Console Management Server

VTS

How-To

Version 0.9.4

2003-07-10

Technical Support

Sena Technologies, Inc.

210 Yangjae-dong, Seocho-gu

Seoul 137-130, Korea

Tel: (+82-2) 573-5422

Fax: (+82-2) 573-7710

E-Mail: support@sena.com

Website: http://www.sena.com

Index

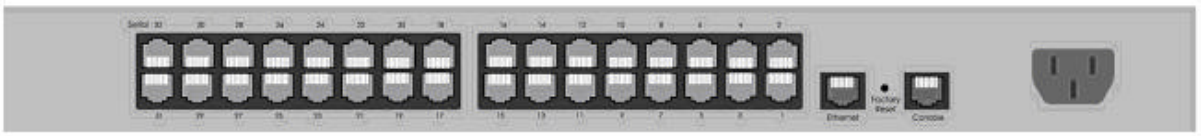
1. Basic configuration

1.1. How to enter the VTS for the first time to set IP of the VTS

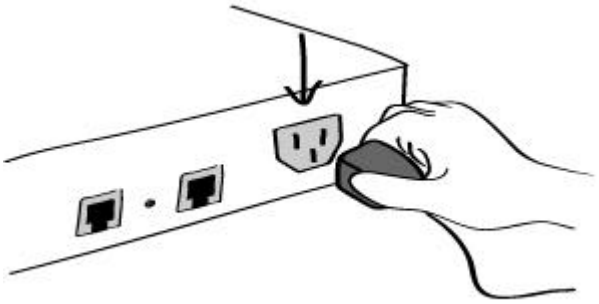
This guide gives you all the necessary information to quickly configure and start using the Sena console server, VTS. Below VTS package (comes along with VTS) is required to get started.

- One power cable (included in the package)
- One-console/Ethernet cables (included in the package)
- Cable kit (included in the package)
- One PC with Network Interface Card (hereafter, NIC) and/or one RS232 serial port.

1) Connect power supply and Switch on the VTS.

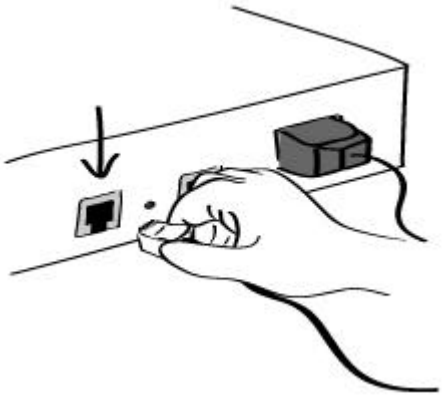


Back panel of the VTS



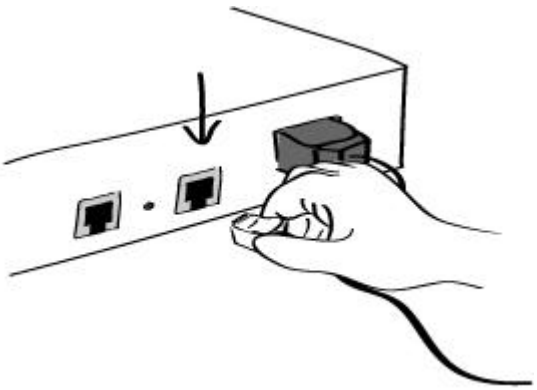
Connect power supply

2) Connect the Ethernet cable to the Ethernet connector on the back panel of the VTS with your hub or switch.



Connect Ethernet cable to the Ethernet connector on the back panel

3) Connect the Console cable with RJ45-DB9F adapter into the console port of the VTS and connect the other end of the Console/Ethernet cable with RJ45-DB9F adapter to the PC's COM port.

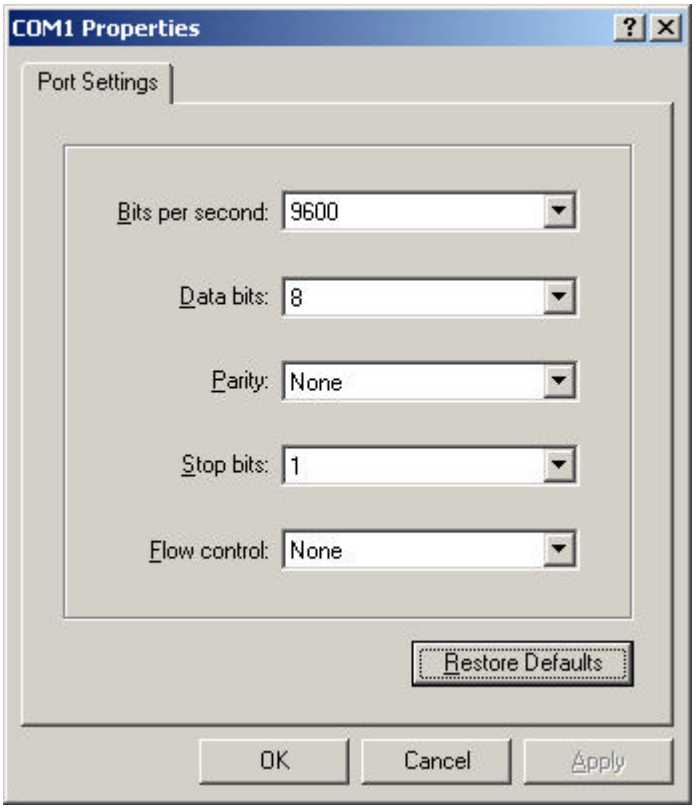


Connect the Console/Ethernet cable with RJ45-DB9F adapter

4) Turn on the power switch on the back panel of the VTS.
5) Confirm that the Power, Ready and Link LEDs are light up.

Confirm the Power, Ready, and Link LEDs

6) Configure a terminal emulation program, such as HyperTerminal, using the following settings: bps=9600, data bits=8, parity=none, stop bits=1, and flow control=none.



Configure a terminal emulation program with above properties, in a typical case

7) Press ENTER key at the terminal emulation program.

8) Enter the factory default login as "admin". Default password for admin is "admin". Then configuration menu appears like below.

```
192.168.161.5 login: admin
Password:

-------------------------------------------------------------------
 Welcome to VTS-1600 configuration page
 Current time : 02/25/2003 16:46:34 F/W REV.     : v1.0.0
 Serial No.   : vts32000302-00001 MAC Address :00-01-95-a1-89-b7
 IP mode      : Static IP           IP Address   : 192.168.161.5
-------------------------------------------------------------------
 Select menu
 1. Network configuration
 2. Serial port configuration
 3. Clustering configuration
 4. PC Card configuration
 5. System Status & log
 6. System administration
 7. Save changes
 8. Exit without saving
 9. Exit and apply changes
 a. Exit and reboot
  <ENTER> Refresh
 ----->
```

Enter VTS authentication details

9) Choose the following to navigate to the IP configuration: ==> 1. Network configuration > 1. IP Configuration >

You may change IP settings here. Factory default IP setting is 192.168.161.5

About your network parameters, please contact your Network administrator.

```
--------------------------------------------------------------------------------
Welcome to VTS-1600 configuration page
Current time : 05/30/2003 08:58:16      F/W REV.     : v1.1.2
Serial No.   : VTS1600-030100001        MAC Address  : 00-01-95-04-2b-ca
IP mode      : Static IP                IP Address   : 192.168.161.5
--------------------------------------------------------------------------------
Select menu
1. Network configuration
2. Serial port configuration
3. Clustering configuration
4. PC Card configuration
5. System Status & log
6. System administration
7. Save changes
8. Exit without saving
9. Exit and apply changes
a. Exit and reboot
 <ENTER> Refresh
-----> 1
--------------------------------------------------------------------------------
Network configuration
--------------------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet configuration
a. TCP service configuration
 <ESC> Back, <ENTER> Refresh
-----> 1
--------------------------------------------------------------------------------
Network configuration --> IP configuration
--------------------------------------------------------------------------------
Select menu
1. IP mode : static IP
2. IP address :  192.168.161.5
3. Subnet mask : 255.255.0.0
4. Default gateway : 192.168.1.1
5. Primary DNS : 168.126.63.1
6. Secondary DNS : 168.126.63.2
 <ESC> Back, <ENTER> Refresh
----->
```

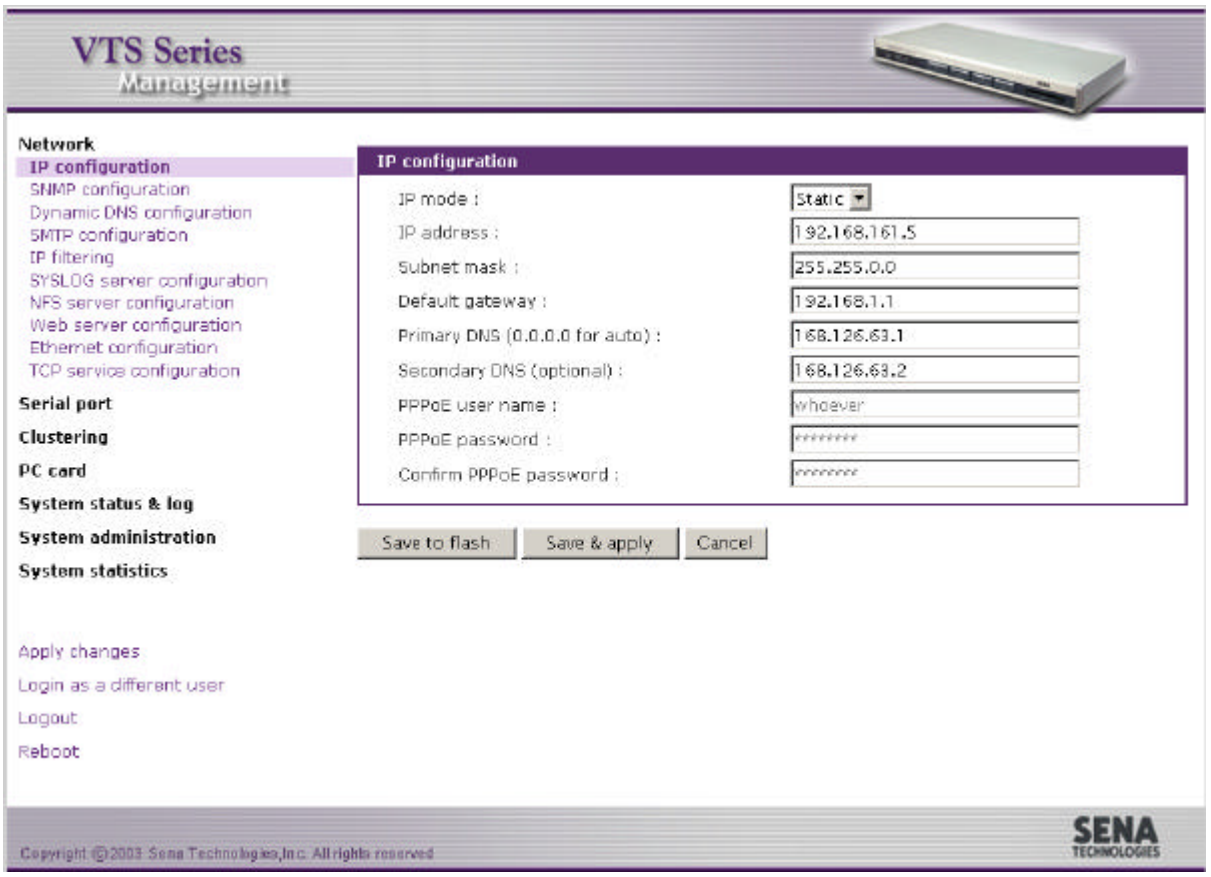
You may change IP settings here

10) Press ESC when done to return to the main configuration menu and enter number 9 to exit and apply changes. Changes are saved and applied immediately. No need to reboot VTS.

```
Welcome to VTS-1600 configuration page
Current time : 05/30/2003 09:01:25      F/W REV.     : v1.1.2
Serial No.   : VTS1600-030100001        MAC Address  : 00-01-95-04-2b-ca
IP mode      : Static IP                IP Address   : 192.168.161.5

Select menu
1. Network configuration
2. Serial port configuration
3. Clustering configuration
4. PC Card configuration
5. System Status & log
6. System administration
7. Save changes
8. Exit without saving
9. Exit and apply changes
a. Exit and reboot
 <ENTER> Refresh
----->
```

Save and apply changes

11) You have successfully configured VTS IP setting. Now, you may access the VTS in management tools such as Web/Telnet/SSH with the IP that you have configured just before. For example, you may test VTS in web interface like below.



You may login into VTS using web browser and change settings

1.2. How to access the VTS to configure its features

You may access and configure the VTS by any one of four methods:

- Access and configure VTS using a Console cable
- Access and configure VTS using Telnet/SSH
- Access and configure VTS using a Web browser
- Access and configure VTS using HelloDevice Manager

1.2.1. Access and configure VTS using a Console cable

1) Connect the console cable.

Connect the console cable to the port labeled “Console” on the VTS with the RJ-45

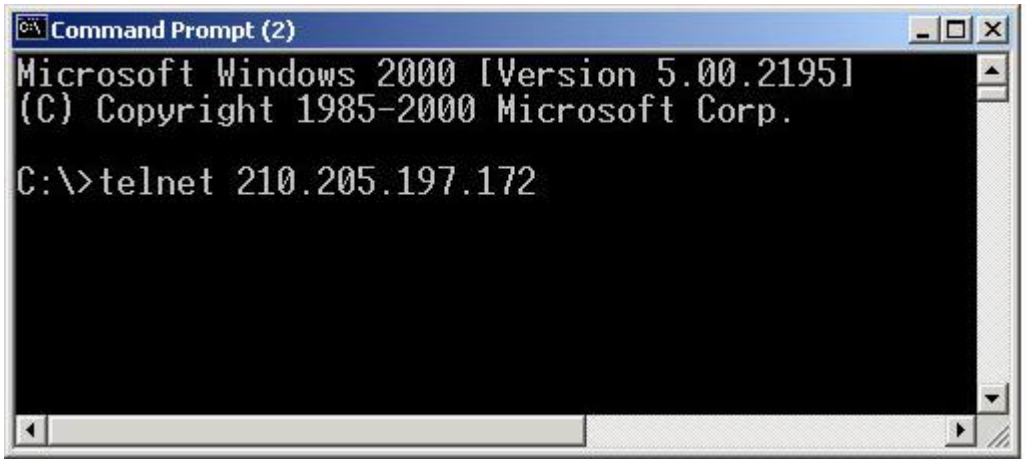
connector end, and to your PC's available COM port with the serial port end.

2) Access the console port of the VTS using terminal emulation program. You will see a login prompt on the console screen. Refer to the chapter 1.1 for details.

3) Enter admin as login name and admin as password, and press Enter.
4) After successful login, you may see the window like below

1.2.2. Access and configure VTS using Telnet/SSH

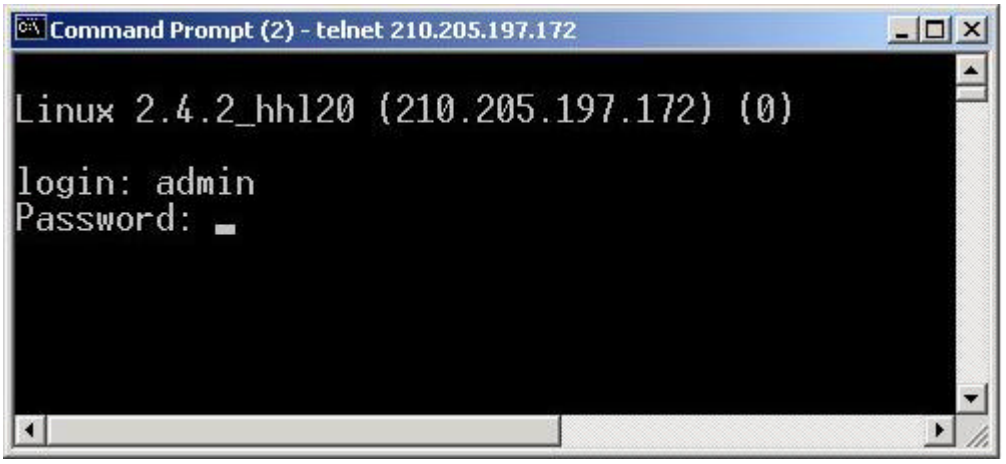
1) Connect Hub to workstation and VTS with Ethernet cable.
2) Telnet to <IP assigned to the VTS>. You may type 'telnet' at the command prompt like below or use a telnet client program.



Access and configure VTS using Telnet

Or if you have SSH client you may use SSH program to connect VTS for Secure connection.

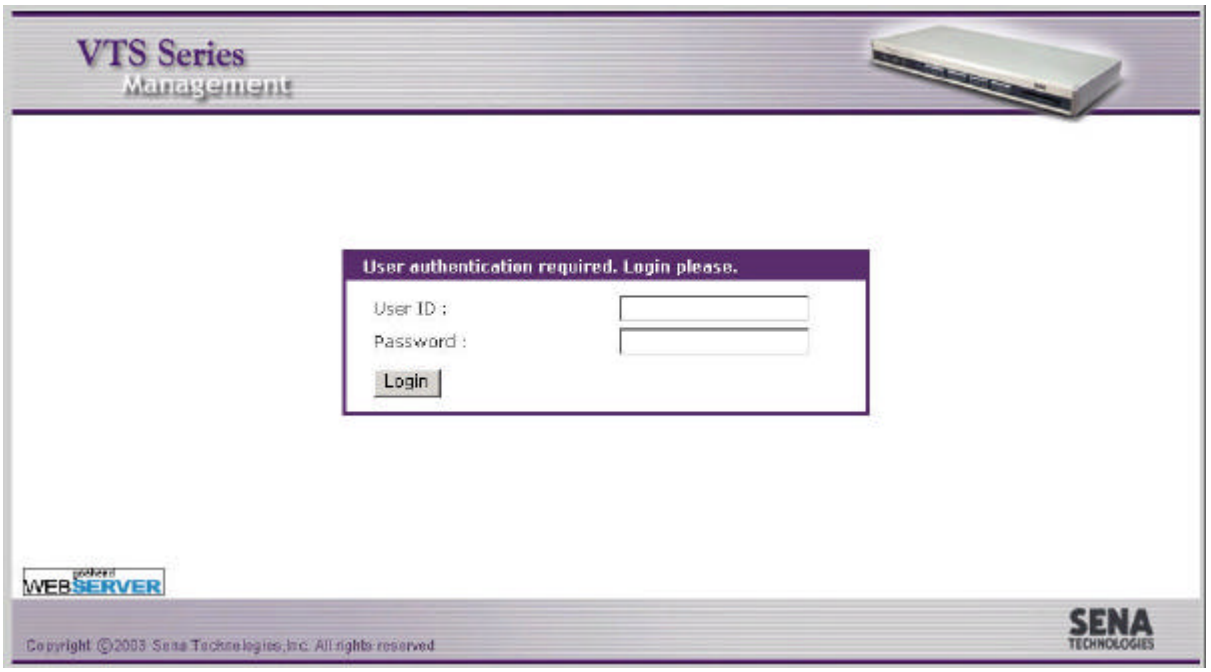
Enter admin as login name and admin as password, and press Enter.



Enter authentication details

1.2.3. Access and configure VTS using a Web browser

1) Connect Hub to workstation and VTS with Ethernet cable.
2) Use standard Browser like Internet Explorer or Netscape and Point your browser to the IP address assigned to the VTS. For e.g., http://192.168.44.100. The login page will appear like below



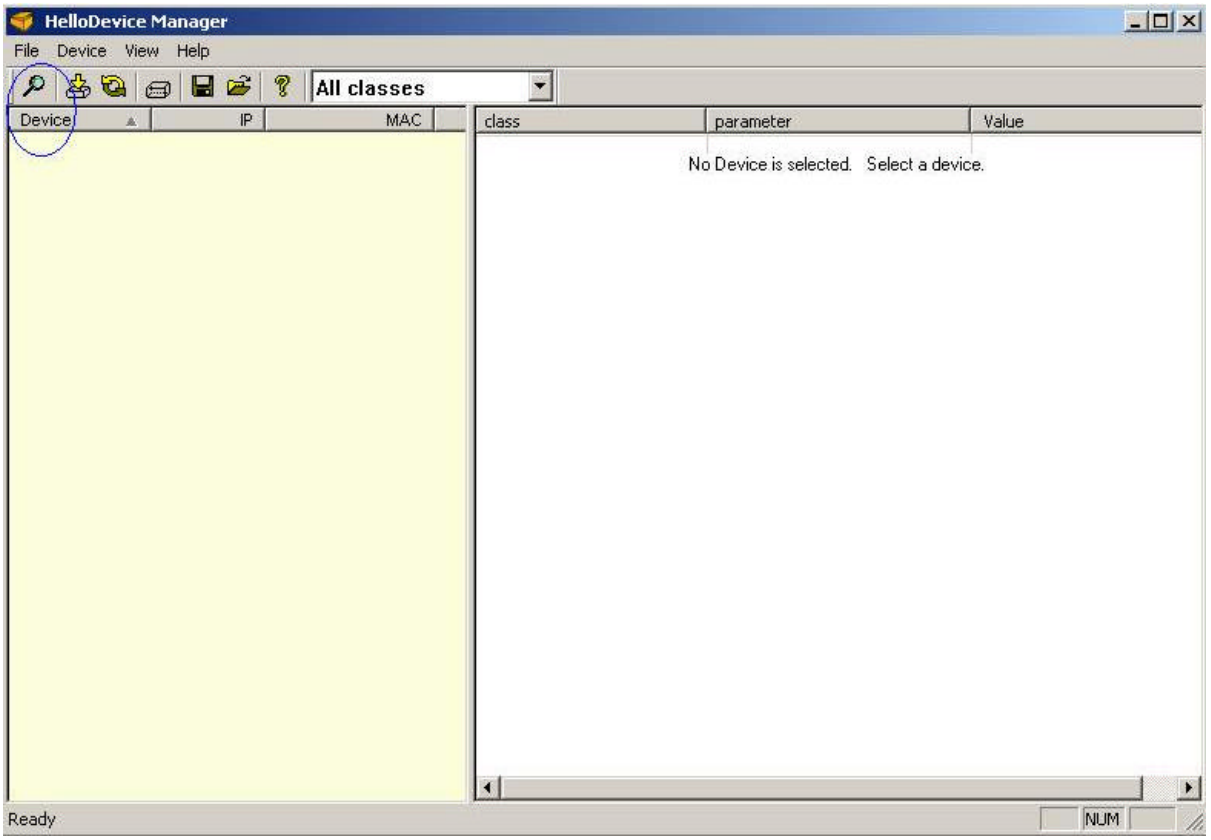
Access and configure VTS using a Web browser

3) Enter admin as login name and admin as password, and click login button.

1.2.4. Access and configure VTS using a HelloDevice Manager.

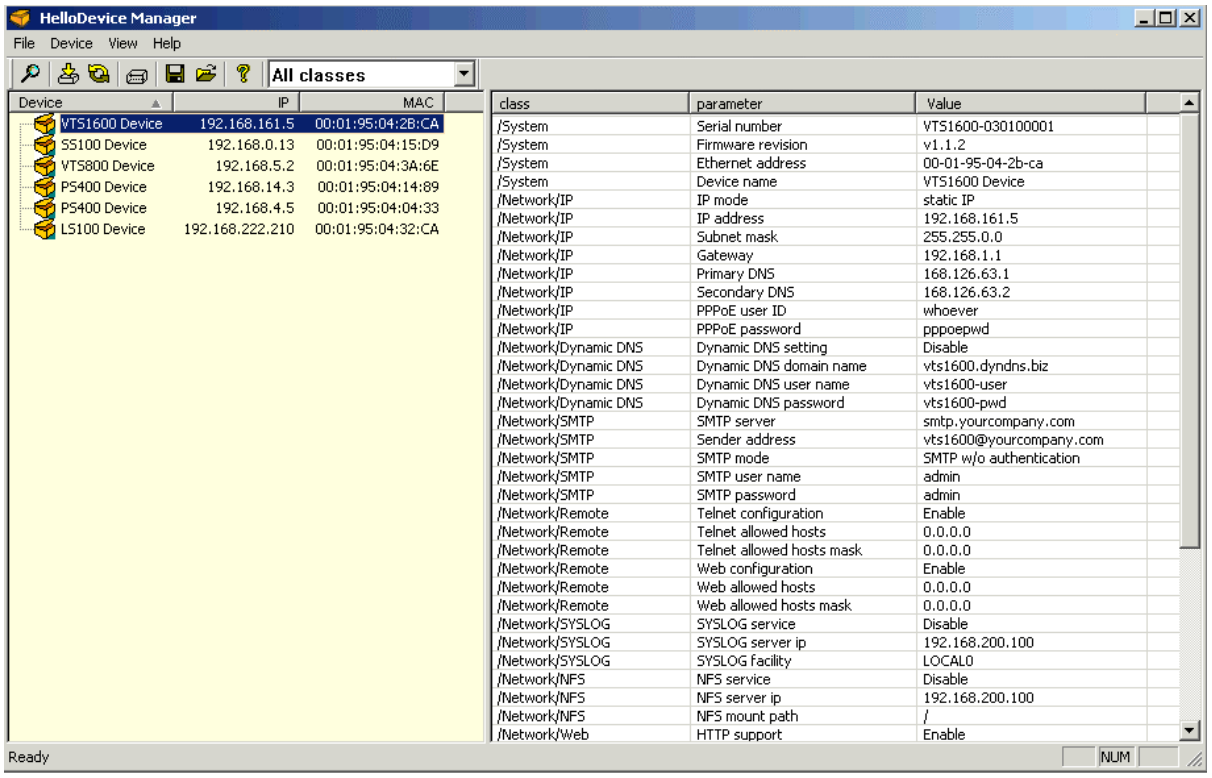
Set up the HelloDevice Manager in your PC. You can get the latest version of the HelloDevice Manager in http://www.sena.com/support/download/

1) Connect the VTS in the network where the PC with HelloDevice manager is installed.
2) Click 'Probe' button to find the IP address of VTS.



Access and configure VTS using HelloDevice Manager

3) Enter admin as login name and admin as password, and press Enter.



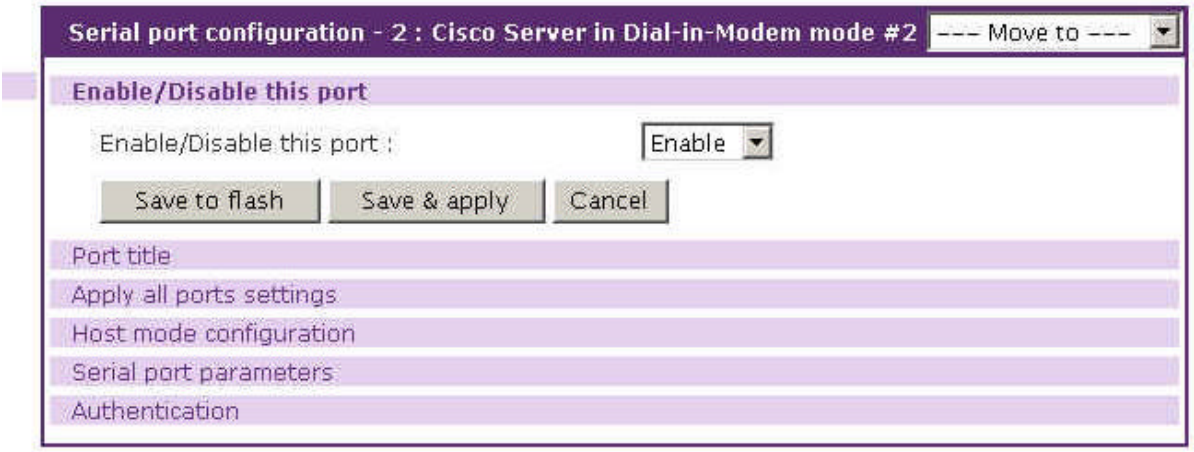
Enter authentication details and get access to access and configure VTS

1.3. How to access a device via modem?

The VTS series facilitates four communication modes between serial devices and remote hosts. Console server, terminal server, dial-in modem, and dial-in terminal server. Below is the brief description about Dial-in modem mode.

About Dial-in modem mode: This mode allows access to the serial port from a remote site via an analog modem connection. When a serial port is configured as dial-in modem mode, the VTS assumes that the serial port is connected with an external modem, and waits for a dial-in connection from a remote site. Using a terminal emulation program to access the VTS will result in the display of all available serial ports. The user can then select a serial port to access.

1.3.1. Options to the user in this mode

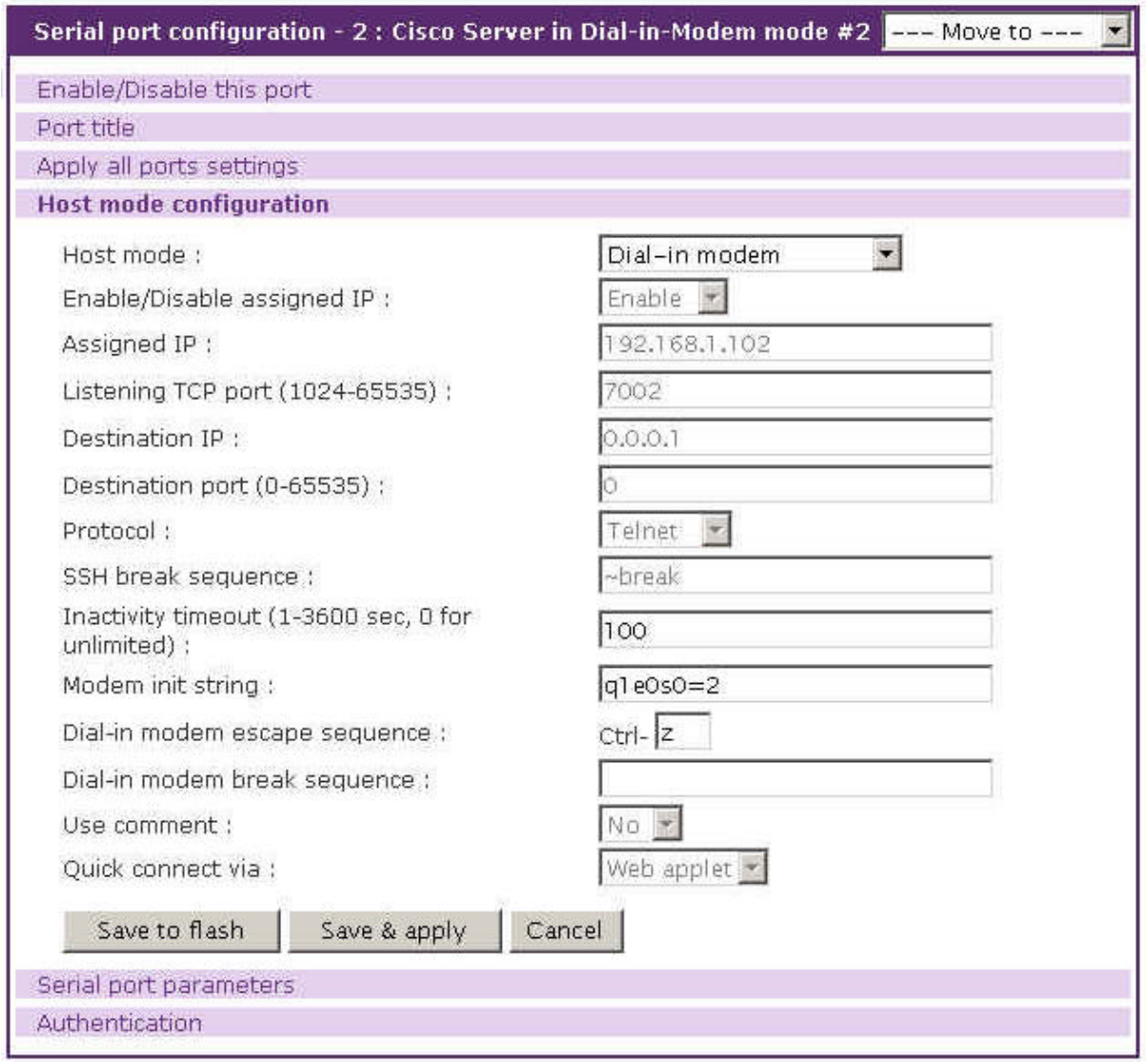


Options in Dial-in-modem mode

1.3.2. Dial-in-modem parameters

In this mode, users need to configure the following parameters in Host mode configuration:

- Inactivity timeout
- Modem init string
- Dial-in modem escape sequence
- Dial-in modem break sequence



Dial-in-modem parameters

1) Inactivity timeout

If there is no activity between the VTS and the dial-in client program during the specified inactivity timeout interval, the existing session will automatically be closed. If the user wants to maintain the connection indefinitely, configure the inactivity timeout period to 0.

2) Modem init string

The modem init string is used to initialize an external modem attached to a serial

port. If the user does not specify any init string, the default init command is used. The default modem init command is ‘q1e0s0=2’. For more information about the modem init string, please refer to the modem manual.

3) Dial-in modem escape sequence

Dial-in modem escape sequence is used to stop using a connected port and return to initial menu. Configured characters should be used while a Ctrl key pressed.

4) Dial-in modem break sequence

Dial-in modem break sequence is used to send a break signal when using a port configured as a Console server mode via Dial-in modem.

When the host mode is configured as either “dial-in modem mode”, the user cannot set the DTR behavior. Also port-logging feature will not be accessible if the serial port is configured to this mode (dial-in modem mode).

2. Connections between VTS and various devices

2.1. How to configure a console port on Linux PC

To use the ordinary serial port of a PC as a console redirection port, a user needs to configure the Linux.

1) A complete documentation of this how-to is http://www.linux.org/docs/ldp/howto/Remote-Serial-Console-HOWTO .
2) Basically, you need to configure a boot loader and an init system to configure a serial console port. See 3) and 4) for this.
3) See the LILO configuration in '5.1. Configure Linux kernel using LILO' of the Linux document.
4) See the inittab configuration in '6.1. init system' of the Linux document.

2.2. How to configure a console port on Windows 2003 server

Windows 2003 Server supports console redirection to the serial port. To utilize this functionality a user should follow the steps below.

1) Run cmd.exe on Windows 2003.
2) Run bootcfg.exe. The following command line configures the COM1 as an EMS redirection port at the baud rate of 9600. This EMS setting is added to the boot entry ID, 1. Boot entries and their ID are displayed by running 'bootcfg /query'.

```
bootcfg /ems ON /port COM1 /baud 9600 /id 1
```

Reference:

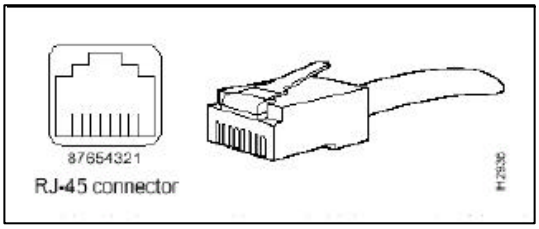
(1) Windows 2003 Server> Start button > Help and Support > bootcfg: Command-line reference, Enabling Emergency Management Services after setup

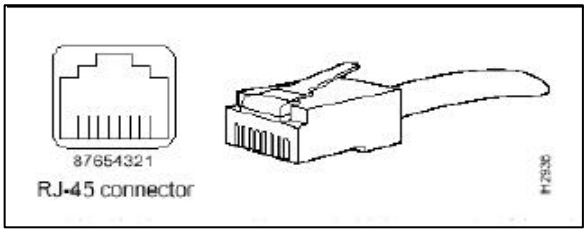
2.3. How to wire between VTS and devices

Devices export different serial interfaces. VTS provides 2 sets of RJ45 straight cables and 4 types of adapters. There lists some categories of devices that a user can connect with the cable and adapter accessories given with VTS.

2.3.1. VTS to DTE(RJ-45)

Sun Netra Server & All Cisco equipments and other RJ45 DTE Device fall in this category. A user just uses the RJ45 straight cable to connect these devices.

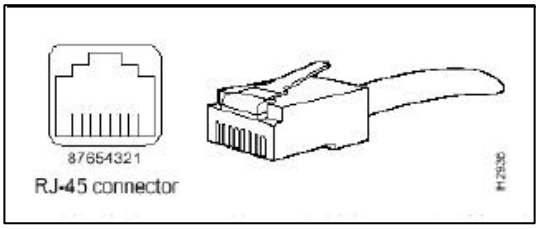


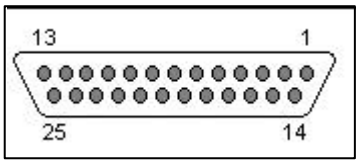


VTS			DTE(RJ-45)	
Pin	Description		Description	Pin
1	CTS	◀——	RTS	8
2	DSR	◀——	DTR	7
3	RxD	◀——	TxD	6
4	GND	◀——▶	GND	4
5	DCD	◀——	DCD	5
6	TxD	——▶	RxD	3
7	DTR	——▶	DSR	2
8	RTS	——▶	CTS	1
RJ 45 Male connector			RJ 45 Male connector	

2.3.2. VTS to DTE(DB25 Female)

Sun Sparc Servers and other DB25 DTE devices fall in this category. The RJ45 straight cable and the RJ45-DB25 female adapter (No. EP0401079) connects the device and VTS.

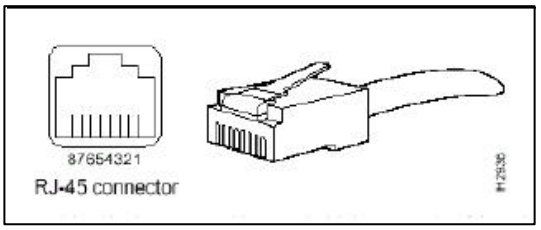


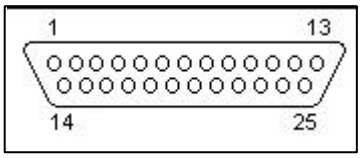


VTS			DTE(DB25 Female)	
Pin	Description		Description	Pin
1	CTS	←	RTS	4
2	DSR	←	DTR	20
3	RxD	←	TxD	2
4	GND	↔	GND	7
5	DCD	←	DCD	8
6	TxD	→	RxD	3
7	DTR	→	DSR	6
8	RTS	→	CTS	5
RJ 45 Male connector			DB25 Male connector	

2.3.3. VTS to DTE(DB25 Male)

Serial Printers and other DB25 DTE devices fall in this category. The RJ45 straight cable and the RJ45-DB25 male adapter (No. EP0401080) connects the device and VTS.

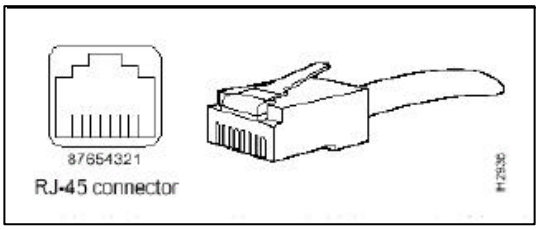


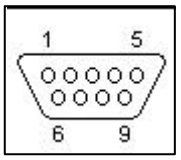


VTS			DTE(DB25 male)	
Pin	Description		Description	Pin
1	CTS	←	RTS	4
2	DSR	←	DTR	20
3	RxD	←	TxD	2
4	GND	↔	GND	7
5	DCD	↔	DCD	8
6	TxD	→	RxD	3
7	DTR	→	DSR	6
8	RTS	→	CTS	5
RJ 45 Male connector			DB25 Female Connector	

2.3.4. VTS to DTE(DB9 Male)

Nortel equipments, HP Server (IA SERVER TC2110, HP 9000, RP2400), IBM Server (RS/6000) and other DB9 DTE devices fall in this category. The RJ45 straight cable and the RJ45-DB9 male adapter (No. EP0401078) connects the device and VTS.

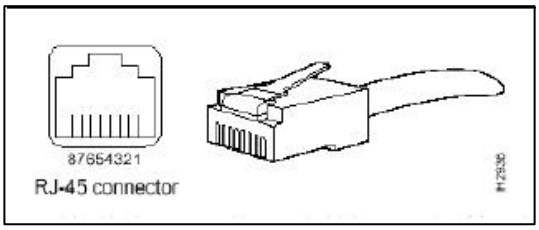


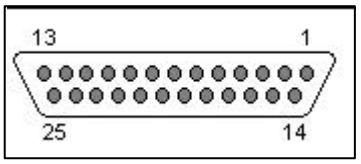


VTS			DTE(DB9 Male)	
Pin	Description		Description	Pin
1	CTS	◀	RTS	7
2	DSR	◀	DTR	4
3	RxD	◀	TxD	3
4	GND	◀▶	GND	5
5	DCD	◀ ● ▶	DCD	1
6	TxD	▶	RxD	2
7	DTR	● ▶	DSR	6
8	RTS	▶	CTS	8
RJ 45 Male connector			DB9 Female Connector	

2.3.5. VTS to DCE(DB25 Female)

Modems, ISDN adapters and other DB25 DCE devices fall in this category. The RJ45 straight cable and the RJ45-DB25 female adapter (No. EP0401081) connects the device and VTS.





VTS			DTE(DB25 Female)	
Pin	Description		Description	Pin
1	CTS	◀	CTS	5
2	DSR	◀	DSR	6
3	RxD	◀	RxD	3
4	GND	◀▶	GND	7
5	DCD	◀	DCD	8
6	TxD	▶	TxD	2
7	DTR	▶	DTR	20
8	RTS	▶	RTS	4
RJ 45 Male connector			DB25 Male connector	

Reference:

(1) VTS user manual > Appendix A: Connections

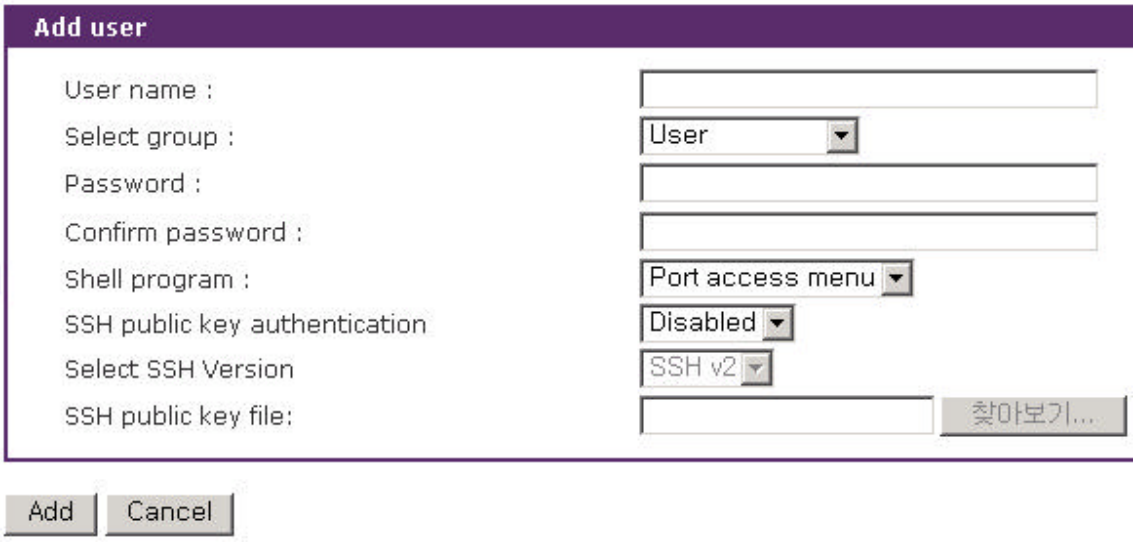
3. User administration and user's connection

3.1. How can I add a user to the VTS local database?

Follow the steps below.

1) From the Web menu, go to 'System administration > Users administration'

2) Select the 'Add User' link and you'll see the 'Add user' pane.



3) Fill out the user information for a new user.

User name/Password/Confirm password – These are mandatory fields to fill out. For other fields, see the reference (1).

4) Click 'Add' button to store the input.

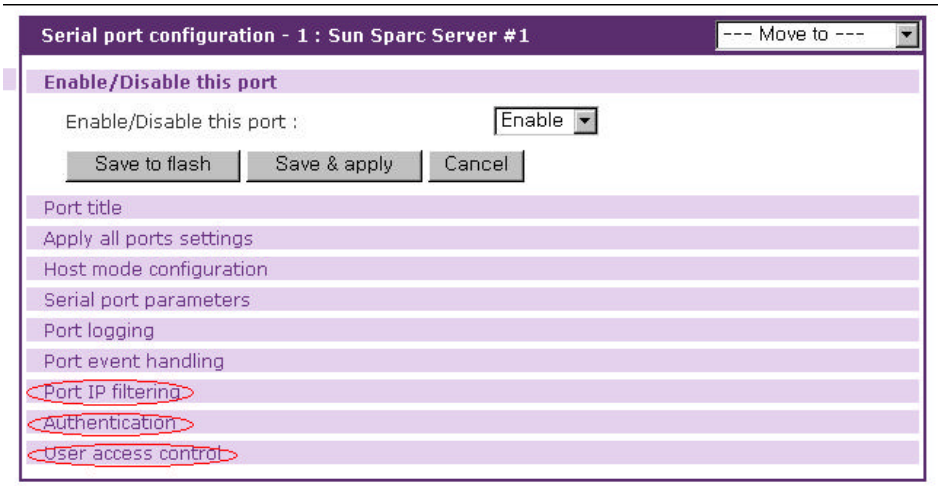
Note:

Once certain user account is added to the VTS local database, the user can access all the ports of the VTS unless the following rules are specified in the port configuration

(1) Port IP filtering

(2) Authentication: External authentication is enabled

(3) User Access Control: permission/restriction



References:

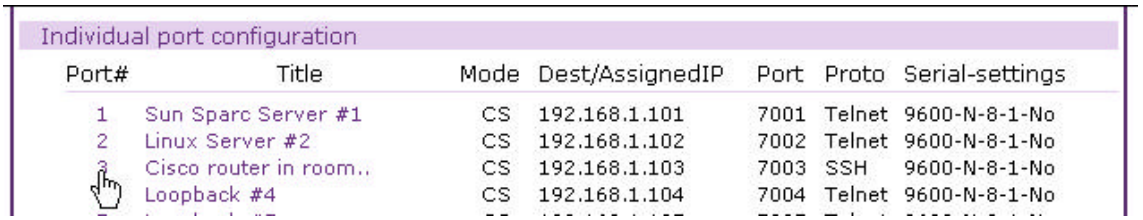
(1) VTS user manual > 8.1 User administration

3.2. How can I configure users' access to the ports?

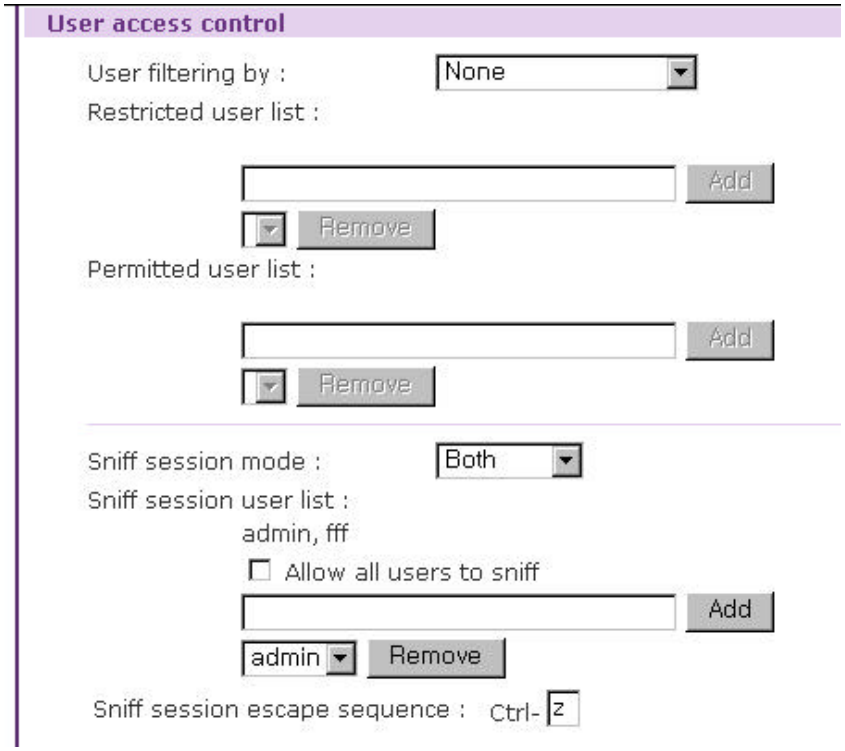
Assuming that

- Cisco equipment is connected to the port 3
- Cisco users are *sam, james, tim*
- Give the right to access to the port 3 to only Cisco users
- Authentication is done locally using VTS local database
- The user accounts for *sam, james, tim* are already created in the VTS local database based on the steps in section 1.1.

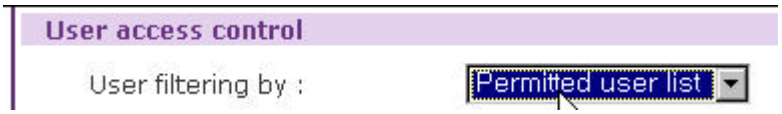
1) From the web menu, go to 'Serial port > Configuration > Individual port configuration > Port# 3'.



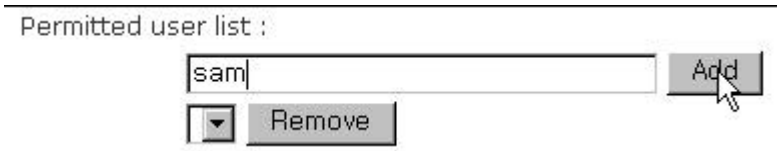
2) Go to '> User access control'.



3) Set the 'User filtering by' option to 'Permitted user list'

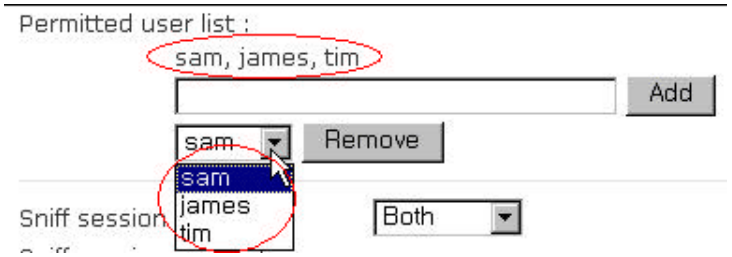


4) Type the user name, *sam* and click 'Add' button.



5) Follow the same steps for adding other users' account.

If the user account addition is completed, you can see the account list

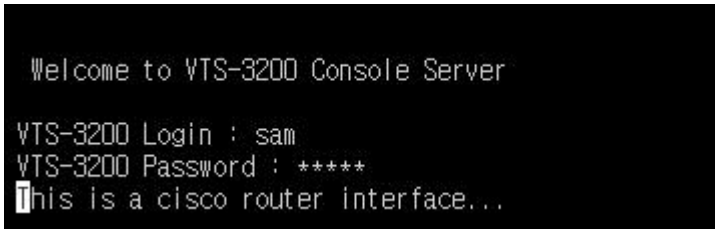


Note:

If the user doesn't add any user accounts to the permitted user list while he enabled user filtering by 'Permitted user list', then no one can access to the port.

6) Click 'Save & apply' button to store the input.

7) Once the users try to access the port# 3, they will find that only the registered users can access the port.



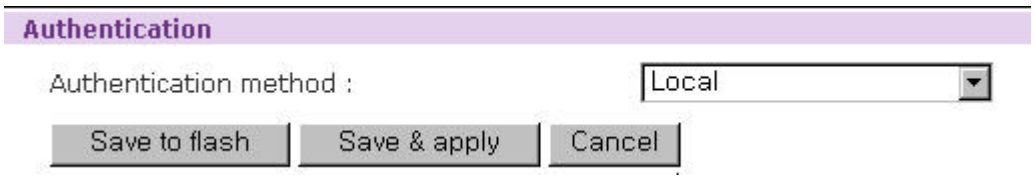
References:

(1) VTS user manual > 4.3.10 User access control configuration

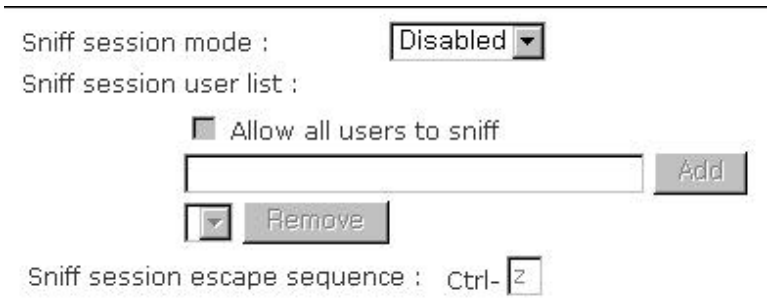
3.3. How can I make multiple local users access the same serial device and enable sniffing?

Unless 'sniff session mode' is enabled, only one user can access the port simultaneously. The factory default setting is 'disabled'.

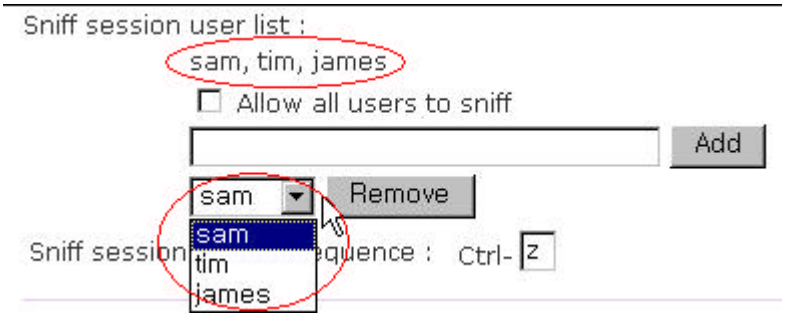
1) From the web menu, go to 'Serial port > Configuration > Individual port configuration > Port# 3'.
2) Go to '> Authentication'
3) Set the 'Authentication method' as 'Local'.



4) Click 'Save & apply' button to store it.
5) Go to '> User access control'

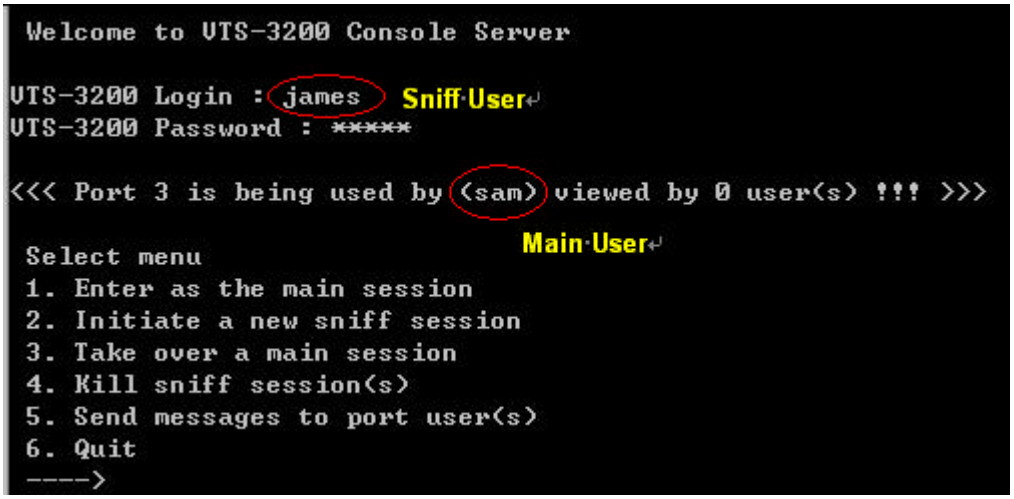


6) Configure the 'Sniff session mode' to one of 'Input', 'Output' and 'Both' to allow multiple sessions per port.
7) Add users to the sniff session user list.



8) Click 'Save & apply' button to store the input.

9) Once the users try to access the port# 3 when there is already a session established, they will see the menu for a sniff user.



References:

(1) VTS user manual > 4.3.10 User access control configuration

3.4. How can I control sessions using hot key in sniff session?

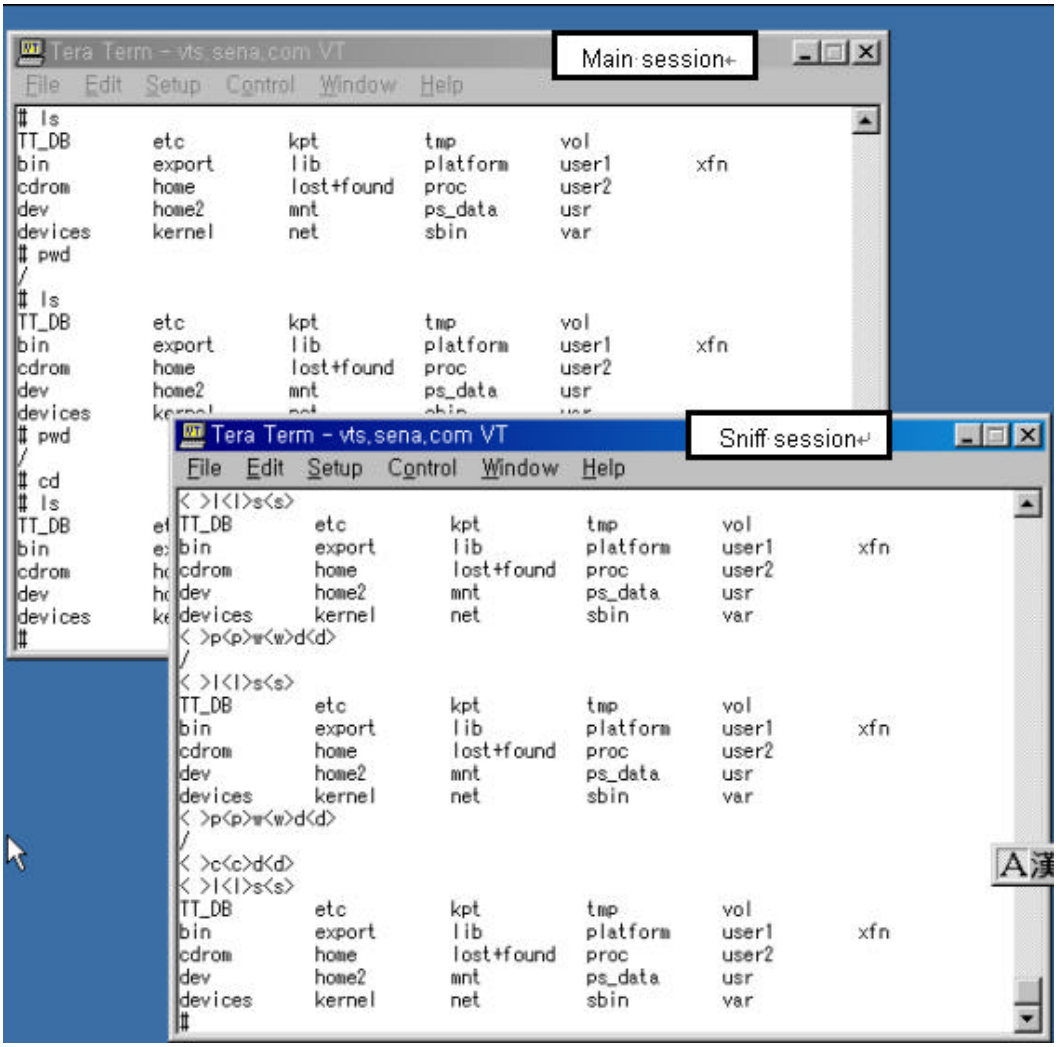
1) Access the port by terminal client program when there is a main session connected to the port.

```
 Welcome to VTS-3200 Console Server

VTS-3200 Login : james
VTS-3200 Password : *****

<<< Port 3 is being used by (sam) viewed by 0 user(s) !!! >>>

 Select menu
 1. Enter as the main session
 2. Initiate a new sniff session
 3. Take over a main session
 4. Kill sniff session(s)
 5. Send messages to port user(s)
 6. Quit
 ---->
```

2) Type '2' and press 'Enter' to create a sniff session to connect to the port.

```
New sniff session started (type '^z' to go back to main menu) ...
```

The user will see all that the main session user types.



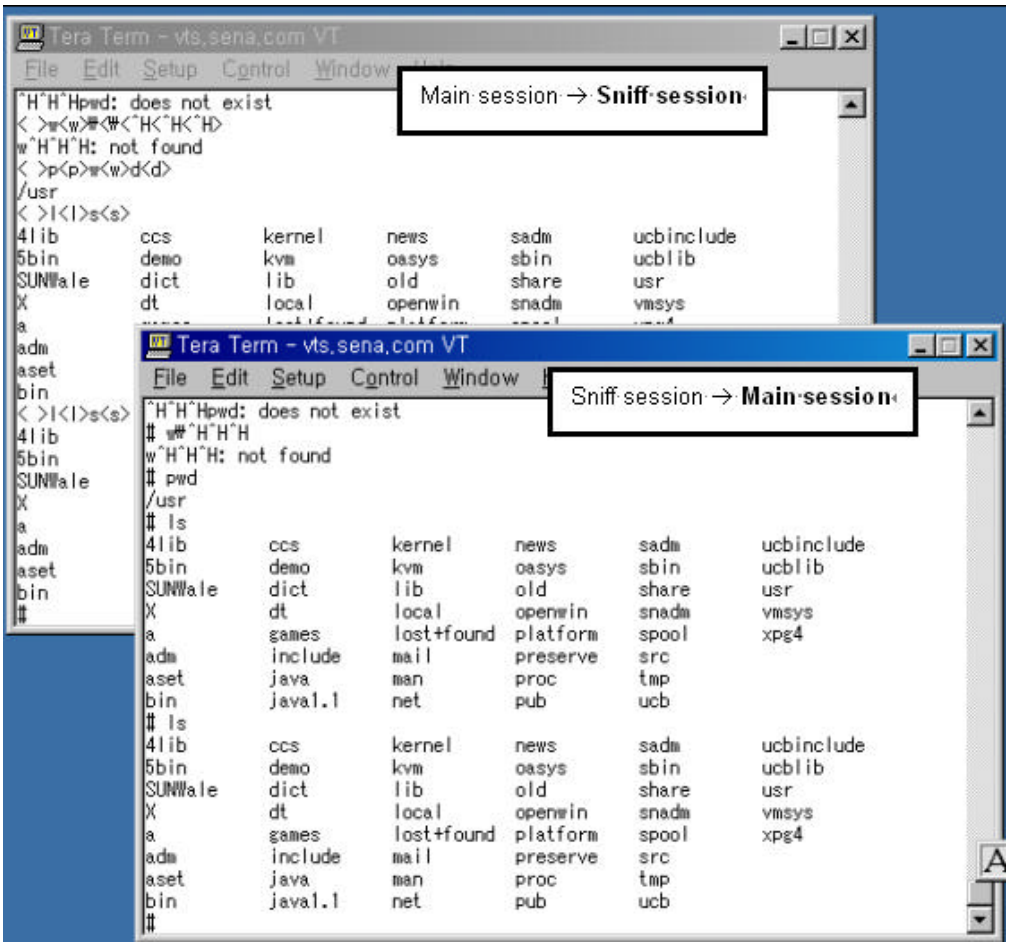
3) Press 'Ctrl+z' to see the sniff user menu again.

```
<<< Port 3 is being used by (sam) viewed by 0 user(s) !!! >>>

 Select menu
 1. Enter as the main session
 2. Initiate a new sniff session
 3. Take over a main session
 4. Kill sniff session(s)
 5. Send messages to port user(s)
 6. Quit
 ---->
```

Note:

- The factory default setting of the hot key is 'ctrl+z', and it is configurable in 'Serial port > Configuration > Host mode configuration' page.
- Only sniff session users can use hot key menu. It is not available to main session user.

4) Type '3' and press 'Enter' to connect to the port as a main session.



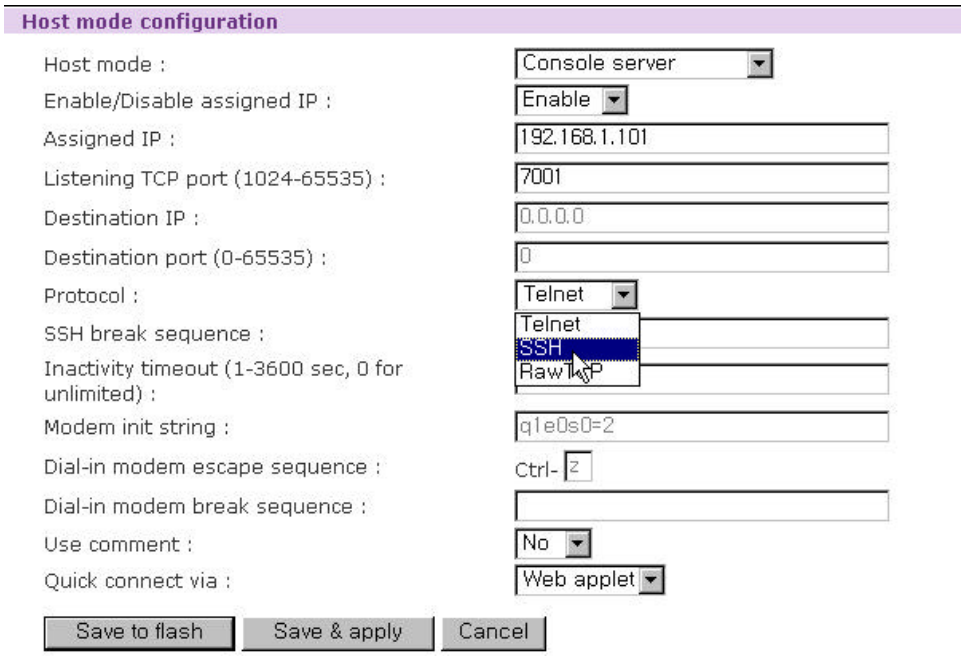
The sniff session user becomes the main session user if he takes over the main session, though the existing main session is converted into sniff session accordingly.

References:

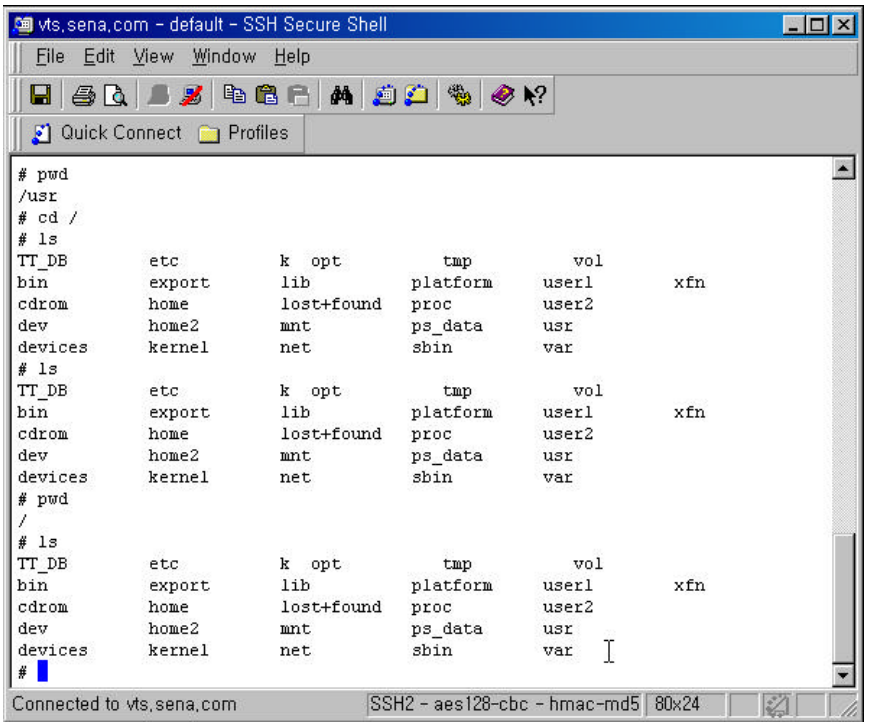
(1) VTS user manual > 4.3.10 User access control configuration

3.5. How can I run a SSH session for secure connection?

1) From the web menu, go to 'Serial port > Configuration > Individual port configuration > Port# > Host mode configuration'.
2) Set the 'Protocol' parameter as 'SSH'



3) Click 'Save & apply' to save the changes.
4) Connect to the port using SSH client program.



Reference:

(1) Free SSH client program can be downloaded at the SSH web site. http://www.ssh.com/support/downloads/secureshellwks/non-commercial.html

3.6. How can I access to the port using SSH public key authentication?

To access the port using public key based SSH connection, the user has to do the following steps.

- Generate SSH public key file
- Modify the public key file to meet the SSH daemon of the VTS
- Configure the VTS port parameters for SSH connection
- Configure the VTS user account for public key authentication
- Access the port using SSH public key authentication

In this guide, we will use the SSH client program provided by SSH Communication Security (http://www.ssh.com).

3.6.1. Generate SSH public key

1) Run SSH client program

2) Go to the screen, 'Edit > Settings'.

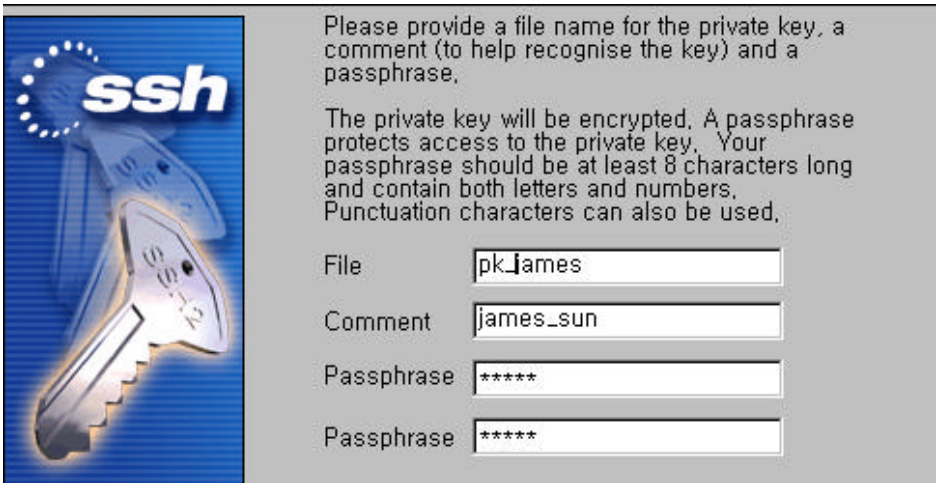
3) Go to the screen, 'Global Settings > User Authentication > Keys'.

4) Create the key by clicking the 'Generate New' button using the following settings.

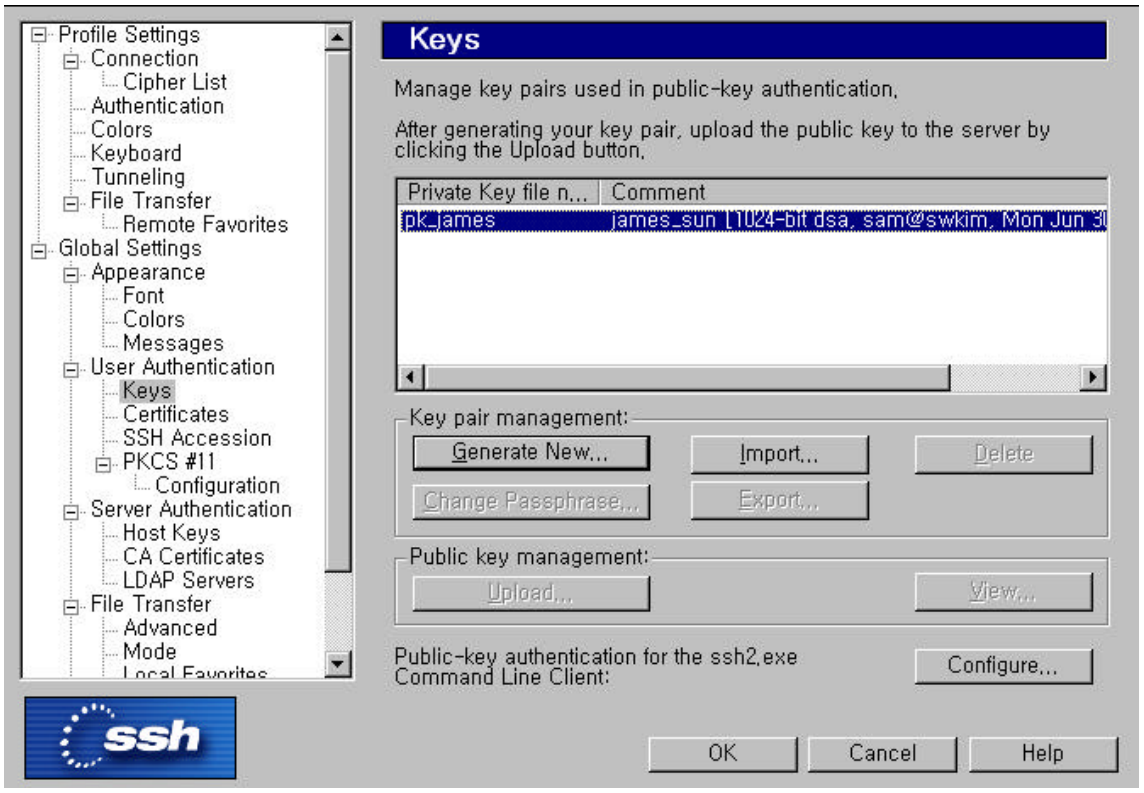
Key: DSA

Key length: 1024

5) Enter the appropriate Passphrase and store the public key file.



6) Press 'Complete' button.

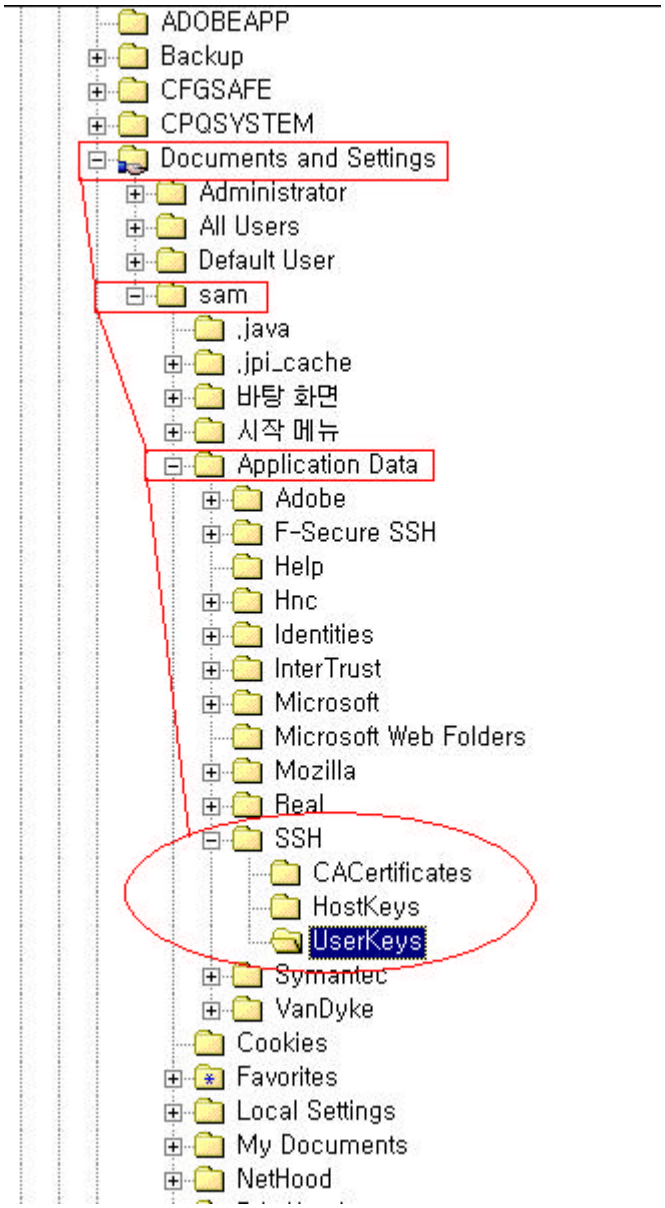


Note:

Do not try to upload the public key file right away, since the user need to modify the key file created to make it understood by the VTS.

3.6.2. Modify the public key to meet the VTS SSH daemon

1) Go to the folder of 'root > Documents and settings > current user account > Application data > User keys'.



2) Save the public key file with different name.

The public key file name created is pk_james.pub. Store the file for the VTS as pk_james_vts.pub.

3) Open the file, pk_james_vts.pub in editor.

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "james_sun [1024-bit dsa, sam@swkim, Mon Jun 30 2003 11:19:23\
]"
AAAAB3NzaC1kc3MAAACBAM8bVY+OBRCAjmPHM2KR3JVlt5IjbrpI/JTjqwyFuSdQHkMJfA
ot3+YjQj4vFFeLTaa9kboy04kOJvrcfLXkkO3WgUTuKamN0gXmMF+nwE4WYF5DOz9R7csV
QGgSwyWkeQJ5g/vaUPg1ax0AaSTsOlcdwLoQw854D6J0wxhCJtpzAAAAFQCj0LmGXnUTXS
g0YQasCweBRTlUAQAAAIEAmO+wuqYIydVZb/Q8uCQDMcWSv4DdQKJIWqEzYJ8LJ6aBeYls
5+4B28wRuUqAdM8jEtYytv04I0pkTwDLwInllNqZ9qoq8mwflVvfnmU3CW9ASF9R2at6K7
n5PdSEVyVuHH8KZ+ztfZd8j8zYd/tCBU4s3DF5UQ+KFGsQznLDZQUAAACAPE4oT6sf+ymb
AXmStkk9FfNk+gtWprrl4JyCHZ884IDn3yNAzCe4SX/v3qbcDoNkixldhx60FNwTkjyvsS
yLkbiISoz2W+d5P5hSIMv6j7iTKZxcGHlo0vfy3AIsVlbCZyzsUE+LwjbFLG8WZUaPTDLl
Y4ccnfUpUjXJE0Eiuyk=
---- END SSH2 PUBLIC KEY ----
```


4) Do the following modifications.

- Add “SSH-dss[space]” before the starting for the key contents.
- Remove all the [newline] characters in the key contents


```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "james_sun [1024-bit dsa, sam@swkim, Mon Jun 30 2003 11:19:23\]"
ssh-dss AAAAB3NzaC1kc3MAAACBAM8bVY+OBRCAjmPHM2KR3JVlt5IjbrpI/JTjqwyFuSdQHkMJfAot3+YjQj4vFFeLTa
---- END SSH2 PUBLIC KEY ----
```

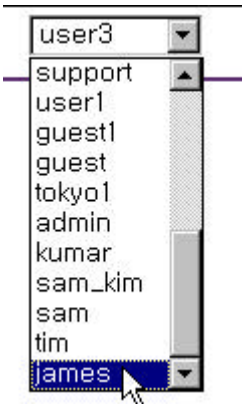

The contents of the file should be composed of four lines, header, comment, key string, footer.

3.6.3. Configure the VTS port parameters for SSH connection

1) From the web menu, go to ‘Serial port > Configuration > Individual port configuration > Port# > Host mode configuration’.
2) Set the ‘Protocol’ parameter as ‘SSH’
3) Click ‘Save & apply’ to save the changes.

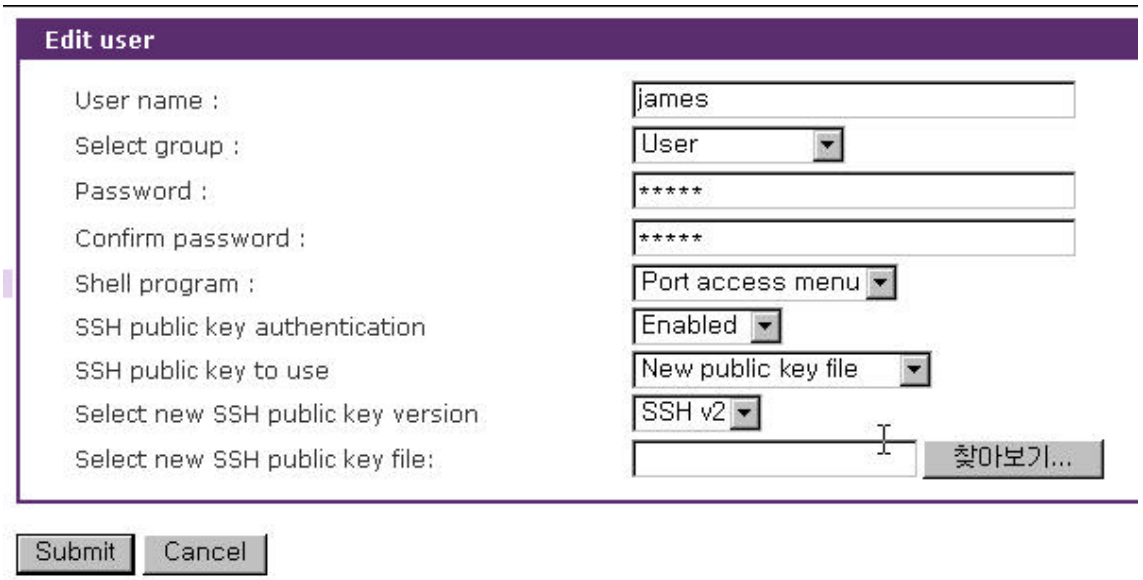
3.6.4. Configure the VTS user account for public key authentication

1) From the web menu, go to ‘System administration > User administration’.
2) Select the existing user account for *james* and click ‘Submit’ button.

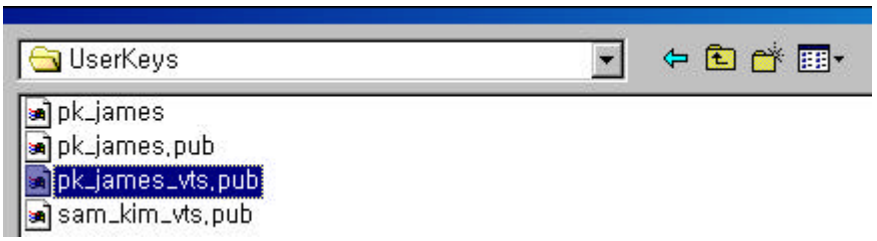


3) Configure the account for *james* as follows.

- SSH public key authentication: Enabled
- SSH public key to use: New public key file”
- Select new SSH public key version: SSH v2



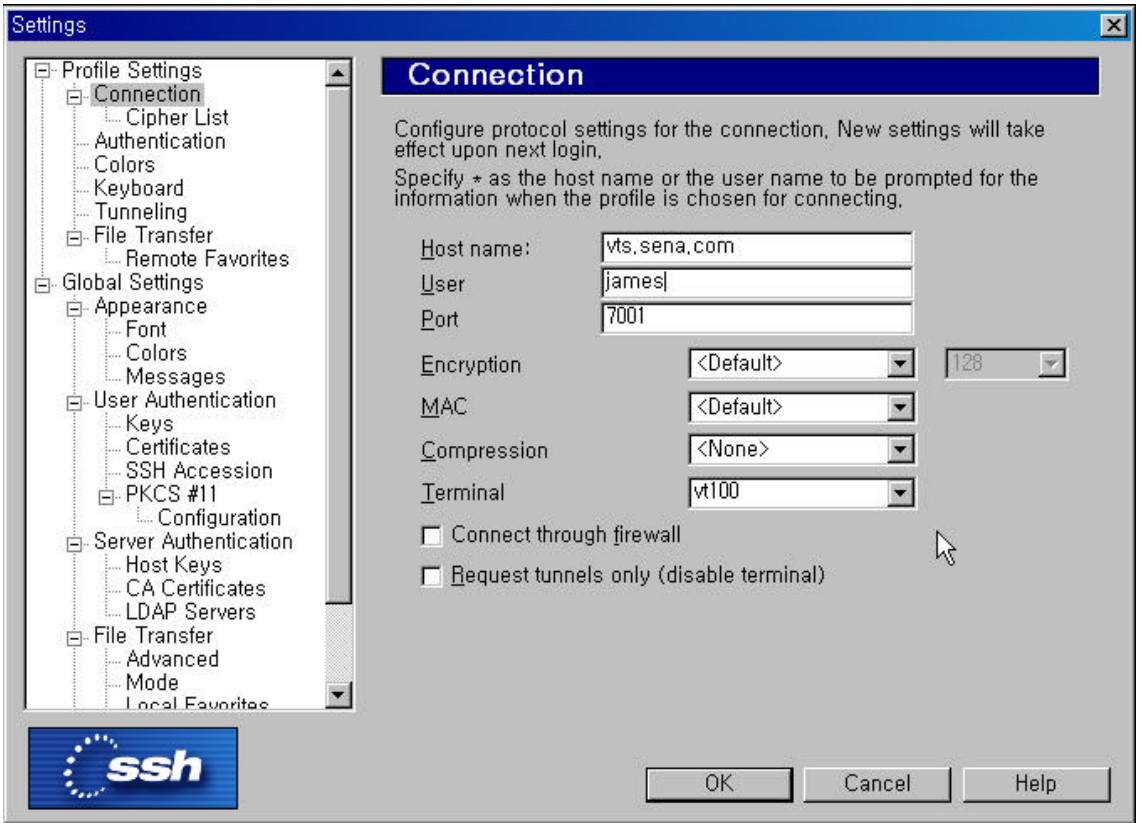
4) Choose the public key file in the ‘root > Documents and settings > current user account > Application data > User keys’ in order to upload to the VTS.



5) Click 'Submit' button to reflect the changes.

3.6.5. Access the port using SSH public key authentication

1) Set up the port connection parameters in SSH client program.



Note:

Keep in mind that the user has an access right to the port.

Look into the following configuration pages to make sure.

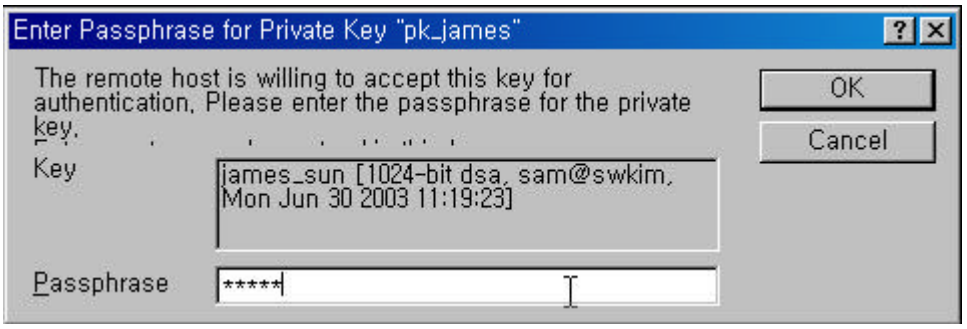
'Serial port > Configuration > Port# > Port IP filtering'

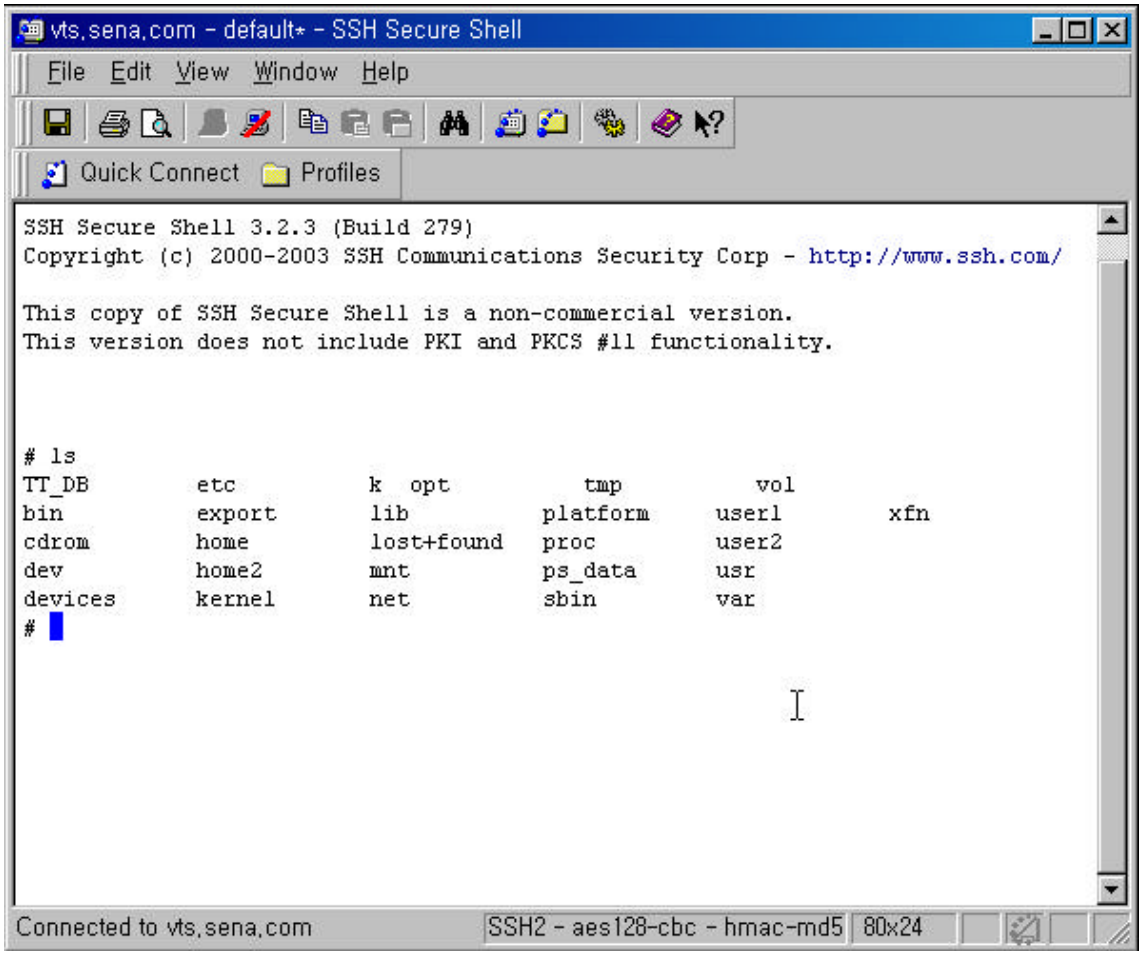
'Serial port > Configuration > Port# > Authentication'

'Serial port > Configuration > Port# > User access control'

2) Connect to the port using public key authentication.

3) Enter Passphrase that the user set up then he can connect to the port.





References:

(1) VTS user manual > 4.3.4 Host mode configuration

(2) VTS user manual > 4.3.9 Authentication configuration

(3) VTS user manual > 4.3.10 User access control configuration

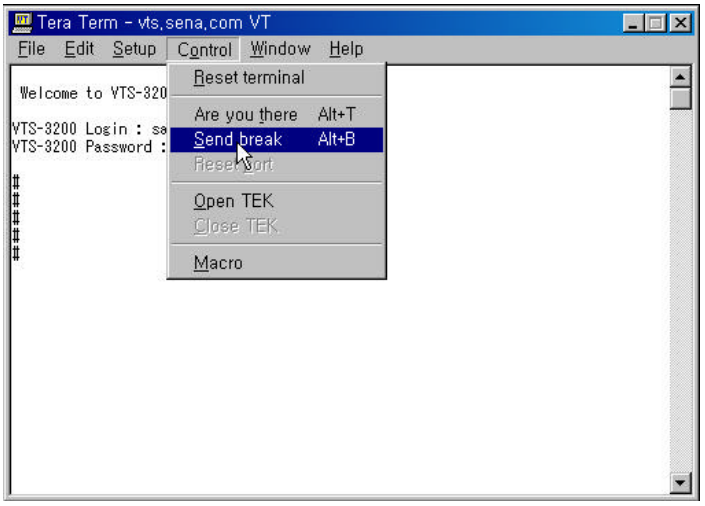
(4) VTS user manual > 8.1 User administration

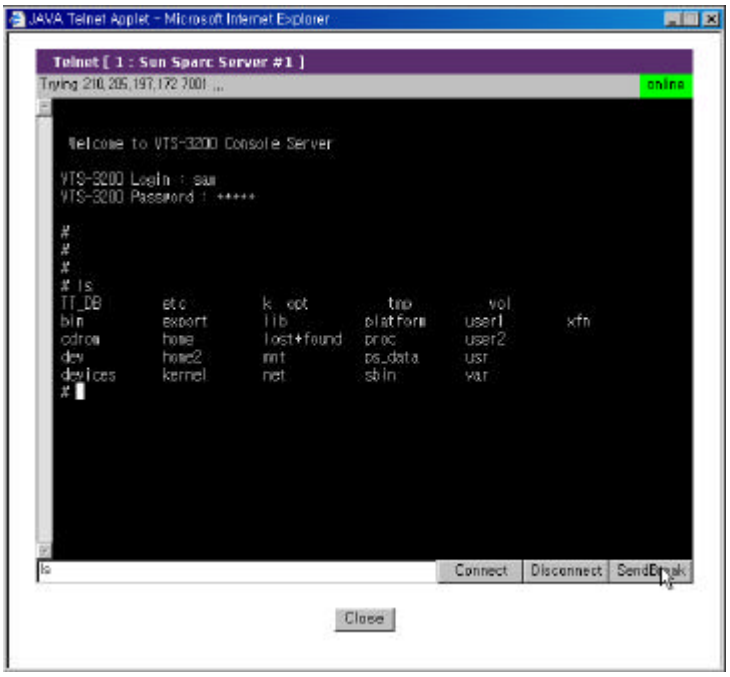
(5) SSH Communication Security web site, http://www.ssh.com

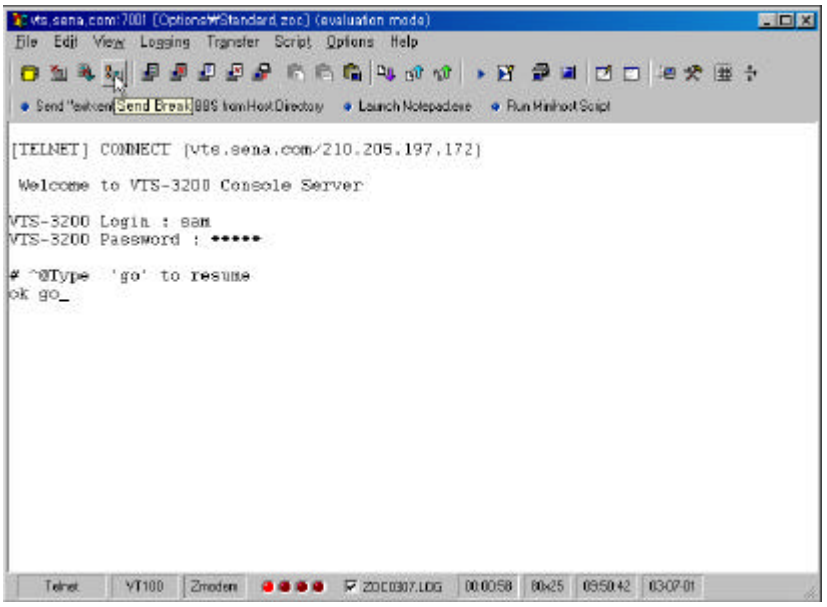
3.7. How can I send a Sun break signal using telnet?

1) Access the port of the VTS where Sun server is hooked up by using built-in Java Telnet applet or the telnet client program.

2) Send the Sun break signal manually by choosing 'Send Break' menu of the program.







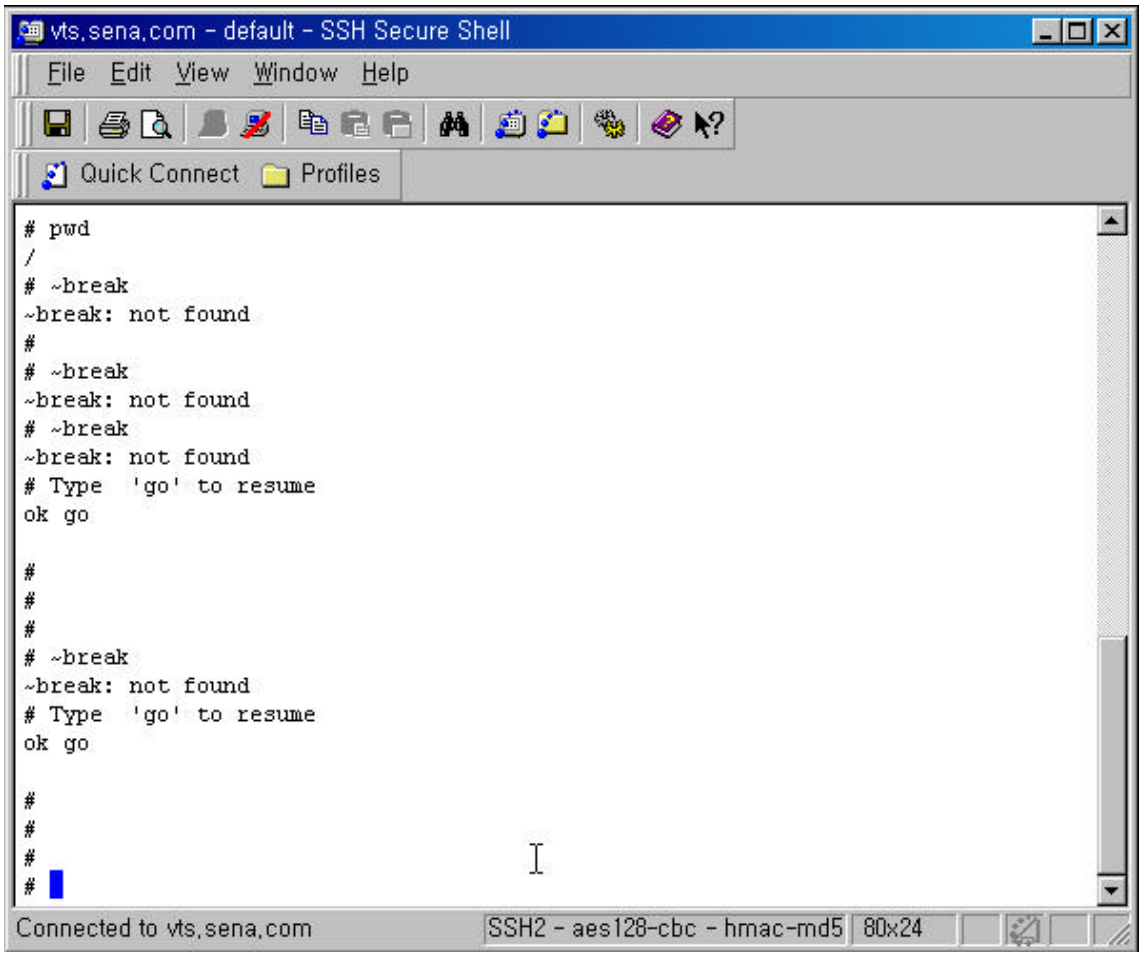
If the Sun break signal is sent to the port, the following message will be coming.

```
# ^@Type 'go' to resume
ok
```

3.8. How can I send a Sun break signal using SSH?

1) From the web menu, go to 'Serial port > Configuration > Individual port configuration > Port# 3 > Host mode configuration'.
2) Set up the SSH break sequence signal in the page.

3) Click 'Save & apply' to reflect the changes.
4) Run SSH client program or SSH Java applet of the VTS.
5) Type the SSH break sequence command that the user defined.

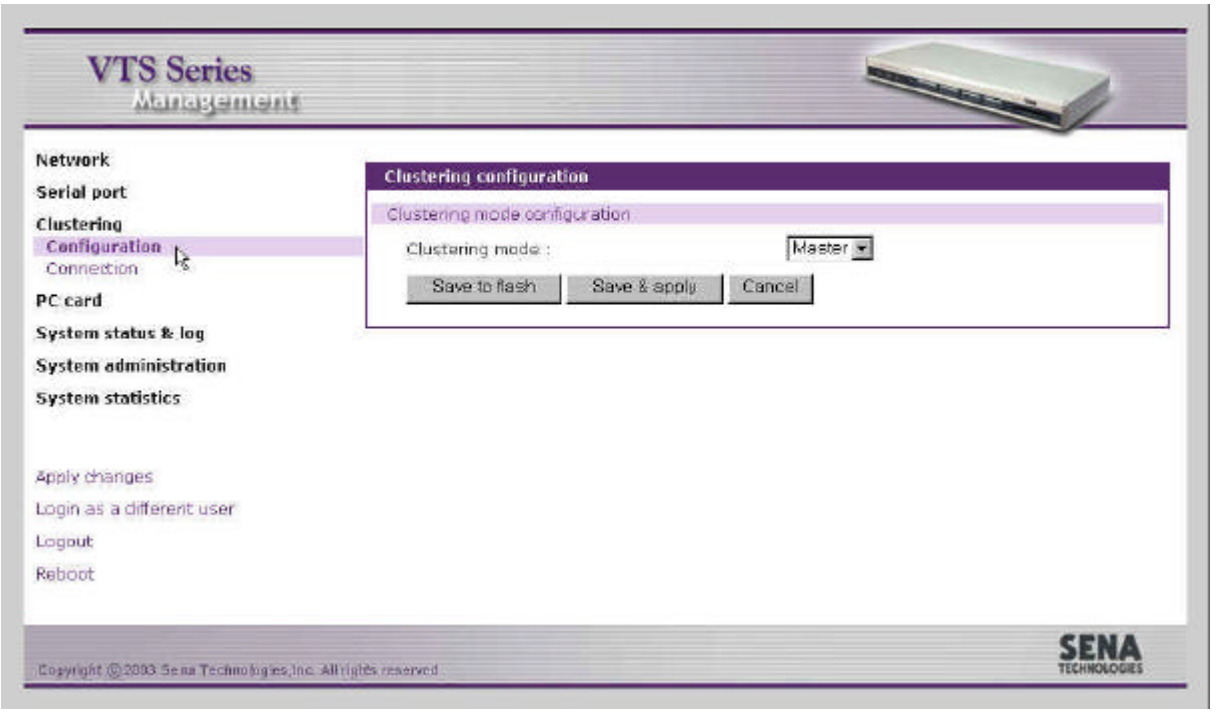


4. Clustering

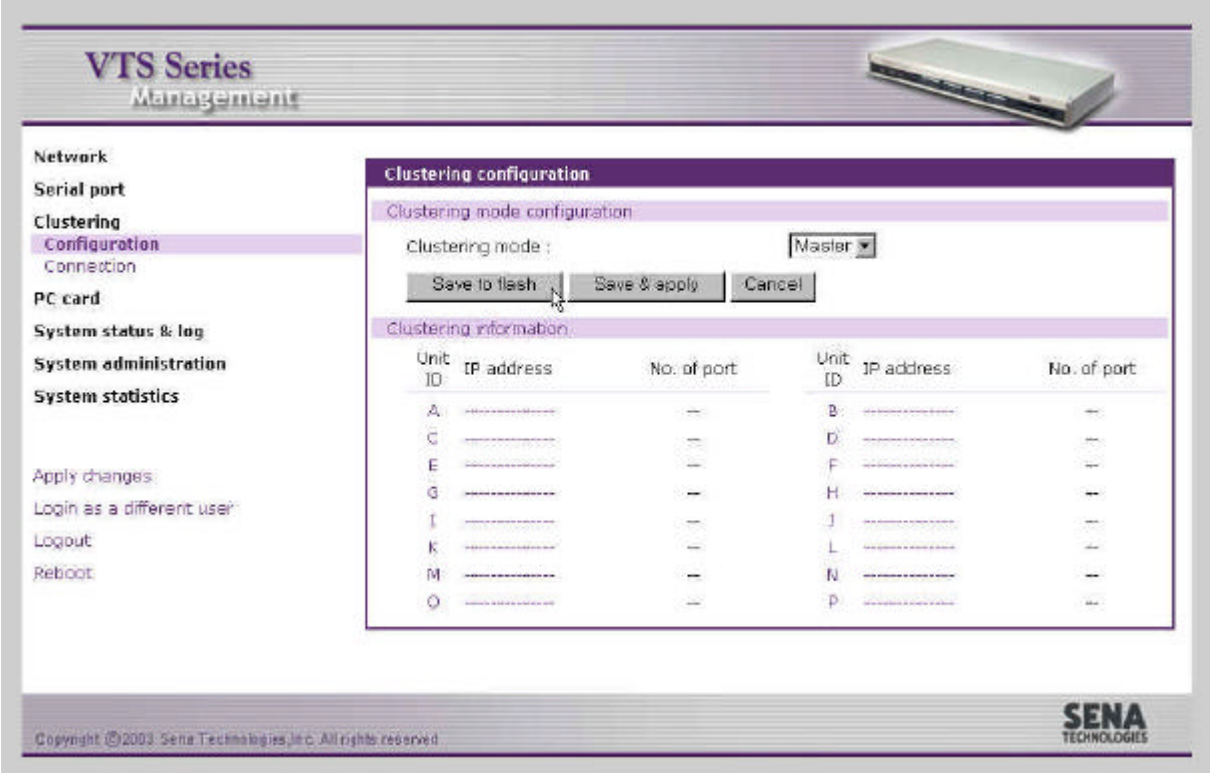
4.1. How can I use the clustering feature of the VTS?

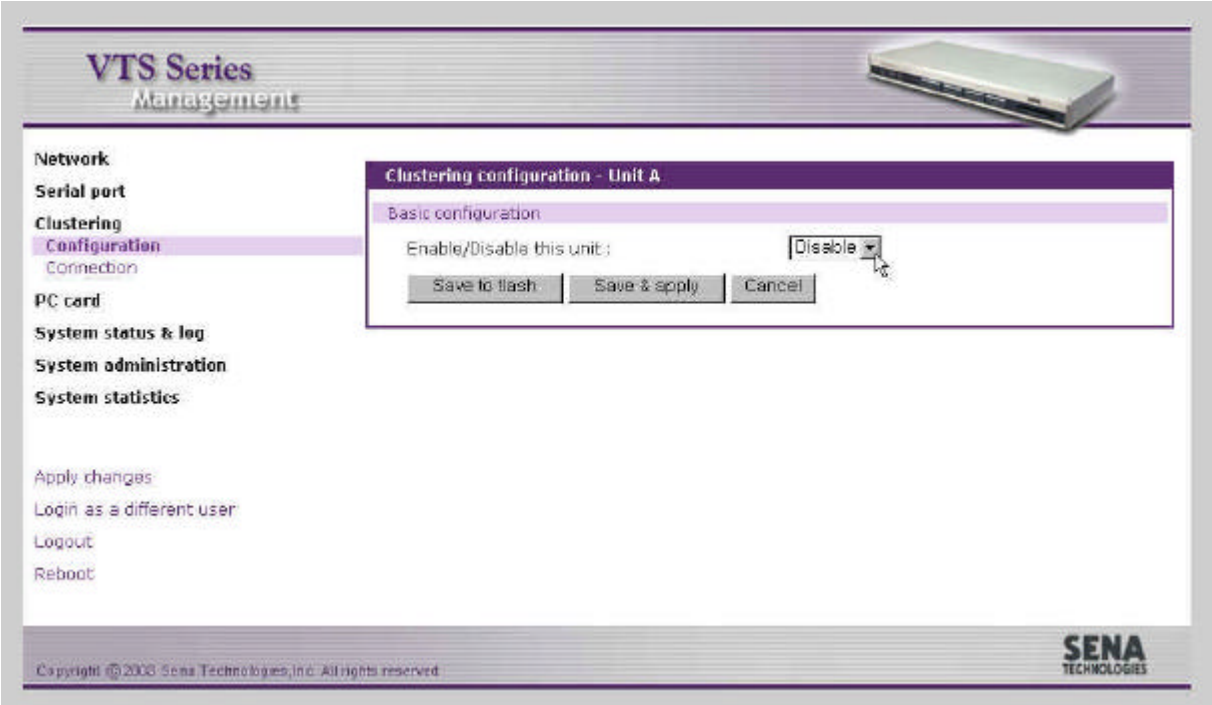
Follow the steps below.

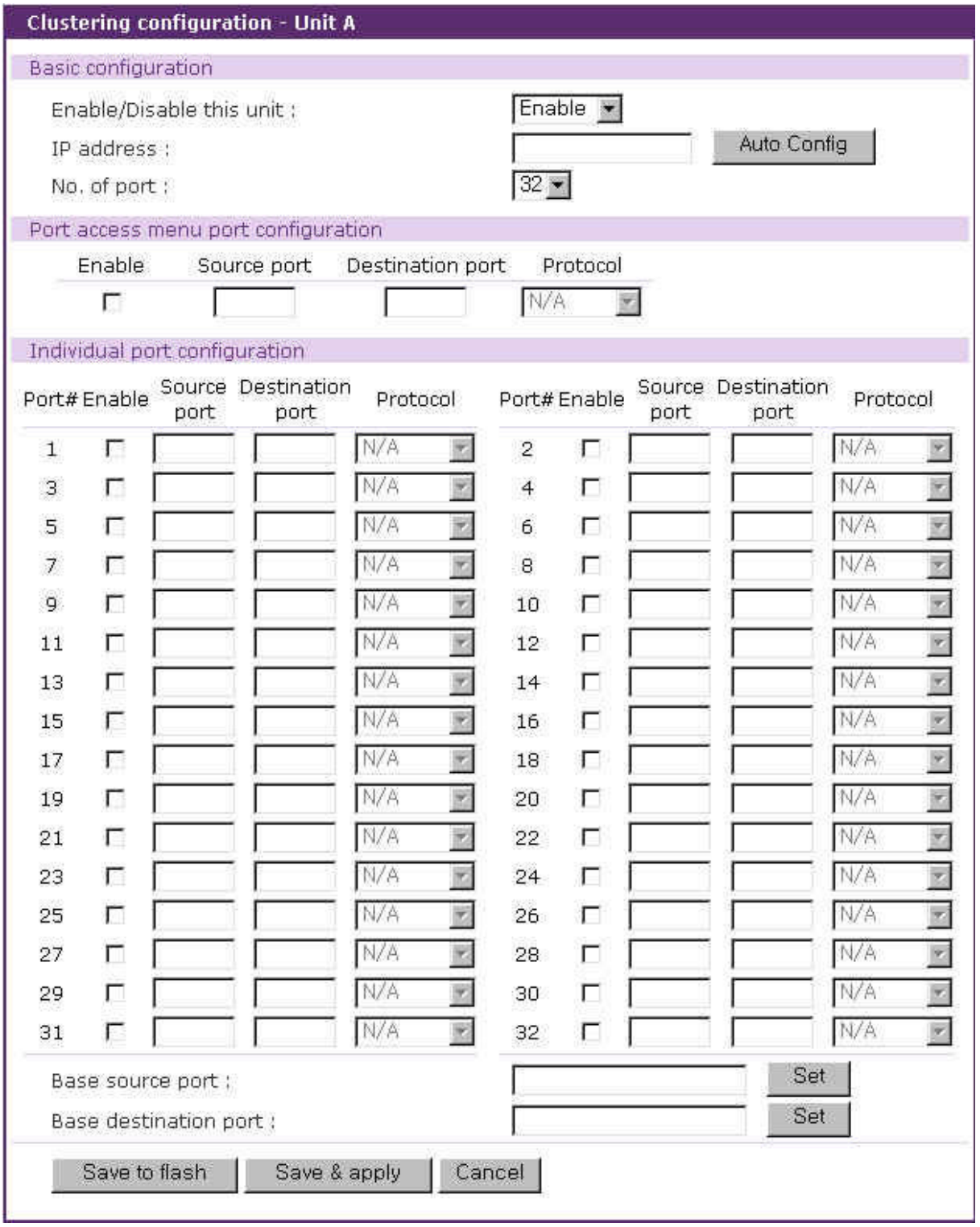
1) From the Web menu, go to 'Clustering and set the clustering mode as "Master" like below.



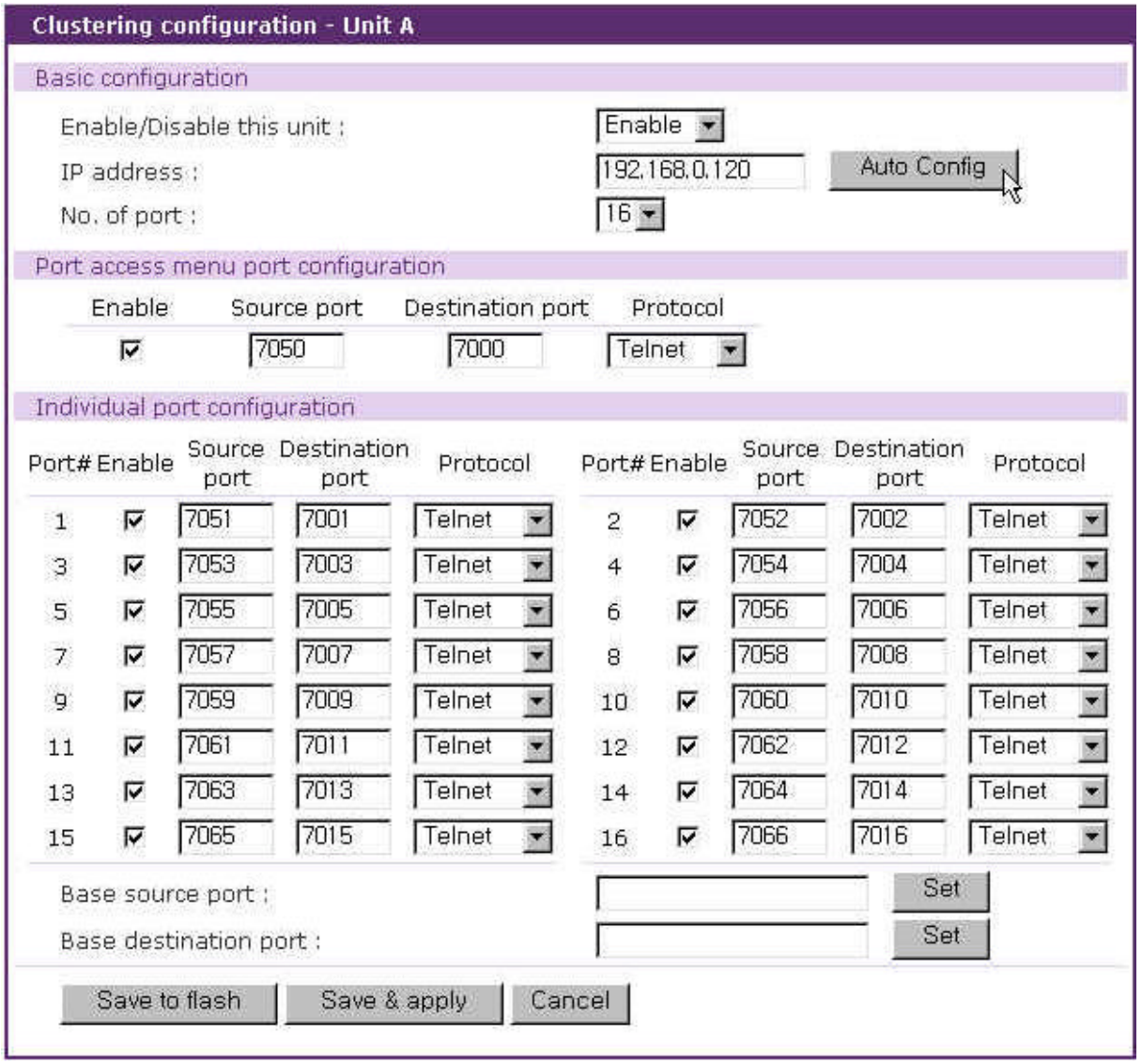
2) After changing clustering mode, you may see the window like below for configuration. Click on the unit and enable the unit.


VTS Series
Management
Network
Serial port
Clustering
Configuration
Connection
PC card
System status & log
System administration
System statistics
Apply changes
Login as a different user
Logout
Reboot
Clustering configuration
Clustering mode configuration
Clustering mode :
Master
Save to flash
Save & apply
Cancel
Clustering information
Unit ID
IP address
No. of port
Unit ID
IP address
No. of port
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Copyright ©2003 Sena Technologies,Inc. All rights reserved
SENA
TECHNOLOGIES

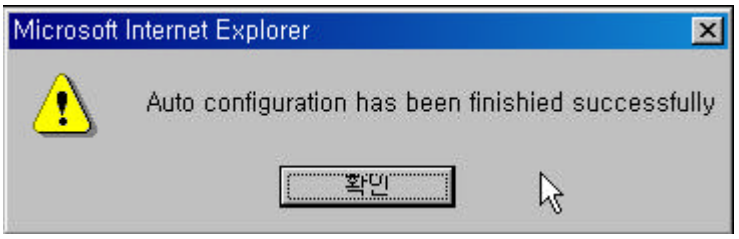

VTS Series
Management
Network
Serial port
Clustering
Configuration
Connection
PC card
System status & log
System administration
System statistics
Apply changes
Login as a different user
Logout
Reboot
Clustering configuration - Unit A
Basic configuration
Enable/Disable this unit :
Disable
Save to flash
Save & apply
Cancel
Copyright ©2003 Sena Technologies,Inc. All rights reserved
SENA
TECHNOLOGIES



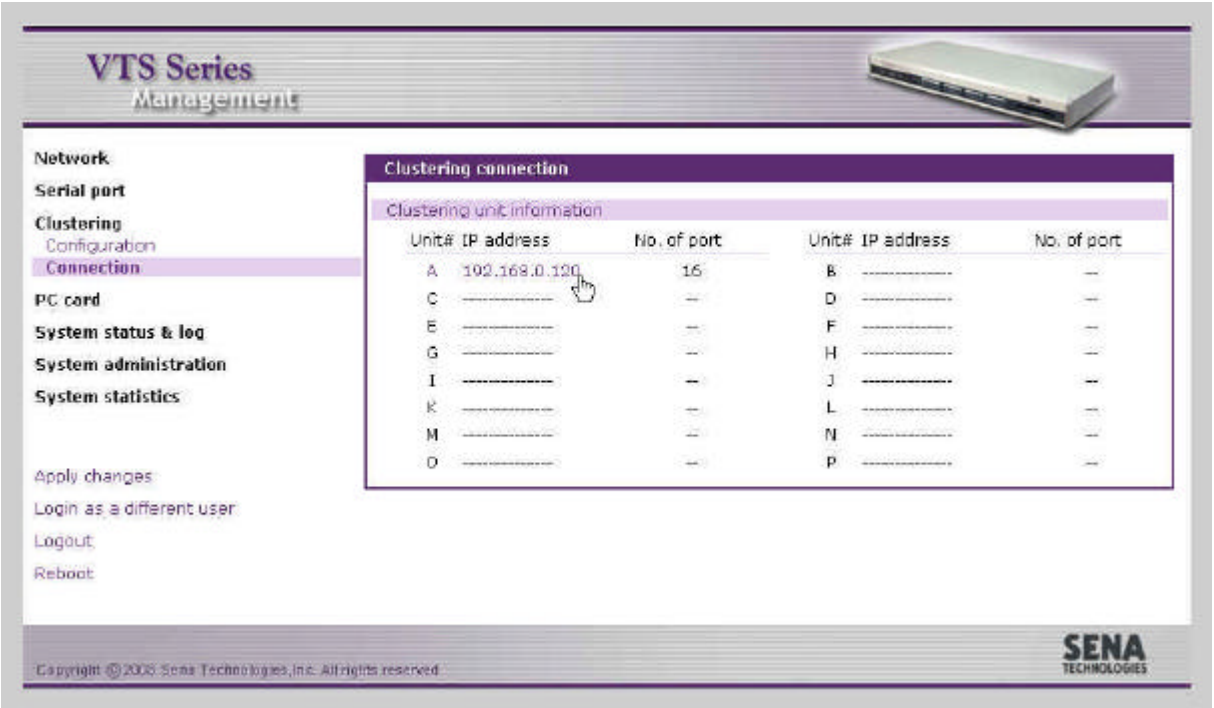
3) Enter the IP address of VTS Slave unit in the IP address field and click "Auto config" button.



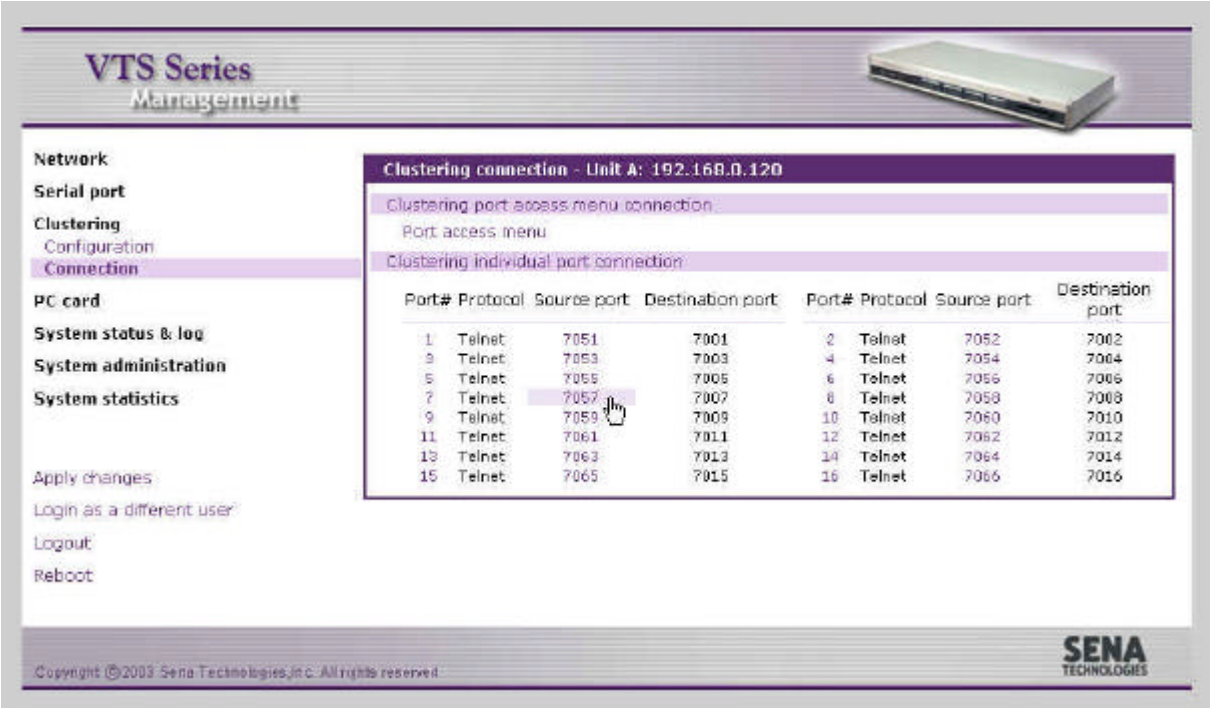
4) If auto configuration finishes successfully, you may see a dialog box like below

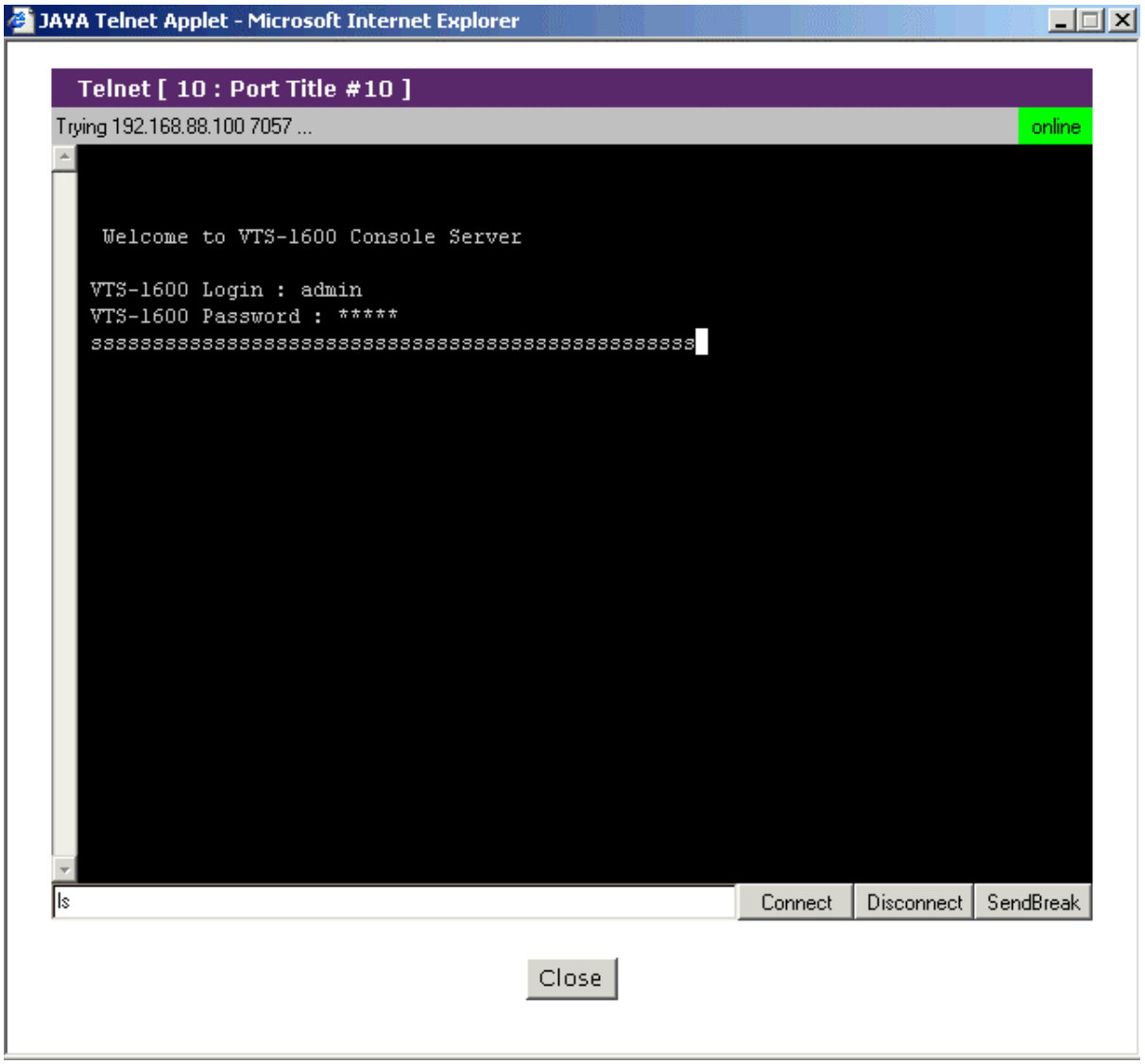


5) User may try to connect to the ports of the slave unit by selecting [Clustering – Connection] menu item on the menu bar.



6) Click on the selected port number to manage your device.





Telnet [10 : Port Title #10]

Trying 192.168.88.100 7057 ...

online

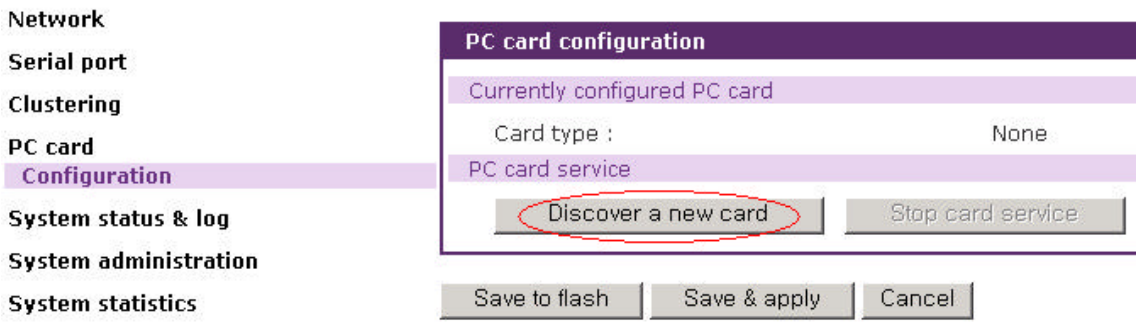
```
 Welcome to VTS-1600 Console Server

VTS-1600 Login : admin
VTS-1600 Password : *****
sssssssssssssssssssssssssssssssssssssssssssssssss
```

ls

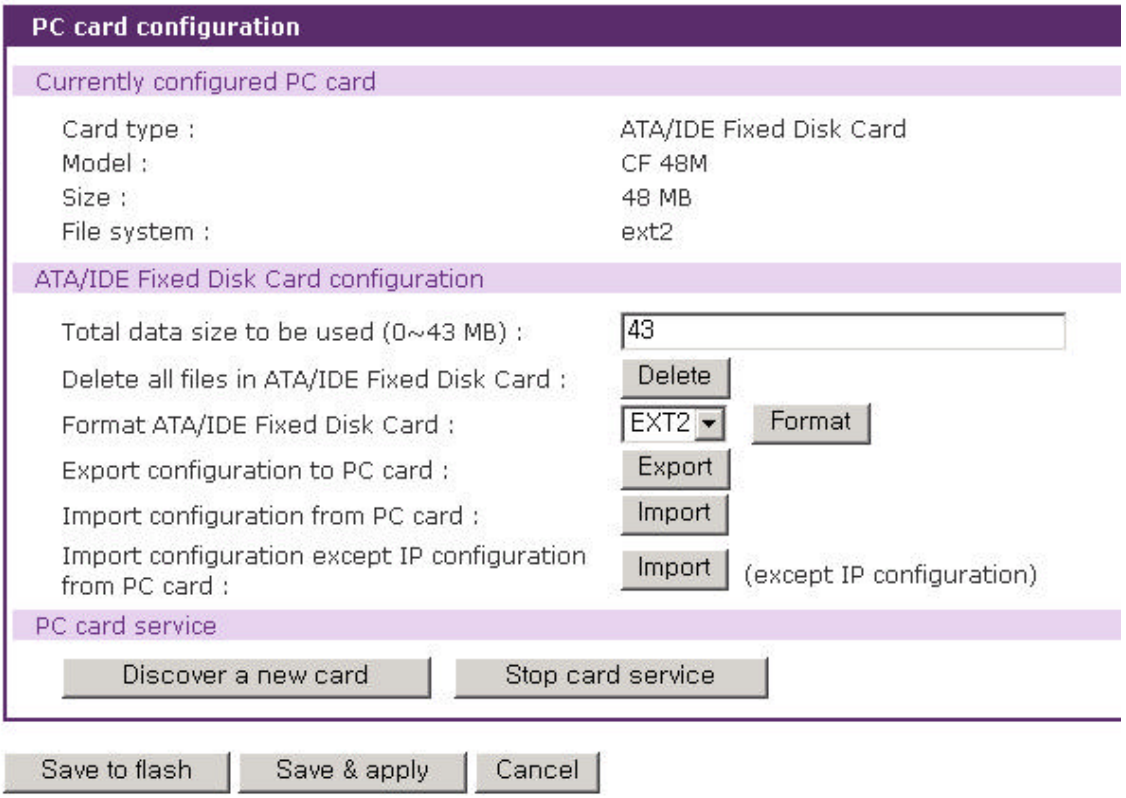
5. Message logging

5.1. How can I use a PCCard as a message storage media?

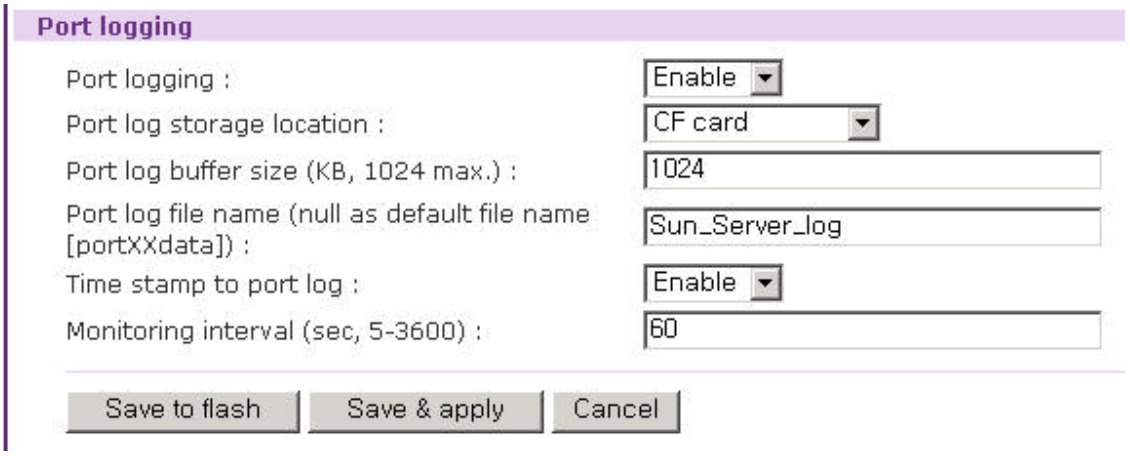
1) Verify that your storage PCCard is on the supported card list. See the reference (1) for the current
2) Insert the PCCard into the PCMCIA slot.
3) Click on the 'Discover a new card button'.



6) If successful, VTS shows you the following information in case of 'Advantech CompactFlash CF48M'.



7) Configure any serial port to use PCCard as a message archive. The following shows how to fill out each item in the 'port logging' pane of serial configuration.



Reference:

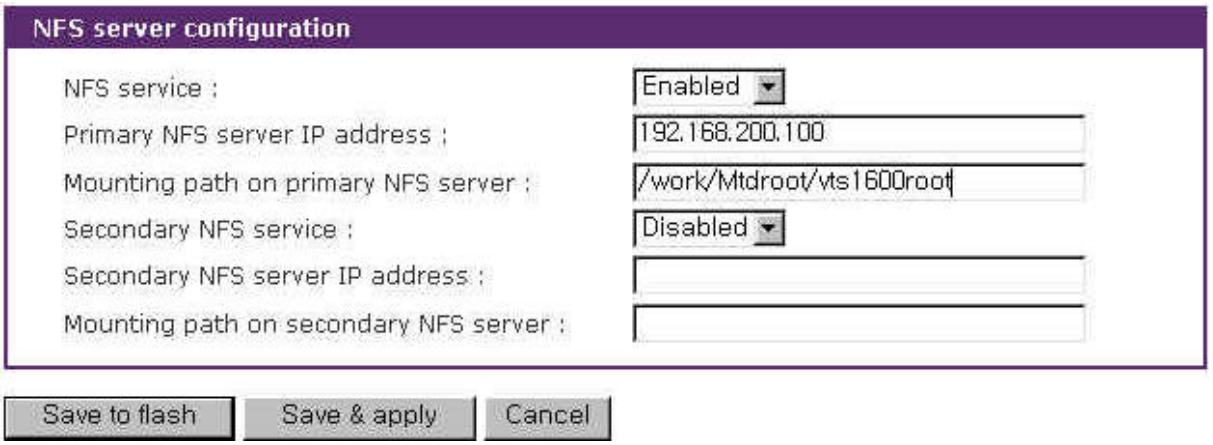
(1) VTS user manual > Appendix B > Table B-3 ATA/IDE Fixed Disk Card

5.2. How can I configure a hard disk to store VTS port logs?

1) You should run a NFS or Syslog server on a hard disk based machine.

8) NFS server setting on VTS

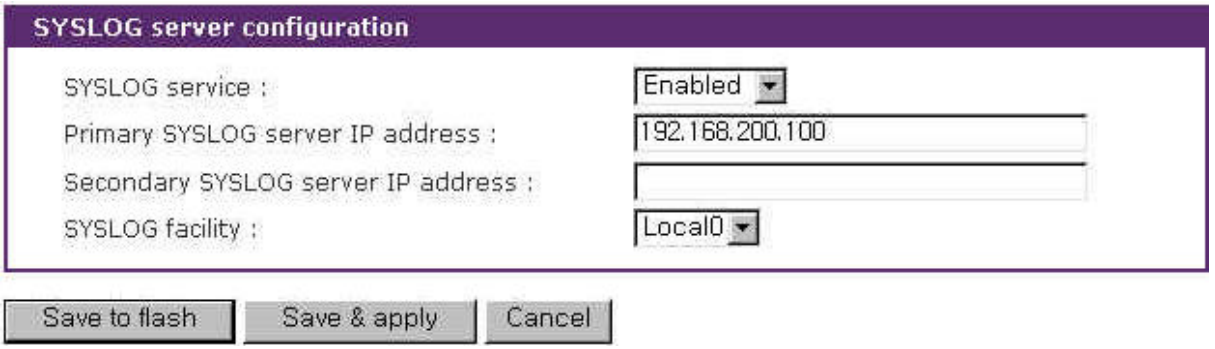
The configuration menu, 'Network > NFS server configuration', will show as the following figure on the Web. The mounting path is a relative path to the mounting root on a NFS server.



Once you fill in the necessary items click on the 'Save & apply' button.

9) SYSLOG server setting on VTS

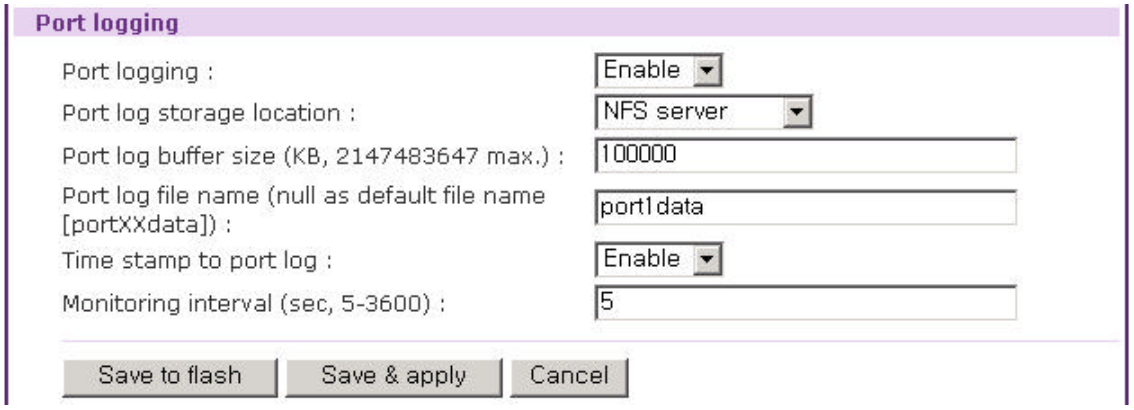
The configuration menu, 'Network > SYSLOG server configuration', will show as the following figure on the Web.



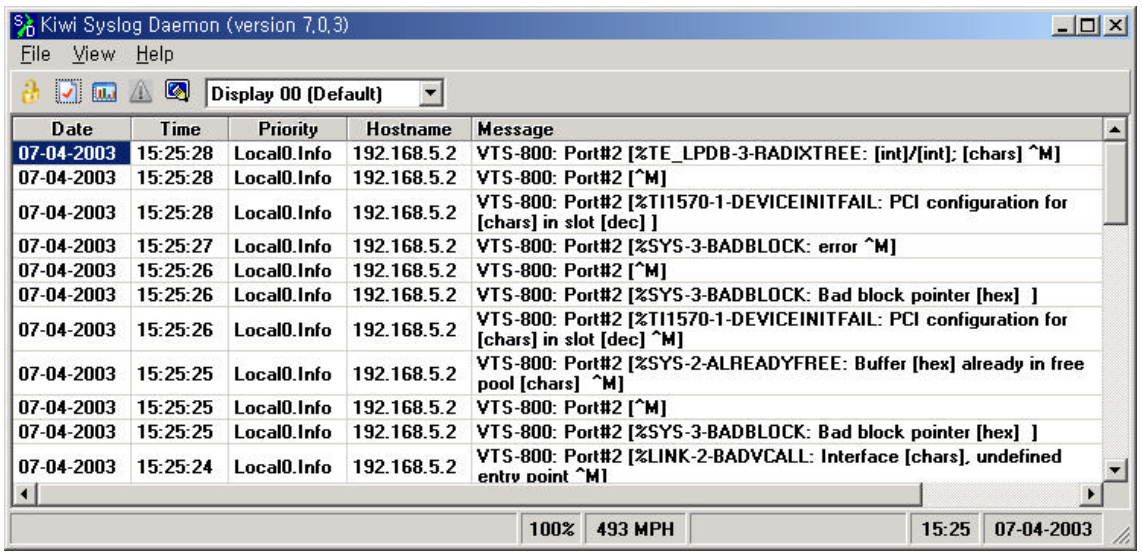
10) Set a serial port to utilize either NFS or SYSLOG server for its message logging.

The Web configuration menu, 'Serial port> Configuration> Port #> Port logging', will show as the following figure.

Select either NFS or SYSLOG server. Click on the 'Save & apply' button.



11) The messages are viewed from SYSLOG server. This screenshot shows Kiwi Syslog Server that saves the messages sent by VTS.



Reference:

(1) VTS user manual > 3.6 SYSLOG server configuration

(2) VTS user manual > 3.7 NFS server configuration

(3) VTS user manual > 4.3.6 Port Logging

5.3. How can I view the port logged messages?

1) All the messages logged in the memory, NFS sever and PCCard are viewed from the edit box on the Web menu, 'Serial port> Configuration> Port #> Port logging'. The time stamp is added as a heading to each message if you enabled the time stamping from the Web menu, 'Serial port> Configuration> Port #> Port logging> Time stamp to port log'.

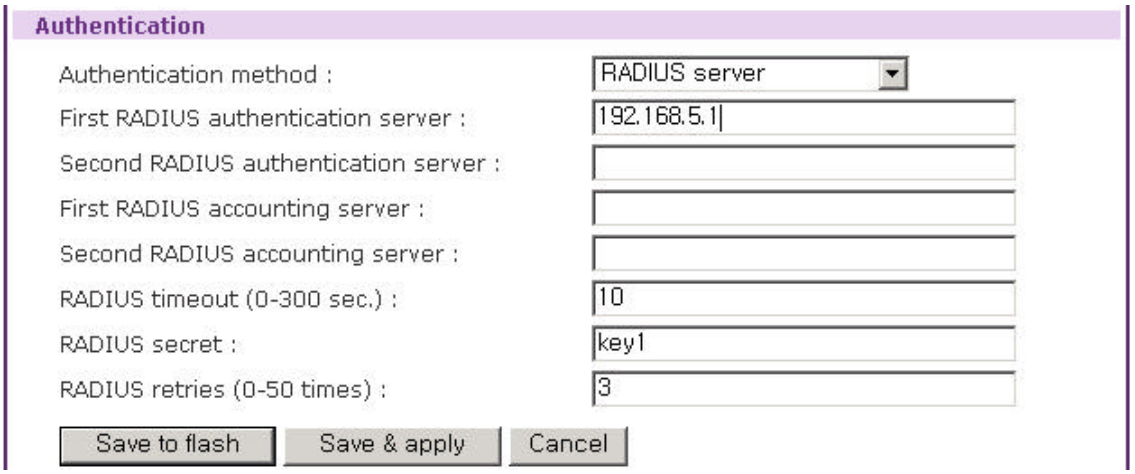
12) The logs in a SYSLOG server are viewed from the port log edit box but it shows recent messages. All the messages can be checked from the SYSLOG server.

6. Authentication

6.1. How can I use an authentication server like RADIUS?

Authentication methods to the serial ports are configured per port basis.

1) From the Web configuration menu, 'Serial port> Configuration> Authentication', choose 'RADIUS server'. Fill in the IP of the RADIUS server and other properties. The 'RADIUS secret' is the property set in the RADIUS server. Click on the 'Save & apply' button.



13) If you chose 'RADIUS server and Local' as the authentication method, an ID and password will be routed to the RADIUS server first. If the server's database doesn't have a match for the request, then the ID and password is tried against the VTS' ID and password database.

Reference:

(1) VTS user manual > 4.3.9 Authentication configuration

7. Port event notification

7.1. How to enable 'Port Event Handling' feature

VTS Serial ports can be configured for system alerts and notifications. It sends email messages when a certain value or when an alarm message is detected in the serial port data. VTS uses SMTP (Simple Mail Transfer Protocol) for sending the email notifications, and supports SNMP (Simple Network Management Protocol), for SNMP traps.

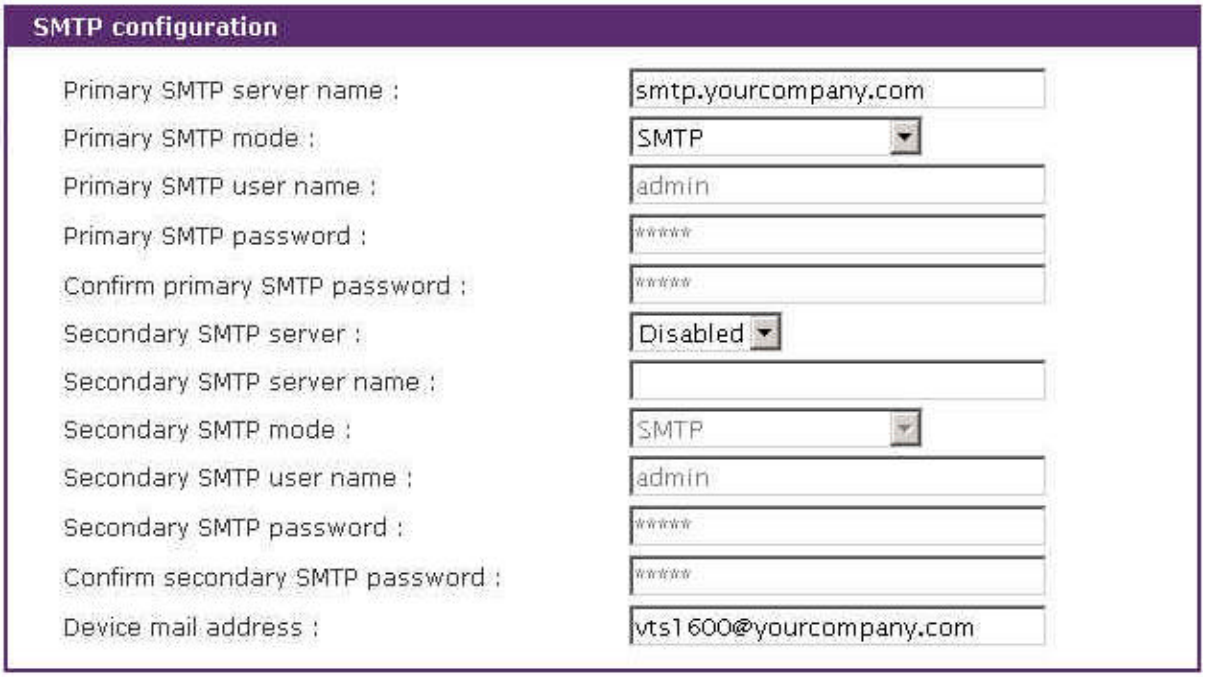


Figure 7.1 SMTP configuration parameters

To use SMTP for Port log emailing, administrator must configure a valid SMTP server for sending the emails. For SNMP traps, administrator will have to configure SNMP parameters at 'Network configuration' heading.

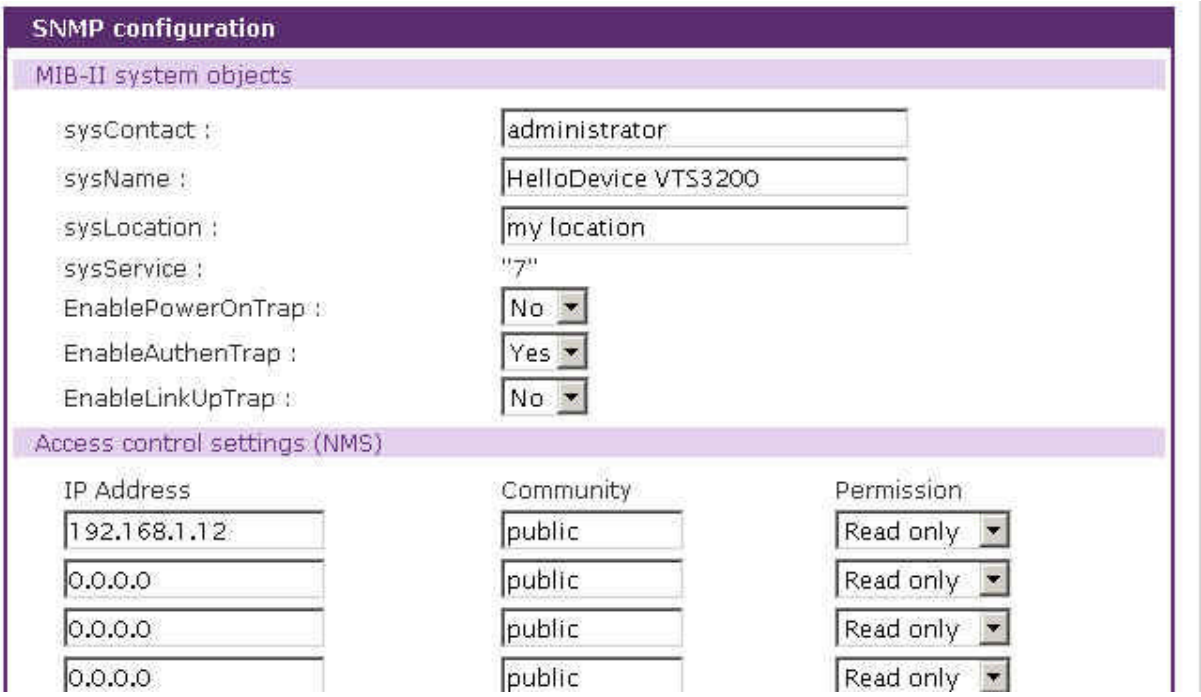


Figure 7.2 SNMP configuration parameters

To use the 'Port Event Handling' feature, user will have to enable the port logging at Serial port configuration window. With 'Port Event Handling' feature, the user can let the VTS to search a defined keyword from the port logging data and send an email or SNMP trap to an administrator by Port event handling configurations. Each reaction can be configured individually upon each keyword. Reaction can be an email delivery, SNMP trap sending or both.

Below steps describe how to enable port event handling feature.

1) Access the VTS web interface.

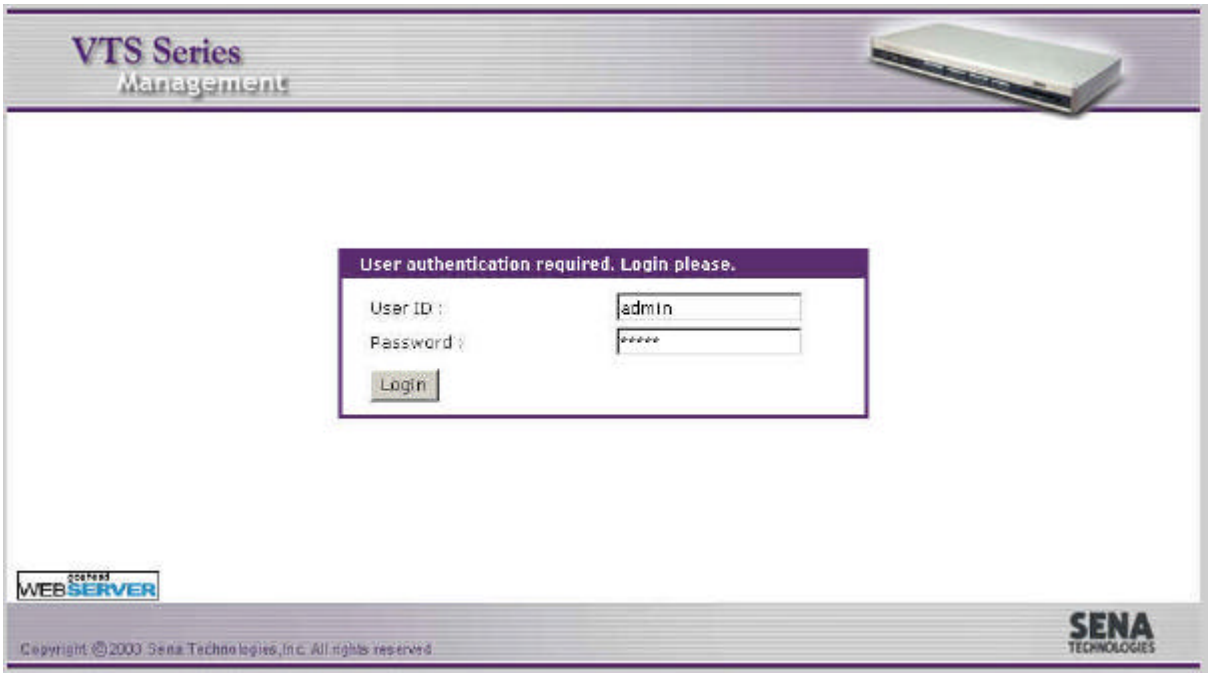


Figure 7.3 Access the VTS web interface

14) Choose Serial port --> Configuration.

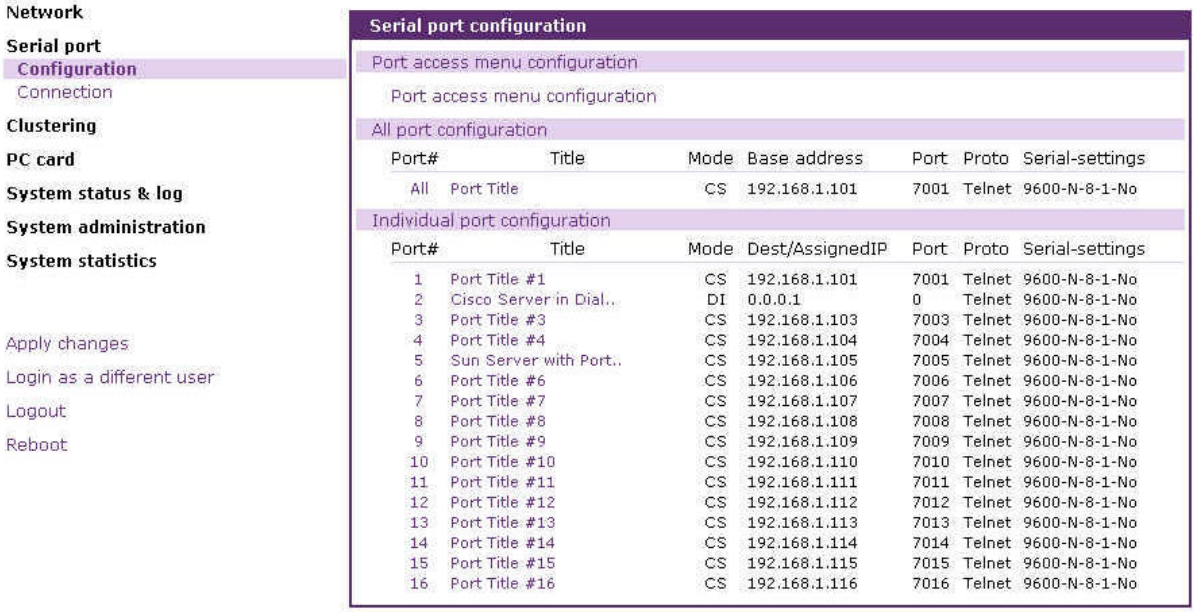


Figure 7.4 Choose Serial port configuration

15) Choose a port to configure and then Port logging.

16) Use the Port-logging page to enable logging.

17) Choose Save & apply.

18) Choose Port event handling.

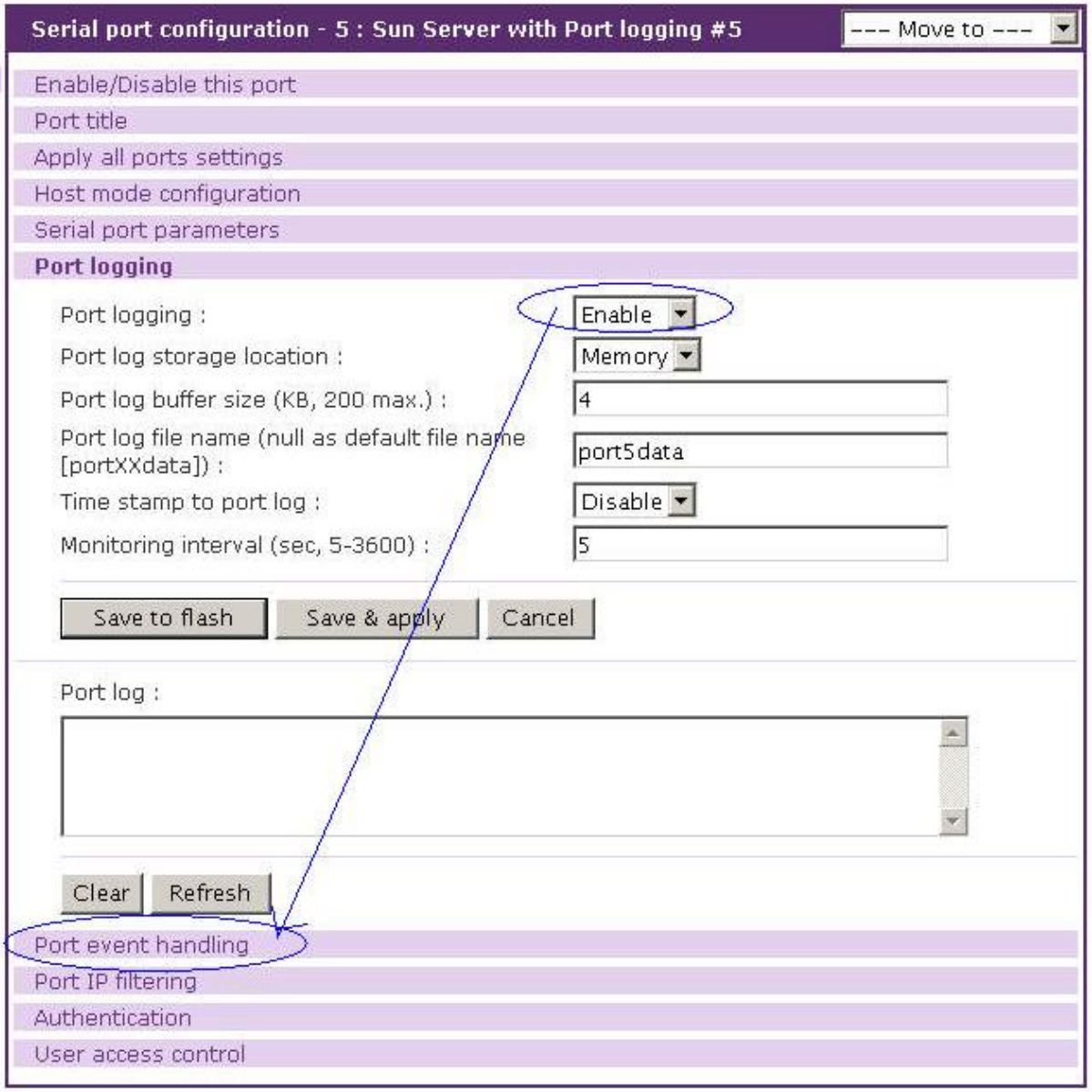


Figure 7.5 Enabling Port logging feature for Port event handling

7.2. How to configure 'Port Event Handling' email notification

7.2.1. Configuration

VTS Serial ports can be configured for system alerts and notifications. It sends email messages when a certain value or when an alarm message is detected in the serial port data. To receive email notification from VTS, user needs to configure SMTP parameters like below.

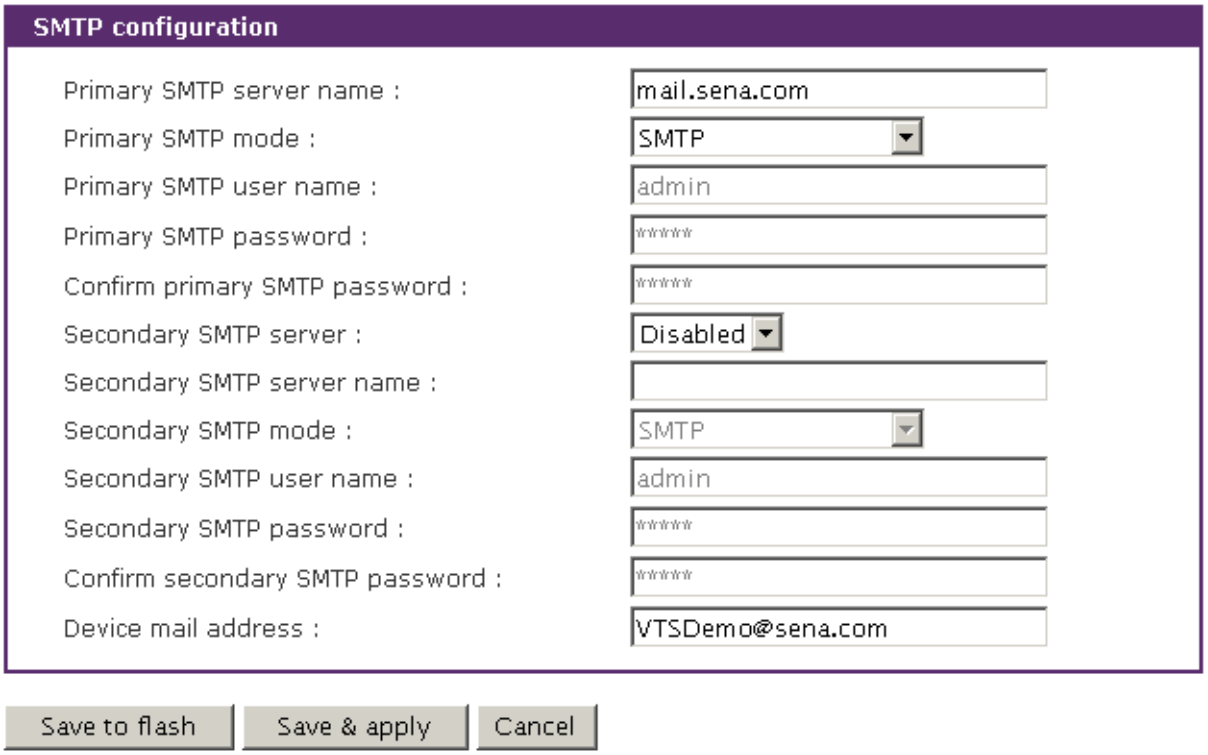


Figure 7.6 SMTP configuration parameters

To receive an email messages when an alarm message is detected in the serial port data, user needs to add 'keywords' in 'Port Event Handling' page. Each reaction (Email/SNMP) can be configured individually upon each keyword.

Below steps describe how to configure email notification for port event handling.

1) Access the web interface.

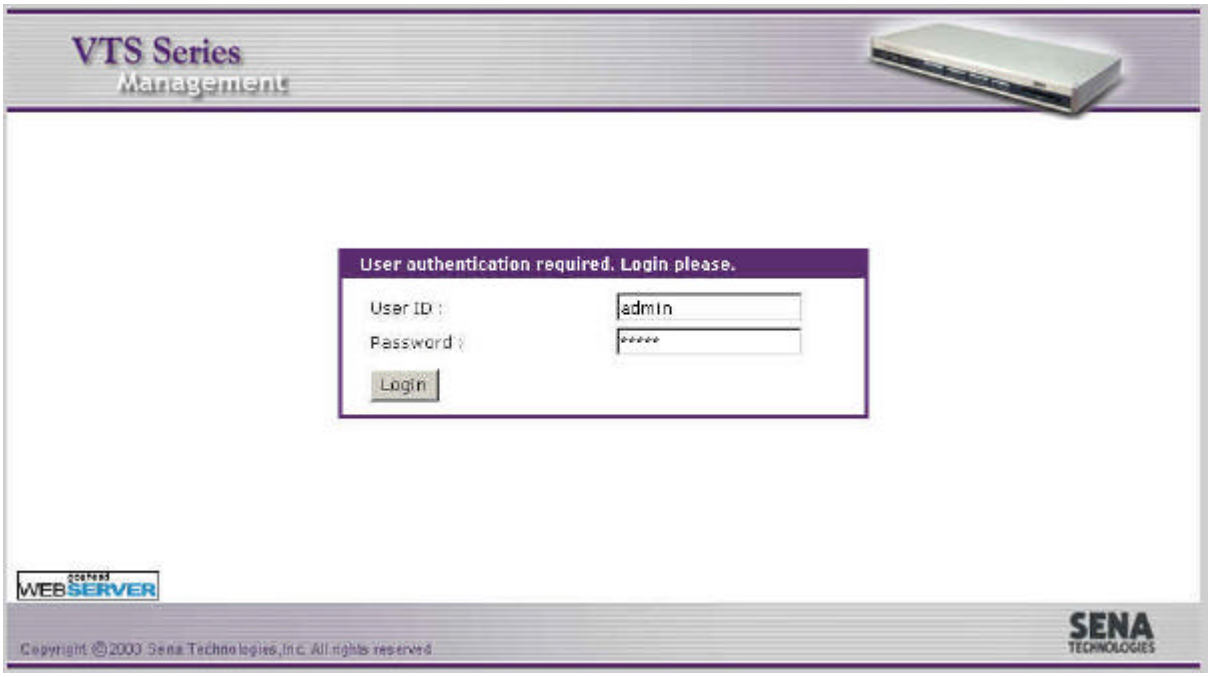


Figure 7.7 Access the VTS web interface

19) Choose Serial port > Configuration.

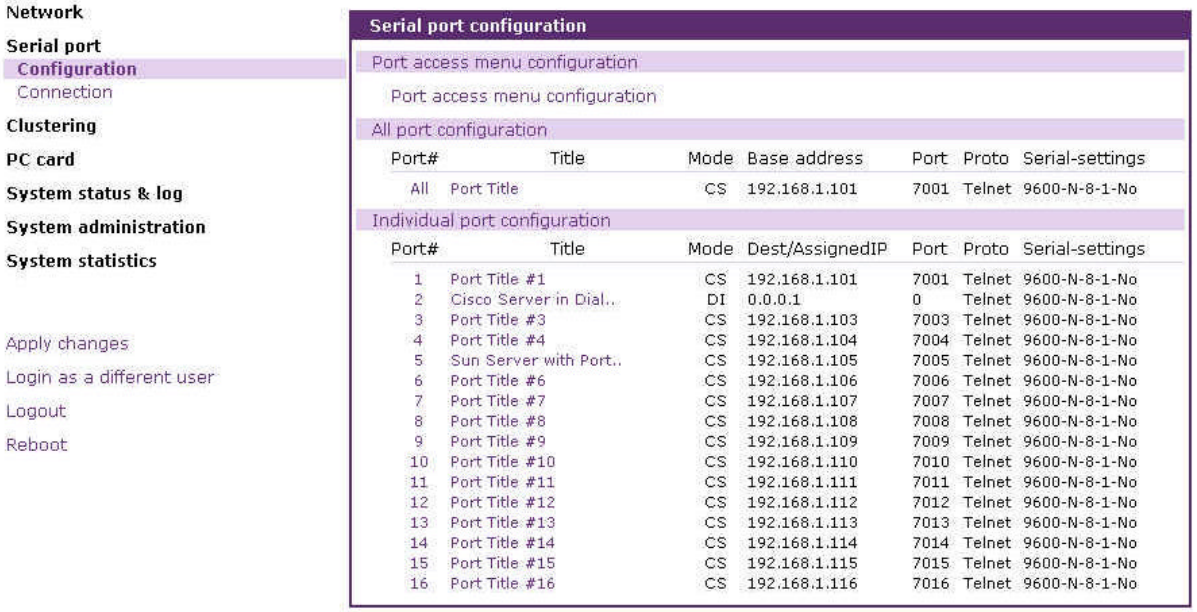


Figure 7.8 Choose Serial port > Configuration

20) Choose a port to configure and then Port logging.

21) Use the Port-logging page to enable logging, and Save & apply

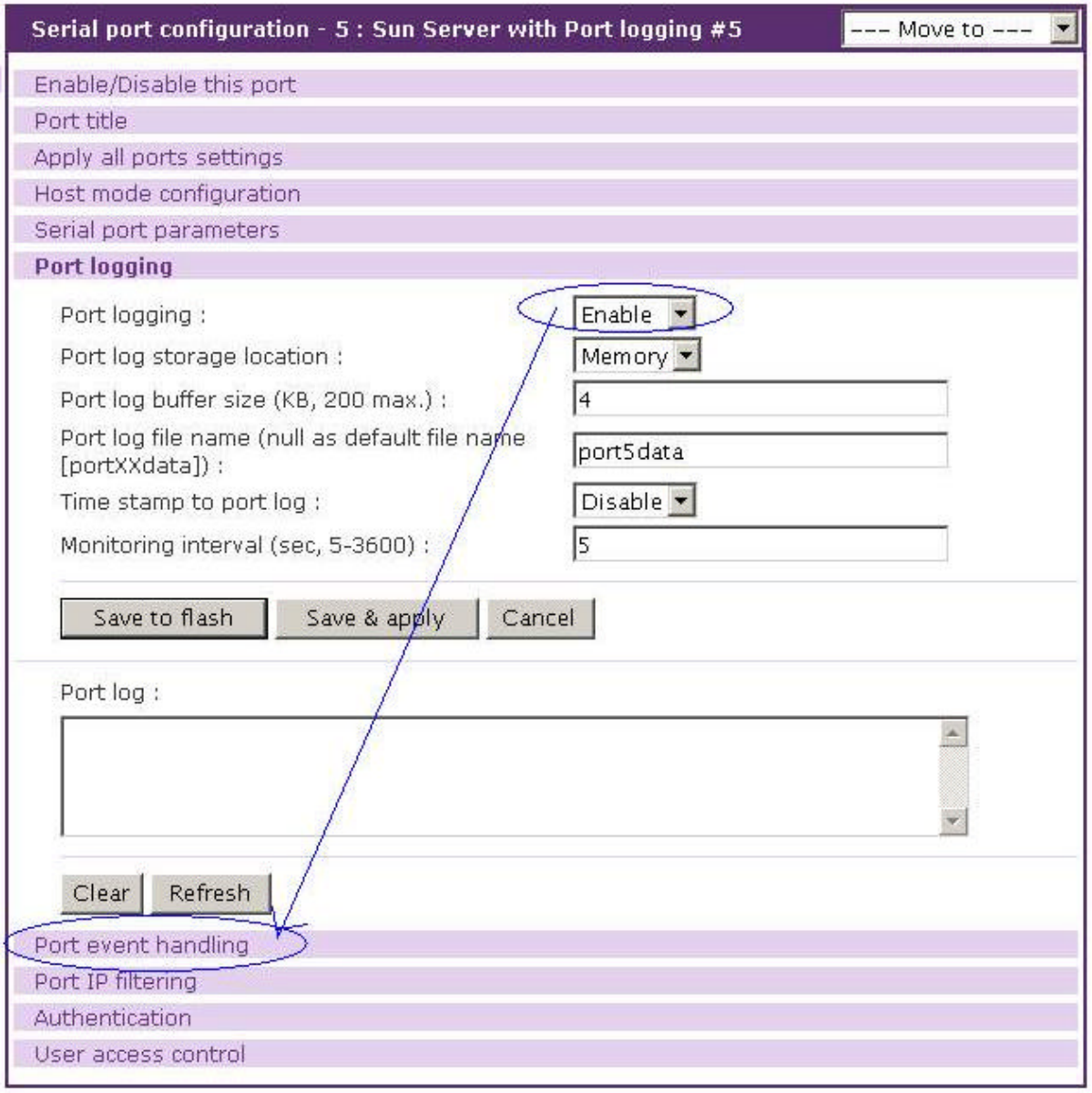


Figure 7.9 Choose Serial port > Configuration

22) Choose Port event handling and fill the email.

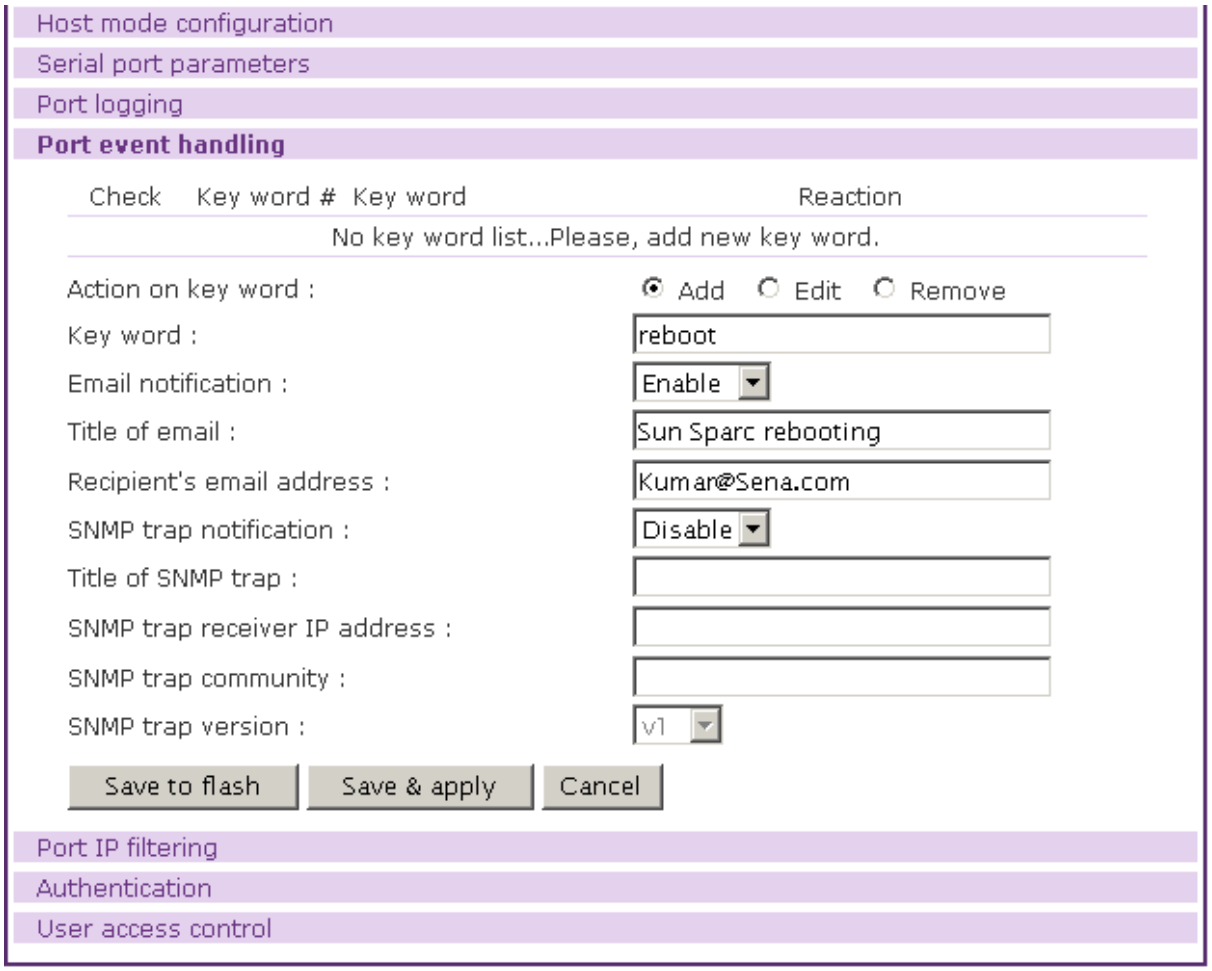


Figure 7.10 Choose Port event handling and fill the email

23) To add more than one email recipient (multiple email recipients), please separate email addresses with a comma (,) like below.

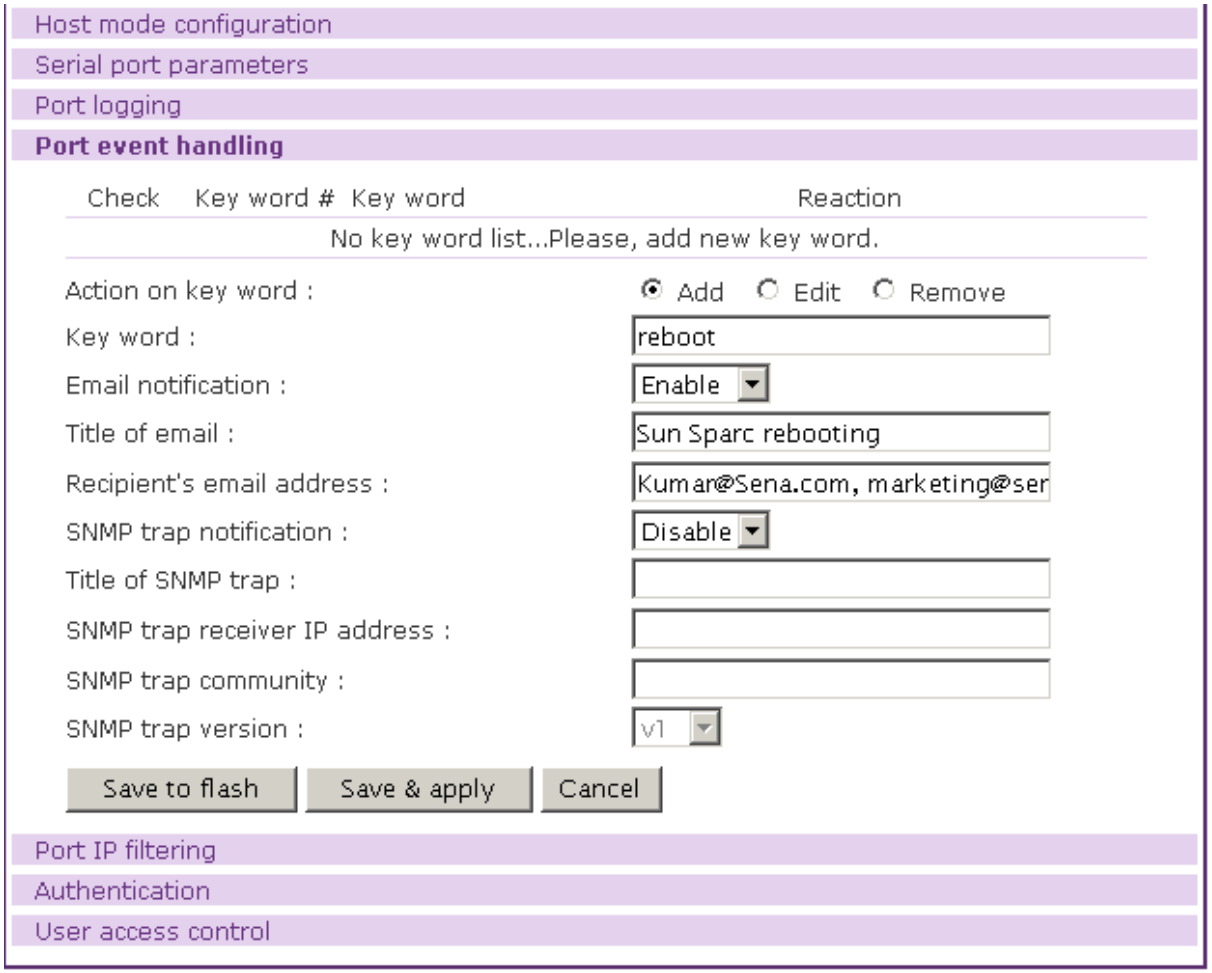


Figure 7.11 Add multiple email recipients

7.2.2. Email notification, if the specified keyword is detected:

Recipients will receive the email notification as soon as the specified keyword is detected at device. For example., recipient will receive the email notification like

below, as soon as the keyword 'reboot' is detected in device.

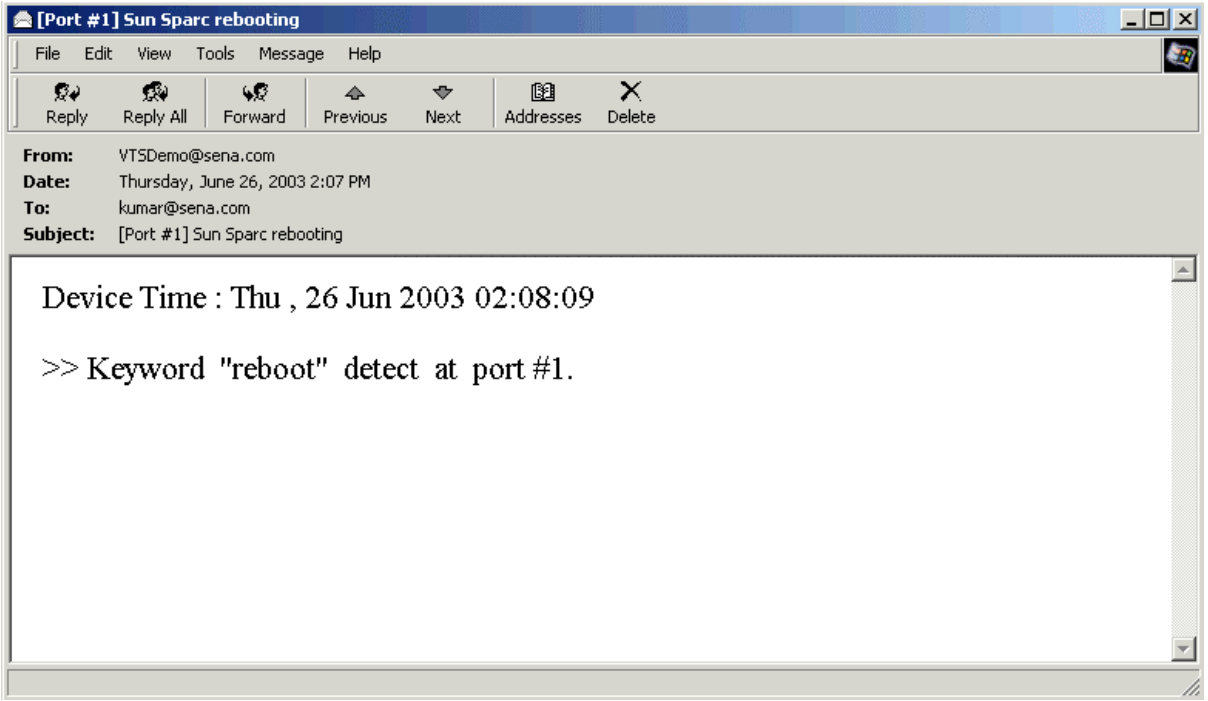


Figure 7.12 Email notification, if VTS detects specified keyword

7.3. How to configure SNMP Trap notification in 'Port Event Handling'

7.3.1. Configuration

VTS Serial ports can be configured for system alerts and notifications. It sends SNMP trap notification when a certain value or when an alarm message is detected in the serial port data. To receive SNMP trap notification from VTS, user needs to configure SNMP parameters like below.

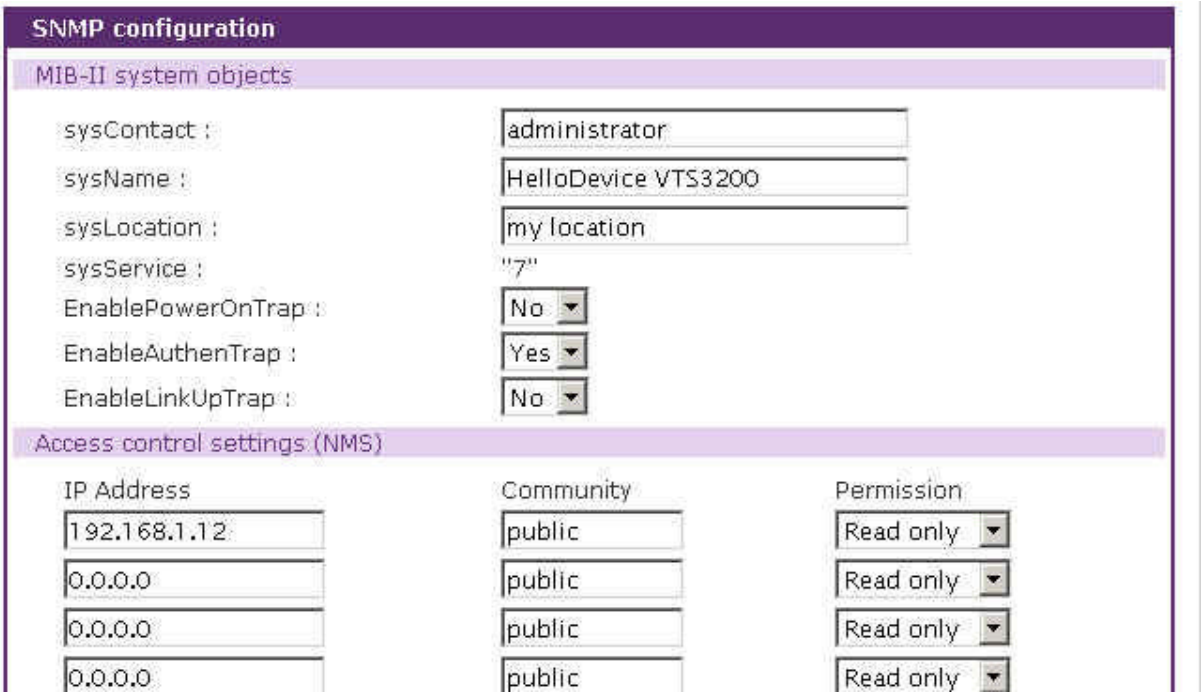


Figure 7.13 SNMP configuration parameters

To receive a SNMP trap notification when an alarm message is detected in the serial port data, user needs to add 'keywords' in 'Port Event Handling' page. Each reaction (Email/SNMP) can be configured individually upon each keyword.

Below steps describe how to configure SNMP trap notification under port event handling.

1) Access the web interface.

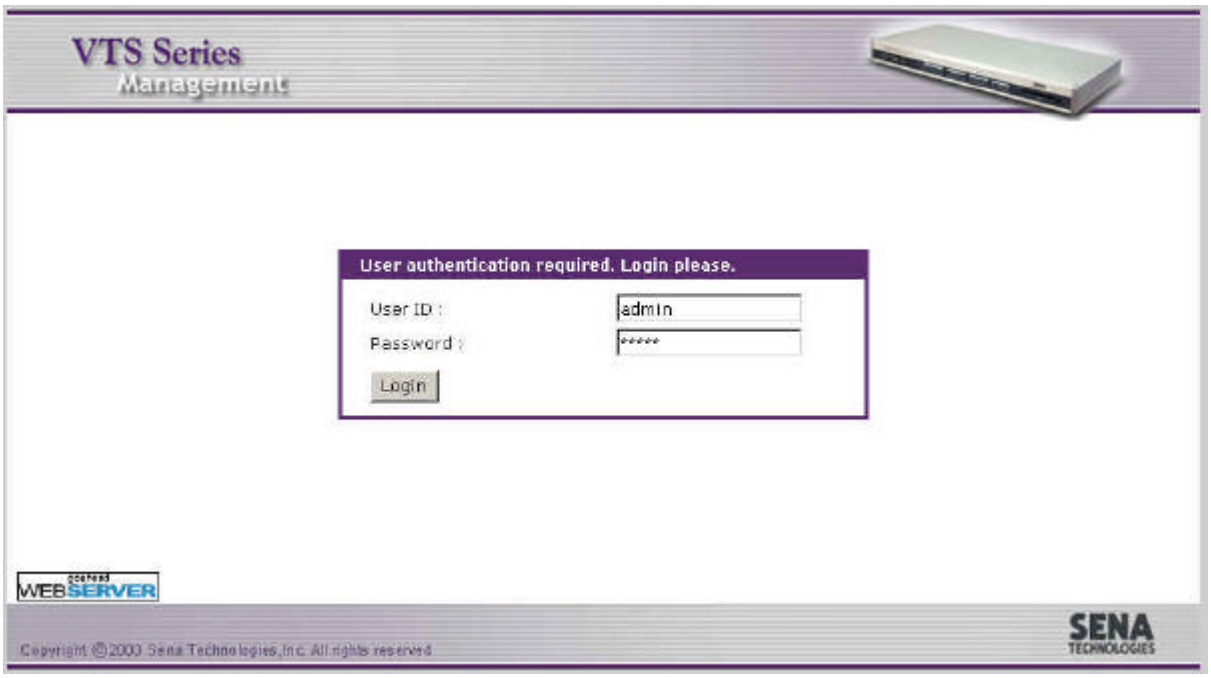


Figure 7.14 Access the web interface

24) Choose Serial port > Configuration.

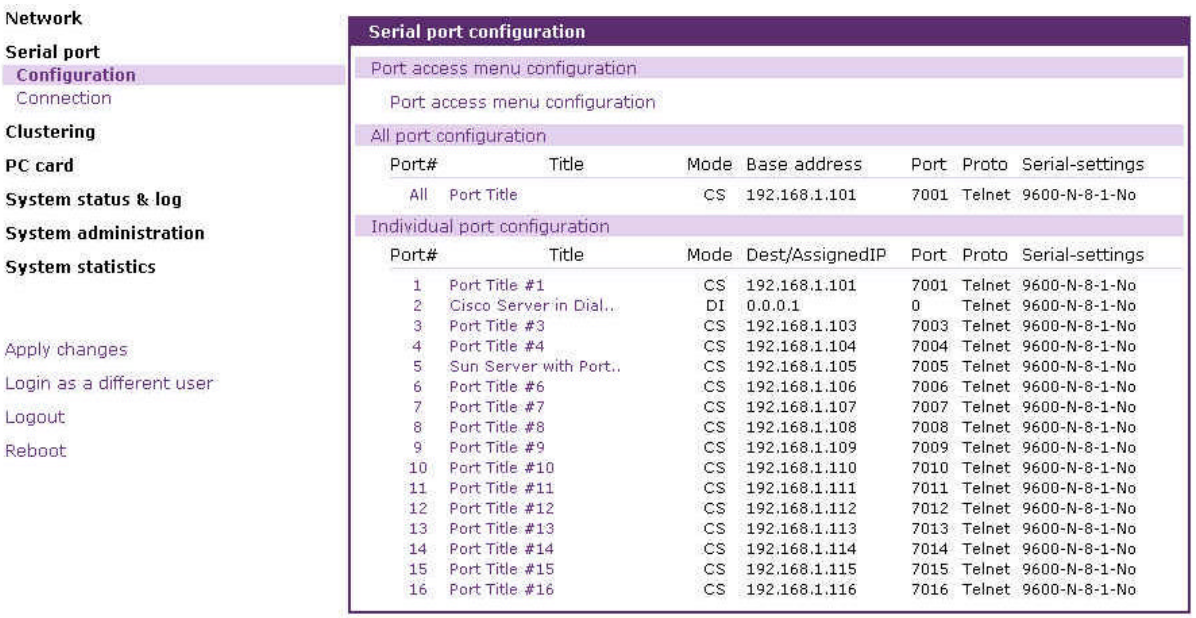


Figure 7.15 SNMP configuration parameters

25) Choose a port to configure and then Port logging.

26) Use the Port-logging page to enable logging, and Save & apply

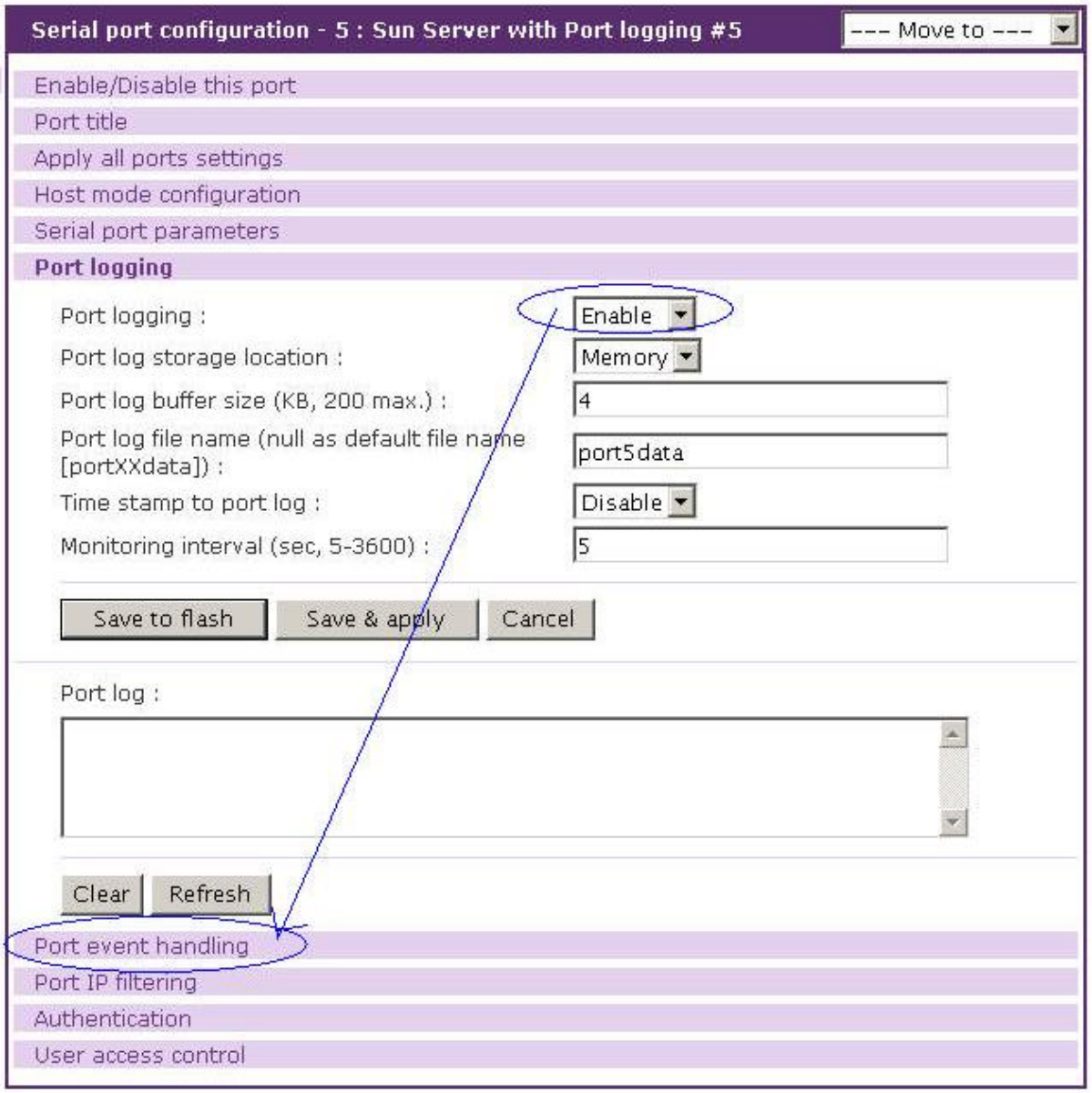


Figure 4.1 Use the Port-logging page to enable logging

27) Choose Port event handling and fill the SNMP parameters like below.

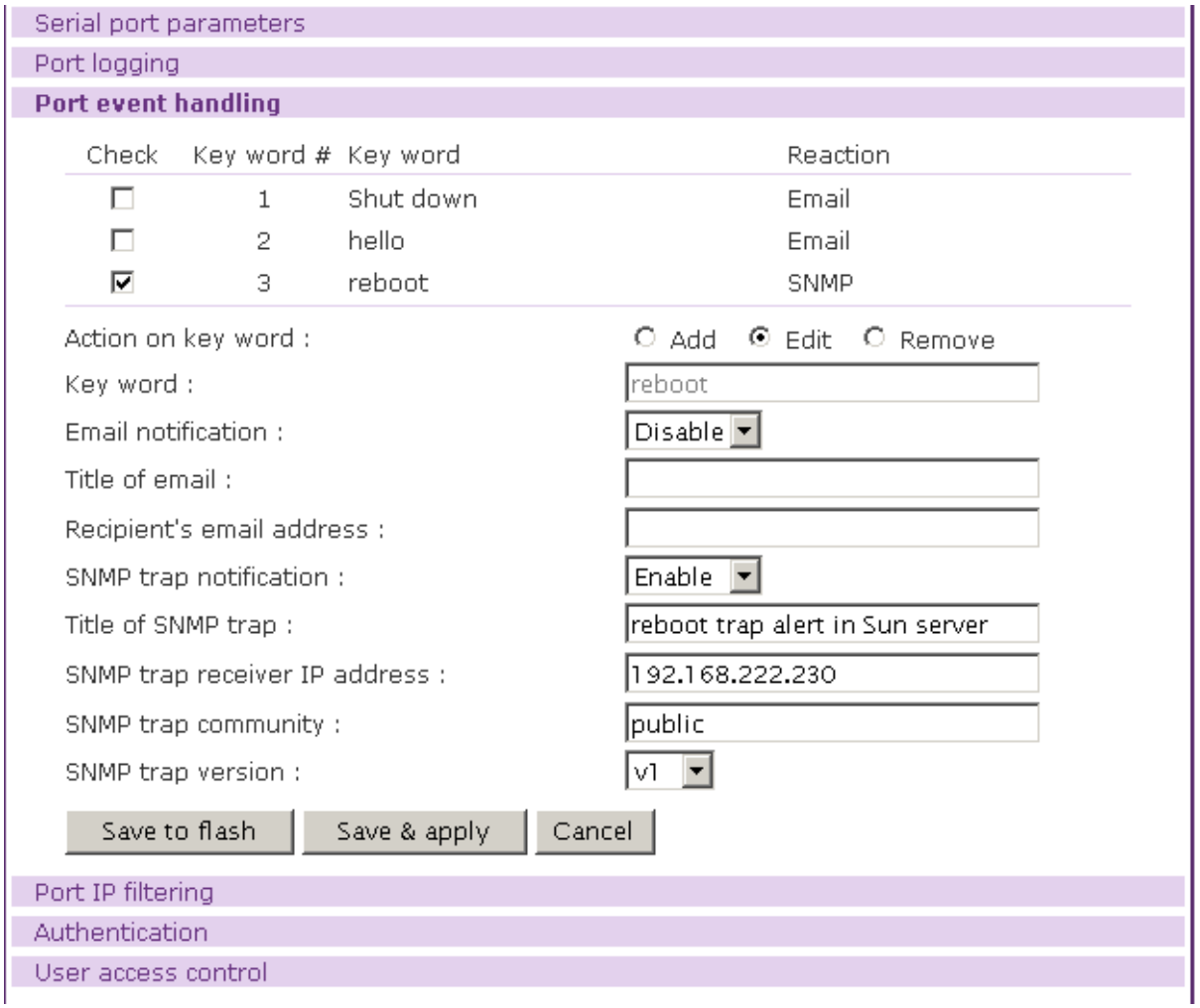


Figure 7.16 Choose Port event handling and fill the SNMP parameters

28) "SNMP trap receiver IP address" should be accurate to receive SNMP alarm.

29) To add more than one keyword, use "Add" radio button like below.

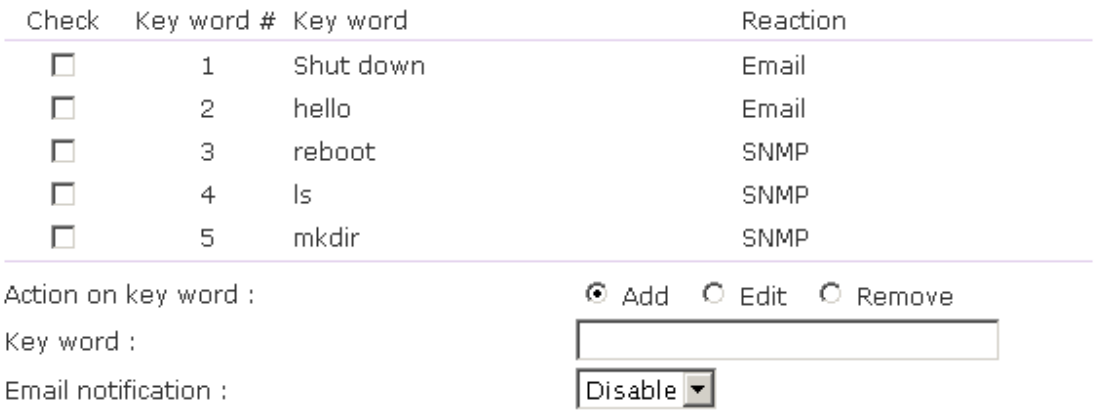


Figure 7.17 To add more than one keyword, use “Add” radio button like below

7.3.2. SNMP trap notification in Kiwi SYSLOG server

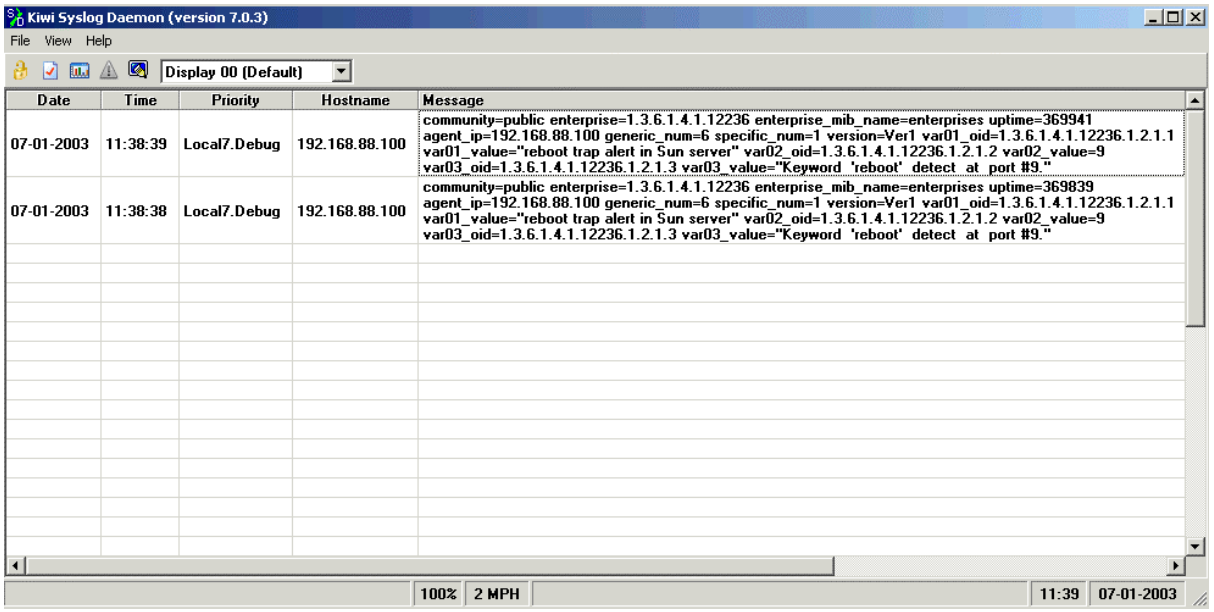


Figure 4.2 SNMP trap notification in Kiwi SYSLOG server

7.3.3. SNMP trap notification in HP Openview NMS software

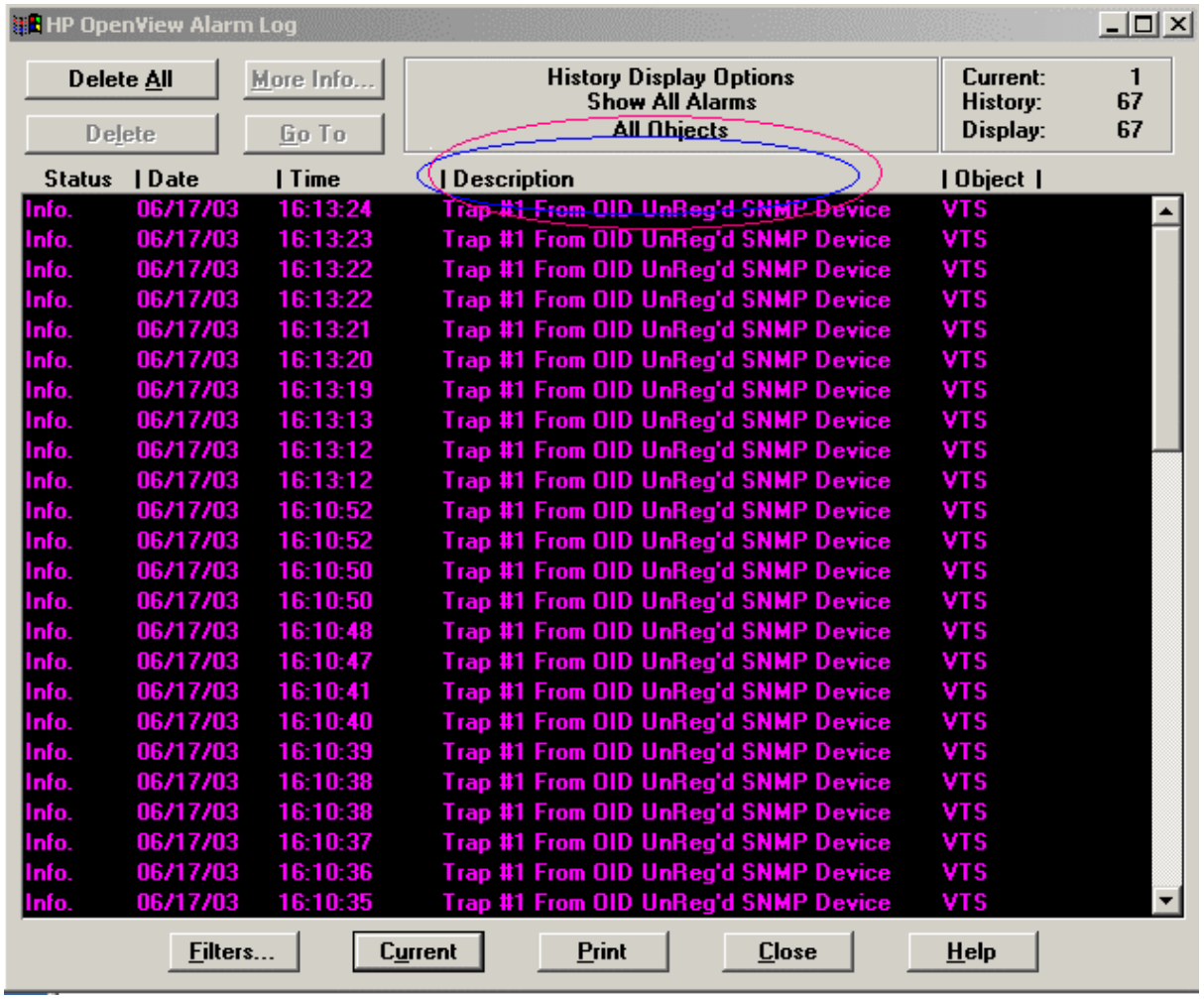


Figure 7.18 SNMP trap notification in HP Openview NMS software

7.4. How can I get notified of important event

There are two ways of notifying users about the alarm message, which is detected from the serial port data.

Email alarm notification

SNMP trap notification

7.4.1. Email alarm notification

Below is the typical setting to receive Email alarm Notification with the keyword "reboot" (sample keyword). As soon as "reboot" is detected in the serial port, which is connected to serial device, VTS will send email alarm to administrator

(recipient) using SMTP and based on SMTP configuration.

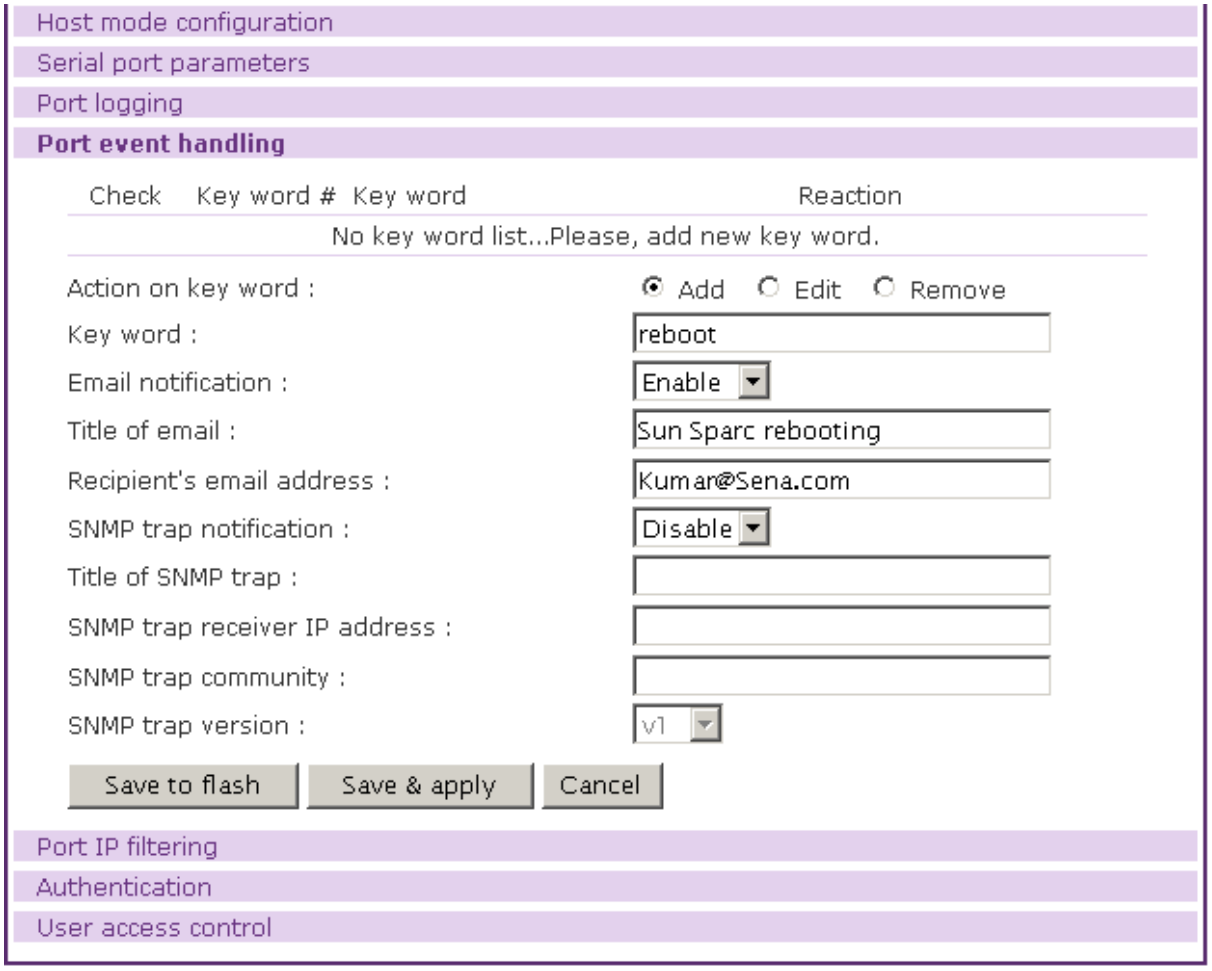


Figure 7.19 Typical setting to receive Email alarm Notification

7.4.2. SNMP trap notification

Below is the typical setting to receive SNMP trap Notification with the keyword "reboot" (sample keyword). As soon as "reboot" is detected in the serial port, which is connected to serial device, VTS will send SNMP trap Notification to administrator using SNMP and according to SNMP settings.

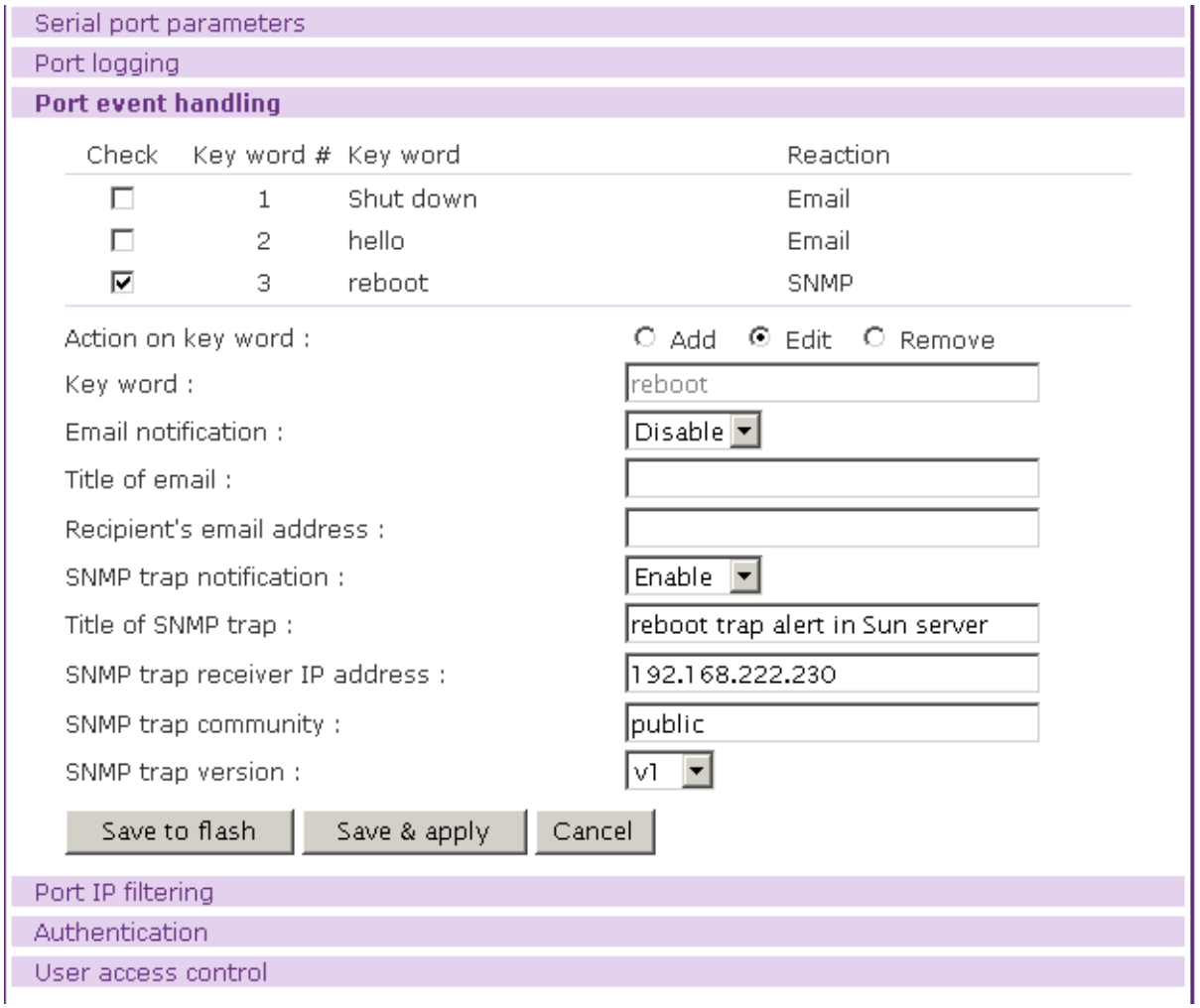


Figure 7.20 Typical setting to receive SNMP Trap Notification

7.4.3. Email notification preview

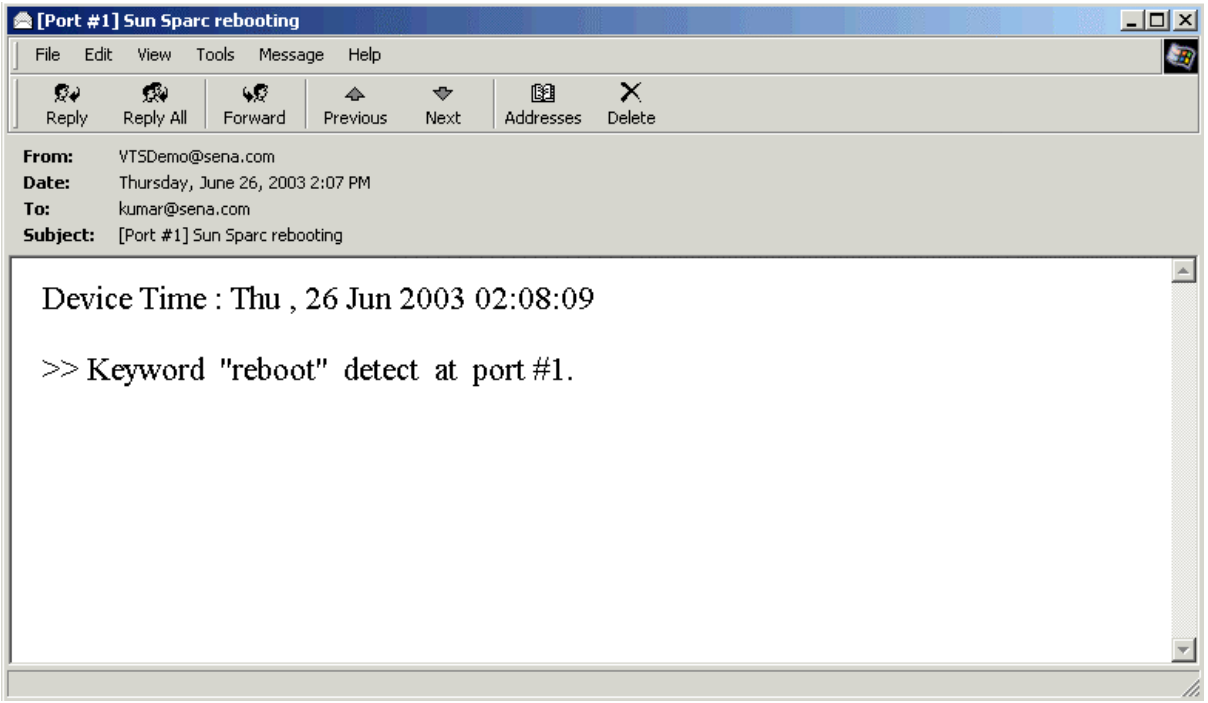


Figure 7.21 Email notification, if VTS detects specified keyword

7.4.4. SNMP trap notification in Kiwi SYSLOG server

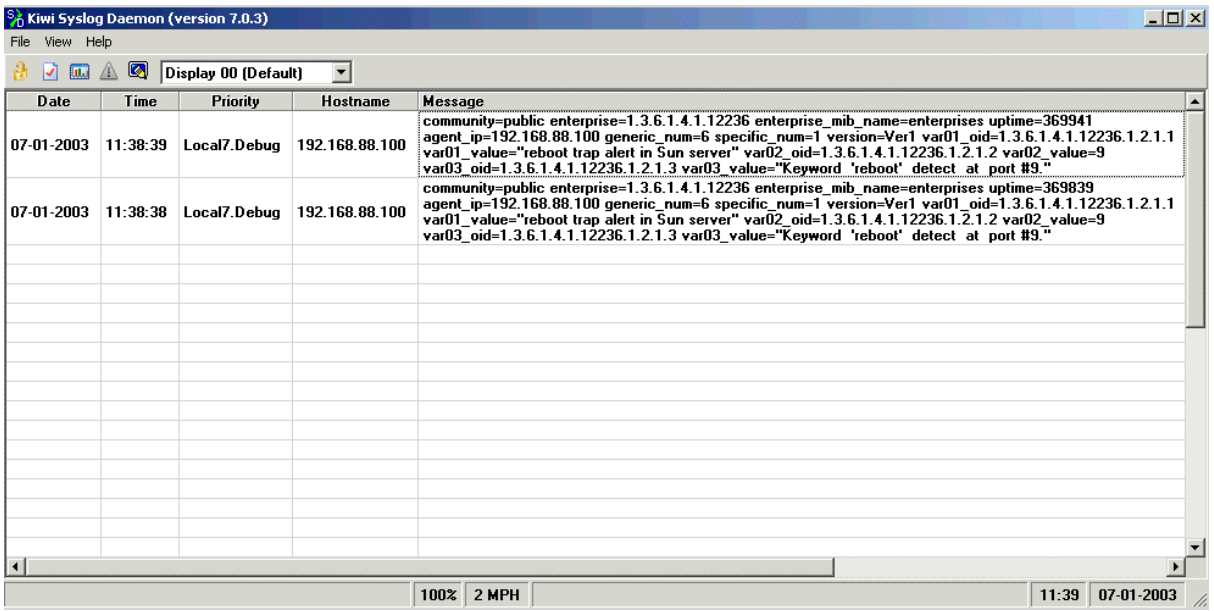


Figure 7.22 SNMP trap notification in Kiwi SYSLOG server

7.4.5. SNMP trap notification in HP Openview NMS software

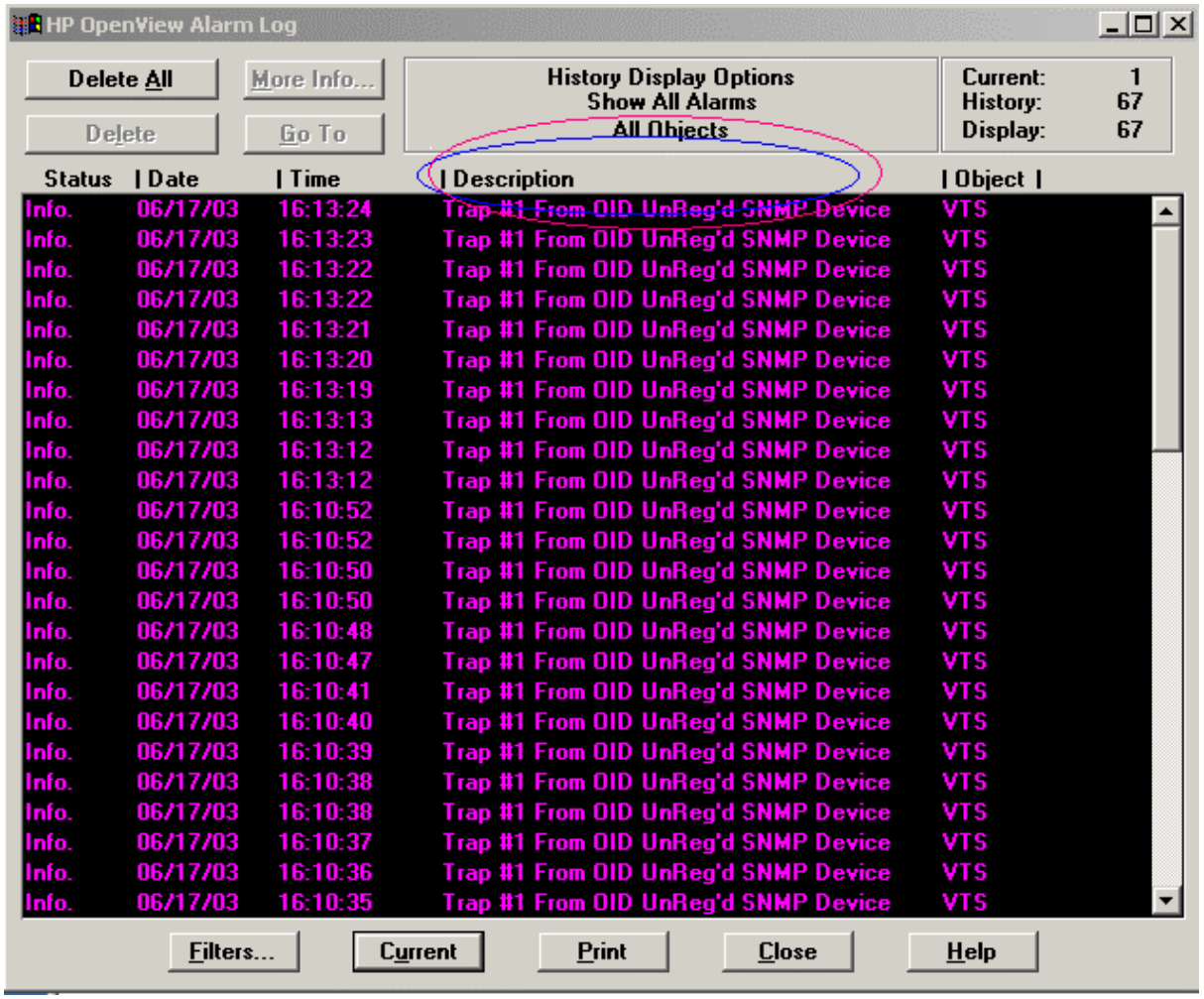


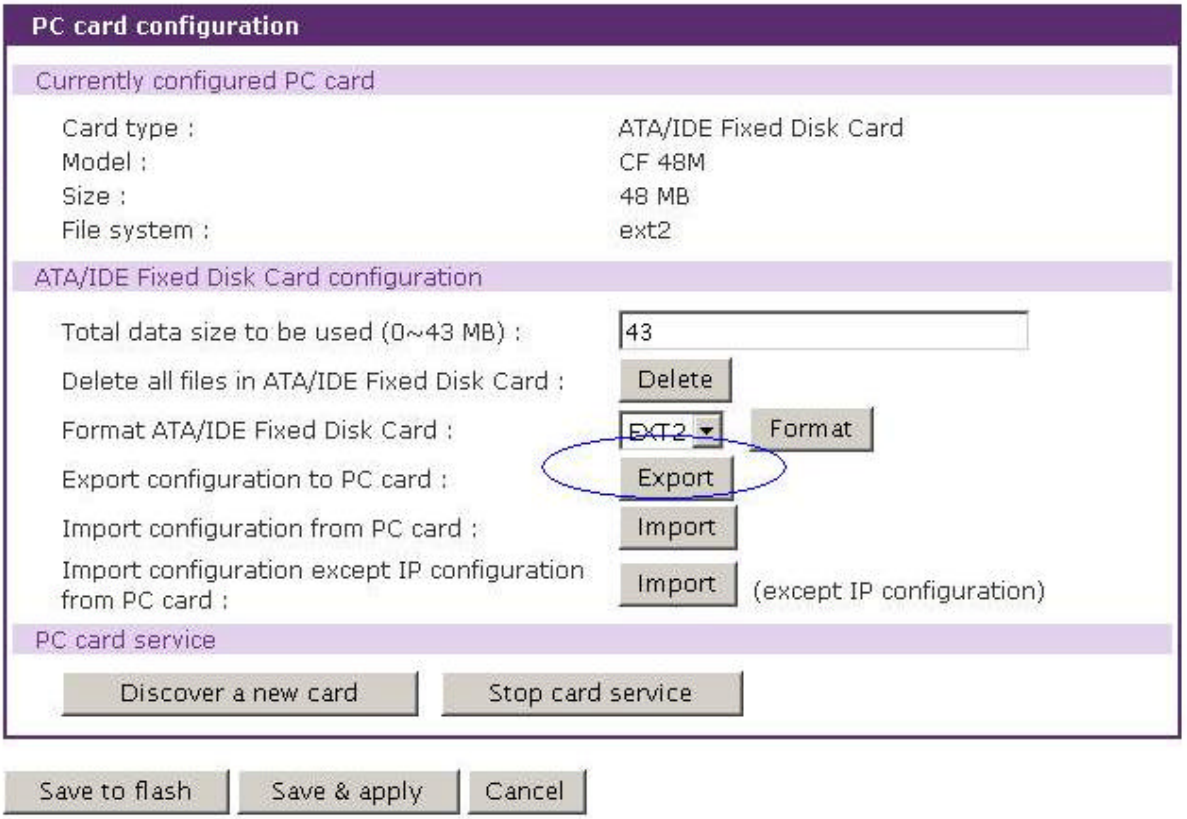
Figure 7.23 SNMP trap notification in HP Openview NMS software

8. VTS administration

8.1. How can I save the configuration of VTS and restore it back to VTS later?

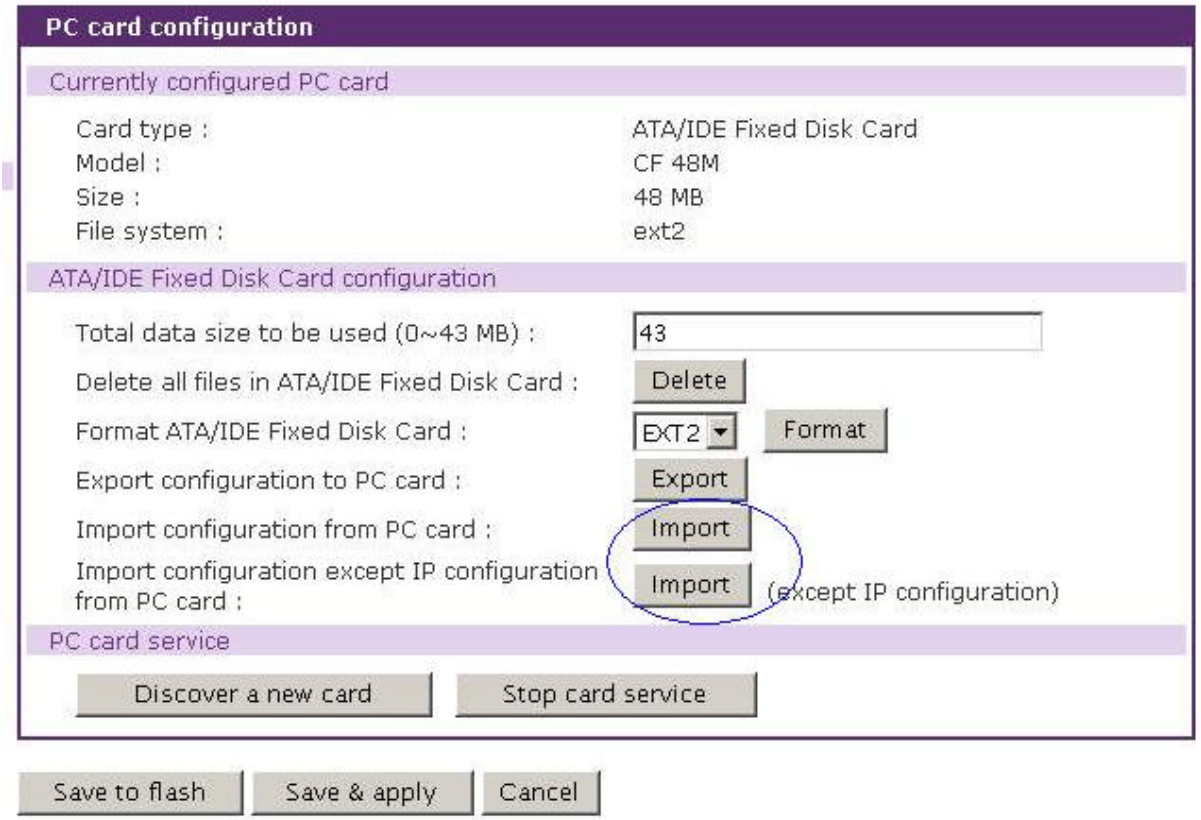
Follow the steps below.

1) From the Web menu, go to 'PC Card configuration and click [Discover a new card]. If there is Flash memory card in VTS PCMCIA slot, you may see the window like below.



2) Click [Export] button to save the configuration of VTS.

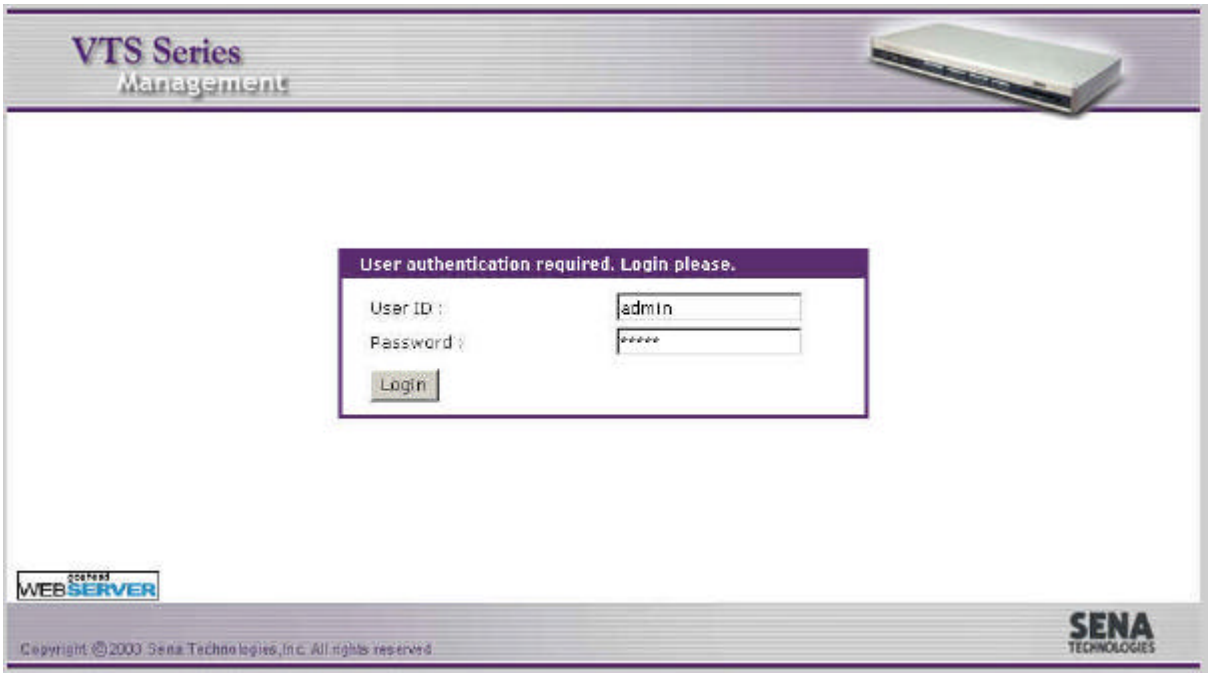
3) To import the saved configuration from Flash card to VTS, click [Import] button. This feature enables administrator to import the configuration from PC Card, which had been exported to PC card earlier.



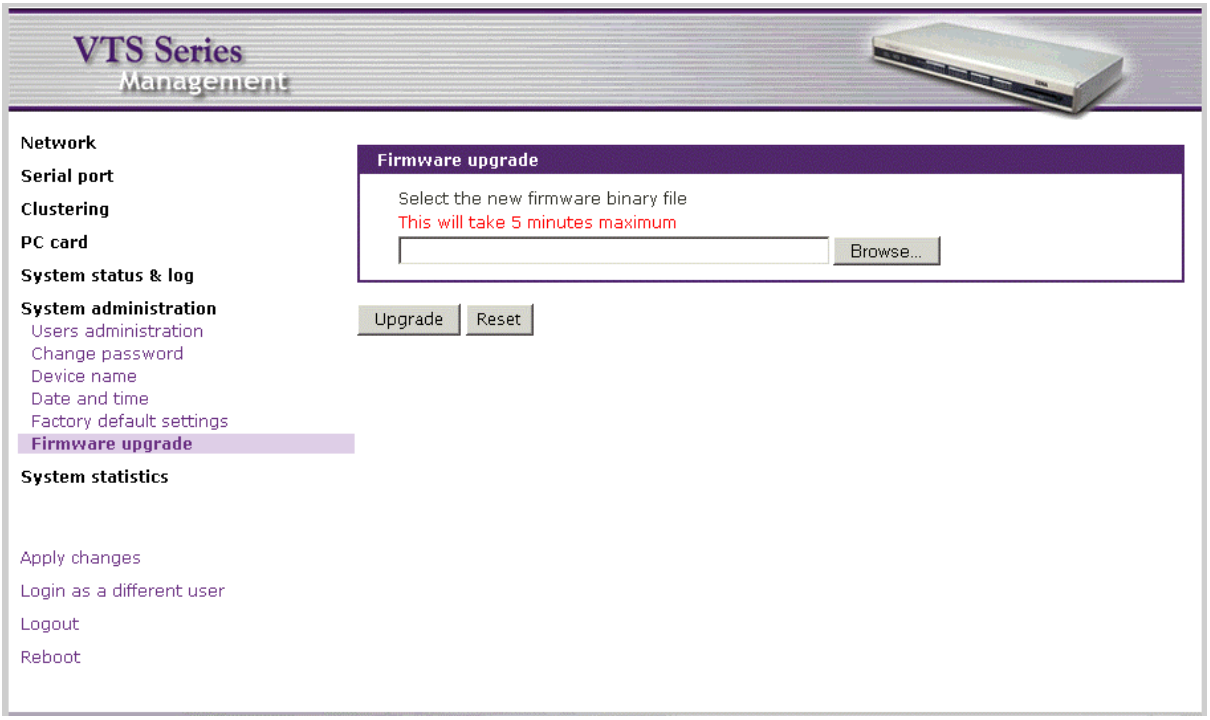
8.2. How can I update the firmware?

Follow the steps below.

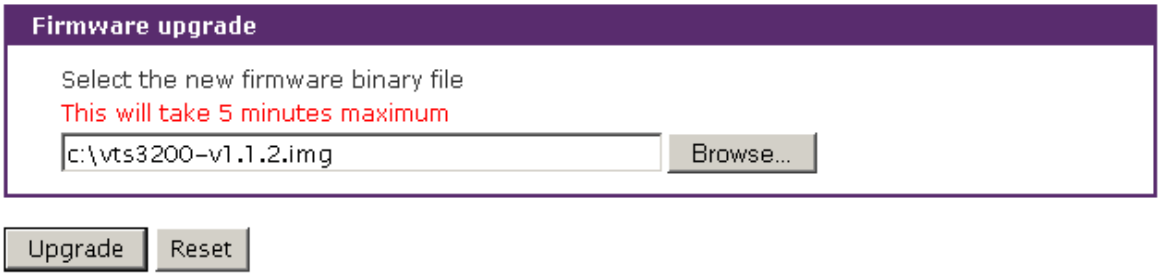
1) Access the web interface.



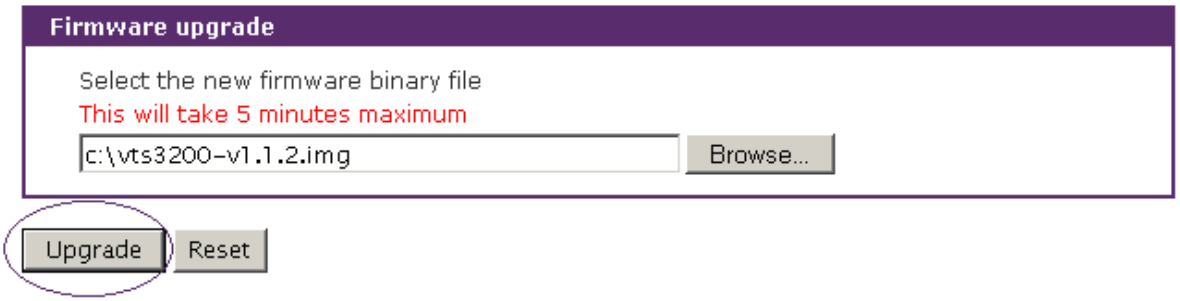
2) Choose Firmware upgrade, under the System administration heading.



3) Click on the Browse button and locate the firmware download.



4) Click on Upgrade button.



9. CLI

9.1. How can I use a shell script?

1) Log in to the VTS CLI.
2) The '/usr2/rc.user' runs at the VTS bootup. So, edit the script.

```
root@192.168.0.161:~# cd /usr2
root@192.168.0.161:/usr2# vi rc.user
… Edit the rc.user …
```

3) See examples in the reference (2).

Reference:

(1) VTS user manual > 10. CLI guide
(2) VTS user manual > 10.8. Examples

9.2. How can I back up or restore VTS configuration files in CLI?

All the VTS configuration files are located in '/tmp/cnf'. A user can back up those VTS configuration files using a storage PCCard or using FTP or SCP on CLI.

9.2.1. Save configuration files on to a PC using FTP

1) VTS has a FTP client. So, there should be a FTP server on the PC side.
2) Log in to the VTS CLI via serial console or telnet connection.
3) From the */tmp/cnf* folder VTS CLI, verify the directory structure by the 'ls –l' command. Two subdirectories are viewed. The 'd' in the red circle indicates it's a directory.

```
C:₩WINNT₩System32₩cmd.exe - telnet 192.168.5.2
root@192.168.5.2:/tmp/cnf# ls -l
-rw-r--r--    1 root     root           19 Jul  9 13:53 chap-secrets
-rw-r--r--    1 root     root         1640 Jul  9 13:53 client.pem
drwxr-xr-x    2 root     root         1024 Jul  7 17:44 cluster
-rw-r--r--    1 root     root          123 Jul  9 13:53 ez-ipupdate.conf
-rw-r--r--    1 root     root           80 Jul  9 13:53 group
-rw-r--r--    1 root     root          194 Jul  9 13:53 interfaces
drwxr-xr-x    2 root     root         1024 Jul  7 17:44 keywords
-rw-r--r--    1 root     root           25 Jul  9 13:53 krb5.conf
-rw-r--r--    1 root     root           19 Jul  9 13:53 pap-secrets
-rw-r--r--    1 root     root          133 Jul  9 13:53 passwd
-rw-r--r--    1 root     root          277 Jul  9 13:53 pppoe.conf
-rw-r--r--    1 root     root         6415 Jul  9 13:53 redirect.cnf
-rw-r--r--    1 root     root           48 Jul  9 13:53 resolv.conf
-rw-r--r--    1 root     root         2136 Jul  9 13:53 server.pem
-rw-r--r--    1 root     root          144 Jul  9 13:53 shadow
-rw-r--r--    1 root     root          139 Jul  9 13:53 snmpd.conf
-rw-r--r--    1 root     root         1695 Jul  9 13:53 system.cnf
-rw-r--r--    1 root     root            7 Jul  9 13:53 version
root@192.168.5.2:/tmp/cnf#
```

4) Run the FTP client from /tmp/cnf. And create the same directory structure on the PC.

```
root@192.168.5.2:/tmp/cnf# ftp 192.168.0.149
Connected to 192.168.0.149.
220 yup-notebook Microsoft FTP Service (Version 5.0).
Name (192.168.0.149:root): yup
331 Password required for yup.
Password:
230 User yup logged in.
Remote system type is Windows_NT.
ftp> mkdir cnf
257 "cnf" directory created.
ftp> mkdir cnf/cluster
257 "cnf/cluster" directory created.
ftp> mkdir cnf/keywords
257 "cnf/keywords" directory created.
```

5) Copy all the files to the PC. Use put/mput FTP command to perform this task.

```
< copy files from local cnf folder to remote cnf folder >
ftp> cd cnf
250 CWD command successful.
ftp> prompt
Interactive mode off.
ftp> mput *
local: chap-secrets remote: chap-secrets
200 PORT command successful.
...
...
<...copy files from local cluster folder to remote cluster folder >
ftp> cd cluster
250 CWD command successful.
ftp> lcd cluster
Local directory now /initrd/tmp/cnf/cluster
ftp> prompt
Interactive mode off.
ftp> mput *
local: cluster.conf remote: cluster.conf
200 PORT command successful.
...
...
< copy files from VTS keywords folder to PC's keyword folder >
ftp> cd /cnf/keywords
530 Please login with USER and PASS.
ftp> lcd /tmp/cnf/keywords
Local directory now /initrd/tmp/cnf/keywords
ftp> mput *
local: port1 remote: port1
200 PORT command successful.
...
...
```

9.2.2. Restore VTS configuration from PC

Let's assume that a user saved VTS configuration as in *'Save configuration files on to a PC using FTP'*.

1) Verify that FTP server is running on the PC.
2) Log in to the VTS CLI via serial console or telnet connection.
3) Copy all the files from the PC. Use get/mput FTP command to perform this task.

```
ftp> cd cnf
250 CWD command successful.
ftp> lcd /tmp/cnf
Local directory now /initrd/tmp/cnf
ftp> mget *
local: chap-secrets remote: chap-secrets
200 PORT command successful.
150 Opening ASCII mode data connection for chap-secrets(20 bytes).
226 Transfer complete.
20 bytes received in 0.00 secs (6.2 kB/s)
...
...
```

9.2.3. Save configuration files on to a PC using SCP and restore them

1) A user should have a SCP client program installed on PC.
2) Copy all the files and directory under /tmp/cnf from VTS(192.168.5.2) to the PC. Type the red boxed command line from the PC. The '-r' option copies recursively all the files under sub-directories.

```
[jungoj@localhost jungoj]$ scp -r root@192.168.5.2:/tmp/cnf/ ./cnf-backup/
The authenticity of host '192.168.5.2 (192.168.5.2)' can't be established.
RSA key fingerprint is c1:70:ab:52:48:ab:e5:dc:47:9c:94:ed:99:6f:94:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.5.2' (RSA) to the list of known hosts.
root@192.168.5.2's password:
system.cnf            100% |*****************************|  1695        00:00
redirect.cnf          100% |*****************************|  6415        00:00
snmpd.conf            100% |*****************************|   139        00:00
pap-secrets           100% |*****************************|    19        00:00
chap-secrets          100% |*****************************|    19        00:00
pppoe.conf            100% |*****************************|   277        00:00
resolv.conf           100% |*****************************|    48        00:00
client.pem            100% |*****************************|  1640        00:00
server.pem            100% |*****************************|  2136        00:00
interfaces            100% |*****************************|   194        00:00
ez-ipupdate.conf      100% |*****************************|   123        00:00
passwd                100% |*****************************|   133        00:00
```

3) Restore the configuration back up. Type the red boxed command line from the PC.

```
[jungoj@localhost jungoj]$ scp -r ./cnf-backup/ root@192.168.5.2:/tmp/cnf/
root@192.168.5.2's password:
system.cnf            100% |*****************************|  1695        00:00
redirect.cnf          100% |*****************************|  6415        00:00
snmpd.conf            100% |*****************************|   139        00:00
pap-secrets           100% |*****************************|    19        00:00
chap-secrets          100% |*****************************|    19        00:00
pppoe.conf            100% |*****************************|   277        00:00
resolv.conf           100% |*****************************|    48        00:00
client.pem            100% |*****************************|  1640        00:00
server.pem            100% |*****************************|  2136        00:00
interfaces            100% |*****************************|   194        00:00
```