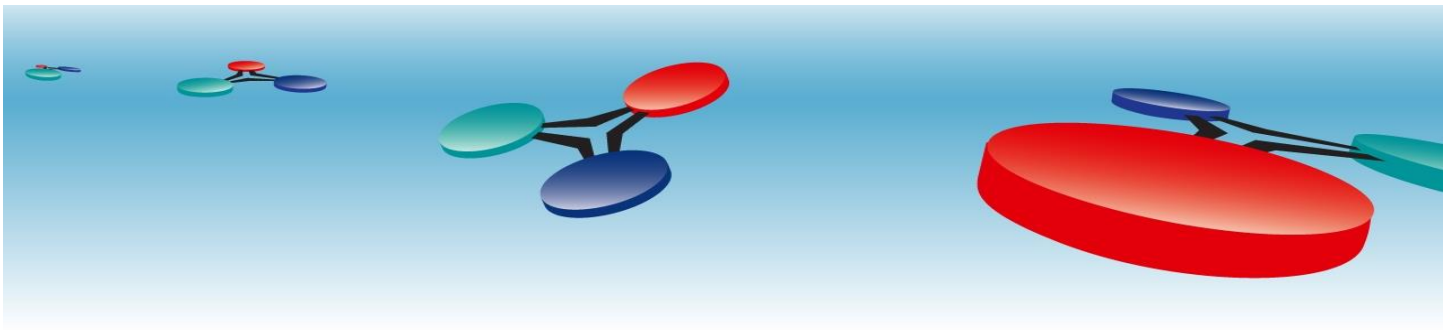


Cimetrics Inc.

SbC3200 BACnet Network Segmentation Device (BNSD)

Supporting BACnet/IP, MS/TP, and BACnet/SC

User's Manual

August 2024

© 2024, Cimetrics Inc.

Contents

Introduction: Who is this manual for?

This manual is written for engineers and technicians who are responsible for the design, installation, and configuration of BACnet-based building automation systems.

To successfully configure the SbC3200's BACnet routing functionality, you will need to be familiar with the following terminology and concepts, at a minimum:

TCP/IP terminology
IP address
IP subnet
Network mask
Default gateway
UDP port
Hostname, path, and URL (used by BACnet/SC)

BACnet terminology
BACnet Device Instance Number (a.k.a. "Device ID")
BACnet Device Name (a.k.a. "Device Name")
BACnet Network (a.k.a. "BACnet LAN")
BACnet Network Number
BACnet Router
BBMD (BACnet Broadcast Management Device) – see **Appendix: What does a BBMD do?**
BACnet/IP
BACnet MS/TP
BACnet Secure Connect (a.k.a. "BACnet/SC")

A good source of information about BACnet is the website of BACnet International.

What does a SbC3200 BACnet Network Segmentation Device (BNSD) do, and why is it used?

Many BACnet-based building automation system (BAS) installations contain more than one BACnet network. BACnet network segmentation devices (BNSDs) are used to selectively route BACnet messages between BACnet networks, allowing the creation of a BACnet internetwork.

BACnet/IP employs the UDP protocol (IETF RFC 768) to enable interoperable communication of BACnet messages over IP (Internet Protocol) networks, typically using Ethernet as the data link technology. Since the release of its specification in 1999, BACnet/IP has become increasingly popular even for relatively low-cost BAS devices. In addition to BACnet/IP, the SbC3200 supports the following:

- BACnet MS/TP, the original BACnet datalink technology for connecting low-end field devices using RS-485 twisted-pair bus wiring.
- BACnet Secure Connect (BACnet/SC), a secure datalink technology that creates encrypted connections between BAS devices using industry standard network protocols (TCP, TLS, HTTPS, WebSocket).

As BACnet Secure Connect requirements increase in buildings, all the BACnet MS/TP and BACnet/IP networks that connect to the new BACnet/SC networks **MUST** be connected to those BACnet/SC networks using a BNSD.

The Secured by Cimetrics™ SbC3200 BNSD supports many of today's and tomorrow's network segmentation requirements. Using BACnet routing, it can:

- Connect a BACnet/IP network to a BACnet MS/TP network
- Connect a BACnet/SC network to a BACnet MS/TP network
- Connect a BACnet/SC network to a BACnet/IP network

When sites start deploying BACnet/SC networks, the customers will not need to replace the SbC3200 BNSDs installed in the field that were routing between BACnet MS/TP and BACnet/IP networks. The SbC3200 can be reconfigured to use BACnet/SC instead of (or in addition to) BACnet/IP.

The SbC3200 BNSD has an optional **BACnet Firewall** that can be configured to restrict the forwarding of certain types of BACnet traffic. In a typical deployment that includes one or more BACnet/SC networks, a Secured by Cimetrics Appliance (SbC4000) monitors the SbC3200's BACnet Firewall to detect and diagnose network and security issues. The SbC3200 BNSD segments the networks, and optionally monitors and enforces policy on BACnet messages flowing between BACnet MS/TP, BACnet/IP and BACnet/SC network segments.

See the following diagrams for simple examples of the deployment of the SbC3200 in a BACnet-based building automation network.

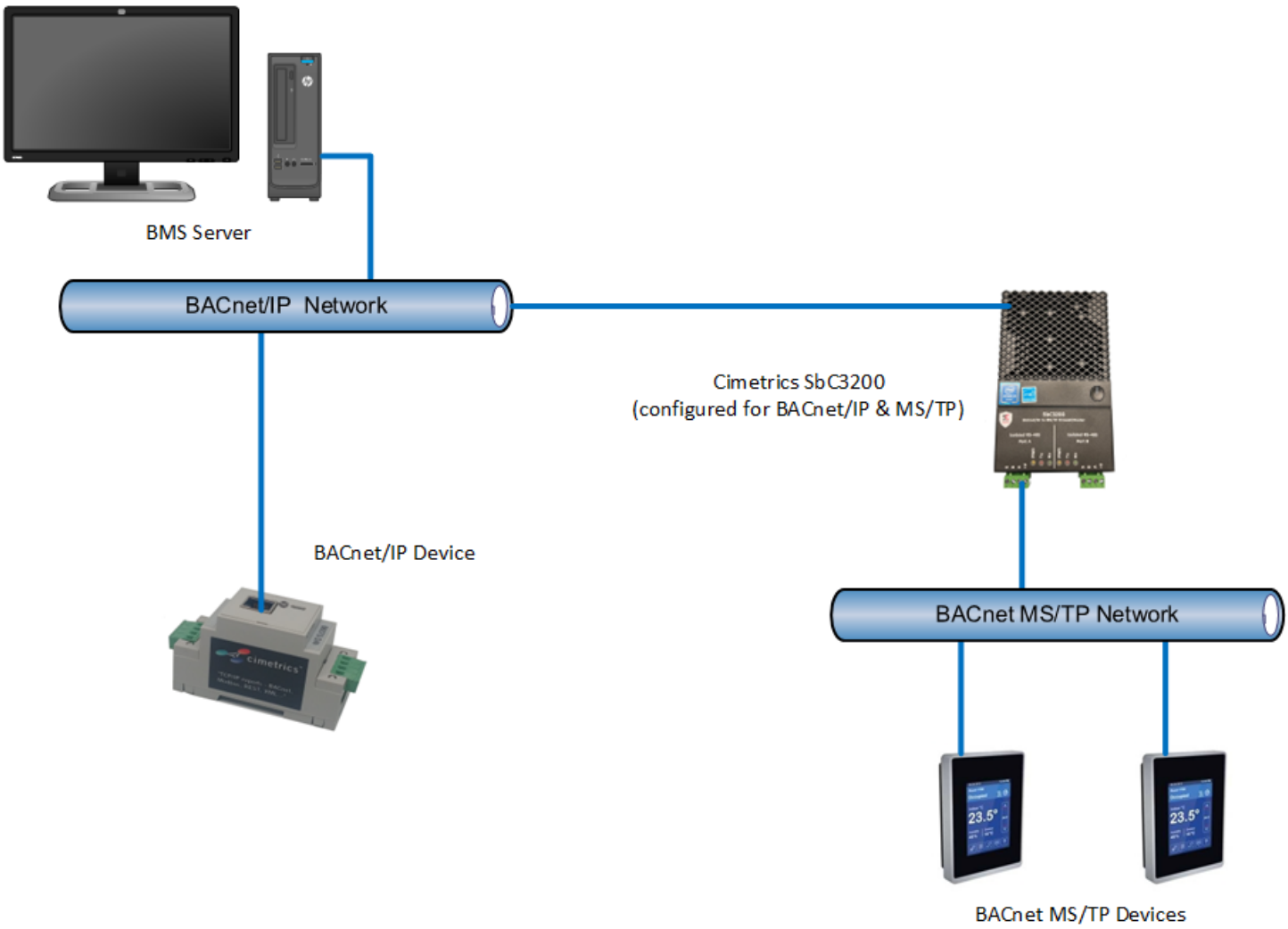


Figure 1: A BACnet internetwork consisting of a BACnet/IP network and an MS/TP network connected through a Cimetrics SbC3200

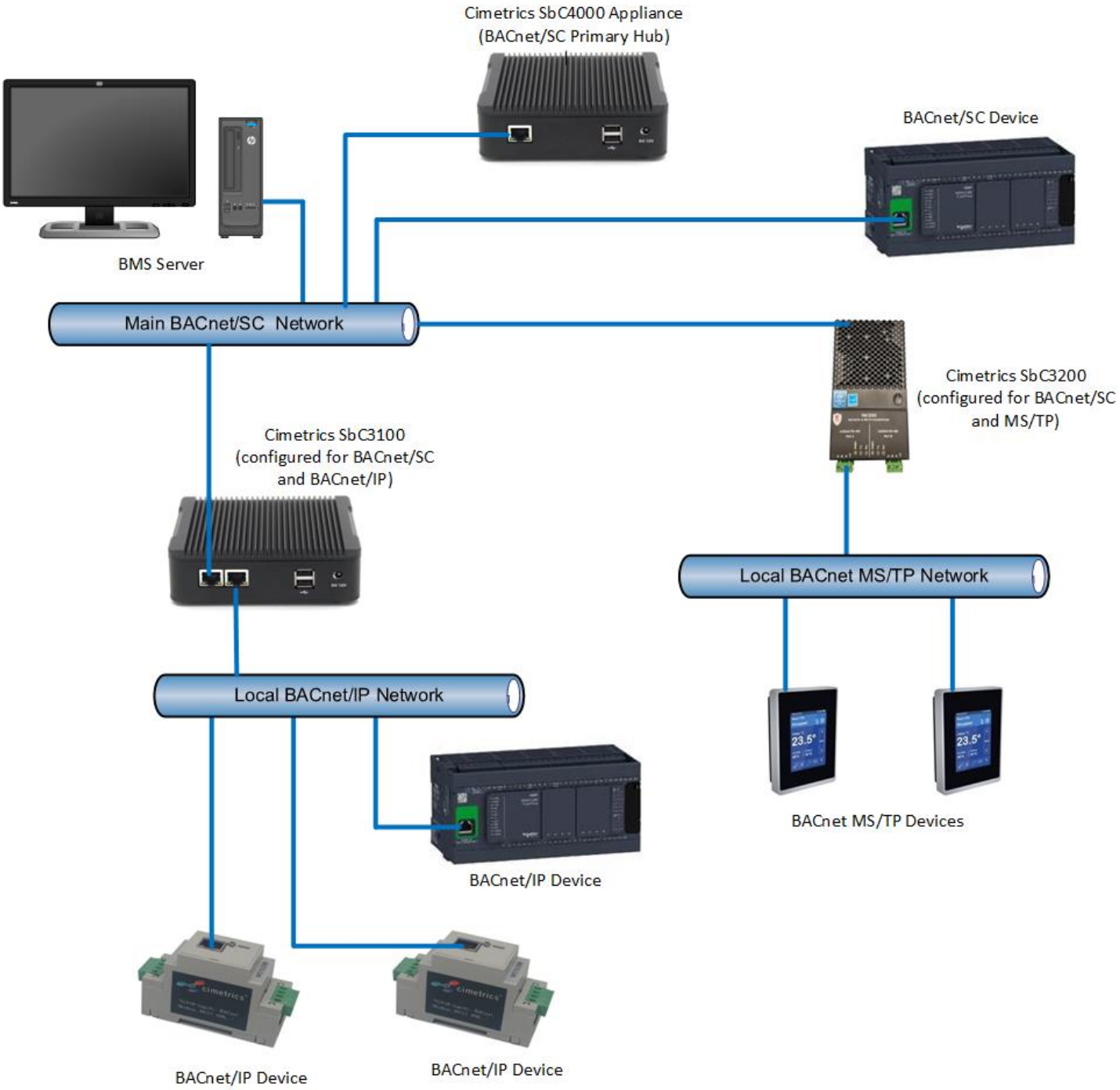


Figure 2: A BACnet internetwork consisting of BACnet/SC, BACnet/IP, and MS/TP networks

SbC3200 Functionality Overview

The SbC3200 BNSD has one Ethernet port for BACnet/IP and BACnet/SC communications and two distinct ports for BACnet MS/TP communications. In this document, we typically refer to those ports as the "BACnet/IP port", "BACnet/SC port" and "BACnet MS/TP ports". Also, the Ethernet port is used for local device configuration, and in that context, it is referred to as the "Configuration Port".

The SbC3200 also has several features that supplement the core BACnet routing functionality. These features are summarized below, and there is additional information later in this document.

Additional BACnet Functionality

The SbC3200 is a BACnet Device, as defined in the *BACnet Standard*. The Device Object instance number (a.k.a. "Device ID") and the Device Object name (a.k.a. "Device Name") are configurable.

BACnet packet capture is also supported for both BACnet/IP and BACnet/SC protocols, and the packet capture files created by the SbC3200 can be imported into software tools such as Wireshark. This feature is disabled by default, but it can be enabled by the administrator.

An optional BACnet firewall can be enabled and configured.

Non-BACnet Functionality

The SbC3200 includes functionality that is designed to make it easier to manage, monitor, and secure the SbC3200, including the following:

1. An internal syslog client can forward logged events to an external syslog server.
2. An internal NTP client can retrieve the current date and time from an external NTP server.
3. An internal DHCP client can communicate with a DHCP server to configure the SbC3200's IP address, network mask, default gateway address, the NTP servers' addresses, and the DNS server's IP address.
4. The factory default private key and TLS certificate used by the built-in web server can be replaced.

Note that this additional functionality is optional. It can be enabled by the administrator using the SbC3200 web-based configuration interface.

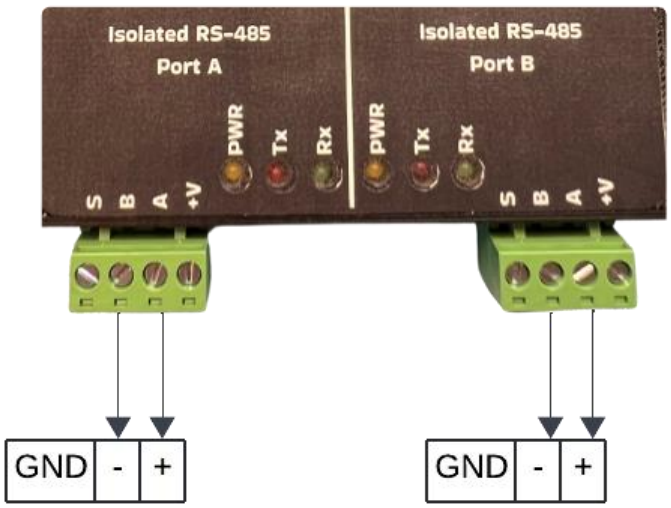
The SbC3200 Hardware

The SbC3200 product consists of the following hardware:

- A small-form-factor computer with one Ethernet port for BACnet/IP and BACnet/SC communication and two ports dedicated for BACnet MS/TP communication.
- An AC-to-DC power adapter
- An AC power cord for the power adapter that is suitable for use in the U.S. and Canada.

BACnet MS/TP physical interface

The SbC3200 has two distinct RS-485 ports that can be connected to MS/TP networks. Their RS-485 transceivers are optically isolated from the rest of the SbC3200. There are internal 10 kiloohm bias resistors connected to each RS-485 transceiver's "A" and "B" terminals. A typical wiring connection to two MS/TP networks is shown in the diagram below. The "S" terminal is for an optional shield connection.



NOTE: Use standard grounding principles for GND.

Limited Warranty

Cimetrics warrants that the supplied SbC3200 hardware is free from defects in materials and workmanship, and that the SbC3200 will perform substantially in accordance with the applicable datasheet, under normal and proper use, for two (2) years from the date the SbC3200 is delivered to the Buyer. This warranty will be void if, in Cimetrics' reasonable opinion, the defect was caused by (a) improper handling, configuration, operation, or testing by anyone other than Cimetrics; (b) failure to install or maintain the SbC3200 in accordance with the current edition of any applicable safety code or Cimetrics' written instructions; (c) modification or alteration by anyone other than Cimetrics; (d) Force Majeure events or acts of vandalism, sabotage, or hacking; or (e) any other cause outside of normal usage in accordance with Cimetrics' written instructions and/or specifications. Cimetrics' liability for breach of this warranty will be limited to replacement, repair, or refund, in Cimetrics' sole discretion, of a defective SbC3200 that has been properly stored, configured, installed, used, and maintained by Buyer, and has not been damaged in transit. All terms hereof (except the limitation of liability in the preceding sentence) are subject to Buyer's return of the defective SbC3200 to Cimetrics without further damage, subject to confirmation of any claimed defect by Cimetrics' inspection. The SbC3200 that Buyer considers defective must be returned per Cimetrics' standard Return Material Authorization (RMA) procedures.

Basic SbC3200 Software Configuration

Before you start

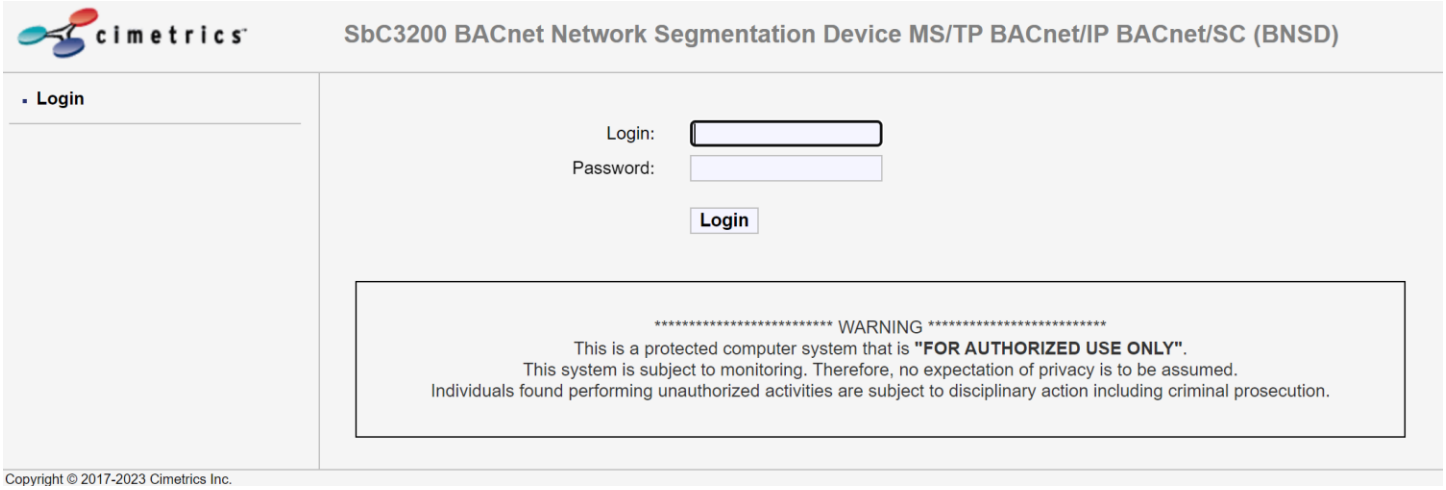
Before configuring and installing the SbC3200, please ensure that you have the following:

- The SbC3200 box.
- The SbC3200's power adapter and an appropriate power cord.
- An Ethernet cable to connect your PC to an Ethernet switch or to the SbC3200's Ethernet port.
- The SbC3200 quick start document, which includes a basic configuration checklist.

You will need to gather the necessary data about your planned installation. Refer to the configuration checklist in Quick Start and to this User's Manual for information about configuring the SbC3200.

Configuration Interface Overview

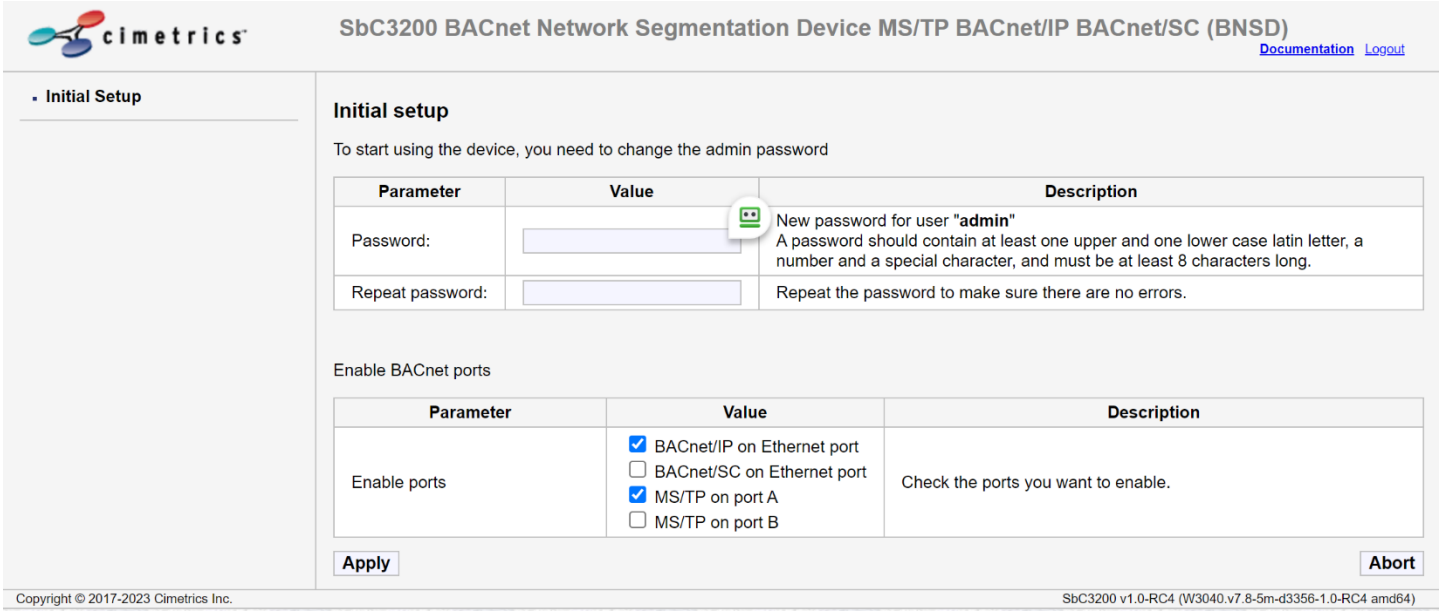
Follow the instructions in the SbC3200 Quick Start document to set up your PC to communicate with the SbC3200's configuration port, and then connect the PC and the SbC3200's configuration port using an Ethernet cable. Enter the IP address of the SbC3200's configuration port in your web browser (169.254.14.14) to access the login page, and if all is well then you should see a login screen like the following:



Enter the login "admin" and the factory default admin password that is written on the label affixed to the bottom of your SbC3200. Note that the "admin" account is always enabled.

You will be required to change the password for the "admin" account upon first use, and the new password must meet the complexity requirement that is displayed. On the same page you can select the BACnet ports to be enabled. You can also enable or disable a port later, by checking a box on an appropriate configuration page. The new password is saved and selected BACnet ports are enabled when "Apply" button is pressed.

> Even if you lose the "admin" password, you can reset the SbC3200 to factory default settings and recover the factory default admin password using the procedure described in section **How to reset to factory default settings if the admin password is unknown**.



After you apply the configuration by clicking on the Apply button, the device reboots and you will see the login page again: Once you have successfully logged in with the new password, you will see the home page which shows basic information about the SbC3200:

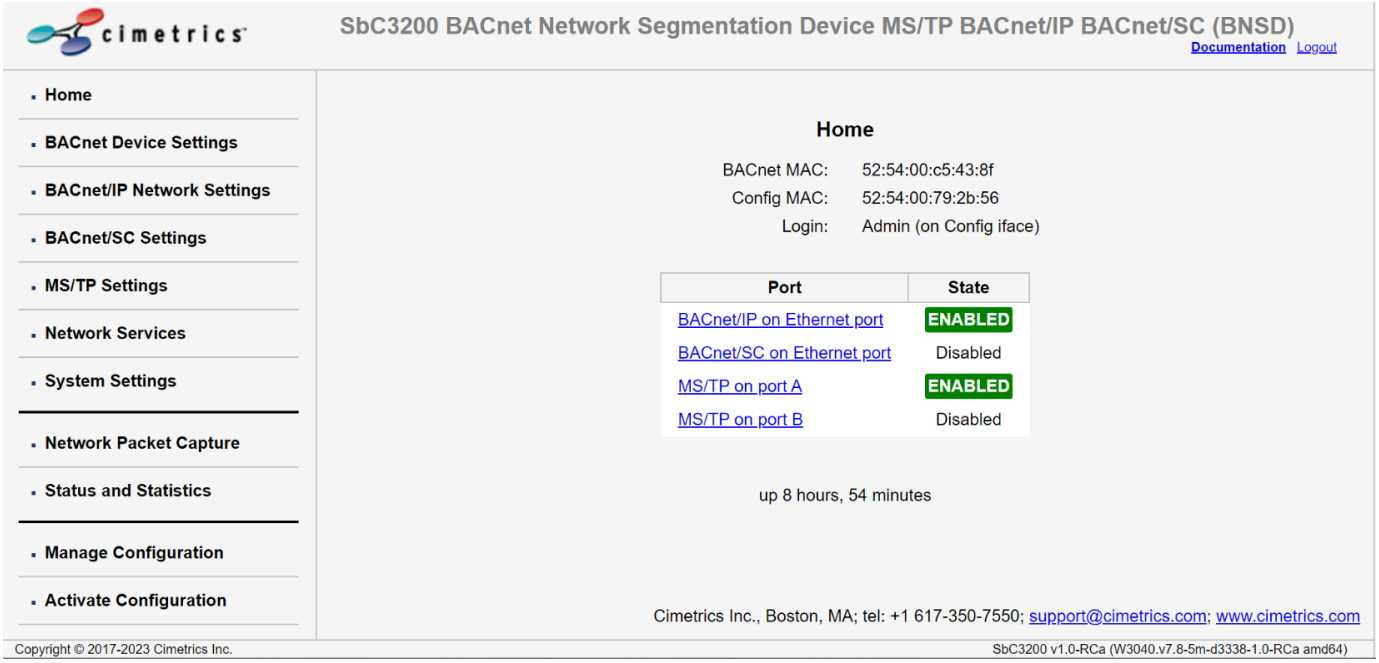


Figure 3: Configuration Home Page

To select a specific web page, click on the corresponding menu item on the left side of the window below the Cimetrics logo. After you have finished modifying the configuration parameters on a page, click the "OK" button on the bottom of the page to accept your changes.

After you finish making changes to the SbC3200's configuration, select "Activate Configuration" from the menu to store your changes on the SbC3200's non-volatile memory and reboot.

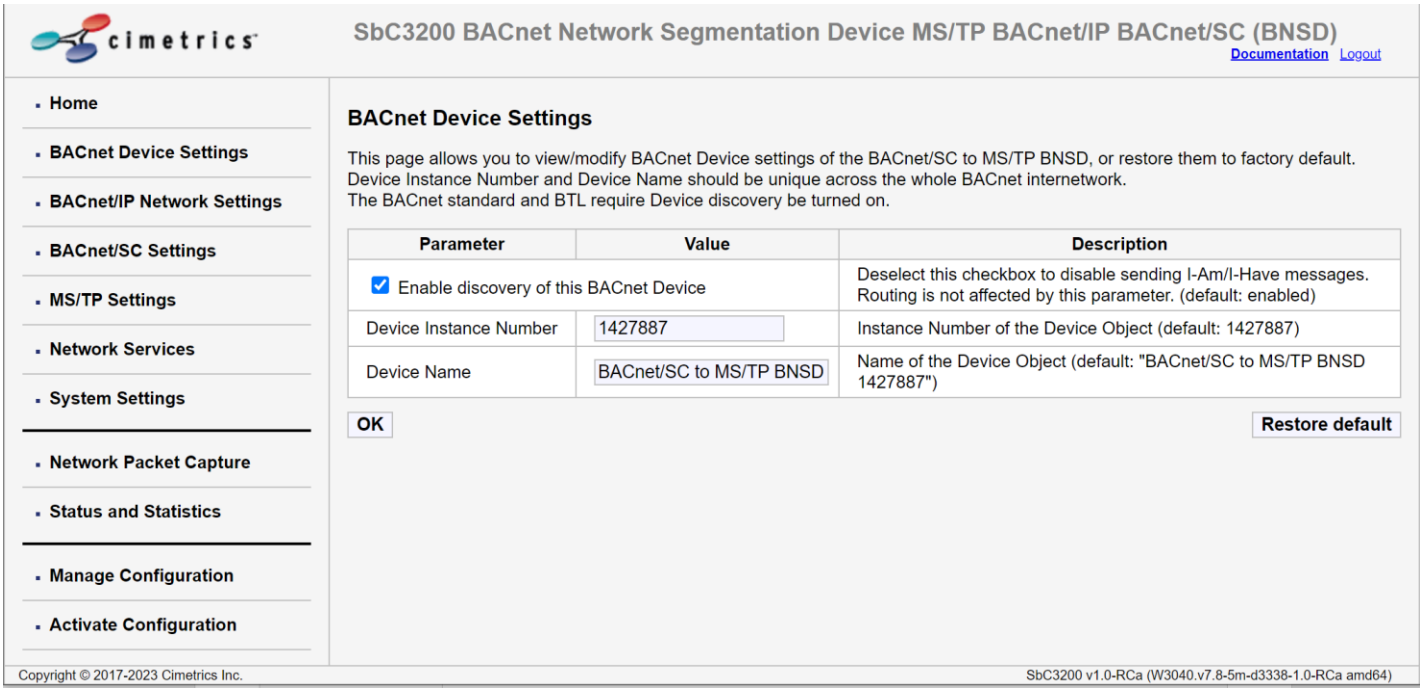
BACnet Device Settings

The SbC3200 contains a basic BACnet Device that will respond to a few BACnet service requests. See the SbC3200's BACnet PICS document for a list of the supported BACnet services.

The default BACnet Device Instance Number is derived from the MAC address of the physical interface, and the default BACnet Device Name is derived from the default Device Instance Number. If you want to change these values, you can do so on the BACnet Device Settings web page, and please remember to click on the "OK" button to accept your changes before you move to a different web page.

> Note that the *BACnet Standard* requires that each BACnet Device have a Device Instance Number and the Device Name that are unique across the entire BACnet internetwork to which the Device is connected. It is the responsibility of the system integrator to configure all the BACnet Devices accordingly.

Enable discovery of this BACnet Device: When device discovery is disabled, the SbC3200 does not respond to Who-Is and I-Have requests. This violates requirements in the *BACnet standard*, but it is sometimes useful when debugging, specifically, when dealing with misconfigured networks in which two or more devices share the same Device ID or Device Name. Discovery should be disabled only temporarily, when troubleshooting the network setup.



BACnet/IP Settings

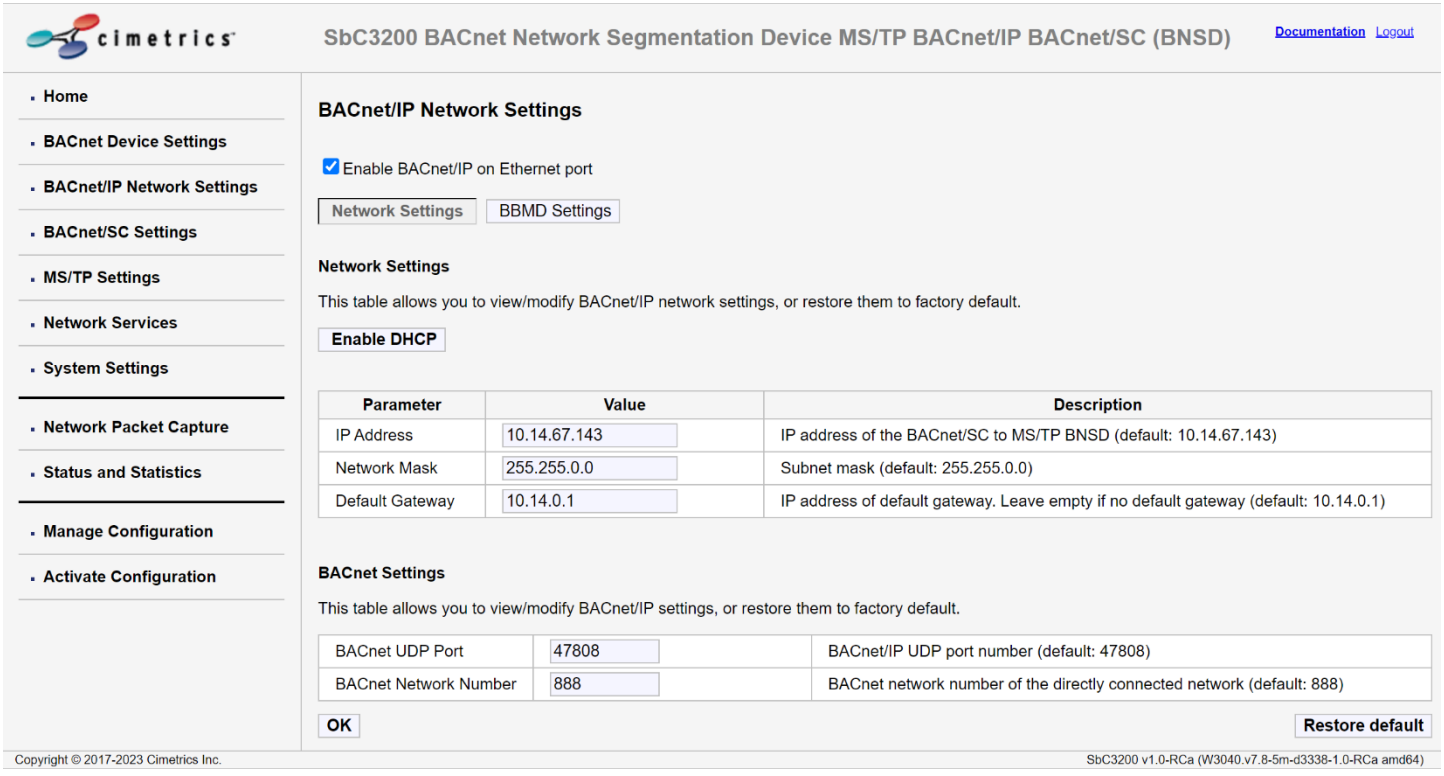
The SbC3200 has one Ethernet port that can be used for BACnet/IP or BACnet/SC communication. The IP protocol configuration is done on the BACnet/IP Network Settings web page.

The SbC3200's port used for BACnet/IP and BACnet/SC communication must be assigned a valid IP address and network mask that are appropriate for the IP networks to which the ports will be directly connected. It can be configured with static IP protocol settings, and in most cases this will be appropriate. It can also be configured to use DHCP to obtain certain network settings if the IP network to which it is connected has a DHCP server.

> Note: Although the SbC3200 can be configured to use DHCP to obtain an IP address and other network parameters, the product is a BACnet anchor point used to maintain the integrity of the building automation network. As such, the stability of this product in the IP network environment is critical. For reliable system operation, the SbC3200's BACnet ports need to be assigned *unchanging* IP addresses and (if required) unchanging DNS names. If DHCP is used, ask the administrator of the DHCP server for a "DHCP Reservation" for the SbC3200. To provide a reserved DHCP-assigned IP address, IT will need the Ethernet MAC address of the SbC3200 .

The Default Gateway parameter must be configured if a SbC3200 port is connected to an IP network that consists of multiple IP subnets and if the SbC3200 should be able to communicate with any device on any other subnet.

In the BACnet Settings, the "BACnet UDP Port" typically has the value 47808. The system integrator is responsible for choosing unique BACnet Network Numbers for each of the BACnet networks in a system, chosen from the range 1 to 65,534. Each of the SbC3200's enabled BACnet ports must be configured with the BACnet Network Number that was chosen for the BACnet network to which the port is connected.



Please remember to click on the "OK" button to accept your changes before you move to a different web page.

BBMD Settings for BACnet/IP

The BBMD function can be enabled on the Ethernet port if BACnet/IP is enabled.

The most complex configuration parameter in a BBMD is the Broadcast Distribution Table ("BDT"), which contains the list of BBMDs (identified by each BBMD's IP addresses and UDP port) that will receive forwarded BACnet/IP broadcasts from this BBMD, as well as the SbC3200's own IP address. In most cases (when the broadcast distribution mask is 255.255.255.255 and the target BBMD's UDP port used for BACnet/IP is 47808) you will only need to type in the target BBMD's IP address. If the target BBMD uses a port other than 47808 then you will need to include that port as well as the target BBMD's IP address; for example, "10.14.1.15:47809" indicates that the BBMD at IP address 10.14.1.15 is using UDP port 47809 for BACnet/IP. It is rare that a broadcast distribution mask other than 255.255.255.255 would be used today, so accepting that default value is recommended. For more information about BBMDs please refer to **Appendix: What does a BBMD do?**

The Enable Foreign Device Registration option should only be enabled if Foreign Devices need to use this BBMD to relay broadcast messages on their behalf. If enabled, the BBMD will accept a valid BACnet/IP Foreign Device Registration request from any device.

> Note: Connecting a SbC3200 so that it is accessible from the Internet or from an untrusted network is not recommended unless appropriate cybersecurity precautions are in place, and this is especially true if the Foreign Device Registration option is enabled.

Please remember to click on the "OK" button to accept your changes before you move to a different web page.

Advanced BBMD Configuration Parameters

Advanced BBMD configuration parameters can be accessed by clicking on "Advanced" near the bottom of the BBMD Settings web page. These advanced parameters rarely need to be modified.

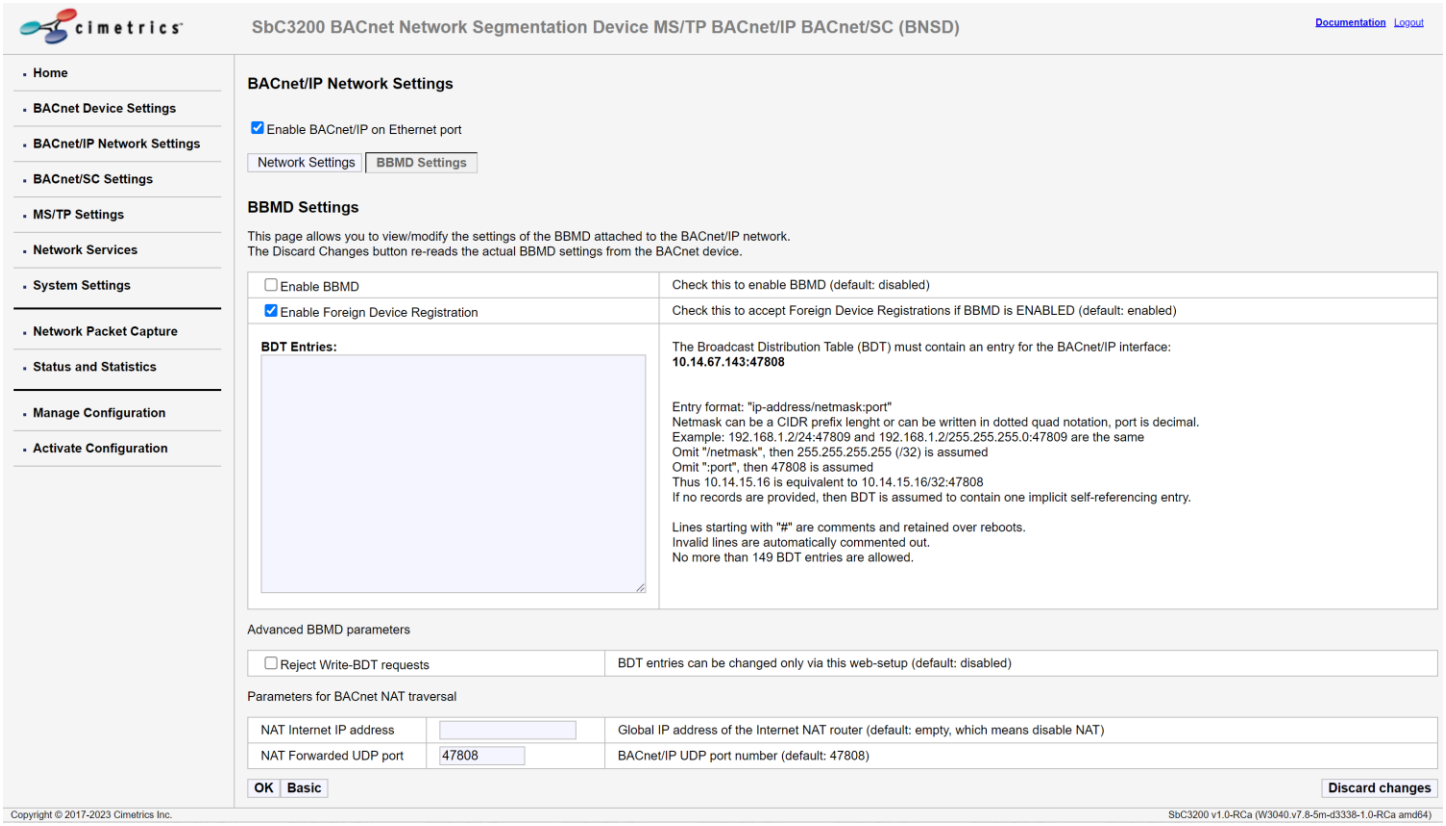
Reject Write-BDT requests

The *BACnet Standard* defines an interoperable method for modifying the Broadcast Distribution Table of a BBMD over the network using a specific BACnet/IP message, Write-Broadcast-Distribution-Table. For security or reliability, it may be desirable to disable the processing of that message, thus preventing other BACnet devices from modifying the SbC3200's Broadcast Distribution Table using this message, although disabling such processing is not in conformance with the *BACnet Standard*. To disable processing of the BACnet/IP Write-Broadcast-Distribution-Table message, select "Reject Write-BDT requests"; processing is enabled by default.

Parameters for BACnet NAT traversal

A SbC3200 with the BBMD function enabled can be configured to communicate using BACnet/IP through an IP network address translation (NAT) router, but this requires careful network design and configuration

of the SbC3200. Please refer to clause J.7.5, “BBMD Operation with Network Address Translation,” in the *BACnet Standard* for details.



BACnet/SC Settings

The SbC3200 has one Ethernet port that can be used for BACnet/IP and BACnet/SC communication. You can enable or disable BACnet/SC on the Ethernet port on the BACnet/SC Settings web page. The IP address and related IP protocol parameters for both BACnet/IP and BACnet/SC are configured on the BACnet/IP Settings web page, and the current values of those settings are displayed at the top of the BACnet/SC Settings web page.

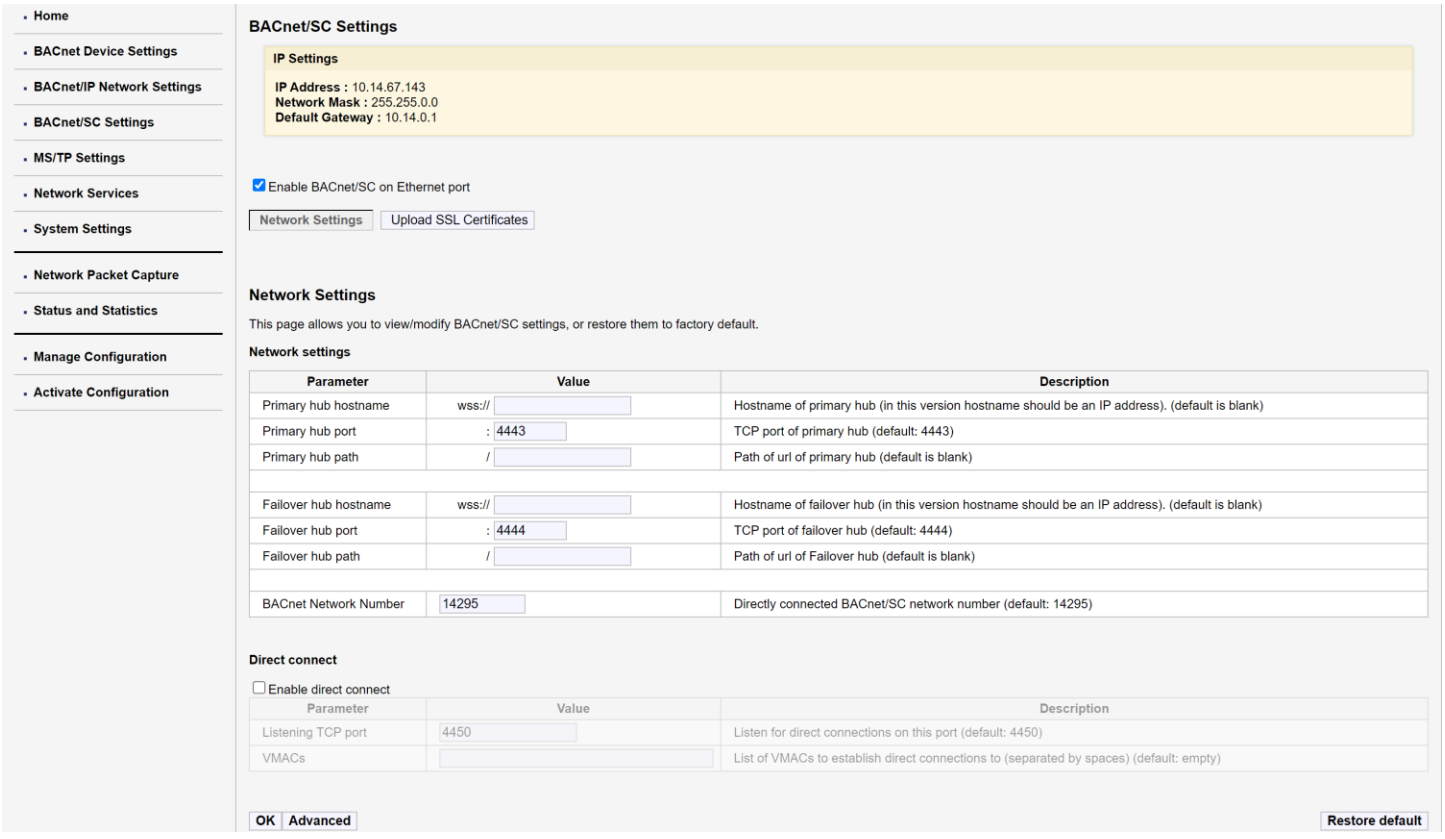
BACnet/SC relies on accurate time to determine whether operating certificates are valid. If BACnet/SC is enabled, you should also enable network-based time synchronization if an NTP server is available.

BACnet/SC Network Settings

The network settings that are specific to BACnet/SC are configured on the BACnet/SC Settings web page, Network Settings tab. If BACnet/SC is enabled, at a minimum you will need to configure the following:

1. The IP address or hostname of the BACnet/SC primary hub for the BACnet/SC network.
2. The TCP port used by the BACnet/SC network's primary hub for BACnet/SC communication.
3. The BACnet network number that has been assigned to the BACnet/SC network.
4. A private key and BACnet/SC certificates (see **BACnet/SC Certificates** for details).

If a failover hub will also be present on the BACnet/SC network, you will need to configure its IP address or hostname as well as its TCP port.

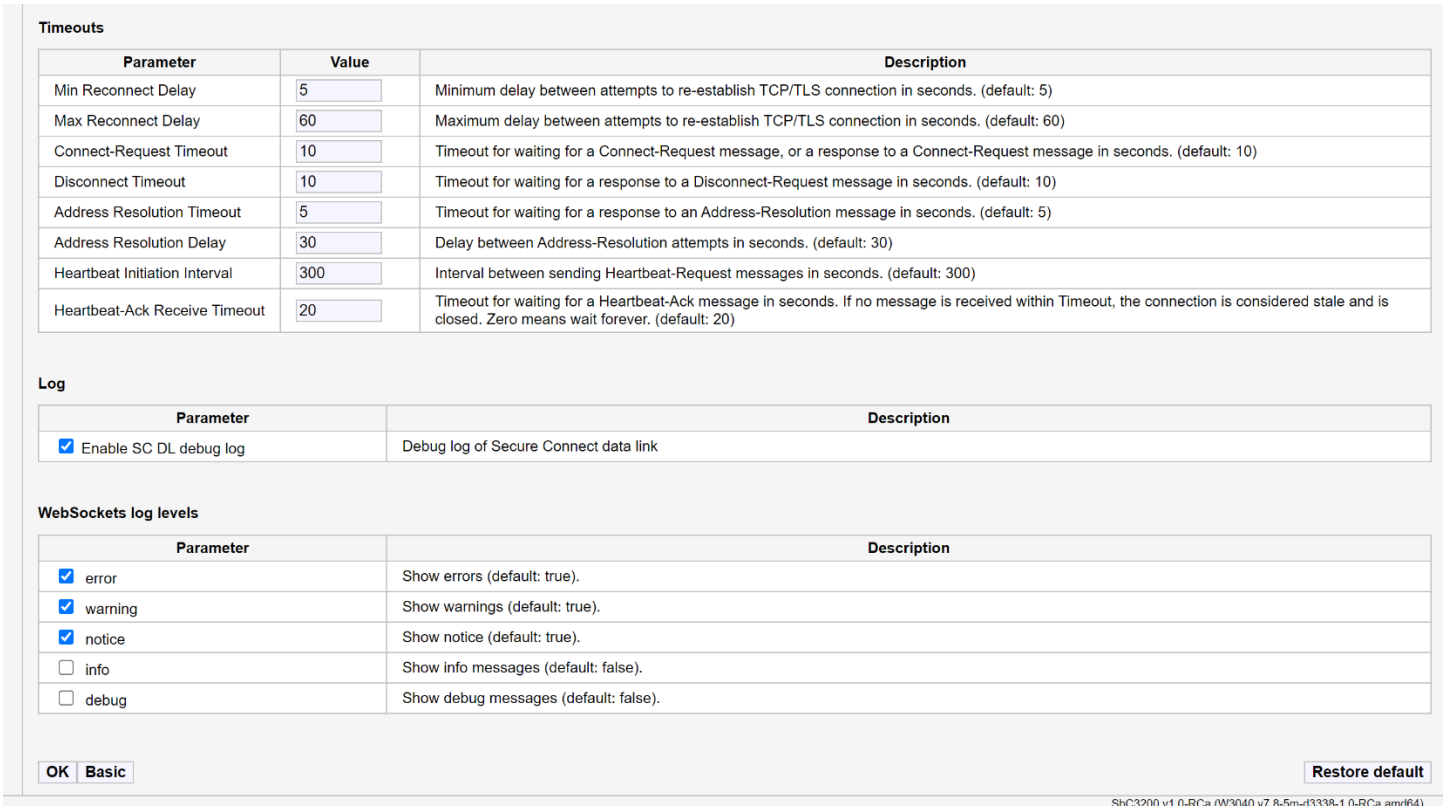


The SbC3200's UUID and the VMAC used for BACnet/SC are automatically assigned. To view the current values, go to the Status and Statistics web page and look for the section "BACnet Secure Connect".

The SbC3200 supports BACnet/SC Direct Connect, in which BACnet/SC nodes (like the SbC3200) can communicate directly with one another, bypassing the BACnet/SC hub(s) for the transmission of BACnet unicast messages. This option may be enabled and configured to improve network performance.

There are also several advanced BACnet/SC settings, including various timeout parameters and delay parameters. Before you modify any of these timeouts and delays, you must have a solid understanding of the associated protocol behavior; if you are in doubt, please retain the default value.

You can also enable the SbC3200's BACnet/SC debug log, which is sent over the network to a configured syslog server. See the **Network Services** documentation for more information on how to configure the SbC3200's syslog functionality.



Timeouts

Parameter	Value	Description
Min Reconnect Delay	5	Minimum delay between attempts to re-establish TCP/TLS connection in seconds. (default: 5)
Max Reconnect Delay	60	Maximum delay between attempts to re-establish TCP/TLS connection in seconds. (default: 60)
Connect-Request Timeout	10	Timeout for waiting for a Connect-Request message, or a response to a Connect-Request message in seconds. (default: 10)
Disconnect Timeout	10	Timeout for waiting for a response to a Disconnect-Request message in seconds. (default: 10)
Address Resolution Timeout	5	Timeout for waiting for a response to an Address-Resolution message in seconds. (default: 5)
Address Resolution Delay	30	Delay between Address-Resolution attempts in seconds. (default: 30)
Heartbeat Initiation Interval	300	Interval between sending Heartbeat-Request messages in seconds. (default: 300)
Heartbeat-Ack Receive Timeout	20	Timeout for waiting for a Heartbeat-Ack message in seconds. If no message is received within Timeout, the connection is considered stale and is closed. Zero means wait forever. (default: 20)

Log

Parameter	Description
☑ Enable SC DL debug log	Debug log of Secure Connect data link

WebSockets log levels

Parameter	Description
☑ error	Show errors (default: true).
☑ warning	Show warnings (default: true).
☑ notice	Show notice (default: true).
☐ info	Show info messages (default: false).
☐ debug	Show debug messages (default: false).

OK Basic Restore default

Figure 4: BACnet/SC Advanced Settings

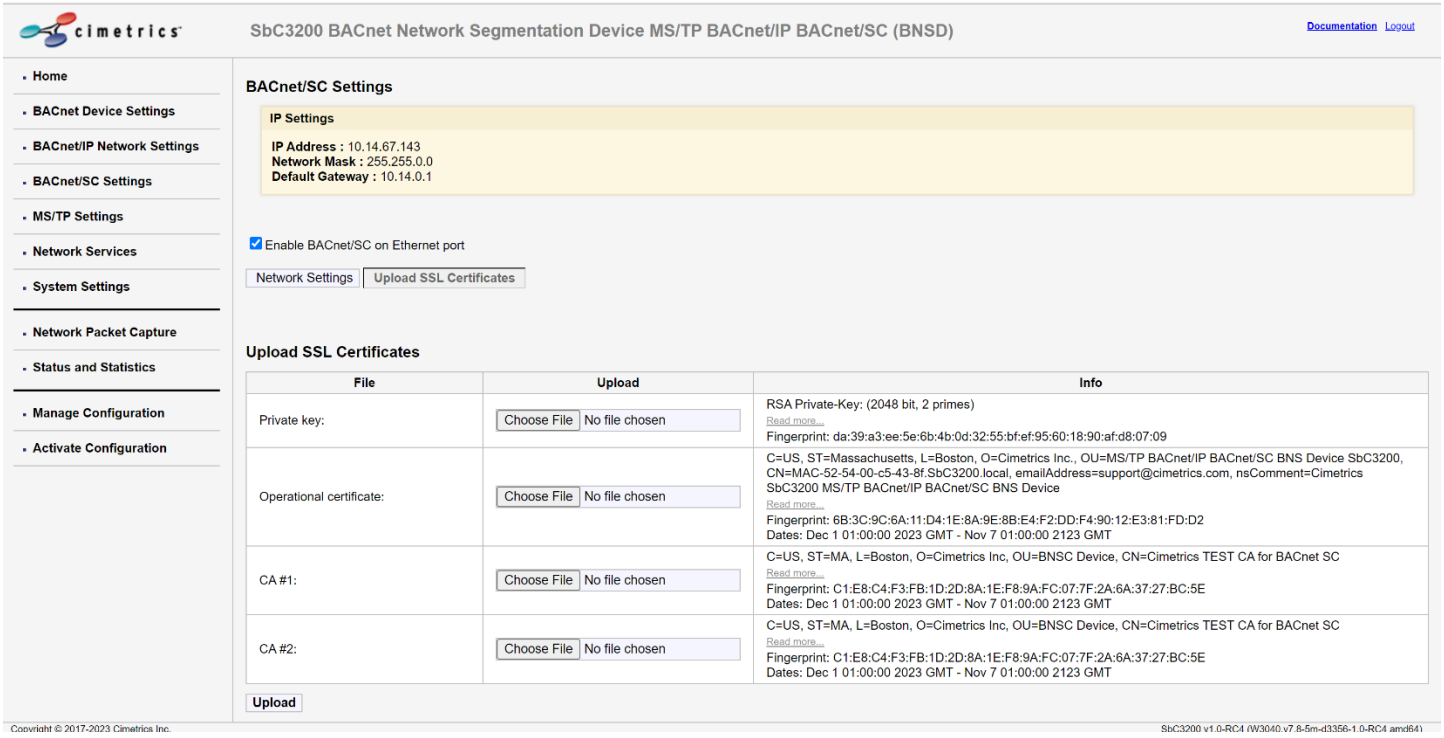
BACnet/SC Certificates

BACnet/SC uses the TLS protocol to secure communication between devices (encryption) and to identify devices that are permitted to join a specific BACnet/SC network (authentication). To accomplish this, BACnet/SC requires that every BACnet/SC device that needs to connect to a specific BACnet/SC network possess an operating certificate that has been signed by the certificate authority (CA) for that specific BACnet/SC network. Good cybersecurity practice dictates that every operating certificate be unique and specific to a BACnet/SC device.

You must upload a private key and all necessary SSL certificates before the SbC3200 can join a BACnet/SC network. The SbC3200 is not capable of generating a private key or a certificate signing request (CSR).

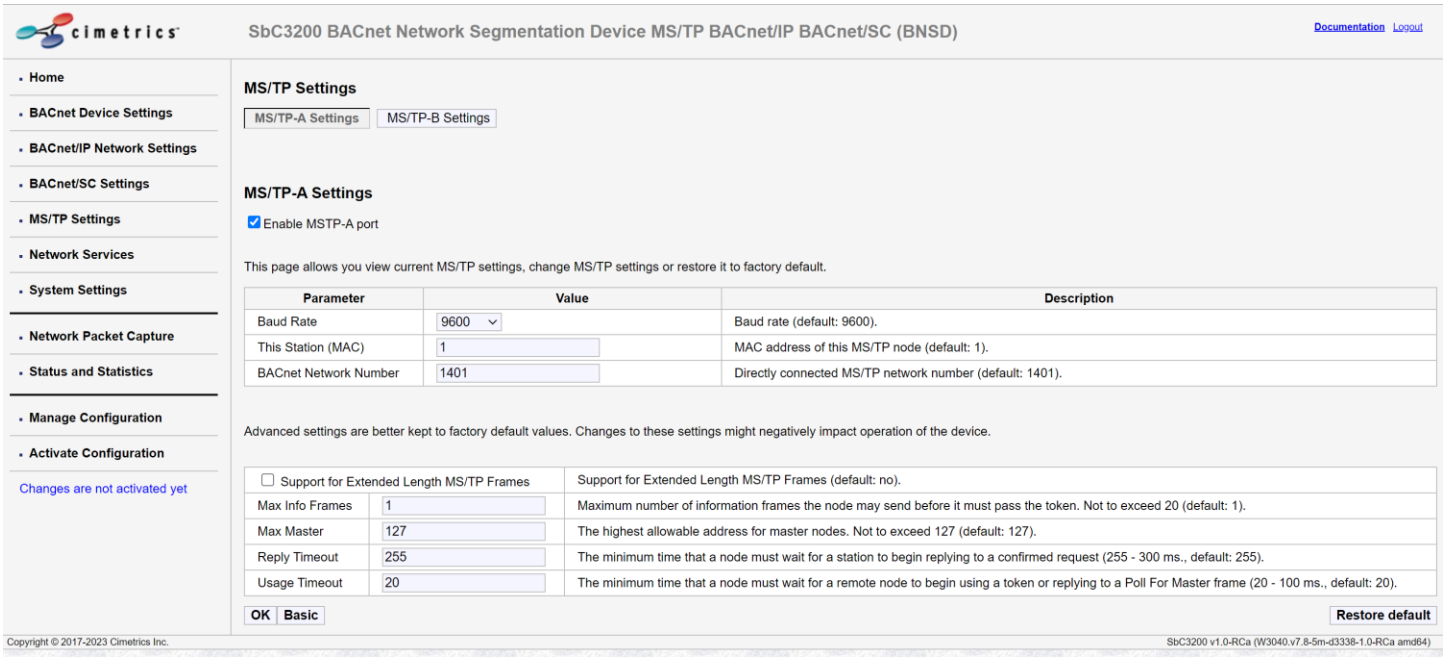
The following sequence of actions is necessary to create the SbC3200's private key and its BACnet/SC operating certificate. You (or knowledgeable IT staff) will need to use specialized software tools to perform some of these actions.

1. Generate a private key file and the corresponding public key file. This can be done using software available from the OpenSSL project. The private key is sensitive and should be handled accordingly.
2. Create a certificate signing request (CSR) file in PEM format. This can be done using software available from the OpenSSL project.
3. Present the CSR file to the manager of the certificate authority (CA) of the BACnet/SC network for signing. Request that the manager provide a PEM format operating certificate as well as the signing CA's certificate.
4. Once you have received the device's operating certificate and the signing CA's certificate from the manager of the CA, upload those files and the private key file to the SbC3200. You upload these files from the BACnet/SC Settings web page, Upload SSL Certificates tab. To upload a file to the SbC3200, click on "Choose file", select a file on your PC to upload, and then click on the Upload button. You will need to activate the changes.



BACnet MS/TP Settings

On this page you can enable and configure MS/TP port A and port B. Note that these two ports are independently enabled and configured.



Baud Rate:

The SbC3200 supports all baud rates specified in the *BACnet Standard*: 9600, 19200, 38400, 57600, 76800, and 115200. From the drop-down list, please select the designated baud rate for your MS/TP network. Please keep in mind that ALL devices connected to an MS/TP network, including the SbC3200, must be configured to use the SAME baud rate. If the configured baud rates are different, the devices will not be able to communicate with each other.

This Station (MAC):

This is the Media Access Control (MAC) address of the SbC3200's MS/TP port. Please note that ALL devices connected to a MS/TP network must have a unique MAC address. Prior to configuring this address, you will need to know the MAC addresses of all the devices on the MS/TP Network. Once you have this information, enter a unique address (0 through 127) for the SbC3200's MS/TP port.

BACnet Network Number:

You must assign a BACnet Network Number to the MS/TP network. This must be a unique number on the *entire* BACnet internetwork. Please note that there is also a parameter called BACnet Network Number in the BACnet/IP Settings web page and on the BACnet/SC Settings web page. All these BACnet Network Numbers must be unique. However, the BACnet Network Number associated with a given port is ignored if the port is disabled.

MS/TP Advanced Settings

If you click on the Advanced button, you will see the advanced MS/TP configuration settings. Before you modify any of these settings, you must have a solid understanding of the associated protocol behavior. If you are in doubt, please retain the default value.

Extended length MS/TP frames:
Check if other MS/TP devices on this network support extended length MS/TP frames. This extension to the core MS/TP protocol, which allows MS/TP devices to transmit frames larger than 512 bytes, was introduced in *Addendum an* in 2014. Keep this option disabled unless your MS/TP network consists of modern devices which support this extension.

Max Info Frames:
A larger value might improve network performance if the SbC3200 forwards many messages to MS/TP devices.

Max Master:
The value of Max Master should be greater than or equal to the numerically highest MAC address of MS/TP Manager devices (formerly "MS/TP Masters") on the network. The default value is 127; lower values may result in slightly better network performance.

Reply Timeout:
This is the amount of time (in milliseconds) that the SbC3200 waits for another MS/TP device to begin replying to a confirmed request.

Usage Timeout:
This is the amount of time (in milliseconds) that the SbC3200 waits for another MS/TP device to begin using the MS/TP token or to reply to a Poll for Master frame.

Click on the "OK" button to accept your changes before you move to a different web page.

Activate New Configuration

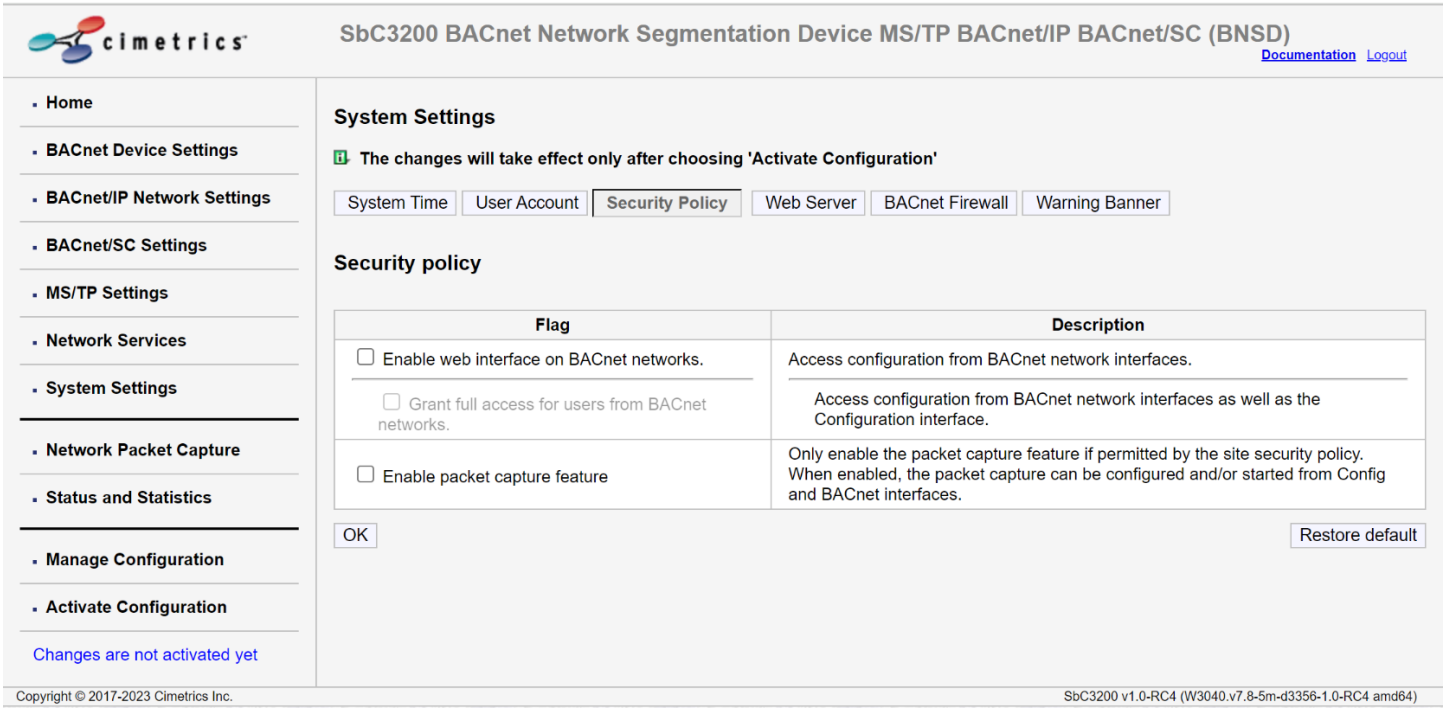
Once changes are made to any configuration parameter on the SbC3200, the changes get saved and applied only after the new configuration is activated from the Activate Configuration web page. Activation is needed if you see the text **"Changes are not activated yet"** below the menu, shown in blue letters in the lower left part of the screen shot below.

One or more configuration warnings or errors may be displayed on the Activate Configuration web page. If the SbC3200 does not detect any configuration errors, then entering the admin password and clicking on the "Confirm" button will initiate a reboot of the device after the configuration changes have been saved in the SbC3200's non-volatile memory.

Note that if the SbC3200 is disconnected from its power source or a logout occurs (manually by the user or automatically due to a timeout), all configuration changes that have not been activated will be discarded.

Additional Features

In addition to the core BACnet routing functionality and the local configuration interface, the SbC3200 provides additional functionality that can be selectively enabled and configured by the user.



Manual setting of time

Accurate local time is needed if BACnet/SC is enabled or if a syslog server is configured. You can set the SbC3200's local time and the local time zone on the System Settings web page, System Time tab. Even if you configure the SbC3200 to get the current time from an NTP server (see **Network Services**), you can select the local time zone on the System Time tab.

Second user account setup

You can create a second user account with a configurable login and password in the User Account tab on the System Settings web page. This account has restricted privileges, generally limited to operations that do not change the configuration of the SbC3200.

Warning banner

You can configure a message to be displayed when any user attempts to login in. This message, commonly known as a warning banner, is typically used to remind the user of laws, regulations, or organizational policies that are relevant to the use of the SbC3200. To configure a warning banner, select the Warning Banner tab on the System Settings web page.

Access to the Configuration Interface from a BACnet Network

By default, access to the web-based configuration interface of the SbC3200 is only possible by using the SbC3200's fixed configuration IP address (169.254.14.14), as described in the *SbC3200 Quick Start*. This is a non-routable address that is intended for access from a PC connected to the same private LAN.

You have the option of also enabling access to the web-based configuration interface through the configured IP address that is used by the SbC3200 for BACnet/IP or BACnet/SC communication. When

enabled, this allows remote management of the SbC3200 through IP routers. To enable access, select the security policy “Enable web interface on BACnet networks” from the Security Policy tab on the System Settings web page. Note that some security-sensitive functions as well as functions not suitable for execution from a remote workstation are not available by default. Check the “Grant full access for users from BACnet networks” check box to make all functions accessible.

Click on the “OK” button to accept your changes before you move to a different web page.

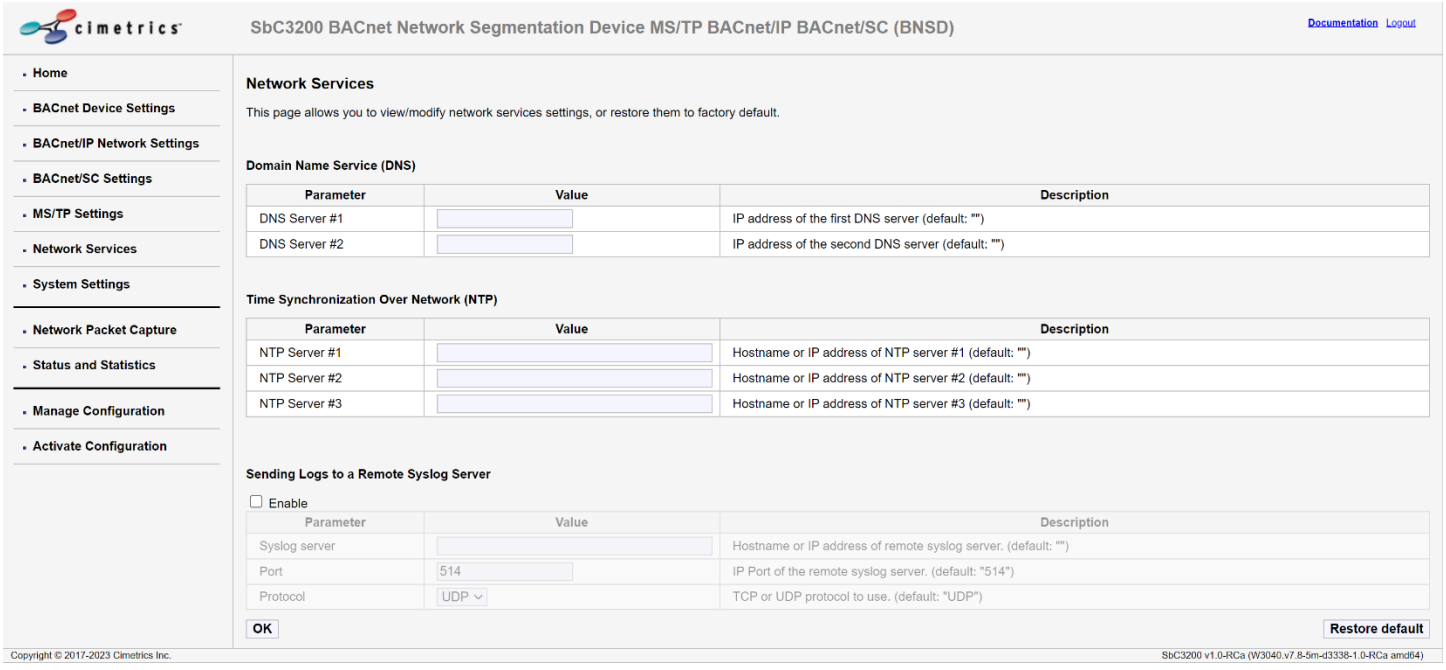
Network Services

This page allows you to view/modify network services settings or restore them to factory default.
You can configure the product to act as a Domain Name Service client (DNS), a Network Time Protocol client, and as a syslog client.

Domain names can be used when configuring BACnet/SC Hub URIs, and when setting up the SbC3200 to communicate with NTP and Syslog servers. Up to two DNS servers can be specified for redundancy. Only IP addresses are accepted.

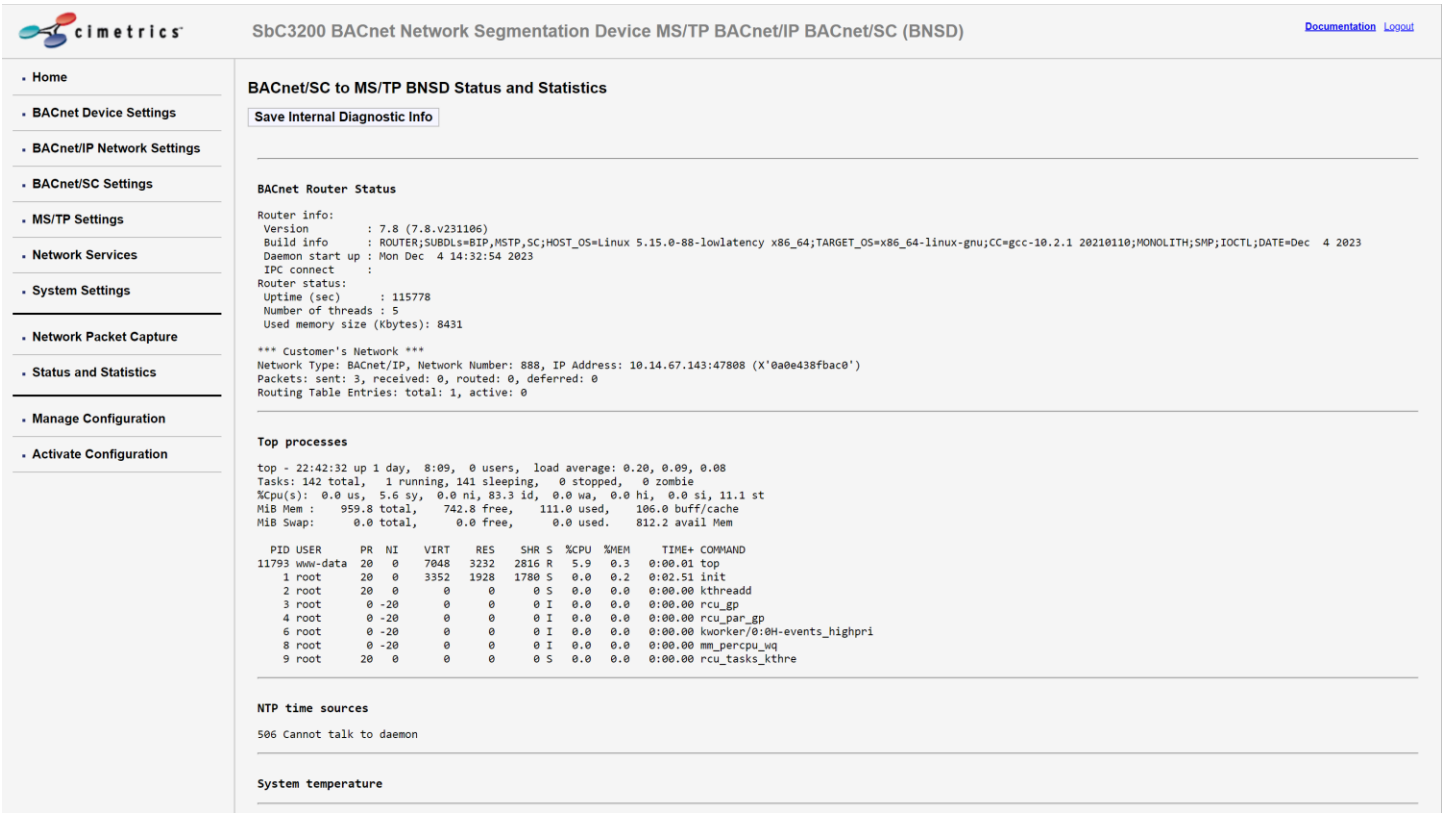
Although the SbC3200’s internal clock can be locally set (see **Manual setting of time**), the SbC3200 can also be configured to communicate with one or more NTP servers. Up to three NTP servers can be configured, and all of them will be used to adjust the SbC3200’s internal clock. The local time zone can be configured on the System Settings web page.

A syslog server is a network host which accepts and archives log messages in standard format (RFC 3164 and RFC 5424). The syslog server host can be identified either by its IP address or hostname (if a DNS server is configured, see above). The default port number for Syslog is 514. Syslog messages can be sent over TCP or UDP. The port number and the choice of TCP or UDP must match the configuration of the Syslog server.



Internal Diagnostics

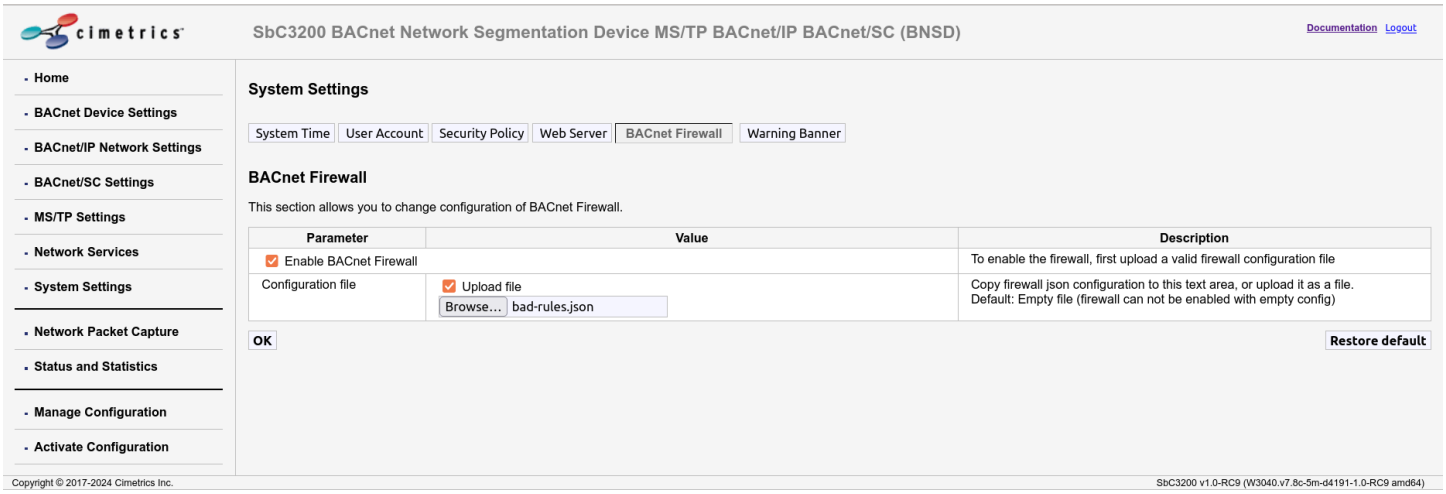
The Status and Statistics web page shows the output of various internal tools that, in aggregate, provide a technically dense view of the health of the SbC3200 since its last reboot. If you suspect that the SbC3200 is malfunctioning or that it might not be correctly configured, you can click the "Save Internal Diagnostic Info" button to save diagnostic information in a file that you can send to Cimetrics technical support. You should also download and send the SbC3200's current configuration file (see **Managing SbC3200** Configuration tab) along with the internal diagnostic file.



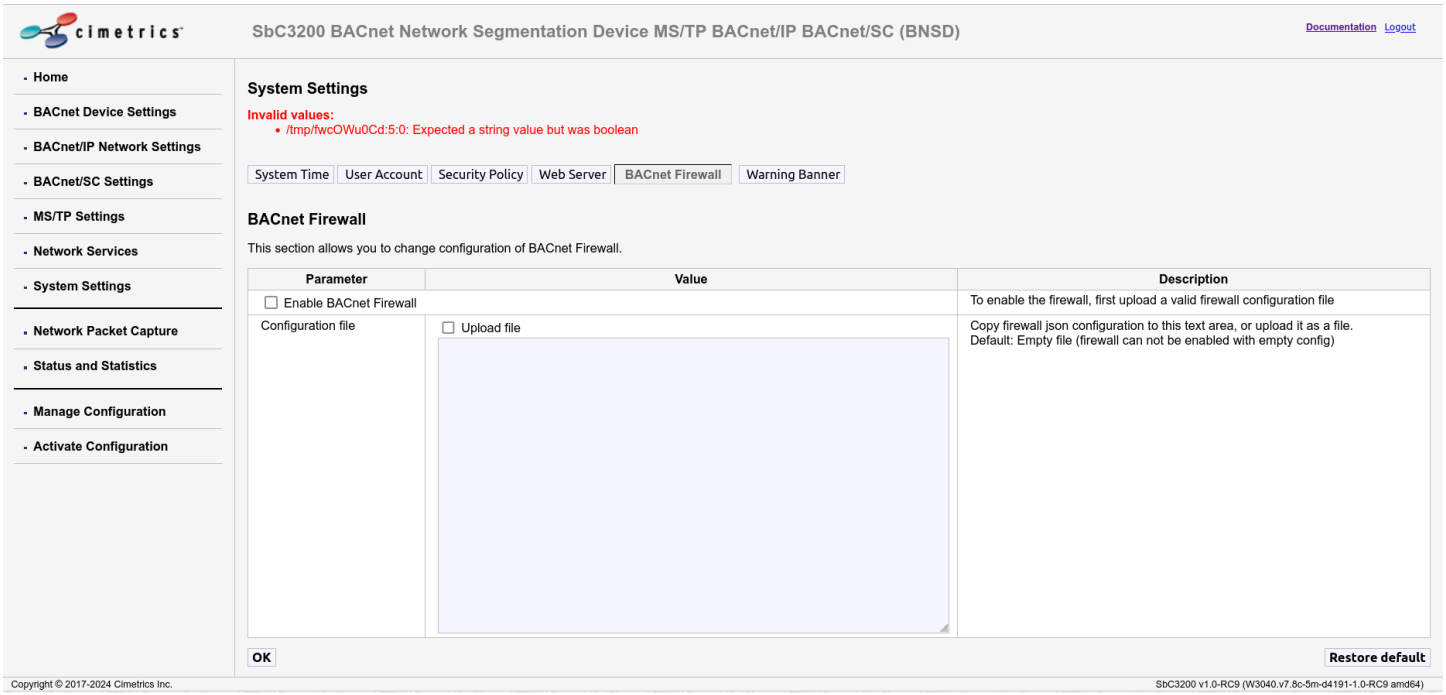
BACnet Firewall

The BACnet firewall can drop or reject certain BACnet messages that would ordinarily be forwarded by the SbC3200 based on multiple criteria, such as source and destination address, BACnet service choice, current time of day, etc. Firewall actions can be sent as events to a syslog server.

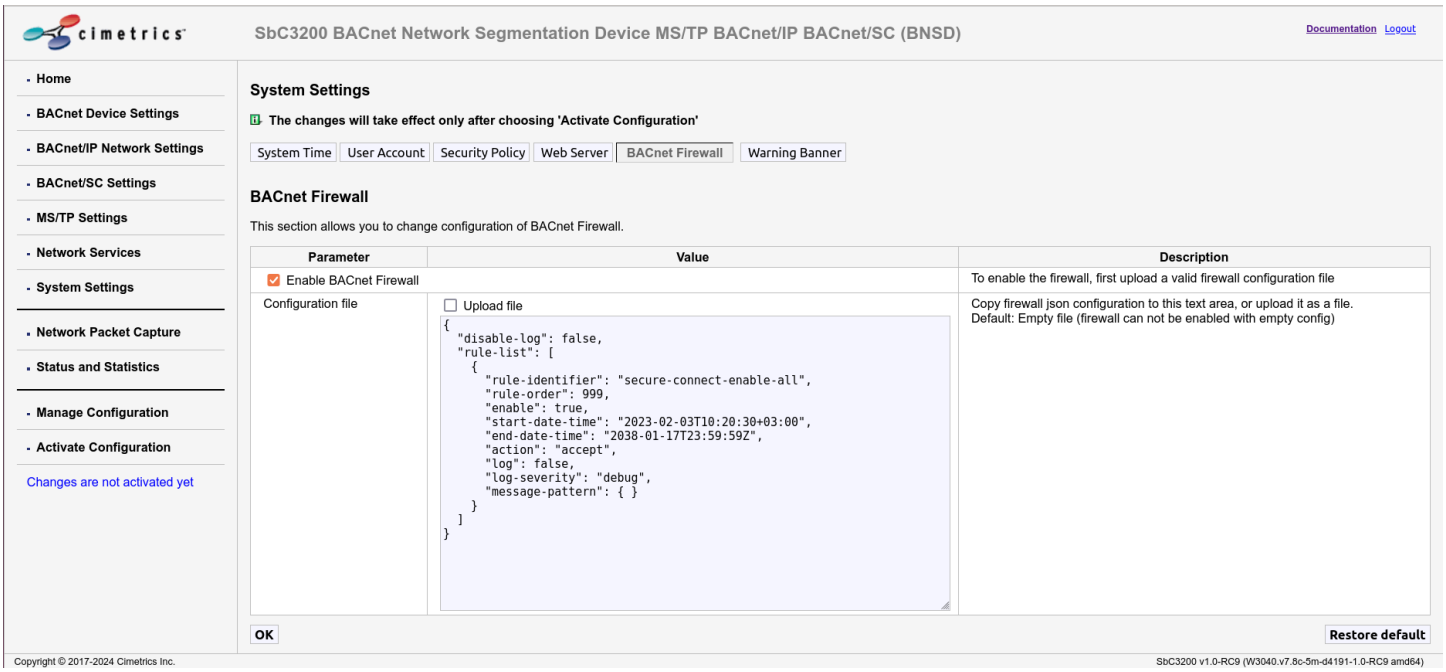
The BACnet firewall is configured by uploading a properly formatted file to the SbC3200 from the System Settings web page. Information about the firewall's configuration file format is beyond the scope of this document; contact Cimetrics technical support for more information.



After you click on the “OK” button, the SbC3200 will check the uploaded firewall configuration file for any formatting errors. If there is an error in the file, an error message will be displayed, such as the following:



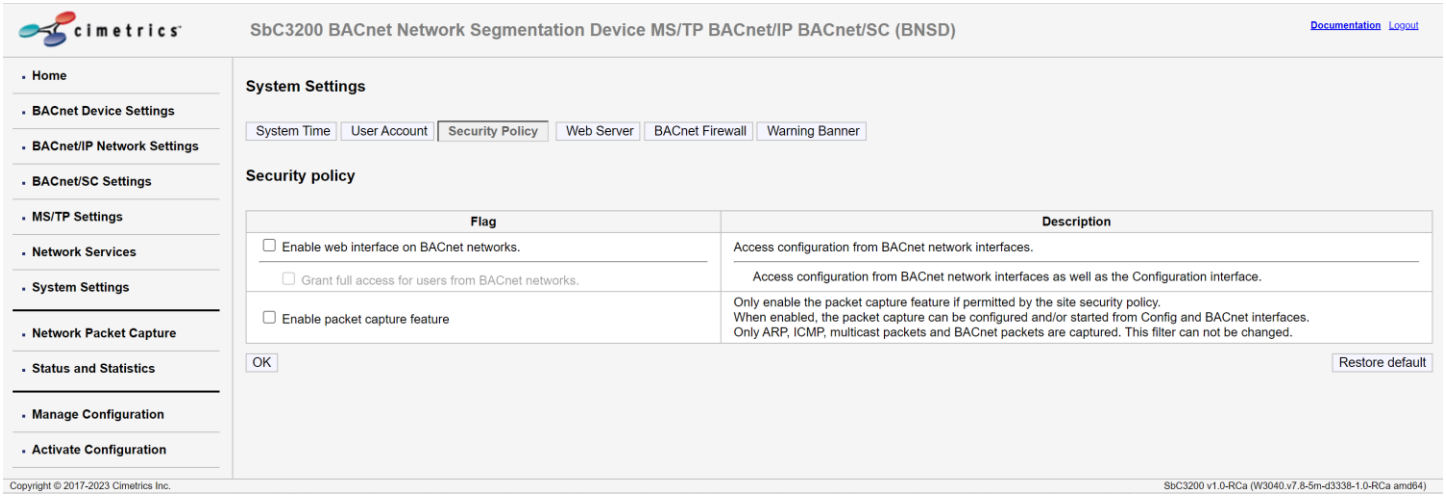
To complete the process of configuring and enabling the firewall after you load a valid configuration file, you must activate the configuration.



Network Packet Capture

The SbC3200 can be configured to capture BACnet/IP and BACnet/SC packets that are sent or received on the Ethernet port. A few other types of packets are also captured. The files containing the captured packets can be downloaded using the configuration interface and then viewed using applications such as Wireshark.

Network packet capture is administratively prohibited by default and must first be enabled through the configuration interface using the checkbox “Enable packet capture feature” on the System Settings web page, Security Policy tab.



Click on the “OK” button to accept your changes before proceeding.

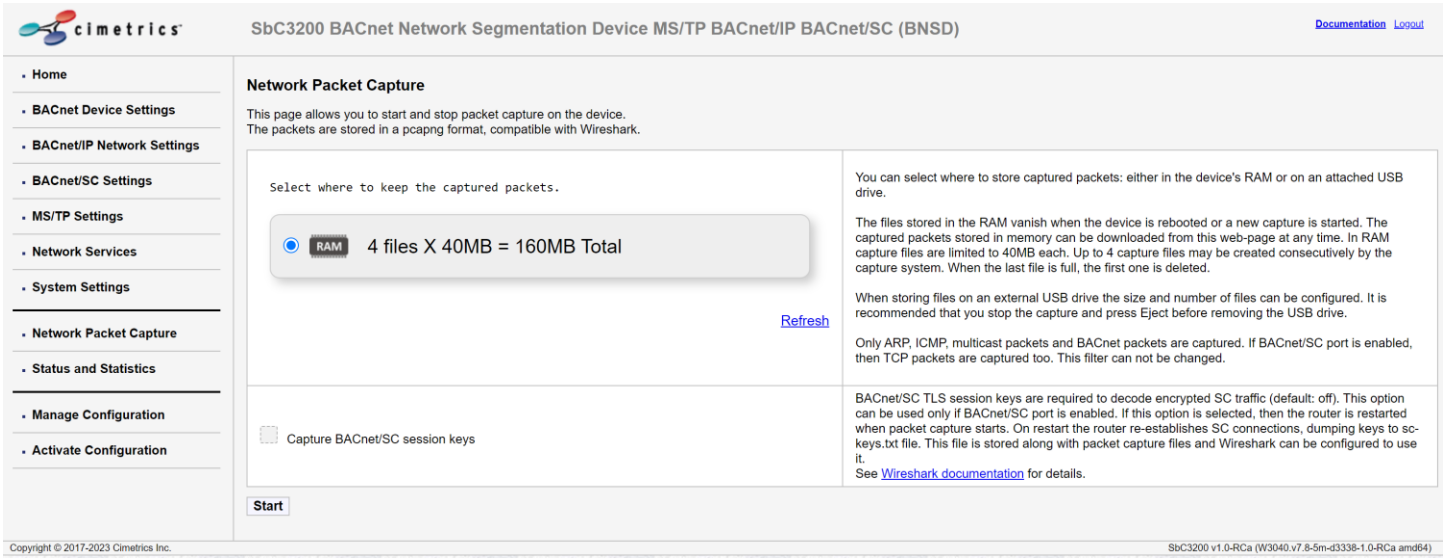
When you enable network packet capture, you should also set the SbC3200’s system time from the System Settings web page (System Time tab) or enable network-based time synchronization (NTP) on the

Network Services page. Setting the time manually will ensure that the packet timestamps will be reasonably accurate, assuming that the connected PC's clock is accurate. (This is not necessary if NTP is being used for time synchronization.)

Navigate to the "Activate Configuration" web page to save the new configuration and reboot. You should now be able to start capturing network packets.

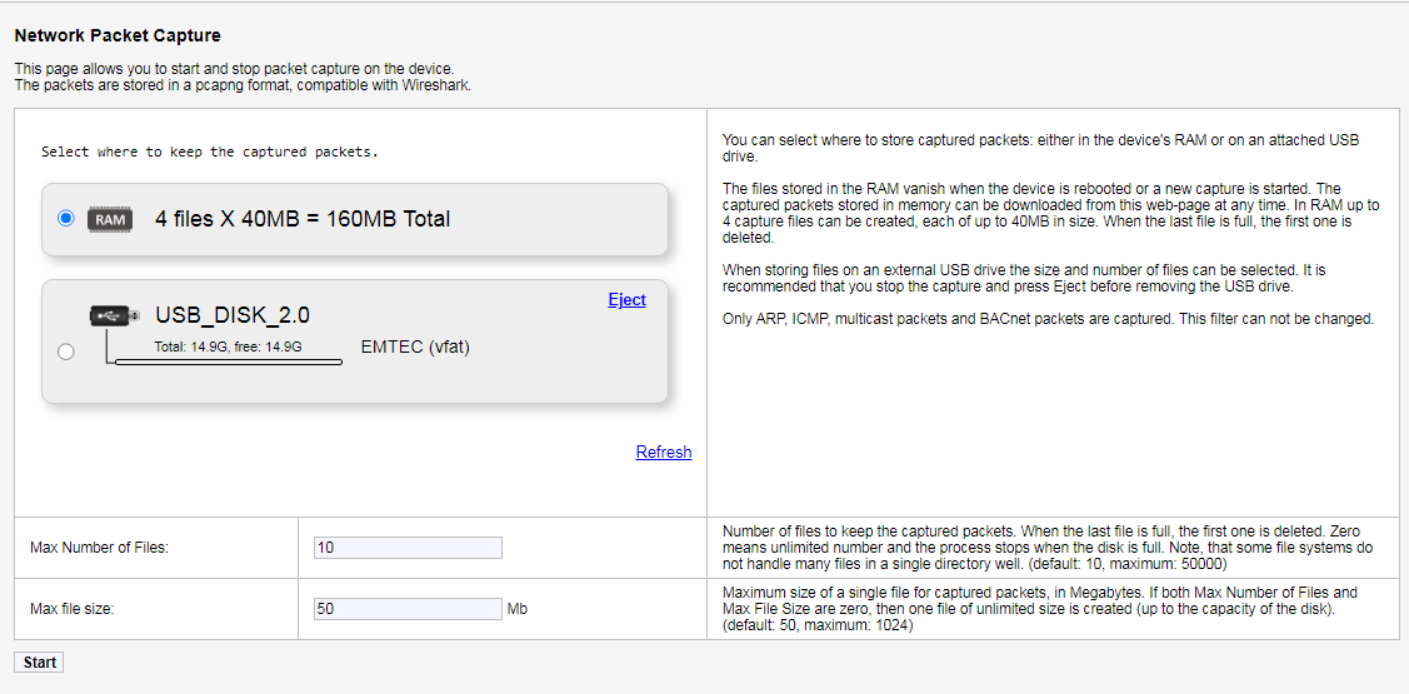
The simplest way to capture packets is to use the SbC3200's internal RAM for temporary packet storage. Click the "Start" button to begin the capture. You can click on the "Stop" button to terminate a running packet capture. At any time, you can click "Download files" to download the compressed packet capture file(s). The packet capture files created by the SbC3200 are managed as a ring buffer: When the last file is full, the oldest file is removed, and the resulting free space is reused to create a new file. Under normal conditions, packet capture continues until explicitly stopped by the user.

> Note: BACnet/SC packets are ordinarily encrypted by TLS. If you want to be able to decode the captured BACnet/SC packets to view their BACnet contents, you should enable the "Capture BACnet/SC session keys" option before you begin the capture, in which case the SbC3200 will reboot before capturing packets. Consult the documentation for your network protocol analyzer software for instructions on how to use the contents of the session keys file "sc-keys.txt".



> Note: The packet capture files stored in the SbC3200's internal RAM are not persistent, so they will be erased when the SbC3200 is rebooted or when a new packet capture is started.

If you want to do a packet capture that is expected to require a considerable amount of memory, you can use a USB memory stick to store the files containing the captured packets. Insert a formatted memory stick into one of the SbC3200's USB ports, and then navigate to (or refresh) the Network Packet Capture web page. If the memory stick is recognized by the SbC3200, you should now see something like the following:



Select the "USB disk" as the location for the captured packets, select the number of packet capture files and the maximum size of each file, then click on the "Start" button to begin capturing packets. You should click on the "Stop" button to terminate a running packet capture.

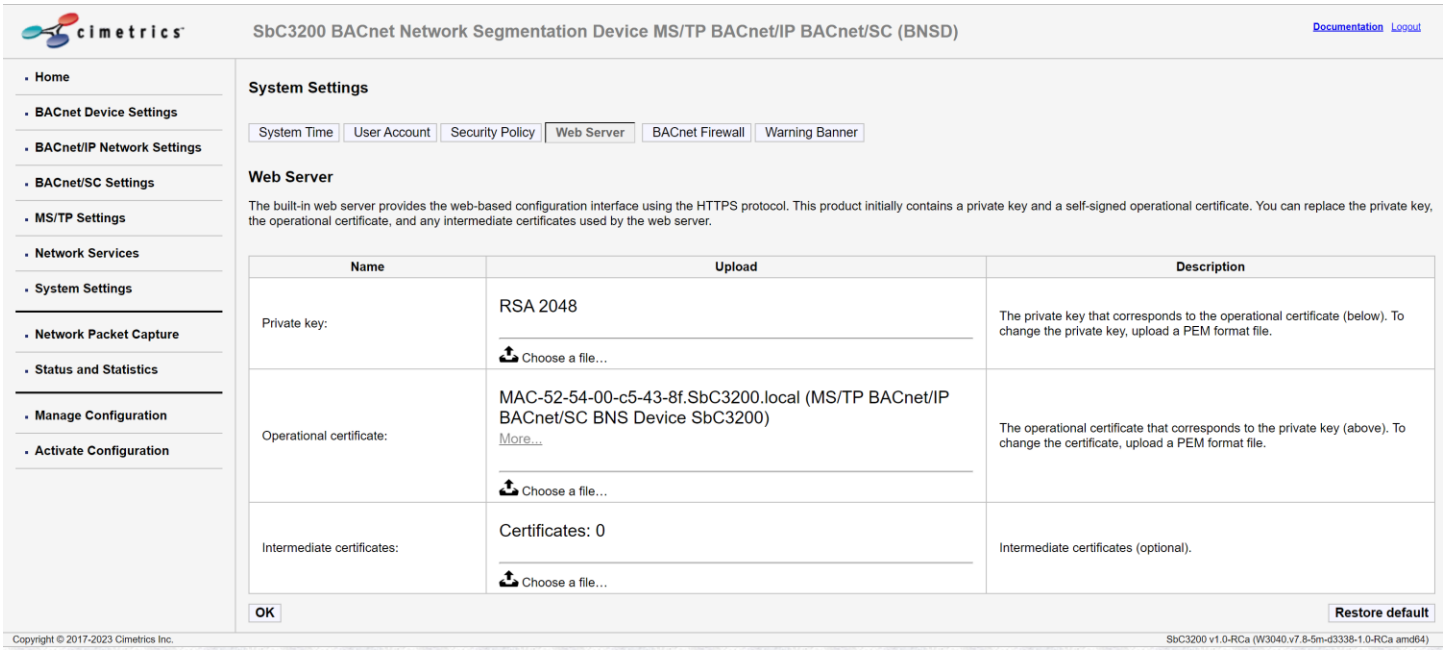
Be sure to click on "Eject" before you physically remove the memory stick from the SbC3200.

Replacing the Configuration Web Server's Private Key and Certificates

The SbC3200's configuration web server uses the HTTPS protocol for communication with web browsers. The SbC3200 ships with a pre-assigned private key and a self-signed operational certificate that are used by the SbC3200's web server.

> Note: Modern web browsers will display security warnings when they navigate to a web server that uses a self-signed certificate. For example, Google Chrome says that the SbC3200's web pages are "not secure" and that the "certificate is not valid". You may be required to confirm the security exception for this host to be able to access configuration pages.

It is possible to replace the SbC3200's pre-assigned private key and the self-signed operational certificate. You can generate these using a software tool such as available from OpenSSL. The use of such tools is outside of the scope of this document. Once you have created the private key file and the corresponding operational certificate files (PEM format), navigate to the System Settings page, and choose the Web Server tab, as shown below. To replace an existing file, click on "Choose a file" and then select a file on your PC to upload to the SbC3200.

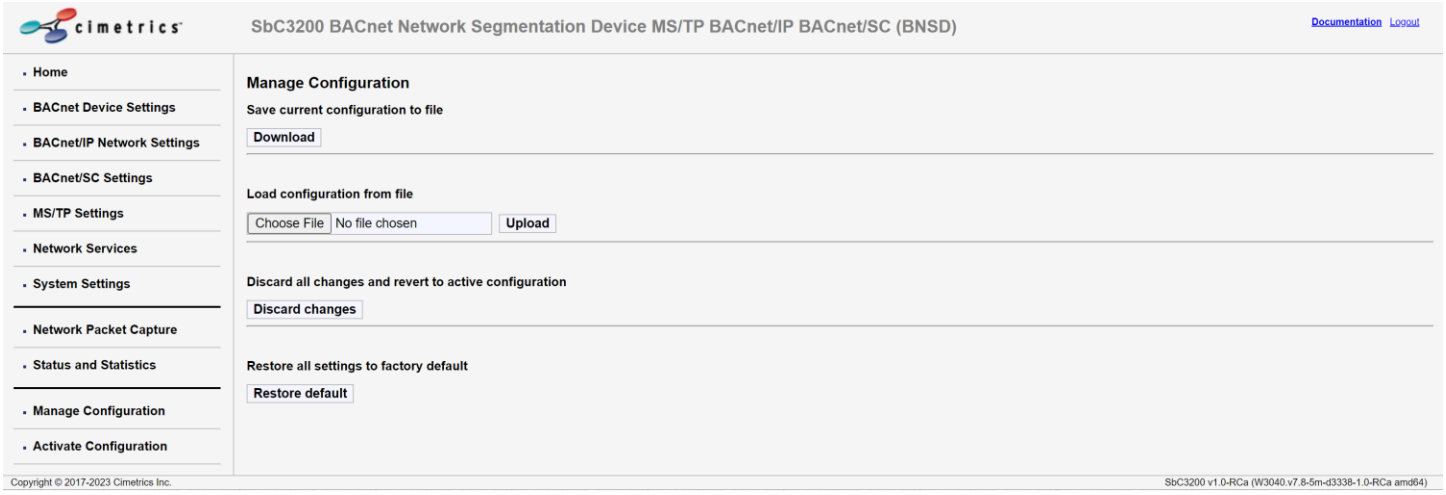


Managing SbC3200 Configuration

You may save the SbC3200's configuration in a file, and later load the configuration file into the same SbC3200 or into a different SbC3200 that is running compatible firmware. After you load a configuration file you may make additional configuration changes if desired. Configuration changes that are made by any method do not take effect until the new configuration is activated (see the Activate New Configuration web page).

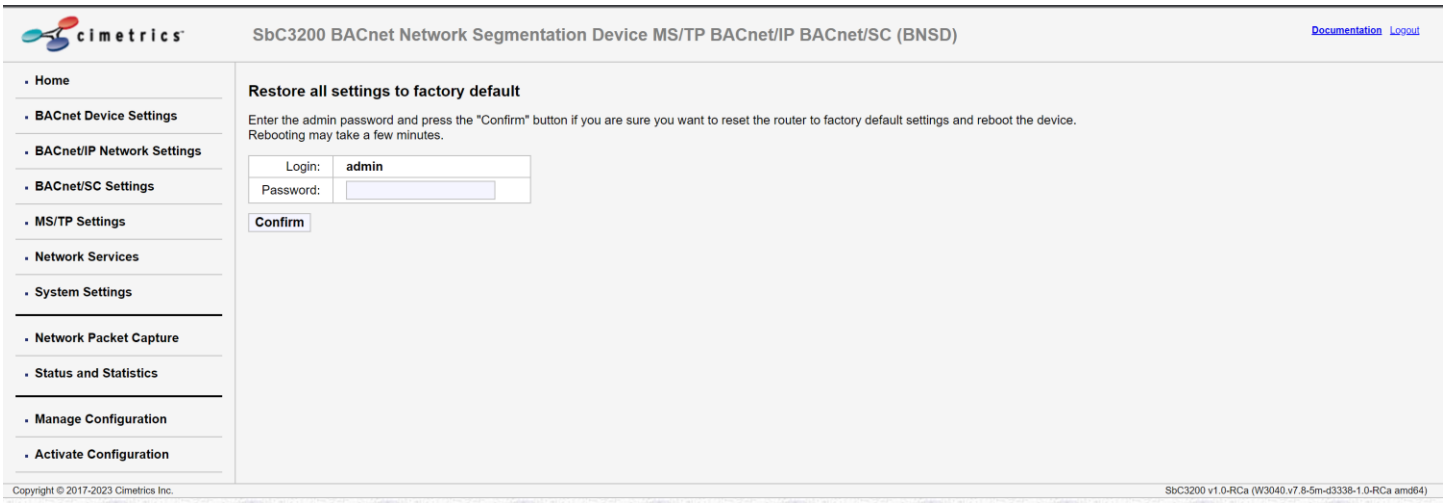
The SbC3200's account passwords, BACnet/SC private key and certificates, and HTTPS-related configuration files are not contained in the SbC3200 configuration file for security reasons. These sensitive data will not be restored when you load a SbC3200 configuration file.

Note that directly editing a saved configuration file is not recommended. All configuration changes should be made via the SbC3200's web interface.



Resetting the SbC3200 to Factory Default Settings

If you know the password for the admin account, you can easily restore the factory default settings. Navigate to the "Manage Configuration" web page. After you click on the "Restore default" button, you will see the following password challenge:

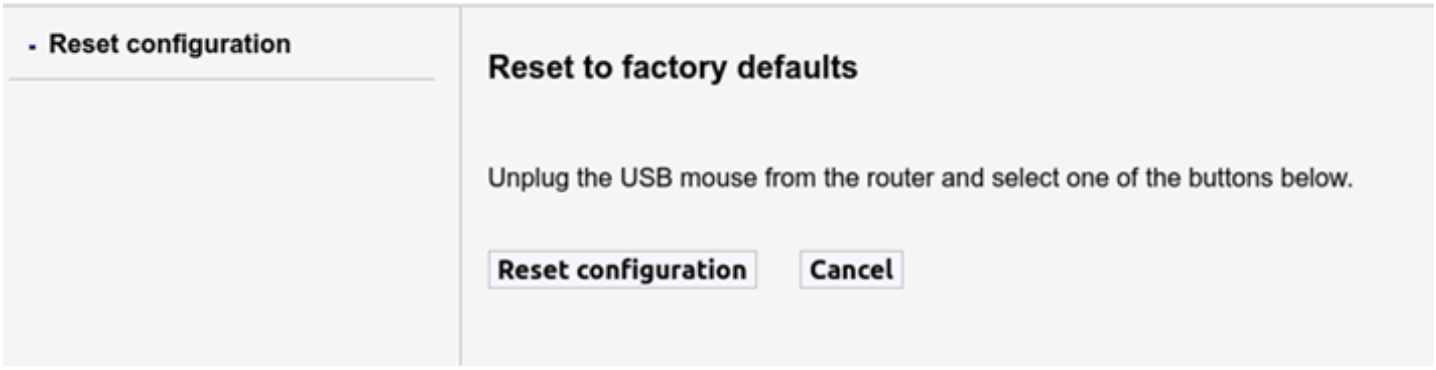


Once you enter the current admin password and then click on the "Confirm" button, the SbC3200's current configuration will be replaced by the factory default configuration, and the SbC3200 will reboot. You can then reconfigure the SbC3200 as required after you login using the factory default admin password. You will be shown the factory default admin password while the system is restarting.

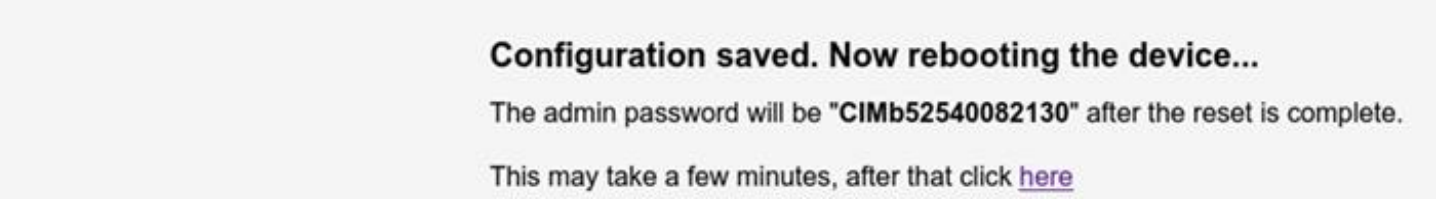
How to reset to factory default settings if the admin password is unknown

Even if you don't know the current password for the admin account, it is still possible to restore all factory default settings and to recover the factory default admin password. To do this, you will need a USB mouse, a PC, an Ethernet cable, and physical access to the SbC3200. The recommended procedure is as follows:

1. Connect a USB mouse to one of the SbC3200's USB ports, and then power cycle the SbC3200 by disconnecting its external power adapter from AC power for several seconds. It will take a couple of minutes for the SbC3200 to reboot after power is restored.
2. Connect a PC to the SbC3200's configuration port using an Ethernet cable, and then using the PC's web browser connect to the SbC3200's built-in web server as described in the SbC3200 Quick Start document.



3. After you see a web page like the one above that instructs you to unplug the USB mouse from the router, please do that. This must be done before the next step.
4. Click on the “Reset configuration” button. If all is well, you should see a web page like the following:



You can reconfigure the SbC3200 as required after you login using the factory default admin password, which is shown on the web page.

Appendix: What does a BBMD do?

BBMDs forward BACnet broadcast messages within BACnet/IP networks that span multiple IP subnetworks. The BACnet protocol utilizes broadcast messages for certain functions, such as the discovery of BACnet devices and for time synchronization. Also, BACnet networks and BACnet routers are discovered using BACnet broadcast messages. See the *BACnet Standard* for more information about BACnet broadcast messages.

IP routers (also referred to as "IP gateways") join IP networks together so messages from devices connected to one network can be sent to devices connected to another network. If your BACnet devices' networks are interconnected via IP routers, then BACnet/IP broadcast messages that are transmitted as UDP broadcasts will normally be blocked by an IP router. To solve this problem the *BACnet Standard* defines the behavior of the BBMD (BACnet/IP Broadcast Management Device) in Annex J.

BBMDs typically use UDP unicast messages to forward BACnet/IP broadcast messages. A BBMD directly forwards a BACnet broadcast message initiated by a BACnet/IP device on the BBMD's subnet to other BBMDs and to its registered Foreign Devices in accordance with its configuration. Upon arrival at a destination BBMD, the message is then transmitted (as a UDP broadcast) on that subnet by the destination BBMD and is also sent to the destination BBMD's registered Foreign Devices.

A BACnet/IP device can register with a BBMD as a Foreign Device if that configuration option is enabled. A registered Foreign Device becomes a member of the BACnet/IP broadcast domain, and it will receive forwarded BACnet/IP broadcast messages from the BBMD. A Foreign Device can also request that messages be broadcasted by the BBMD on the Foreign Device's behalf. Foreign Devices are typically connected to an IP subnetwork that does not have a connected BBMD.

Here are some other important characteristics of BBMDs that should be noted.

1. BBMDs only forward BACnet/IP broadcast messages, not unicast messages. BACnet/IP unicast messages are sent directly by the originating device to the destination device.

2. There is no standard method for a BBMD to discover other BBMDs that it should communicate with, so each BBMD must be configured with a list of the addresses of the other BBMDs to which it should forward BACnet/IP broadcast messages.

3. A BBMD that receives a forwarded BACnet/IP broadcast message from another BBMD will not forward that message to any other BBMDs.

4. To ensure that BACnet/IP broadcast messages flow in both directions between two BBMDs and between devices connected to their respective IP subnets, each BBMD must be configured to forward broadcasts to the other BBMD.

5. In almost all situations, there should be at most one BBMD attached to an IP subnetwork containing BACnet/IP devices.

To find out more about BACnet broadcast management and how to build a wide area network with BACnet you may refer to the classic article "Building Wide-Area Networks with BACnet" written by Bill Swan.