Those are provided here. The definition of "user" can include other machines that wish to query the MIB in the IoTServer. **IMPORTANT:** Use a passphrase of at least 10 characters. A very short phrase will be rejected by the encryption algorithm and be indicated as an encryption error.

Access permissions: Web SNMP MIB (Agent) SNMP Trap Receiver

SNMP Settings

Authentication type: MD5 Authentication Passphrase: MyAuthPhrase

Privacy type: DES Privacy Passphrase: MyPrivPhrase

Trap receiver only

Engine ID: 0x800000000300c0b7eb4e1

Update

Any device that will be sending SNMPv3 traps to this IoTServer will require its own user credentials. In addition to the authentication and privacy settings required for any SNMPv3 user, the trap receiver user must also include the Engine ID of the device that will be sending traps to this IoTServer. If all credentials including Engine ID do not match, then the received trap will be discarded.

Other Notes

Note: Users logging in via RADIUS will not have the opportunity to edit their profiles. In this case, they are defaulted to web only users with a default Modbus number display format. Passwords and usernames are controlled by the registered RADIUS server.

Logs

Dashboard / System / Logs

Logs

Select list:

chan7_err_log

Showing log file: chan7_err_log

```

csiSnmpClient on channel 7 start at: 2019-05-01 02:31:49
Wed May 1 02:31:49 2019 Chan 7 SNMP Client active on all ports, primary.
Wed May 1 02:32:21 2019 Configuration loaded from /home/customer/configs/snmpc11.xml.
Wed May 1 02:32:21 2019 SNMP client configuration load complete.

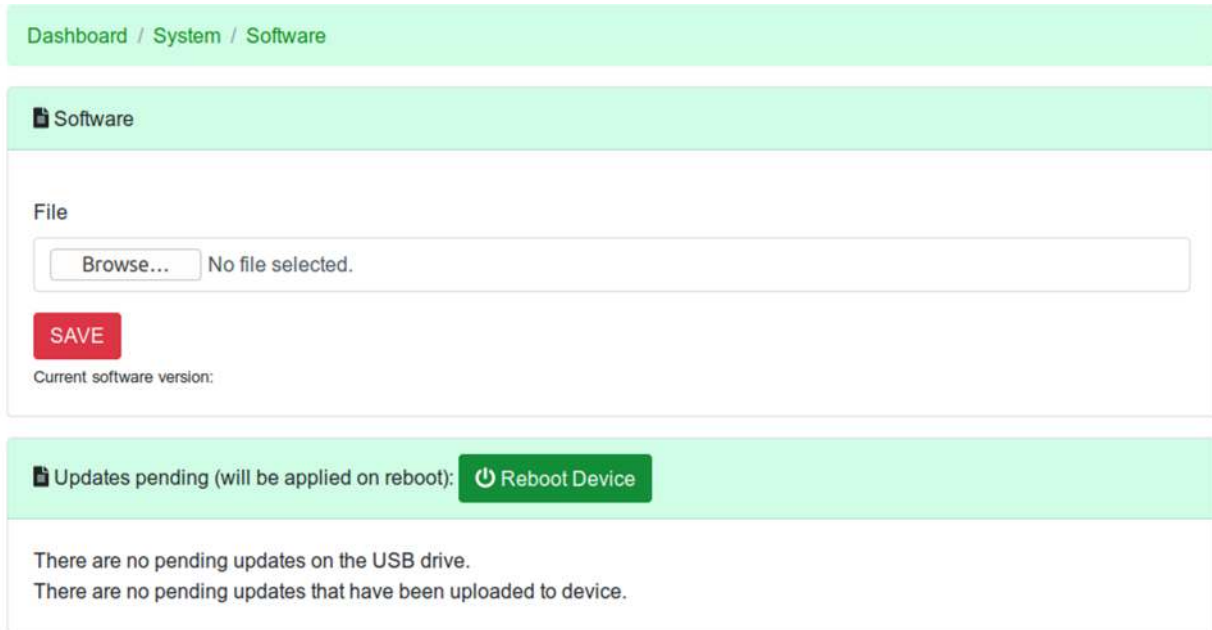
```

Every task will log key events and errors to its own log file. Certain key functions will have log files with recognizable names, but most will have a name like "chan7_err_log". The number appended to "chan" is the task number. You can correlate this with the task list under Task Status or Task Configuration. The log files are primarily a trouble shooting aid.

All files in the logs directory will be included in the drop-down list at the top of the page. Simply select the file you want to see and it will be displayed.

Software

From time to time, you may need to update the software on this device. Control Solutions provides two easy methods for the device to access and install an update.



Update via Upload Form

To get to the upload page, simply go to "System->Software" in the navigation menu on the device. Once the update file has been uploaded to your device, you simply need to reboot the device to cause the update to be applied.

Update via USB Drive

If an update package is found on the USB drive at startup, it will be automatically applied. Simply copy the provided update package to a USB drive, insert the drive and power up the device.