

## VTS Series Firmware Version 1.7.0 Release Notes

June 22, 2005

Copyright (c) 1998-2005, Sena Technologies, Inc.

### INTRODUCTION

=====

These release notes describe new features added and bugs fixed since the firmware V1.6.5 release.

### ENHANCEMENTS

=====

- + Added the access lists for grouping users
- + Added the remote ports supports
- + Added the VTS manager supports (Removed the HD Manager support)
- + Enhanced clustering features
  - \* Integrating the ports of the slave units into connection page of master unit.
  - \* Clustering slave unit web pages which are linked through clustering master unit can be accessed
    - without prompting authentication.
- + Added the automated way to backup configuration
- + Upgraded the OpenSSH to v4.0p1
- + Added the delimiter support in RawTCP protocol
- + Added uptime information at system status page
- + Enhanced security in VTS
  - \* Enhance logging(all connection to CM and Ports)
  - \* Log all changes to configuration
  - \* Add security profile configuration
  - \* Add Stealth mode
  - \* Enhanced login security – forced to use strong password rules
    - Minimum password length
    - Maximum password age
    - Enforce password history
    - Enforce password complexity
      - 1) Not contain all or part of the user's account name
      - 2) Be at least eight characters in length

- 3) Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, \$, #, %)
  - 4) Six characters of a password may only occur once.
  - 5) No null or blank characters may be used.
  - 6) No consecutive numbers or letters.
  - 7) Users should not use a password that is the same as the USERID or user's name.
  - 8) May not be a password that was used within the previous nine password changes.
  - 9) Differ from the old password by at least three characters.
- Add Enable/disable option for SNMP daemon(get/set)
  - Configure use of SSH v1/v2 (default SHOULD BE v2 if Java applet supports v2)
  - Option to use JTA on /usr2
  - Disable account after 2 wrong password attempts
- + Upgraded the TACACS+ implementation using PAM module
  - + Added the support for user customizable PAM module
  - + Extended the hash file format for automatic firmware upgrade to add a "run command"
  - + Added Radius down local authentication option for Web UI
  - + Changed to accept a hostname in syslog server configuration
  - + Added the notification if NFS mounted partition was disconnected (server down)
  - + Added the firmware upgrade option from CF card.
  - + Disable the assigned IP of serial ports by default.
  - + Added an option to disable the port escape menu.
  - + Added the support the Active Directory in LDAP authentication.
  - + Added the built-in JTA option with SSH1 and SSH2.
  - + Added an option to make a back-up log files on log storage location.
  - + Added the feature to confirm callback phone number in Dial-in modem connection
  - + Added the power status and control MIB.
  - + Added the support in connecting the slave port through ssh port(22th) of master unit
  - + Moved case sensitive option to port event handling configuration page
  - + Enhanced the method to disconnect port user in Port Escape Menu so that user can receive a message to confirm the disconnection.

ENHANCEMENTS

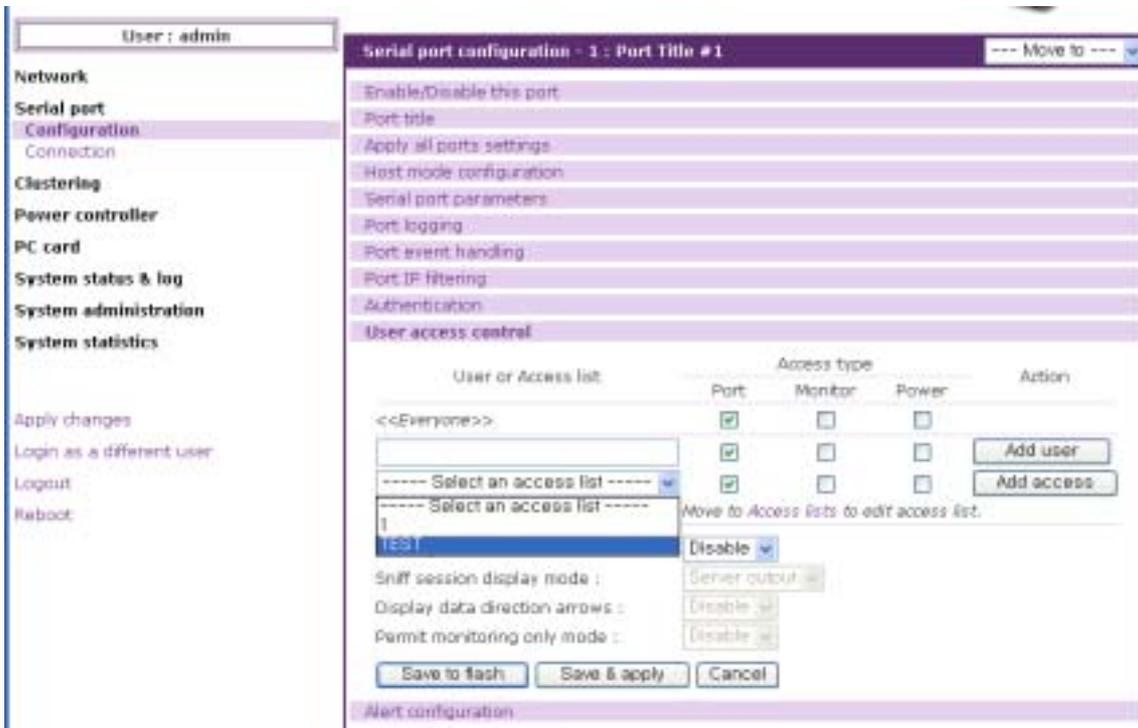
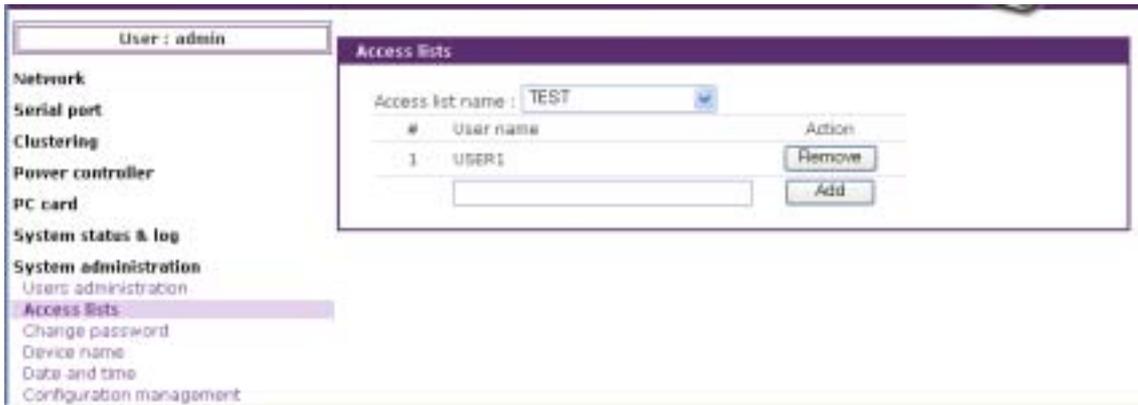
=====

+ Added the access lists for grouping users

User access control

가 User access control 가 User

9.2 (Page 124)



+ Added the remote ports supports

VTS

(remote port)

Console server

mode

VTS

Console server mode

Serial port parameters

Remote port parameters

4. (Page 43,47) 4.3.5 Serial port parameters /

Remote port parameters(Page 65)

User : admin

Network

Serial port

Configuration

Connection

Clustering

Power controller

PC card

System status & log

System administration

System statistics

Apply changes

Login as a different user

Logout

Reboot

### Serial port configuration

Port access menu configuration

Port access menu configuration

All port configuration

Port#	Title	Mode	Base address	Port	Proto	Serial-settings
All	Port Title	CS	0.0.0.0	7051	Telnet	9603-N-0-1-No

Individual port configuration

Port#	Title	Mode	Dest/AssignedIP	Port	Proto	Serial-settings
1	Port Title #1	CS	0.0.0.0	7051	Telnet	9603-N-0-1-No
2	Port Title #2	CS	0.0.0.0	7052	Telnet	9603-N-0-1-No
3	Port Title #3	CS	0.0.0.0	7053	Telnet	9603-N-0-1-No
4	Port Title #4	CS	0.0.0.0	7054	Telnet	9603-N-0-1-No
5	Port Title #5	CS	0.0.0.0	7055	Telnet	9603-N-0-1-No
6	Port Title #6	CS	0.0.0.0	7056	Telnet	9603-N-0-1-No
7	Port Title #7	CS	0.0.0.0	7057	Telnet	9603-N-0-1-No
8	Port Title #8	CS	0.0.0.0	7058	Telnet	9603-N-0-1-No

Remote port configuration

<input type="checkbox"/>	Title	Mode	Assigned IP	Port	Proto	Remote-settings
<input type="checkbox"/>	Test Remote Port	CS	0.0.0.0	7051	Telnet	0.0.0.0/0

Click [Remove] button to remove the checked remote port profile.

Remote port title :

Remove Add

User : admin

Network

Serial port

Configuration

Connection

Clustering

Power controller

PC card

System status & log

System administration

System statistics

Apply changes

Login as a different user

Logout

Reboot

### Serial port configuration - R1 : Test Remote Port

Enable/Disable this port

Port title

Apply all ports settings

Host mode configuration

Remote port parameters

IP address :

Port :

Protocol :

Save to flash Save & apply Cancel

Port logging

Port IP filtering

Authentication

User access control

Alert configuration



\* Clustering slave unit web pages which are linked through clustering master unit can be accessed without prompting authentication.

, VTS

, SSH

## 5.2 Clustering (Page 99)

JTA

"http://<IP>/connect.asp?p=<port number>"

"<http://<IP>/connect.asp?t=<port title>>"

+ Added the automated way to backup configuration

가

The screenshot displays the 'Configuration management' section of a web interface. On the left is a navigation menu with categories like Network, System administration, and System statistics. The main content area is divided into three sections:

- Configuration export:** Includes radio buttons for Location (CF Card, Primary NFS server, User space(/usr2), Local machine), an Encrypt dropdown set to 'Yes', and a File name field containing '.system'. An 'Export' button is present.
- Configuration import:** Includes radio buttons for Location (CF Card, Primary NFS server, User space(/usr2), Local machine, Factory default), a 'Configuration selection' list with checkboxes for 'Select all', 'System configuration (Including IP configuration)', 'Serial port configuration', 'Clustering configuration', and 'System user configuration', an Encrypt dropdown set to 'Yes', and a 'File selection' field with a 'Local' field and a file browser icon. An 'Import' button is present.
- Automatic backup configuration:** Includes an 'Automatic backup option' dropdown set to '10 minutes after last change', radio buttons for Location (CF Card, Primary NFS server, User space(/usr2), Send via email), an Encrypt dropdown set to 'Yes', a File name field containing '.system', a 'Backup interval (hour, 1 - 720)' field, and a 'Recipient's email address' field. 'Save to flash', 'Save & apply', and 'Cancel' buttons are at the bottom.

+ Upgraded the OpenSSH to v4.0p1

OpenSSH

+ Added the delimiter support in RawTCP protocol

RawTCP

Delimiter

가

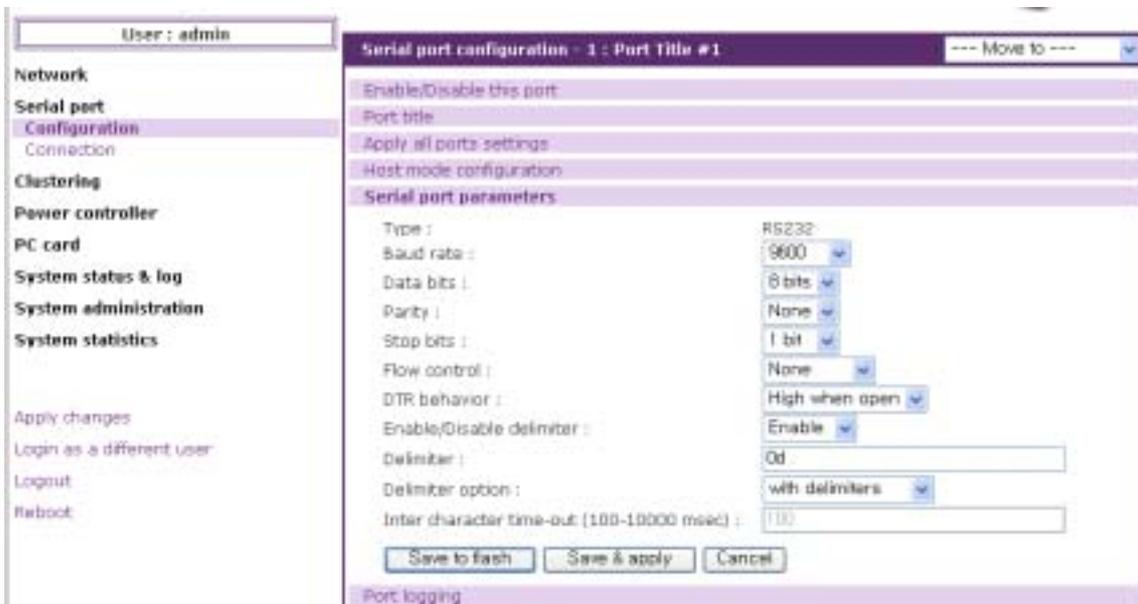
Delimiter가

. Disable

Inter character time-out

가

### 4.3.5 Serial port parameters / Remote port parameters(Page 65)

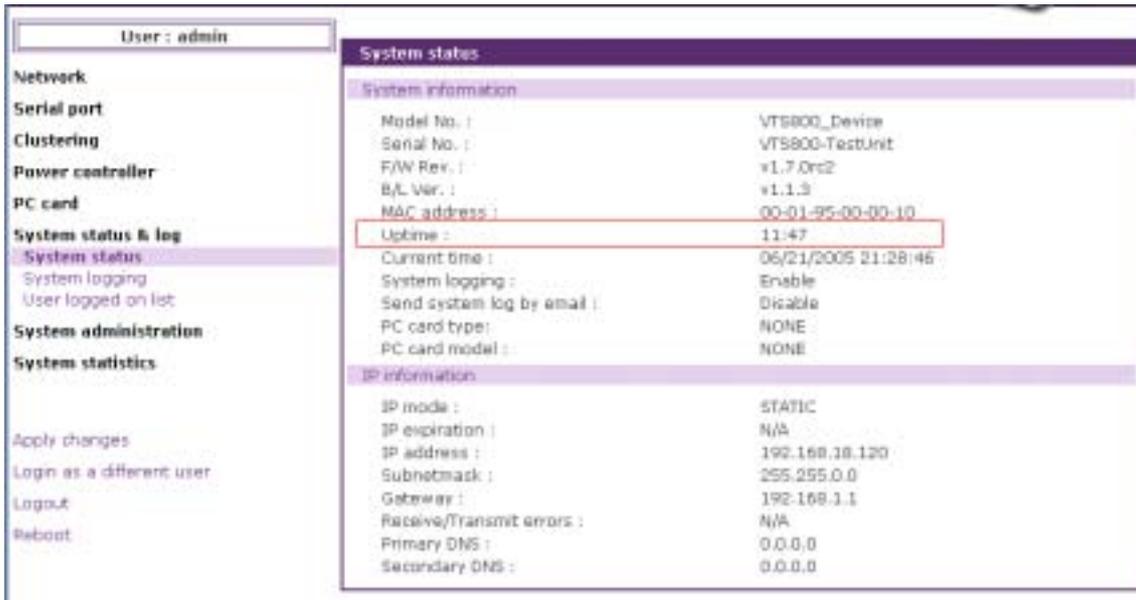


+ Added uptime information at system status page

System Status page

System Uptime

가



+ Enhanced security in VTS

VTS

\* Enhance logging(all connection to VTS and Ports)

System logging

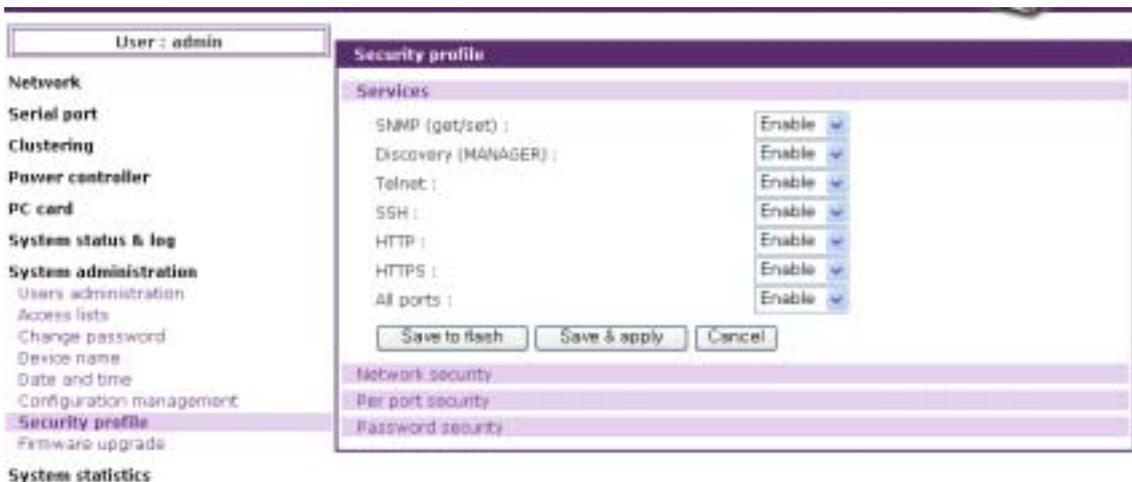
\* Log all changes to configuration

\* Add security profile configuration

VTS

VTS

### 9.7 Security Profile(Page 130)



\* Add Stealth mode.

Stealth 가 가

Stealth mode가 Enable , 가

VTSGA

\* Enhanced login security – forced to use strong password rules

### 9.7.4 Password Security (Page 133)

- Minimum password length
- Maximum password age
- Enforce password history
- Enforce password complexity
  - 1) Not contain all or part of the user's account name
  - 2) Be at least eight characters in length
  - 3) Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, \$, #, %)
  - 4) Six characters of a password may only occur once.
  - 5) No null or blank characters may be used.
  - 6) No consecutive numbers or letters.
  - 7) Users should not use a passwords that is the same as the USERID or user's name.
  - 8) May not be a password that was used within the previous nine password changes.
  - 9) Differ from the old password by at least three characters.

- Add Enable/disable option for SNMP daemon(get/set)

SNMP Enable/Disable 가

- Configure use of SSH v1/v2 (default SHOULD BE v2 if Java applet supports v2)

SSH 1 . Disable SSH  
2 .

- Option to use JTA on /usr2

가 Java applet 가 Java applet  
/usr2/jta.jar Web applet option User-defined 가  
가 /usr2/jta.jar가 Java applet

- Disable account after 2 wrong password attempts

3 가

+ Upgraded the TACACS+ implementation using PAM module

PAM TACACS+ 11.9.3 CLI  
 TACACS+ (Page 158)

+ Added the support for user customizable PAM module

**Custom PAM** Linux-PAM (Pluggable Authentication Modules for Linux)  
 /ets/pam.d/custom  
 Custom-PAM 11.8.2 CLI RADIUS (Page 152)  
 11.8.3 CLI TACACS+ (Page 158)

+ Extended the hash file format for automatic firmware upgrade to add a "run command"

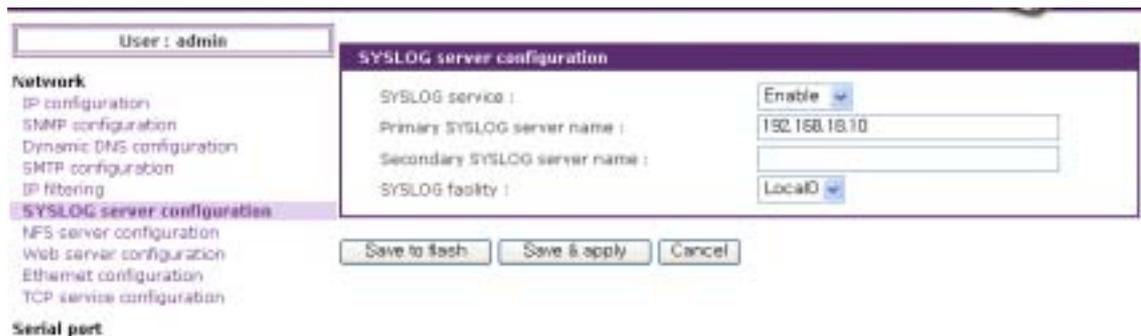
Hash  
 9.8 Firmware Upgrade (Page 138)

+ Added Radius down local authentication option for Web UI

Web UI Radius down local 가

+ Changed to accept a hostname in syslog server configuration

SYSLOG SYSLOG server IP address SYSLOG server name



+ Added the notification if NFS mounted partition was disconnected (server down)

NFS 가 SNMP 가  
 3.7 NFS (Page 38)



Serial port configuration - 1 : Port Title #1 --- Move to --- ▾

Enable/Disable this port

Port title

Apply all ports settings

**Host mode configuration**

Host mode : Console server ▾

Enable/Disable assigned IP : Disable ▾

Assigned IP : 0.0.0.0

Listening TCP port (1024-65535) : 7001

Protocol : RawTCP ▾

Inactivity timeout (1-3600 sec, 0 for unlimited) : 100

Enable/Disable port escape sequence : Enable ▾

Port escape sequence : Disable ▾

Port break sequence : ~break

Use comment : No ▾

Quick connect via : Web applet ▾

Web applet encoding : English (latin1) ▾

Save to flash Save & apply Cancel

Serial port parameters

Port logging

Port event handling

Port IP filtering

Authentication

User access control

Alert configuration

+ Added the support Active Directory in LDAP authentication

LDAP

active directory

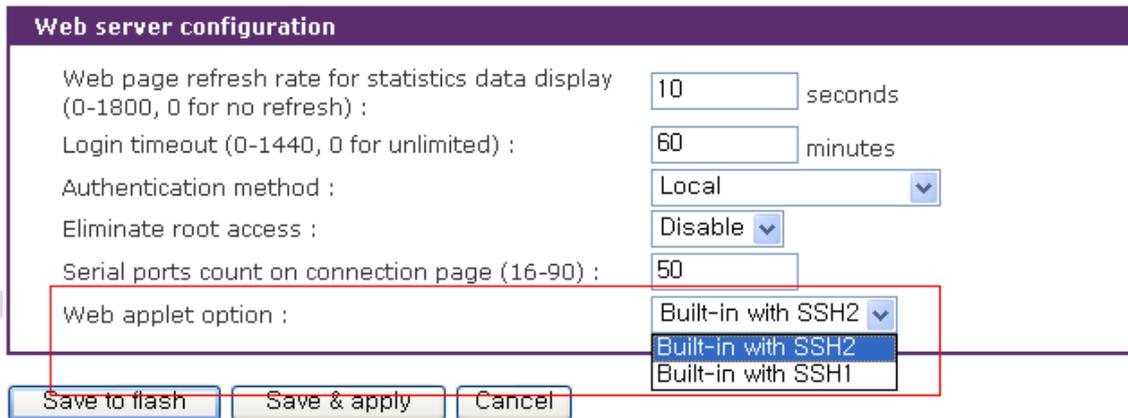
+ Added the built-in jta option with SSH1 and SSH2

JTA

SSH

3.8

(Page 40)



+ Added an option to make a back-up log files on log storage location

Port log storage location    CF card    NFS server

enable

default

, 1.7.0

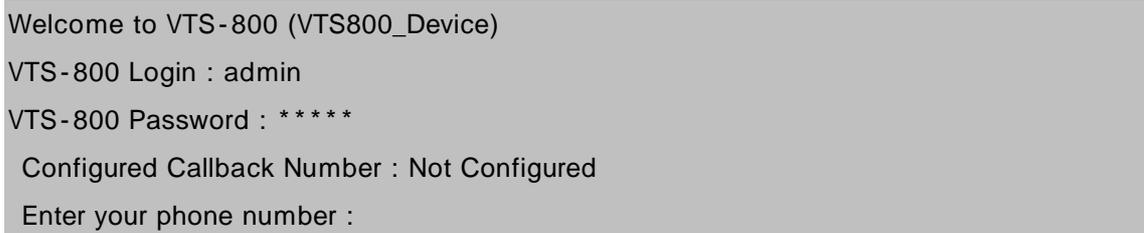
가

+ Added the feature to confirm callback phone number in Dial-in modem connection

Dial-in modem callback phone number

가

.)



+ Added power status and control MIB

SNMP    Power

MIB    가

Sena VTS MIB

+ Added the support in connecting the slave port through ssh port(22th) of master unit

Unit    SSH

Unit

4.5 Serial Port

(Page 89)

+ Moved case sensitive option to port event handling configuration page

Port Logging                      Case sensitive                      Port Event Handling

+ Enhanced the method to disconnect port user in Port Escape Menu so that user can receive a message to confirm the disconnection

Port Menu                      d. disconnect a sniff session                      Sniff                      Disconnect 가

