Belkin OmniView Serial Console Server

User Manual

V1.0

P75598

Contents

F i g u r e s

1. Product Overview

1.1 Introduction

Thank you for purchasing the Belkin OmniView Serial IP Console Server (Console Server). This device provides administrators secure monitoring and control of servers, routers, switches, and other serial devices from anywhere on the corporate TCP/IP network, over the Internet, or through dial-up modem connections, even when the server is unavailable through the network.

The Console Server provides the following:

- Data path security by means of SSH or Web/SSL
- A secure, encrypted web interface over SSL (HTTPS)
- SSHv2 encryption, to keep server access passwords safe from hackers
- Support for all popular SSH clients
- Secure access from any Java-enabled browser.
- Connections to serial console ports using standard CAT5 cables, eliminating the hassles of custom cabling.

1.2 Package Contents

1 x OmniView Serial IP Console
1 x AC Power Cord
1 x Serial to RJ45 Adapter Kit, (5pcs)
1 x 6ft., RJ45-RJ45 CAT5 Cable
1 x Quick Start Guide
1 x User’s Manual
1 x Rack Mount Brackets and screws
1 x Footpad set

1.3 Serial Console Features

- **In-band and Out-of-band managements**
  Console port management solutions offer remote, reliable and secure access to serial console ports through in-band networks and out-of-band connectivity options, such as serial terminal access and dial-up modem.
- **Manage network devices/servers centrally, remotely, and securely**
  Reliable console port management solutions all allow you to encrypt sensitive data using proven protocols such as SSH/v2, SSL.
- **Diverse devices management**

Simple ASCII or VT100 terminal emulation is not sufficient to manage these wide-ranging device types. Today's data centers contain a broad mix of Unix, Linux, RISC, mainframe, and Windows servers, as well as other serially managed devices such as router, gateway, firewall, PBX, UPS, SAN and NAS devices, and intelligent power strips.

- **Proactive monitoring and warning to assist system diagnosis**
  Applications, and even operating systems, send messages to the system console. These messages contain error and panic information that often precedes a system crash. Unlike terminal servers, console port servers buffer these messages in real time and allow administrators to page through and search this data at a later time, and spontaneously send an e-mail to alert IT administrator of the critical event.
- **Remote and Secure Power Controller**
  Via serial port, this device acts as control master for controlling power strip. Since it supports RS-485 serial interface, it can control multiple power strips (up to 15).
- **Provides Serial-to-Serial function**
  To incorporate with Terminal Converter to provide VGA and keyboard ports locally, or connect the VGA/keyboard ports to KVM switch to consolidate the administration.
- **Access Port Lists for Users**
  Thanks to the Access Control List (ACL) of user account administration, all users except root account are authorized a set of serial ports. Users can access, make configuration change to those authorized serial ports assigned by root account.

1.4 Equipment Requirements

- Universal Connectivity Kit (Included)
- RJ45-RJ45 CAT5 Cable (included)

1.5 System Requirements

Web browser

	Browser			
Operating System	Microsoft Internet Explorer version 6.0 SP1 and later	Firefox version 2.0 and later	Netscape version 7.2 and Later	Mozilla version 1.7.3 and later
Windows 2000 SP2	Yes	Yes	Yes	Yes
Windows Server 2003	Yes	Yes	Yes	Yes
Windows XP	Yes	Yes	Yes	Yes
Windows Vista	Yes	Yes	Yes	Yes
Red Hat Linux 3 and 4	No	Yes	Yes	Yes
Sun Solaris 9 and 10	No	Yes	Yes	Yes
Novell SUSE Linux 9 and 10	No	Yes	Yes	Yes
Fedora Core 4 and 5	No	Yes	Yes	Yes
Mac OS X 10.4+	No	Yes	Yes	Yes

Java Plug in

The Serial Console web interface requires installing JRE (Java Runtime Environment) v6.0 and above. You can get the latest Java Software from the website http://www.java.com/en/download/manual.jsp

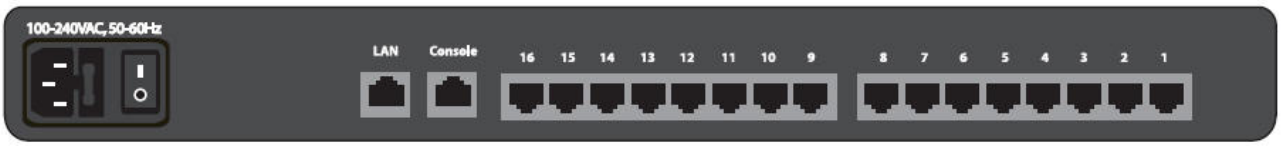
2. Unit Display Diagrams

2.1 Front/Rear Panel

Front View

Callouts:
Port LEDs
Link LED
Ready LED
Power LED
Reset button

Figure 1 Rear View



Call outs
IEC power
LAN port
Console Port
Device ports

2.2 LED Indicators, Button, and Connectors

LED	Indication
Power	**Red** – power indication *ON: power is applied*
Link	**Ethernet Link/Act/10/100Mbps:** **Orange** -- 10BaseT Ethernet connection established **Green** -- 100BaseT Ethernet connection established *Blinking: when data in activity* *ON: when no data in activity and link connected*
Ready	**Green** -- blinking per second when system is ready
Port Activity (one LED per port)	**Blue** – traffic activity *ON: In Use (successful port login)* *Blinking: traffic activity on the serial port*

- **RESET** button: Quickly press and release the button to reboot the Serial Console. Press and hold the Reset button for more than 5sec to set the unit to its default configuration settings.
- **ETHERNET** RJ45 connector: Ethernet interface
- **CONSOLE** RJ45 connector: RS232 console interface
- **Other** RJ45 connectors: serial ports

2.3 Specifications

Feature	Specification
General	LEDs
	Power(Red), **Ready**(Green, normally blinking), **Link**/Act/10/100Mbps(Ethernet Orange:10Mbps, Green:100Mbps)
	Activity(Blue for each serial port)
	Push button for Reset, or Restore to default
	RTC (real time clock)
Serial Interface	16-port (F1DP116S)
	Serial Port Mode (RS-232)
	Serial Connector (RJ-45)
	Baudrate (300 to 115200)
	Flow Control (None, RTS/CTS, Xon/Xoff)
LAN Interface	RJ-45 connector
	IEEE802.3 - 10/100BaseT
	Auto-detecting, Full/Half-duplex selectable
Port Function	Operation Modes
	Console server
	Terminal server

	Dial-in modem
	Serial-to-serial (on port 16 only)
Protocols	TCP, UDP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP, PPP
	SMTP, DNS, NTP
	Dynamic DNS
Protocol Relative Function	TCP Inactivity Time (TCP keep-alive time)
	Serial Inactivity Time
	Port Monitoring
Security	Password Access
	IP Filtering
	SSHv2
	HTTPS / SSL
Authentication	Local user database
	PAP/CHAP (for modem dial-in)
	RADIUS
Management	Local Console (menu or command line)
	SSH, Telnet
	Web pages (HTTP/HTTPS)
	Firmware upgrade via Web interface
	Port buffering and logging
	Full-featured system status display
Power & Environment	AC Input (100 ~ 240 VAC, 50 ~ 60 Hz)
	Operating Temperature: -10 to 80 °C
	Storage Temperature: -20 to 85 °C
	Humidity: 0 – 90% non-condensing
Certifications	CE, FCC
	UL
Mechanical	1U 19” Rack mount
	Dimensions (cm): 43.2 x 18.0 x 4.2

Note: Specifications are subject to change without notice.

2.4 Local Installation

Where to place the Console Sever:

The enclosure of the Console Server is designed for stand-alone or rack-mount configuration. The Console Server can be mounted to a standard 19-inch server rack using the included rack-mount brackets and screws.

Consider the following when deciding where to place the Switch:

• the location of your target devices in relation to your console

• the lengths of the cables you use to connect your devices to the console

• the power source - Connect only to the power source specified on the unit. When multiple electrical components are installed in a rack, ensure that the total component power ratings does not exceed circuit capabilities

Cable-Length Requirements (for CAT5)
Serial binary data signals (RS-232) transmit best up to distances of 50 feet (15m). Beyond that length, the probability of signal degradation increases. For this reason, Belkin recommends that the length of the CAT5 UTP cable between the Switch and the connected servers does not exceed 50 feet (15m).

Cables and Adapters
Belkin highly recommends you use Belkin Category 5e, FastCAT5e, or Category 6 Patch Cables for your Serial Console to help ensure the signal integrity.

Belkin UTP Patch Cables:
A3L791-XX-YYY (CAT5e)
A3L850-XX-YYY (FastCAT™ 5e)
A3L980-XX-YYY (CAT6)
Refer to Appendix B on page ___ for pin-out guide

Belkin Serial adapter:
F1D120 (RJ45F – DB9F DCE)
F1D121 (RJ45F – DB25F DCE)
F1D122 (RJ45F – DB25M DTE)
F1D123 (RJ45F – DB25M DCE)
F1D124 (RJ45F – RJ45M CISCO)
F1D120-8PK (8pack of F1D120)
F1D124-8PK (8pack of F1D124)
Refer to Appendix A on page ___ for detail drawings of each Serial adapter

2.4.1 Desktop or Rack mounting
The Console Server can be placed on desktop or rack mounted on 19”/1U racks:

Note: Before you begin, locate the MAC address and device number on the back of the Switch. You may need these numbers later in the installation process, so it is highly recommended that you record these numbers below before mounting the Switch to your rack.

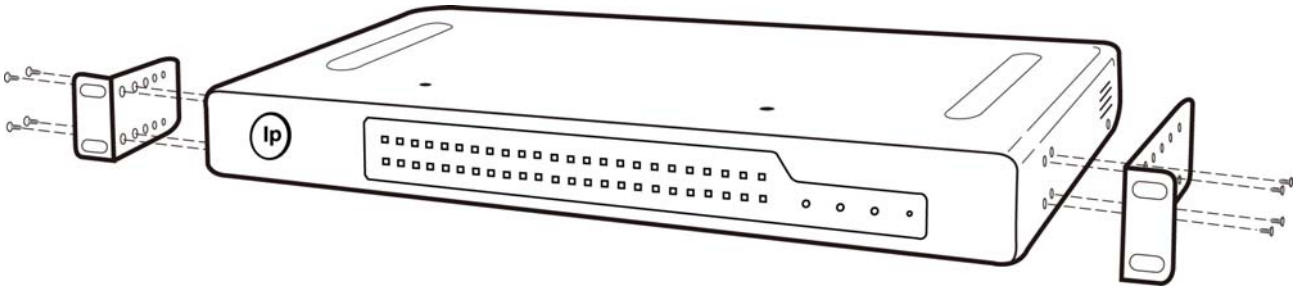
MAC Address	Serial Number

The Switch includes adjustable mounting brackets ideal for installation in 19-inch racks. The mounting brackets feature three adjustment positions that allow you to set the Switch's face flush with the ends of the rails, or to extend the Switch past the front of the rails. Please follow these simple steps to achieve the desired adjustment.

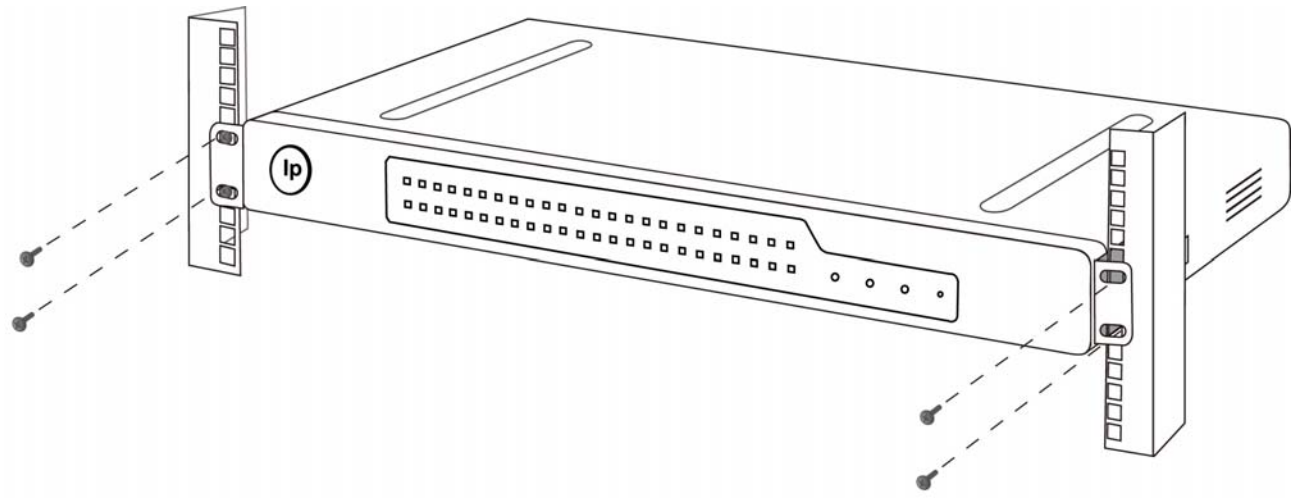
Rack Mounting

1.1 Determine how far you would like the Serial Console to protrude from the rack. Select a bracket-hole scheme.

1.2 Attach the bracket to the side of the Console using the Phillips screws provided. (Refer to diagram below.)



1. Mount the Switch to the rack rails and secure with screws. (Refer to diagram below.)



Your Serial Console is now mounted securely to the rack and you are ready to connect your target devices.

Connecting the target devices to the Serial Console

1. Power down the target device(s) the will be connected to your Serial Console
2. Connect the Ethernet cable to the to the port labeled LAN
3. Locate the included power cord and plug the appropriate end into the power socket on the rear of the Serial Console. Plug the other end into an appropriate AC wall outlet.

Note: Allow about 100 seconds for the Serial Console to complete the bootup process.

4. Choose an available numbered port on the rear of your Serial Console. Plug one end of a UTP patch cable (4-pair, up to 15 meters) into the selected port and plug the other end into the target device. You may need to add the appropriate adapter to interface with your target device. Please refer to Appendix ___ in this manual for more details.
5. Repeat this procedure for all target devices. (Refer to diagram below.)

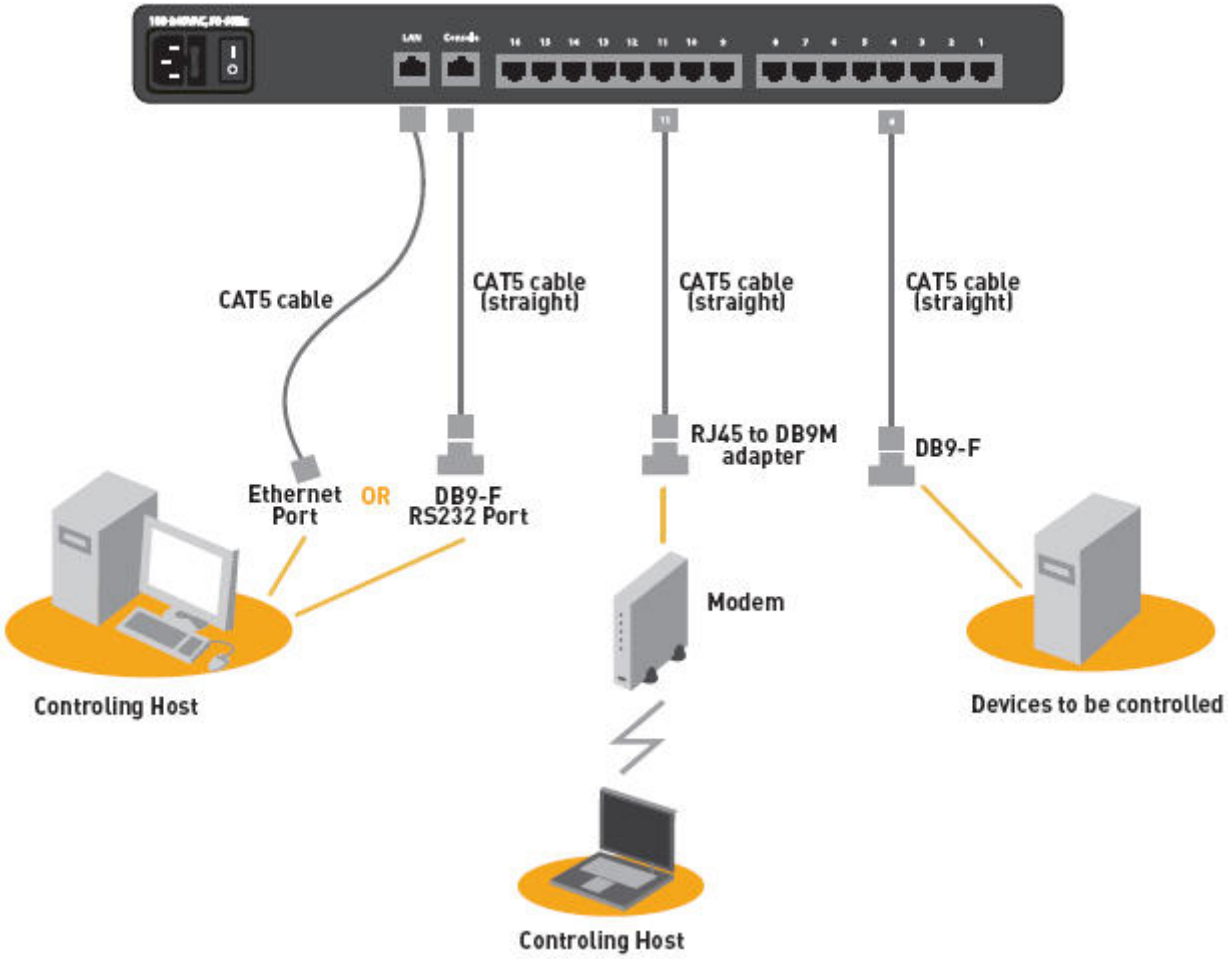


Figure 1 –Cable Connection Setup- This diagram depicts sample cable connections for different interfaces.

Network Configuration

Before you can connect to a target device you will need to configure the network settings. The Serial Console offers two methods of setting the network: via Web browser interface

or through the local console port.
The Serial Console offers support for both Dynamic Host Configuration Protocol (DHCP) and static IP addressing. Belkin recommends that IP address be reserved for the Serial Console and that it remains static while connected to the network.

Web Browser Interface
The web interface provides an easy way to configure the Serial Console. The administrator can configure all features through the web.

Initial Settings
The following section provides instructions for setting the IP address for the OmniView Serial Console.

Step 1 Identifying the IP Address

Once your Serial Console has been connected to your network and is powered up, a Dynamic Host Configuration Protocol (DHCP) server on your network will automatically assign the Switch an IP address, gateway address, and subnet mask.

To identify the IP address on your network, use the MAC address located on the back of the Switch. If no DHCP server is found on your network, the Switch will boot with the following static IP address: 192.168.2.156.

If you want to connect more than one Serial Console to the same network and there is no DHCP server available, connect each Serial Console to your network one at a time and change the static IP address of each unit before connecting the next unit.

Note: If a DHCP server later becomes available on your network, the Switch will take a new IP address from the DHCP server. To keep the original static IP address, you will need to disable DHCP (see page ___).

Step 2 Logging into the Web Interface
After you identified the IP address of your device, open your web browser. A list of supported browsers can be found on page ___).

Type in the Serial Console's IP address in the browsers address field, using this format: http://XXX.XXX.XXX.XXX (example: http://76.255.43.173) . The login page will appear (see Fig. 2). Bookmark the page for easy reference.

Note: HTTPS can be used for communication over an encrypted secure socket layer

(SSL). When first connecting to the Switch's HTTPS configuration page, two browser security warnings may appear. Click "Yes" on both warnings.

Fig. 2 Login Page

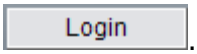
Type in the following default user name and password (case-sensitive):

User	Password
admin	admin

There are two levels of access privileges:

User Name	Default Password	Access Privileges
admin	admin	full access
(user define)	(user define)	only can access to **Serial Port** and **System Status**

The administrator can add or remove a user easily via the web pages of System administration.

Click 

. The web interface will open at the Connect page (see Fig. 3).

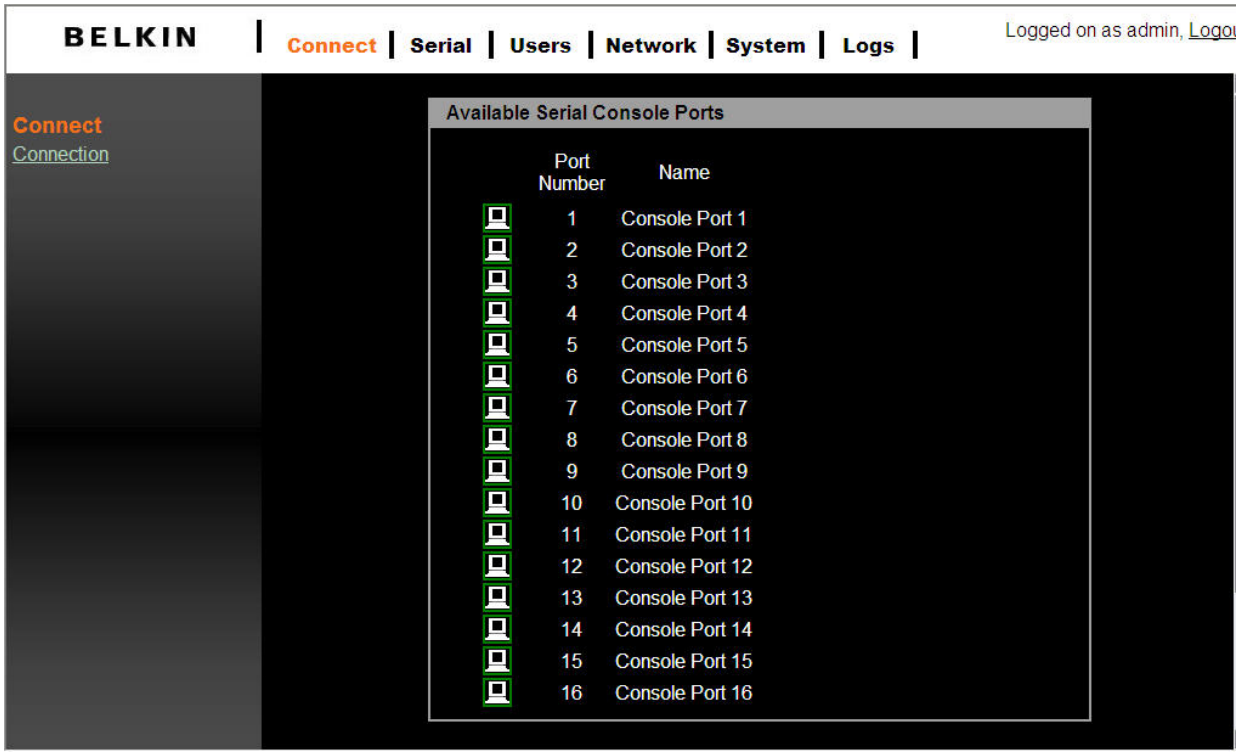


Fig. 3 Main-Connect Page

Step 3 Network Configuration

Click on Network to go to open the Network-Configuration page (see Fig. 4).

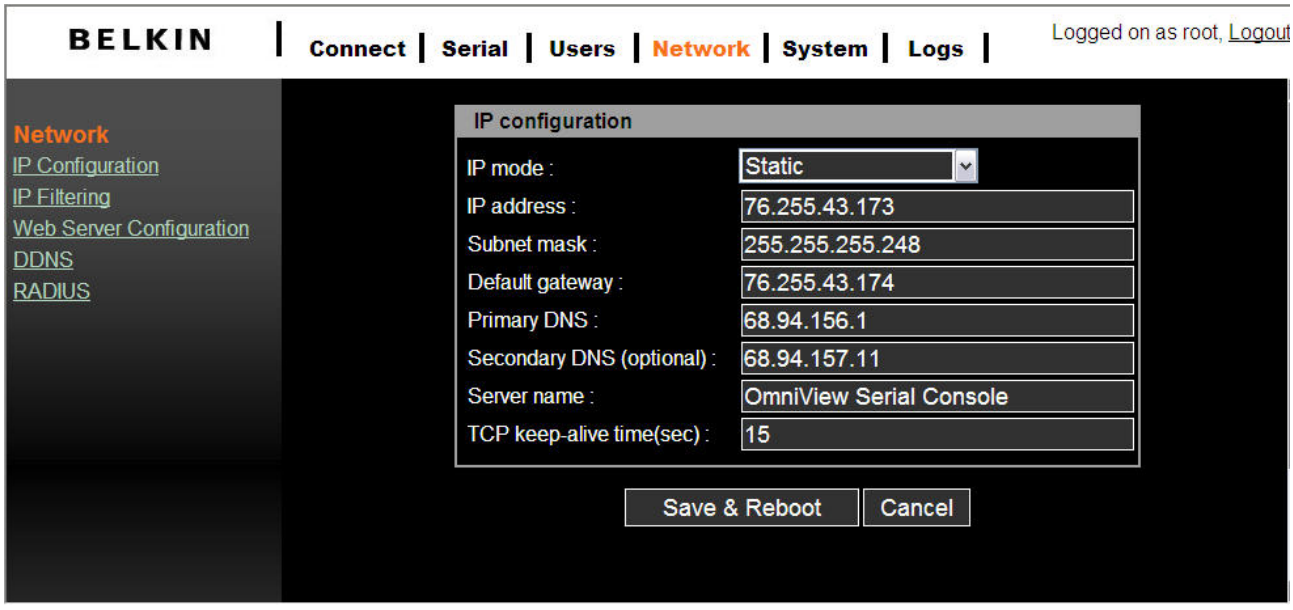


Fig. 4 Network Configuration Page

Here you can assign a static IP and other network settings.
Click on Save& Reboot to store any Network configuration settings

Note: If the user leaves the web browser idle for more than 30 **minutes** the login session

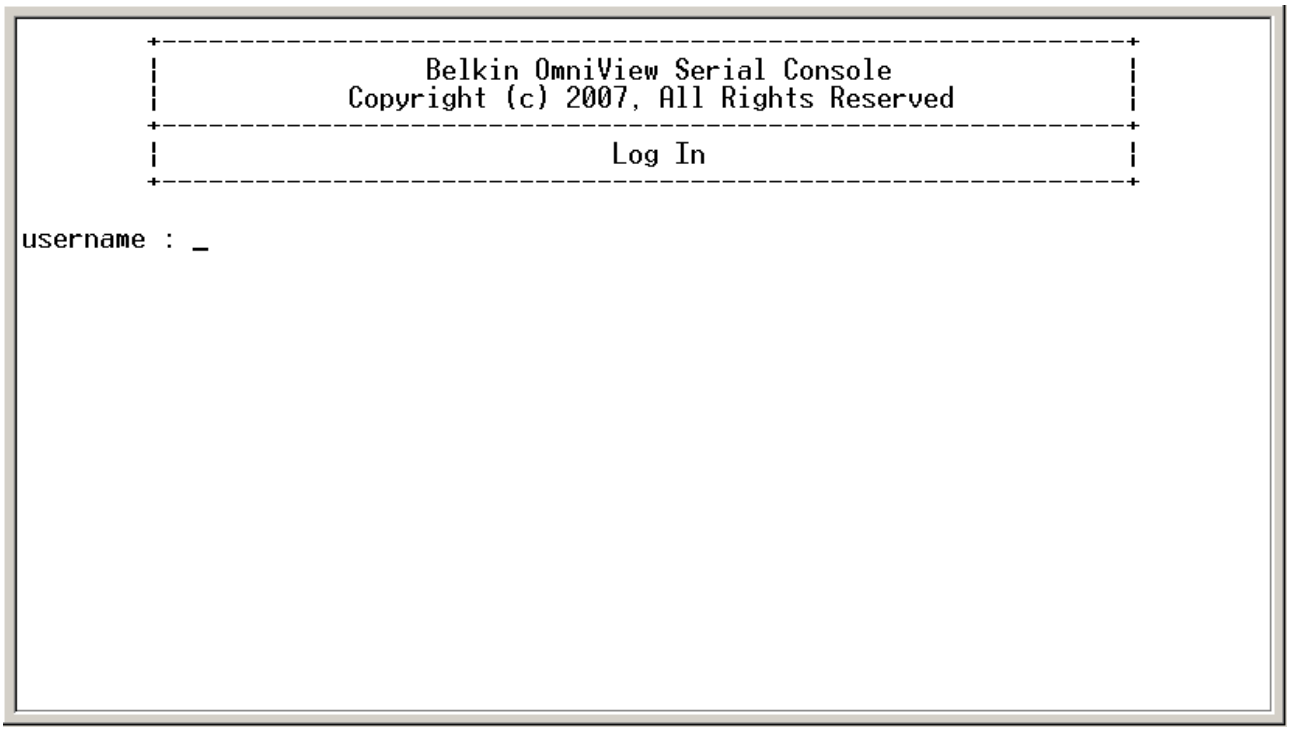
will time-out and terminate the session.

Assigning IP from the Local Console Port - VT-100 (Console, Telnet, SSH)

The Serial Console also offers a user-friendly menu-driven Command Line interface. You can simply connect a VT-100 terminal to the local console port to access to the Serial Console. This is useful when you do not know the network settings of the Serial Console, and can not access it. Through the local Console port you can view or change the settings (IP address, subnet mask, etc).

Step 1

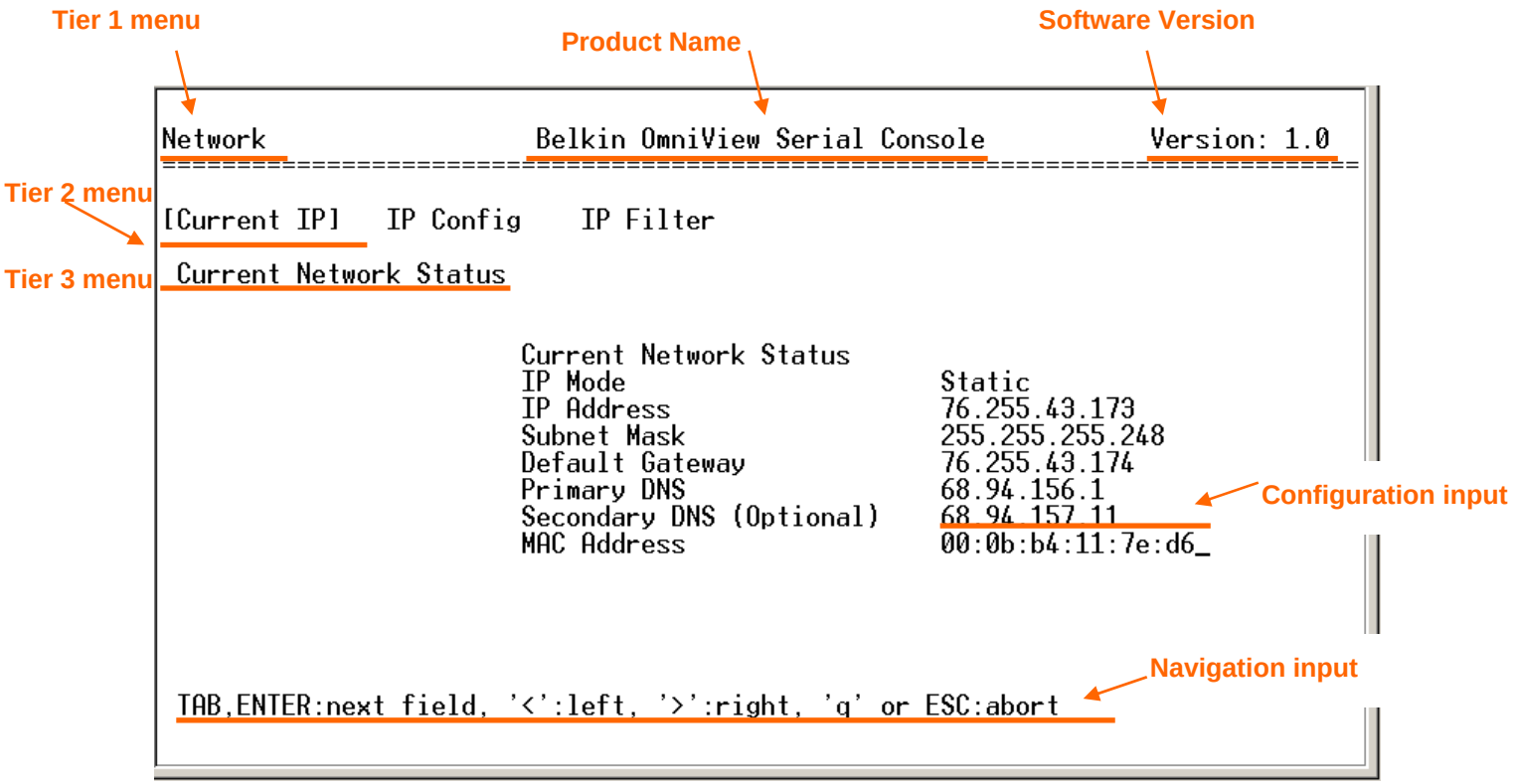
1. Connect the console port on the rear panel to a serial port on a PC host using the CAT5 cable and the appropriate RJ45/DB9F adapter included with the Belkin Serial Console.
2. Configure a terminal emulation program, such as HyperTerminal, using the following parameters:
   - Baudrate = 115200
   - data bits = 8
   - stop bits = 1
   - parity = none
   - flow control = none

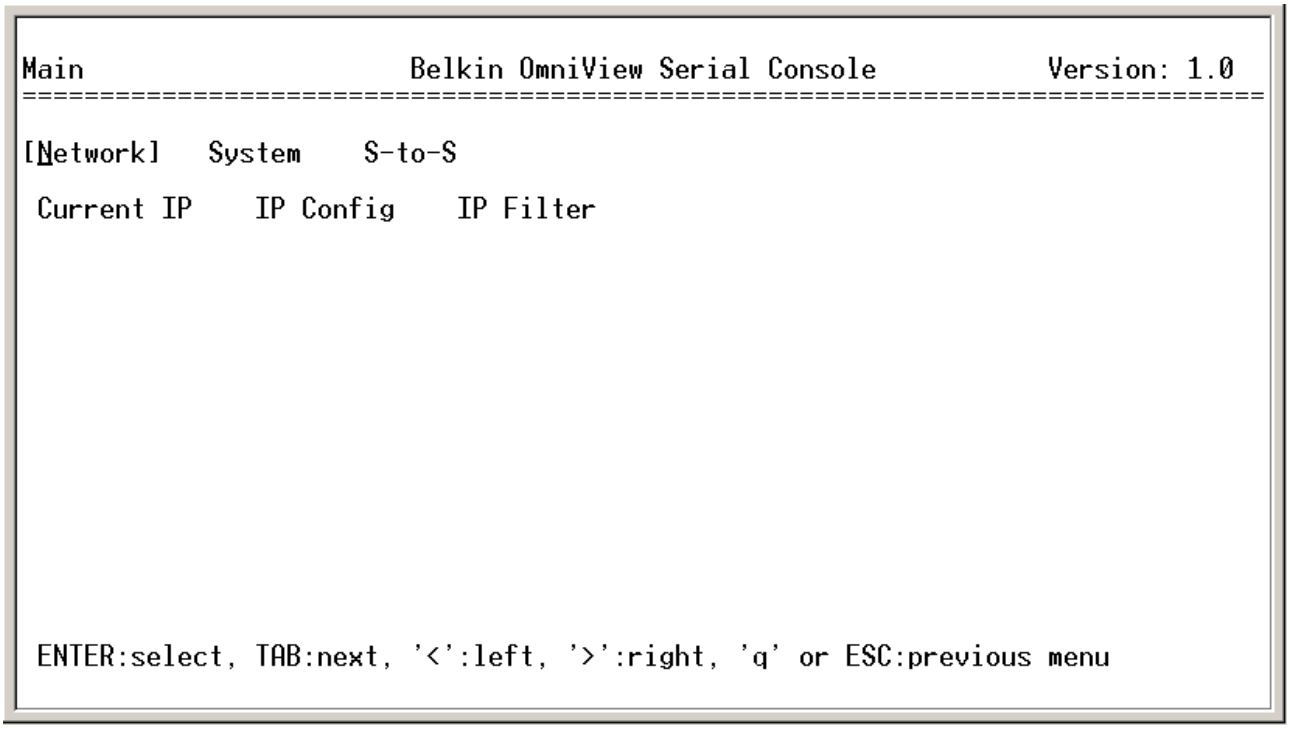


Note: User names and passwords are the same as set through the Web Interface. The defaults are **admin/admin.**

The following figure depicts the structure of the interface.

The menu layout





Network > IP Config

The following page shows the IP configuration items.

1. For **IP mode --** you can press **SPACE** bar to select **Static** mode or **DHCP** mode.
2. For **IP Address**, **Subnet mask**, **Default Gateway**, **Primary DNS**, and **Secondary DNS** -- you can change these network settings.
3. After changing the settings, the final enter, the Serial Console will prompt to confirm YES or NO. If select YES, the Serial Console will reboot and save the settings into the Flash memory.

Network > Current IP

To show the current network settings.

Network > IP Filter

To enable/disable IP filter function.

System > Reboot

To reboot the Serial Console

System > Reset to Default

To reset configuration to Factory Default Settings.

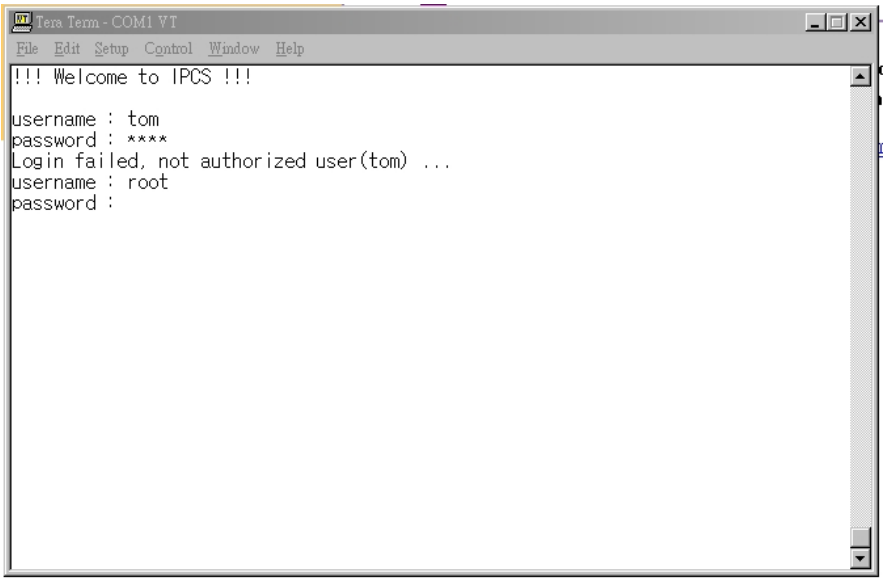
Note: Only the **admin** user has the privilege to perform this function.

System > Status

To show the system status.

S-to-S > Select Serial to Serial port

To configure an internal serial port-to-serial port connection. The last serial port or internal port can be configured. Refer to section ___ **Serial-to-Serial Function** for more details.



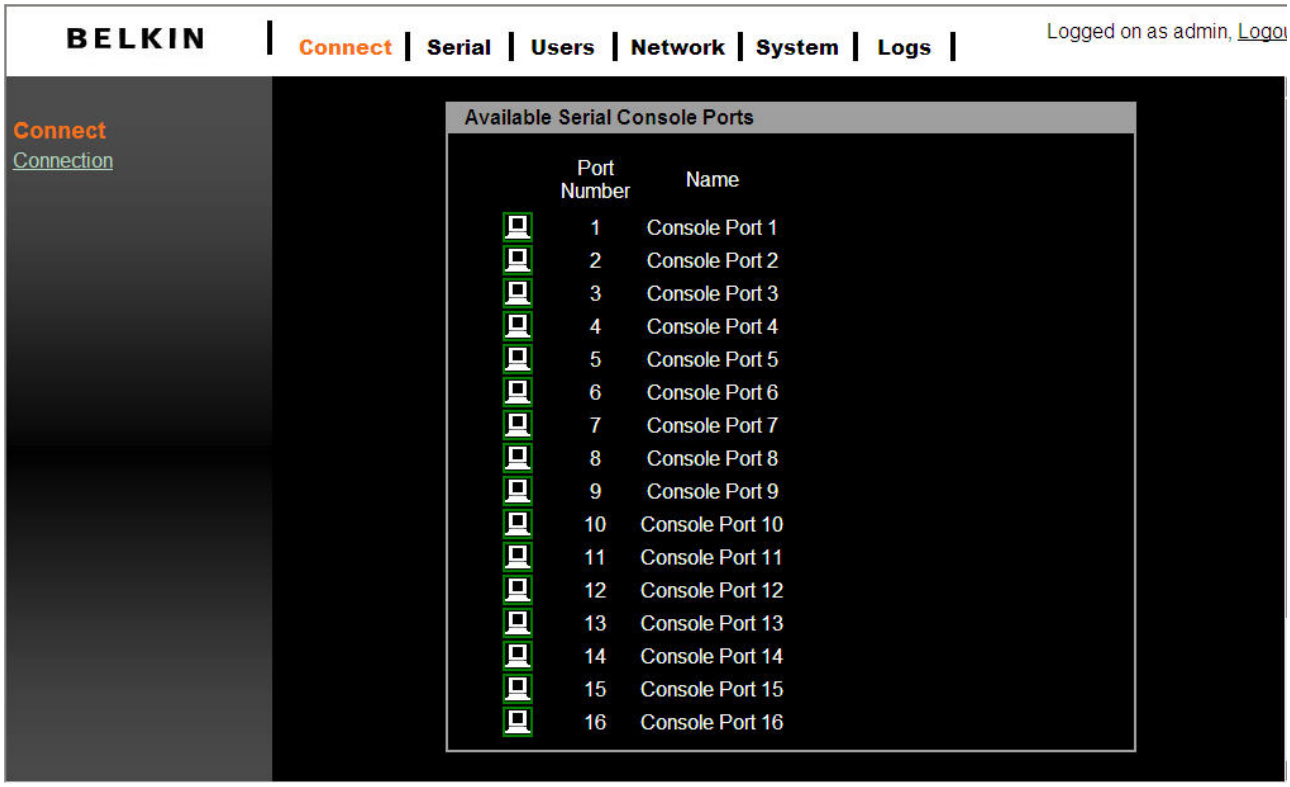
Note:
Only the **admin** user has the privilege to login to VT100. All the other users are not authorized to make configuration with VT100.

2.5 Web Browser Management Interface

The Serial Console supports both HTTP and HTTPS (HTTP over SSL) protocols. The users must authenticate themselves by logging into the system with a correct user name and password

To access the Serial Console Web management pages, enter the unit's IP address or resolvable hostname into the web browser's URL/Location field. This will direct you to the login screen.

Figure below shows the homepage of the Web management interface. A menu bar displays along the top of the page. The submenu will display along the left side of the page and will allow you to modify parameter settings for top-menu item selected.



Where available the page will allow the user to **Apply** or **Cancel** their actions. To apply all changes, select **Apply and** the new values will be applied to the configuration.
If you do not want to save the new values, then simply click **Cancel** and all changes made will be removed and the previous values restored.

3. Network

You can configure the network IP settings via VT-100 or web interface. This section describes configuration through the web interface.

3.1 IP Configuration

The Serial Console requires a valid IP address to operate within the user's network environment. If the IP address is not readily available, contact the system administrator to obtain a valid IP address for the Serial Console.

There are two types of IP assignments you can choose from:

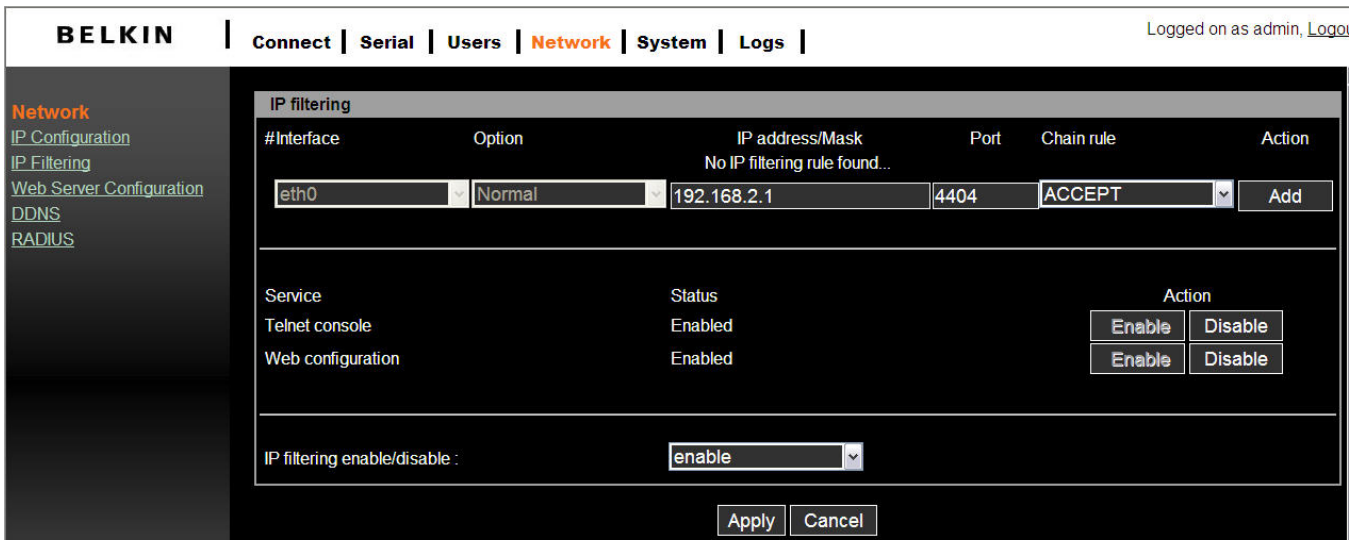
- Static IP
- DHCP (Dynamic Host Configuration Protocol)

The unit ships with DHCP set to default. If no DHCP server is found on your network, the Switch will boot with the following static IP address: 192.168.2.156.

The new IP configuration setting can be saved by clicking **Save & Reboot**.

3.2 IP Filtering

The IP filtering function keeps unauthorized hosts from accessing the Serial Console by specifying rules.



The **IP address/Mask** specifies the host range by entering base host IP address followed by **/** and subnet mask. The host IP addresses to be filtered based on the rule defined. The table below provides examples of IP address/Mask settings.

Specified host range	Base Host IP address	Subnet mask
Any host	0.0.0.0	0.0.0.0
192.168.2.120	192.168.2.120	255.255.255.255
192.168.2.1 ~ 192.168.2.254	192.168.2.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.2.1 ~ 192.168.1.126	192.168.2.0	255.255.255.128
192.168.2.129 ~ 192.168.2.254	192.168.2.128	255.255.255.128

The **Port** is a port or port range of the Serial Console which hosts try to access to.

Chain rule

The **Chain rule** determines whether the access from the hosts is allowed or not. It can be one of two values:

- ACCEPT : access allowed
- DROP : access not allowed

When the Serial Console receives a TCP packet, it will process the packet with the chain rule depicted below. The process order is important; The packet will enter the chain rule 1 first, if it meets the rule then it will take action, otherwise it will go on to chain rule 2.

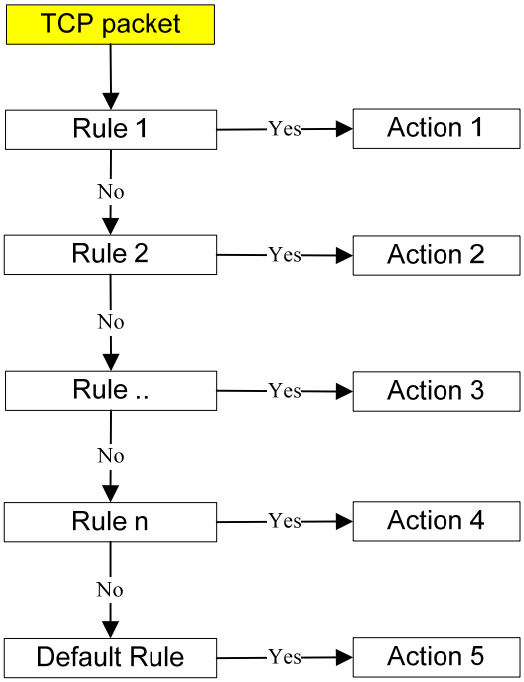
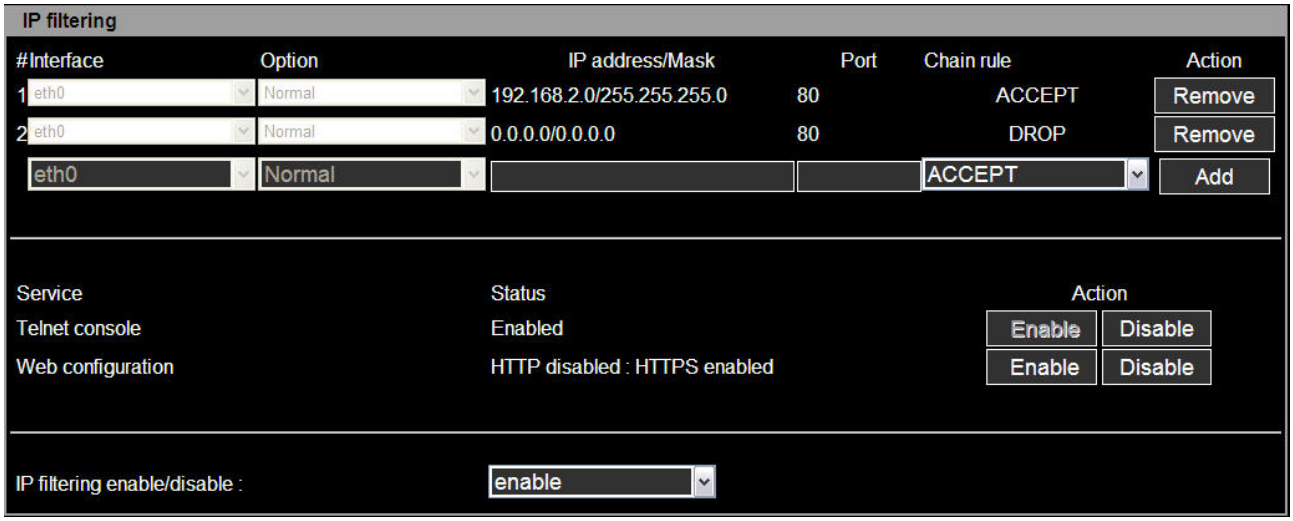


Figure 2 Chain Rule of IP Filter

You can add a new IP filtering rule by setting the properties at adding line and then clicking the button **Add**. You can remove a rule by clicking the button **Remove**.



In the example above, the rules applied in the following order:

#1. Those hosts belonging to subnet 192.168.2.x are allowed to access to the Serial Console (through http port 80).

#2. All hosts are not allowed to access to the Serial Console (through http port 80).

After these rules are applied, only the hosts which belong to the subnet 192.168.2.x can access to the Serial Console (through http port 80).

In addition to the IP filter chain rule mentioned above, the web interface also provides a convenient way to **Enable** / **Disable** telnet (port 23) or web configuration port (port 80 / 443). These services are mainly for the Serial Console configuration. Click on Enable / Disable button on Action field will help to add / modify chain rule quickly without the hassle of manually editing the rule

> **Note**:
> In order to get a better text alignment, a VT100-awared telnet client is preferred to align the text output. PuTTY a one of recommended telnet clients to get better UI text alignment. It is downloadable from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

3.3 Web Server Configuration

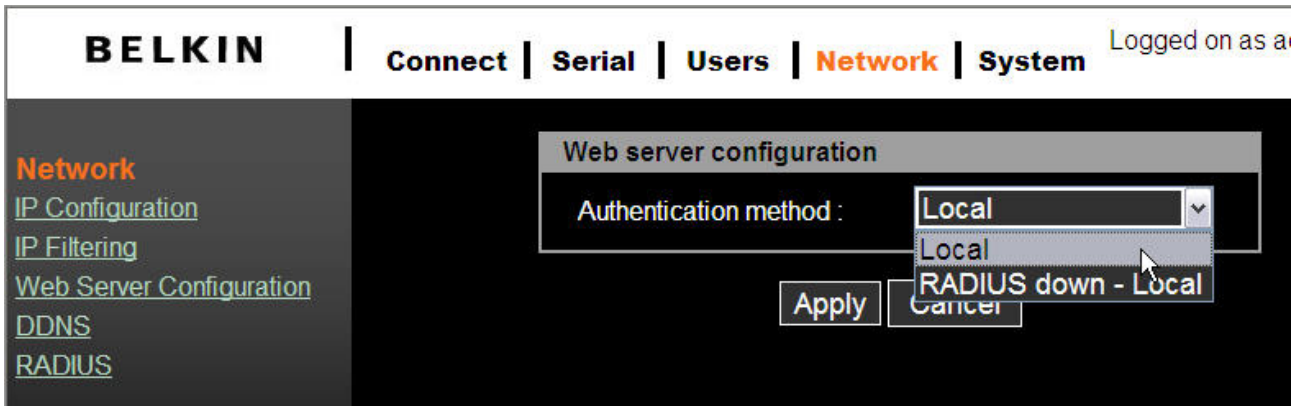
The Serial Console Web server supports both HTTP and HTTPS (HTTP over SSL)

services simultaneously.

You can select user authentication method for the web login. The Serial Console currently provides authentication methods of **Local** and **RADIUS**.

3.3.1 Local

The Serial Console by default points to the local database for the web server login user authentication.



3.3.2 RADIUS and Local

The Serial Console refers to RADIUS server for user account authentication first. If the user account is not found or RADIUS server is down, the Serial Console looks up its own local database to find the user account. The unit will not permit a user to login if neither RADIUS nor local database account is found. The RADIUS server setting is user-configurable via RADIUS server configuration page. Refer to page ____

3.4 Dynamic DNS

If a user connects the Serial Consoles to a DSL line or uses a DHCP configuration to get a dynamic IP address from the network, the IP address may not the same as previous. This can make it difficult to know if an IP address has changed, or what the new IP address is.

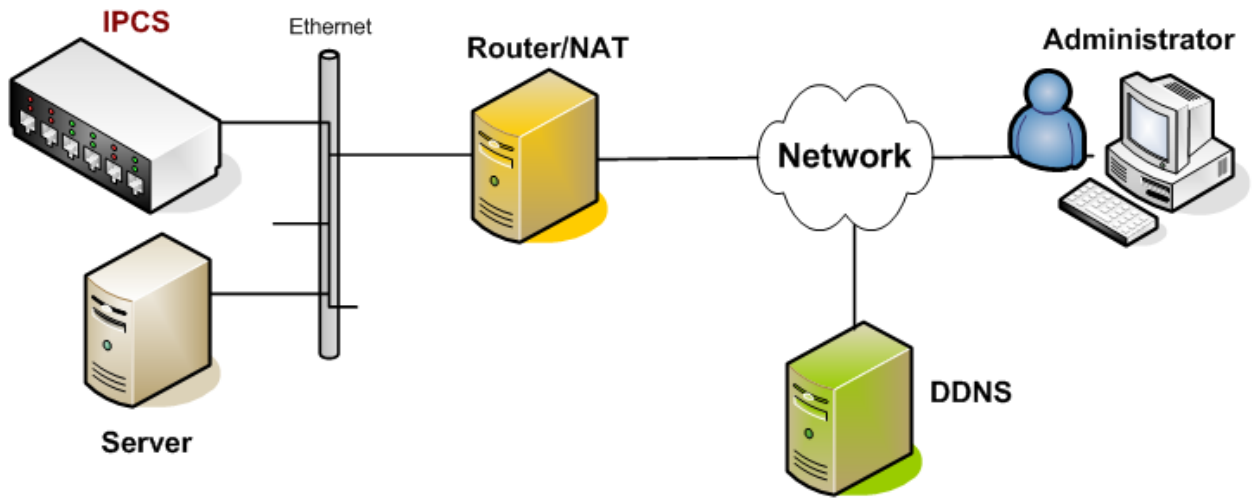
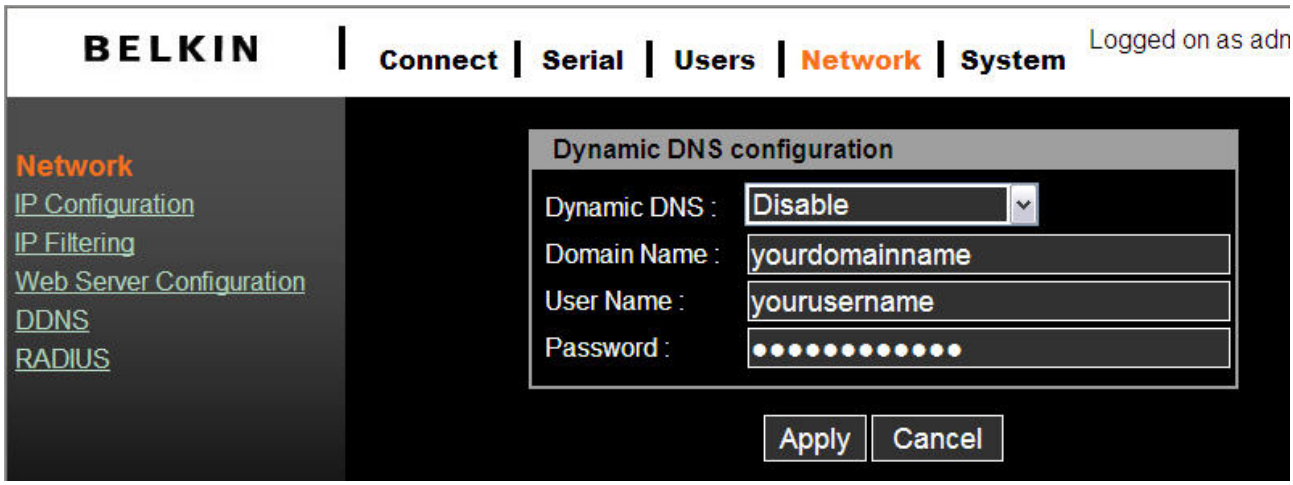


Figure 3 Dynamic DNS

Dynamic DNS service is provided by various ISPs and organizations to deal with the above issue. By using a Dynamic DNS service, you can access the Serial Console through the hostname registered in the Dynamic DNS Server regardless of any IP address change. By default, the Serial Console only supports Dynamic DNS service offered at Dynamic DNS Network Services, LLC (www.dyndns.org).

To use the Dynamic DNS service provided by Dynamic DNS Network Services, the you must set up an account in their Members' NIC (Network Information Center - http://members.dyndns.org). You may then add a new Dynamic DNS Host link after logging in to their Dynamic DNS Network Services Members NIC.

After enabling the Dynamic DNS service in the Dynamic DNS Configuration menu, you must enter the registered Domain Name, User Name, and Password. After applying the configuration change, you will be able to access the Serial Console by using only the Domain Name. The DNS (Domain Name Systems) is the internet service that translates your domain names into IP addresses.



Note:
The domain name field requires a Qualified Domain Name (FQDN) instead of just registered hostname.

3.5 RADIUS

Authentication is the process of identifying an individual, usually based on a username and password. The Serial Console supports various authentication options, such as **Local, RADIUS,** to authenticate the users who access the serial port. When the authentication is

set to **Local**, the unit will use its own user list to authenticate a user. If configured otherwise, the Serial Console will request authentication from the external authentication servers (i.e. RADIUS) Figure below shows conceptually the user authentication process when using an external authentication server.

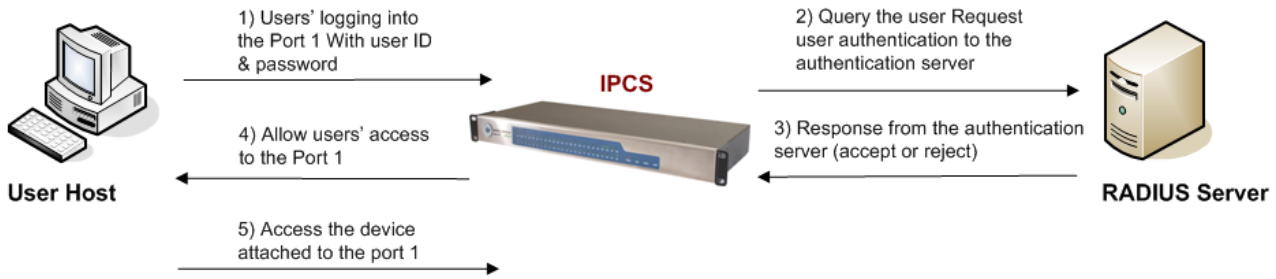
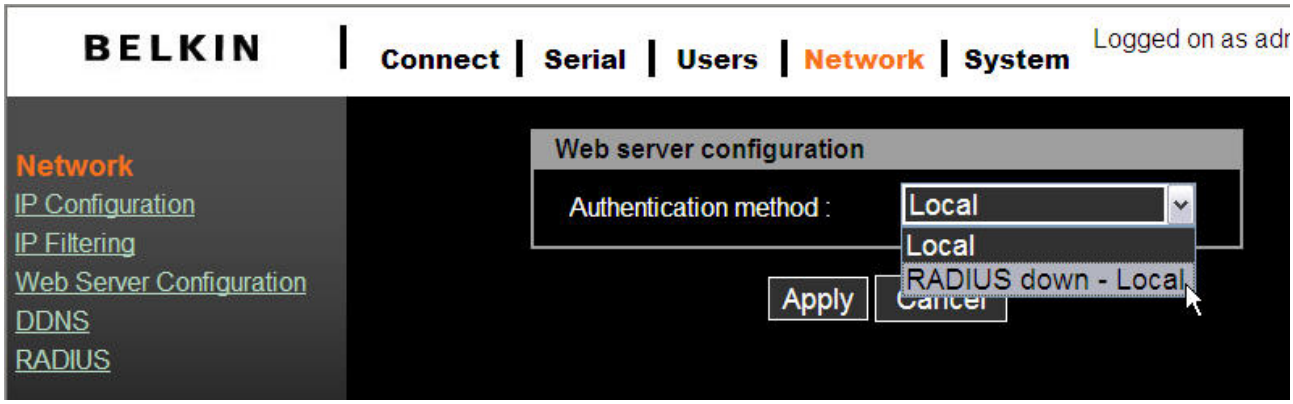
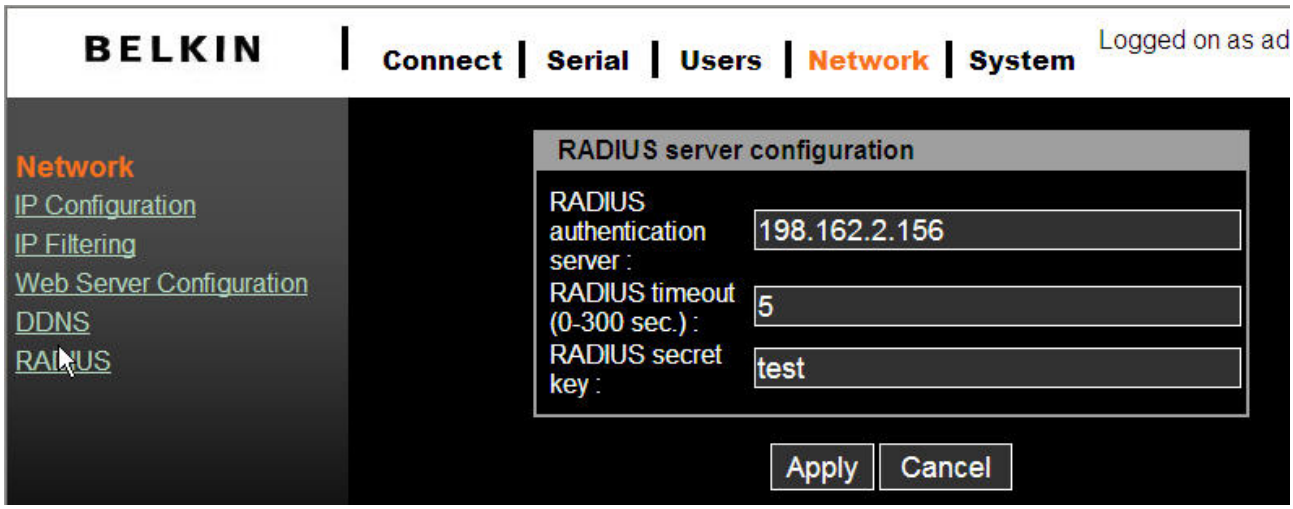


Figure 4 RADIUS



Radius server configuration



Note:
In order to make RADIUS service effective, a RADIUS server must be installed prior use.

3.6 HTTPS/SSL

The Serial Console supports both HTTP and HTTPS (HTTP over SSL) services simultaneously. You can to enable or disable security function of each port individually. HTTPS provides a secure, encrypted web interface over SSL (secure sockets layer). The following steps should be used for HTTPS protocol:

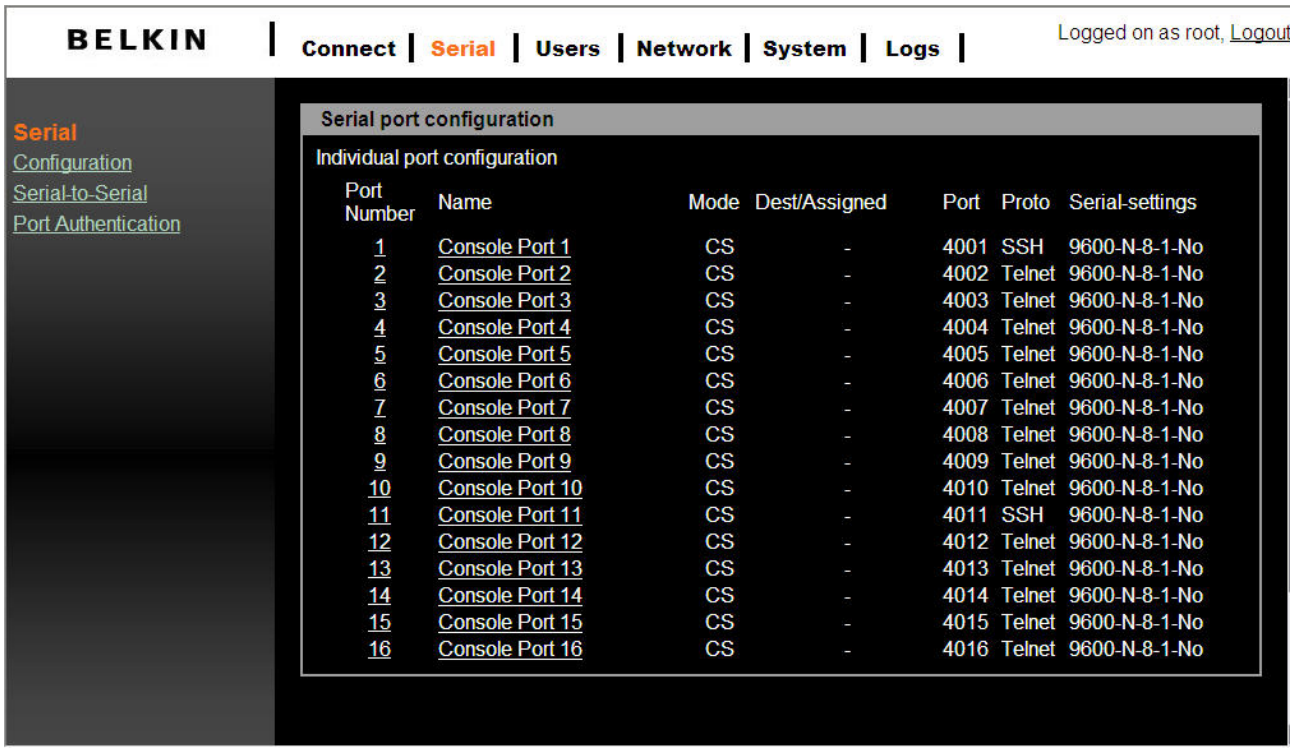
1. Change the URL from "http://xxx.xxx.xxx/" to "https://xxx.xxx.xxx/".
2. After the connection is established, your browser will display a "Lock" icon.

Double click on the lock symbol to display detailed certificate information.

4. Serial

4.1 Configuration

Under the **Serial** menu heading, click **Configuration** to show the port summary list.

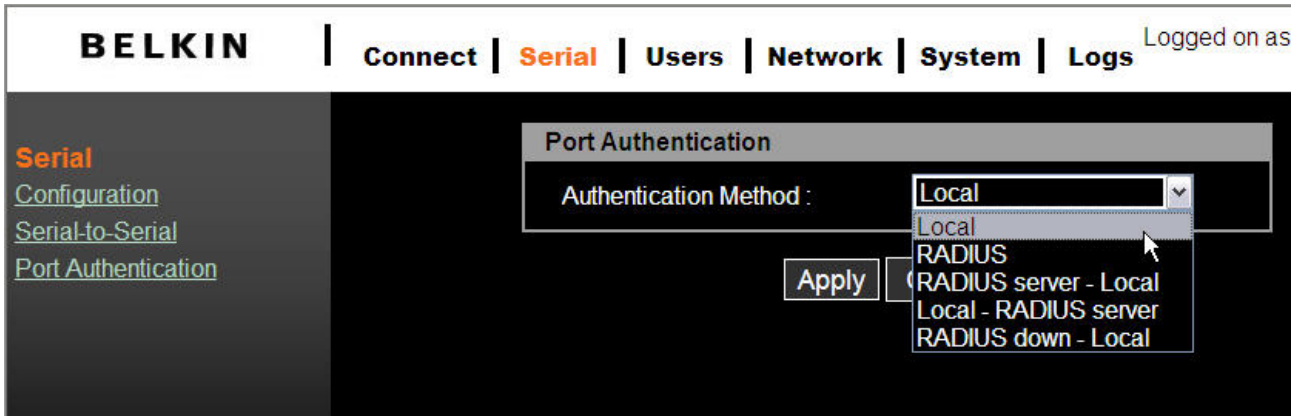


Note that if the **Serial Port** is disabled, **Serial port configuration** panel will display the port in dark grey font. An enabled serial port will be displayed in white bold font.

4.1.1 Port Authentication

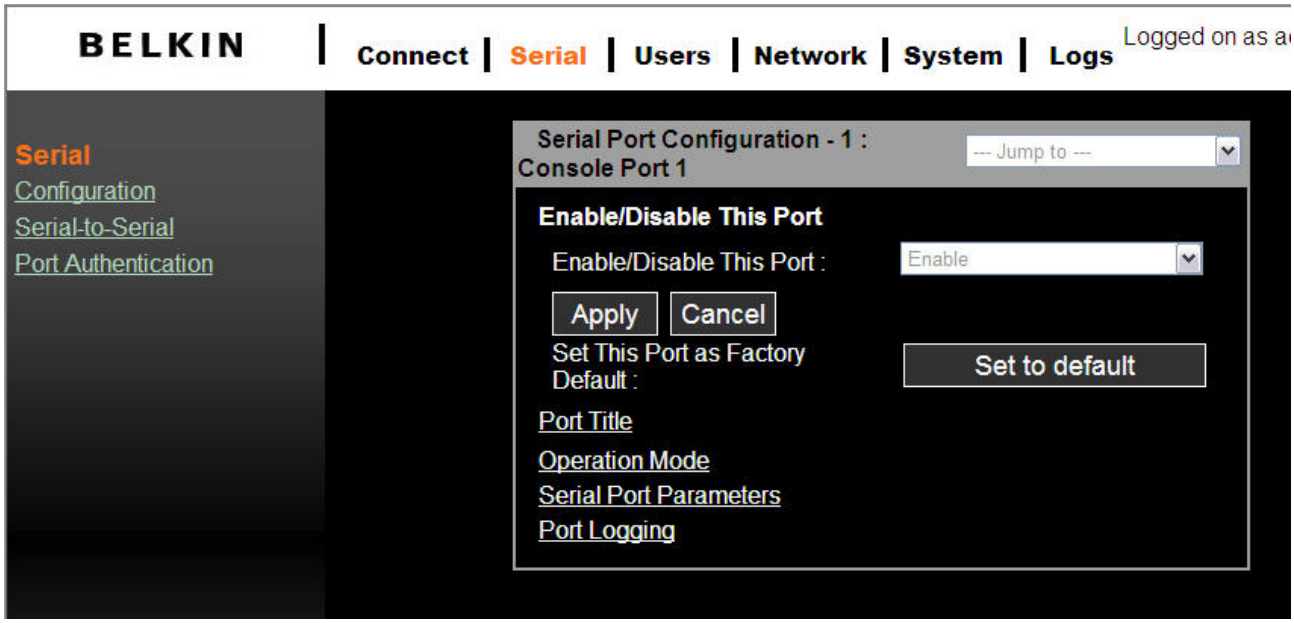
Authentication is the process of identifying an individual, usually based on a username and password. The Serial Console supports various authentication options, such as **Local, RADIUS,** to authenticate the users who access the serial port. Refer to page ___

When the authentication is set to **Local**, the Serial Console will use its own user list to authenticate a user. If configured for RADIUS, the unit will request authentication from the external authentication servers (i.e. RADIUS) Figure below conceptually illustrates the user authentication process when using an external authentication server.



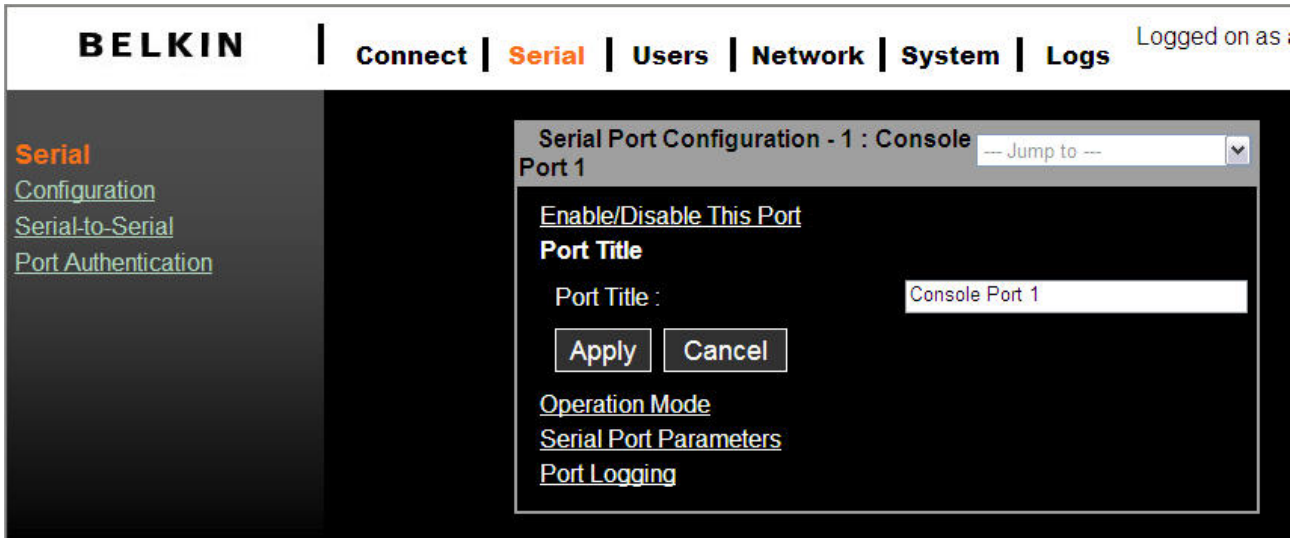
4.1.2 Port Enable/Disable

Each serial port can be individually enabled or disabled. A disabled serial port cannot be accessed by user. User can reset the serial port to default settings by clicking the button **Set to default**.



4.1.3 Port Title

Users can enter descriptive information for each port based on the device attached to it.



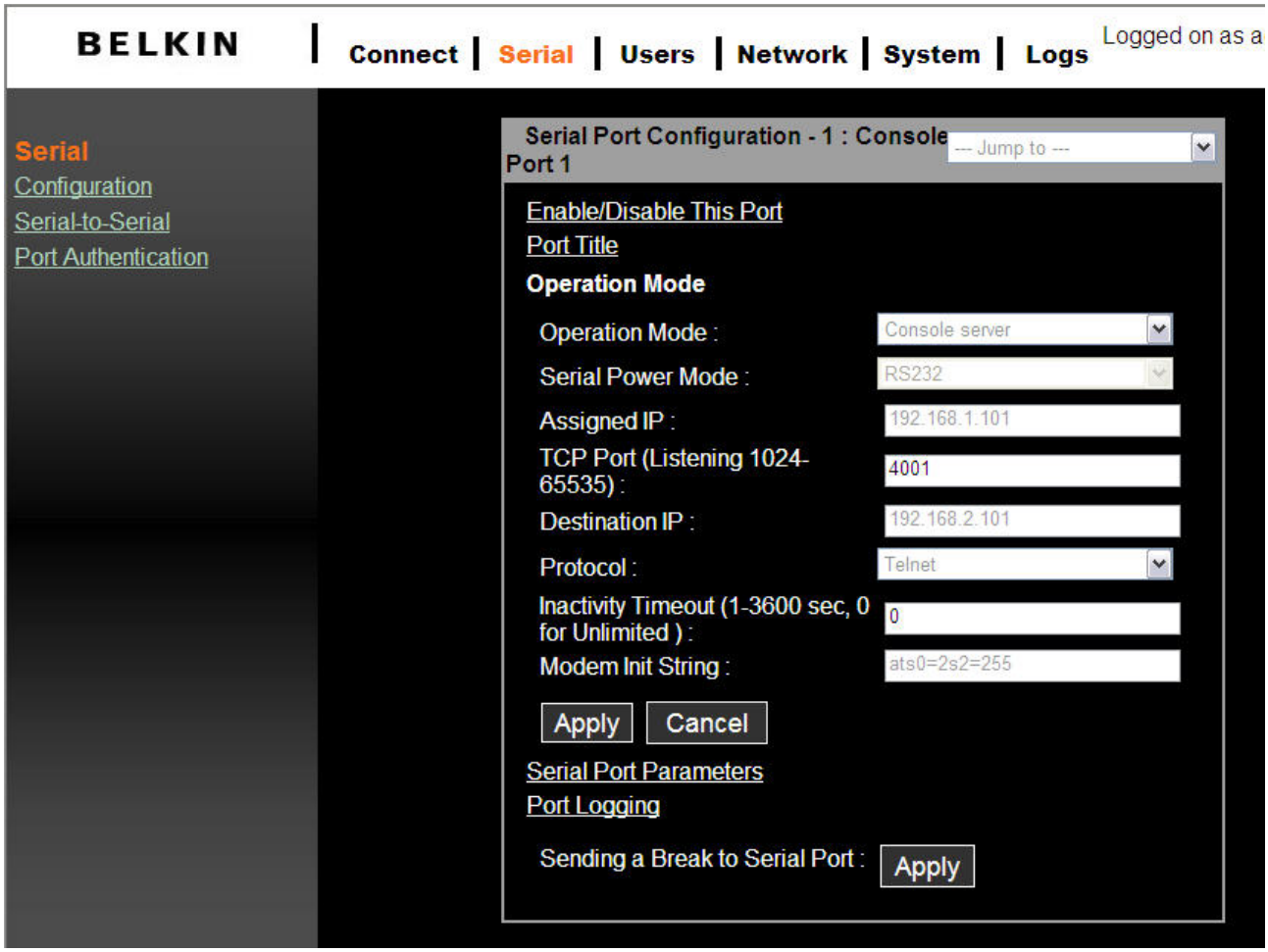
We can use the shortcut ***--Jump to--*** on the upper-right corner to select and configure a different port.

4.1.4 Operation Modes

The Serial Console unit provides four types of operation modes. These are described below.

Notes:

- The last port (e.g., Port #16) can also be used as **External ESP (Entry Serial Port)** in **Serial-to-Serial** operation mode. Refer to the section **Serial-to-Serial** Function for details.



4.1.4.1 Console Server Mode

Configuring a serial port as a console server creates a TCP socket on the unit that listens to a Telnet or SSH client connection. When you connect to the TCP socket, you have access to the device attached to the serial port as if the device were connected directly to the network. Data stream can be sent back and forth between the device and the Telnet/SSH client program.
RawTCP is also supported with the Console Server Mode.

The following parameters are configurable In **console server** mode:

Listening TCP port number
You can also access a serial port through the IP address of the Serial Console and the Listening TCP port number of the serial port.
If the IP address of the Serial Console and the serial port are assigned as 192.168.123.100 and Listening TCP port number 4001, the user can connect to the port as follows:
telnet 192.168.123.100 4001

Protocol

Select **Telnet, SSH** or **Raw TCP** as the protocol. If the users are using a Telnet client program, select **Telnet**. If the users are using an **SSH** client program, select **SSH**. When **Raw TCP** is selected, direct TCP socket communication is available between the Serial Console and the remote host.

Inactivity timeout

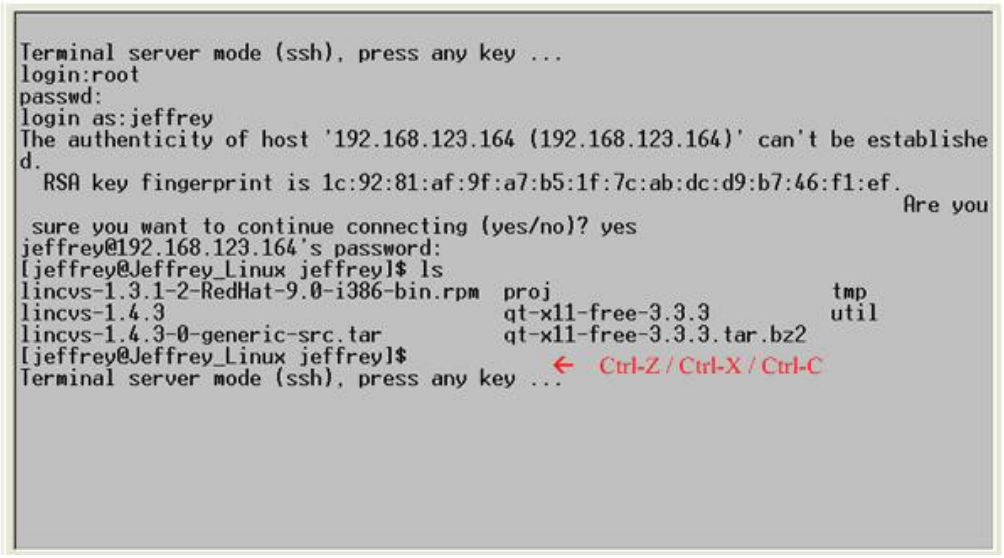
Enable this feature to avoid a client holding on to a TCP connection while there has been no activity on a serial port for a long period of time. If the **Inactivity timeout** is enabled, and no data activity between the Serial Console and the Telnet/SSH client for the specified inactivity timeout interval (i.e., no data activity through the serial port), the existing TCP session will automatically be closed. If you want to maintain the connection indefinitely, configure the inactivity timeout period to 0.

TCP Keep-alive (no configuration required)

In order to avoid TCP connection lockup, the Serial Console will continue to check the connection status between the Telnet/SSH client and the Serial Console by periodically sending “keep alive” packets. If the Telnet/SSH client does not answer the packets, the system will assume that the connection is down. The Serial Console will then close the existing Telnet/SSH connection, regardless of the inactivity setting. This will prevent the TCP connection from locking when an application is improperly closed or the network link is interrupted.

4.1.4.2 Terminal Server Mode

In terminal server mode, the Serial Console’s serial port is configured to wait for data from the device connected to the port. If data is detected, the Serial Console will initiate a TCP session as a Telnet or SSH client to a pre-defined server. The server must be defined by users before the port can be configured for a Telnet or SSH client. This mode can be used to access servers on the network from a serial terminal. RawTCP is also supported with the Terminal Server Mode.



In order to terminate a Telnet/SSH/RawTCP session in Terminal Server Mode, you may use these three control key sequences (Ctrl-Z / Ctrl-X / Ctrl-C).

4.1.4.3 Dial-in Modem Mode

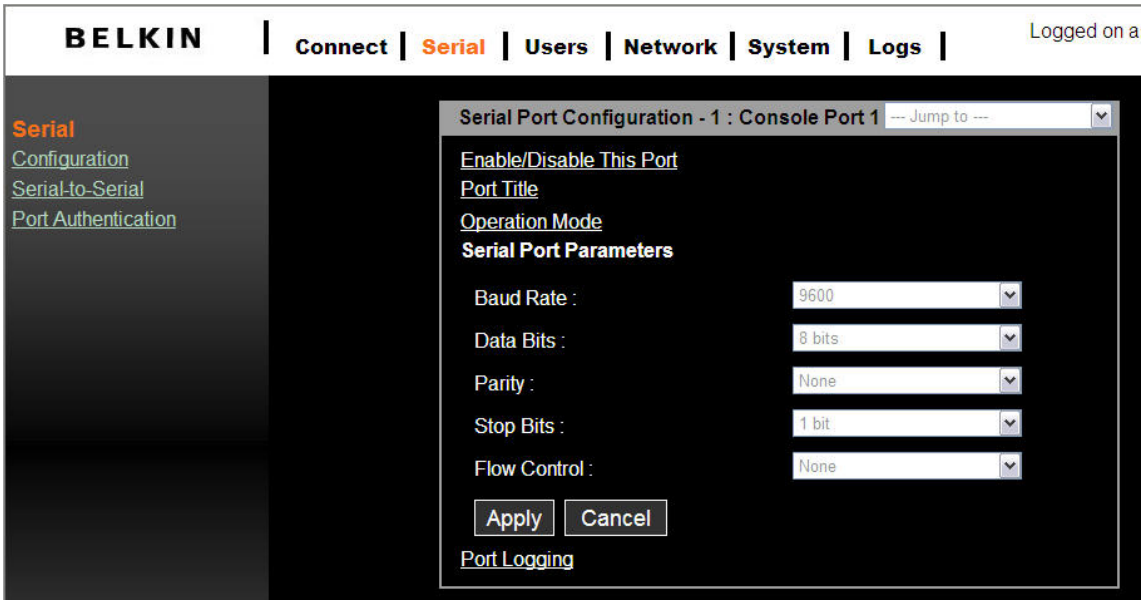
In this mode, the Serial Console assumes an external modem is attached to the serial port and waits for a dial-in connection from a remote site. When a user dials-in using a terminal application, the Serial Console will accept the connection and display the appropriate prompt or menu for you that logged in.

4.1.4.4 Serial –to Serial Mode

In Please refer to section 4.3 for details for this mode.

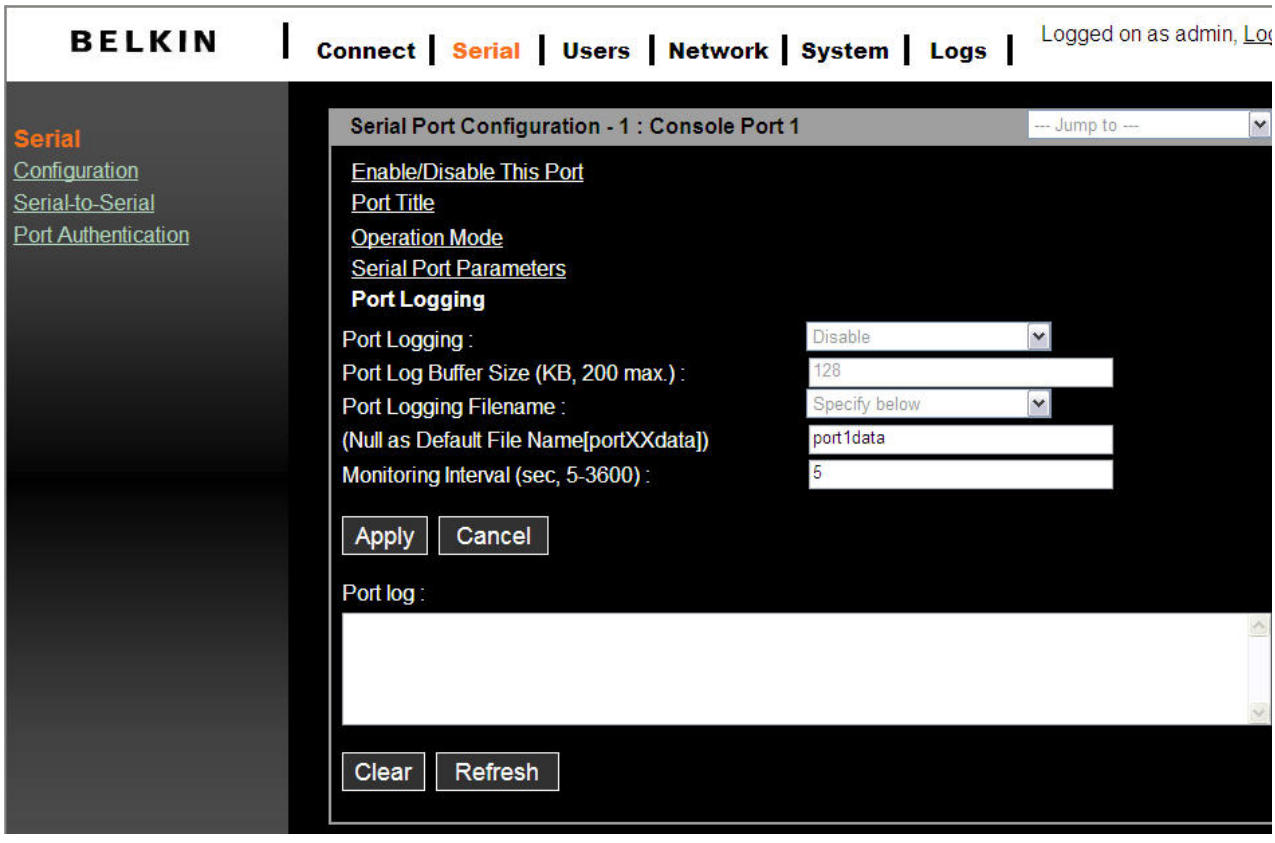
4.1.5 Serial Port Parameters

To connect the serial device to the Serial Console serial port, the serial port parameters of the Serial Console should match exactly to the requirements of the attached serial device.



4.1.6 Port Logging

While in Console Server mode, the data received from the tracking serial port will be buffered in the unit's memory.

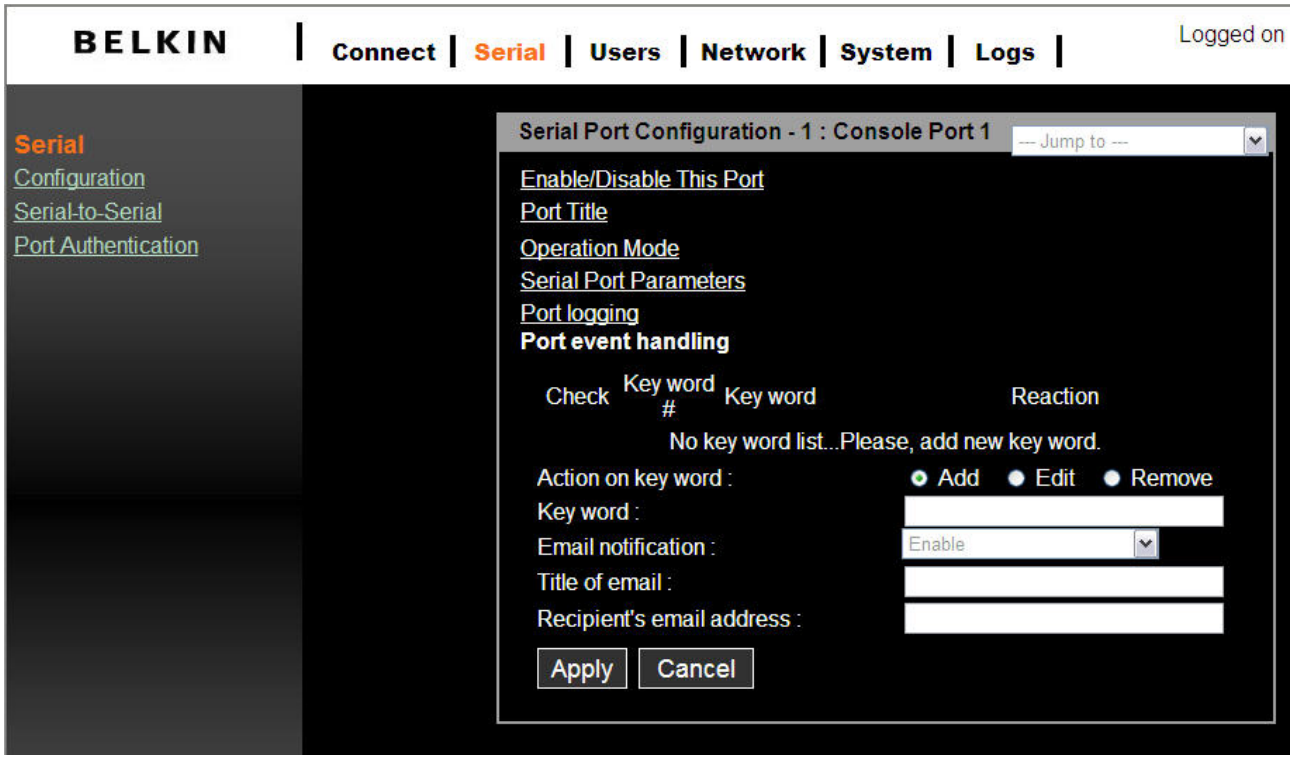


The **Port logging** feature is valid and visible only if the operation mode of the serial port is configured to console server mode.

If **Port logging** option is enabled, the user can let the Serial Console search a defined

keyword from the port logging data and send an email to an administrator by **Port event handling** configurations. Each reaction can be configured individually upon each keyword. Reaction can be an email delivery.

Click **Port event handling**



The memory buffer size for logging data is 192K per port.
If the log data grows larger than the memory size, the new data will overwrite the old data.

4.1.7 Break Function

In Console Server mode, Serial Console is capable of sending a “break” signal to connected serial device. A break is sometimes used to reset a communications line or change the operating mode of communications hardware like a MODEM. Some target devices such as Sun Solaris server requires a null character (break) to generate OK prompt. The effect of “sending a break through serial port” is equivalent to issuing a STOP-A from Sun keyboard. In order to send a break to serial device, configure it to **Console Server** mode and use **Telnet** or **RawTCP** as Protocol. Click the **Apply** button to send a break signal to the designated serial port and then to the attached computer or server.

4.2 Connect

The Serial Console provides web-based access to a target serial device without requiring a separate Telnet client program. This is done through a Java.

A Java applet is used to provide the text-based user interface to access the serial port. This Java applet supports only Telnet in Console Server mode. The user cannot access the serial port via the web when the host mode of the port is set to Raw TCP connection. The user is asked to enter user ID and password to access the port. Once authenticated, the user now has access to the serial port.

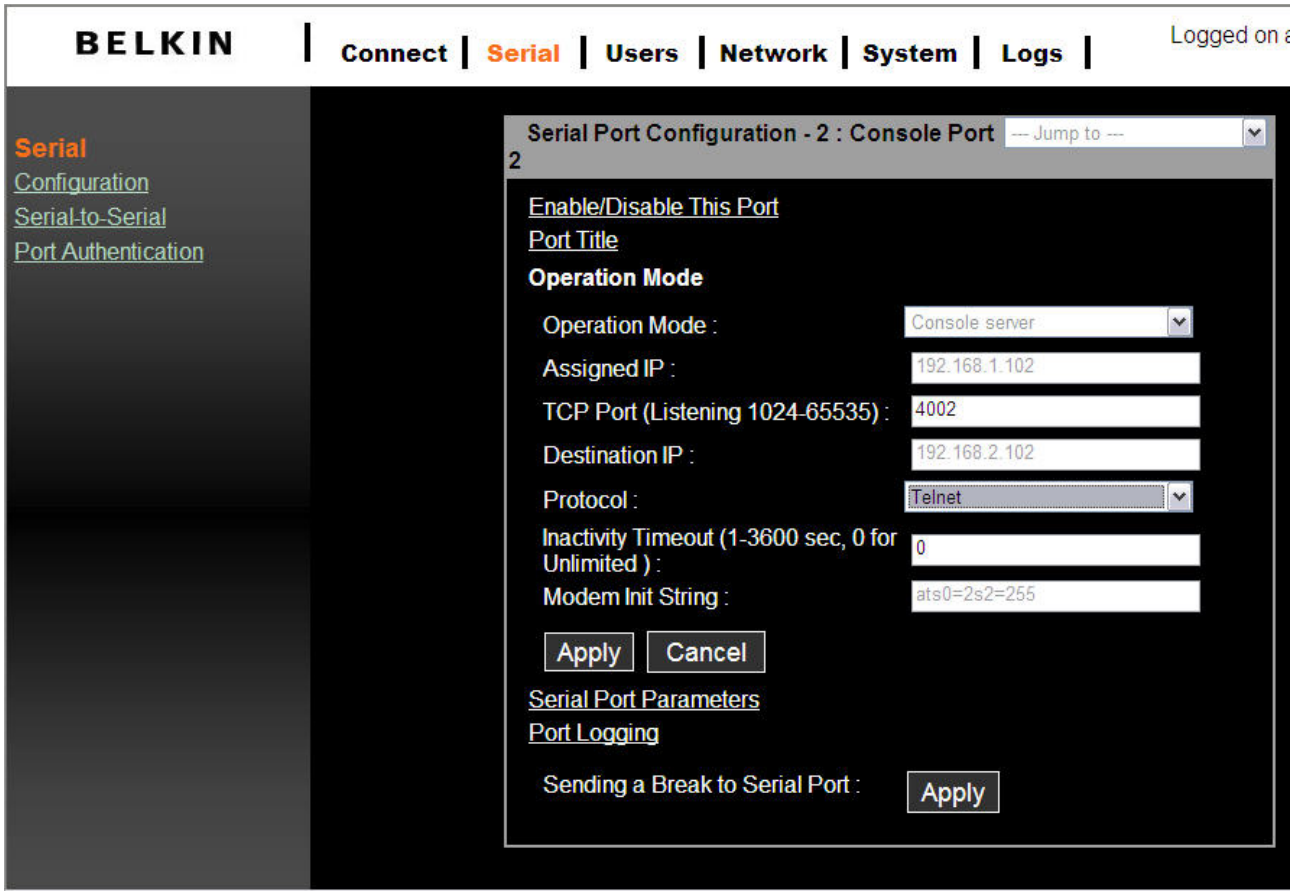
Use the hyperlink located at the bottom of the Connect Page to test your Java compatibility. Or use the bottom link to download the latest Java version.

Make sure that you enable your browser's Java support option and also check your Java Runtime Environment version (known as JRE version). You will need version 1.6.0 or above if you also need secure HTTP service (https).

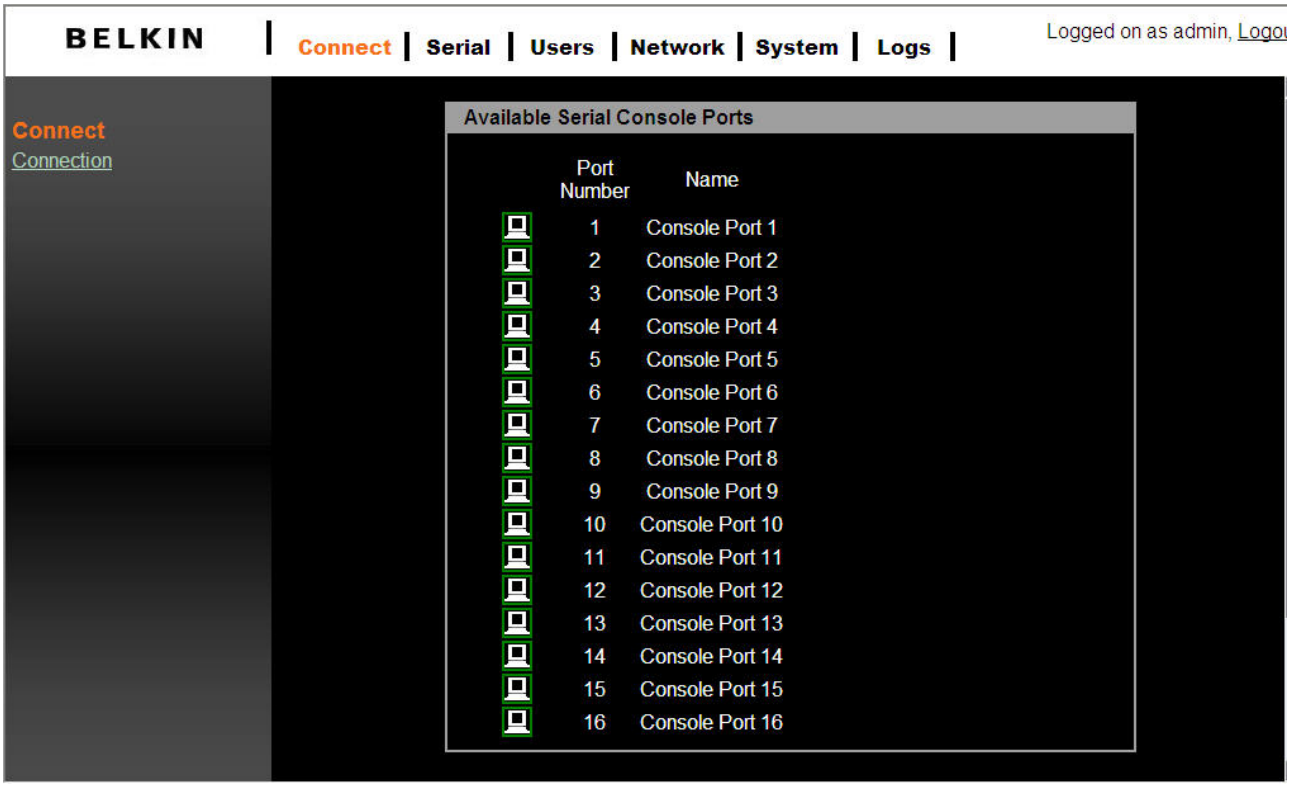
Notes:
In order to run this function, the system requires installing JRE (Java Runtime Environment) 6.0 and above. You can get the Java Software from the website http://www.java.com/en/download/

4.2.1 Telnet Java Applet

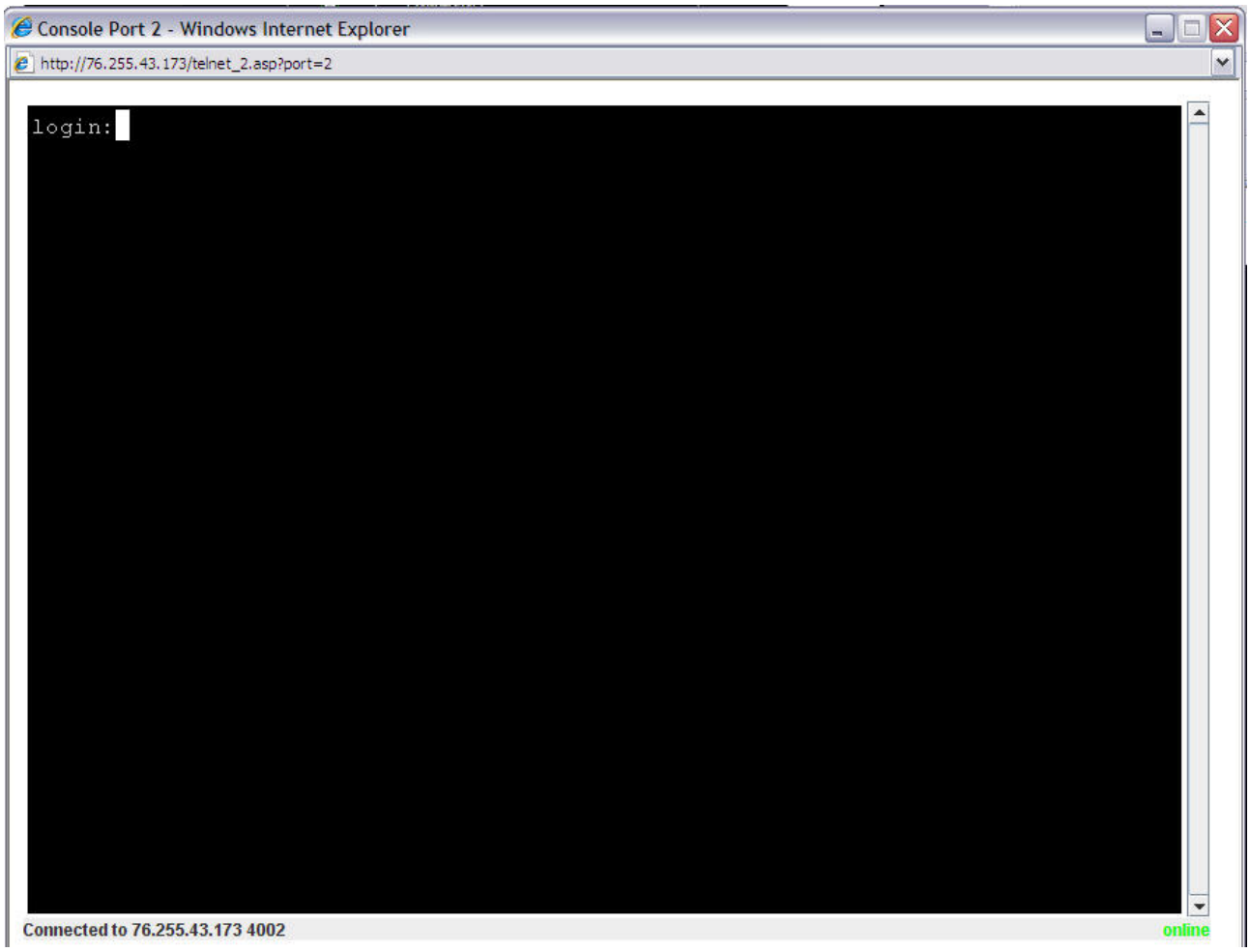
1. Select Telnet protocol under Serial > Configuration > Operation mode.



Select the Connect from the top menu and click on the terminal icon on the left. The Terminal emulation application will pop in a new window and prompt you to login. If you see a blank window check your System for Java version compatibility.



2. Enter user name and password to log in, so can start to use it as if running a Telnet client program (e.g., Telnet DOS program, PuTTY).



Note: The active Serial port's name will appear on the window bar. A connection status indicator will also appear on the lower right side of the window.

4.3 Serial-to-Serial Function

The Serial-to-Serial function allows you to use a simple terminal device (video display and keyboard) to access and control any device connected to the Serial Console on ports 1 through 15. You may also use an external Terminal Converter like the Belkin F1D084E, to connect your Serial Console to a KVM switch and consolidate the control

4.3.1 Installation

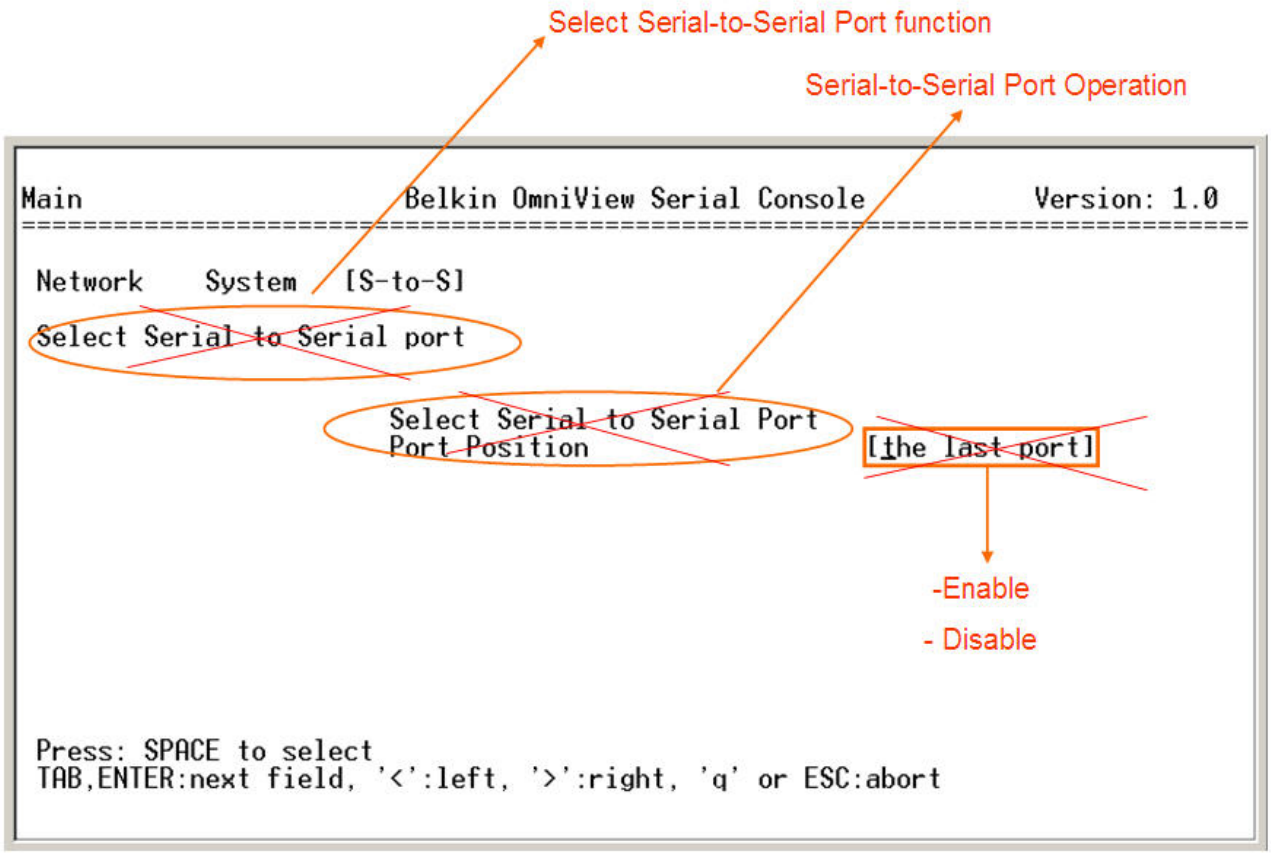
To install, connect our terminal device to port 16 of the Serial console. This will allow you access to serial device connected to ports 1 through 15 only.

4.3.2

Enable and Configure Serial-to-Serial

To configure the Serial-to-Serial function

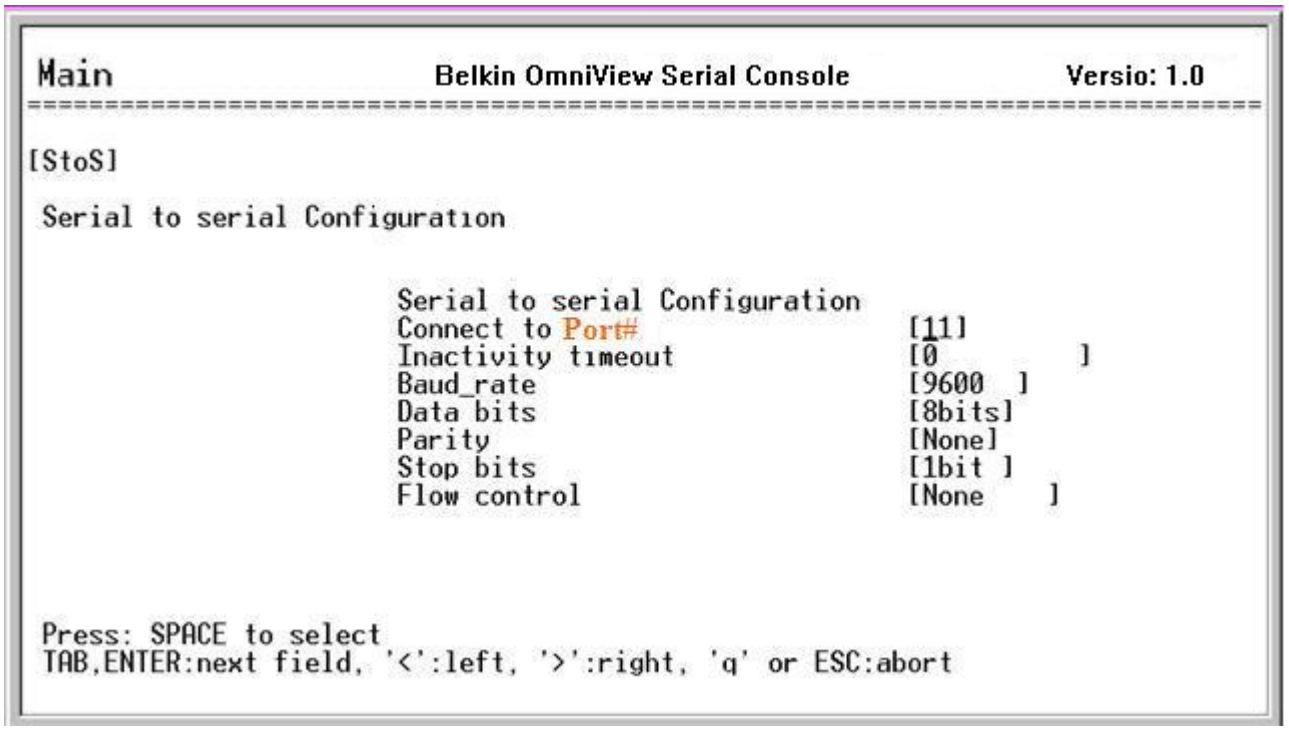
1. Enter VT100 console mode (see the section VT-100 for details) to show up the window screen as below.
2. Go to the item **Serial-to-Serial port operation**, hit **SPACE** bar to select ENABLE. Confirm the change to auto-reboot the system



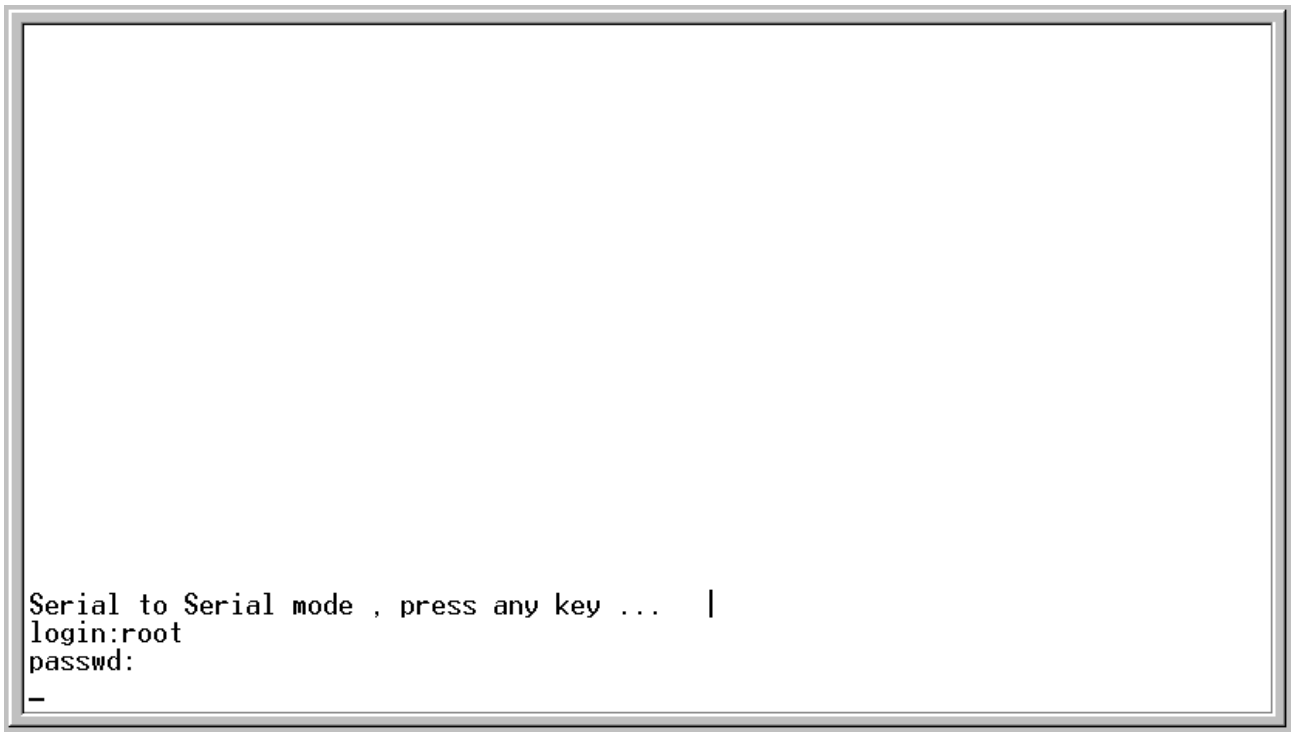
4. After the reboot (will take about a minute), the screen below will appear. Configure each configuration setting. Note that one should **type in** the value for **Inactivity**

timeout, and press **SPACE bar** to select the setting for the other items.

> **Note**:
> In order to show the following Serial-to-Serial configuration screen, you need to be sure to Enable the Serial-to-Serial function. The default baud rate is fixed as 9600 8N1 (not re-configurable) in order to get the best compatibility with third party terminal monitor device.

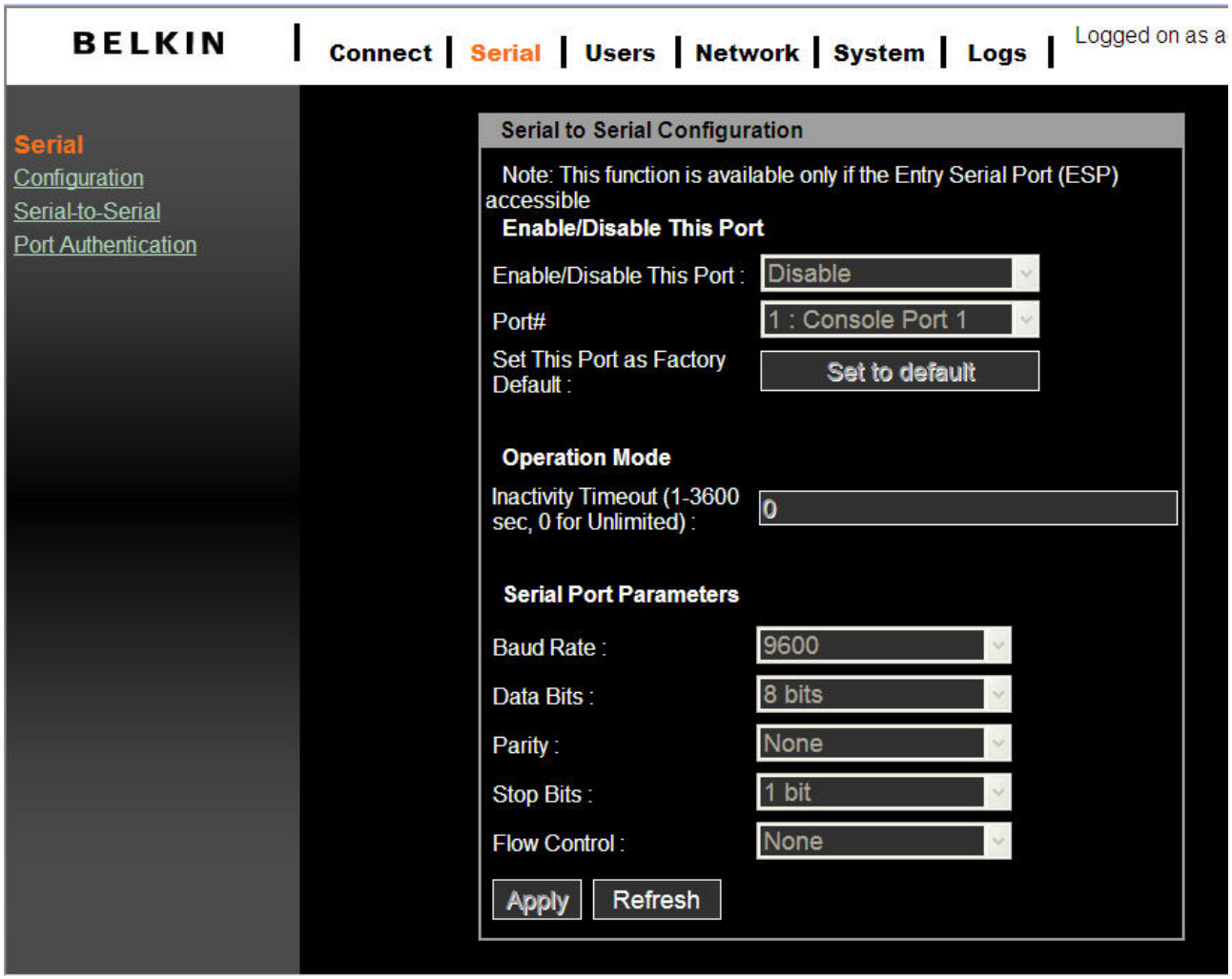


5. Confirm the choice the screen below will appear.



6. Type in user name and password. Then the data channel connection between port 16 and the selected serial port will be built. So the administrator can control the serial device or server.
7. Press **Cntl and C** keys to get out of Serial-to-Serial function and back to main console screen.

The web page also gives read-only settings of Serial-to-Serial function, it will automatically changed according to the setting change on VT100 console. Click **Cancel** will refresh the values.

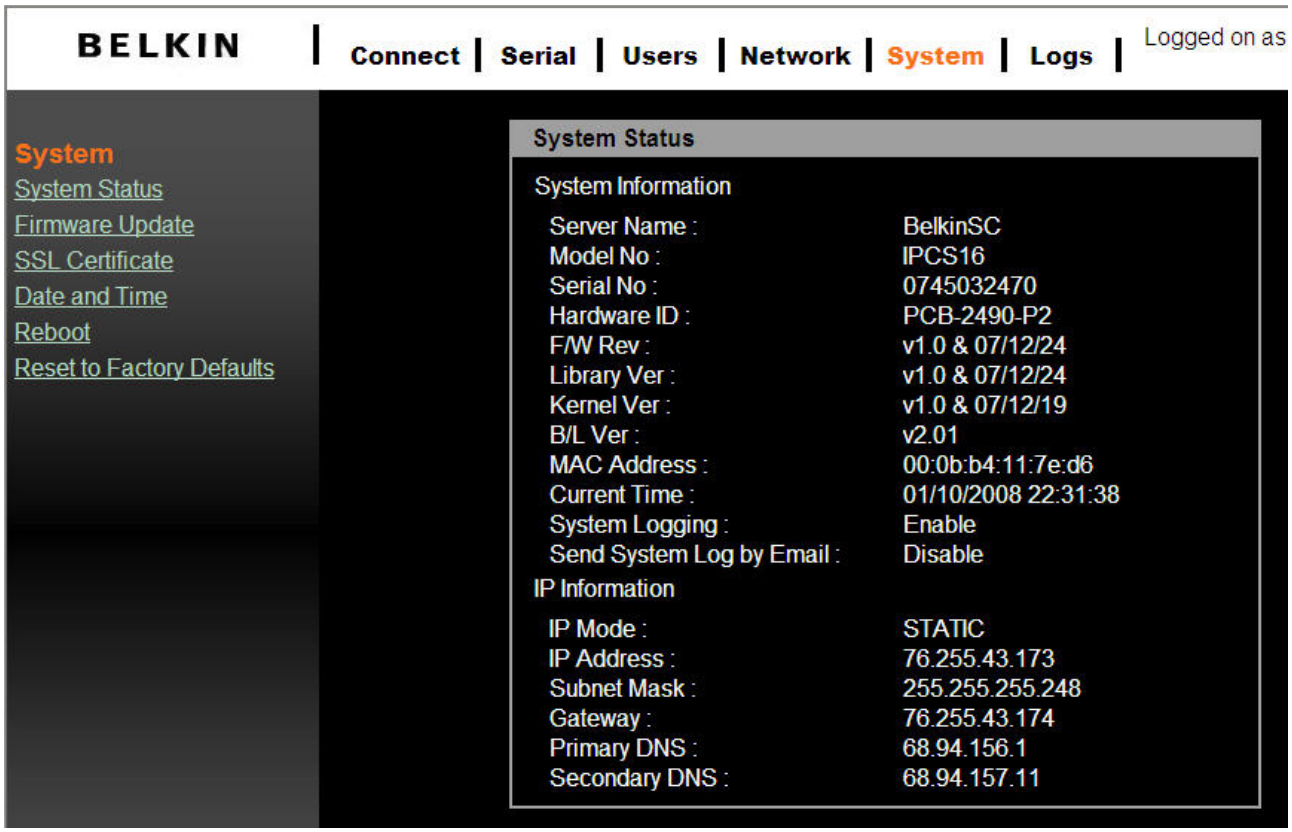


5. System Status & Log

5.1 System Status

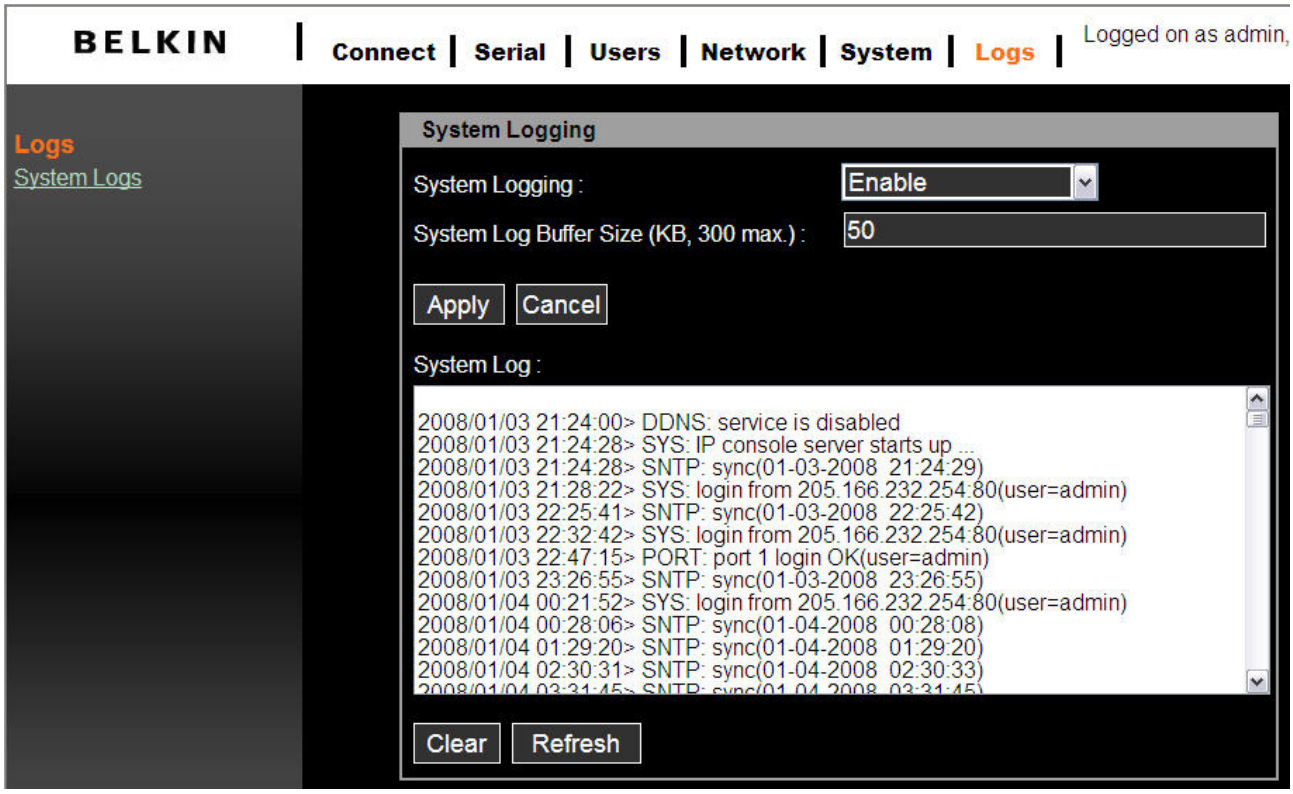
The System status page list current system information such as, name, serial number,

firmware versions, MAC address, current time, and the network settings. Data cannot be changed from this page. This page refreshes automatically every 10 seconds.



5.2 System Logging

You may enable or disable system logging process and set the log buffer size. The system log buffer‘s default value is 50K bytes and can be allocated up top 300KB maximum. If the logged data grows larger than the pre-allocated buffer size, the new data will overwrite the old data.



The following system events are logged in volatile storage cyclically:

i) SYS (system startup, idle timeout, login account authentication)

ii) SNTP (network time synchronization)

iii) LOG (clear system event log)

iv) PORT (serial port access authentication)

v) DDNS (register dynamic IP address event)

6. System Administration

6.1 User Administration

At startup of the AP, the system will prompt user to enter the password to access to the system. The administrator can add or remove a user easily via the web pages.
There are two levels of access privileges:

User Name	Default Password	Access Privileges
admin	admin	full access
(user define)	(user define)	only can access to **Serial Port** and **System Status**

An **Access Deny** page will be shown if user is not authorized to access the web page.

6.1.1 Add User

To Add a user,

- Check the users at the **User administration** screen
- Click the button **Add**
- Type the new User Name and password.

User name and password guidelines

- The first character of User name must be alphabet.
- The password should be at least 3 characters long
- The user name or password must not longer than 32 characters.
- Only **admin** user can access to **Network** and **System administration**

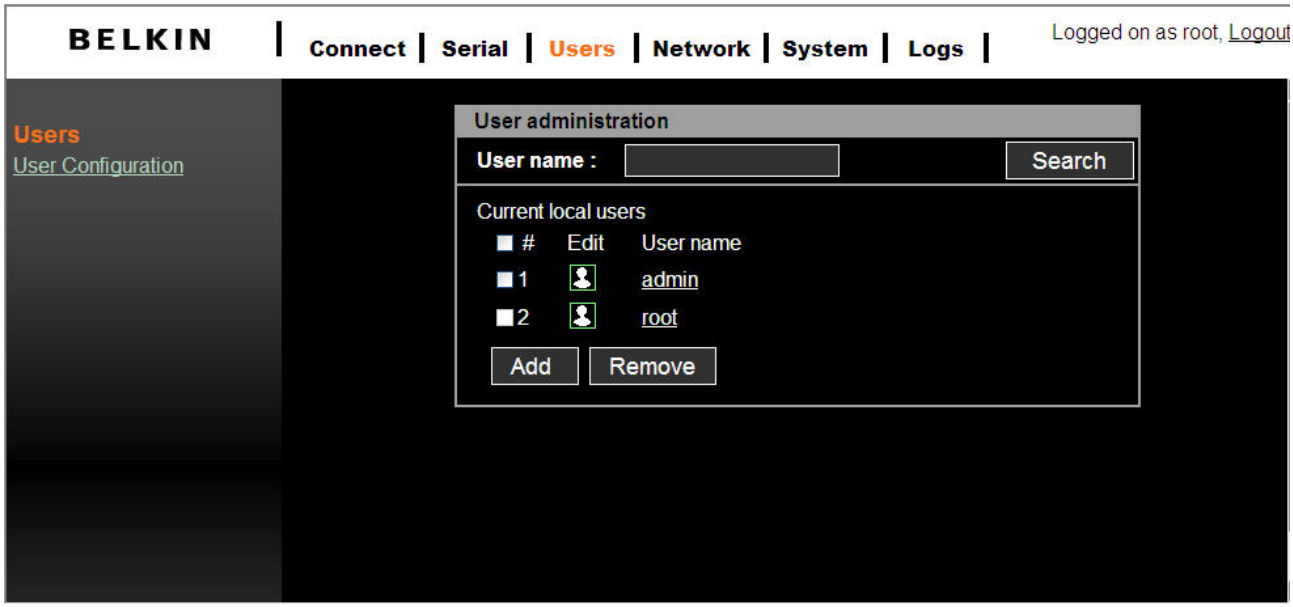
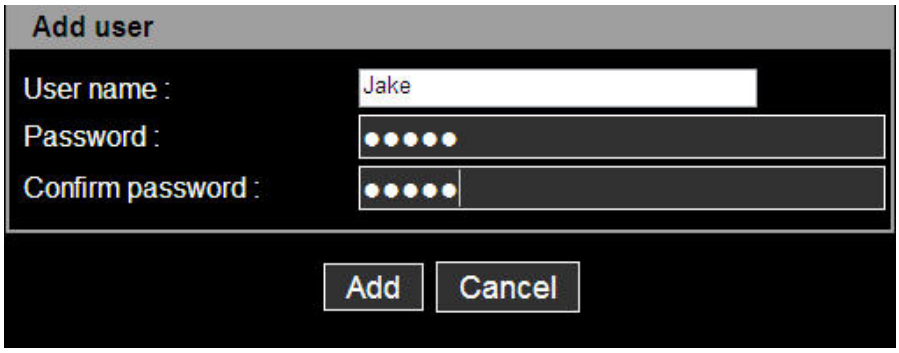
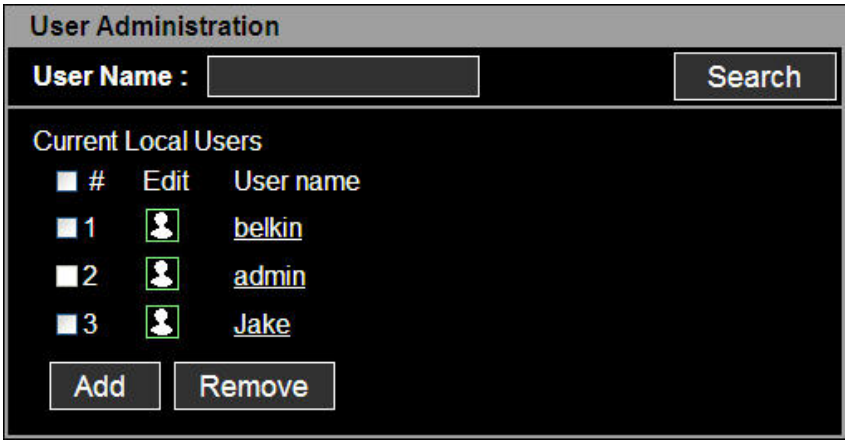


Figure below shows the **Add User** screen.



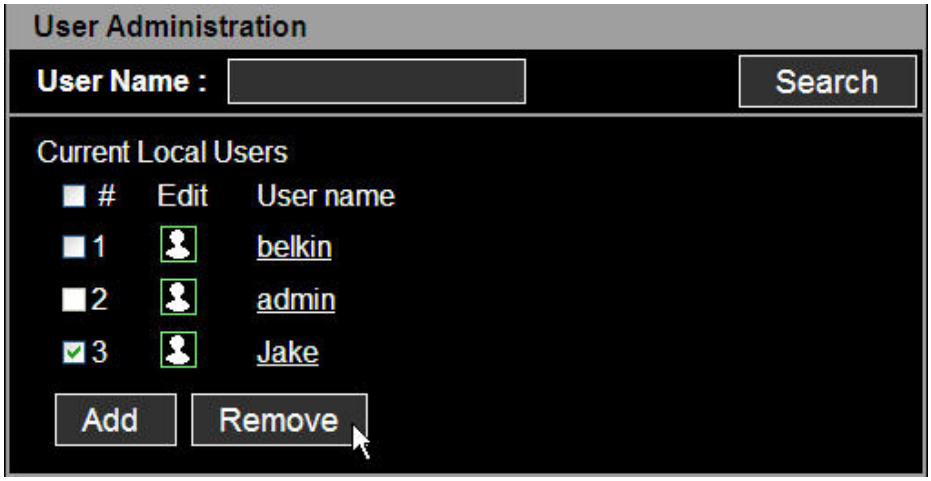
The new user will now appear under the User Name list.



6.1.2 Remove User

To remove a user,

- Check the users at the **User administration** screen
- Click the button **Remove**



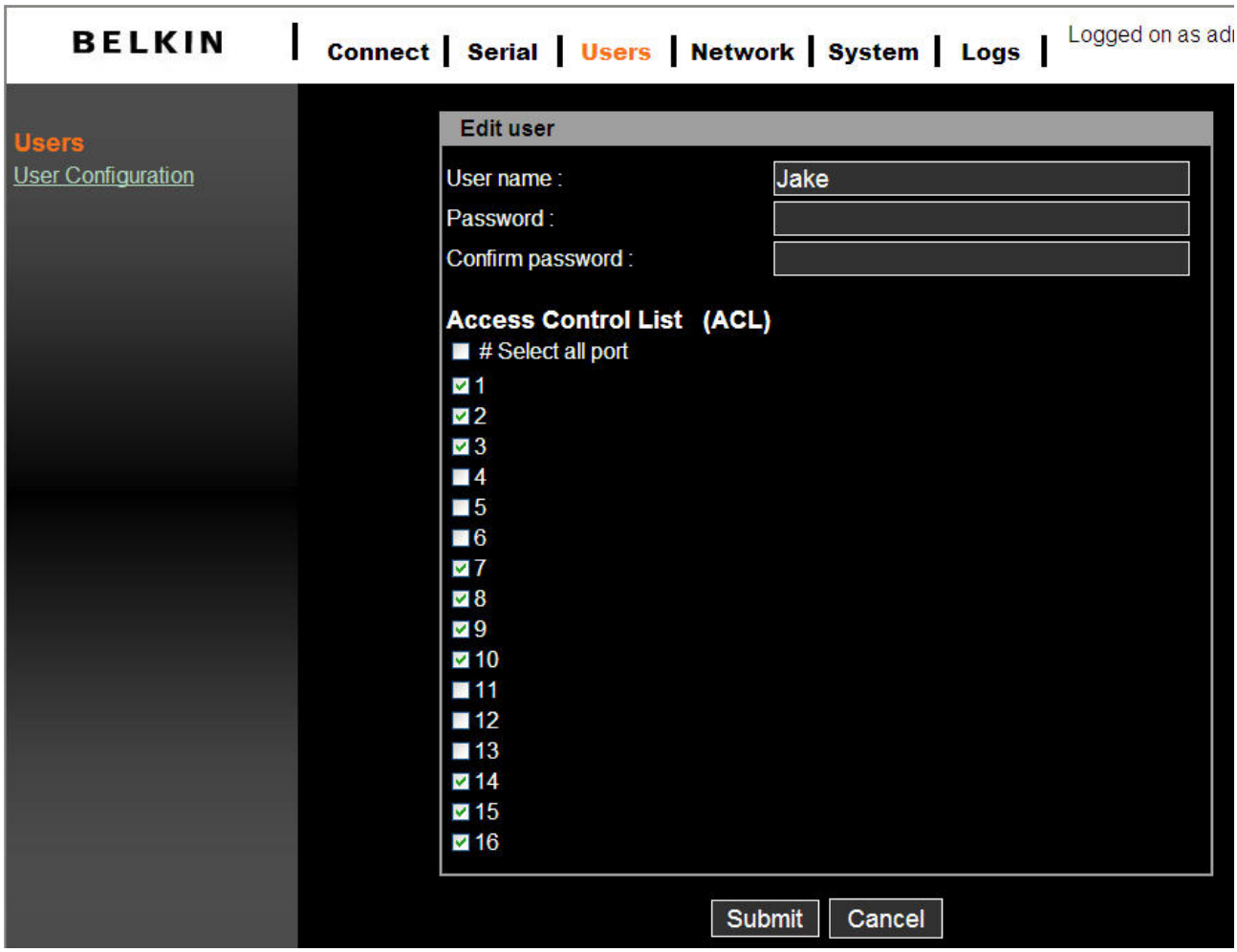
6.1.3 Edit the Access Control list (ACL)

The Serial Console Provides ACL (Access Control List) security where you can specify user access discretely by individual ports only, instead of all ports.

To edit the ACL,

- Check the users at the **User administration** screen
- Click the **Edit** icon
- Enter user name & password
- Select the port to access to
- Click the button **Submit**

Once the user account ACL is set, users can access or make configuration change to the authorized serial ports only. Users will not be able to view or configure the unauthorized serial ports.



6.1.4 Change password

To change the parameters of the user account, open the edit user screen by selecting the user name at the **User Configuration** screen and then edit the parameters of user account like adding user.

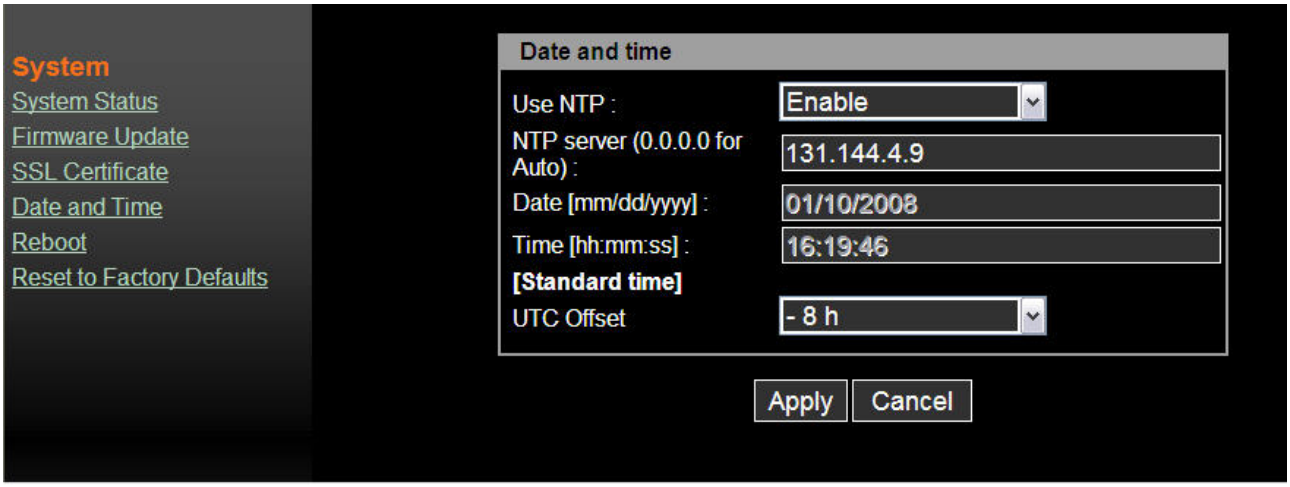
6.2 Date and Time (NTP)

The Serial Console maintains current date and time information. The clock and calendar settings are backed up by an internal battery. The user can change the current date and time.

There are two options for setting the date and time. The first option is to allow the NTP server to maintain the date and time settings. If the NTP feature is enabled, the Serial Console will obtain the date and time information from the NTP server at each reboot, then automatically align with the NTP server time every hour. If the NTP server is set to 0.0.0.0, the Serial Console will automatically use the default NTP servers. In this case, the it should be connected from the network to the Internet. The second method is to set date and time manually without using the NTP server. In this case the date and time information

is maintained by the internal battery backup.

By convention, weather scientists use one time zone, Greenwich Mean Time (GMT). This time is also known as Universal Time (UTC). You may set the time zone and the time offset from UTC depending on the user location to set system date and time exactly, and the time offset from UTC. The **Time offset** value **x** could be positive or negative integer. Please refer to the website http://time_zone.tripod.com/ for the time offset from UTC.



Note:

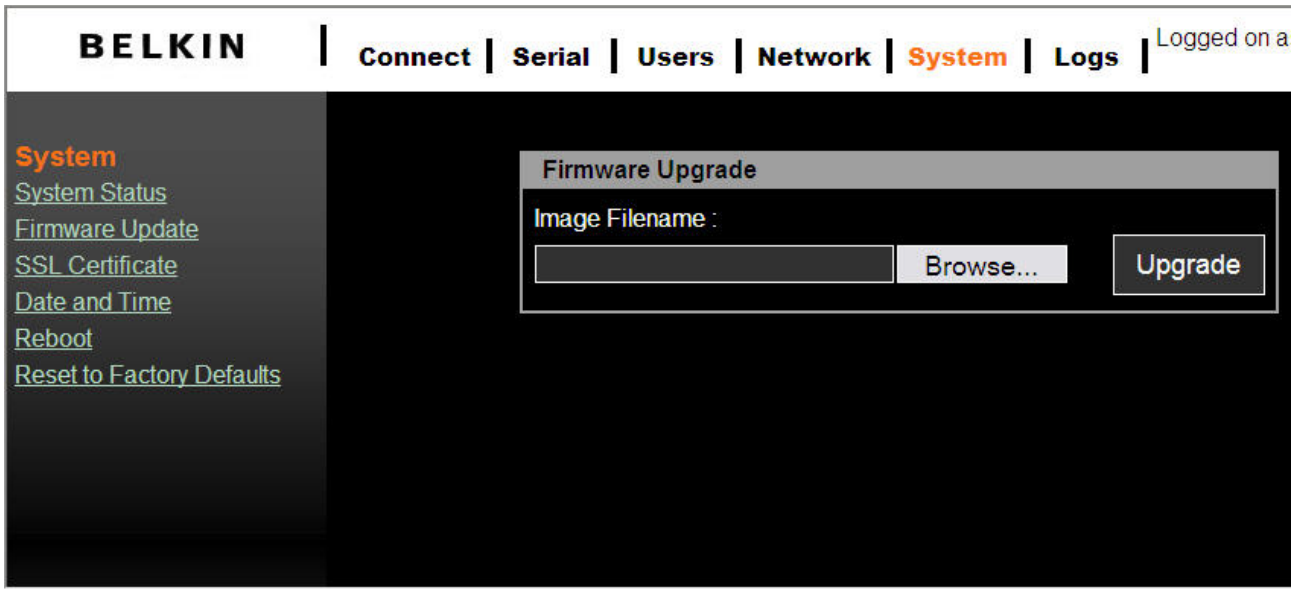
- The Serial Console provides RTC (Real Time Clock) function powered by a lithium battery (CR2032, 3V). So the date/time will be maintained even encounter power loss to the unit.
- If you repeatedly lose the date/time information please replace the battery.
- Replace the 3-Volt CR2032 battery only with the same or equivalent type recommended by the battery manufacturer. A new battery can explode if it is incorrectly installed. Discard used batteries according to the battery manufacturer's instructions.

6.3 Firmware Upgrade

Firmware can be easily upgraded via web page. This section describes the upgrade procedures.
The latest firmware version is available from www.belkin.com/support.

6.3.1 Upgrade from the web interface

Refer to web page System → Firmware Upgrade :

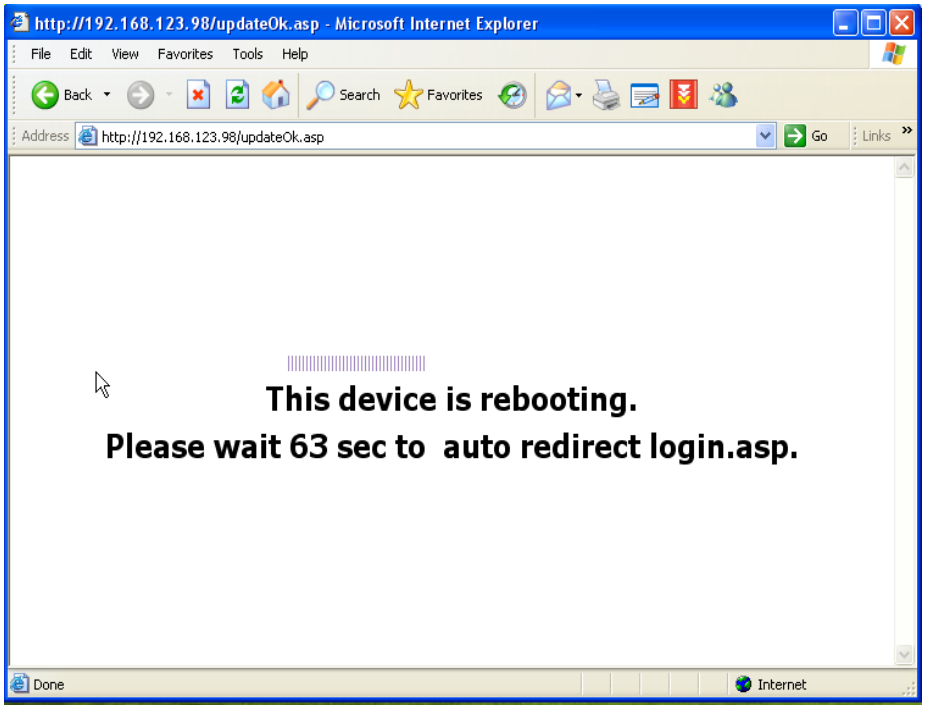


Click **Browse** to search the firmware file from the explorer window.
Navigate through your PC and select firmware file. Click **Open** to confirm your selection.

Once the appropriate firmware file is selected, click **Upgrade** to initiate the firmware upgrade process. The web interface will display the progress bar to indicate the proceeding of the file transfer. At the same time the port LED on front panel will also blink in series to indicate the upgrade procedure is in process.

Warning !!! DO NOT disconnect the power or the Ethernet cable during this upgrading process. Doing sot may cause upgrade failure and destroy the image in memory.

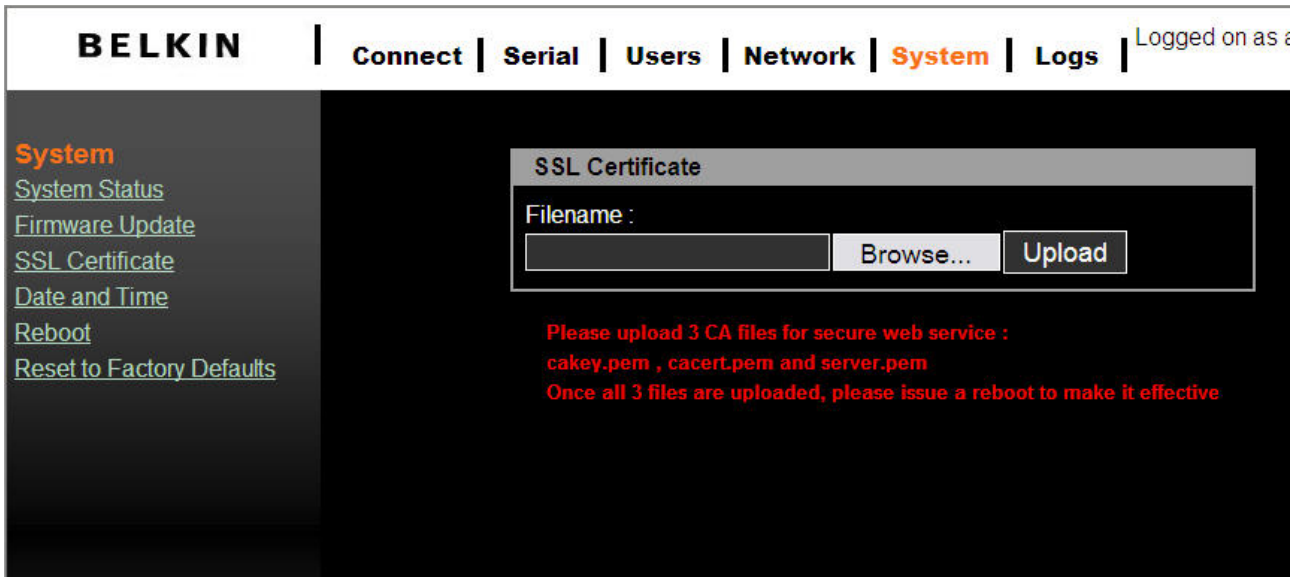
The Serial Console will automatically initiate a self-reboot upon completion of upgrade process to activate the new firmware. Once the counter expires, the browser will redirect you to the login homepage. You can refer to System Status page to check the firmware version and confirm the upgrade operation.



6.4 SSL Certificate

A SSL certificate is a digital identification which contains information to attest that certificate belongs to specific person, organization, server or other entity noted in the certificate. The Serial Console supports secure HTTP (a.k.a https) to make configuration change via web page. The server side SSL certificate identifies the Serial Console so that you can rely on the certificate and make the configuration change confidently.

The Serial Console is capable of uploading customized certificate files to web server. The certificate file suite include three files (cacert.pem, cakey.pem and server.pem). All three certificate files shall be uploaded to complete certificate upgrade. The file upload interface is similar to firmware upgrade. Once all certificate files are uploaded, users shall initiate a reboot command manually to make the new certificate effective.



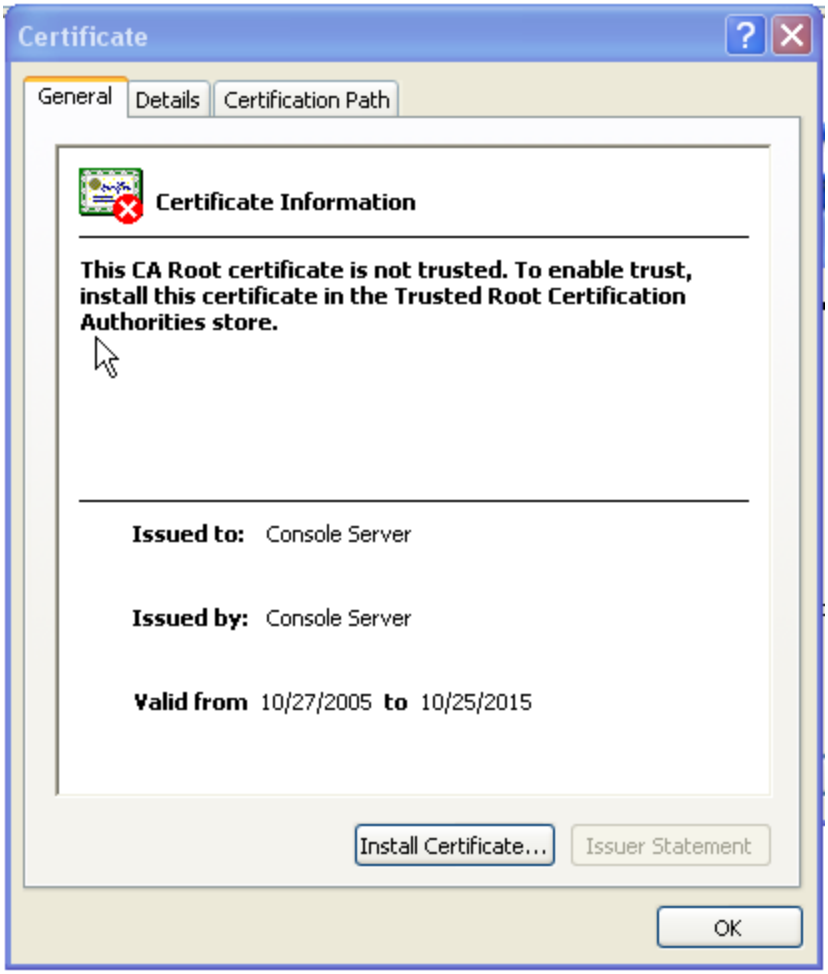
Browse prepared CA files (follow procedure in Appendix E to prepare exactly the three CA files with same assigned filenames) and upload these files to the Serial Console. Please double check each files before uploading. A false CA file suite may disable secure HTTP function.

Notes:

- If CA files are damaged, users can roll back the CA files to factory default by System → Reset to Factory Default Setting. The old CA files will be recovered.
- Because the length CA file pathname is limited (256 characters), it is recommended to put all your files under **C:\upgrade** for easy administration.
- Appendix E details the way to create CA files from scratch.

6.4.1 Secure HTTP Certificate

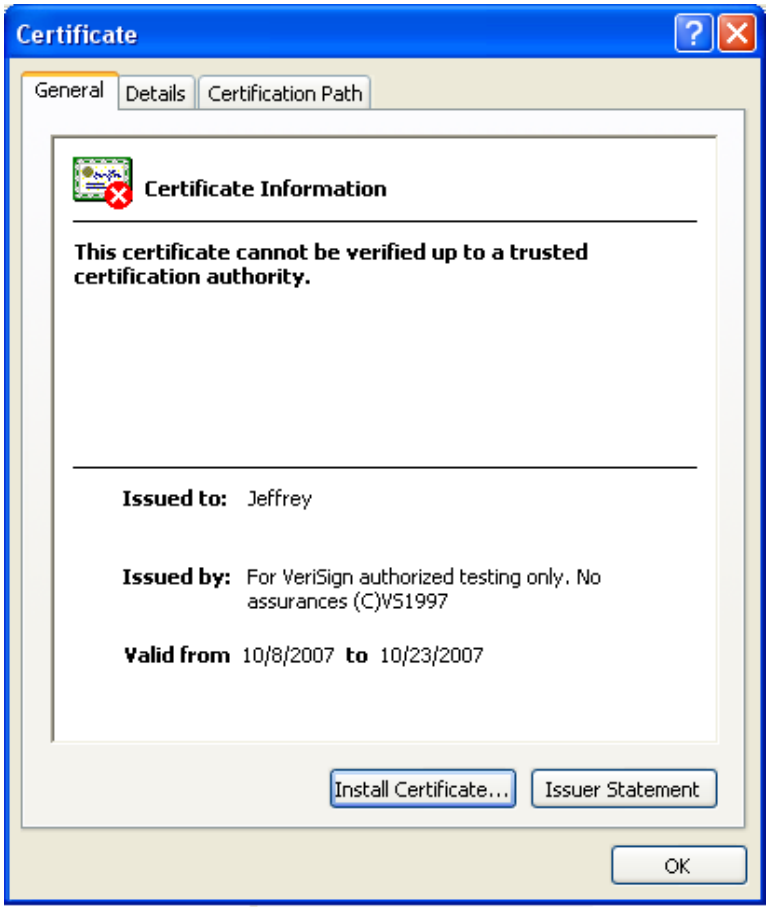
A secure Serial Console web service is launched by the browser's https connection (service port 443). The browser will prompt you with a security alert to notify of the certificate. You must accept the certificate to start the secure web service. Users can **View Certificate** and justify whether the connected web server is trustworthy.

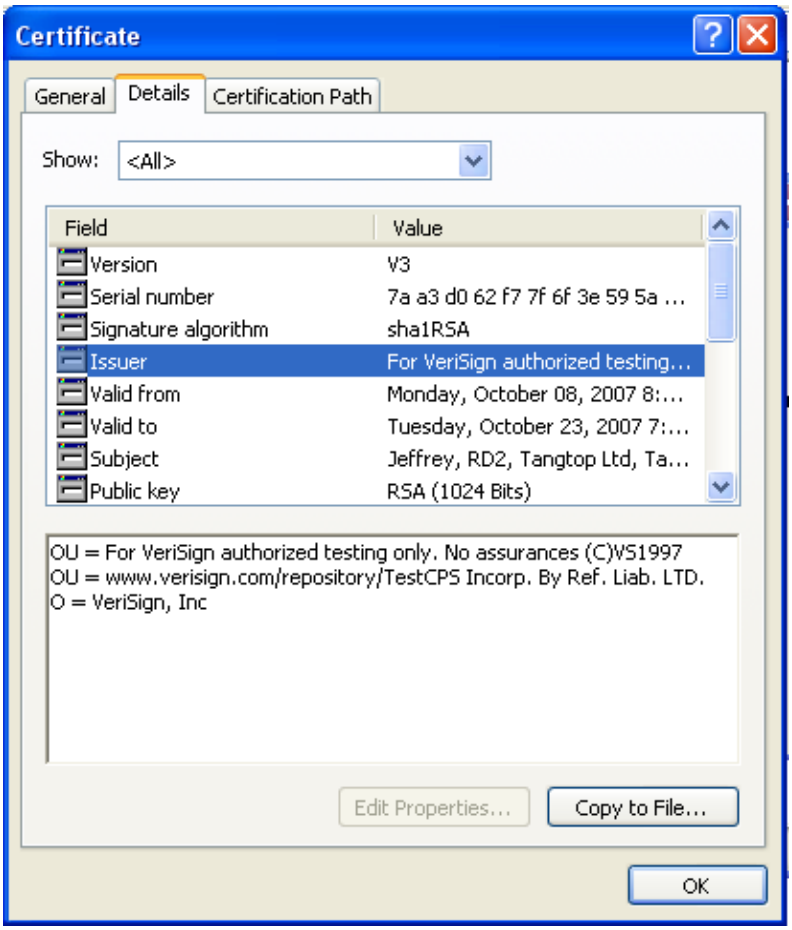


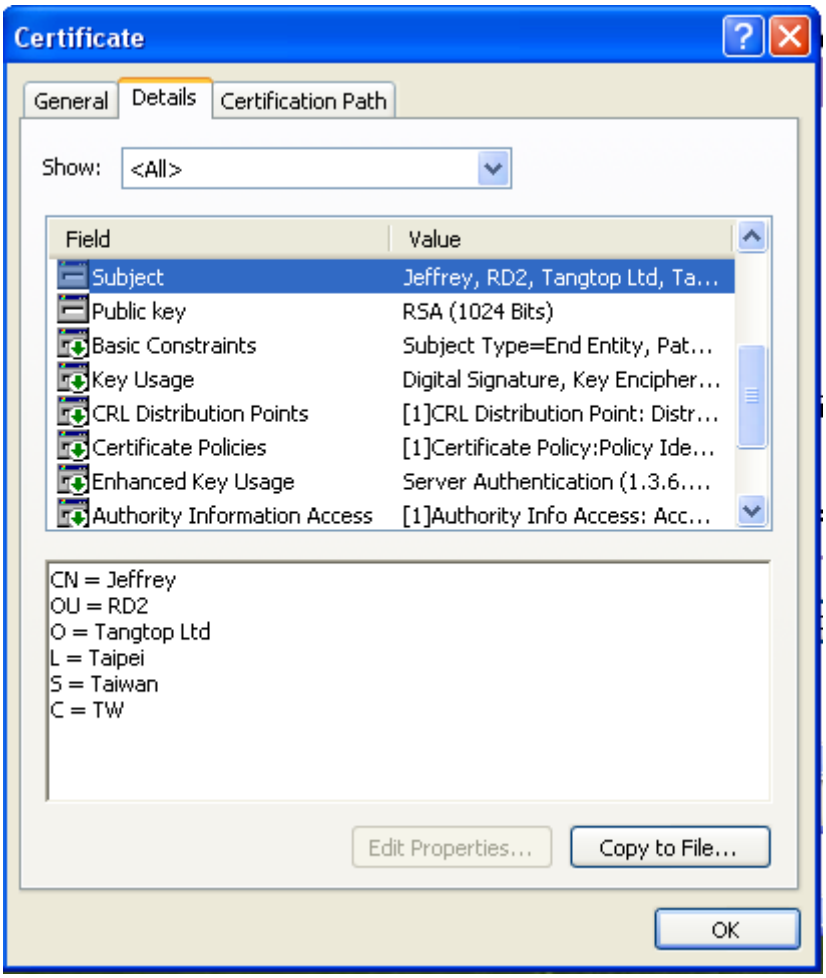
The other way to tell a secure web connection from unsafe one is by looking up a lock symbol on your browser (bottom-right of IE browser). You can double click on the symbol to examine the detail information of server side certificate.

Once you have prepared a publicly signed CA suite of files, upload them from the SSL Certificate page. A system reboot is required to take into effect.

The following example demonstrates a publicly signed certificate and information registered to certificate authority (VeriSign).

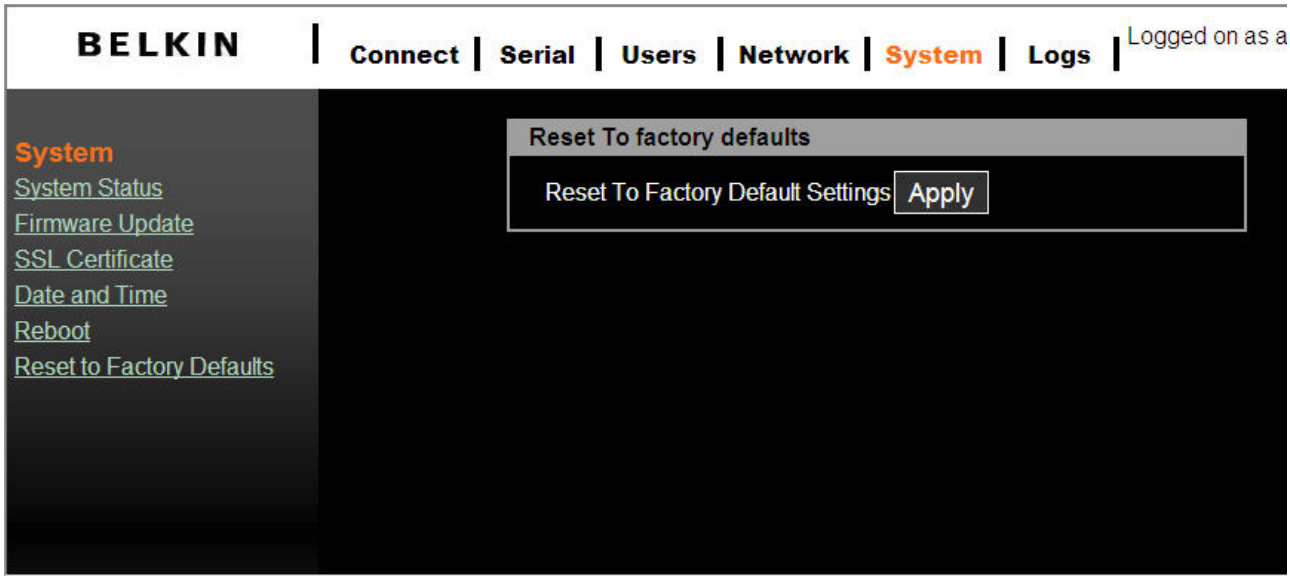



Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
7a a3 d0 62 f7 7f 6f 3e 59 5a ...
Signature algorithm
sha1RSA
Issuer
For VeriSign authorized testing...
Valid from
Monday, October 08, 2007 8:...
Valid to
Tuesday, October 23, 2007 7:...
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
OU = For VeriSign authorized testing only. No assurances (C)VS1997
OU = www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
O = VeriSign, Inc
Edit Properties...
Copy to File...
OK



6.5 Reset to Factory Default Settings

To roll back to factory default settings, click on **Apply** .



6.6 Reboot

You can trigger the Serial Console to perform a software reboot via network. The reboot

function is mandatory when CA certificate upload is complete.

7. Technical Data

7.1 Default Settings

Server Name	BelkinSC
DHCP	Enabled
IP Address	192.168.2.156
Net Mask	255.255.255.0
Gateway	192.168.2.1
Serial Number	**xxxxxxxxx**(printed on bottom of unit)
MAC Address	**xx:xx:xx:xx**(printed on bottom of unit)
Version & Date	current firmware version number & date
User Name	admin
Password	admin
Protocol (serial)	Telnet
Protocol (web)	HTTP
IP Filter	Disable
Serial ports --	
Baud Rate	9600
Data/Stop	8-1
Parity	None
Flow Control	None
Serial timeout	0 seconds
Operation Mode	Console Server
TCP port	**Port 1:** 4001 **Port 2:** 4002 **- - - - - - - -** **Port 16:** 4016

Appendix A: Adapters

F1D120 (RJ45F – DB9F DCE)

(Insert Pin out table here)

F1D121 (RJ45F – DB25F DCE)

(Insert Pin out table here)

F1D122 (RJ45F – DB25M DTE)

(Insert Pin out table here)

F1D123 (RJ45F – DB25M DCE)

(Insert Pin out table here)

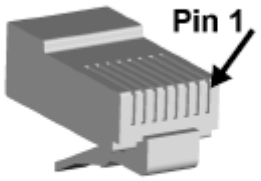
F1D124 (RJ45F – RJ45M CISCO)

(Insert Pin out table here)

Appendix B: Ethernet pin-outs (RJ-45)

Standard Ethernet Cable RJ-45 Pin-out

Pin	Description
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC



Appendix C: Well-Known TCP/UDP Port Numbers

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Table below shows some of the well-known port numbers. For more details, please visit the IANA website: http://www.iana.org/assignments/port-numbers

Port Number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UCP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

Appendix D: Protocol Glossary

BOOTP (Bootstrap Protocol)
Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)
A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)
Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers): A system that allows a network name server to translate text host names into numeric IP addresses.

Kerberos
A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)
A protocol for accessing directory information.

NAT (Network Address Translation)
An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)
A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user’s access to each file.

NIS (Network Information System)
System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management System)
NMS acts as a central server, requesting and receiving SNMP-type information from any

computer using SNMP.

NTP (Network Time Protocol)
A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)
A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)
A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)
An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

SNMP (Simple Network Management Protocol)
A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)
TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)
A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)
A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)
A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

Telnet
A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.

Appendix E: Creating CA files

The Serial Console server supports secure web page configuration (a.k.a. https). There are two types of certificate files for server side authentication.

- self-signed : Users can create the certificate files by themselves. The downside is that the client will be prompted to accept a certificate signed by an authority not known to the browser. Usually the client browser will have to accept the certificate only once and it will not be prompted further.

- signed by a Certification Authority: Users create CA files and send out to a CA for signing. The main advantage is that the client will not be prompted to accept a certificate.

Users need to install openssl toolkit before create the CA files mentioned above. We explain here how to generate the certificate for the Serial Console web server using openssl and the Linux shell. For openssl toolkit, it can be downloaded from : http://www.openssl.org/

1. Self-signed CA:

i) Create a key and X.509 certificate:

under Linux command prompt:

openssl req -x509 -newkey rsa:1024 -days 1024 -keyout cakey.pem -out cacert.pem

The options that can be changed here are:

* the PK algorithm can be changed from rsa to dsa and also the length of the key in bits (512, 1024, 2048, 4096).

* time period for the certificate validity, we set it to 1024 days which is less than 3 years.

You can also set start / end date for the validity of the certificate.You will be prompted for the PEM pass phrase twice for the key and than you have to enter some information necessary for the certificate:

Here is an example prompt:

Country Name <US>
State or Province Name <YourState>
City or Locality <Anchorage>
Organization Name <Your business name>
Prolix Organizational Unit <R & D>
Common Name (SERVER HOST NAME) <IPCS>
Server Admin's email address <you@yourdomain.dom>

ii) Strip pass phrase

openssl rsa -in cakey.pem -out cakey-nopassword.pem

iii) Combine the key and X.509 certificate files into server.pem

cat cakey-nopassword.pem cacert.pem > server.pem

iv) Collect all 3 PEM files and prepare to upload to IPCS server

server.pem , **cacert.pem** , **cakey.pem**

2. Signed by trustworthy CA :

i) Prepare private key ***cakey.pem***

openssl genrsa –des3 –out cakey.pem 1024

meaning of parameters:

genrsa : generate RSA private key
des3 : encrypt certificate by DES3
1024 : the key size is 1024 bit

ii) Prepare a Certificate Signing Request

openssl req –new –key cakey.pem –out server.csr

openssl toolkit will prompt user with message to guide user to fill out a registration form. Once it is complete users can submit the CSR file to www.verisign.com for testing or refer to http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp (located in Taiwan) to apply for a signed certificate. Get the certificate and name the file as ***cacert.pem***

iii) Strip pass phrase

openssl rsa –in cakey.pem –out cakey-nopassword.pem

iv) Combine the key and X.509 certificate files into ***server.pem***

cat cakey-nopassword.pem cacert.pem > server.pem

v) Collect all 3 PEM files for upload

server.pem , cacert.pem , cakey.pem