SERVIS IP-KVM

1p Converter

User's Guide

(for ES)

Version 3.0

FUJITSU

Revision Record

Version No.	Date	Detail
01	2005/11/28	First Version
02	2006/04/25	Change and add web pages layouts. Add 2.5.8 USB Setting Window 2.5.9 KVM Setting Window Add 5.1 Trouble Shooting contents
03	2006/05/25	Add 2.3 Logon to this Product: “Select Your Language” page 2.5.5 Virtual Key Window: Sun keyboard, German layout support 3.5.5 Copyright Notices 5.1 Trouble Shooting contents

Introduction

Thank you for purchasing *SERVIS IP-KVM* 1p Converter (hereafter referred to as "this product").

This product is intended to enable operating the DOS/V (PC/AT compatible) and the SUN (USB) server (hereafter referred to as "host server") by keyboard, video and mouse (KVM) from remote locations via a network.
It is equipped with a server connecting port to connect a host server. It is possible to connect the KVM switch (SERVIS series) to a server connecting port. It enables operating multiple host servers connected by KVM switch from remote locations via network.
It also encodes data in a network with the data encryption function (SSL and SSH) and offers safe network communications.
This product also has virtual disk function by USB connection, which enables use of this product as a USB disk drive from host servers and realizes file to file transfer between remote terminal units and host servers.
This product has two independent power configurations (redundant) to offer a redundant power supply. It prevents system breakdown caused by disconnection of the power adapter and power cables or failure of the power supply unit and its components after in this product.

This guide provides methods for setting up, basic operations and various functions of this product.

About this Guide

This guide contains important information regarding the safe and proper use of this product.
Before using this product, please read carefully and understand the contents of this guide.
After reading, retain this guide in a safe place for future reference.
We have made every effort to ensure the safety of the users and other personnel, and to prevent property damage. When using this product, carefully follow the instructions described in this guide.

The contents of this guide are subject to change without prior notice for the purpose of improvement. If you have any questions or comments about this product and the contents of this guide, contact our maintenance service department.

CAUTION: HAZARDOUS VOLTAGE.
SERVICE ENGINEER ONLY TO OPEN COVER.

CAUTION: FOR CONTINUED PROTECTOIN
AGAINST RISK OF FIRE.
REPLACE ONLY WITH SAME TYPE AND RATING OF FUSE.

Precautions for Use

It is the customer's responsibility to use this product including this guide, the device, and firmware.
Fujitsu Component Limited bears no responsibility for damages or loss of data that may occur as a result of using this product. Also note that restitution for damages due to malfunctioning of this product shall not exceed the total cost of this product, regardless of the range of the damages covered by the warranty.
The firmware shipped with this product and update firmware for this product provided by Fujitsu Component Limited must not be used with systems other than this product, and must not be modified or disassembled.
Problems may occur with this product in the event of an instantaneous voltage drop of the power supply due to lightning, etc.

Notes on Maintenance

This product must not be dismantled, modified, or repaired by personnel other than our maintenance engineers. It contains dangerous, high voltage components. Contact our maintenance department for repairs.

Connection to Servers and Countermeasures against Static Electricity

When attaching/removing connectors to connect the server port of this product to a host server, ensure that host server is turned off. In addition, be sure to discharge static electricity before connecting the cables.
Twisted pair cables (e.g. LAN cables) may be charged with static electricity depending on your operating environment. Connecting twisted pair cables charged with static electricity to devices including this product could cause a malfunction or failure of the devices or their LAN ports.
Use a static eliminator or any other tool immediately before connecting, and discharge static electricity in twisted pair cables to ground wires.
Note that if the cables remain unconnected for a long time after discharging static electricity, they may be charged with static electricity again.

High Safety Measures

This Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter “High Safety Required Use”), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system.
You shall not use this Product without securing the sufficient safety required for the High Safety Required Use. Neither Fujitsu Component Limited nor its affiliates shall be responsible for any damages that occur to the user of this product or a third party due to the use of this product in a situation that requires advanced safety measures.

Green Products

This is a "Green Product" that has met the severe environment standards of the Fujitsu Group. It is an earth-friendly product with a low impact on the environment.

Major features

Compact and resource saving
Low power consumption
Lead free

For environmental efforts of the Fujitsu Group, visit the "Environmental Activities" page of the Fujitsu website (http://eco.fujitsu.com/jp/).

Disposal of this Product

Dispose of this product must no be performed by the user.

When this product is no longer necessary, contact the dealer where you purchased this product.

Conventions

The following are conventions used throughout this guide.

Font or symbol	Definition
AaBbCc123	Indicates output from this product or connected devices, which is displayed on the screen.
AaBbCc123	Indicates characters that you enter in a command line or configuration file.
Enter↵	Indicates an “Enter” key you press.
🕮 Refer to	Indicates a reference (chapter, section, and page number).
⚠CAUTION	Indicates points to note when using this product.

Contents

MEMO

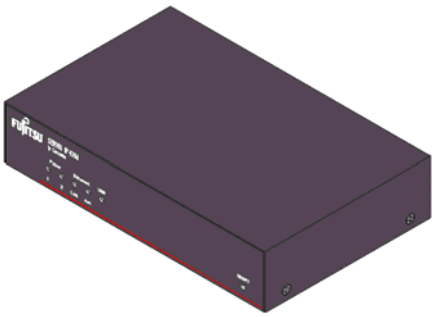
Chapter 1 - Setup

This chapter provides information of SERVIS IP-KVM device as required for its setup. Please make sure to read this manual before the operation.

Contents

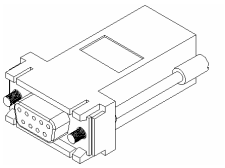
1.1. Device Components

Check and make sure the components listed below are included. Keep the original shipping box for future transport of the device.

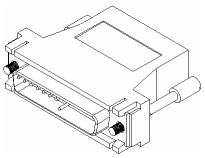


SERVIS^{TM} *IP-KVM* 1p Converter FX-7001NP Main Unit ... 1

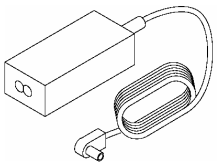
Rubber Foot...1set (4)



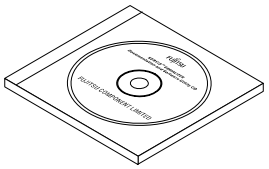
RJ45–D-Sub 9-pin Conversion Adapter FP-AD009RJX ... 1



RJ45–D-Sub 25-pin Conversion Adapter FP-AD025RJX ... 1



Power Adapter ... 1

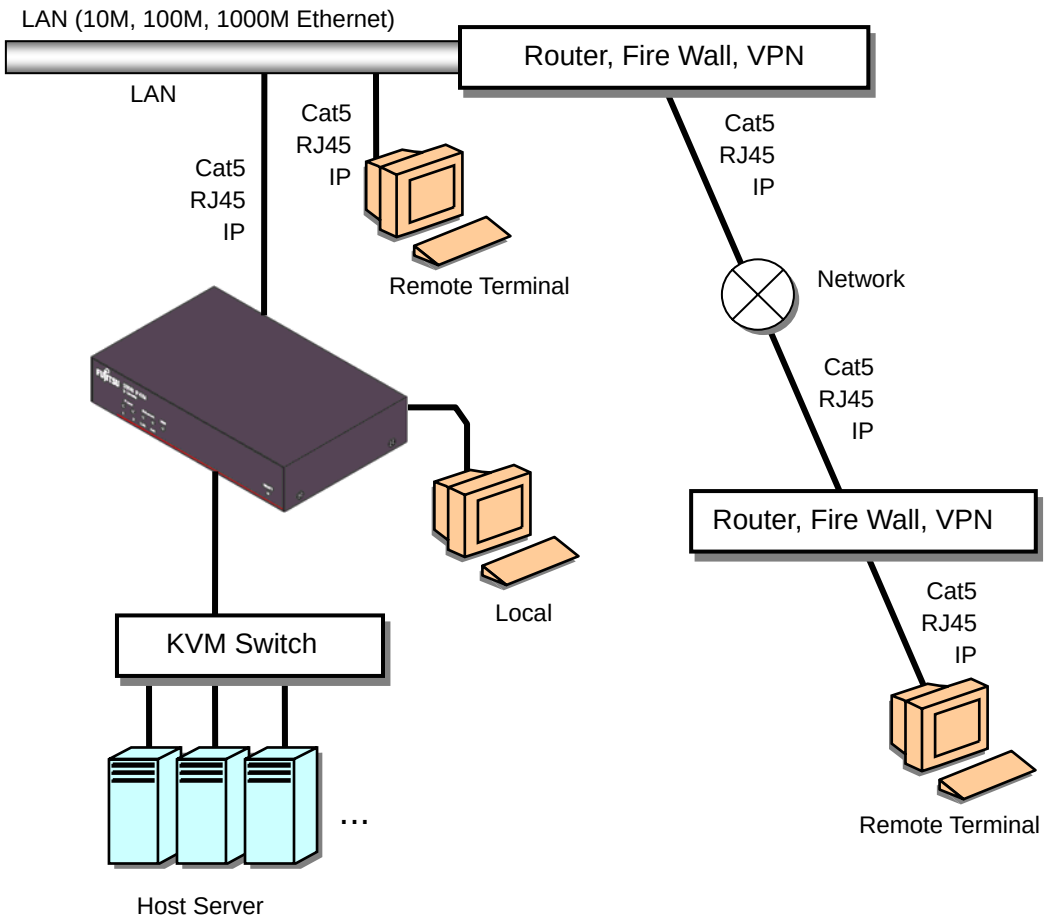


CD-ROM (this guide) ... 1

1.2. Product Outline

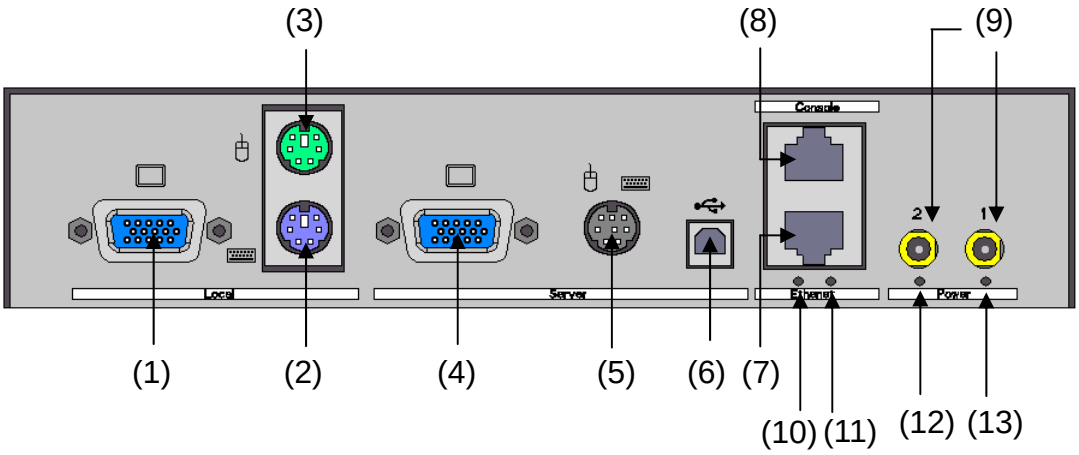
This product is a device to connect the keyboard, mouse and video port of target device (hereinafter called Host server) to the remote terminal unit in the remote location via network.

It is also able to switch and operate the multiple host servers from the remote location by connecting to the KVM switch.



1.3. Parts and Functions

1.3.1 Rear



(1) Local Video Port

Connects the video monitor for local operation.
Connector type is female Mini D-sub15 pin.

(2) Local Keyboard Port

Connects the PS/2 keyboard for local operation.
Connector type is Mini-DIN6 pin.

(3) Local Mouse Port

Connects the PS/2 mouse for local operation.
Connector type is Mini-DIN6 pin.

(4) Server Video Port

Connects to the host server or KVM switch to be controlled with the optional composite cable for server connection.
Connector type is female Mini D-sub15 pin.

(5) Server PS/2 Port

Connects to the host server or KVM switch to be controlled with the optional composite cable for server connection.
Connector type is Mini-DIN8 pin.

(6) Server USB Port

Connects to the host server to be controlled with the optional USB connection cable.
Connector type is USB type B.

(7) Ethernet Port

Ethernet connector which is compliant with 10BASE-T/100BASE-TX.
Both UTP and STP cables are available.
Connector type is RJ45 modular jack.
🕮 Refer to 4.2 RJ45 Connector Signal Assign (page 141)

(8) Console Port

For RS232 Connection.
Connects to this product using this Console port and set the network at initial installation.
Connector type is RJ45 modular jack.
🕮 Refer to 1.5.4 Serial Console Connection (page 12)

(9) Power Adapter Connector

Connects the power adapter (DC5V input).
This product can connect up to 2 power adapters, redundant configuration is supported.

(10) Ethernet Act LED

Blinks green when a data packet is sent or received by VNC connection.

(11) Ethernet Link LED

Lights up green when the Ethernet port is linked up.

(12) Power LED 2

Lights up green when the adapter is connected to power connecter 2 and power is supplied.

(13) Power LED 1

Lights up green when the adapter is connected to power connector 1 and power is supplied.

1.3.2 Front

(1) Power LED

1: Lights up green when the adapter is connected to power connector 1 and power is supplied.
2: Lights up green when the adapter is connected to power connecter 2 and power is supplied.

(2) Ethernet LED

Link: Lights up green when the Ethernet port is linked up.
Act: Blinks green when a data packet is sent or received by VNC connection.

(3) USB LED

Lights up green when this product and the host server is connected by USB.
Blinks green if there is keyboard or mouse input when USB keyboard/mouse are enabled.

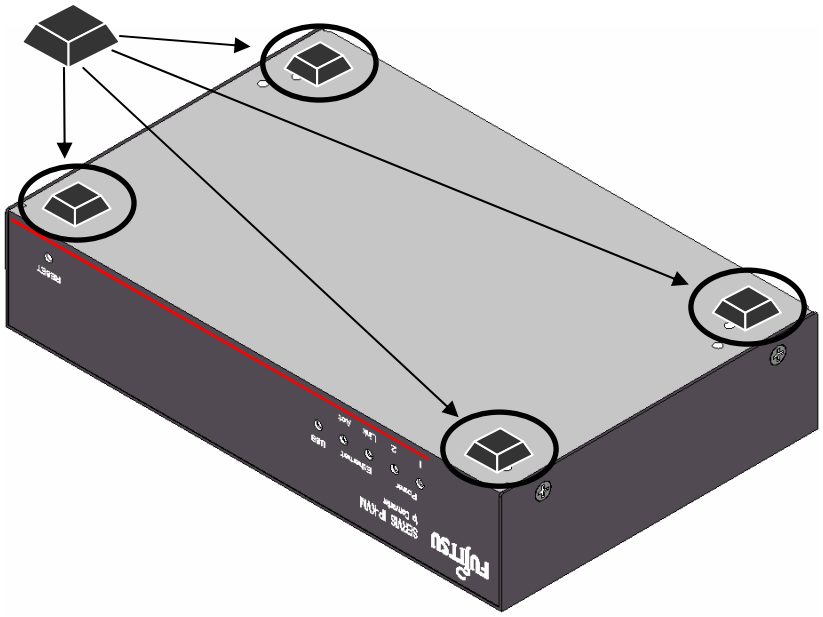
(4) RESET Button

Resets the CPU when this product is active.
This product will be restarted in approx. 15 seconds.

1.4. Installation Method

1.4.1 Placing On a Level Surface

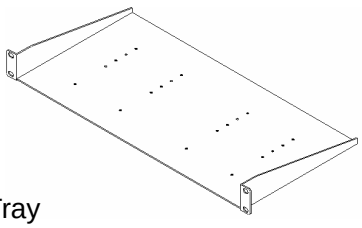
When placing this product on a level surface such as desk, attach the provided rubber feet to the bottom of the device. The feet cushion shock and protect slipping.



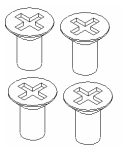
1.4.2 Rack Mount

By using optional rack mount kit, you can mount the device on a EIA standard 19 inch rack.
🕮 Refer to 4.4 Optional Accessories (page 141)

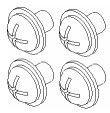
Rack Mount Kit



Rack Mount Tray

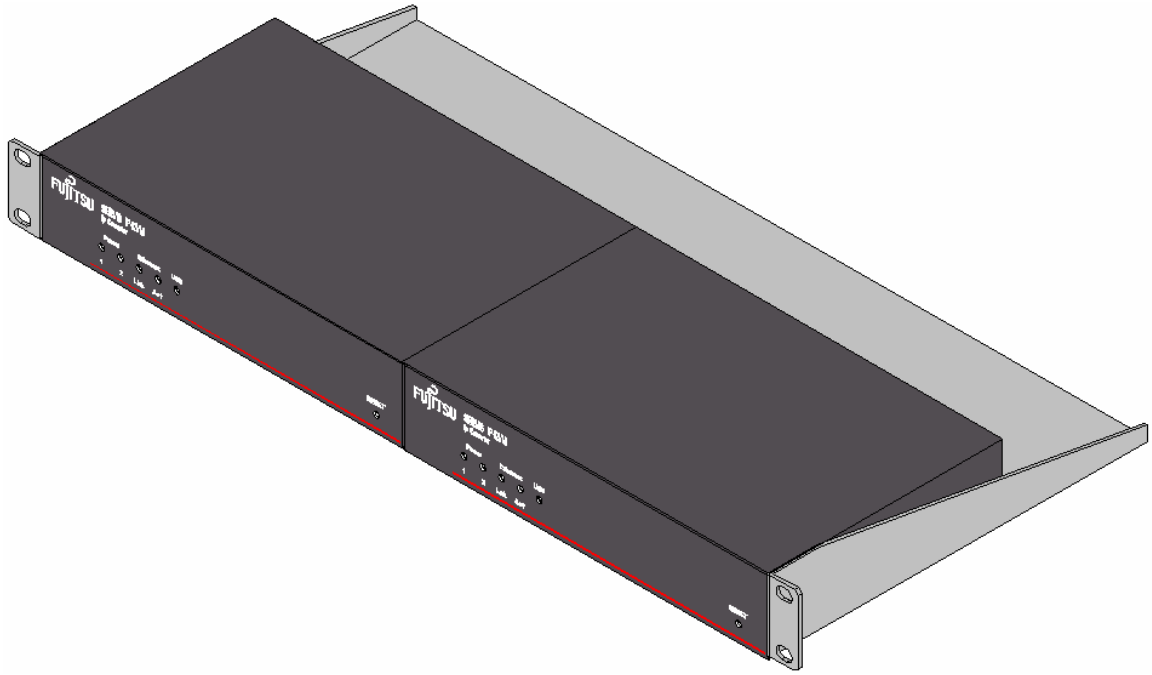


Unit/tray Screw ...4



Tray/rack support Screws... 4

Example of rack mount setting



Up to 2 devices can be mounted in an EIA standard 1U rack.

CAUTION

When mounting the product on a 19 inch rack, remove the rubber feet.

1.5. Connecting Method

1.5.1 Not Provided Necessary Components

(1) Composite cable for Server Connection (option)

Composite cable connects this product to the server or KVM switch.

(2) USB Connection Cable (option)

USB cable connects this product to the server.

(3) Video Monitor, Keyboard and Mouse for local operation.

Prepare a video monitor, keyboard and mouse for local operation.
PS/2 connection is only supported for a keyboard and mouse.

(4) Serial console terminal

Prepare a PC with RS-232C interface (D-Sub 9-pin or D-sub 25-pin). This is necessary in order to set the IP address for this product at initial installation.

(5) Cat5 Cable

Prepare a Cat5 straight cable, adapted for the environment, for network connection. Any UTP or STP is acceptable; however the cable must be shorter than 20m.

(6) Switching Hubs, etc.

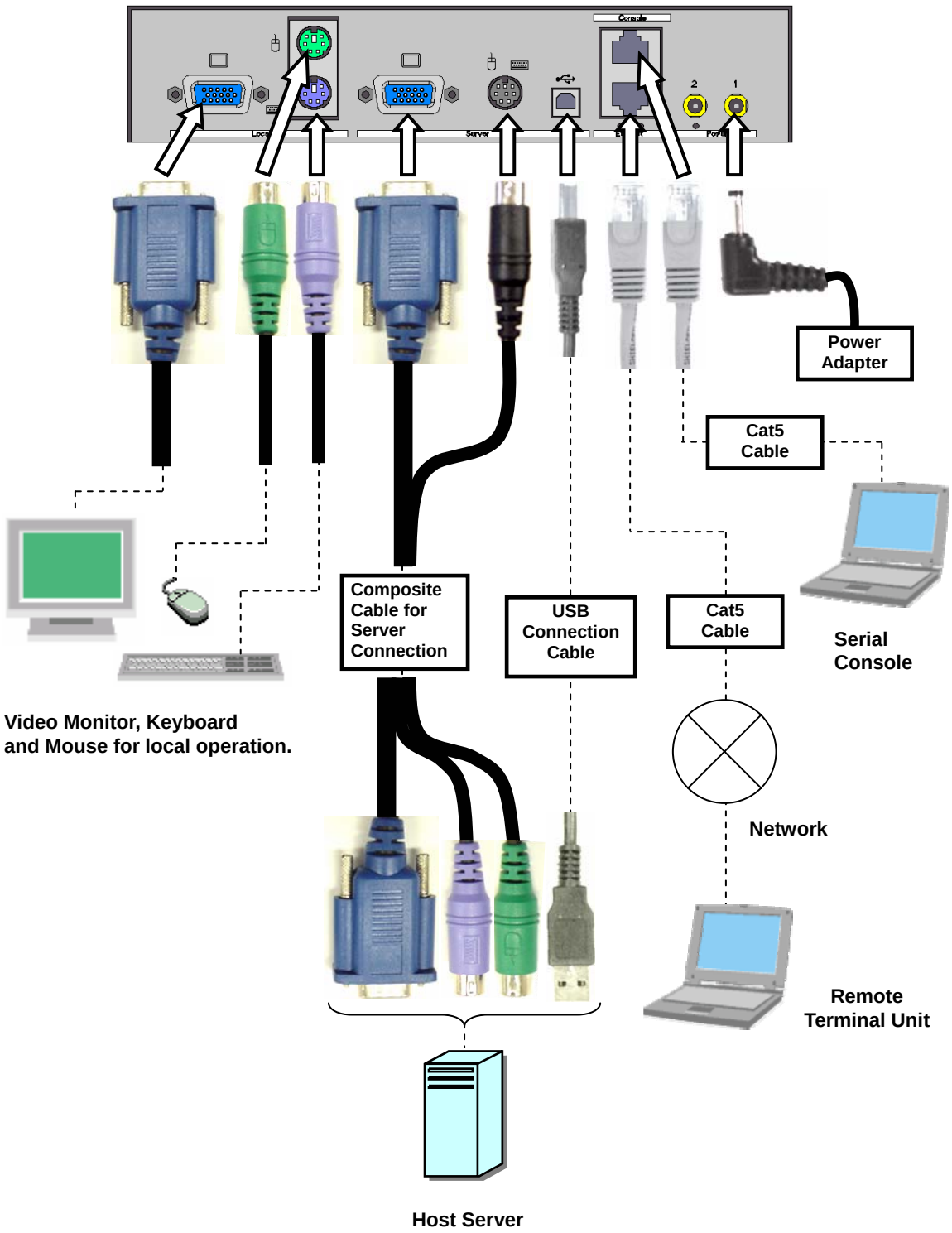
Prepare the routers and switching hubs for network connection.

(7) Remote Terminal Unit

Prepare a PC that supports an Ethernet connection.
A terminal device to operate the host server from a remote location.
An environment that Java applet runs on is needed. Any OS and browser are acceptable.

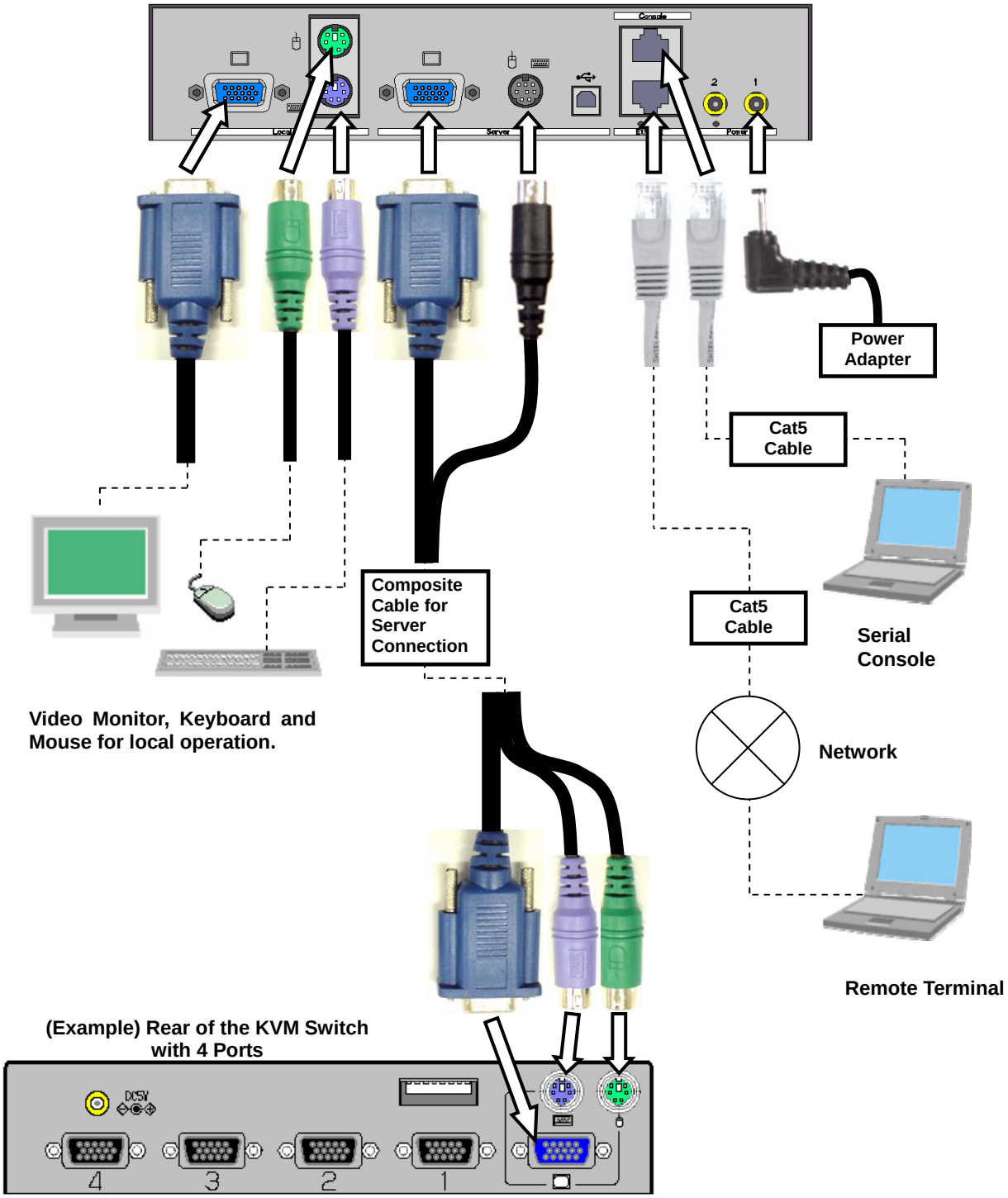
1.5.2 Connection to the Host Server

Connect cables to this product, as shown below.



1.5.3 KVM Switch Connection

When you combine our KVM switch and this product, connect the cables as shown below. Connect the KVM cable to the local port in the KVM switch side.

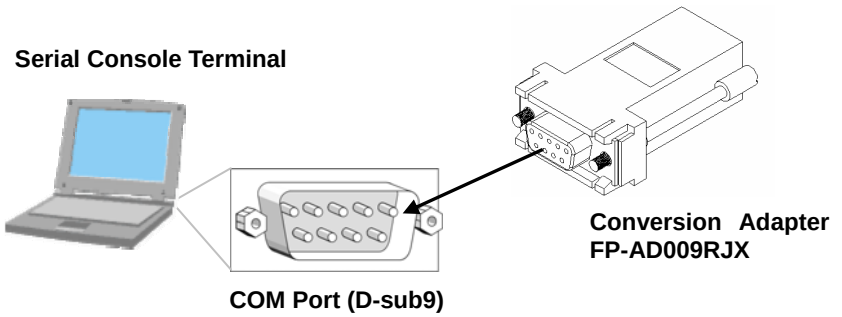


1.5.4 Serial Console Connection

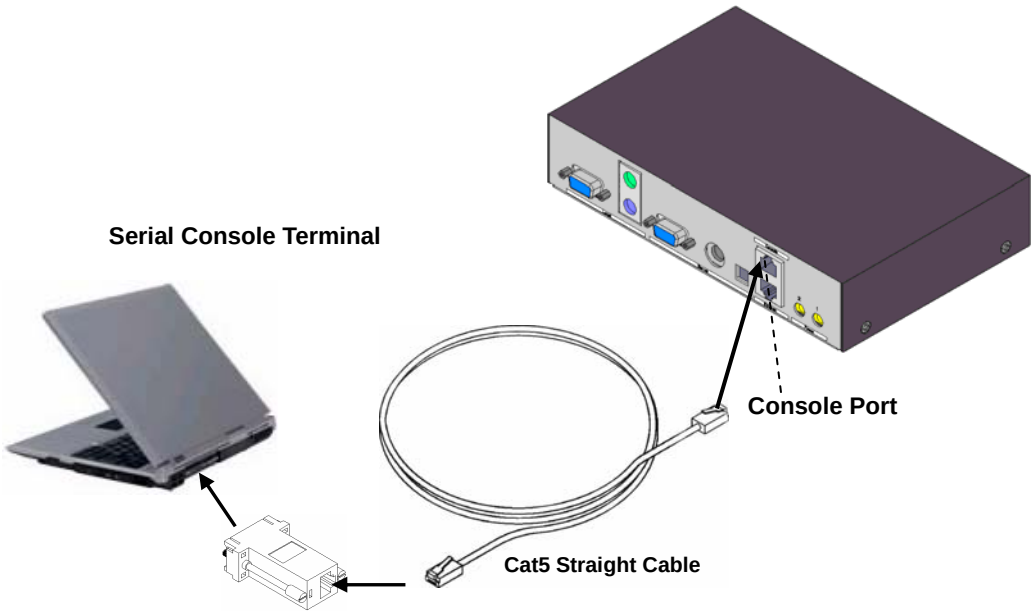
If the COM port of serial console has a D-sub 9-pin or D-sub 25-pin connector, the serial console can also be connected to this product with the optional D-sub–RJ45 conversion adapter and commercially available Cat5 straight cable.

FP-AD009RJX	The conversion adapter to configure RS-232C cross cable by combining Console port and Cat5 straight cable. D-Sub side is female 9-pin.
FP-AD025RJX	The conversion adapter same as FP-AD009RJX, but its D-Sub side is male 25-pin.

1. Connect the **FP-AD009RJX** conversion adapter (for D-sub9) to the serial console.



2. Connect the conversion Adapter hooked up in Step1 and Console port of this product by a Cat5 cable.



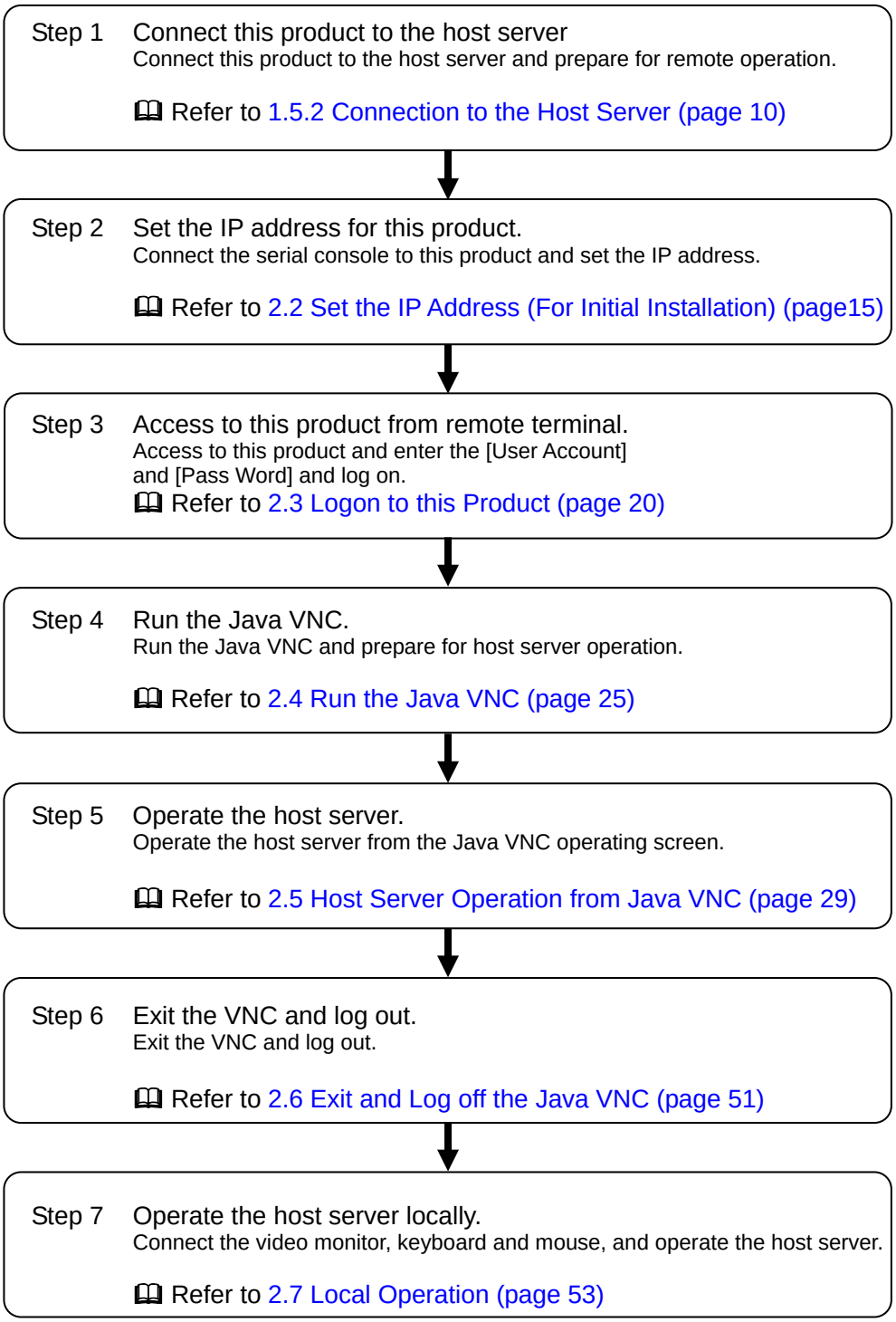
Chapter 2 - Basic Operation

This chapter provides basic operating procedure to control the host server from a remote location via network with this product.

Contents

2.1. Basic Operation Flow

The following provides the basic operating procedure to control the host server from a local or remote location via network with this product.



2.2. Set the IP Address (For Initial Installation)

Set the IP address for this product using serial console at initial setting. The operation method is described below.

1. Connect the console port of this product and the serial console terminal.
   🕮 Refer to 1.5.4 Serial Console Connection (page 12)

2. Run the emulator application (Tera Term, etc.) at the serial console and specify the parameter as follows.

Condition for Communication	Value
Baud Rate	115200bps
Data Length	8bit
Parity	none
Stop Bit	1bit

3. The “login:” prompt is displayed. Enter the default administrator account: admin.

```
login: admin Enter↵
```

4. The “password:” prompt is displayed. Enter the default admin password: admin (The password is not displayed)

```
login: admin Enter↵

password:     Enter↵
```

5. The following set up menu is displayed.

```
--------------------------
SERVIS IP-KVM Network Setup
--------------------------

NOTE: This interface is used to set network parameters and perform
certain recovery procedures, but the majority of setup and
configuration can only be done using the web interface.

Primary Ethernet Port (LAN)    (00:0e:00:ee:04:03)
  DHCP is enabled. Current lease information:
  IP Address: 192.168.0.2
     Netmask: 255.255.255.0
     Gateway: Disabled
   Broadcast: 192.168.0.255

   Machine name: noname
Default Gateway: <none>  (DHCP: 192.168.0.1)

Commands (press one key, then Enter):
    D - Disable DHCP, and use fixed IP address.
 *  I - Set IP address.
 *  N - Set netmask.
 *  G - Set network gateway.
 *  B - Set broadcast address (optional).
    M - Change machine name (DHCP client name).
    H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
    F - Reset everything to factory defaults.
    S - Change system admin password.
    P - Send ICMP ping packets (testing purposes).
    ? - Show TCP/IP ports and servers enabled.
    V - Show Firmware Information.
    R - Revert to current settings (undo changes).
    W - Commit changes to configuration.
    Q - Logout.

 *  -> These values ignored due to DHCP.

Choice:
```

CAUTION

DHCP is enabled as the factory setting. Log on this product and be sure to specify the fixed IP address if you operate the host server from a remote location extended periods of time.

6. To assign an IP address, disable the DHCP. The “Choice:” prompt is displayed and enter “d”.

```
Choice: d Enter↵
```

7. The following is displayed and DHCP is disabled. Press the [Enter] key.

```
DHCP has been disabled.

Press Enter to continue... Enter↵
```

8. The following is displayed. Confirmed that the DHCP is disabled.

```
---------------------------
SERVIS IP-KVM Network Setup
---------------------------

NOTE: This interface is used to set network parameters and perform
certain recovery procedures, but the majority of setup and
configuration can only be done using the web interface.

Primary Ethernet Port (LAN)    (00:0e:00:ee:04:03)
    D.H.C.P.: Disabled
  IP Address: 192.168.0.2
     Netmask: 255.255.255.0
     Gateway: Disabled
   Broadcast: 192.168.0.255

   Machine name: noname
Default Gateway: <none>

Commands (press one key, then Enter):
    D - Enable DHCP for dynamic IP address.
    I - Set IP address.
    N - Set netmask.
    G - Set network gateway.
    B - Set broadcast address (optional).
    M - Change machine name (DHCP client name).
    H - Reset/disable firewall, TCP ports, SNMP, RADIUS.
    F - Reset everything to factory defaults.
    S - Change system admin password.
    P - Send ICMP ping packets (testing purposes).
    ? - Show TCP/IP ports and servers enabled.
    V - Show Firmware Information.
    R - Revert to current settings (undo changes).
>>> W - Commit changes to configuration.
    Q - Logout.

    NOTE: Your changes are still pending.

Choice:
```

9. Specify the IP address. Enter "i" in the “Choice:” prompt.

```
Choice: i Enter↵
```

10. Current IP address is displayed in square bracket. Enter the new IP address and press the [Enter] key.

```
IP Address [192.168.0.8]: 192.168.0.100 Enter↵
```

11. Specify the subnet mask. Enter "n" in the “Choice:” prompt.

```
Choice: n Enter↵
```

12. Current subnet mask is displayed in square bracket. Enter the new subnet mask and press the [Enter] key. Press the [Enter] key if the subnet mask is not changed.

```
Netmask [255.255.255.0]: 255.255.255.0 Enter↵
```

13. Specify the default gateway. Enter "g" in the “Choice:” prompt.

```
Choice: g Enter↵
```

14. Current default gateway is displayed in square bracket. Enter the new IP address of default gateway and press the [Enter] key.

```
Default gateway (or 0.0.0.0 for none) [0.0.0.0]: 192.168.0.1 Enter↵
```

15. The “Choice:” prompt is displayed again. Enter "w" to save the new setting.

```
Choice: w Enter↵
```

16. The following is displayed and the setting is changed.

```
Writing... Done.
Applying settings...
eth0: IBM EMAC: link up, 100 Mbps Full Duplex, auto-negotiation complete.
eth0: IBM EMAC: MAC 00:0e:00:ee:04:03.
eth0: IBM EMAC: open completed

SNMP agent started.
Redir Server started (br0/eth0=80, eth1=0).
rhub: No such file or directory
VNC Server: Version V1L20ES
Done.

Changes commited.

Press Enter to continue...
```

17. Press the [Enter] key again after the setting and display the “Choice:” prompt. Enter "q" to log off. The “login:” prompt is displayed after the log off.

```
Choice: q Enter↵

login:
```

Then the network setting is changed as following value.

IP address:	192.168.0.100
Subnet mask:	255.255.255.0
Default gateway:	192.168.0.1

This is the operation method to change network initial settings.

The following table shows the items can be specified from the serial console.

Command	Items
D	Switches enable/disable the DHCP setting.
I	Set the IP address.
N	Set the subnet mask.
G	Set the default gateway.
B	Set the broadcast address.
M	Set the device name.
H	Reset/disable the Firewall and TCP port settings.
F	Reset to the factory default.
S	Set the system administrator password.
P	Transmit the ICMP ping packet.
?	Display the TCP/IP port and the server.
V	Display the firmware information.
R	Reset to the former settings.
W	Save the current settings.
Q	Logs off the menu.

CAUTION

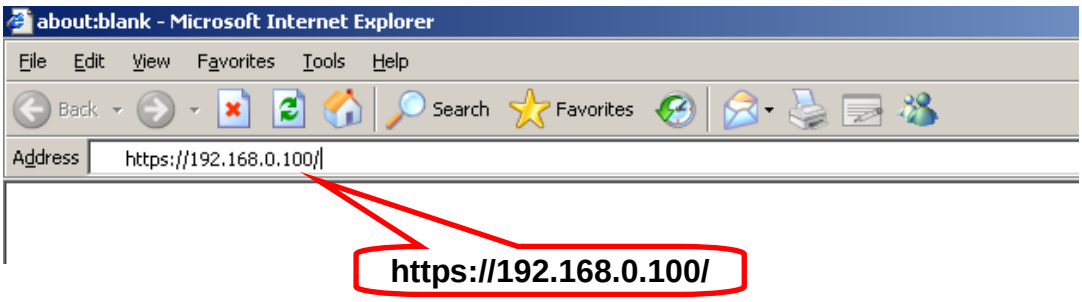
Set the IP address of this product, net mask and default gateway at initial installation.

2.3. Logon to this Product

The following describes how to log on to this product from a remote terminal.

1. Start up the browser at the remote terminal and access to the specified IP address of this product by https protocols. (The following provides the procedure for Microsoft Internet Explorer 6.0.)

   This product is set as follows.
   - IP Address: 192.168.0.100
   - Subnet mask: 255.255.255.0
   - Default Gateway: 192.168.0.1



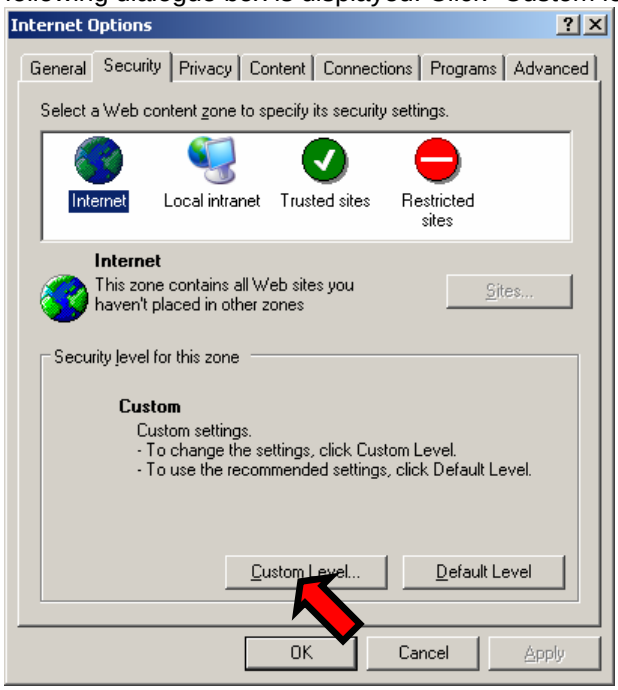
2. The [Security Alert] dialogue box is displayed. Click [Yes] button.

3. If JavaScript is disabled in the browser setting, the following [Language Select] page is displayed. If JavaScript is disabled, this product does not operate properly.Please enable your JavaScript and click English or Japanese.
   If JavaScript is enabled, the [Language Select] page is not displayed.Refer to the next section 4.

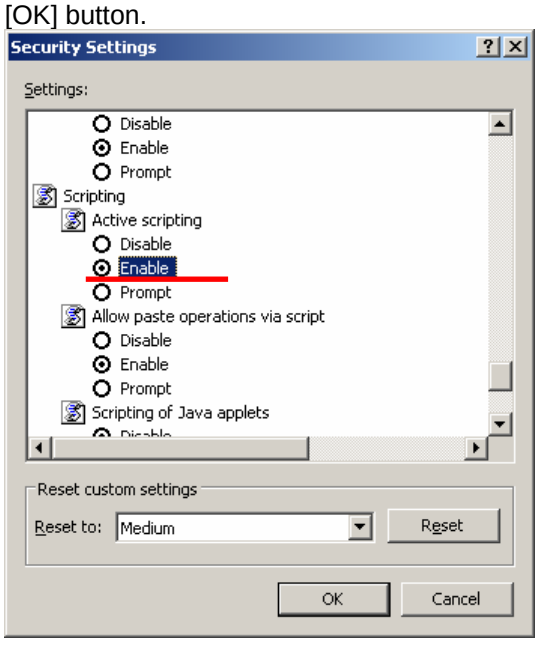
Setting procedure of enabled JavaScript.

For Internet Explorer 6.0

Click [Tools] menu → [Internet Options] → [Security] tab and the following dialogue box is displayed. Click "Custom level" button.

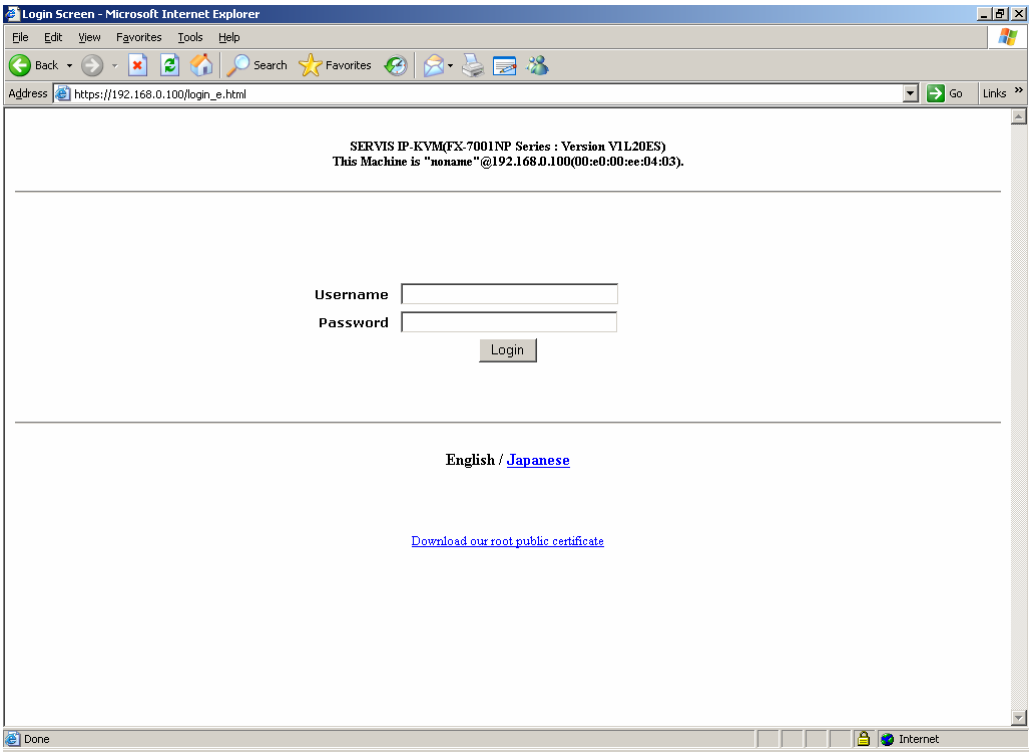


The following [Security settings] setting is displayed.
Check the under Scripting category enable Active Scripting, and click [OK] button.



The following [Warning] dialogue box is displayed. Click [Yes] button.
Then JavaScript is enabled.

4. The web page login screen is displayed. Click English or Japanese on the center of the screen to switch the language.
   The administrator account [admin] and the password [admin] are set by default. Enter [admin] for the user name and the password and click [Login] button.



Click Download our root public certificate and you can download the security certificate.

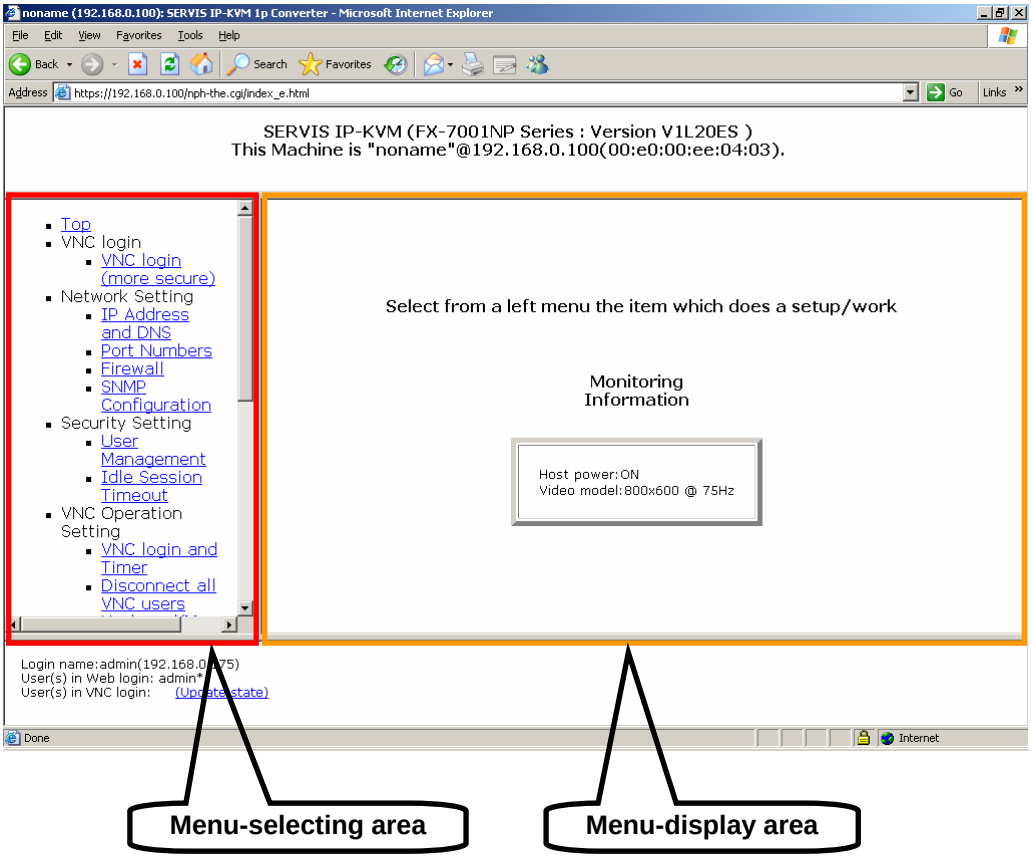
CAUTION

If cookie is disabled, you can't login to the setting page. Please enable cookie and click [Login] button.
🕮 Refer to 5.1.6 Cannot Login to the Setting Page (page146)

5. The following screen is displayed. Click the menu from the menu selection in the left and the selected contents are displayed in menu display area in the right. The server information is displayed in the menu display area in the top page. It is possible to confirm power status (on/off) and the video mode (screen resolution and refresh-rate) of the connected host server.

   All management/setting for this product, besides the IP address setting in the initial installation can be specified in this web page. Log on with administrator account to specify/manage this product.

   🕮 Refer to 3.1 Network Setting (page 56)



2.4. Run the Java VNC

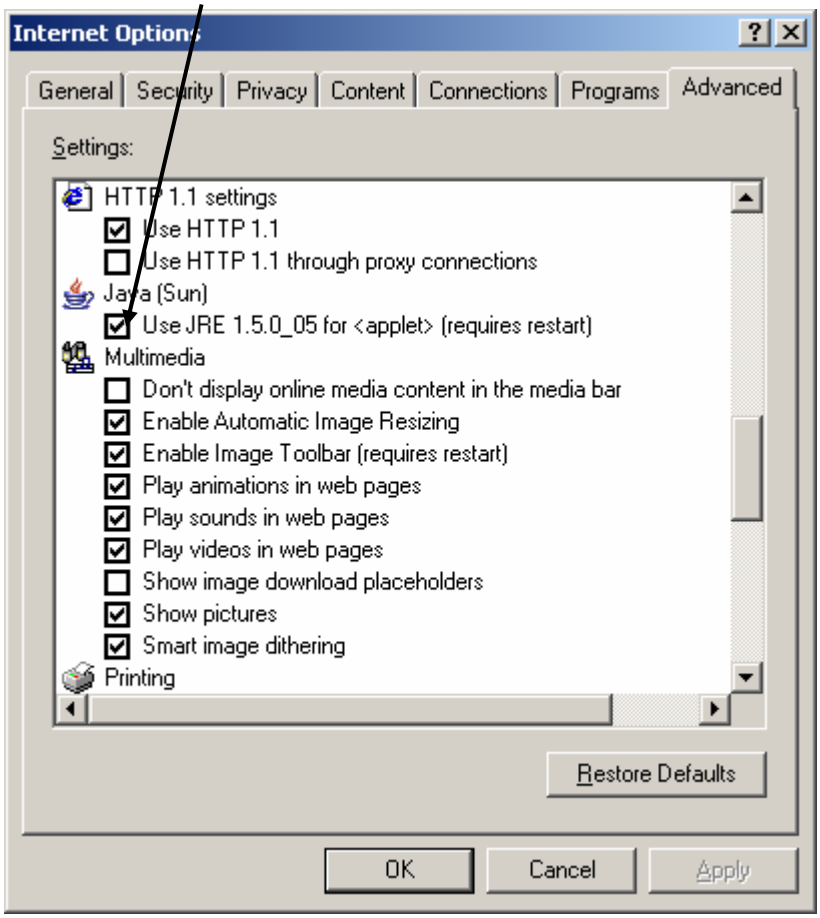
It is necessary to run the Java VNC to operate the host server after logging on from the remote terminal.

CAUTION

Confirm whether the Sun Java applet is installed or not in the remote terminal to run the Java VNC.

For Internet Explorer:

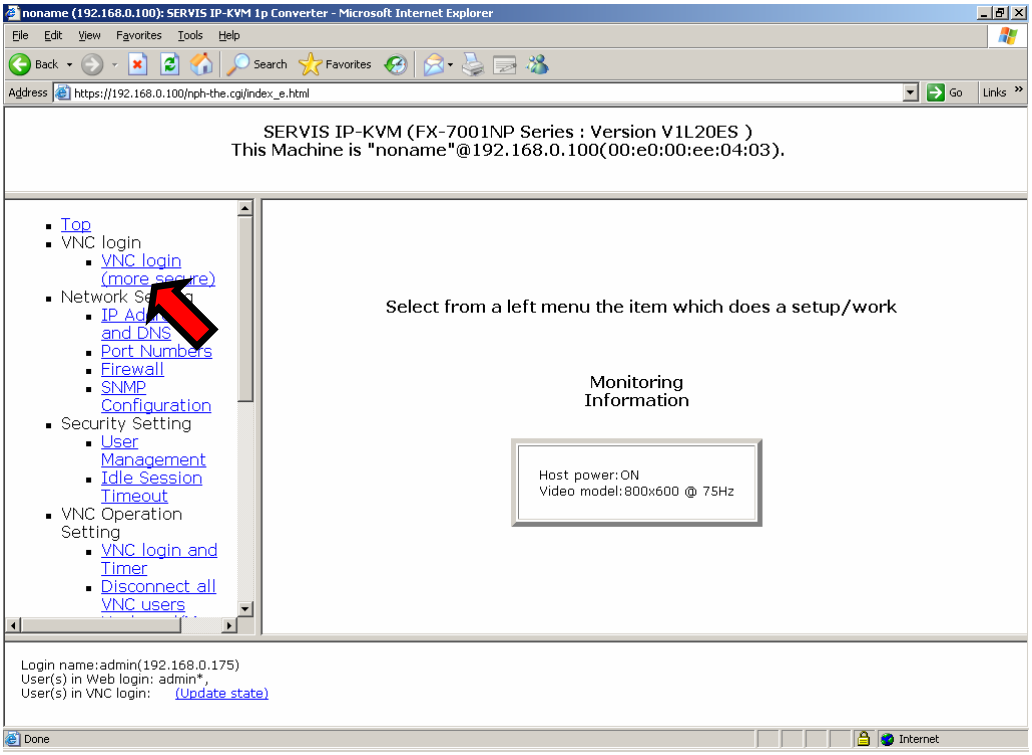
Click [Tools] menu → [Internet Options] → [Advanced] tab. Make sure that Java Sun [Use JRE 1.x.x._xx for <applet> (requires restart)] is checked. (x is version No.)



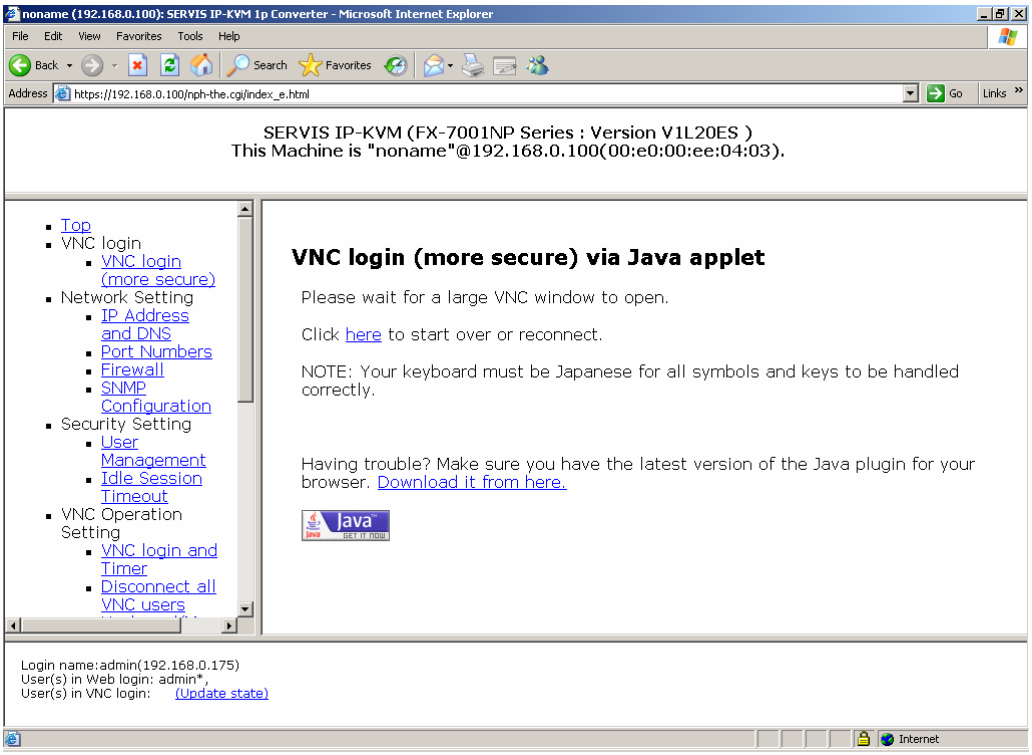
If not,

Download Java software in the following web site and install it.
http://www.java.com/ja/ (Download page for the Java software).

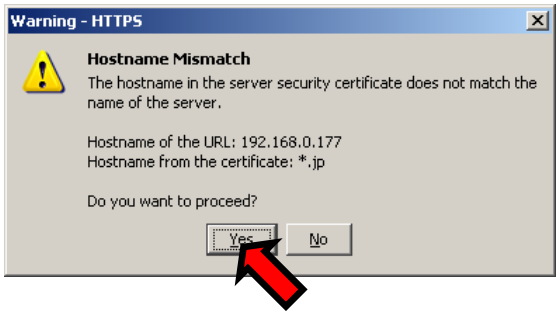
1. Click VNC login (more secure) in the menu-selecting area.



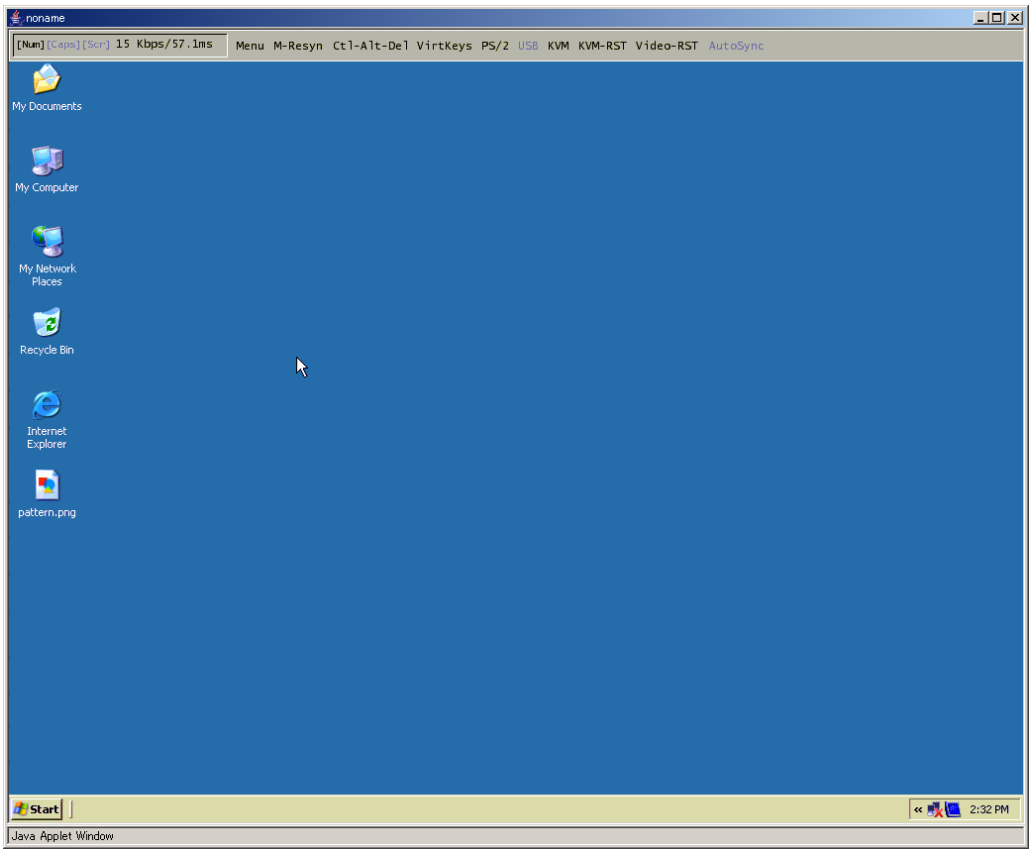
2. [VNC login (more secure) via Java applet] screen is displayed.
   If the Java applet is not installed, the screen remains the same and the Java VNC is not run. Download the latest Java software.
   (Support Java version: JRE 5.0 Update 6, J2SE v1.4.2_11 JRE)



If the Java applet is installed, the following [Warning - Security] dialogue box is displayed. Click [Yes] button. (Dialogue window depends on Java version)



3. Once the VNC window opens and the host server screen is displayed, operation is possible.



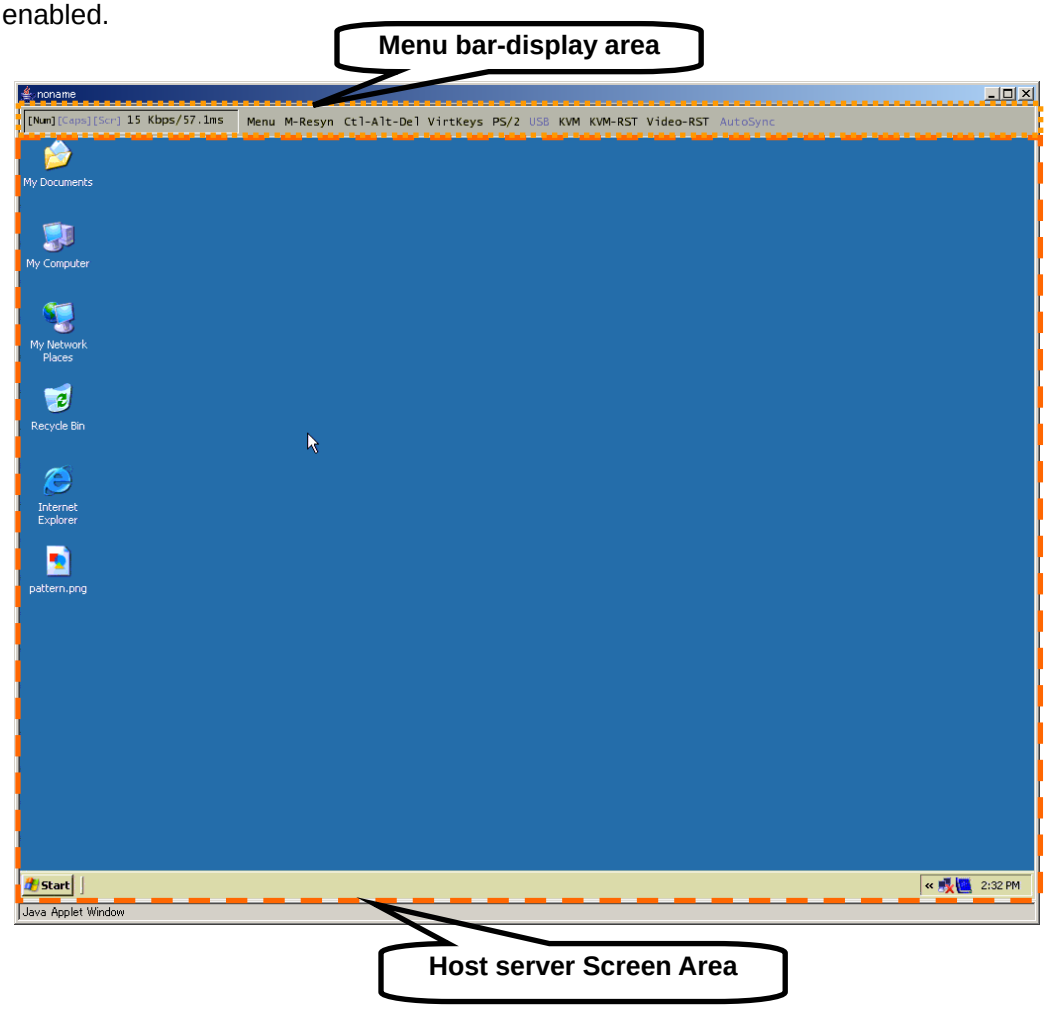
Refer to the next section for details about the VNC window.

CAUTION

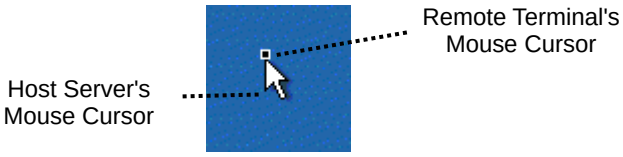
If you update the Java applet, uninstall the old version, and then install the latest version.
If you don't uninstall the old version of the Java applet and you install the latest version, this product may not operate normally.

2.5. Host Server Operation from Java VNC

Starting up VNC, the following window is displayed and the host server operation is enabled.



The black square cursor is for the remote terminal side and white arrow is for the host server side. The host server cursor follows the remote terminal cursor's movement.



CAUTION

To synchronize the remote terminal and host server cursor position, disable the acceleration setting for the host server mouse.

📖 Refer to 2.5.1 Host Server Initial Setting (page 30)

2.5.1 Host Server Initial Setting

To synchronize the remote terminal and host server cursor position, disable the [Acceleration] setting and the [Move to Default Button] setting.

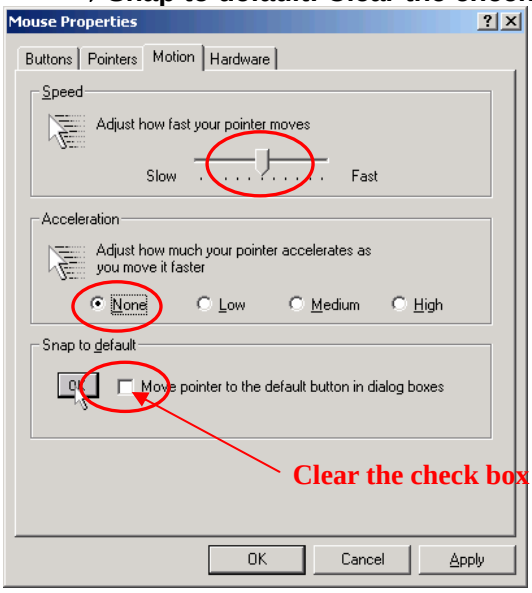
➢ For Windows OS based host servers

Click [Control Panel] - [Mouse] and display the mouse properties.

For Windows 2000

→ **Speed: Middle, Aceleration: None**

→ **Snap to default: Clear the check box**

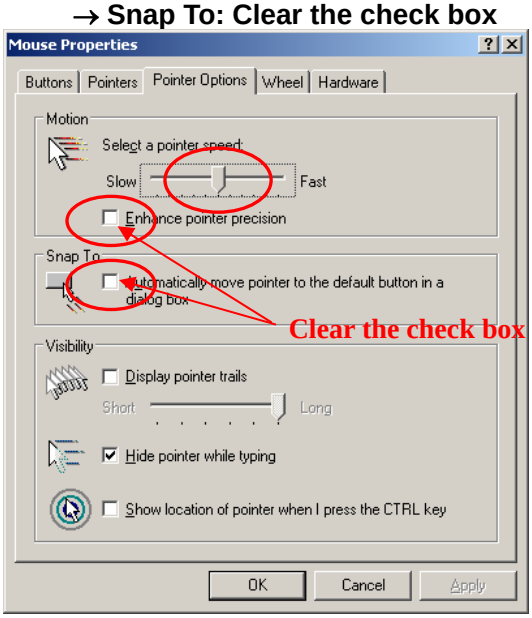


For Windows XP and Windows Server 2003

→ **Motion: Middle,**

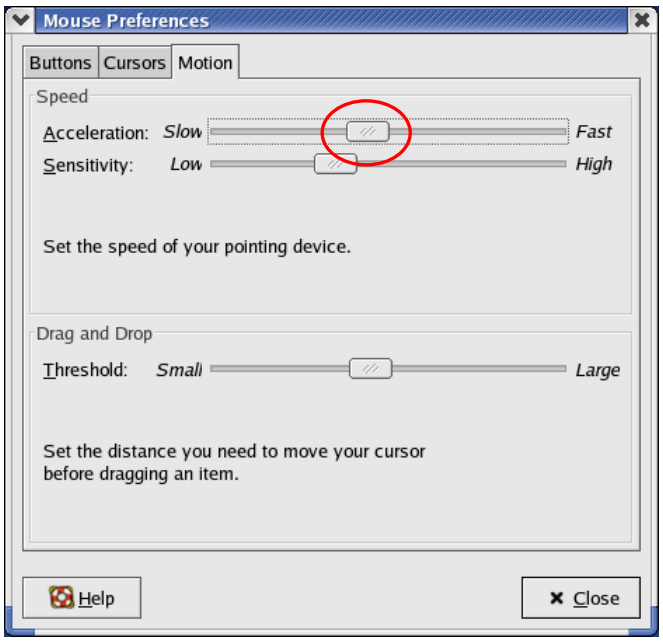
Enhance Pointer precision: Clear the check box

→ **Snap To: Clear the check box**



➢ For RedHat Linux (GNOME) Based Host Server.
Click [Preferences] - [Mouse] and display the mouse preferences.

→ Aceleration: Middle (For slowish side)

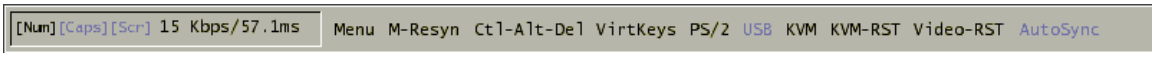


CAUTION

When PS/2 keyboard/mouse is enabled and the host server is a Windows OS, The **mouse cursor is not synchronized before login to the server.**

2.5.2 VNC Menu

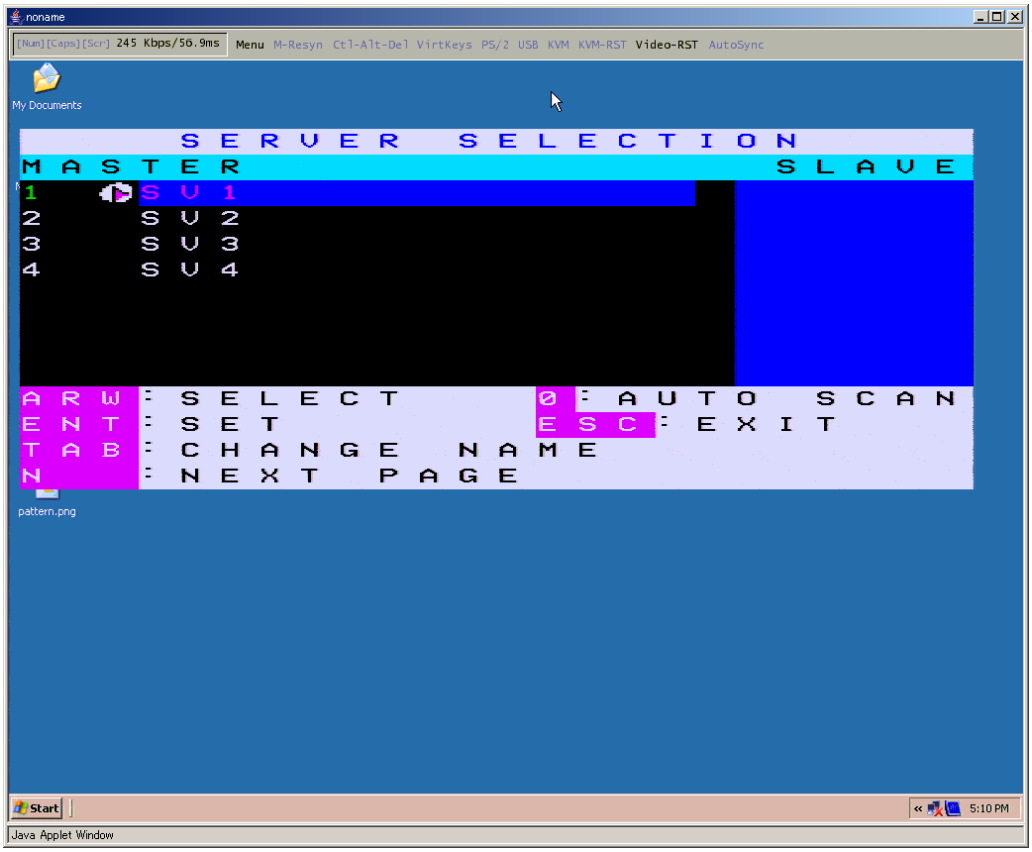
The following menu bar is displayed at the top of the VNC window.
Menu bar buttons provide various functions.



VNC Menu Bar	
[Num][Caps][Scr]	Shows the LED status from the left Num Lock, Caps Lock and Scroll Lock. If the LED off, it is displayed in gray.
15 Kbps/57.1ms	Shows current transmission capacity (baud rate) / delay time.
Menu	Display the menu window. 🕮 Refer to 2.5.3 Menu Window (page 34)
M-Resyn	Correct the difference between host server side and remote terminal side mouse pointers position. If the USB absolute mouse enabled, the button cannot be selected. 🕮 Refer to 3.3.3.4 Disable USB Absolute Mouse Support (page 88)
Ctl-Alt-Del or Strg-Alt-Entf	Input [Crtl] - [Alt] - [Delete] key to the host server. Ctl-Alt-Del button is displayed if you select "Generic or US/English" or “Japanese (106/109 keys)” in [Keyboard Mapping (for localization)]. Strg-Alt-Entf button is displayed if you select “German (QWERTZ layout)” in [Keyboard Mapping (for localization)]. 🕮 Refer to 3.3.3.2 Keyboard Mapping (for localization) (page86)
VirtKeys	Display the virtual key window. 🕮 Refer to 2.5.5 Virtual Key Window (page 38)
PS/2	Reset the PS/2 emulation. Use this button in case the mouse pointer or PS/2 keyboard is disabled. If the USB keyboard/mouse enabled, the button cannot be selected.
USB	Display the USB menu window. If the device is not connecting to the host server by USB cable, the button cannot be selected. 🕮 Refer to 2.5.9 USB Setting Window (page 47)
KVM	If using with a KVM switch, output the specified hot keys to the KVM switch. It is not displayed in default. The button is displayed if you select other than "Disable" in [Hot Key configuration of FCL KVM Switch]. (Refer to ‼ REF _Ref118884558 ¥r ¥h ┌ ¥* MERGEFORMAT ¶ 3.3.3.1⊥ ‼ REF _Ref118884562 ¥h ┌ ¥* MERGEFORMAT ¶ Hot Key configuration of FCL KVM Switch (page 85)
KVM-RST	If using with a KVM switch, reset the KVM switch. It is not displayed in default. The button is displayed if you select other than "Disable" in [Hot Key for FCL KVM Switch setting]. 🕮 Refer to 3.3.3.1 Hot Key configuration of FCL KVM Switch (page 85)
Video-RST	Update the host server display area.
AutoSync	Indicates the mouse pointer's automatic correction function. Click this indication to enable/disable the function. If the function disabled, the indicator is displayed in gray.

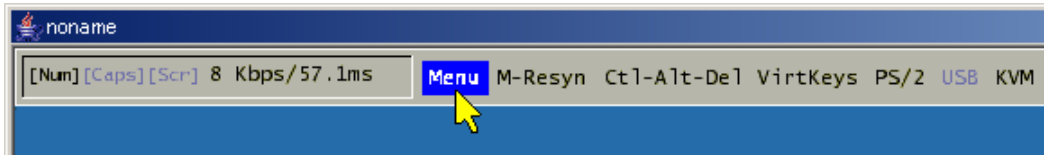
If you use this product with a KVM switch, click [KVM] button. The following OSD screen is displayed.
(The following diagram shows the combination with SERVIS Multi and FS-1004MT).

Select the number by cursor ↑ or ↓ and press the Enter key. Host servers connected to the selected port are displayed and operation is enabled.

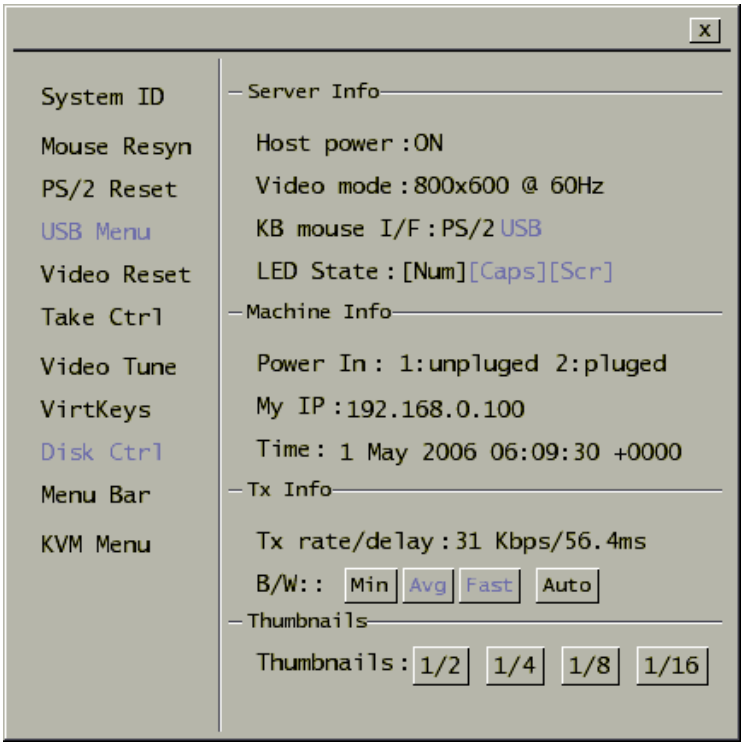


2.5.3 Menu Window

Press the F7 key twice or click [Menu] button in VNC menu bar, following menu window is displayed.



This menu window provides various VNS connection settings.

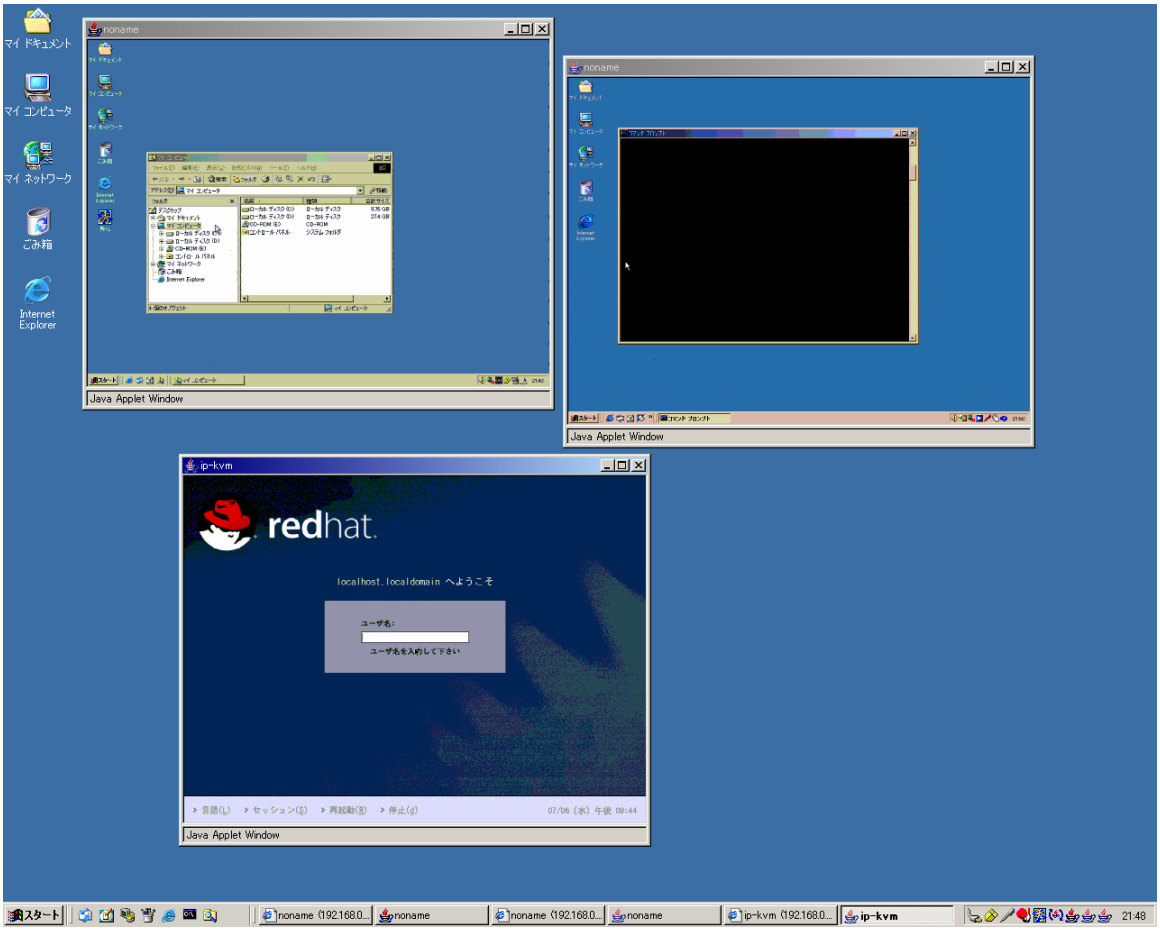


The following table shows the details about the menu window.

Operation Selecting Area (Left of the menu window)	
System ID	Displays the specified system information. 🕮 Refer to 3.4.1 Identification (page 114)
Mouse Resyn	Synchronises the remote terminal and host server cursor position. If the USB absolute mouse is enabled, the button is displayed in gray. 🕮 Refer to 3.3.3.4 Disable USB Absolute Mouse Support (page 88)
PS/2 Reset	Reset the PS/2 emulation. Use this button in case the mouse pointer or PS/2 keyboard is disabled.
USB Menu	Display the USB menu window. If the device is not connected to the host server by USB cable, the button is displayed in gray. 🕮 Refer to 2.5.9 USB Setting Window (page 47)
Video Reset	Update the host server display area.
Take Ctrl	When multiple users connect to the same system and the other user establishes the control authority, takes control authority from the user. Only one user can operate by keyboard and mouse. 🕮 Refer to 3.8 Concurrent Connection of Network Users (page 136)
Video Tune	Displays the Video Tune window for fixing the video image. It is used when video tuning is performed manually. 🕮 Refer to 2.5.6 Video Tune Window (page 41)
VirtKeys	Displays the virtual keyboard that provides special key (Control-Alt-Delete, etc.) for the host server. 🕮 Refer to 2.5.5 Virtual Key Window (page 38)
Disk Ctrl	Displays the disk operation window to emulate the USB virtual disks. 🕮 Refer to 2.5.7 Disk Operation Window (page 45)
Menu Bar	Switches display/hide the menu bar at the top of the VNC window.
KVM Menu	Displays the KVM menu window. 🕮 Refer to 2.5.10 KVM Menu Window (page 49)
Close	Closes the menu window

Setting Display Area (Right of the menu window)	
Host power:	If the host server is on: On is displayed, if the host server is off: Off is displayed.
Video mode:	Displays the graphic mode setting for host server. (Example: 800 x 600 @ 60Hz) If the host server is off: No power is displayed.
KB mouse I/F:	Displays the host server keyboard and mouse are connected whether PS/2 or USB.
LED State:	Displays keyboard LED is on/off. (If the LED is off, the menu is displayed in gray). Indicates each LED status, [Num] for NumLock, [Caps] for CapsLock, and [Scroll] for ScrollLock.
Power In:	Displays the connecting status of the product's power port 1 and 2. If the power port is connected, "plugged" is displayed and "unplugged" for unconnected status.
My IP:	Displays the IP address.
Time:	Displays the specified current date and time.
Tx rate/delay:	Displays current network transmission rate and delay time.
B/W:	Specify the bandwidth control. Specify Fast: for less than 12Mbps, Avg for less than 4Mbps, and Min for less than 700kbps.
	Select "Auto" for this setting, appropriate setting is automatically selected.
Thumbnails:	Resizes the screen image from half size down to one sixteenth by clicking [1/2]. [1/4], [1/8] and [1/16]. Restore the image to the original size by clicking the screen.

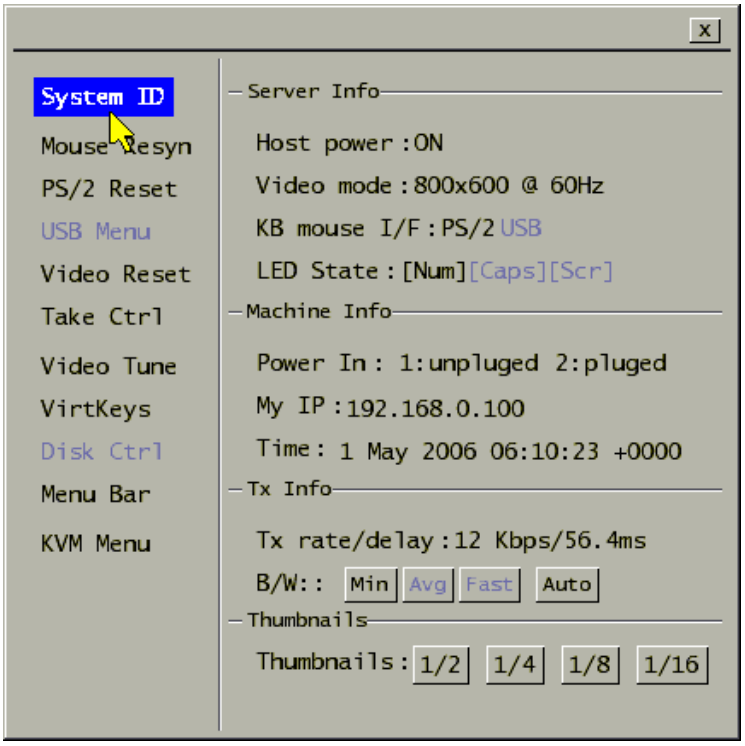
If multiple products are set up on the same network, each VNC screens is displayed as small thumbnail images. (Select the size from [1/2], [1/4], [1/8] or [1/16] in the menu window).
This function allows control of multiple host servers.



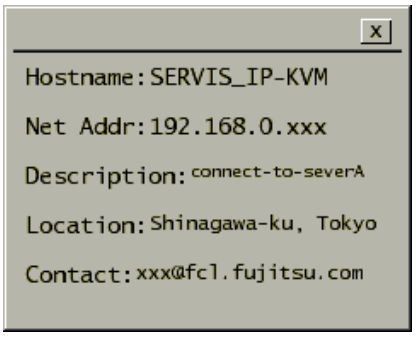
Restore the image by clicking the thumbnail screen.

2.5.4 System ID Window

Click [System ID] in the menu window and the following system ID window is displayed.



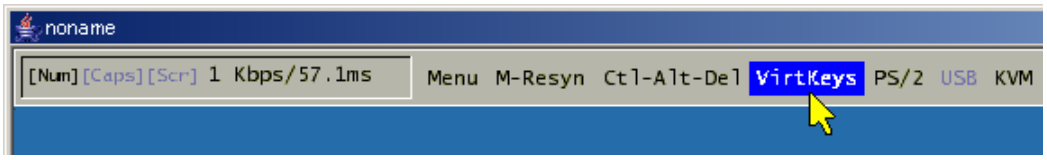
Display the system ID of this product specified in Identification in the web site.
🕮 Refer to 3.4.1 Identification (page 114)



System ID Window	
Hostname:	Display the ID of this product.
Net Addr:	Display the user-defined value; the DNS name for console, etc.
Description:	Display the user-defined construction for controlled devices.
Location:	Display installation site of this product.
Contact:	Display the contact information; mail addresses relating to this product, etc.

2.5.5 Virtual Key Window

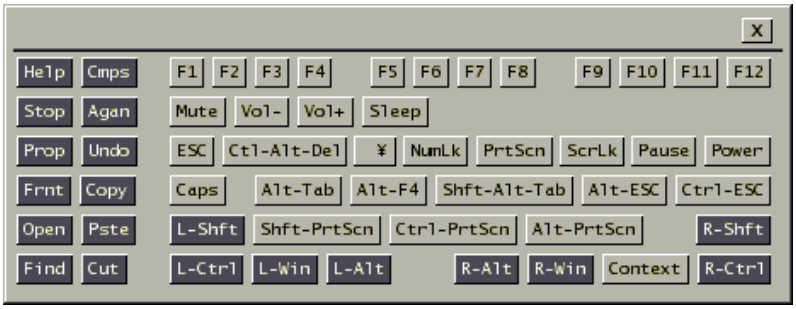
Click [VirtKeys] from the VNC menu bar or click [VirtKeys] in the menu window, virtual key window is displayed.



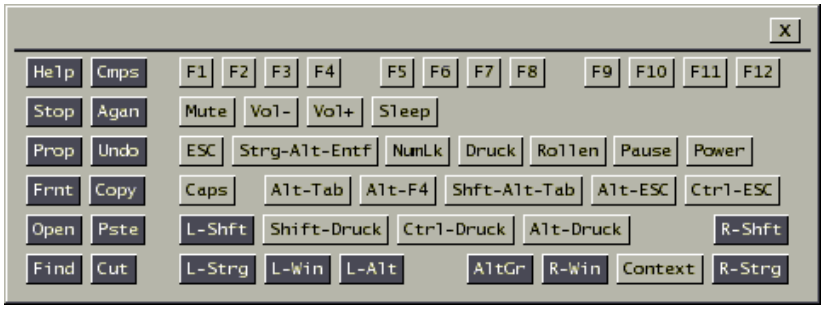
This window provides specific keys, which cannot be directly input into the host server from the remote terminal unit (Ctrl + Alt + Del for example).

The layout of the virtual key window changes by "Keyboard Mapping" setup of the Web page.
📖 Refer to 3.3.3.2 Keyboard Mapping (for localization) (page86)

- The case of ”Generic or US/English” or “Japanese (106/109 keys)”

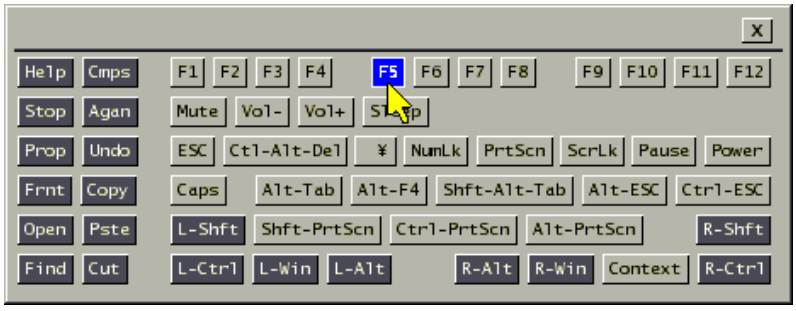


- The case of ”German (QWERTZ layout)”



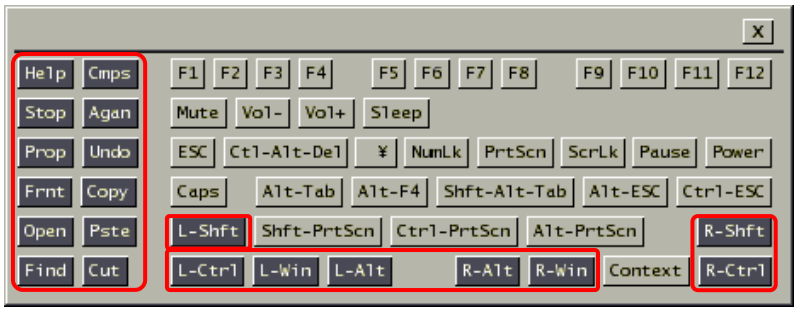
- Virtual Key Input Method

By clicking the virtual keys, the items in the square frame are input to the host server.

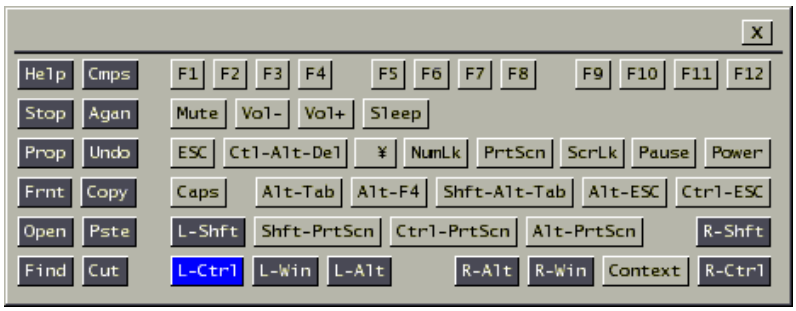


- Usage of the Toggle Keys

The keys of the dark gray surrounded in the red in the virtual key window shown below show the toggle keys. By clicking the toggle key in the virtual key window, the key becomes a toggle key in the host server.



The diagram below shows the [L-Ctrl] button clicked in the virtual key window and the key in toggle status.



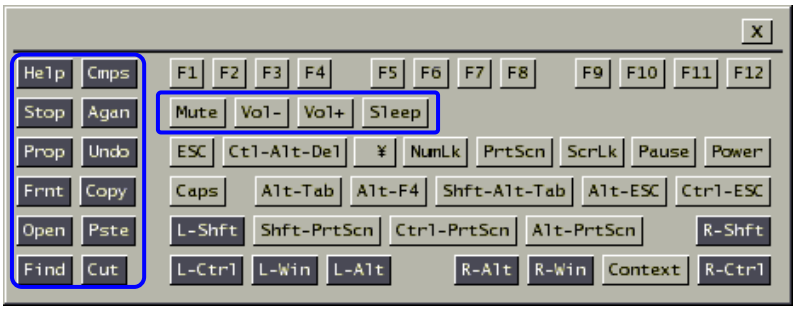
Switch focus from the virtual key window and enter "a" from the keyboard in this status, will transmit the "L-Ctrl + a" command to the host server.
Click [L-Ctrl] button in the virtual key window again, the toggled status is deactivated and the button becomes normal.

CAUTION

Switch focus from the virtual key window to enter commands to the host server from the keyboard.

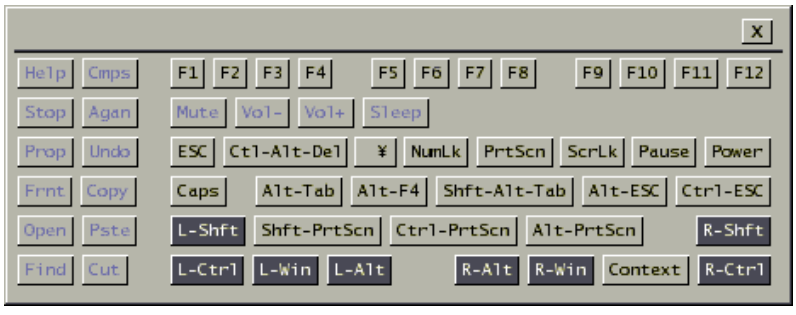
- Virtual Keys for Sun PC

The key surrounded in the blue in the virtual key window shown below is a key corresponding to a Sun keyboard.



Key	Contents
Mute	Input [Mute] key to the host server.
Vol-	Input [Vol-] key to the host server.
Vol+	Input [Vol+] key to the host server.
Sleep	Input [Sleep] key to the host server.
Help	Input [Help] key to the host server. (Toggle Key)
Cmps	Input [Compose] key to the host server. (Toggle Key)
Stop	Input [Stop] key to the host server. (Toggle Key)
Again	Input [Again] key to the host server. (Toggle Key)
Prop	Input [Props] key to the host server. (Toggle Key)
Undo	Input [Undo] key to the host server. (Toggle Key)
Frnt	Input [Front] key to the host server. (Toggle Key)
Copy	Input [Copy] key to the host server. (Toggle Key)
Open	Input [Open] key to the host server. (Toggle Key)
Pste	Input [Paste] key to the host server. (Toggle Key)
Find	Input [Find] key to the host server. (Toggle Key)
Cut	Input [Cut] key to the host server. (Toggle Key)

These keys are displayed in gray if you connect by PS/2 and select "Disable" in [Hot Key configuration of FCL KVM Switch].
📖 Refer to 3.3.3.1 Hot Key configuration of FCL KVM Switch (page85)



Click [X] button to close the virtual key window.

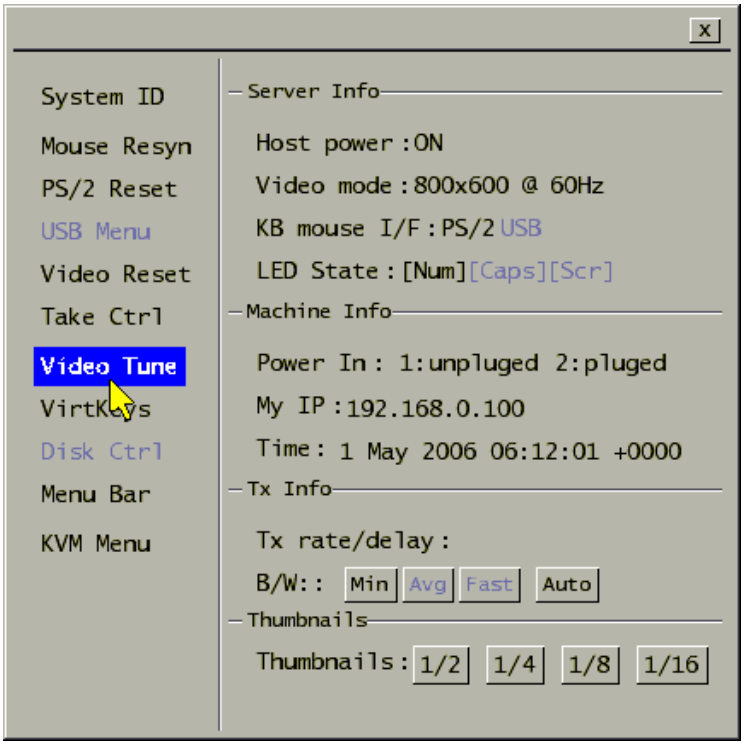
CAUTION

Even if the Ctrl + Alt+ Del key is entered from the remote PC, the command is not transmitted to the host server.
Click [Crtl + Alt + Del] key from virtual key window to command the host server.

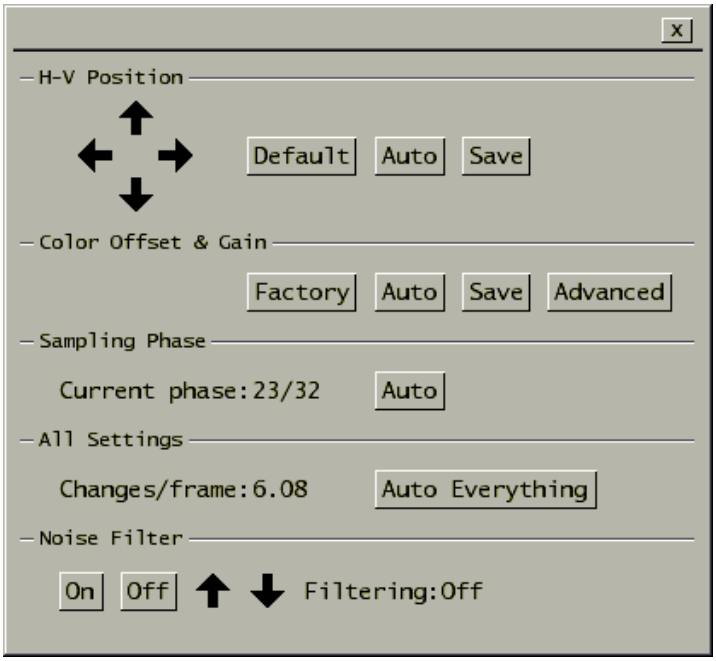
2.5.6 Video Tune Window

Click [Video Tune] in the menu window and the following Video Tune window is displayed. Refer to the following chapter for details about Video Tunes.

📖 Refer to 5.1.13 Increase Image Quality (page 156)



Use this window to fix the video images.



The following table provides description for every particular item in the window.

H-V Position	
←	Moves the host server screen to the left.
→	Moves the host server screen to the right.
↑	Moves the host server screen to the top.
↓	Moves the host server screen to the bottom.
Default	Moves the host server screen to the default position.
Auto	Automatically corrects the display position in the host server display area.
Save	Saves the current host server screen position,

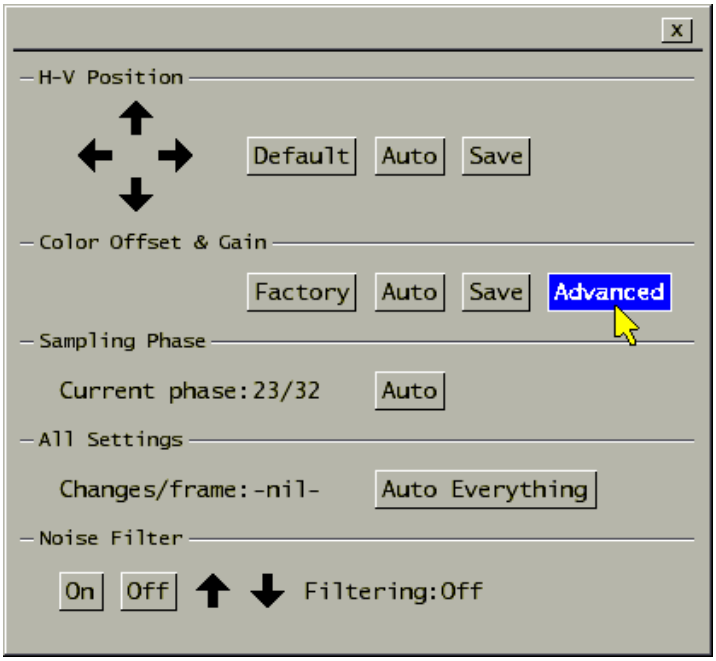
Color Offset & Gain	
Factory	Back to the factory default setting.
Auto	Automatically corrects the Color Offset value based on the test pattern.
Save	Saves the current Color Offset value.
Advanced	Displays the advanced settings screen for the video image and enables to fix the value manually.

Sampling Phase	
Auto	Automatically adjusts the video signal phase.

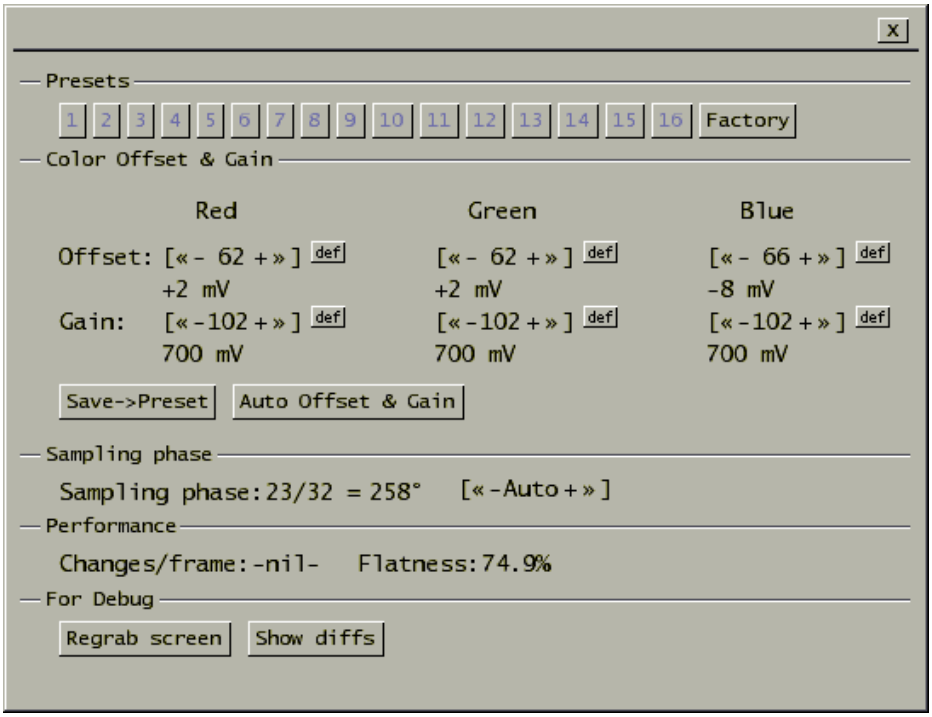
All Settings	
Auto Everything	Adjusts Picture Positioning, Color Offset & Gain, and Sampling Phase automatically.

Noise Filter	
On	Enables filtering the video signal noise.
Off	Disables the filtering function.
↑	Raise the filtering level. Click ↑ or ↓ button to adjust the filtering level.
↓	Decrease the filtering level.
x	Close the [Video Tune] screen.

Click [Advanced] button in the [Video Tune] window, the following setting window is displayed.

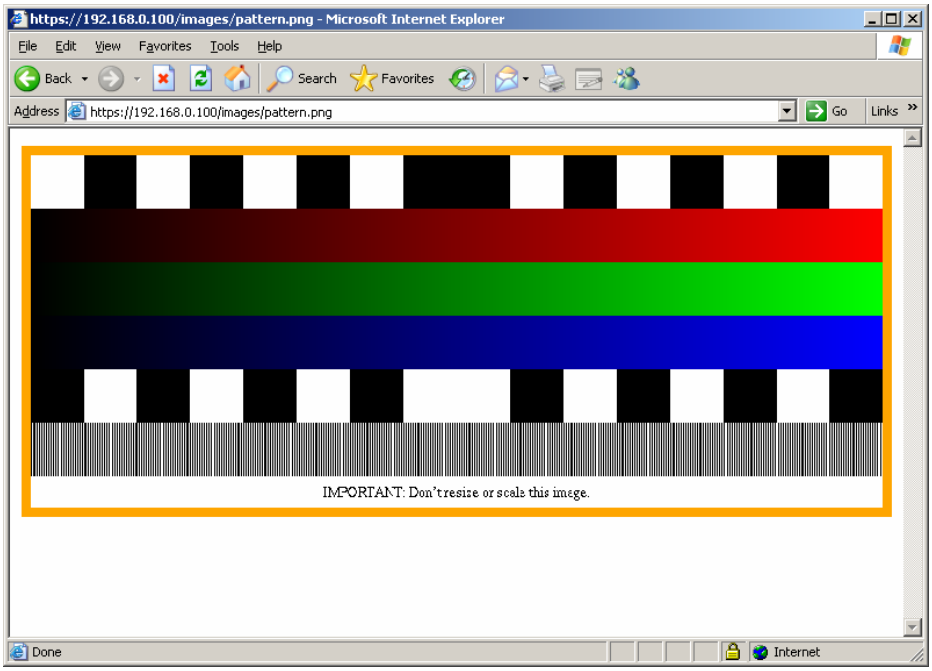


This window provides the manual advanced setting for image quality.



— Presets	
1 – 16	Save up to 16 video settings. If the setting is saved, the button is displayed. If not, the button is displayed in gray.
Factory	Changes the video setting back to the factory default settings.
— Color Offset & Gain	
Offset	Manually specify the offset.
Gain	Manually specify the gain.
def	Reset to the default setting.
Save->Preset	Click this button and presets number button; current setting is saved to the specified number.
Auto Offset & Gain	The offset and gain is automatically set.
— Sampling phase	
[« -Auto+ »]	Manually specify the sampling phase.
— For Debug	
Regrab screen	Redisplay all the parts in the screen.
Show diffs	Display the updated parts.
X	Close the advanced settings screen for the video image.

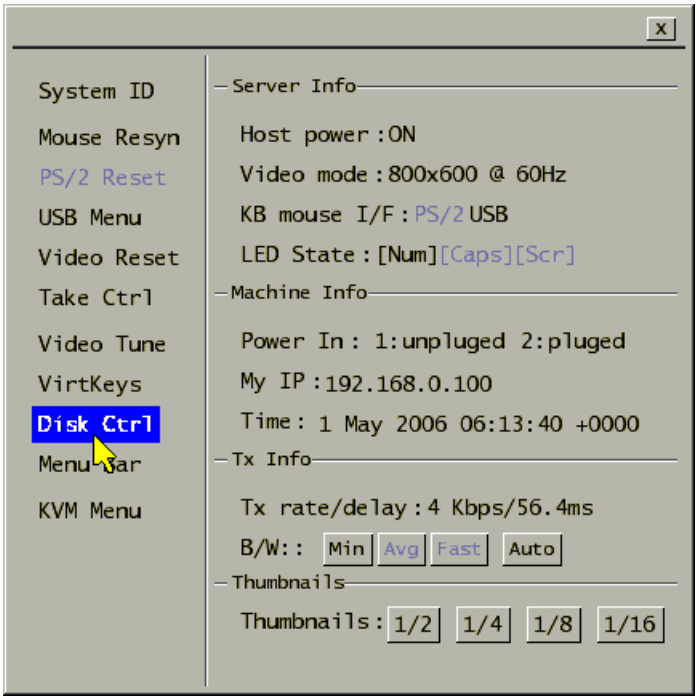
Refer to https://IP address for this product/images/pattern.png for the test pattern used in Color Offset tuning.



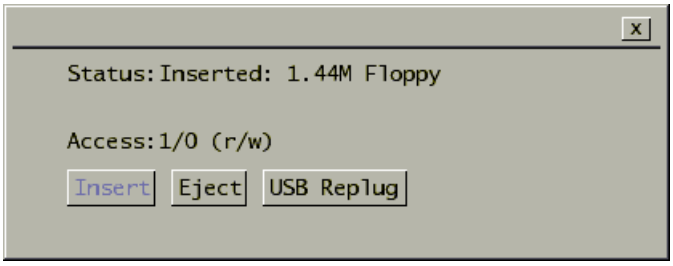
Save this test pattern in the host server as a png file.
To set the [Color Offset & Gain] in the Video Tune window, display this test pattern in the host server screen.

2.5.7 Disk Operation Window

Click [Disk Ctrl] in the menu window and the following virtual disk operation window is displayed. (It is necessary to be connected with an USB cable.)



This window displays the USB virtual disk status and whether it is inserted or ejected.

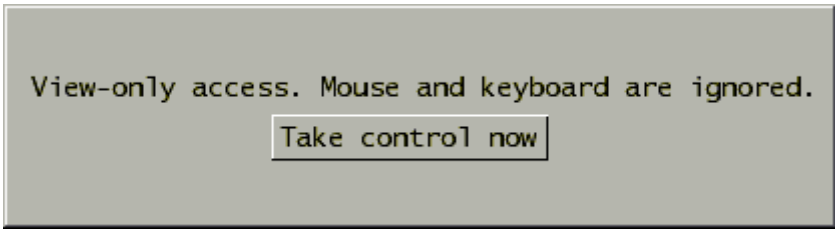


Disk Ctrl Window	
Status:	Displays whether virtual disk is inserted or ejected. Ejected: Host server does not recognize the virtual disk. Inserted: Host server recognizes the virtual disk.
Access:	Displays the USB disk type (CD-ROM, 8M RAM, and Floppy).
Insert	Inserts the virtual disk. (The menu is displayed in gray while the disk is inserted). This makes the host server recognize the virtual disk.
Eject	Ejects the virtual disk. (The menu is displayed in gray while the disk is not inserted). This makes a remote user access the virtual disk.
USB Replug	Disconnects the USB connection and connect again.
x	Closes the [Disk Operation] window.

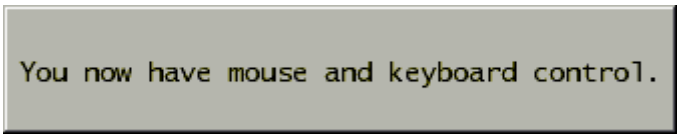
Refer to the following section for further details about the virtual disk.
📖 Refer to 3.3.4 Virtual Disk Setting (page 91)

2.5.8 Take Control Window

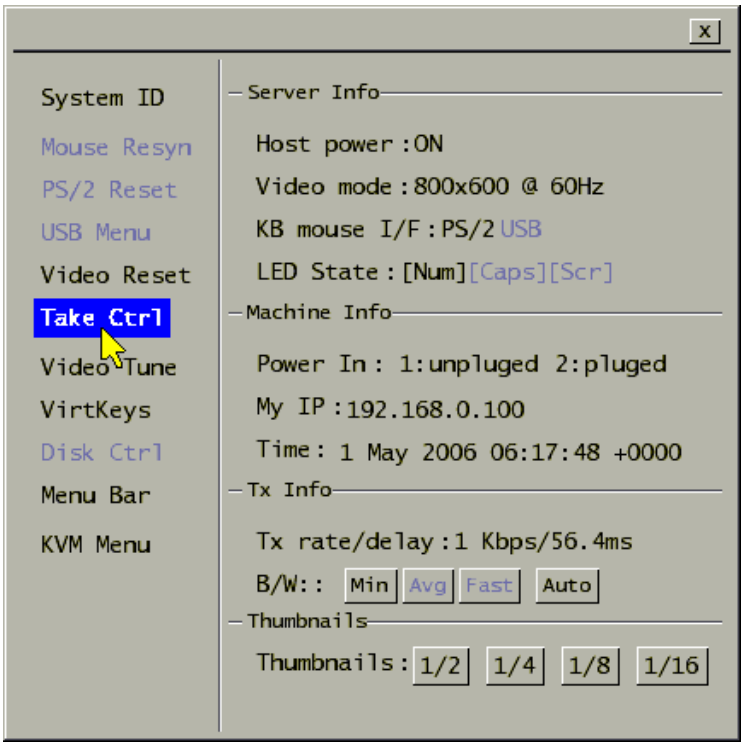
If an user is already operating the host server when another user try VNC connection, the latter user can only monitor the screen, but cannot operate the keyboard and mouse.
If you move the mouse cursor or press the keys on the VNC screen area, the following dialogue box is displayed.



Click [Take control now] button and the following dialogue is displayed, and then you can obtain the host server control authority.

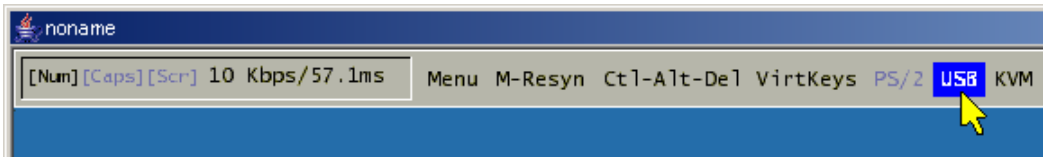


You can also obtain the operating authority by clicking [Take Ctrl] from the menu window.

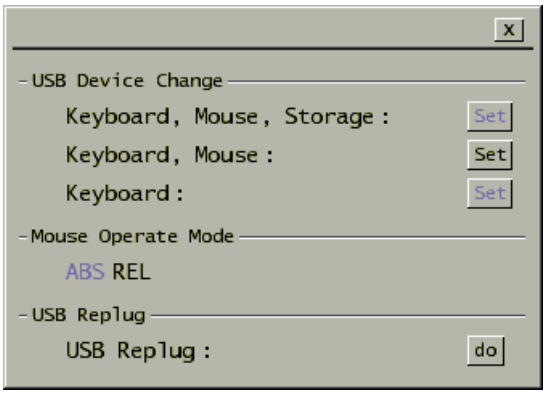


2.5.9 USB Setting Window

Click [USB] on the VNC menu bar to display the USB setting window.



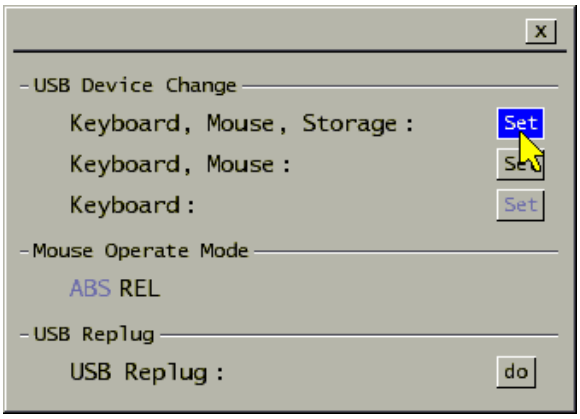
This window sets USB keyboards, mouse and storages.



USB Setting Window	
USB Device Change Select one USB device setting from the following three. The selected button is displayed.	
Keyboard, Mouse, Storage :	Click [Set] button to enable USB keyboard, USB mouse and USB virtual disk.
Keyboard, Mouse :	Click [Set] button to enable USB keyboard and USB mouse. (Default setting) USB virtual disk is disabled.
Keyboard :	Click [Set] button to enable only USB keyboard. USB mouse and virtual disk are disabled.
Mouse Operate Mode	
ABS	It shows the absolute mouse is enabled. If the relative-value mouse is enabled, the button is displayed in gray.
REL	It shows the relative-value mouse is enabled. (Default setting) If the absolute-value mouse is enabled, the button is displayed in gray.
USB Replug	
USB Replug :	Click [do] button to simulate connect and disconnect of the USB connector. This button fixes error in case an access error occurred in the host server.
X	Close the USB Menu window.

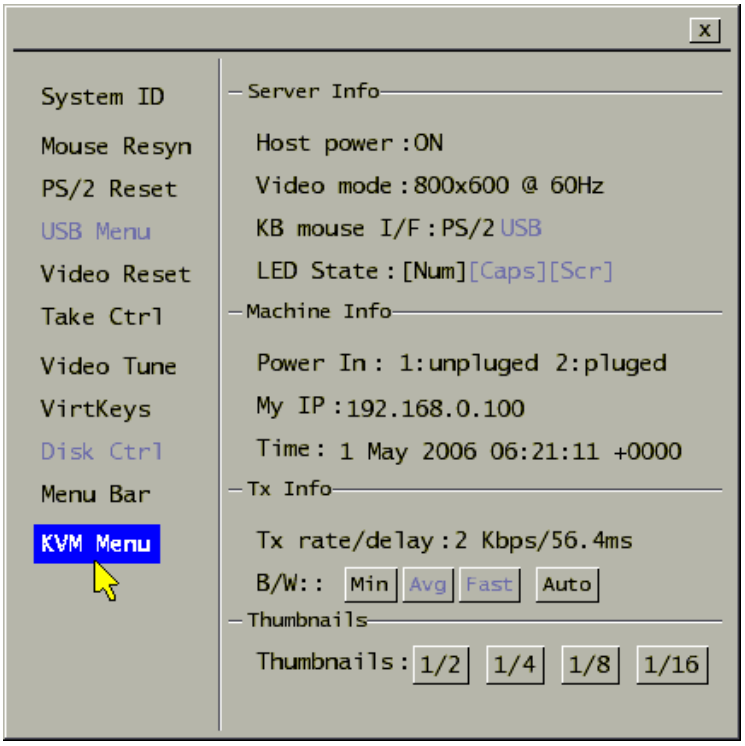
CAUTION

If the host server is rebooted, USB virtual disk function will be ”Disable” automatically.
When you use USB virtual disk function again after the host server starts, please set USB Device setup as [Keyboard, Mouse, Storage].

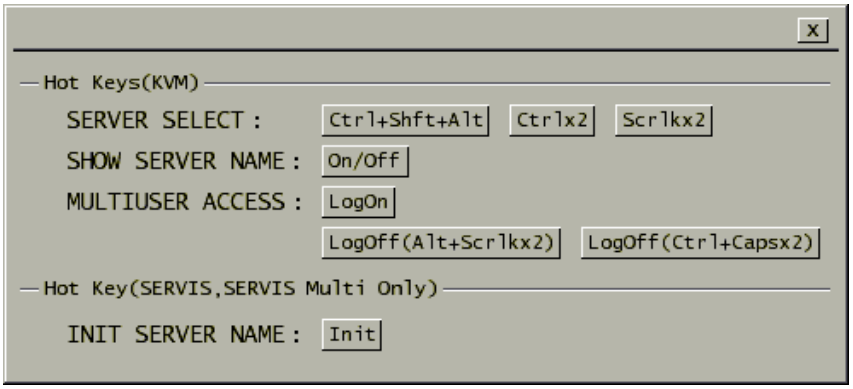


2.5.10 KVM Menu Window

Click the [KVM Menu] in the VNC menu bar and the following KVM hot key setting window is displayed.



Input hot keys to the connected KVM switch from this window.



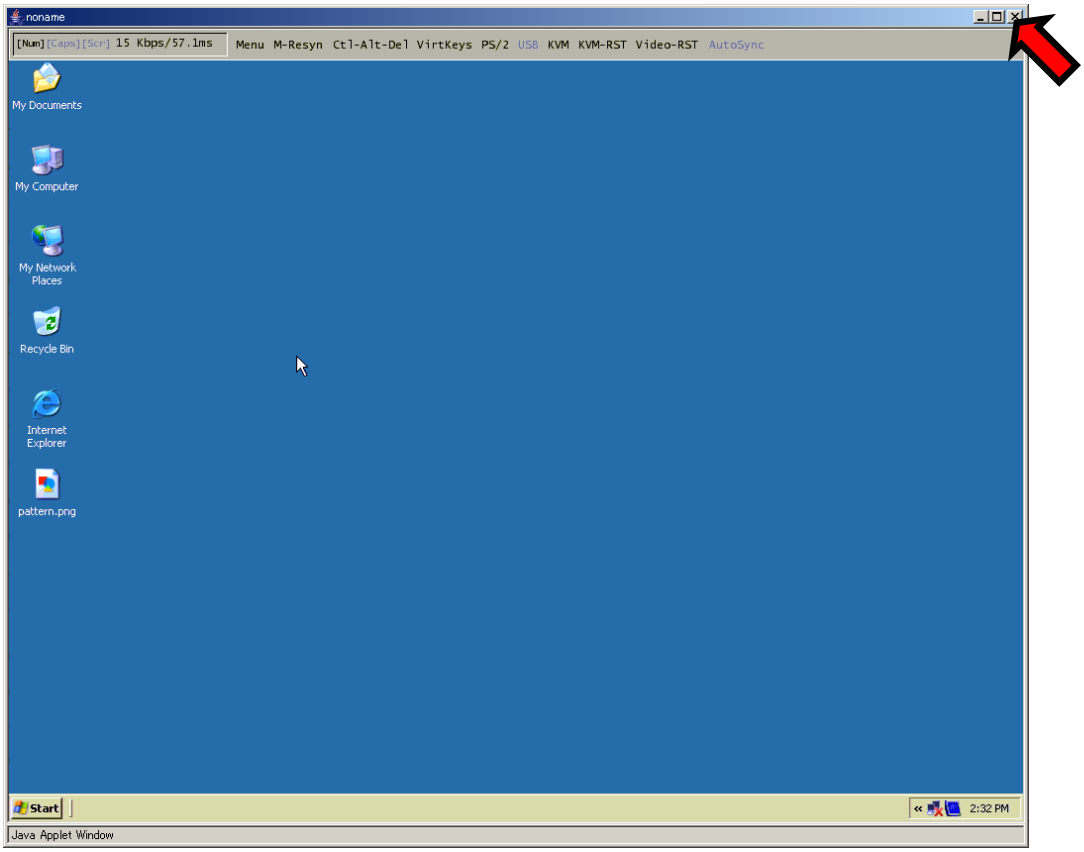
KVM Hot Key Setting Window	
— Hot Keys(KVM) —	
SERVER SELECT:	Click [Ctrl+Shift+Alt] button to display the server select screen.
	Click [Ctrl x 2] button to enter the server select mode.
	Click [Scroll Lock x 2] button to display the server select screen.
SHOW SERVER NAME:	Click [On/Off] button to switch always display / not display the server name in the top-left of the host server screen.
MULTIUSER ACCESS:	Click [Log On] button to display the log on screen.
	Click [LogOff (Alt+Scroll x 2)] button to log off the KVM switch-setting screen.
	Click [LogOff (Ctrl+Caps x 2)] button to log off the KVM switch-setting screen.
— Hot Key(SERVIS,SERVIS Multi Only) —	
INIT SERVER NAME:	Click [Init] button to reset the server name in the top-left of the host server screen.
— Close —	
X	Close the KVM hot key setting window.

Hot keys to be used depend on the connected KVM switch models.
Refer to the KVM switch instruction about hot key specifications.

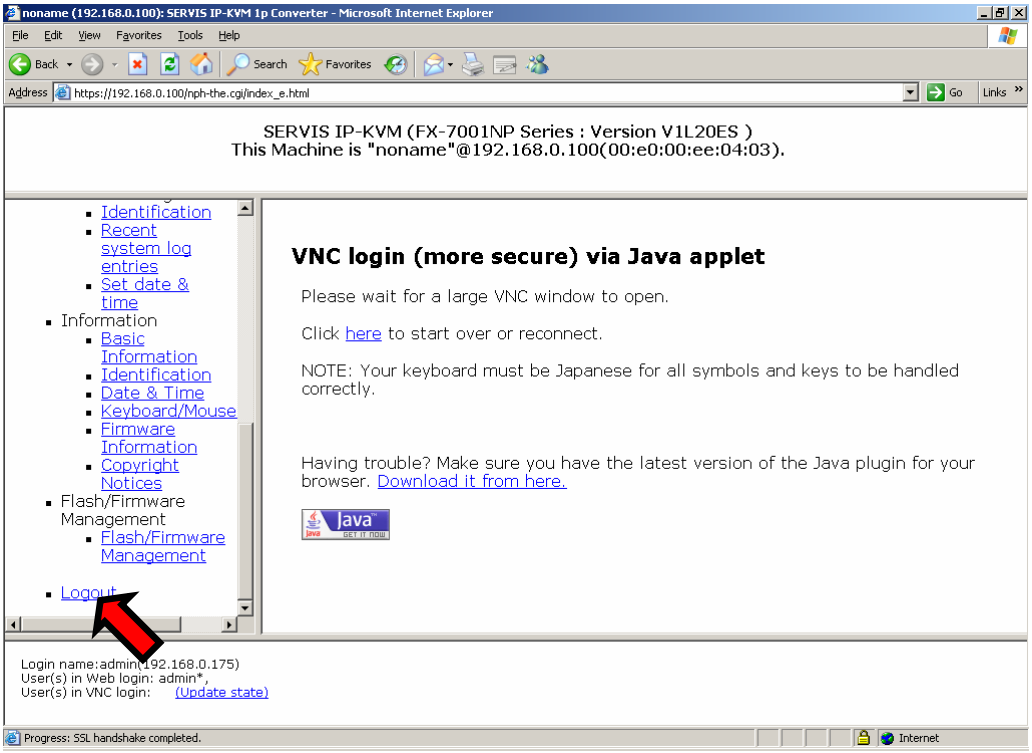
2.6. Exit and Log off the Java VNC

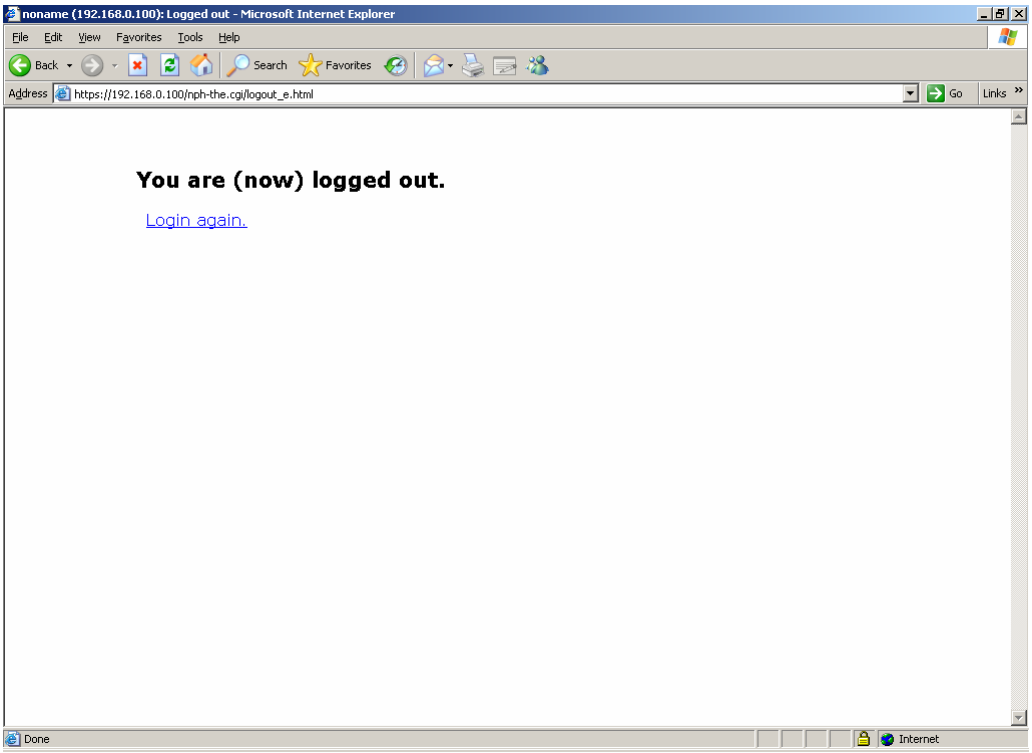
Exit the VNC connection after finishing the operation to the host server. Then log off of the web site.

1. Click [x] button in top right of the Java VNC window to exit the VNC.



2. Click logout from the menu selection area in the web site. The session is over and the log on screen is displayed again.



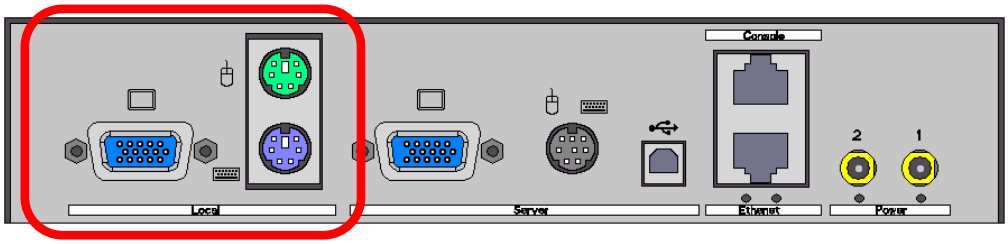


Click Login again to return to the log on screen again.

2.7. Local Operation

Connect video monitor, keyboard and mouse to the local port for local host server operation.
Even if the remote terminal cannot access this product because of network errors, it is possible to connect to the local port and operate the host server.

Only PS/2-compliant keyboard and mouse can be connected.



🕮 Refer to 1.5.2 Connection to the Host Server (page 10)

The Video monitor, keyboard, and mouse should be left unconnected during normal operation and only be connected when necessary.

Refer to the following section about information for when an online user and a local user operate the host server concurrently.
🕮 Refer to 3.3.1.4 VNC Idle Timeout (page 80)

CAUTION

As restriction, local connected keyboard LEDs (NumLock, CapsLock and ScrollLock) is not lit up. However, the self-luminous keyboard is excluded.

MEMO

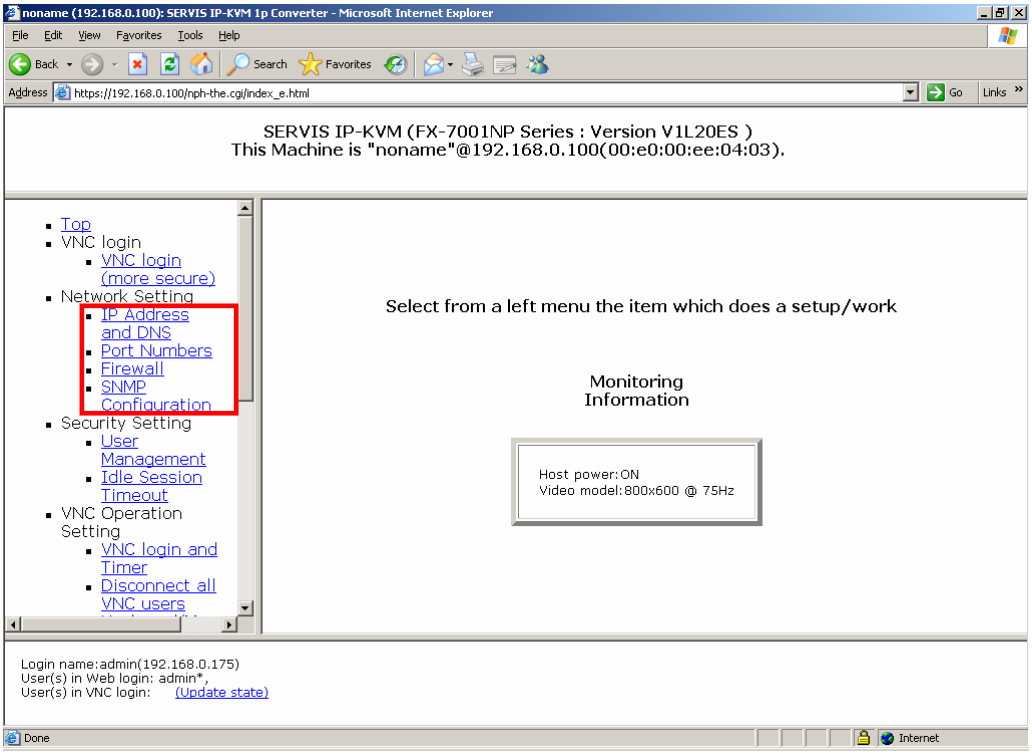
Chapter 3 - Function Details

This chapter provides the function details of the product.

Contents

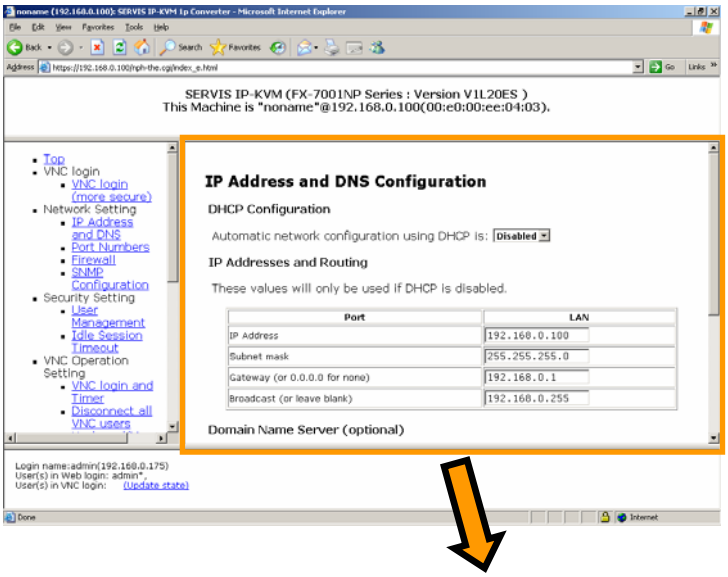
3.1. Network Setting

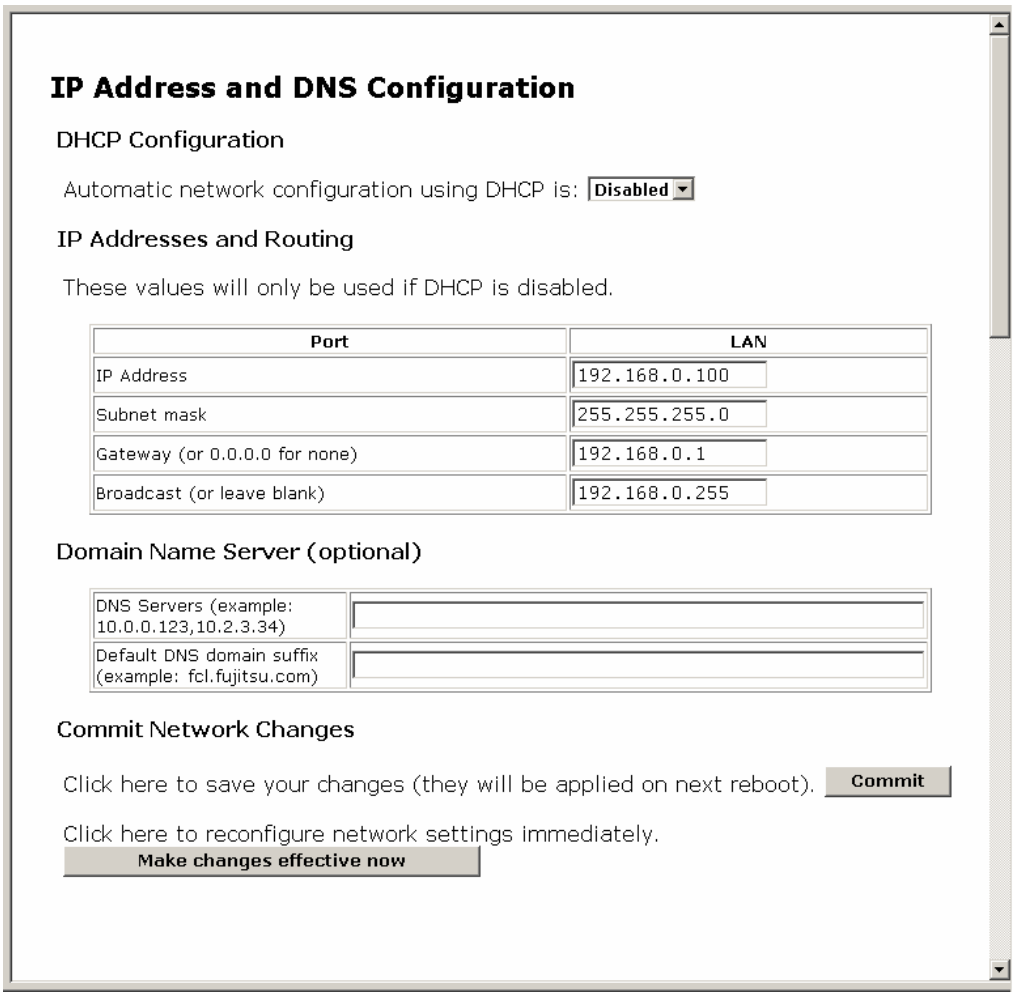
The network setting for this product is performed on web page (for initial installation, it is specified from the serial console).
Refer to the following sections for each item of network settings.



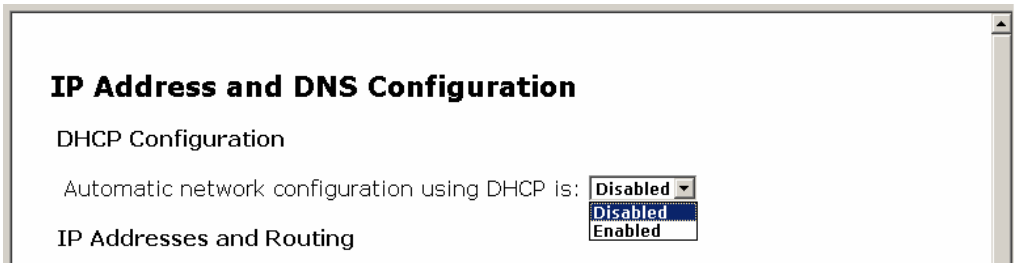
3.1.1 IP Address and DNS

Click IP Address and DNS Configuration from the menu selecting area and following setting menu is displayed.
The IP address and DNS of this product can be changed in this menu.

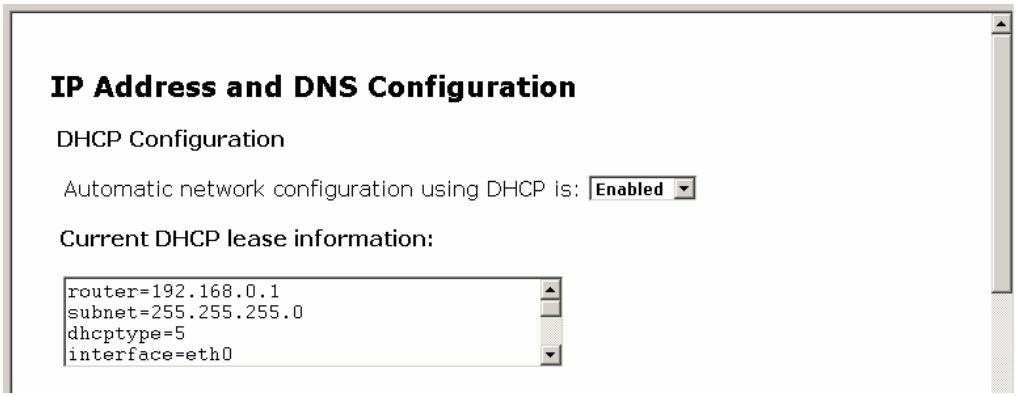




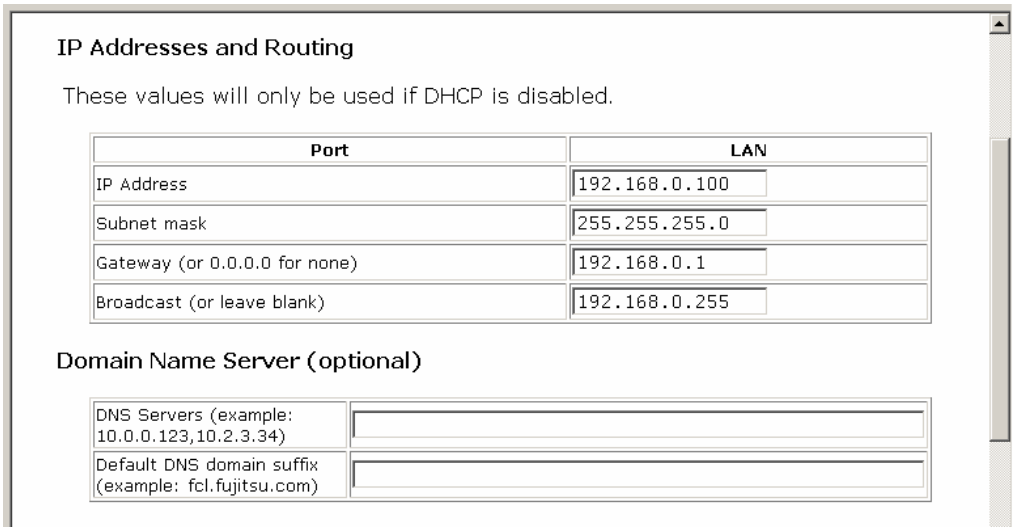
Select enabled/disabled from the list for setting the IP address dynamic allocation by DHCP as shown below.



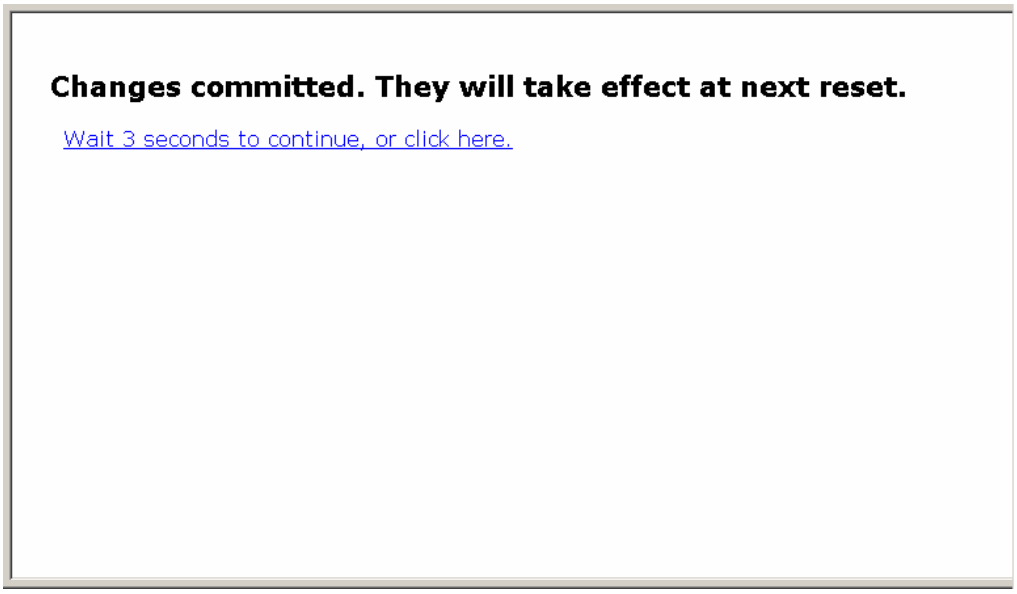
When DHCP is enabled, [Current DHCP lease information] is displayed as shown below.



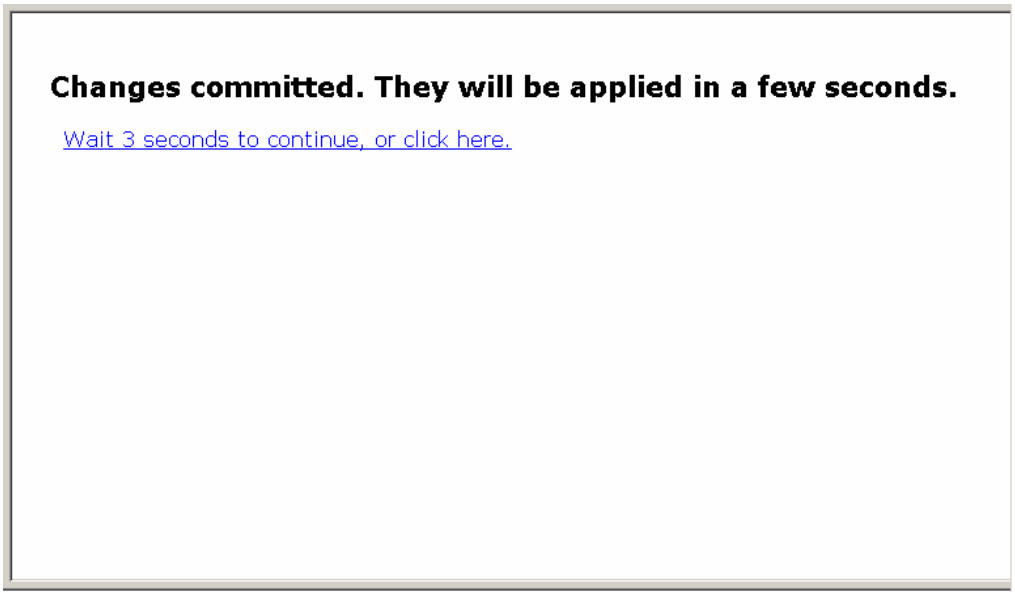
When DHCP is disabled, input the following settings to the web page.



After inputting the setting, click [Commit] button. The following message is displayed and the settings are saved.



Click [Make changes effective now] button. The following message is displayed and the changed settings applied.

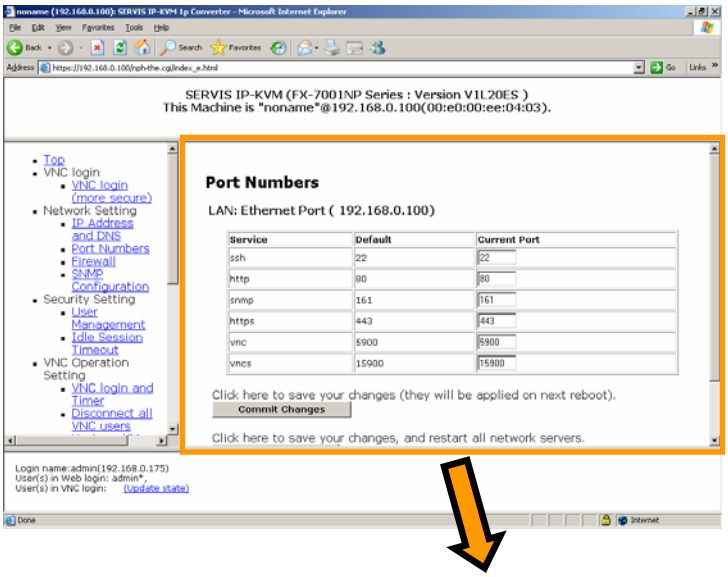


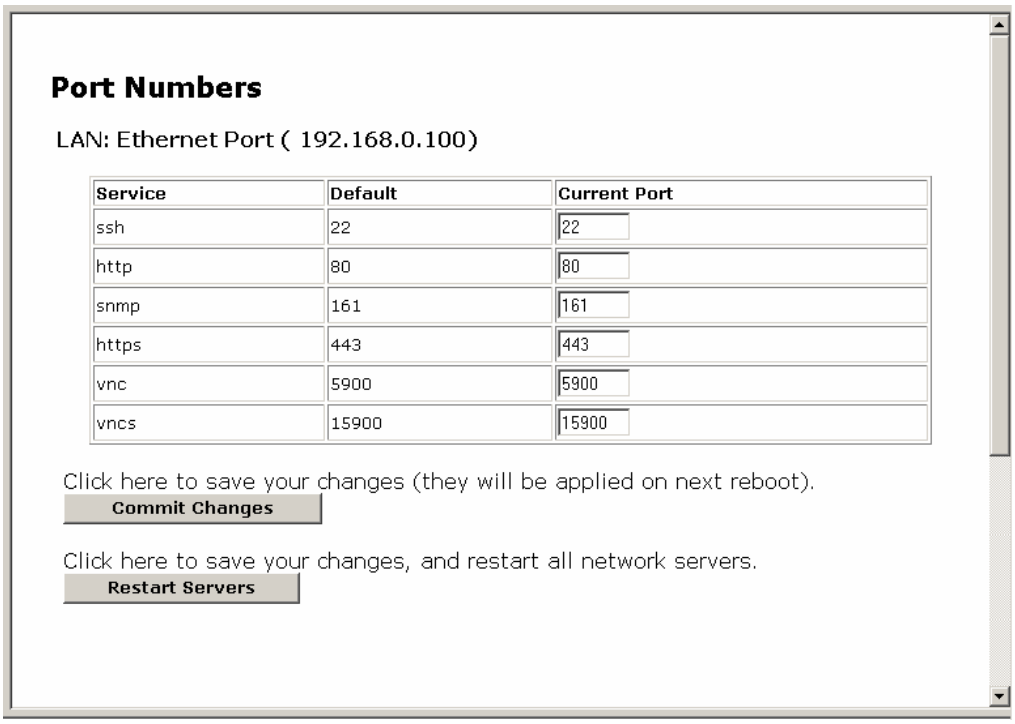
CAUTION

Make sure to specify the fixed IP address when you log on this product and operate for a long periods.

3.1.2 Port Numbers

Click Port Numbers from the menu-selecting area, the following setting page is displayed.
Network port numbers can be changed on this page.



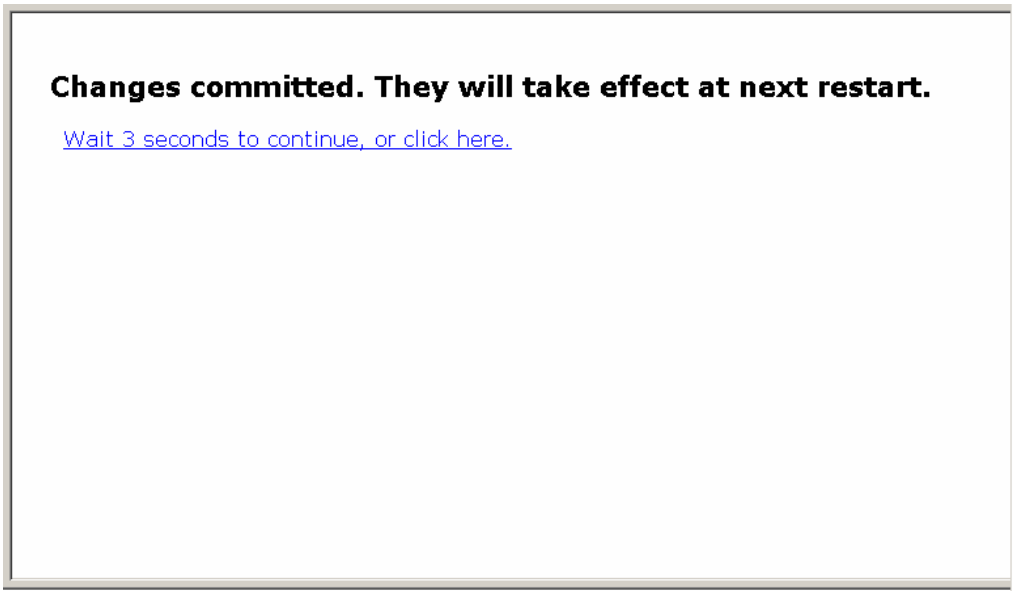


The following table shows the network servers currently running on this product. This function enables to disable some of these services and set any network port number.

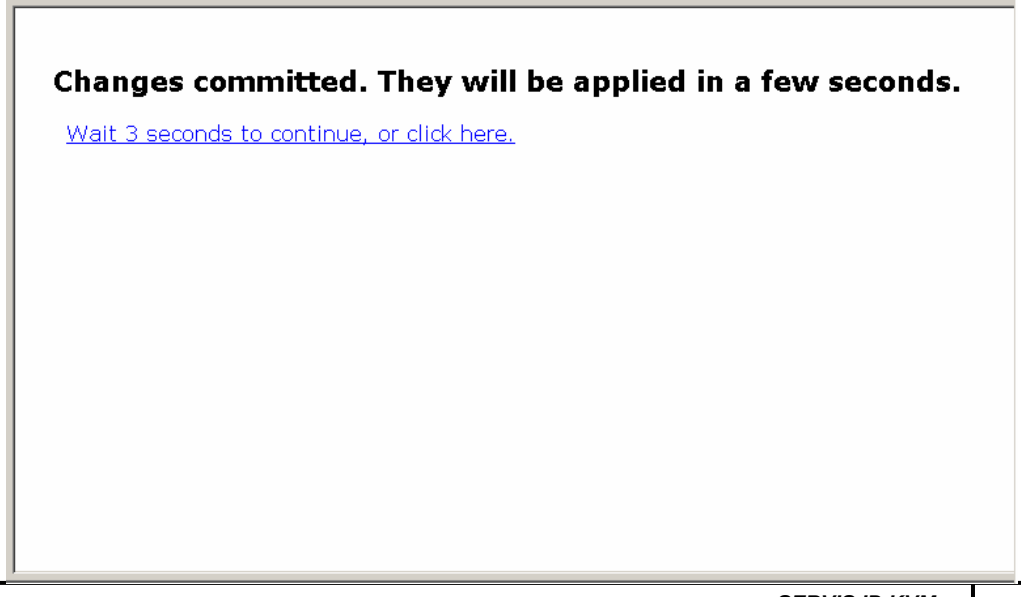
Service	Explanation	Default Network Port Number
ssh	Secure Shell	22
http	HyperText Transfer Protocol	80
snmp	Simple Network Management Protocol (UDP)	161
https	Hypertext Transfer Protocol Security (SSL encryption)	443
vnc	VNC/RFB Protocol	5900
vncs	VNC (SSL encryption)	15900

Specify "0" for the port number to disable the service.

After inputting the port number, click [Commit Changes] button. The following message is displayed and the setting is saved.



After inputting the port number, click [Restart Servers] button. The following message is displayed and the network servers are restarted.



CAUTION

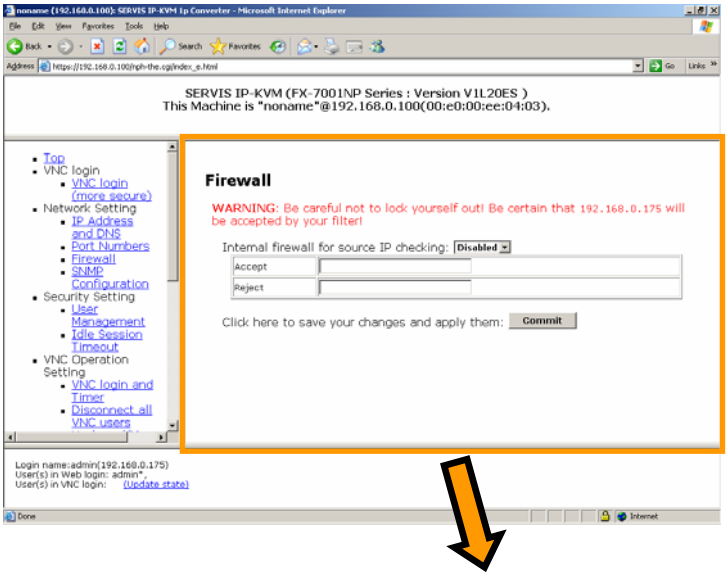
Specify the efficient port number between 1 and 65535.
The network port number must be the unique number in the IP address.
Local Host: 127.0.0.1

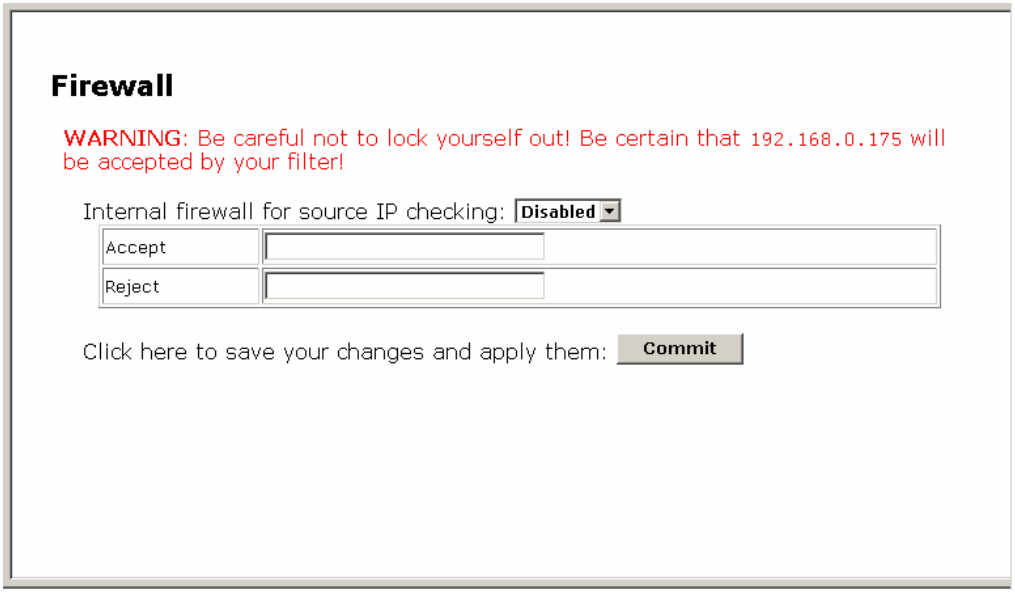
Only the running process on this product can receive the following ports. The following ports do not accept external access and cannot change the number.
These numbers will be required after ssh establishes the tunnel connection. Note that all services use default port numbers.

Service	Explanation	Default Network Port Number
http	HyperText Transfer Protocol	80
snmp	Simple Network Management Protocol (UDP)	161
vnc	VNC/RFB Protocol	5900

3.1.3 Firewall

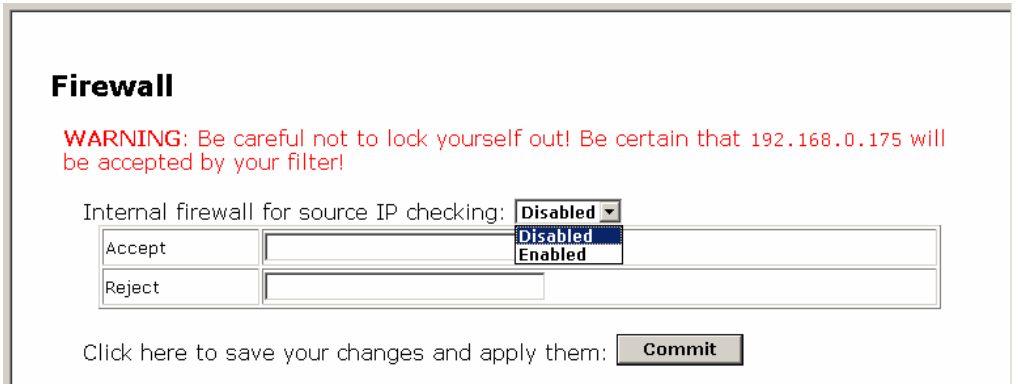
Click Firewall from the menu-selecting area, the following setting page is displayed. Security items are set in this page.





The internal Firewall function is supported to protect the network.
If this function is enabled, the hosts on authorized list can access the server, but all packets from an unauthorized host are omitted.

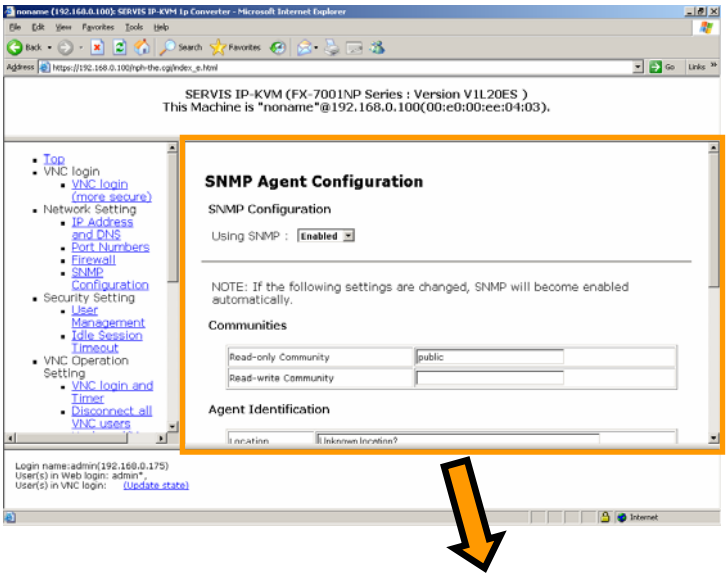
Authorized addresses or unauthorized addresses can be listed. Enter the particular IP address, network range or host name.
Separate by commas to specify multiple addresses.
(Example: 192.168.0.101, 192.168.0.102)

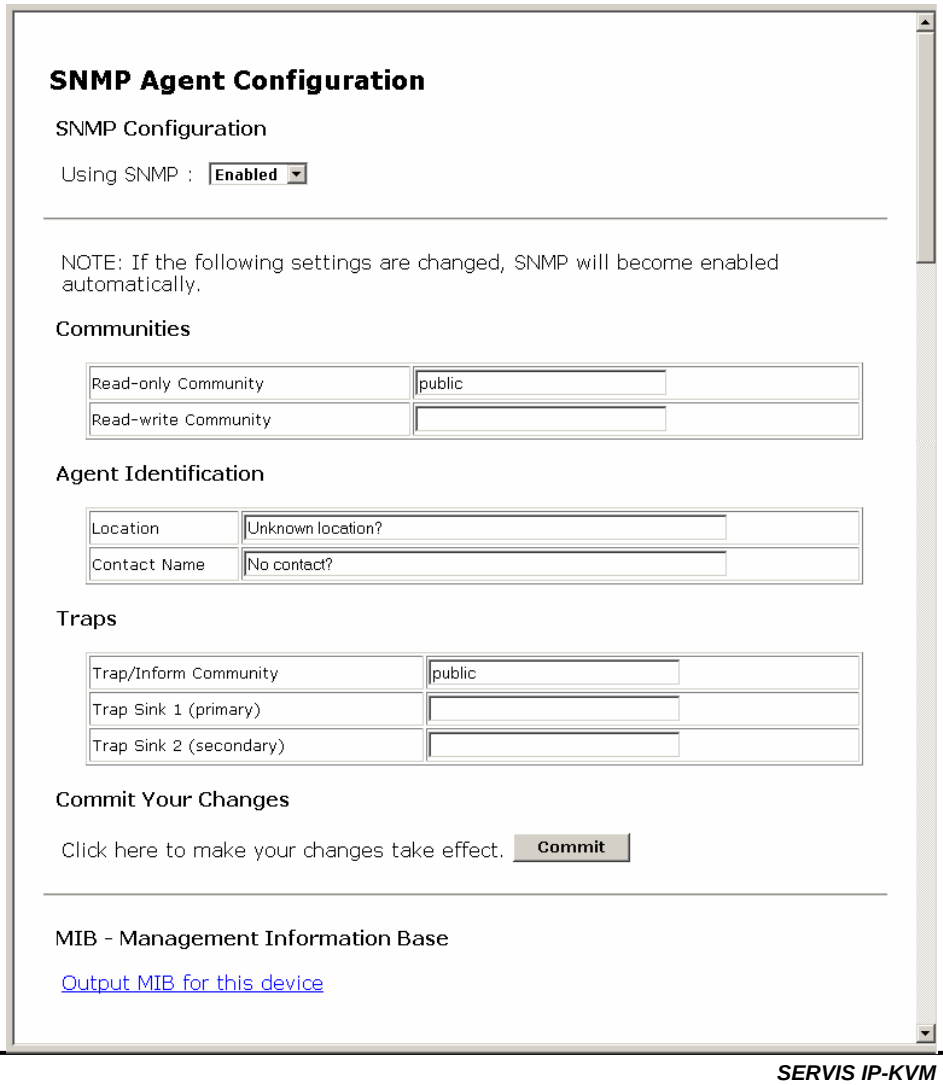


The firewall is set to “Enabled” and enters the IP addresses, and then click [Commit] button. The following message is displayed and the setting is reflected.

3.1.4 SNMP Configuration

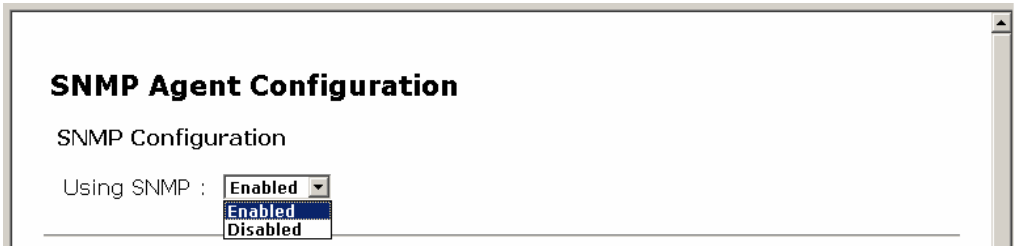
Click SNMP Configuration from the menu-selecting area, the following setting page is displayed. Enable/disable of the SNMP function and SNMP agent are set in this page.





SNMP Agent Configuration

Enable/disable of the SNMP is set in this page. Select enabled/disabled from the list. The following message is displayed and the setting is applied.



Communities

- Read-only Community

  This community allows reading, writing and changing all values. If community name is not specified in this item, the reading access is disabled. Default name is "public".

- Read-write Community

  This community allows reading all values and performing all changes. Specify a unique value in this item and keep it secret for security reasons.
  If you know the value, you can control all systems of this product. Keep this item empty to disable SNMP writing access.

Agent Identification

- Location

  This item is transmitted as system.sysLocation value. Describe the location of this product.

- Contact Name

  This item is transmitted as system.sysContact value. Describe who will receive notification about this product. It usually includes e-mail address.

Traps

- Trap/Inform Community

  Use the community in this item when transmitting the trap message. Specify the community in the trap server.

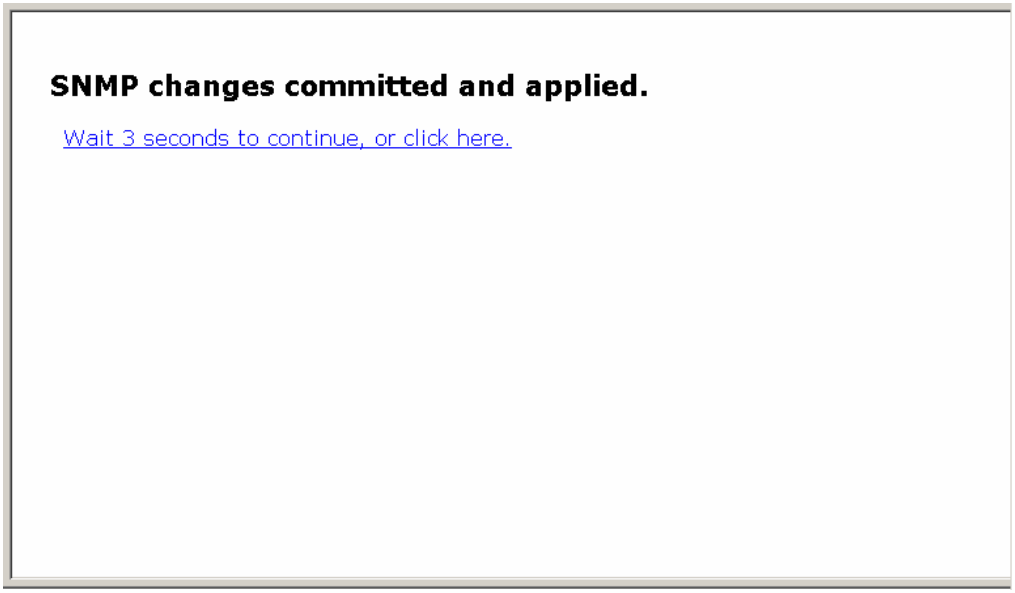
- Trap Sink 1 (primary)

  This host receives all the trap reports and information messages. This address must be specified with numerical characters.

- Trap Sink 2 (secondary)

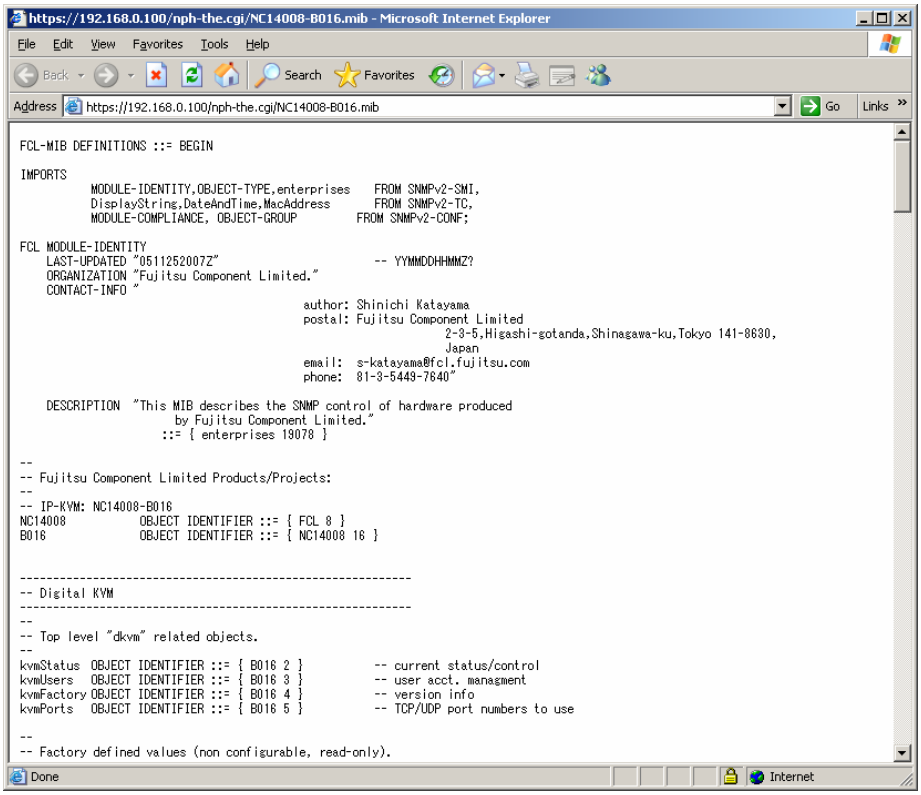
  If this item is specified this host server, it also receives all the trap reports and information messages. This address must be specified with numerical characters. If it is not necessary, keep this item empty.

Click [Commit] button. The following message is displayed and the SNMP setting is changed.



- MIB – Management Information Base

Click Output MIB for this device to display the MIB copy of this product. SNMP shows the operating method for this product. It provides reading status, power on/of, reset operation, changing system configuration and user account management of connected devices. Other detail for normal network management is supported by standard MIB-2 definition.



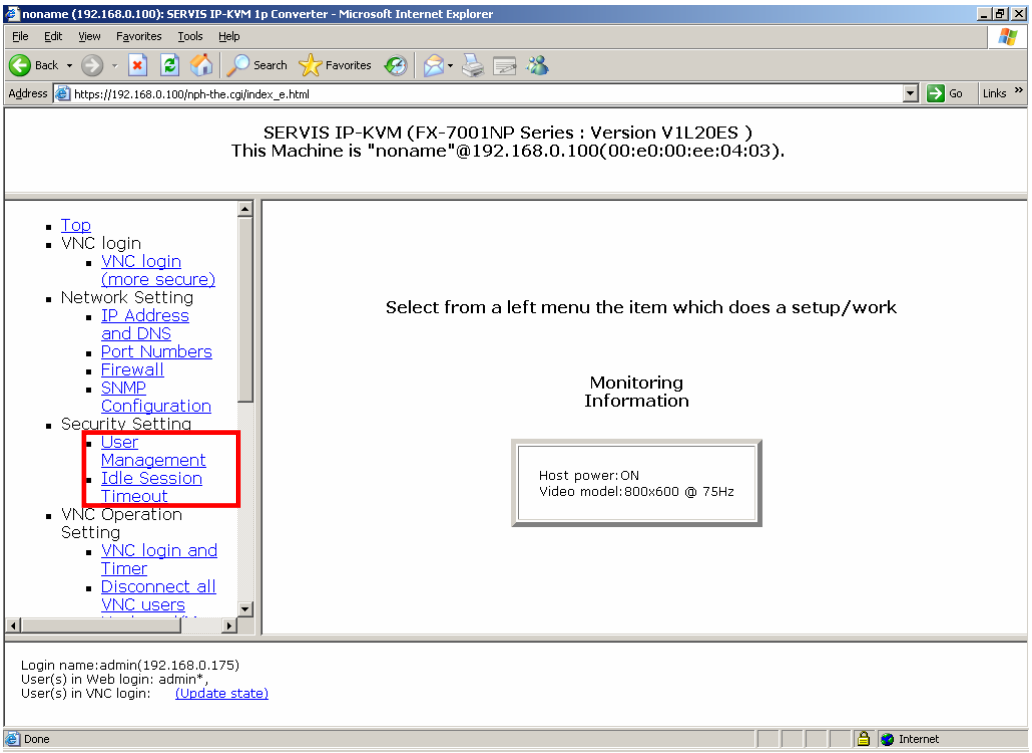
CAUTION

If SNMP function is not "Enabled", SNMP is inactive.

When SNMP function is “Disabled”, if you input one setup of Communities, Agent Identification, and Traps and click [commit] button, SNMP function will be in "Enabled" state.

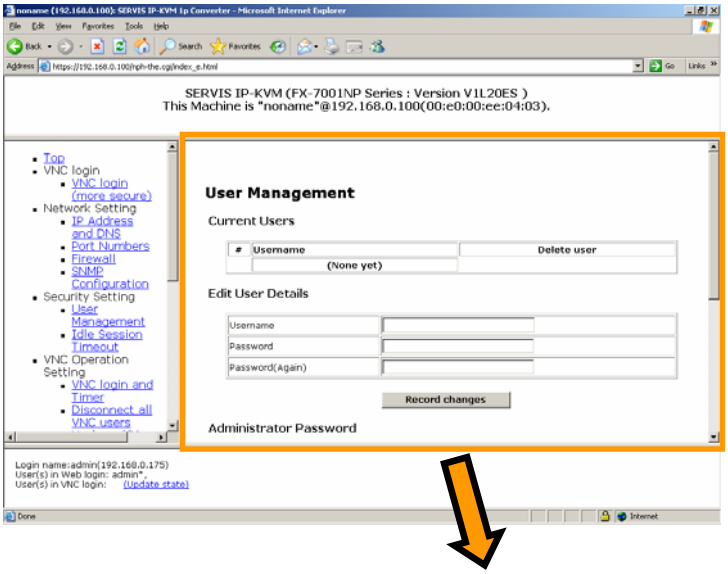
3.2. Security Setting

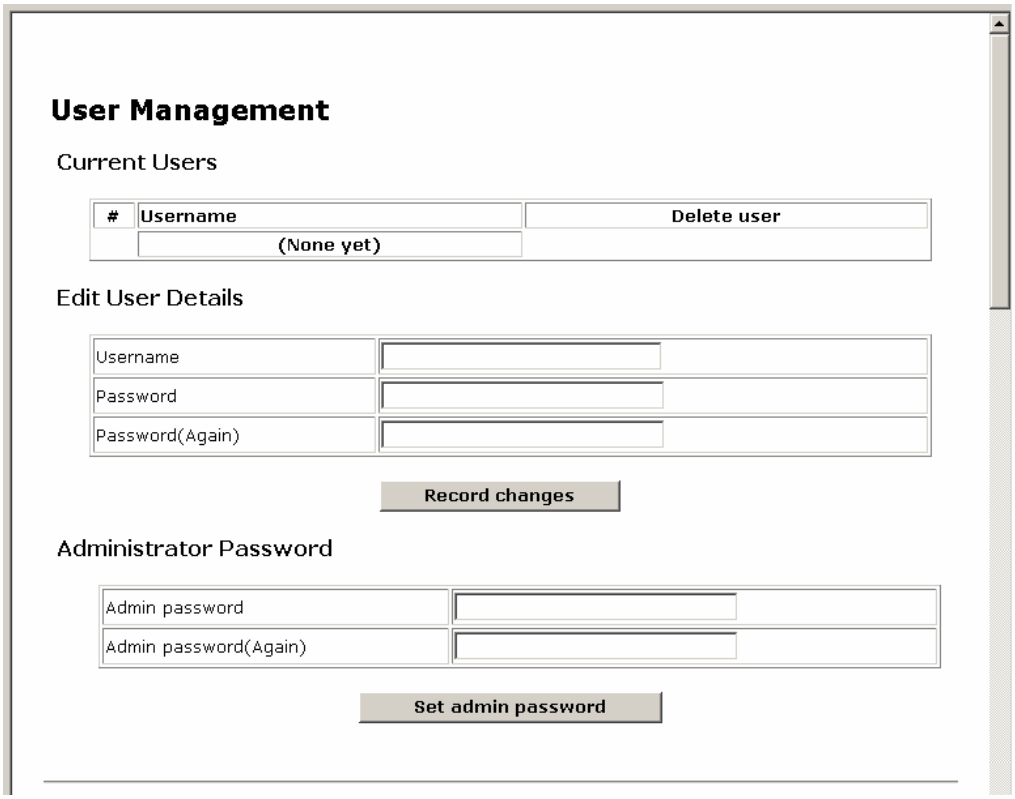
Refer to the following sections for each item of security settings.



3.2.1 User Management

Click User Management from the menu-selecting area, the following setting page is displayed.
User account settings are set in this page.

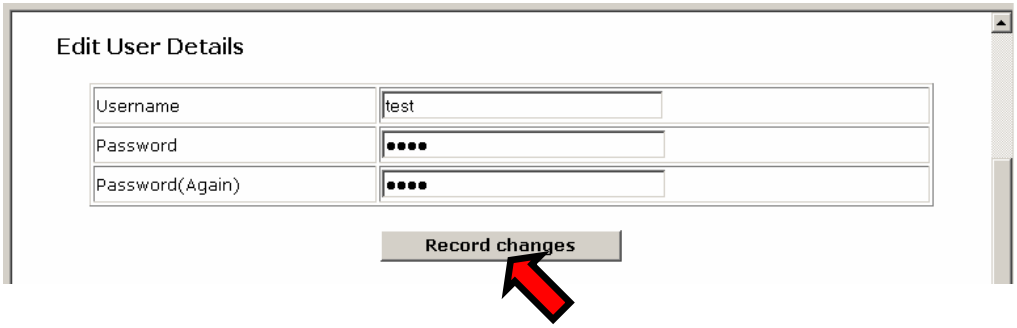




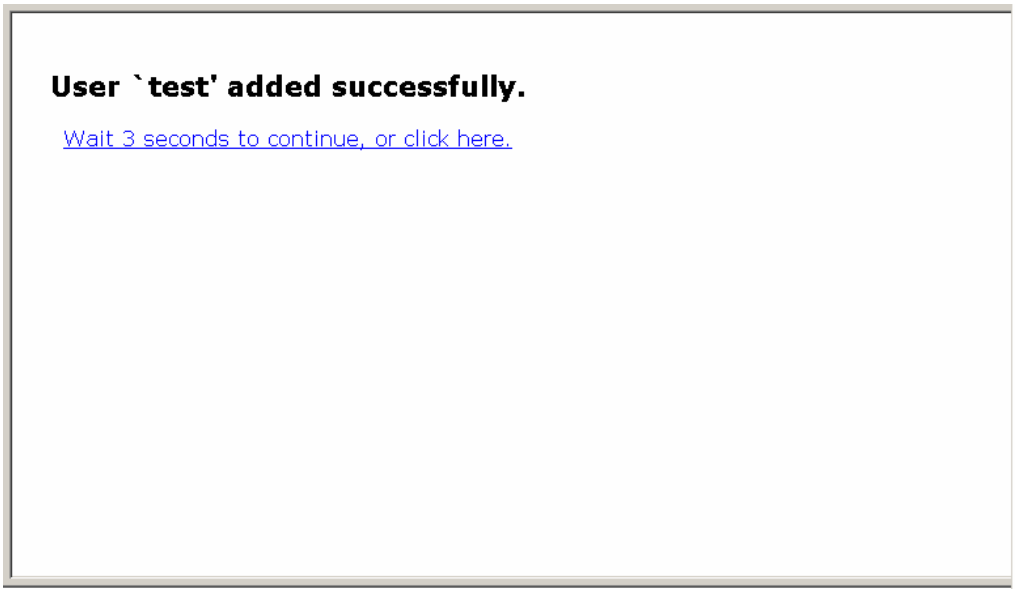
Account for administrator is set as "root", "admin" and "administrator" by default. Account for administrator cannot be added or changed.

3.2.1.1 Edit User Details

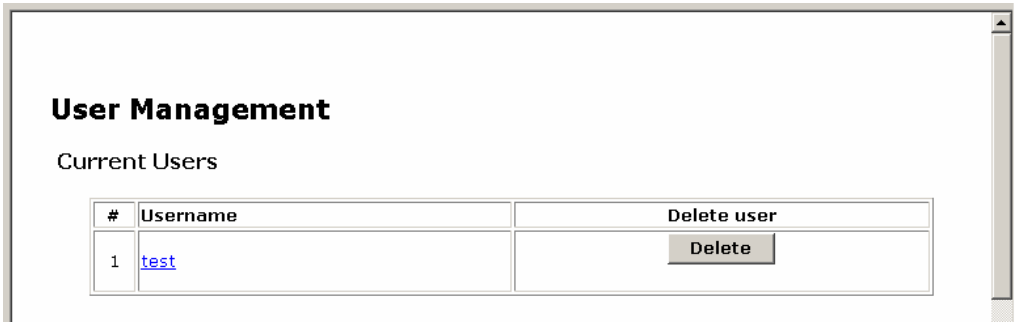
Enter User name and password and click [Record Changes] button to add general users.



The following screen is displayed and the user is registered.

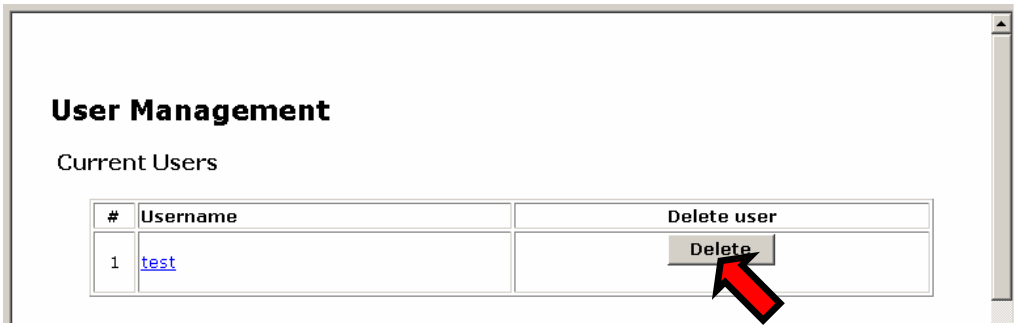


The registered users are displayed as follows.



Refer to following section about authorized operations for general users.
📖 Refer to 3.7 Operation for General User (page 135)

Click [Delete] button in the user list to delete the registered user.

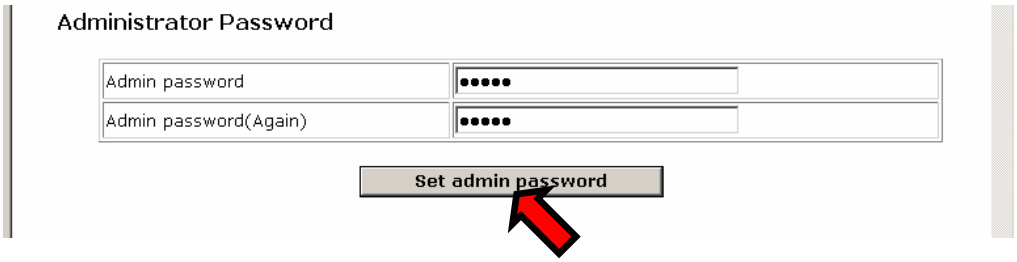


The following screen is displayed and the user is deleted.

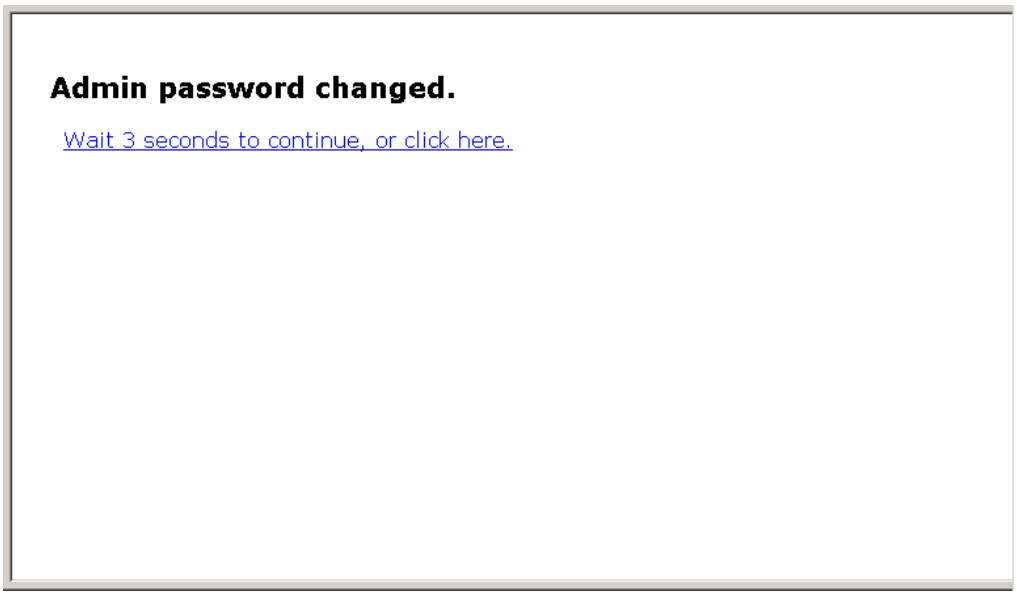
3.2.1.2 Changing Password for Administrator

The administrator's password (default: admin) can be changed. It is recommended to change the administrator's password for the security of the system.

Enter new password and click [Set admin password] button.



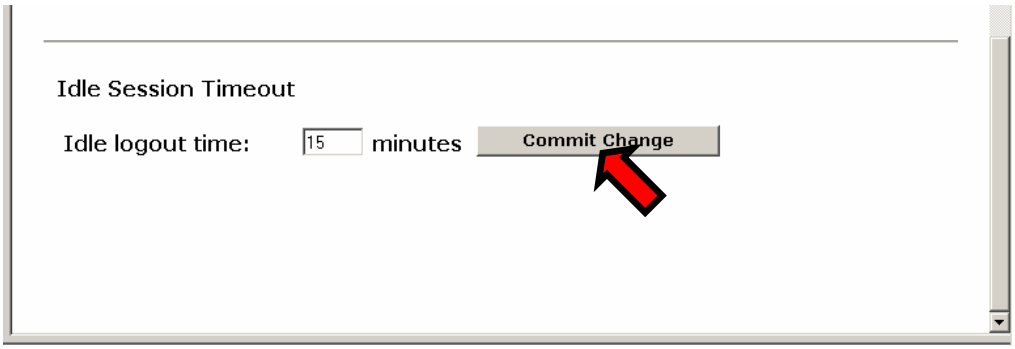
The following message is displayed and the password is changed.



3.2.2 Idle Session Timeout

Shut down the user connection after a certain period of time without using log on session. (Default setting: 15 minutes)

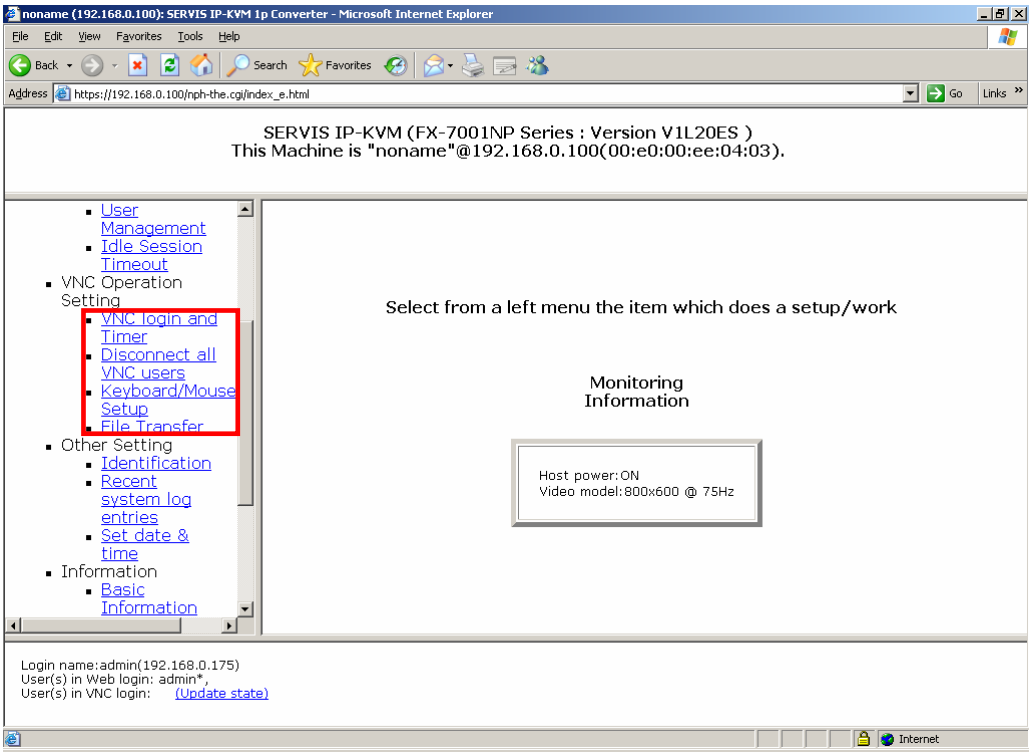
Enter the numerical characters (by the minute) in the [Idle logout time] text box. Click the [Commit Change] button to apply the setting. Specify the value between 1 and 360 minutes.



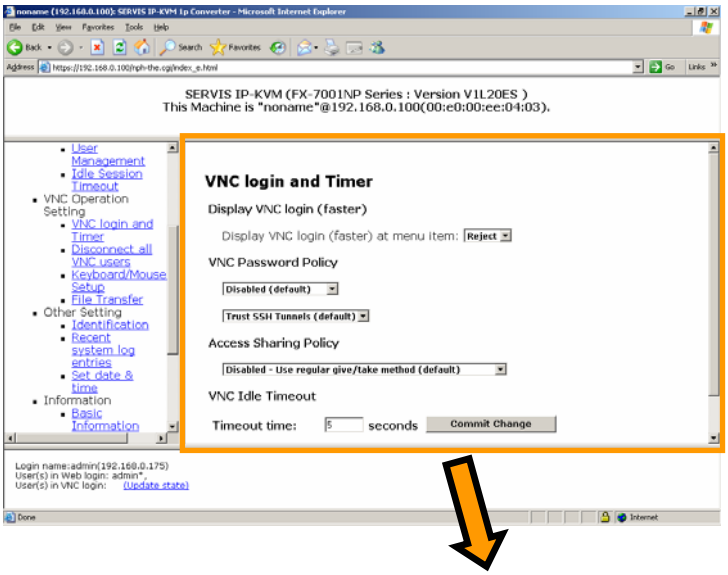
If a value besides 1 to 360 is entered, the following error message is displayed and the setting is not changed.

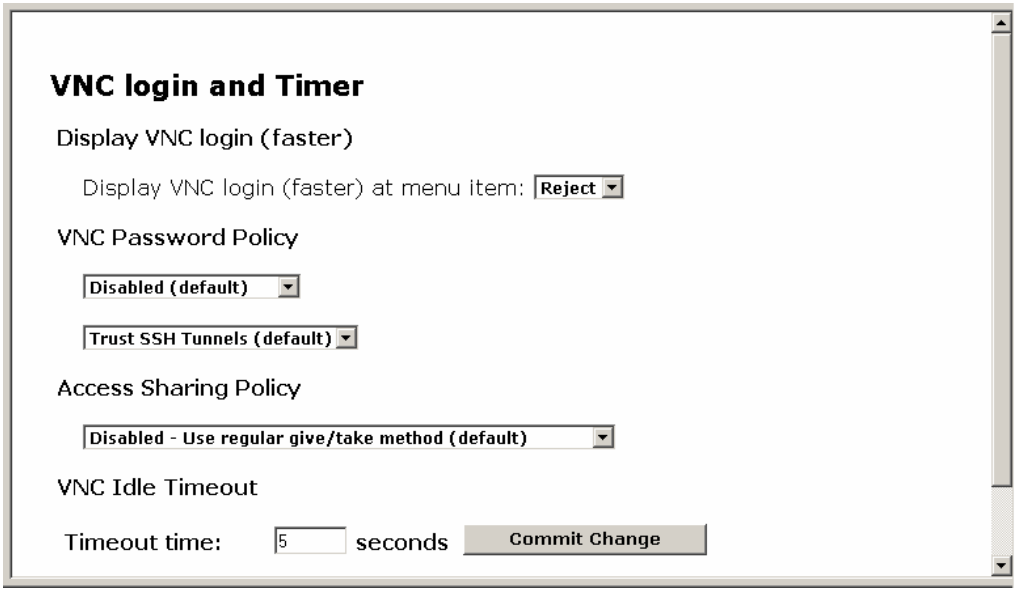
3.3. VNC Operation Setting

Refer to the following sections for each item in VNC Operation Setting.



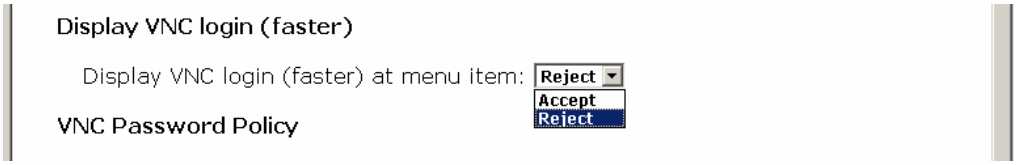
3.3.1 VNC login and Timer



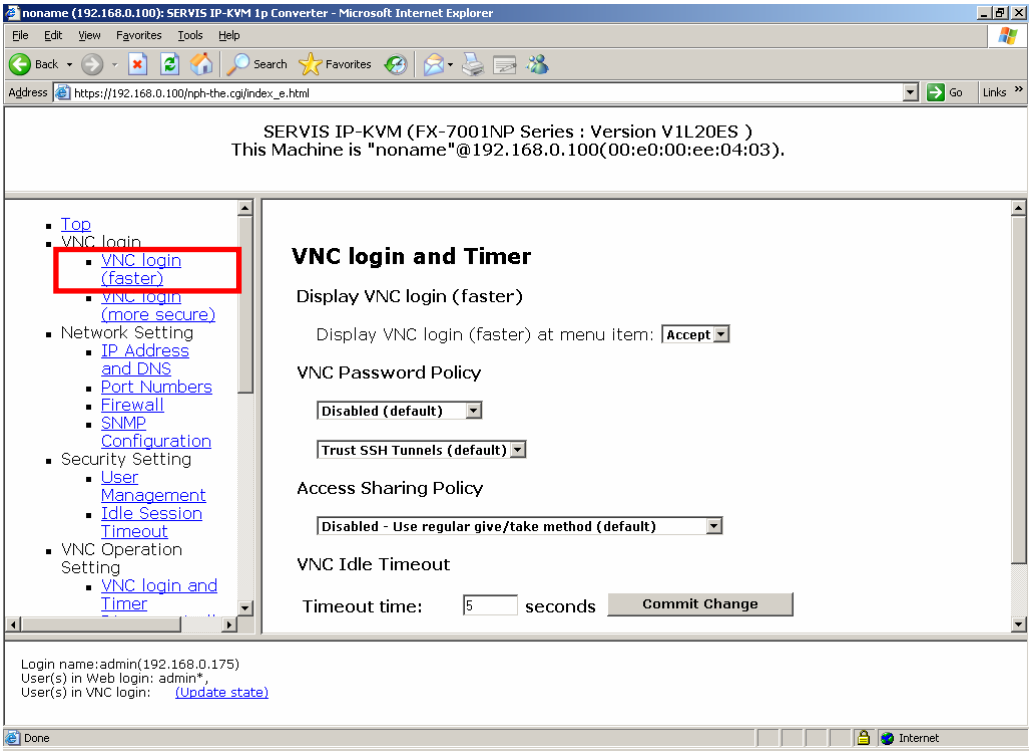


3.3.1.1 Display VNC login (faster)

Set display/nondisplay the link for VNC connecting without SSL encryption.
Select the Reject / Accept from the list. (Default is [Reject].)
The selected setting is reflected immediately.



The item "VNC Login (faster)" is displayed after selecting "Accept" as shown below.



Clicking "VNC Login (faster)" and VNC connection is performed without encryption.
Keep in mind are inferior in respect of security.

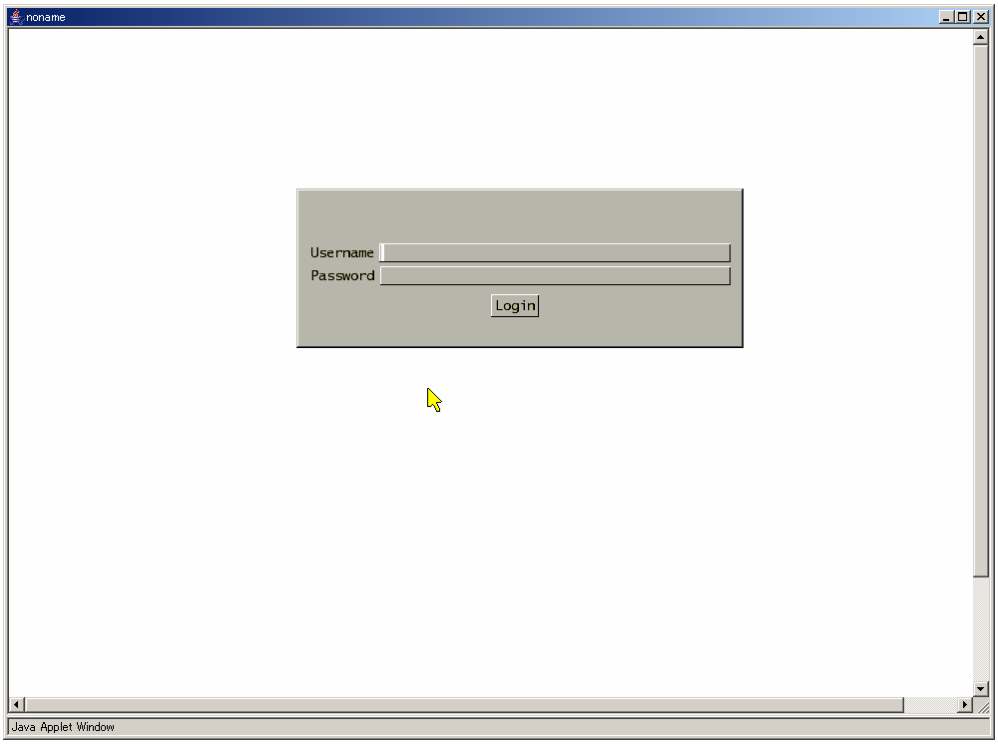
3.3.1.2 VNC Password Policy

(1) VNC Password Setting

To establish a new VNC connection, it is necessary to authenticate the remote user.
Standard VNC protocol does not support "user name", but does support password.
This setting allows the use of the VNC login screen, which requires a user name and password.

Select enabled/disabled the function from the list as shown below. The selected setting is reflected immediately.

Select [Use VNC login screen] and start up the VNC, the following login screen is displayed.



Enter username and password in the login window and click [Login] button. The log on certification is performed and the host server screen is displayed.

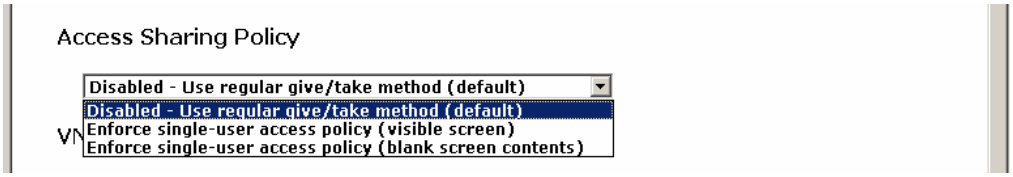
(2) SSH Tunnel Setting

If the VNC connection is transmitted via SSH tunnel, the combination of the SSH user name and password are used for certification. Consequently, there is no need to enter the password. Make sure not to use this function when the SSH client machine is not safe and there is a possibility other users use the SSH tunnel.

Select enabled/disabled the function from the following lists. The selected setting is reflected immediately.

3.3.1.3 Access Sharing Policy

Specify the access setting when multiple remote users perform VNC connection at the same time. Select enabled/disabled from the list as below and the setting is reflected immediately.



- Disabled – Use regular give/take method (default)
  In case you do not have control, click-left on the VNS window display area to obtain the control.

- Enforce single – user access policy (visible screen)
  When a user is connected to the VNC, other remote users are only allowed to view the screen. Other users are not allowed to obtain the control.

- Enforce single – user access policy (blank screen contents)
  When a user is connected to the VNC, other remote users are not allowed to connect.

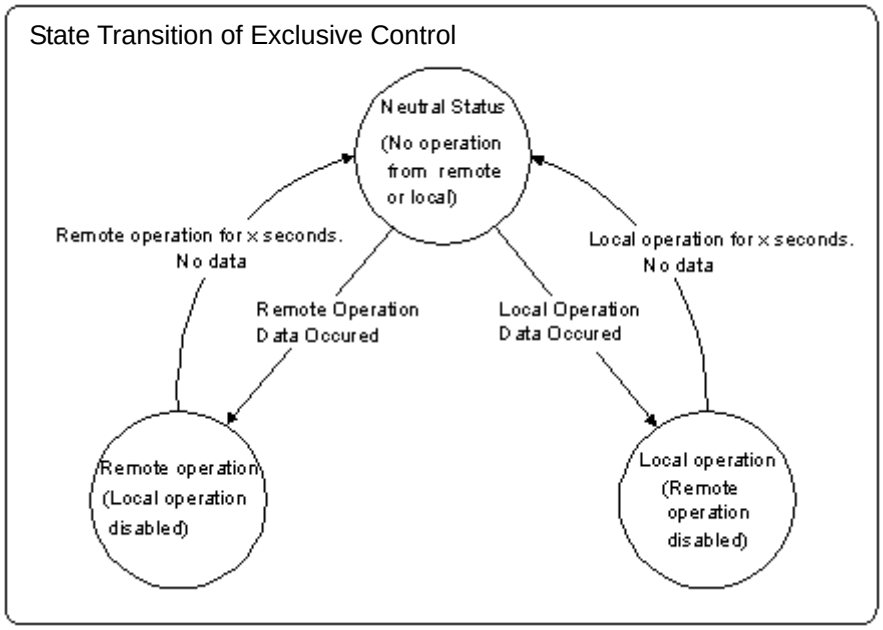
📖 Refer to 3.8 Concurrent Connection of Network Users (page 136)

CAUTION

In every setup, administrator can obtain the control.

3.3.1.4 VNC Idle Timeout

Operation control from network and local to this product is exclusive access control. Local operation is not allowed while other users are continuously operating the host server via network. (It is possible to monitor the screen.) Also, remote operation is not allowed while a local user is operating the host server.



The following three are operating data.

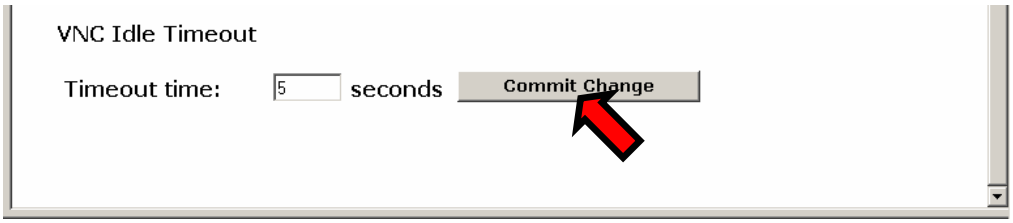
- Entry from the keyboard
- Mouse Cursor Movement
- Mouse Button Click

The VNC goes to neutral status if there is no operating data, and provides operating authority to the first user who enters data while the VNC is in neutral status.

If a remote user does not have control, VNC menu bar is displayed as follows.

A time-out period is set until the VNC becomes neutral here.

Enter numerical characters (by the second) in the [Timeout time] text box. Click the [Commit Change] button to apply the setting. Specify a value between 5 and 300 seconds.



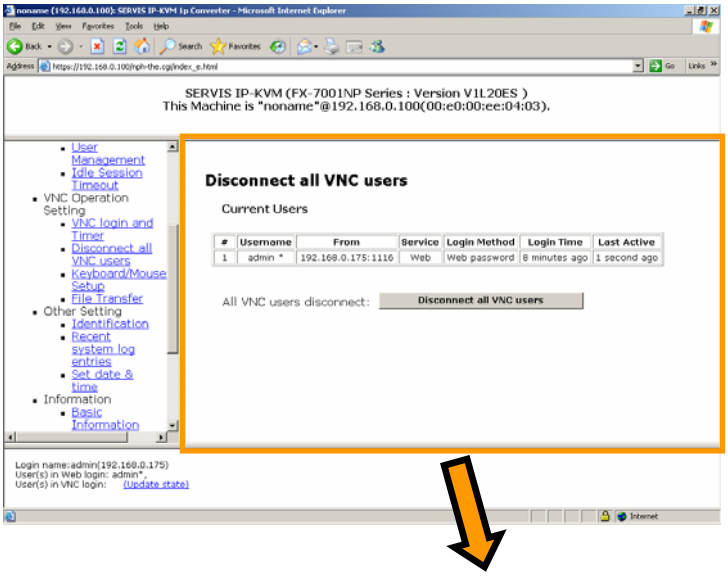
If a value besides 5 to 300 is entered, the following error message is displayed and the setting is not changed.

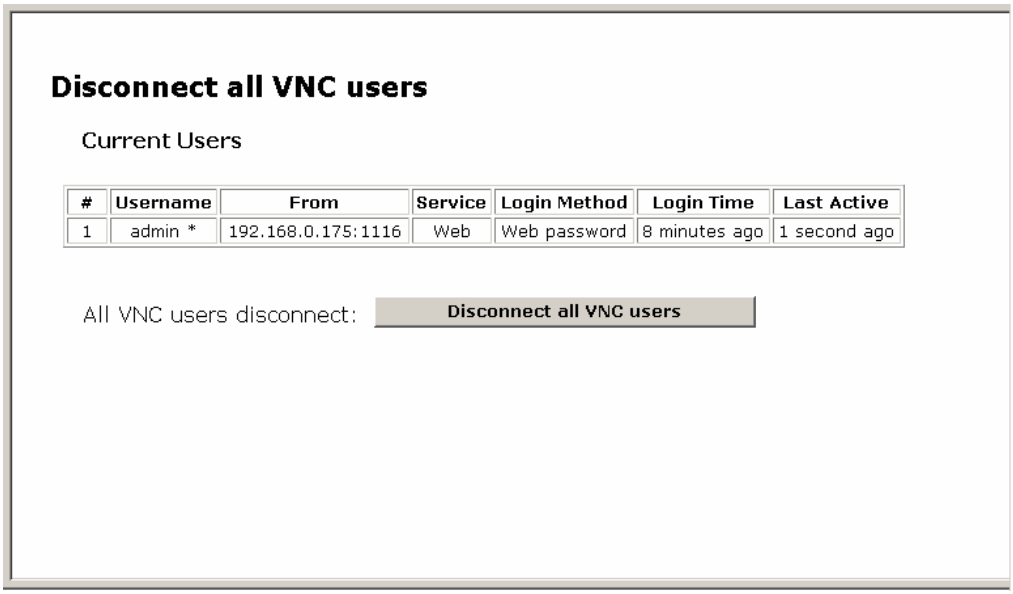
CAUTION

The time-out period depends on the network condition. Please note that the time-out period would give or take a few seconds because of network traffic.

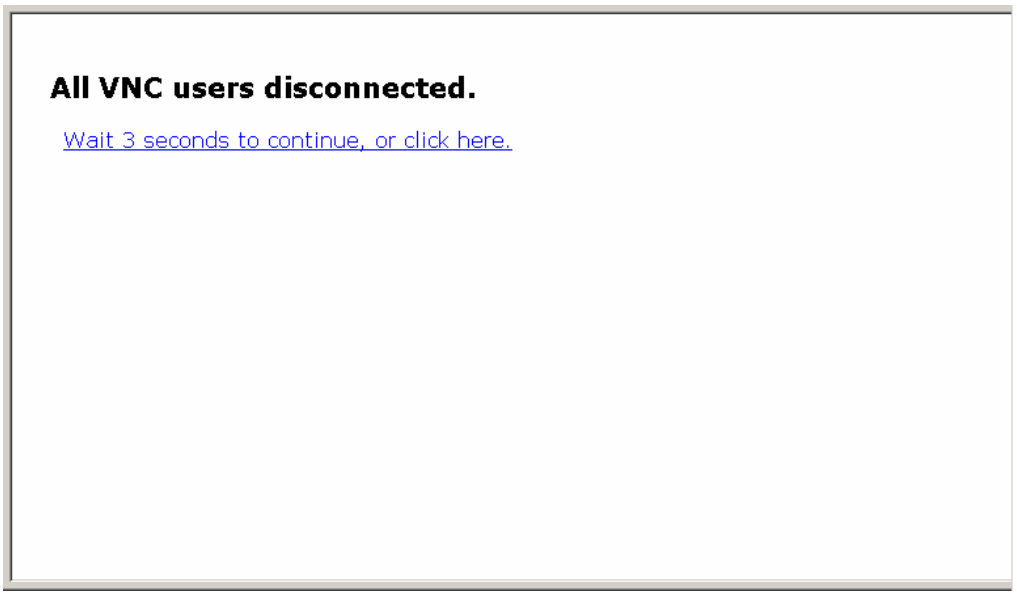
3.3.2 Disconnect all VNC users

Click Disconnect all VNC users in the menu-selecting area, the following setting page is displayed. All active VNC users can be disconnected in this page.

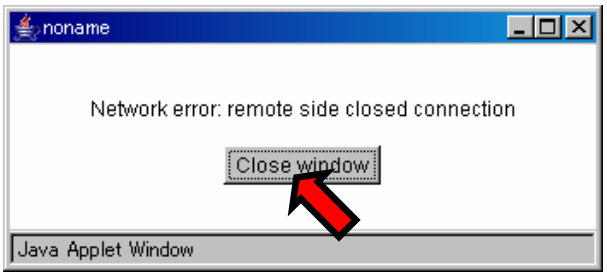




Click [Disconnect all VNC users] button, the following message is displayed and all active VNC users are disconnected.

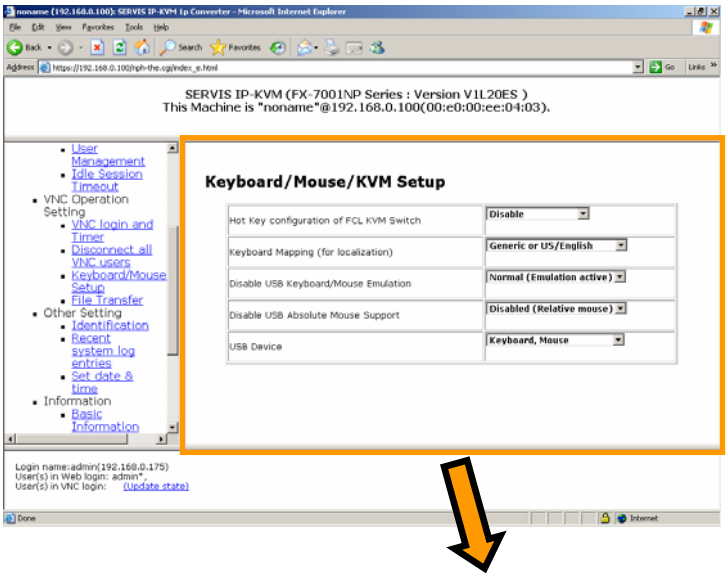


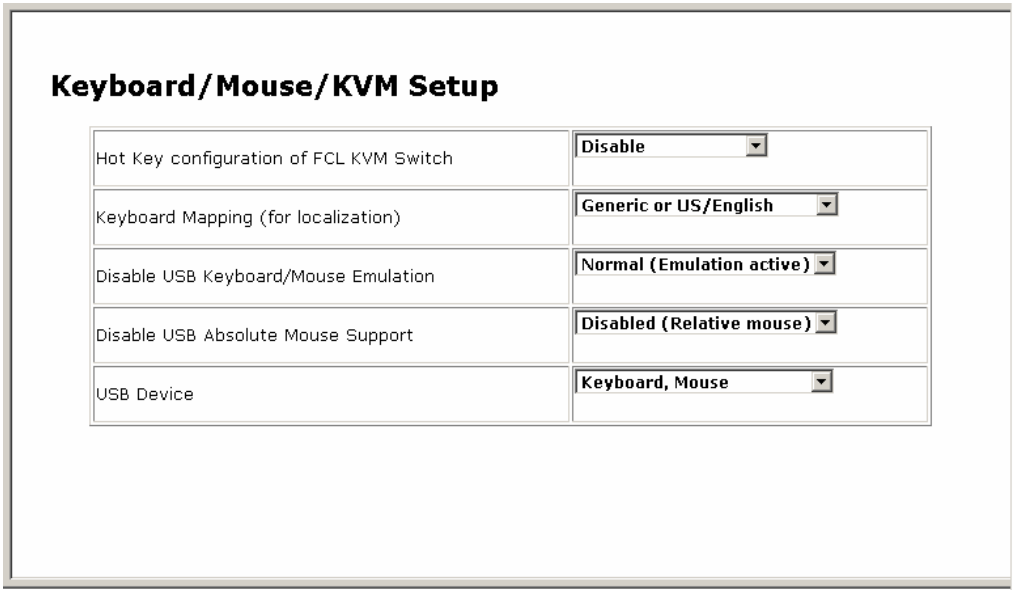
After the VNC disconnection, Java VNC displays the following message. Click [Close window] button to exit. If you want to connect to the VNC again, click VNC login (more secure) or VNC login (faster) from the menu selecting area in the web page.



3.3.3 Keyboard/Mouse/KVM Setup

Click Keyboard/Mouse/KVM Setup from the menu-selecting area, the following setting page is displayed.
On Screen Display (OSD) hot key setting to use this product with the KVM switch, and keyboard and mouse setting is performed in this page.





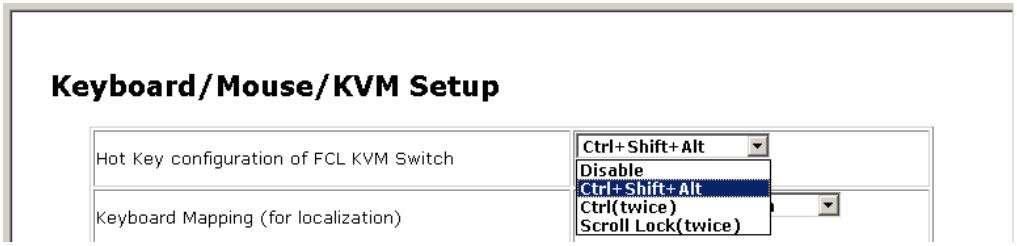
3.3.3.1 Hot Key configuration of FCL KVM Switch

To use this product with the FCL KVM switch, click [KVM] button in the VNC screen to display the server-selecting menu for the KVM switch.
📖 Refer to 2.5.2 VNC Menu (page 32)

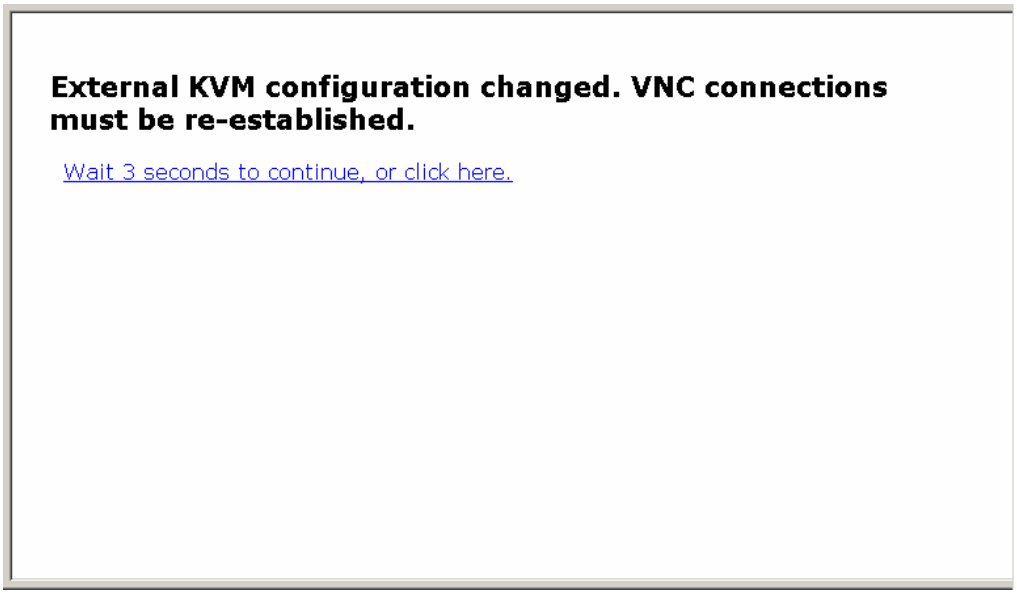
There are three OSD display hot key operation for FCL KVM switch as follows.

- Ctrl + Shift + Alt key (click all at once)
- Ctrl key (click twice)
- Scroll Lock key (click twice)

Click [KVM] button in the VNC window menu bar to select hot key operation to input KVM switch from the list.



The following message is displayed after selecting and the setting is reflected.



[Disable] is specified as the initial setting. [KVM] and [KVM-RST] button are not displayed in the VNC menu bar in this setting.
📖 Refer to 2.5.2 VNC Menu (page 32)

CAUTION

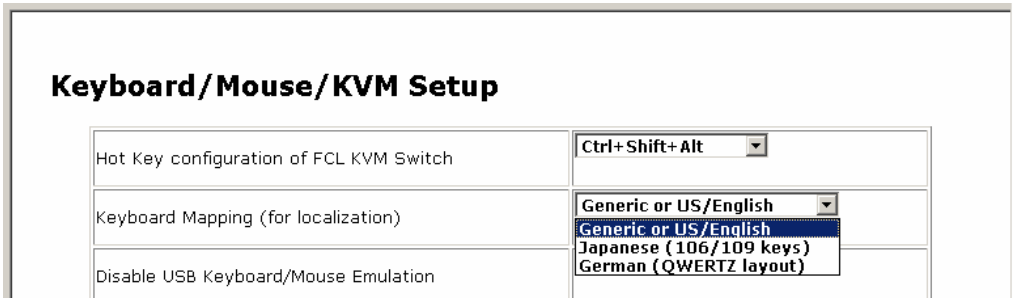
Connection with non-Fujitsu KVM switch is not supported.

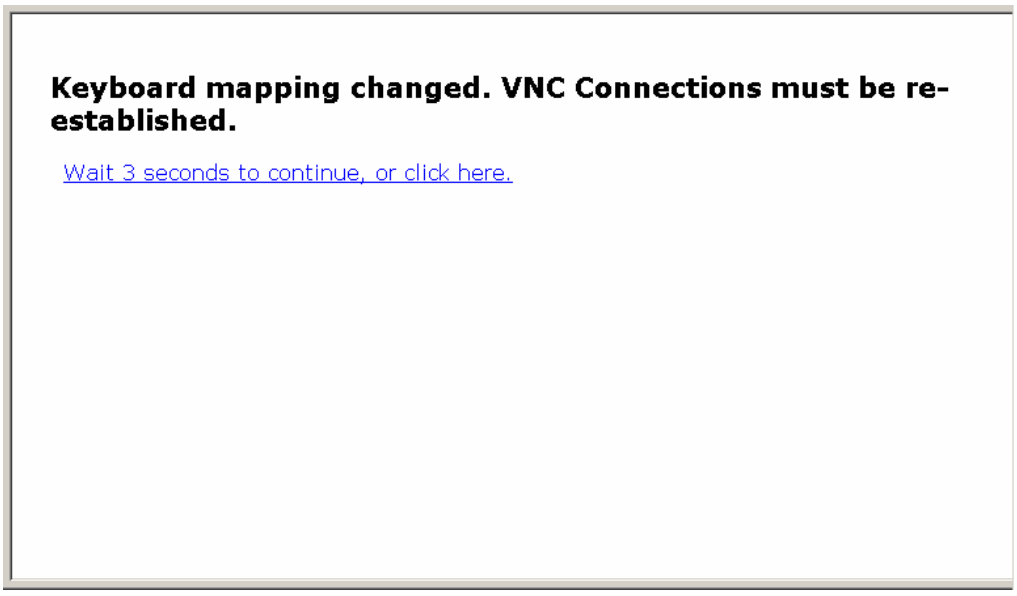
3.3.3.2 Keyboard Mapping (for localization)

Select the keyboard type to match the connecting host servers OS language. Three keyboards are available as follows.

- Japanese (106/109 keys)
- Generic or US/English
- German (QWERTZ layout)

Select the keyboard type from the list as in the following diagram. The selected setting is reflected immediately.





CAUTION

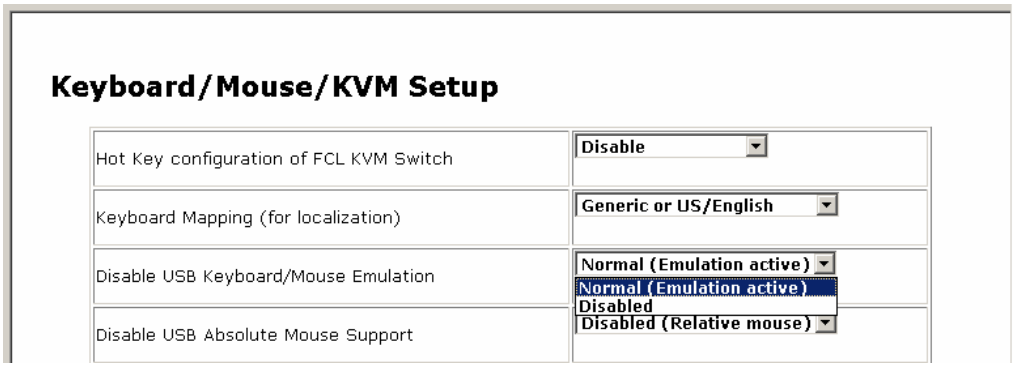
If the keyboard type is different from the host server OS language, unexpected key could be entered.

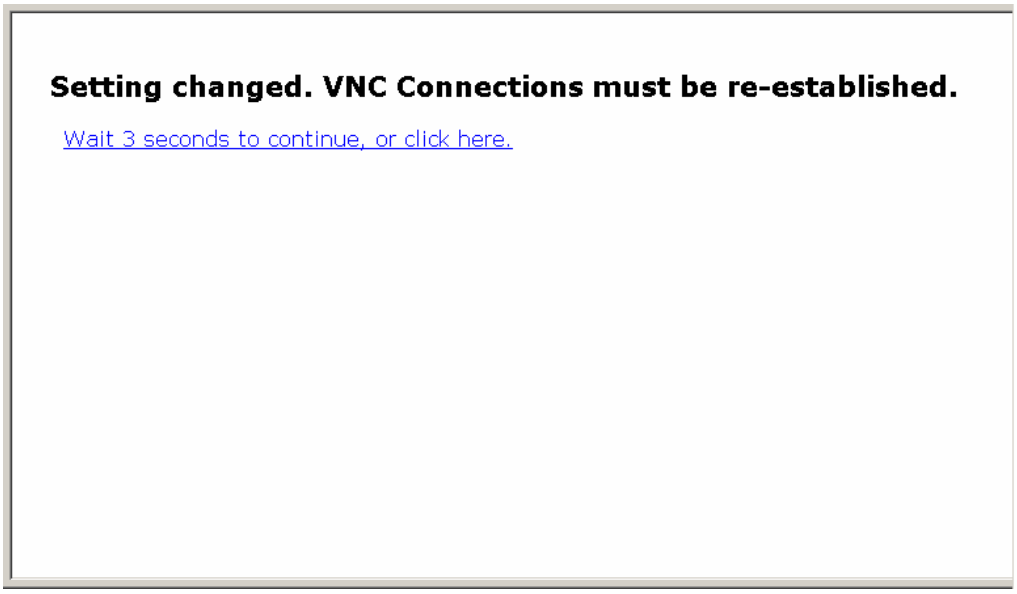
3.3.3.3 Disable USB Keyboard/Mouse Emulation

USB keyboard and mouse emulation setting is performed here.

When this product and the host server is connected by both PS/2 and USB cables and "disabled" is selected in this setting, the host server recognizes the PS/2 keyboard and mouse as connected.

Select enabled/disabled the USB keyboard/mouse emulation function from the list as follows. The selected setting is reflected immediately.





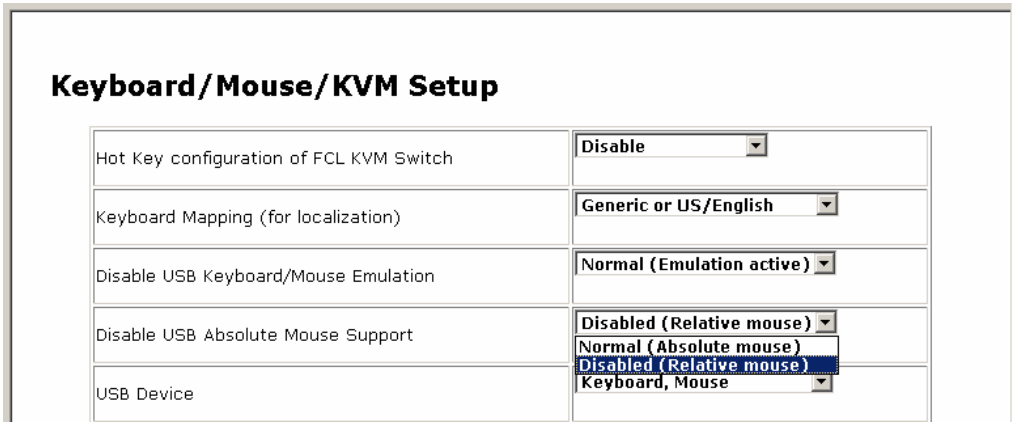
The virtual disk function is available even if the USB keyboard and mouse emulation is set to "disabled".

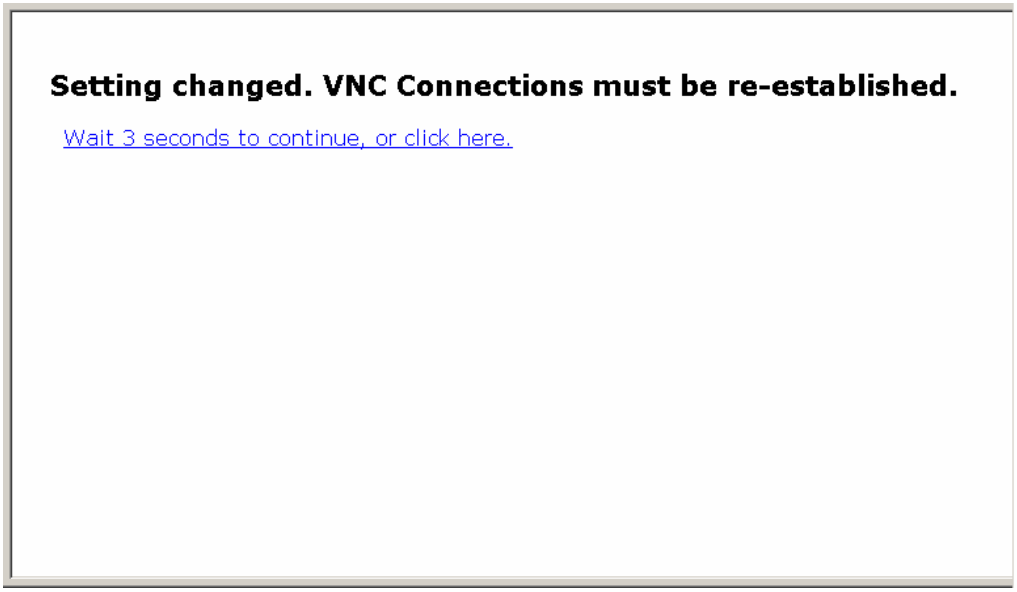
3.3.3.4 Disable USB Absolute Mouse Support

Select enabled/disabled the absolute mouse when this product and host server is connected with USB.

Absolute mouse: The mouse pointer does not move anywhere but the specified position (absolute-value).
Relative mouse: The mouse pointer will move more than the specified value.
Click mouse pointer correction button in the VNC menu bar to re-synchronize the cursor.

The USB absolute mouse is disabled by the default settings.
Select enabled/disabled from the list to change the absolute mouse setting as follows. The selected setting is reflected immediately.





CAUTION

If the USB absolute mouse setting is enabled, mouse pointer correction button and AutoSync setting display is displayed in gray.

3.3.3.5 USB Device

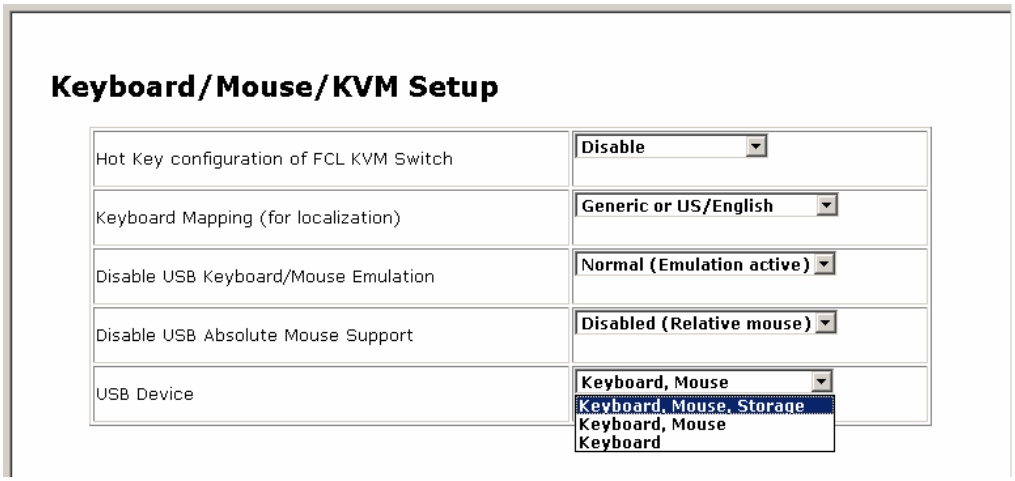
Set the USB keyboard, USB mouse and virtual USB device to be enabled/disabled when this product is connected to the host server with USB.
Default setting is [Keyboard, Mouse].

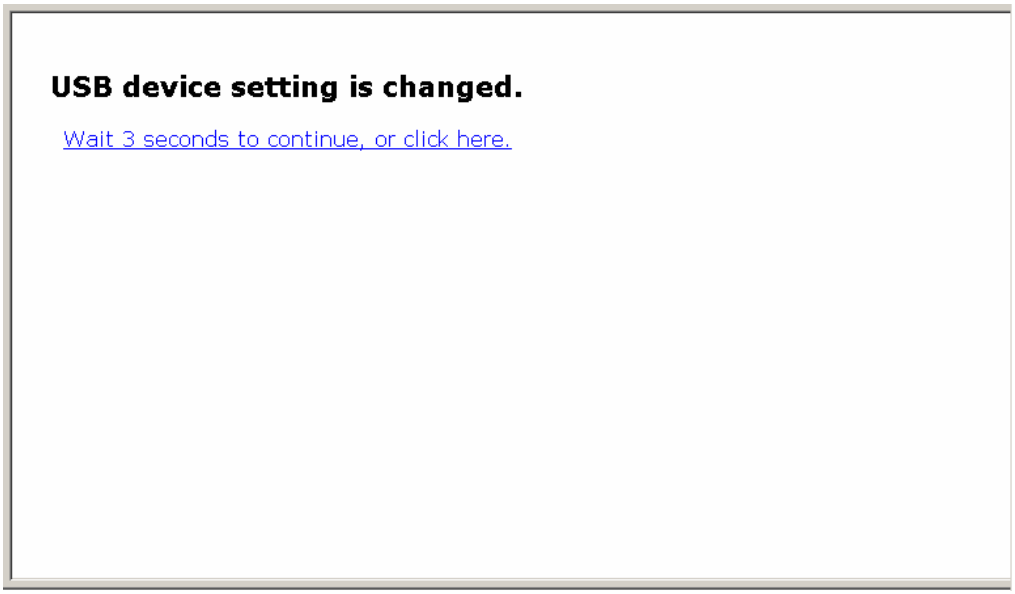
Keyboard, Mouse, Storage:
Enables to use the USB keyboard, USB mouse and USB virtual disk.

Keyboard, Mouse (**default setting**):
Enables to use the USB keyboard and USB mouse. USB virtual disk is disabled.

Keyboard:
Enables to use only the USB keyboard. USB virtual disk and mouse is disabled.

Select [Keyboard, mouse and storage] from USB device setting list to enable the USB virtual disk function as follows.
The setting is reflected immediately.





CAUTION

USB keyboard and mouse function is enabled only when the USB keyboard/mouse emulation setting is “Normal (Emulation active)".
USB keyboard and mouse do not work when the USB keyboard/mouse emulation setting is "disabled".

CAUTION

If the host server is rebooted, USB virtual disk function will be ”Disable” automatically.
When you use USB virtual disk function again after the host server starts, please set USB Device setup as [Keyboard, Mouse, Storage].

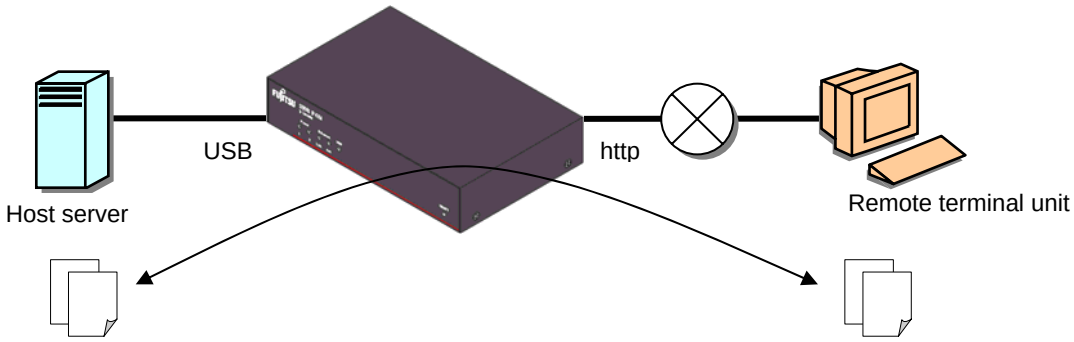
3.3.4 Virtual Disk Setting

Select [Keyboard, mouse and storage] from USB device setting list in the [Keyboard, mouse and KVM setting] page to enable the virtual disk function.
📖 Refer to 3.3.3.5 USB Device (page 89)

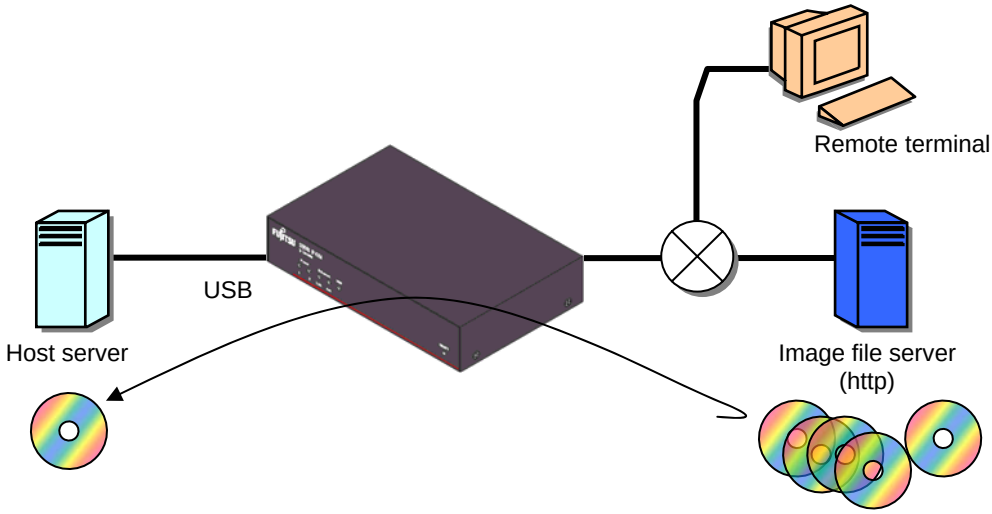
3.3.4.1 Outline of Functions

By connecting via USB to the host server, this product can be emulated to the host server as any of USB floppy disk, USB RAM disk, or USB CD-ROM drive.

Virtual floppy disk and RAM disk provides memory area of this product to the host server as virtual drive. This enables file data exchange between the host server and remote terminal units and facilitates the host server deployment process.



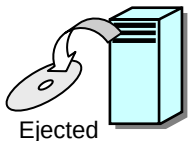
The virtual CD-ROM drive is realized by USB interface and image file server (http) established in the same network as this product. This product converts image files (iso file) to virtual CD-ROM drive and provides them to the host server.



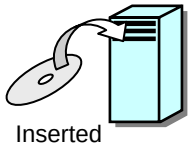
3.3.4.2 Virtual Disk Status

Virtual disk status must be changed [Ejected] from/to [Inserted] on the web page or VNC screen to use files in the virtual disk.

[Ejected]: Use (reference, save, addition and delete) virtual disk files in the remote terminal.

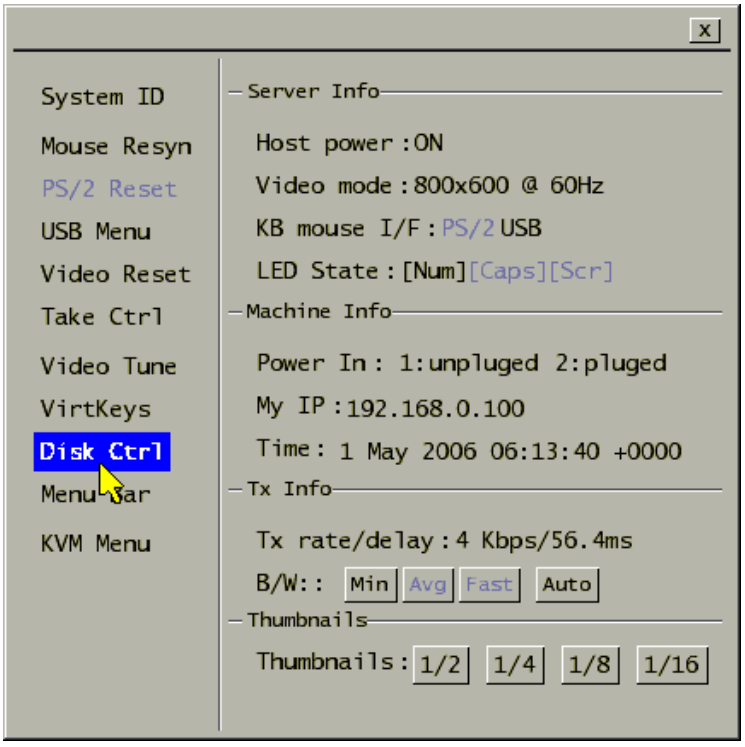


[Inserted]: The host server recognizes virtual disk as a USB drive. It is able to read and write the files in the virtual disk (Read only for virtual CD-ROM drive).

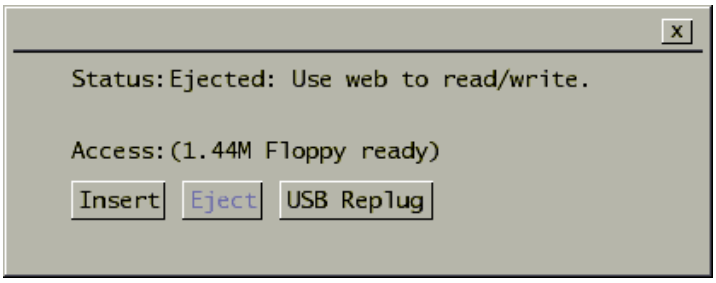


Switching virtual disk status in VNC screen method

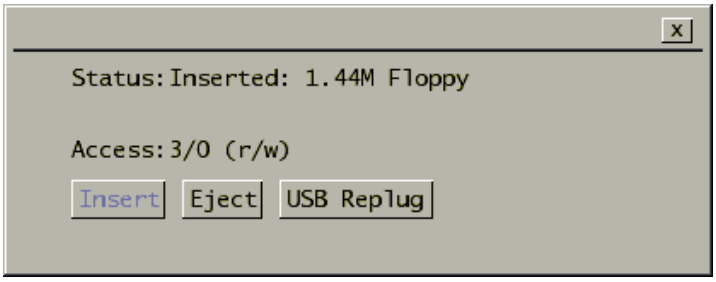
1. After VNC connection, click [Disk Ctrl] in the menu window to display the disk operation window.



2. The following message is displayed when the USB virtual disk status is [Ejected].
   Click [Insert] button to switch to [Inserted] status.



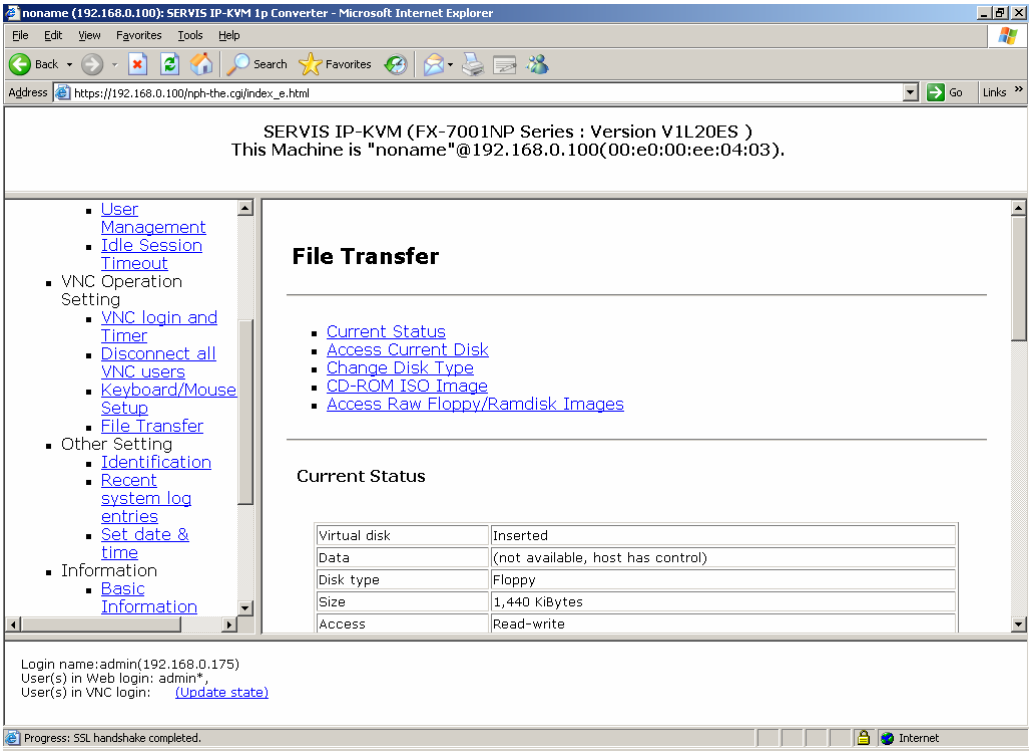
3. The following message is displayed when the USB virtual disk status is [Inserted].
   Click [Eject] button to switch to [Ejected] status.

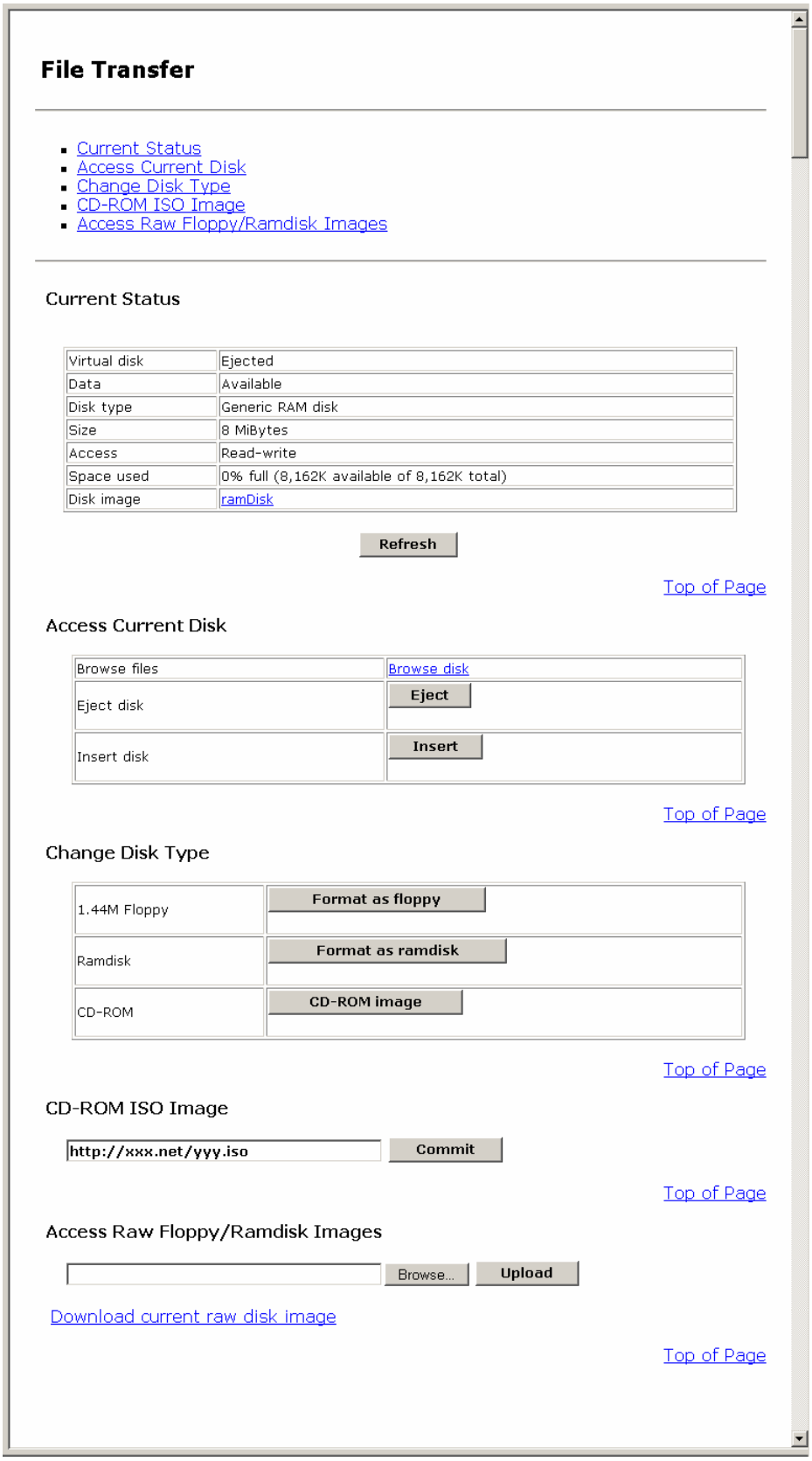


Disk operation window screen and operating method

Disk Operation Window	
Status:	Display the insert or eject status of virtual disk. Ejected: the host server does not recognize Virtual disk. Inserted: Host server recognizes the virtual disk.
Access:	Display the USB disk type (CD-ROM, 8M RAM, Floppy).
Insert	Insert the virtual disk. (The menu is displayed in gray while the disk is inserted.) This will enable the host server to recognize the virtual disk.
Eject	Eject the virtual disk. (The menu is displayed in gray while the disk is not inserted.) This will enable remote user to access the virtual disk.
USB Replug	Disconnect the USB connection and connect again.
x	Close the [Disk operation] window.

Click File Transfer from the menu selecting area and for virtual disk setting on the web page is performed on the following page.





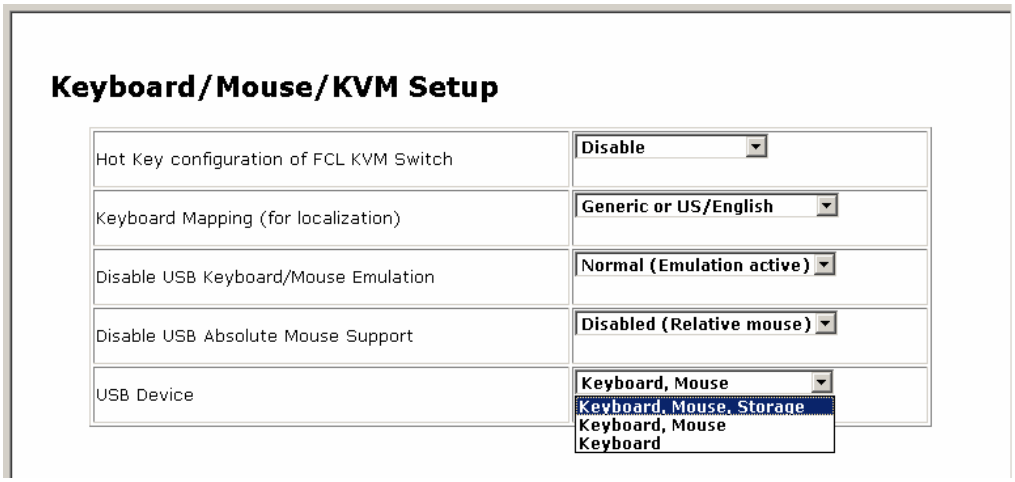
Refer to the following steps for detailed operation methods of three different virtual disks.

3.3.4.3 Virtual Floppy Disk

This function makes the host server recognize this product as 1.44M-floppy disk drive and enable file transfer between remote terminal and the host server.
Virtual floppy disk drive setting method is described below. (The following method is for the Windows OS host server.)

Setting Procedure

1. Select [Keyboard, Mouse, Storage] from the [Keyboard/Mouse/KBM Setup] page for USB device setting.
   📖 Refer to 3.3.3.5 USB Device (page 89)



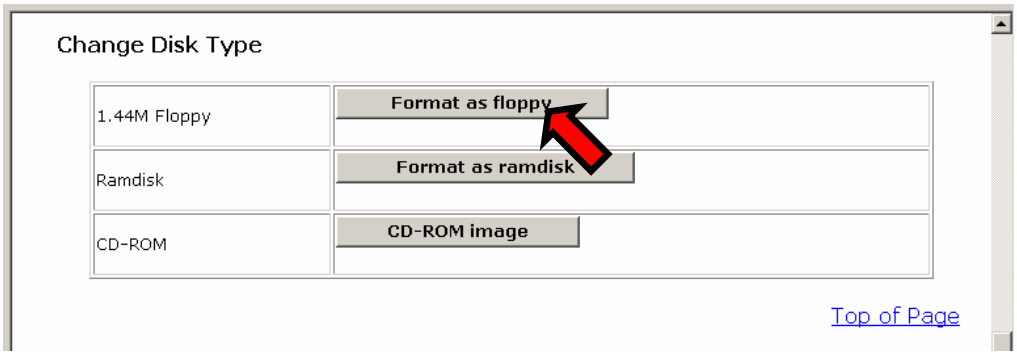
CAUTION

If the host server is rebooted, USB virtual disk function will be ”Disable” automatically.
When you use USB virtual disk function again after the host server starts, please set USB Device setup as [Keyboard, Mouse, Storage].

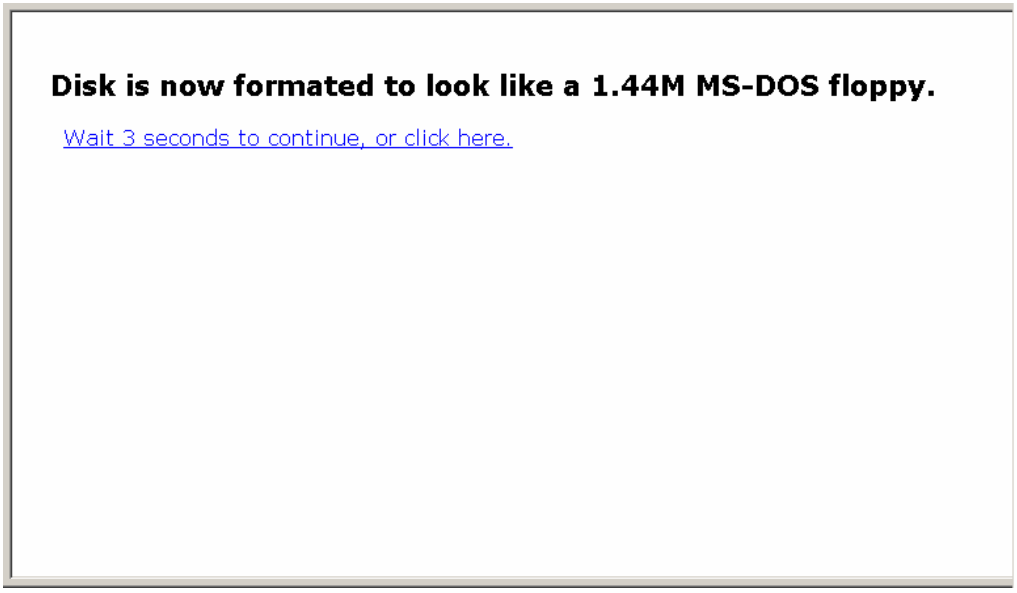
In the case where it sets up on the Web page:
📖 Refer to 3.3.3.5 USB Device (page 89)

In the case where it sets up on the VNC window:
📖 Refer to 2.5.9 USB Setting Window (page 47)

2. Click [Format as floppy] in the File Transfer page.

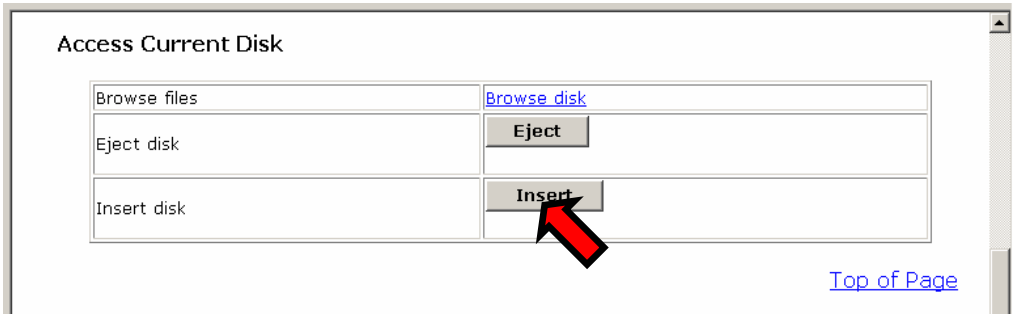


3. The following message is displayed. The setting is reflected after 3 seconds and return to the File Transfer page.



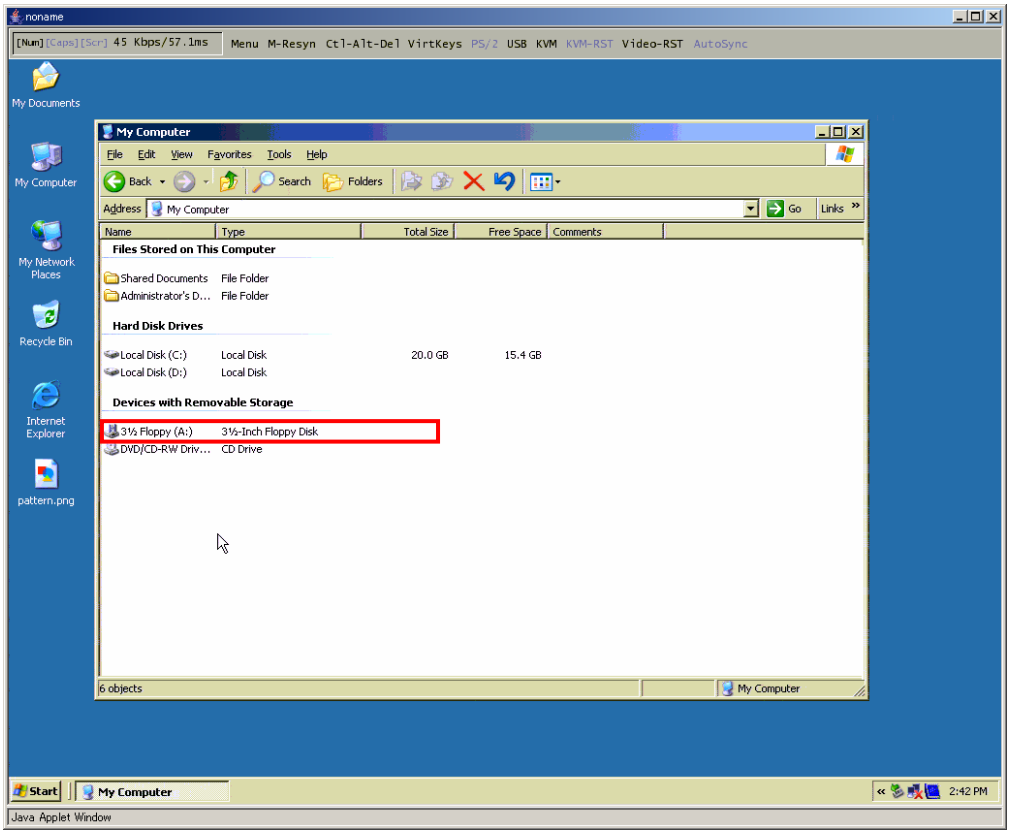
The disk is formatted as 1.44M floppy disks for MS-DOS (for Windows).

4. Click [Insert] button.

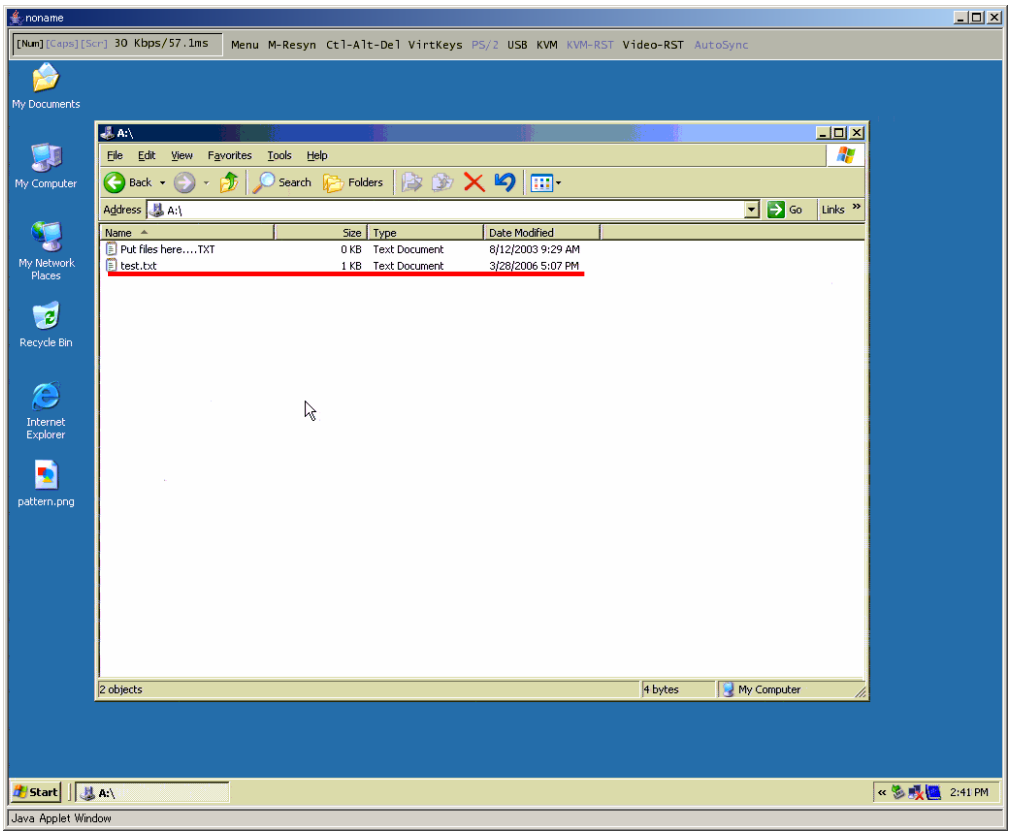


5. The following message is displayed and the virtual disk is inserted in the host server. Returns to the File Transfer page after 3 seconds.

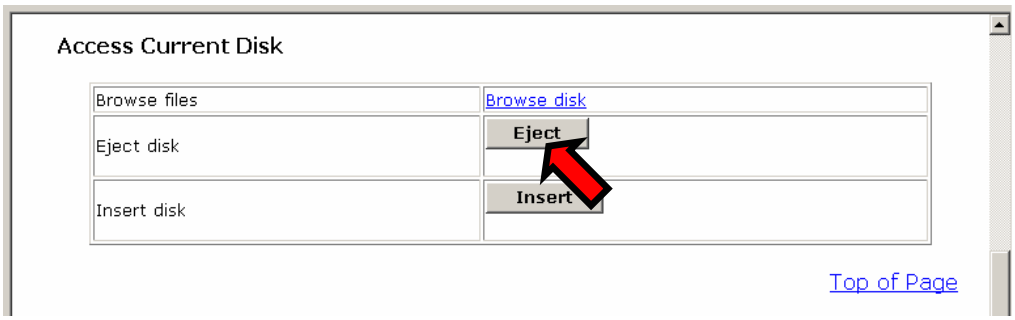
6. Execute VNC login and check [My computer] in the host server. The new disk is recognized as [3.5 inch floppy disk].



7. You can save the files in the host server as follows.



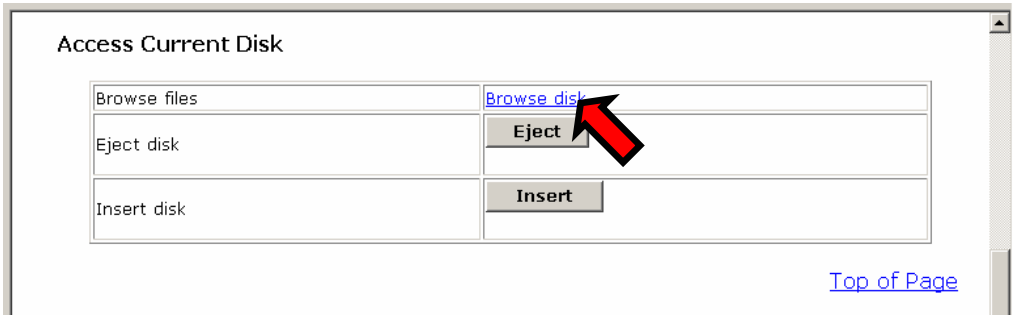
8. The following provides the method to refer to the files in the host server from the remote terminal. Return to File Transfer page and click [Eject] button.



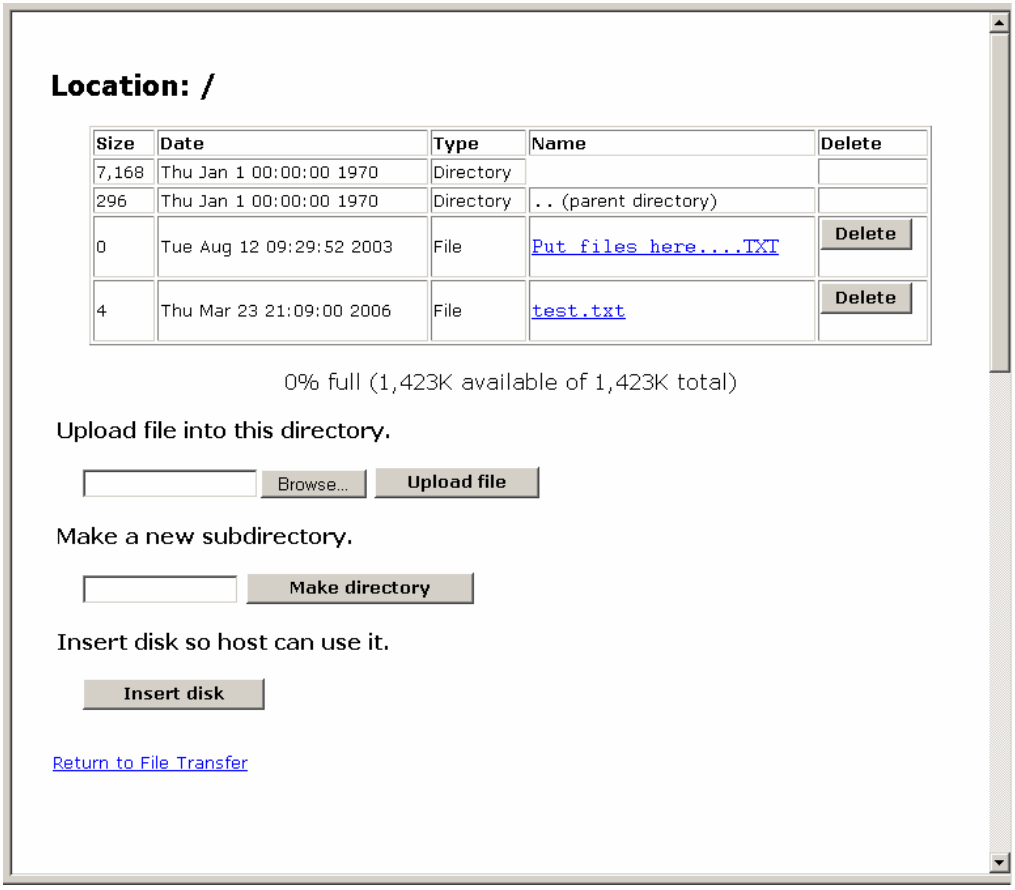
The following dialogue box is displayed. Click [OK] button.

The following message is displayed and the virtual floppy disk is ejected from the host server.

9. Click Browse disk after ejecting the virtual disk.



10. The directories and file contents in the virtual disk are displayed as follows. The files saved in the host server can be confirmed.

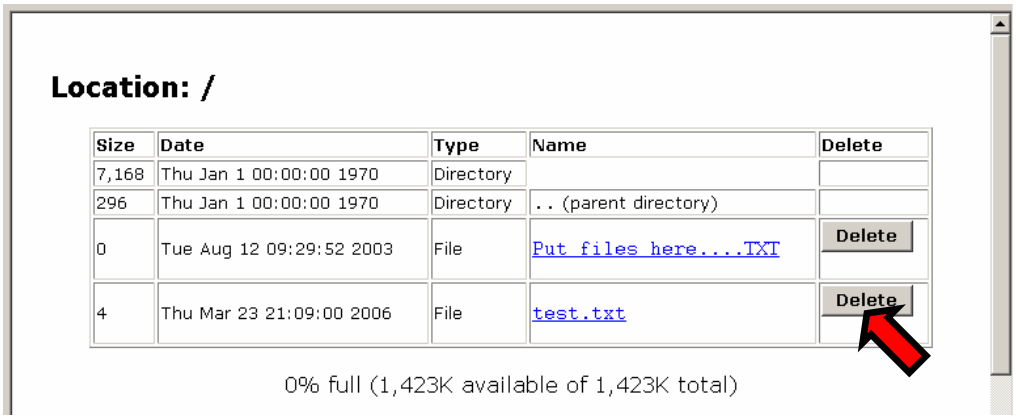


Click the file name to display that file in the html form.

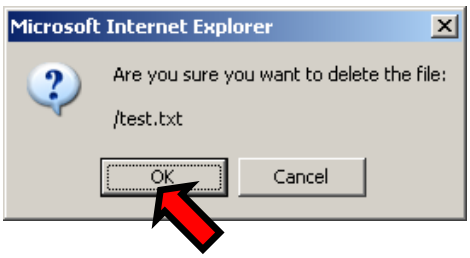
CAUTION

Virtual disk status must be [Ejected] to confirm its contents.
The file larger than 1.4M-byte cannot be saved.

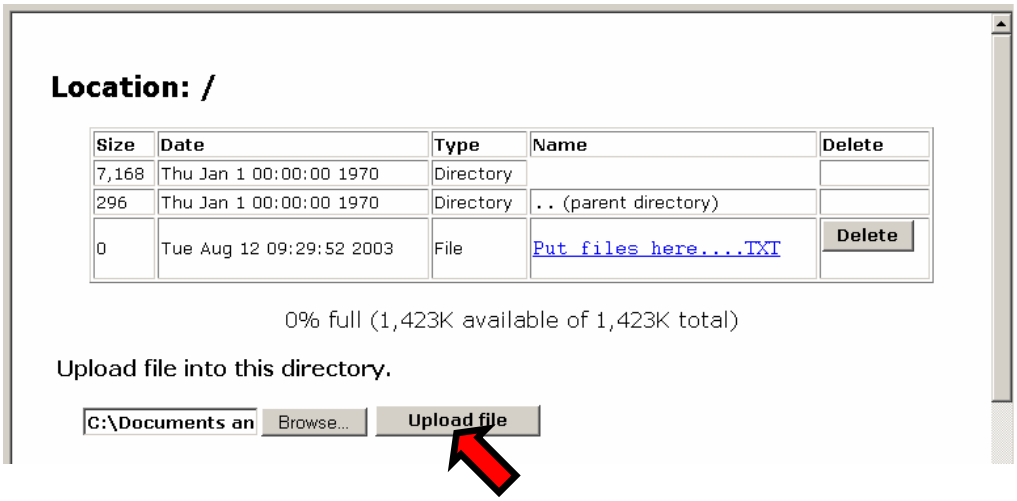
Click [Delete] button to delete the file.



The following confirmation dialogue box is displayed. Click [OK] to delete the file.



11. To upload the files to the virtual disk, specify the path of the files in the remote terminal and click [Upload file] button.



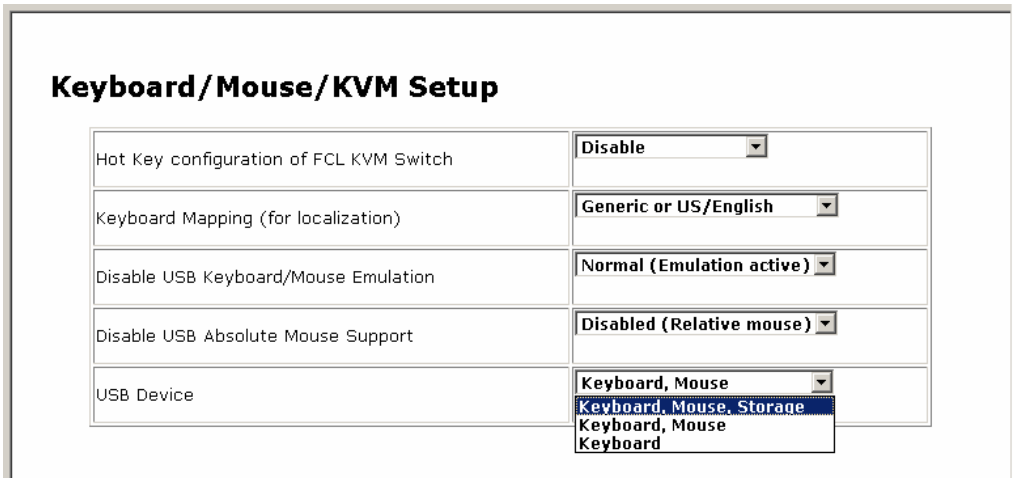
The file uploaded from the remote terminal can be handled at the host server.

3.3.4.4 Virtual RAM Disk

This function makes the host server recognize this product as 8M-RAM disk drive and enable to file transfer between remote terminal and the host server.
Virtual RAM disk drive setting method is described below.
(The following method is for when the host server is Windows OS).

Setting Procedure

1. Select [Keyboard, Mouse, Storage] from the [Keyboard/Mouse/KVM Setup] page for USB device setting.
   📖 Refer to 3.3.3.5 USB Device (page 89)



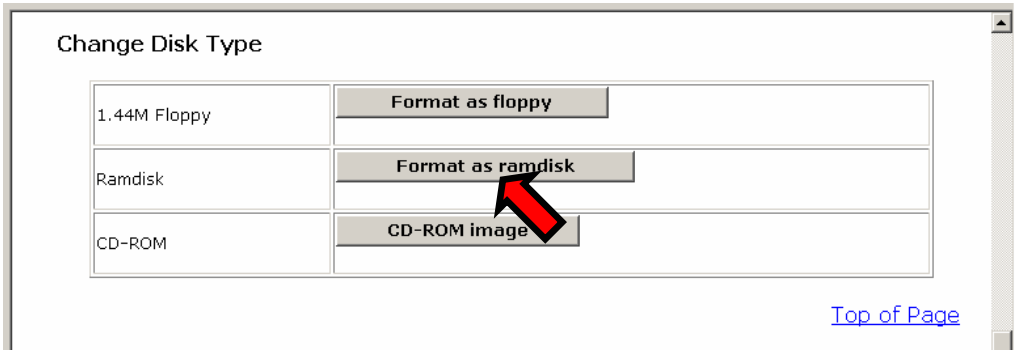
CAUTION

If the host server is rebooted, USB virtual disk function will be ”Disable” automatically.
When you use USB virtual disk function again after the host server starts, please set USB Device setup as [Keyboard, Mouse, Storage].

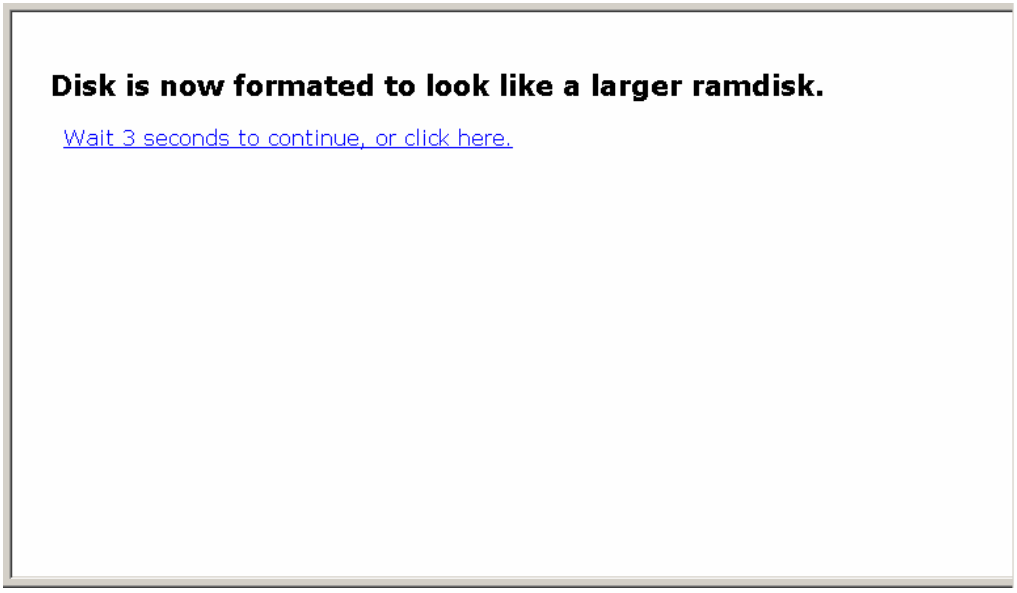
In the case where it sets up on the Web page:
📖 Refer to 3.3.3.5 USB Device (page 89)

In the case where it sets up on the VNC window:
📖 Refer to 2.5.9 USB Setting Window (page 47)

2. Click [Format as ramdisk] in the File Transfer page.

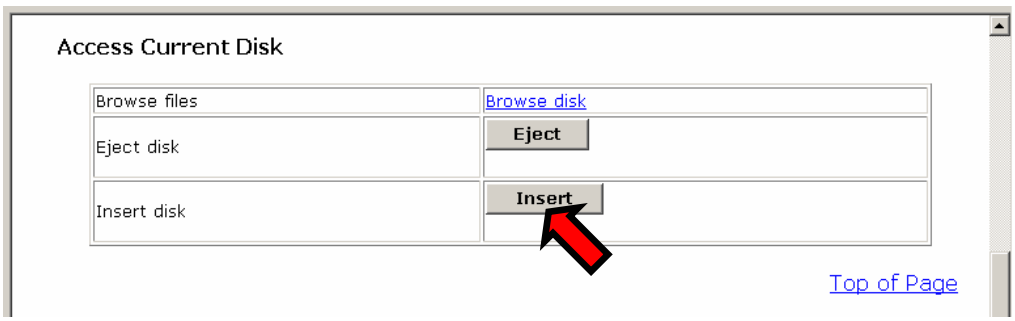


3. The following message is displayed. The setting is reflected after 3 seconds and the screen returns to File Transfer page.



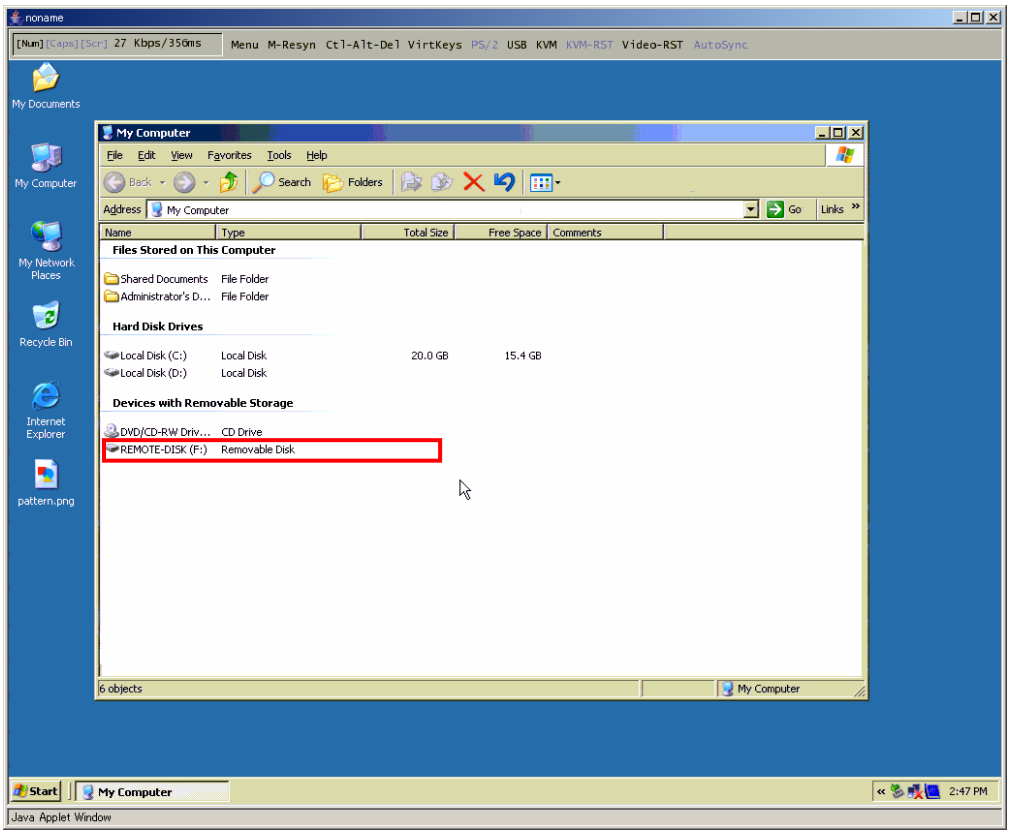
The disk is formatted as 8M-RAM disk for MS-DOS (for Windows).

4. Click [Insert] button.

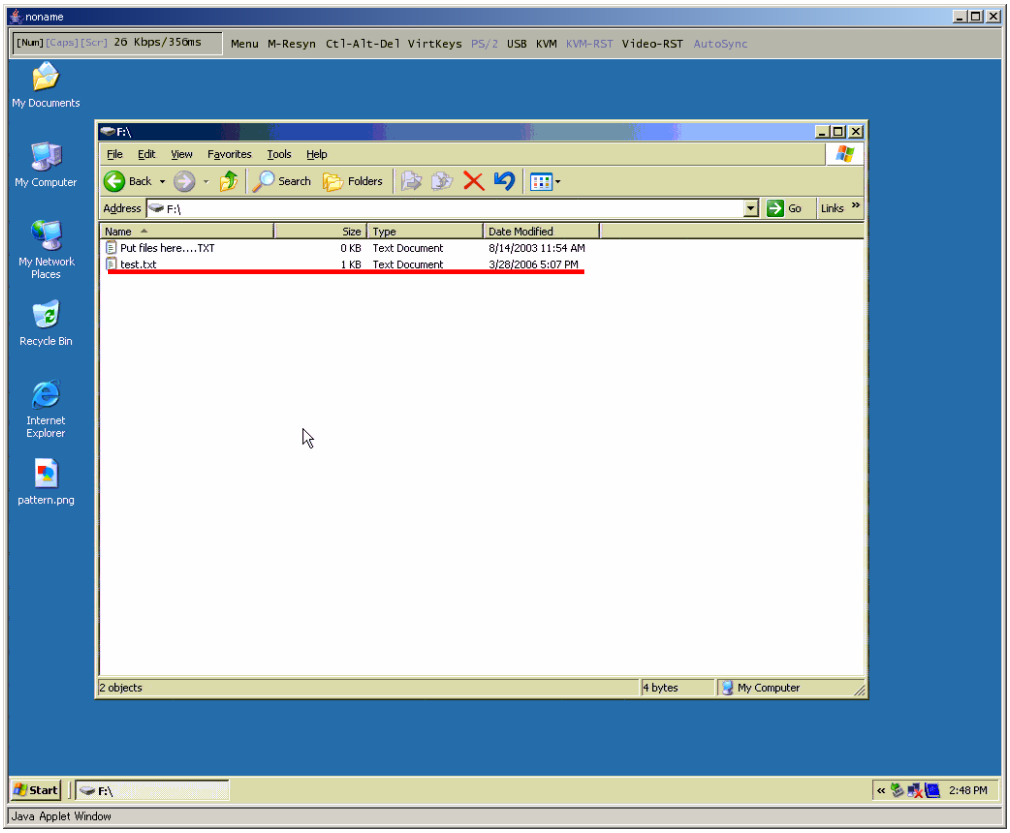


5. The following message is displayed and the virtual disk is inserted in the host server. Return to the File Transfer page after 3 seconds.

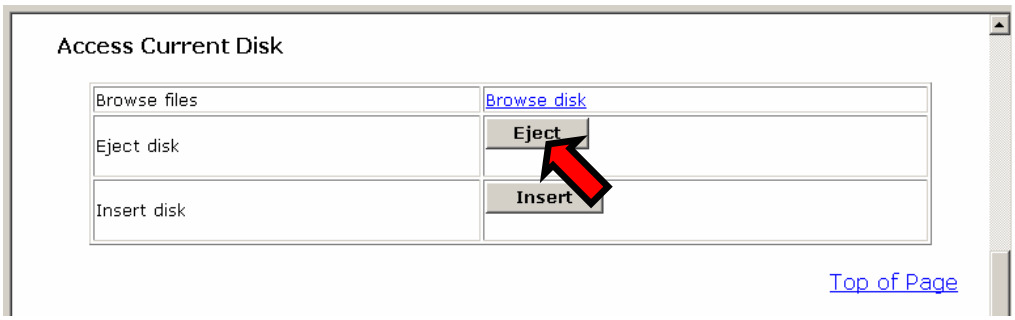
6. Execute VNC log on and check [My computer] in the host server. The new disk is recognized as [Removable disk].



7. You can save files on the host server as follows.



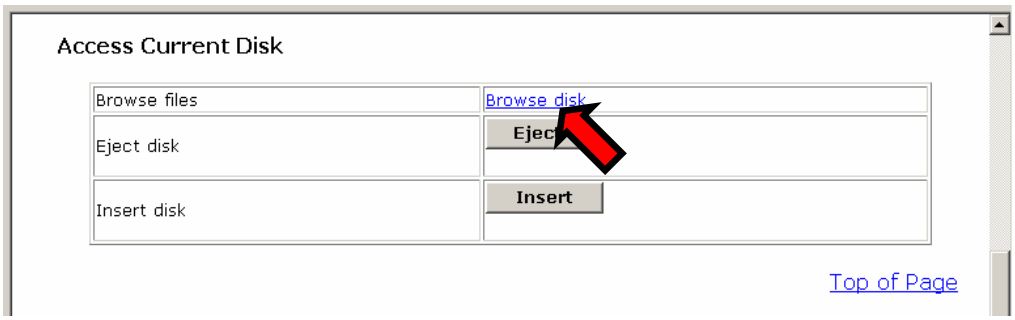
8. Transmit the files saved in the host server to the remote terminal unit. Back to File Transfer page and click [Eject] button.



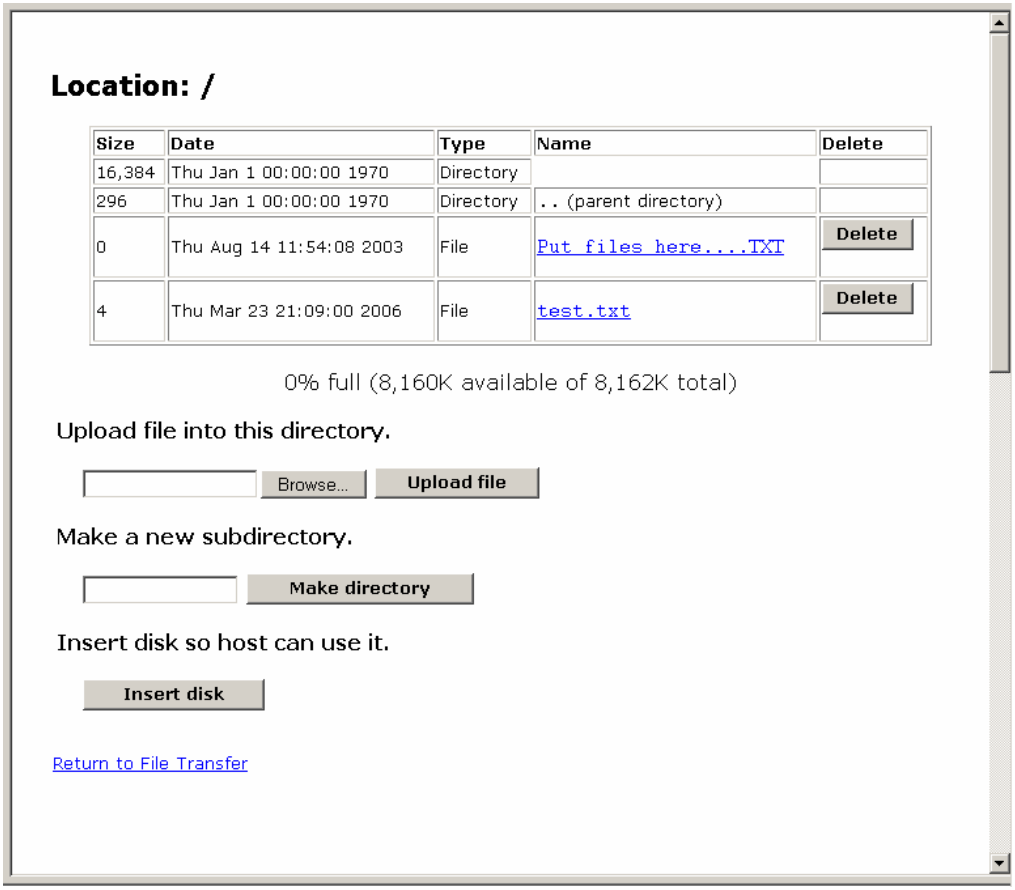
The following dialogue box is displayed. Click [OK] button.

The following message is displayed and the virtual RAM disk is ejected from the host server.

9. Click Browse disk after ejecting the virtual disk.



10. The directories and file contents in the virtual disk are displayed as follows. The files saved in the host server can be confirmed.

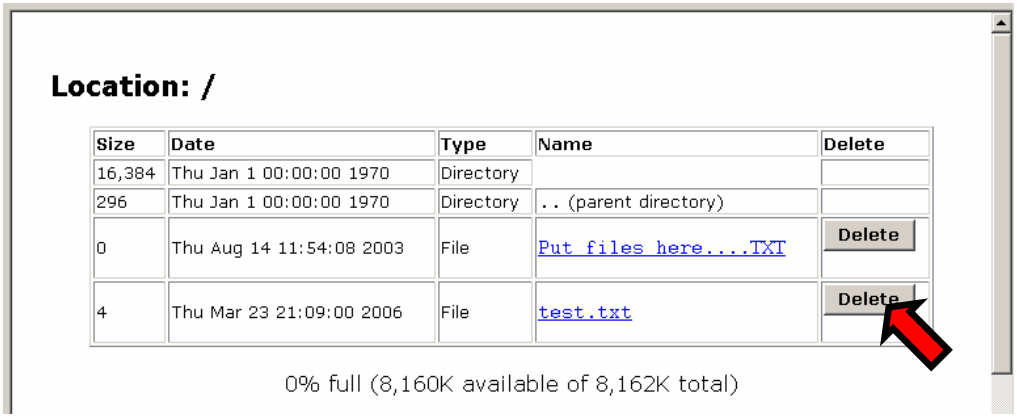


Click the file name to display that file in the html form.

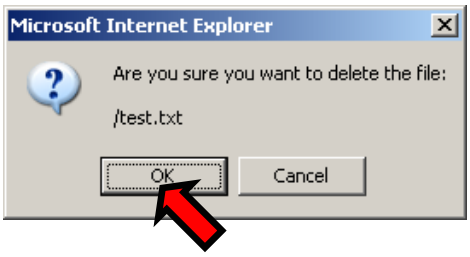
CAUTION

Virtual disk status must be [Ejected] to confirm its contents.
The file larger than 8M-byte cannot be saved.

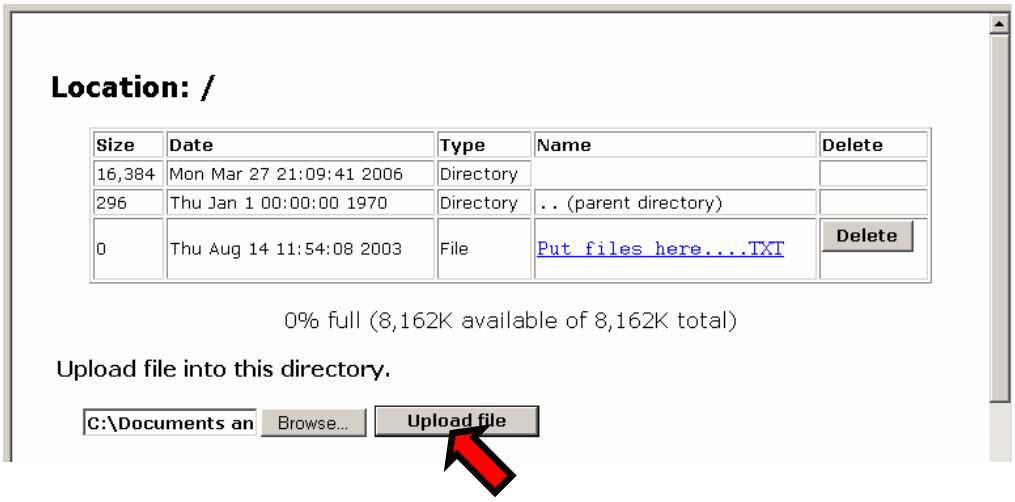
Click [Delete] button to delete the file.



The following confirmation dialogue is displayed. Click [OK] to delete the file.



11. To upload the file to the virtual disk, specify the path of the file in the remote terminal and click [Upload file] button.



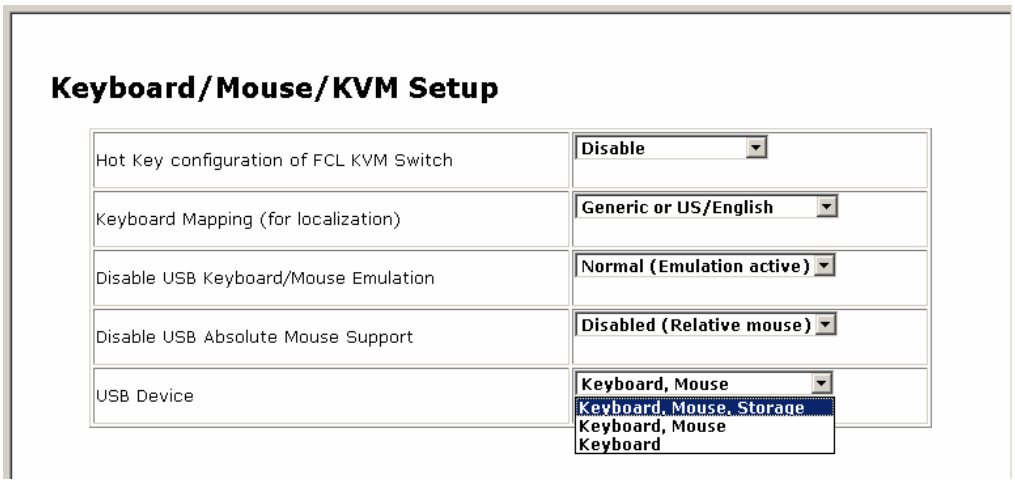
The uploaded file from the remote terminal can be handled at the host server.

3.3.4.5 Virtual CD-ROM Drive

By specifying the URL for the ISO files in the file server, the product can be emulated to the host server as a virtual CD-ROM drive.
ISO files are emulated in the accessible file server of this product.
Store the ISO files in the online file server.
The virtual CD-ROM drive setting method is described below. (The following method is for the Windows OS host server.)

Setting Procedure

1. Select [Keyboard, Mouse, Storage] on the [Keyboard/Mouse/KVM Setup] page for USB device setting.
📖 Refer to 3.3.3.5 USB Device (page 89)



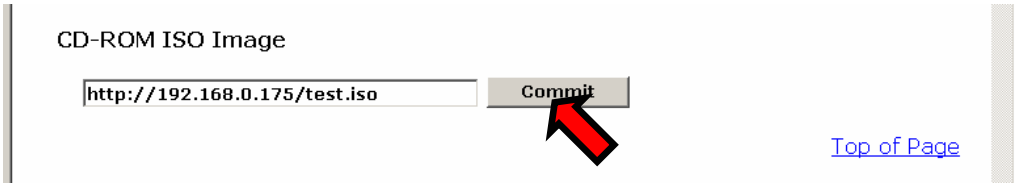
CAUTION

If the host server is rebooted, USB virtual disk function will be ”Disable” automatically.
When you use USB virtual disk function again after the host server starts, please set USB Device setup as [Keyboard, Mouse, Storage].

In the case where it sets up on the Web page:
📖 Refer to 3.3.3.5 USB Device (page 89)

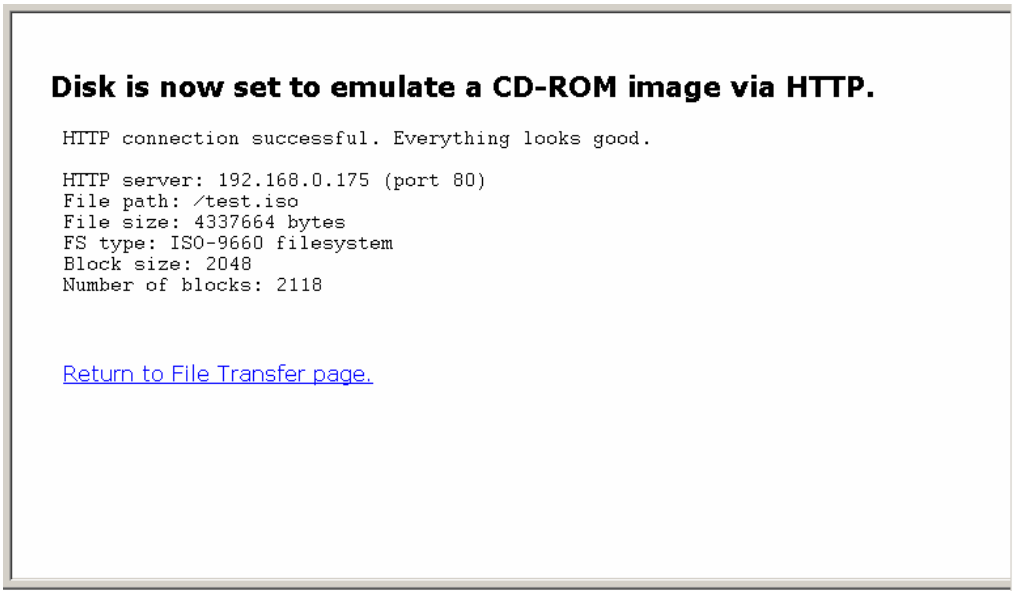
In the case where it sets up on the VNC window:
📖 Refer to 2.5.9 USB Setting Window (page 47)

2. Specify URL for ISO files to the [CD-ROM ISO image] in the [File Transfer] page and click [Commit] button.

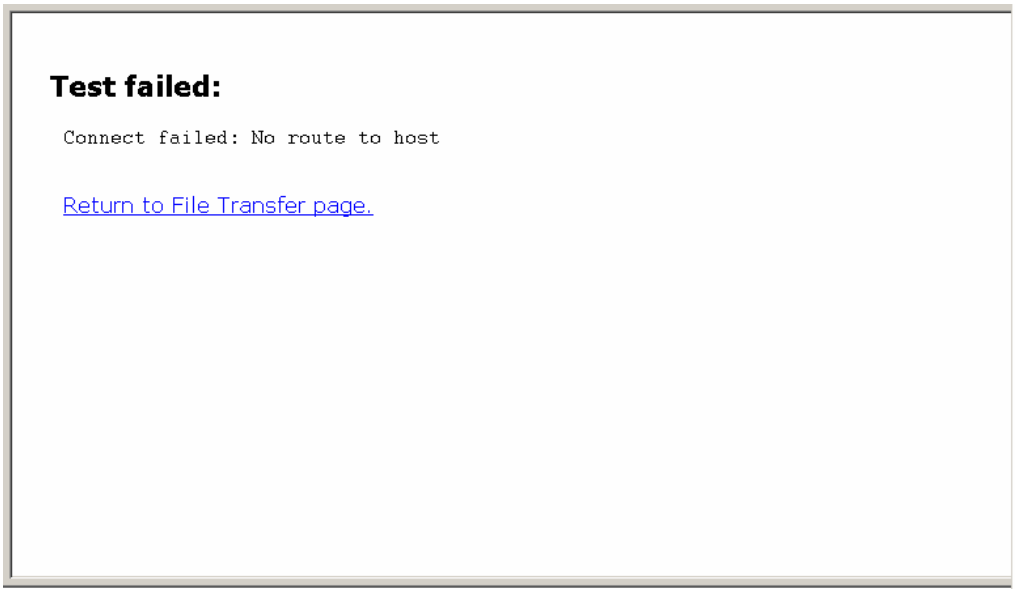


(It is also specified by entering the URL and clicking [CD-ROM image] button.)

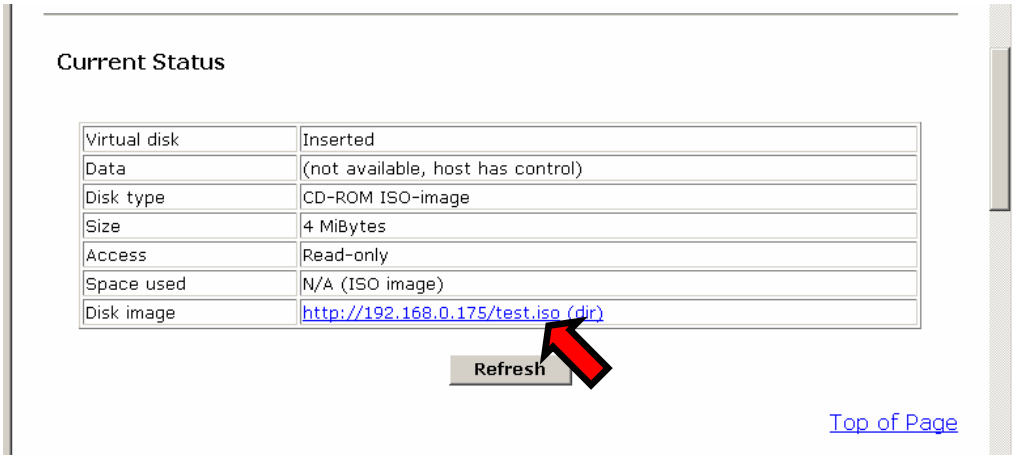
3. When iso files exist in the online file server, it is displayed as follows. Click Return to File Transfer page.



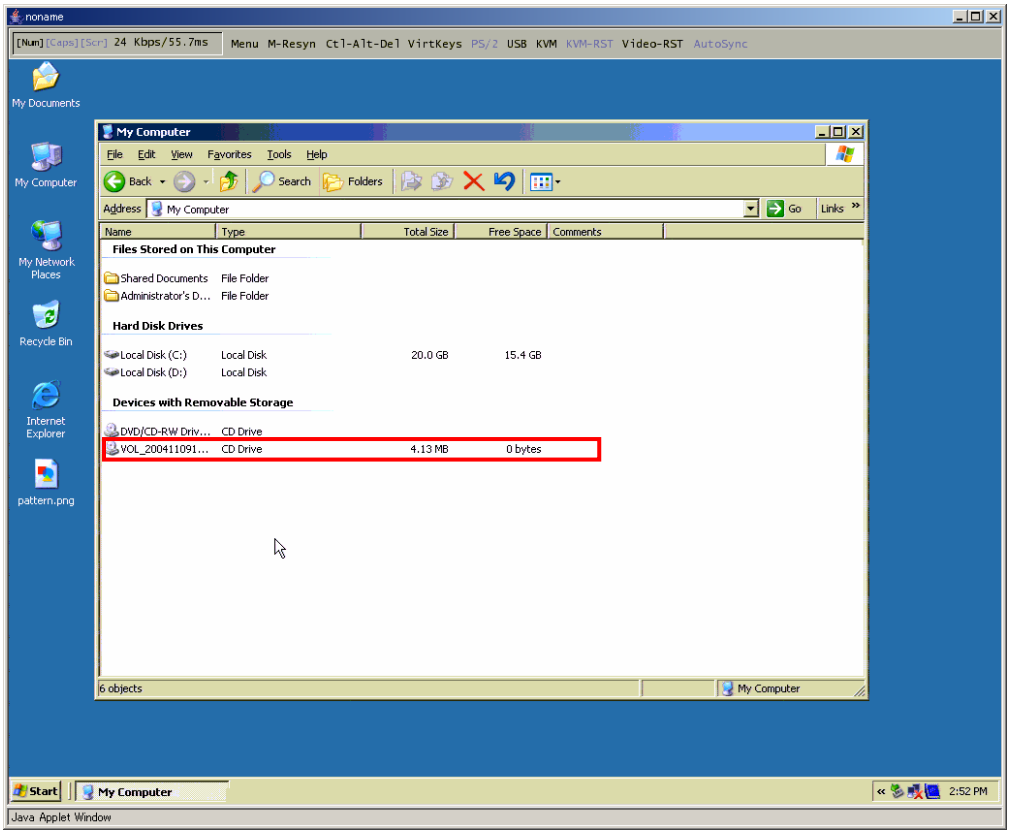
If the link failed or the ISO files are disabled, the following message is displayed and the virtual CD-ROM function could not execute.



4. Check [Current Status] in File Transfer page. If [Virtual disk] is "Inserted", the host server recognizes the virtual CD-ROM.
   By clicking [Disk Image] URL, it is also able to download ISO files from the file server to the operating terminal.



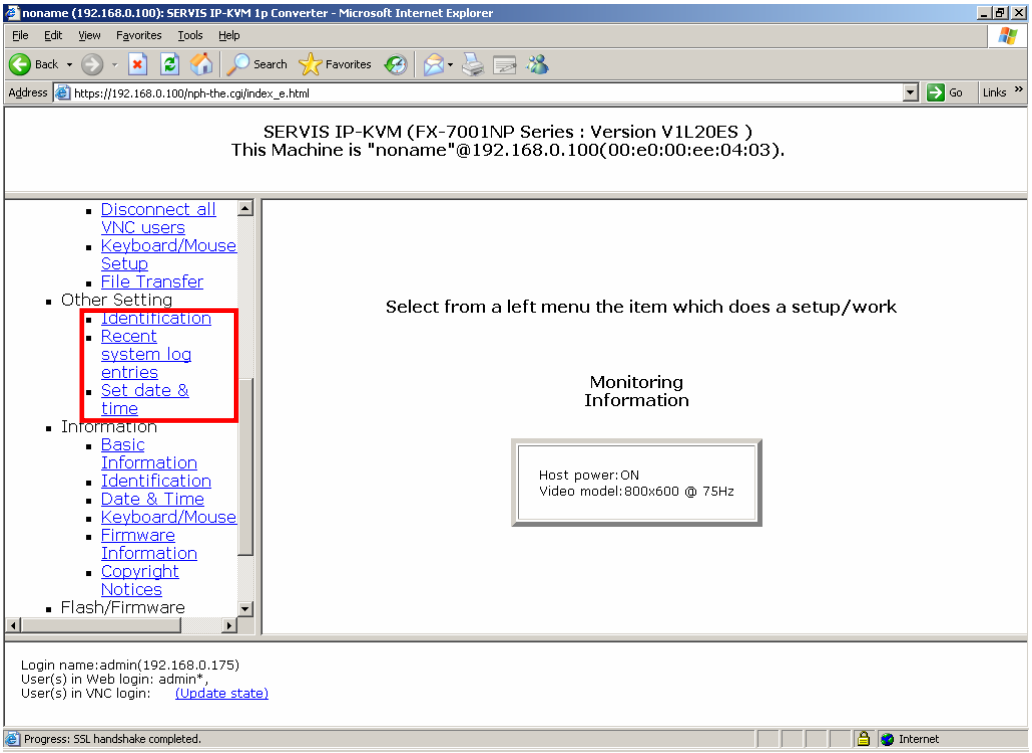
5. Execute VNC log on and check [My computer] in the host server. It is confirmed that the CD-ROM drive is recognized.



The CD-ROM drive is accessible in this status (Read only).

3.4. Other Setting

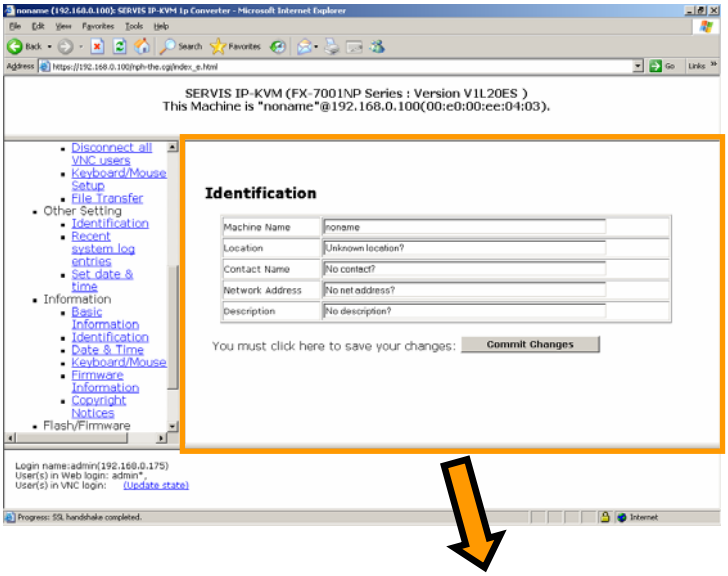
This section provides explanations for other setting items.

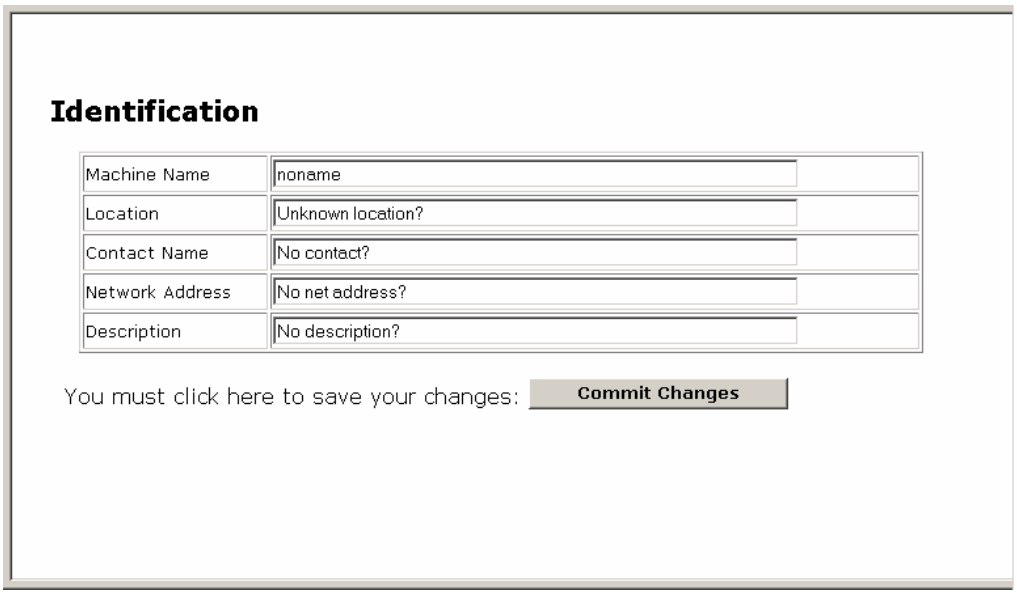


3.4.1 Identification

Click Identification from the menu-selecting area, the following setting page is displayed.
Set the identification name and identifier settings for this product.
The setting value is displayed as device information in the System ID Window of the VNC connection.
📖 Refer to 2.5.4 System ID Window (page 37)

It has no effect on the operation, even if it is not set.





- Machine Name

  Name to identify this product. The Machine Name is enabled to provide HCP server as the "client name" when you create DNS entry conform to this name. It is also to be displayed in the each top of web browser interface pages and used as "desktop name" for the VNC client.

- Location

  Enter the information where the system is located. This value transmitted as system.sysLocation value via SNMP.

- Contact Name

  Enter the contact information relating to this product. (Usually enter e-mail address etc.)
  This value is transmitted as the system.sysContact via SNMP.

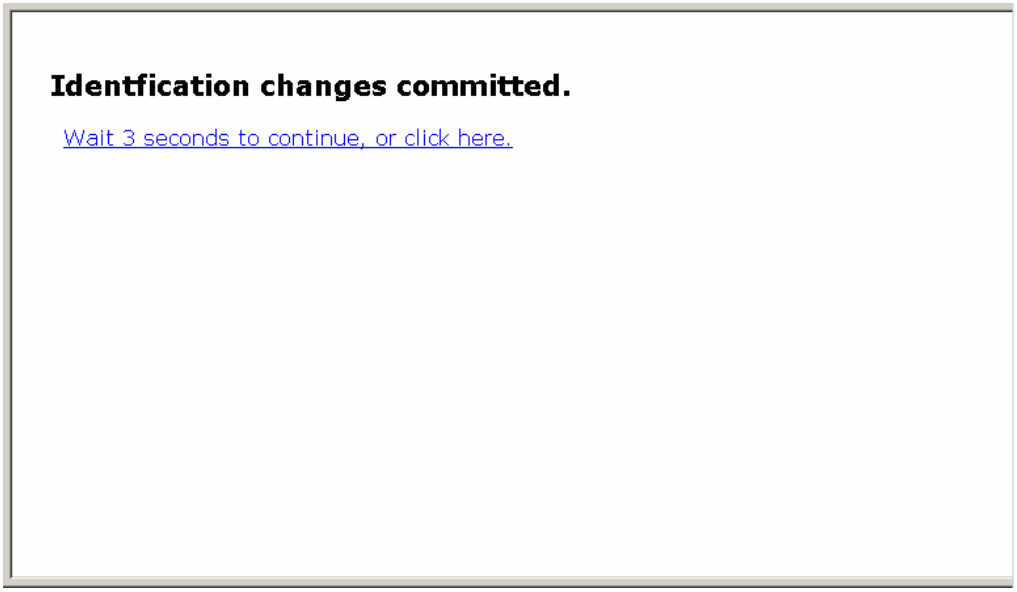
- Network Address

  This value is not used for system configuration, but it stores user-defined value to identify the operated device in the network. Enter the DNS name for the operating device. This item is not required and can be used at your discretion.

- Description

  Enter the user-defined descriptions for controlled devices.

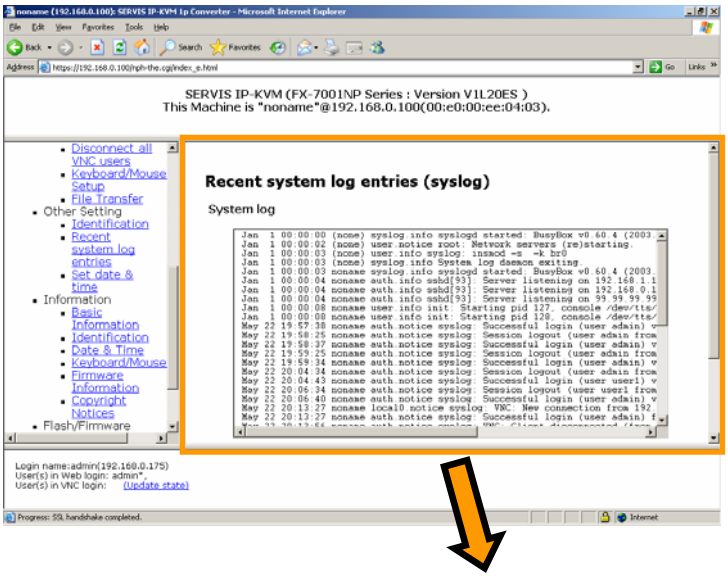
After entering the setting, click the [Commit Changes] button. The following message is displayed and the setting is reflected.

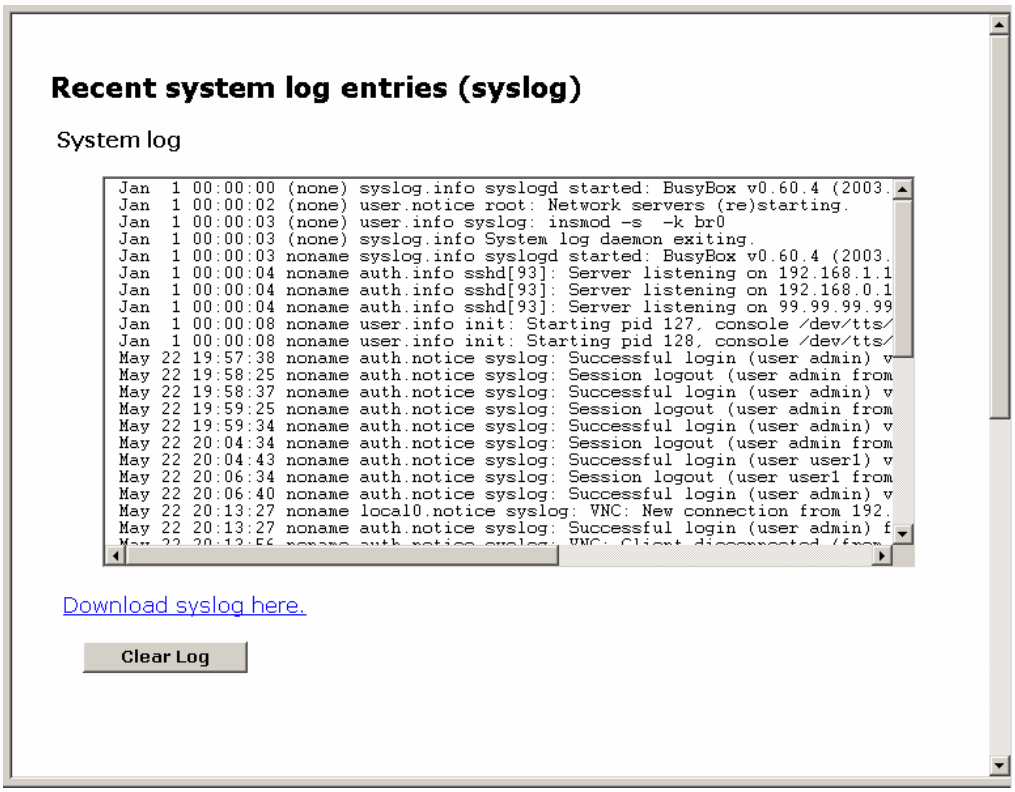


No Japanese font is acceptable for system ID setting. Use English one-byte characters for this item.

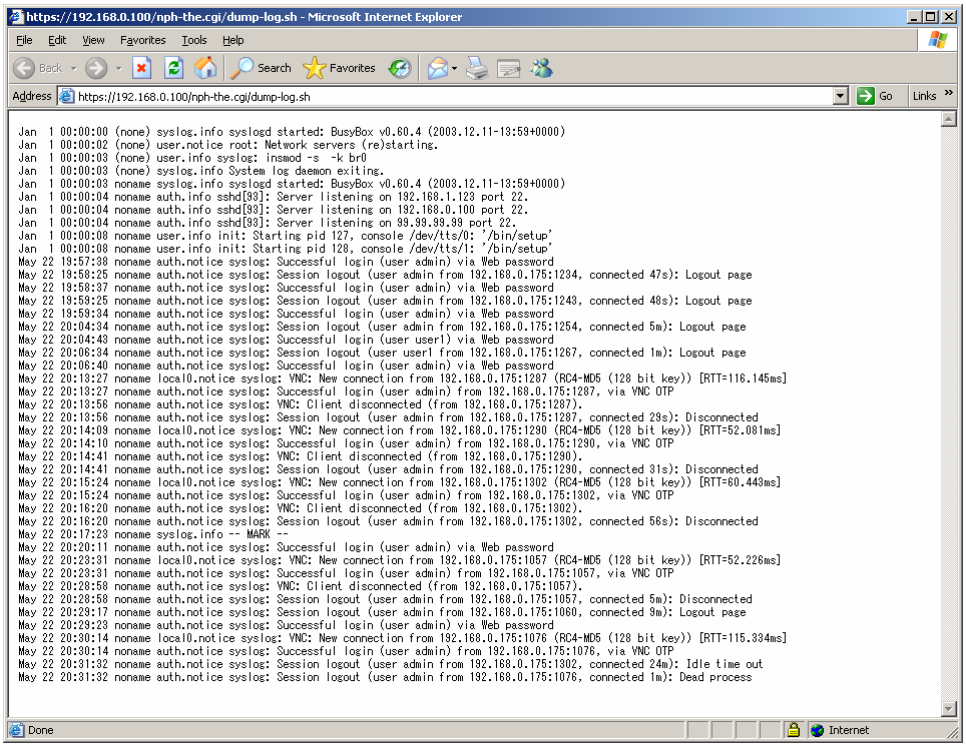
3.4.2 Recent system log entries

Click Recent system log entries from the menu-selecting area, the following setting page is displayed.
Specify system log items in this page.

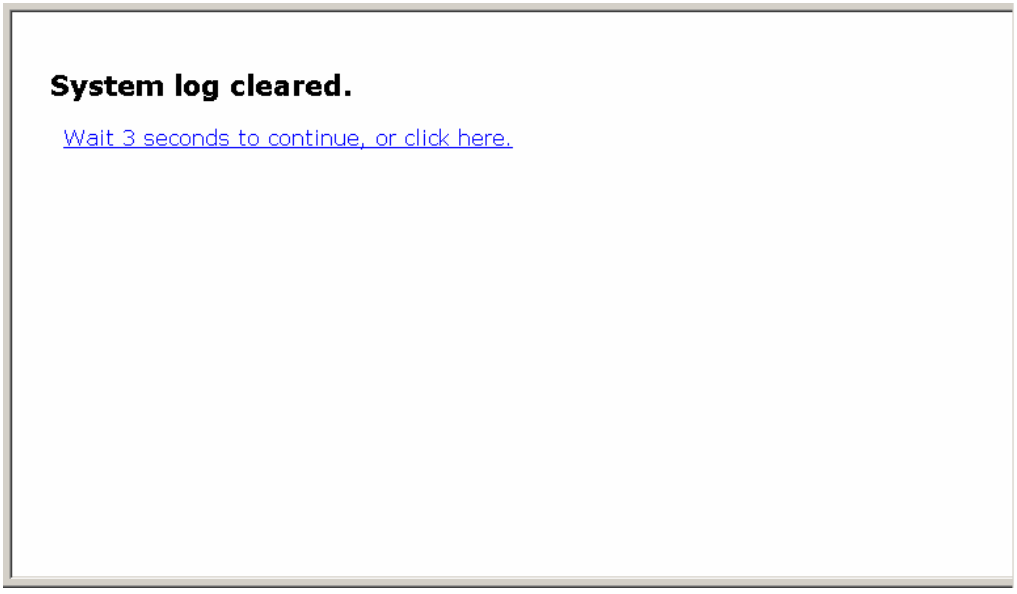




Click [Download syslog here.] to display system logs in another window.

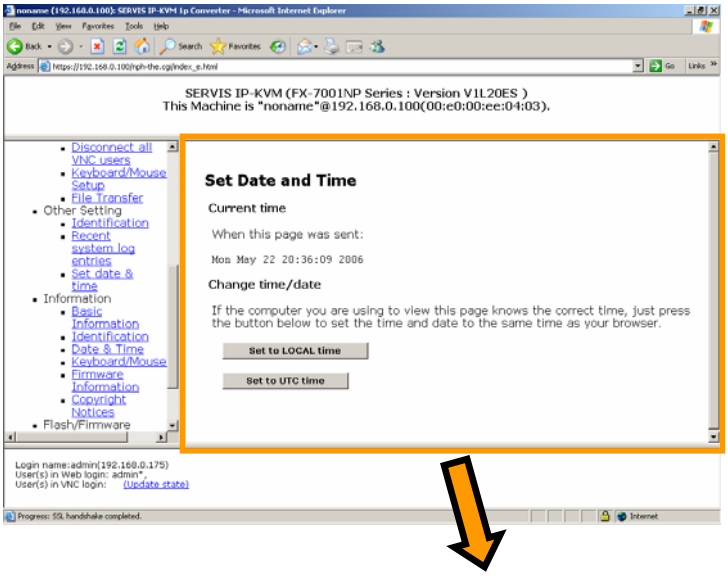


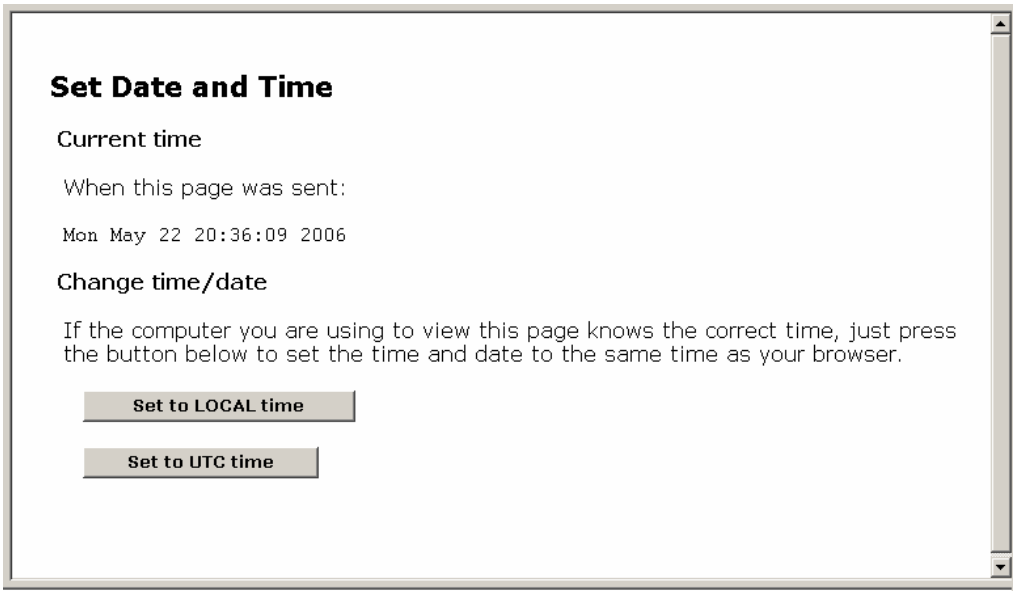
Click the [Clear Log] button. The following message is displayed and the system log is cleared.



3.4.3 Set date & time

Click Set date & time from the menu-selecting area and the following setting page is displayed. Specify date and time settings in this page.

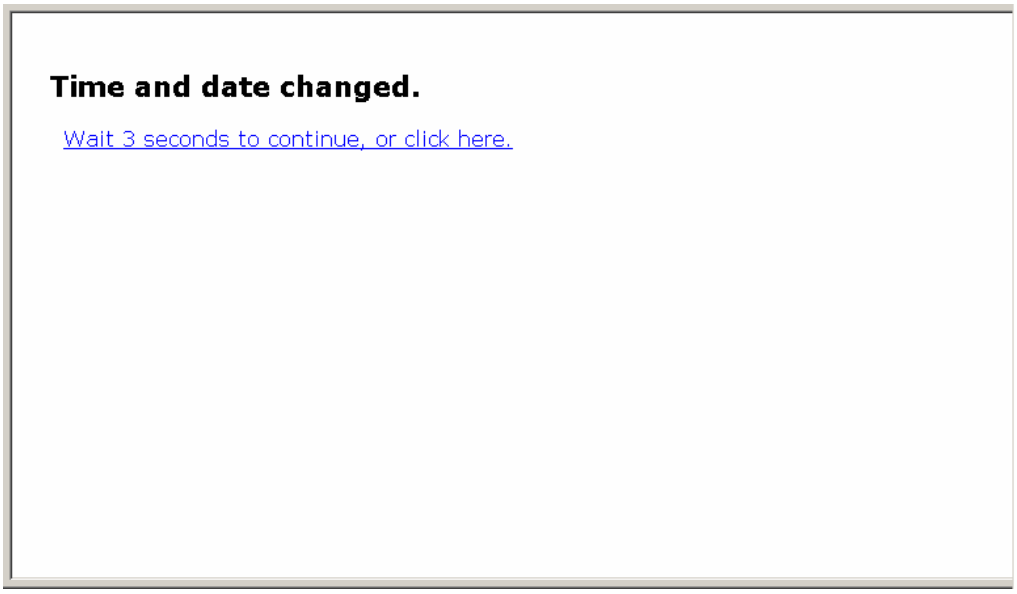




The following two kinds of date and time settings are available.

- Date and time specified in the local terminal PC (Local) that displays the web pages.
- UTC (Coordinated Universal Time, GMT or Zulu).

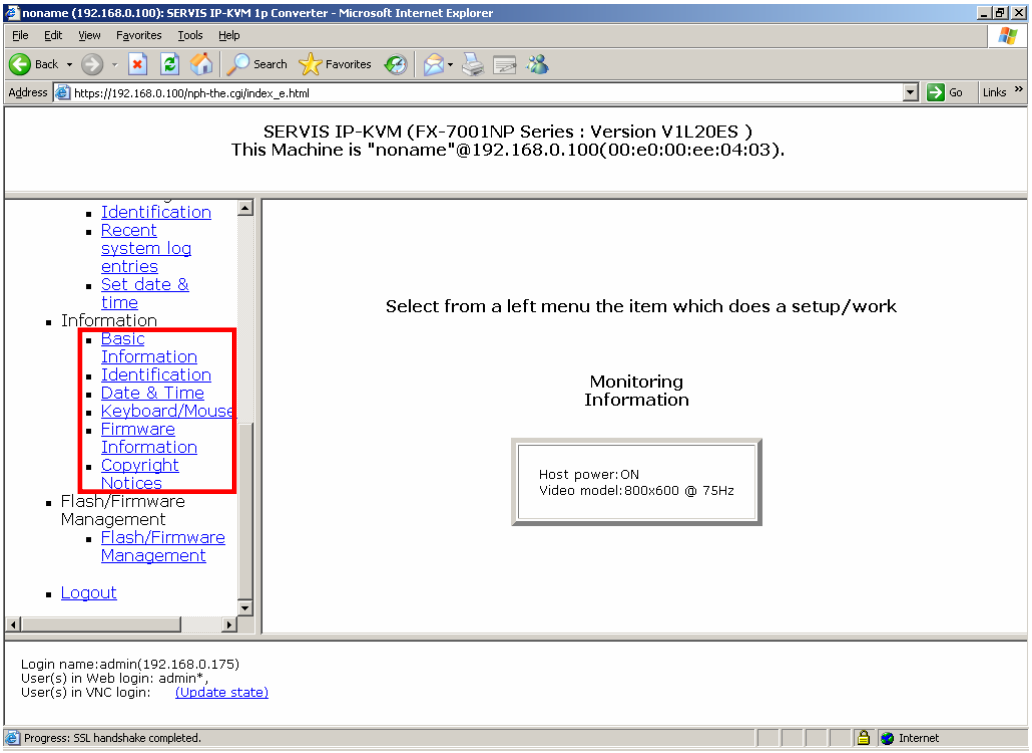
Click [Set to LOCAL time] or [Set to UTC time] button, the following message is displayed and the time is set.



3.5. Information

Displays the setting status of this product. General users can check this item.

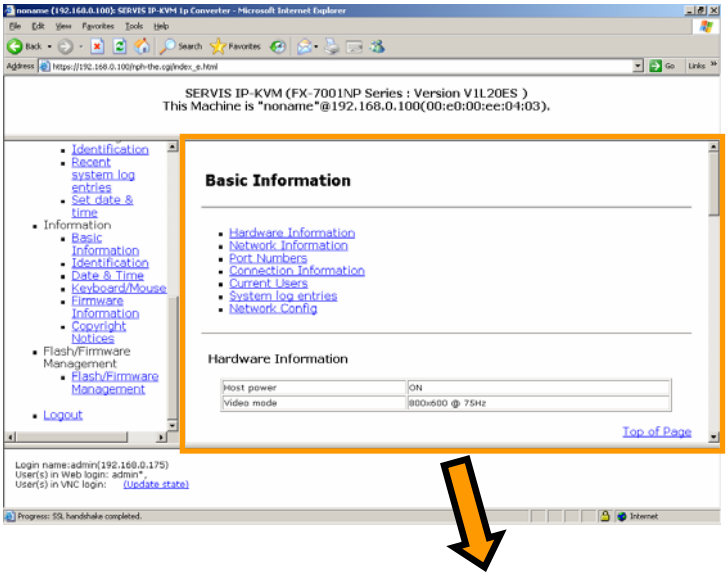
Click setting items from the menu-selecting area of the web page, the setting value is displayed in the right screen.

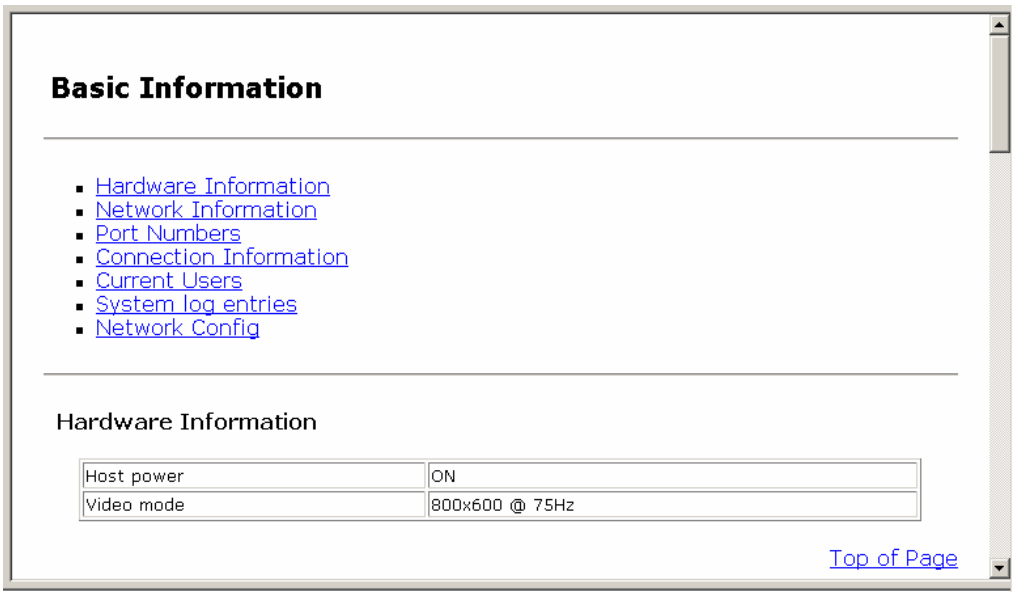


Refer to the following section for information.

3.5.1 Basic Information

Click Basic Information from the menu-selecting area, and the following contents are displayed.
You can check basic information here.

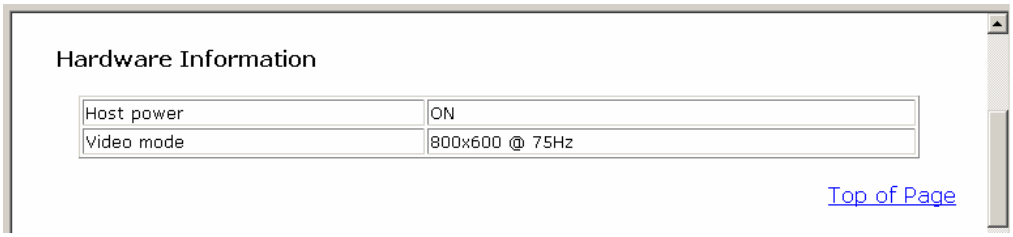




Items in "Basic information" are explained in the following section.

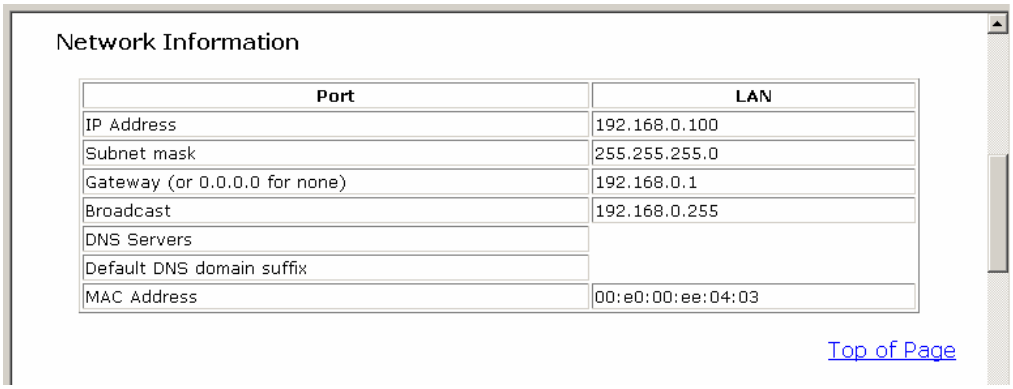
3.5.1.1 Hardware Information

The power on/off status and video mode of the host server is displayed.



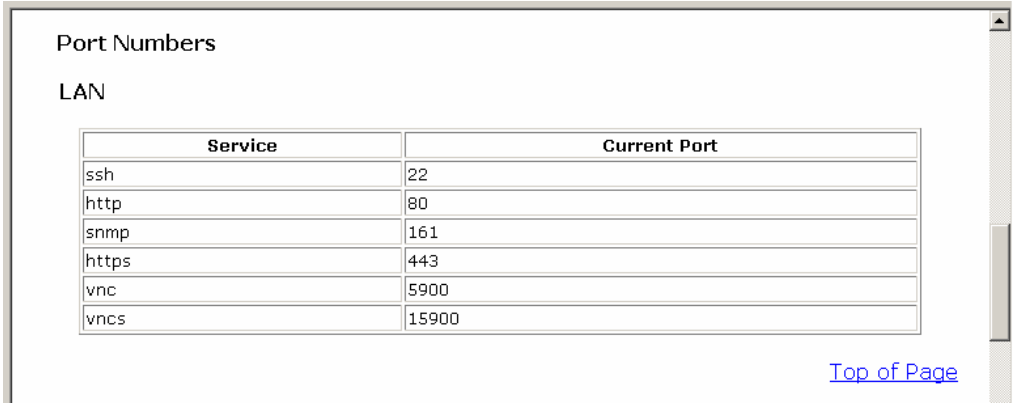
3.5.1.2 Network Information

The specified network information of this product is displayed.



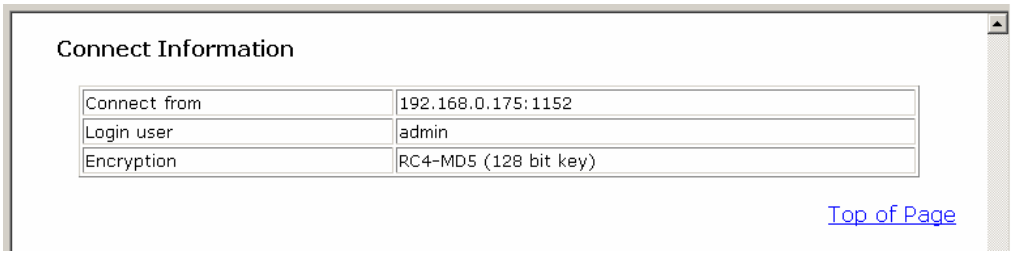
3.5.1.3 Port Numbers

The specified network port numbers of this product is displayed.



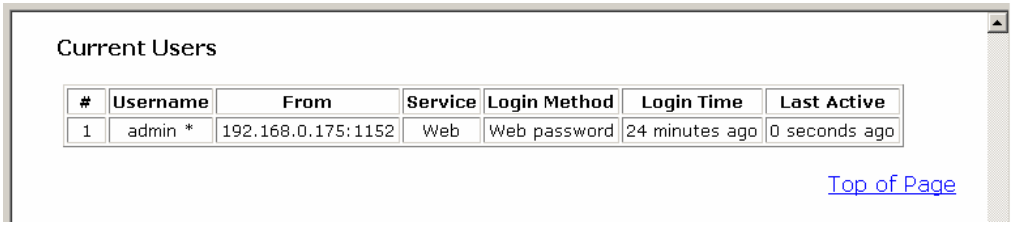
3.5.1.4 Connection Information

The user information currently connecting to this product is displayed.



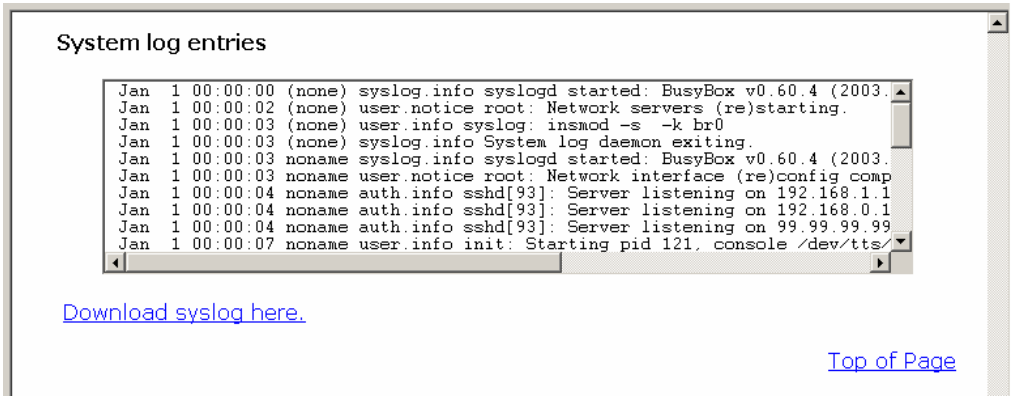
3.5.1.5 Current Users

The user account information currently logged on to this product is displayed.



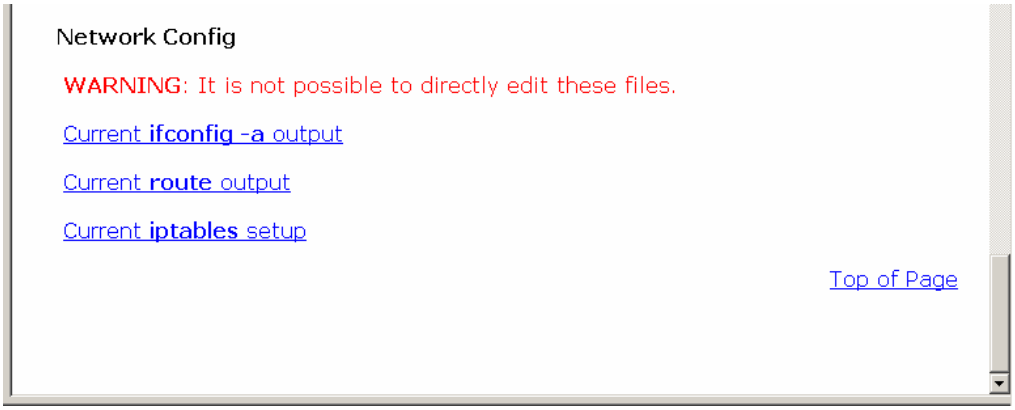
3.5.1.6 System log entries

System logs of this product are displayed.

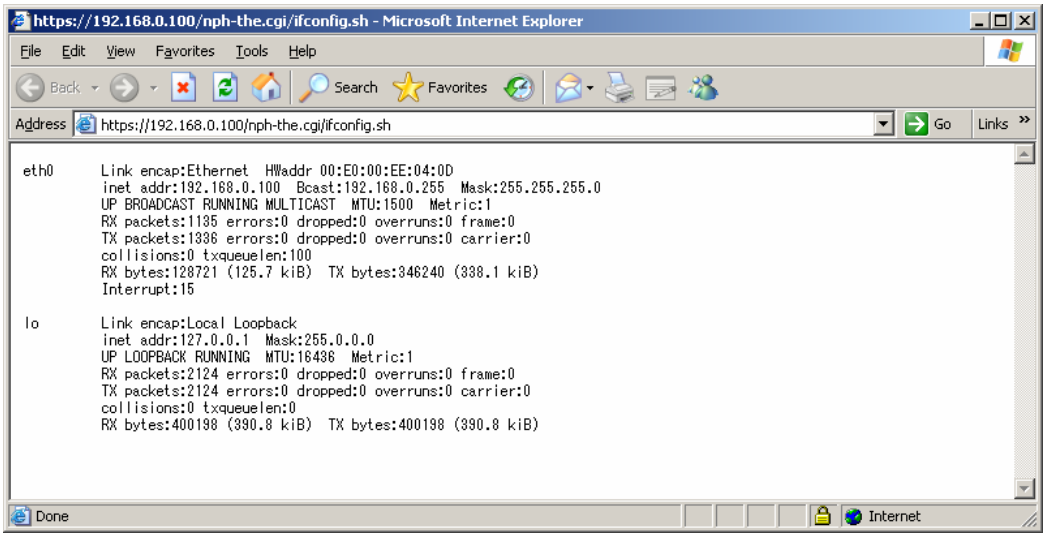


3.5.1.7 Network Config

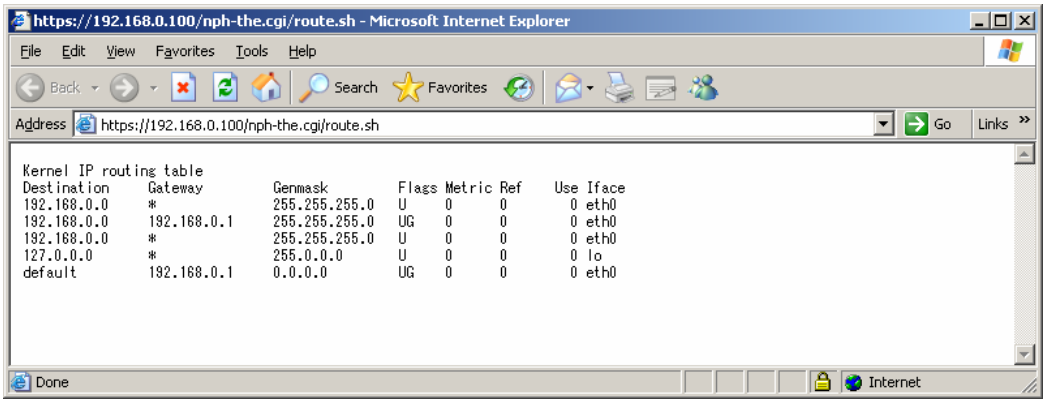
You can check the current device setting with the following items. It is possible to debug trouble spots in the network configuration with these settings. (Cannot edit the following logs directly.)



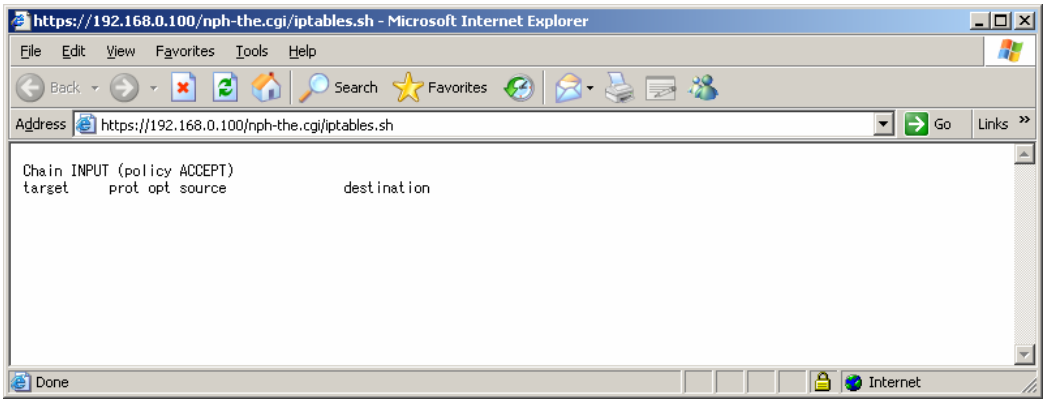
Click [Current ifconfig -a output], and the following screen is displayed.



Click [Current route output], and the following screen is displayed.

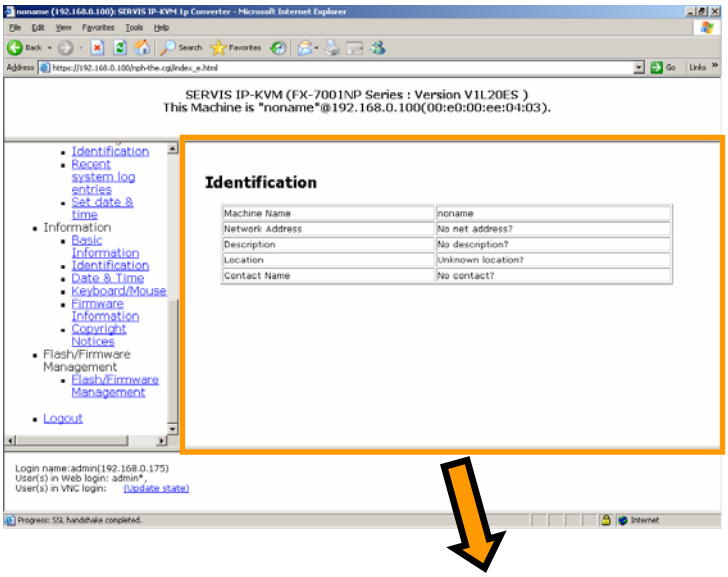


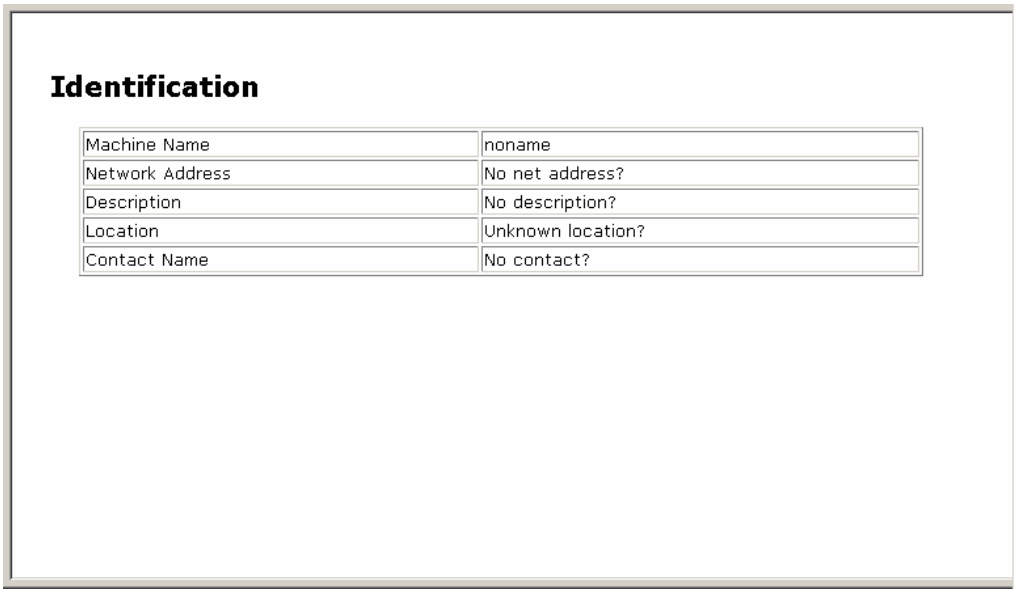
Click [Current iptables setup], and the following screen is displayed.



3.5.2 Identification (Information)

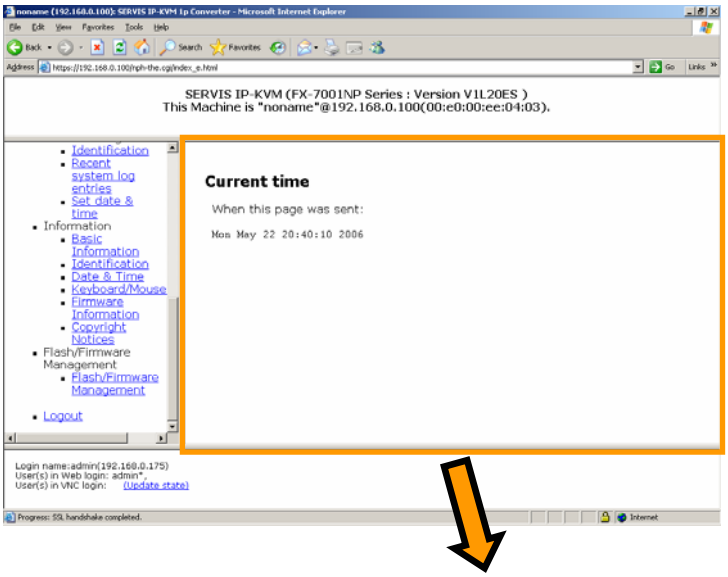
Click Identification from the menu-selecting area, and the following setting page is displayed.
Check the system ID of this product here.





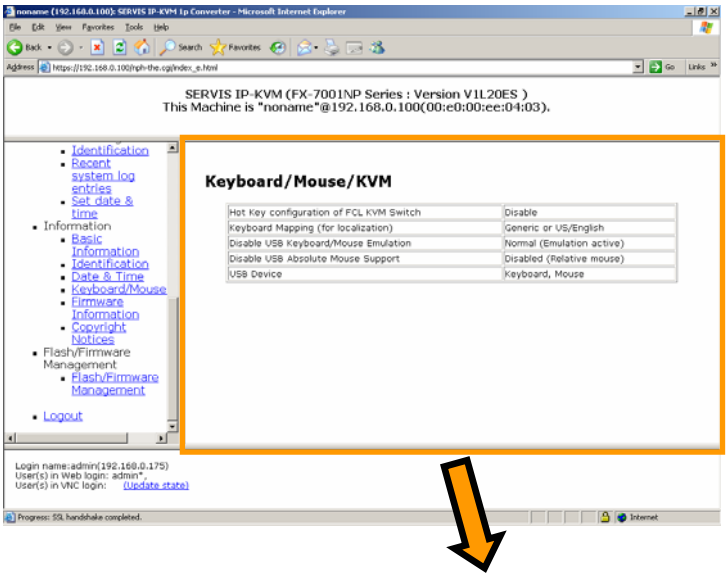
3.5.3 Date & Time

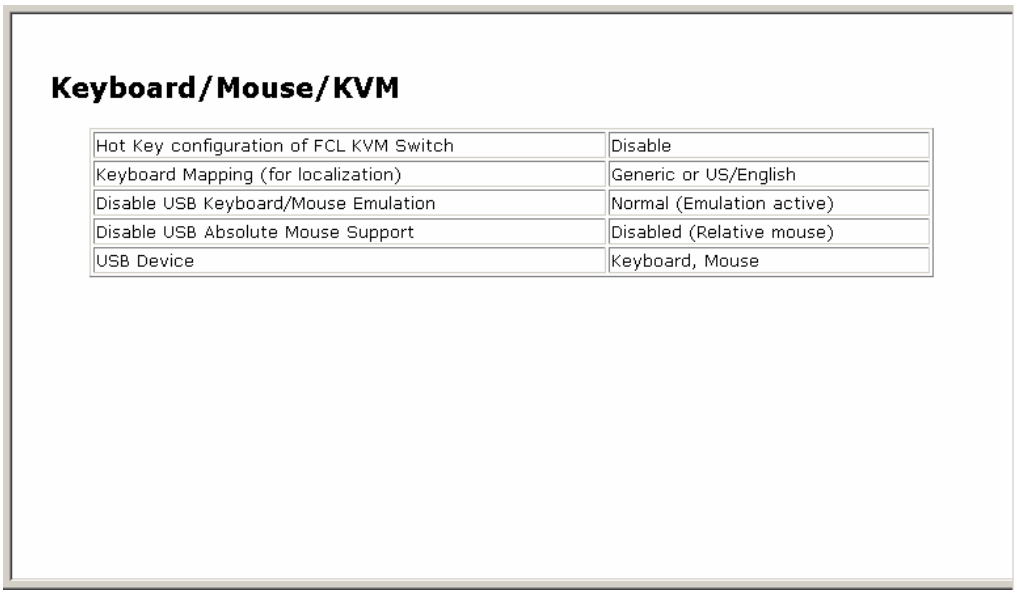
Click Date & Time from the menu-selecting area, and the following setting page is displayed.
Check date and time specified in this product here.



3.5.4 Keyboard/Mouse/KVM

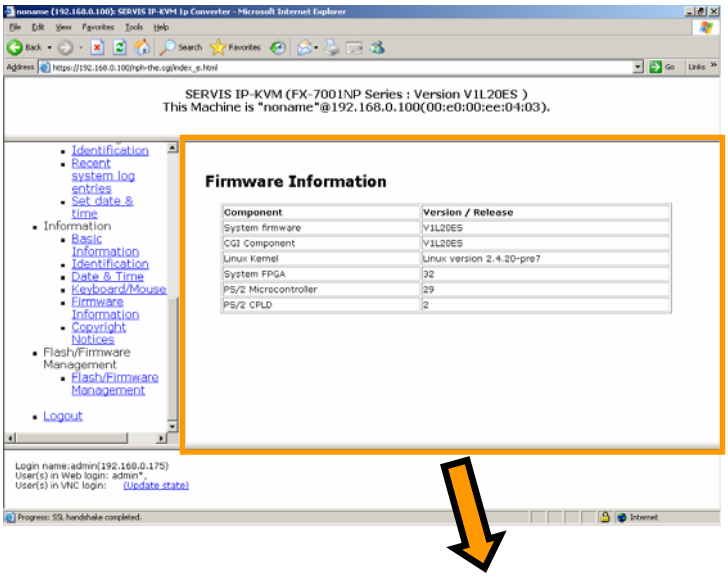
Click Keyboard/Mouse/KVM from the menu-selecting area, and the following setting page is displayed.
Check the input interface information of this product here.

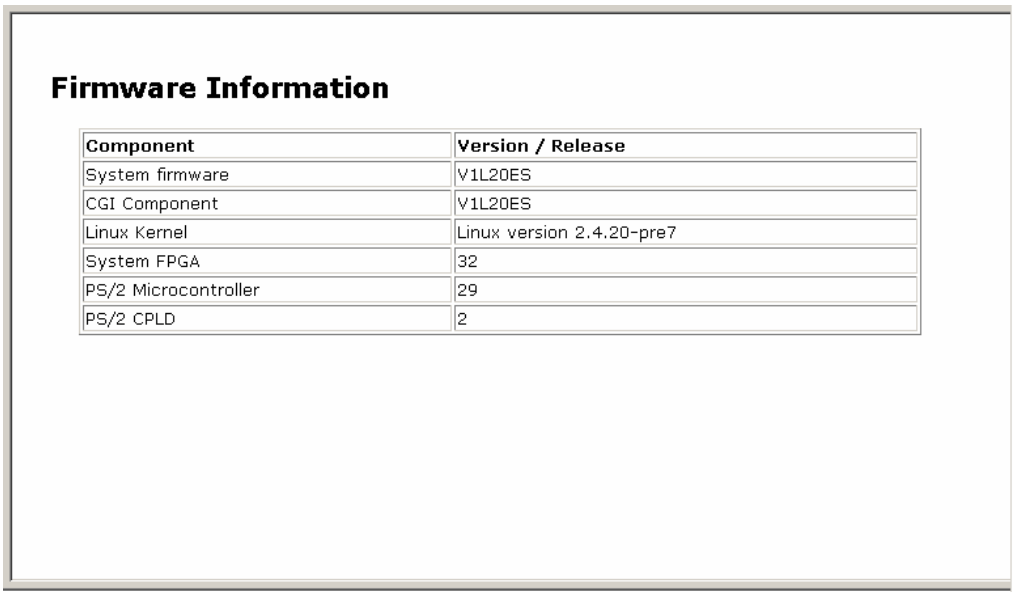




3.5.5 Firmware Information

Click Firmware Information from the menu-selecting area, and the following page is displayed.
Check the firmware information of this product here.



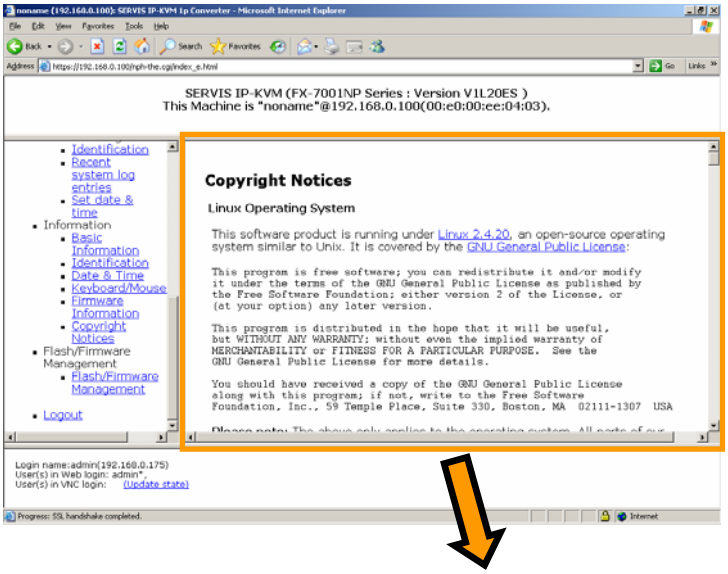


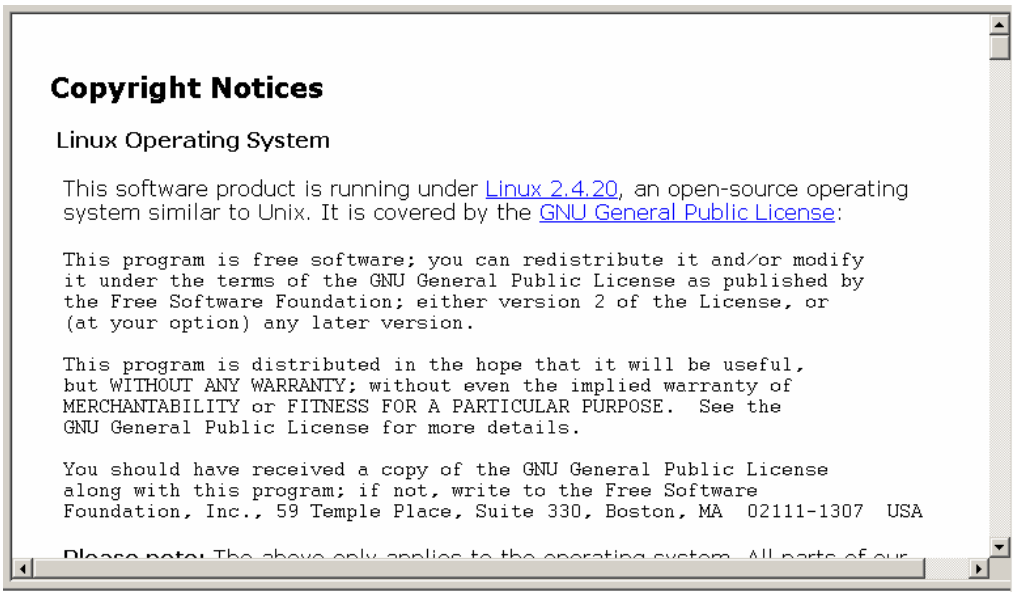
Firmware Information

Component	Version / Release
System firmware	V1L20ES
CGI Component	V1L20ES
Linux Kernel	Linux version 2.4.20-pre7
System FPGA	32
PS/2 Microcontroller	29
PS/2 CPLD	2

3.5.6 Copyright Notices

Click Copyright Notices from the menu-selecting area, and the following page is displayed.
Check Copyright information of this product here.

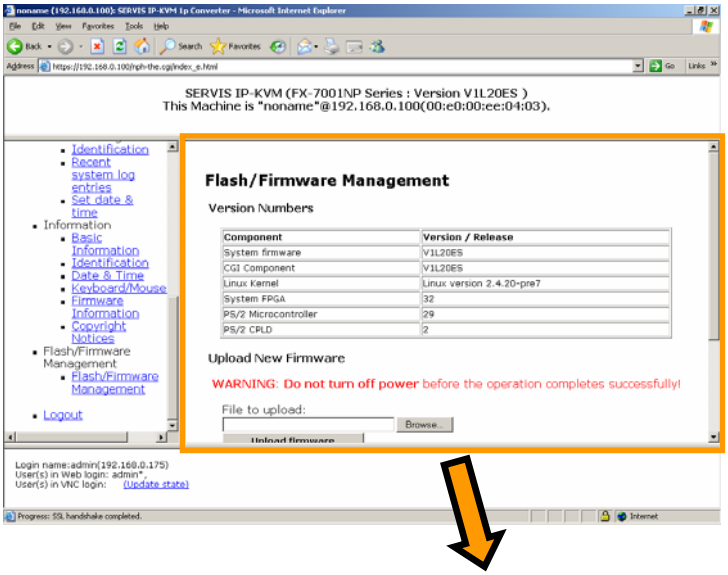


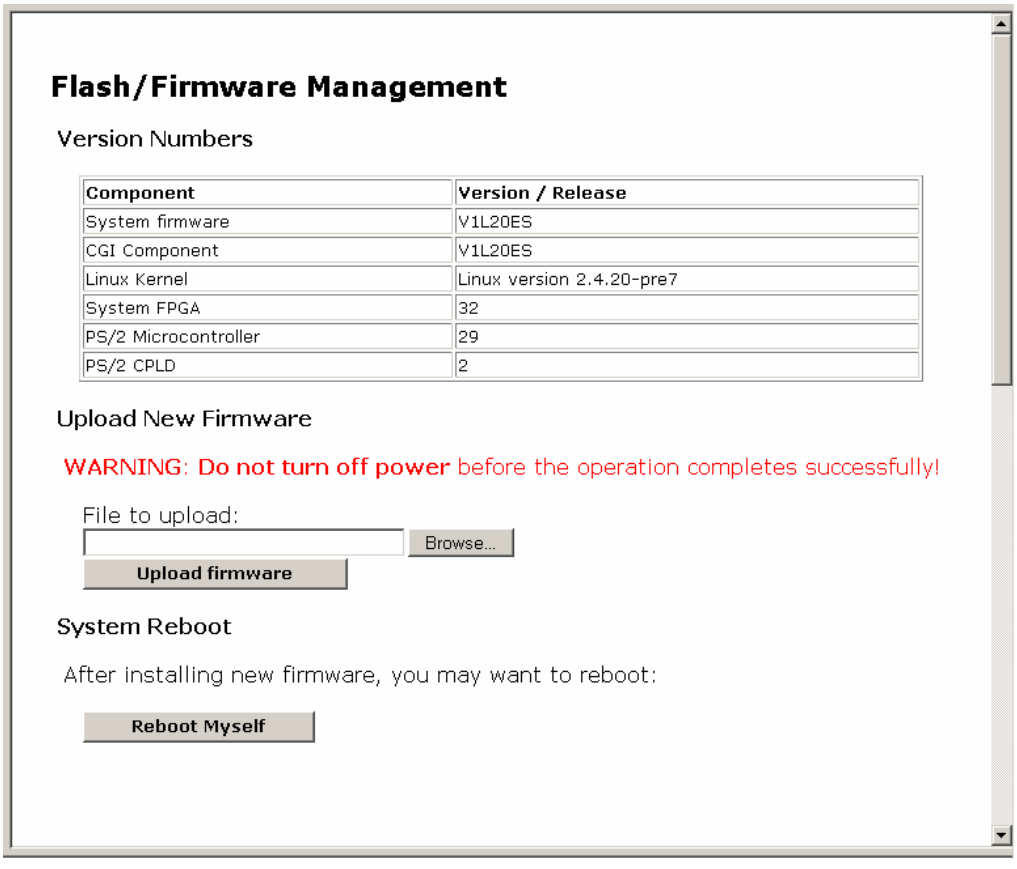


3.6. Flash/Firmware Management

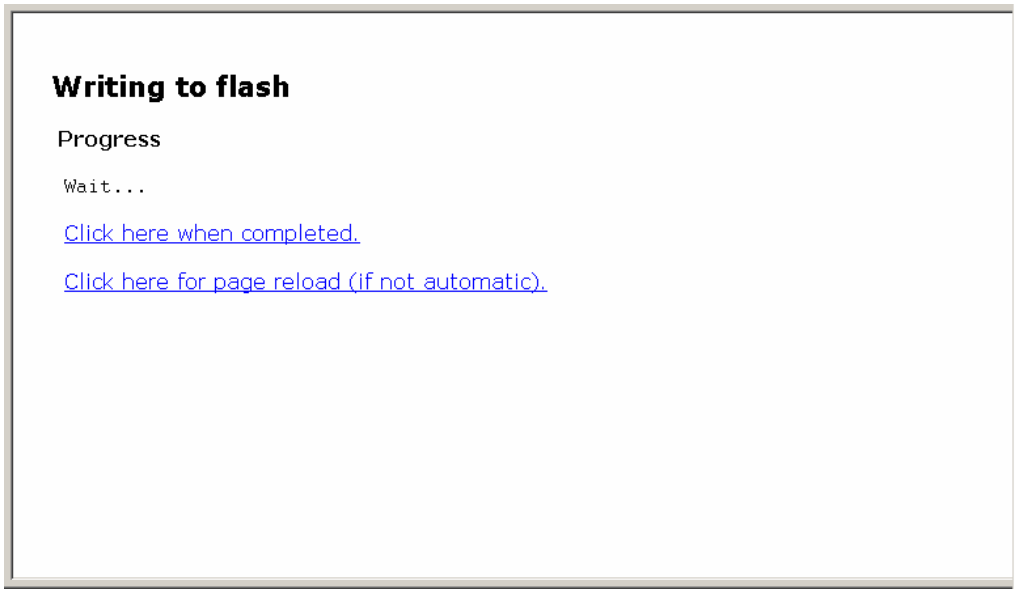
3.6.1 Flash/Firmware Management

Click Flash/Firmware Management from the menu selecting area, and the following setting page is displayed.
Confirm the current firmware version information and upload new firmware.

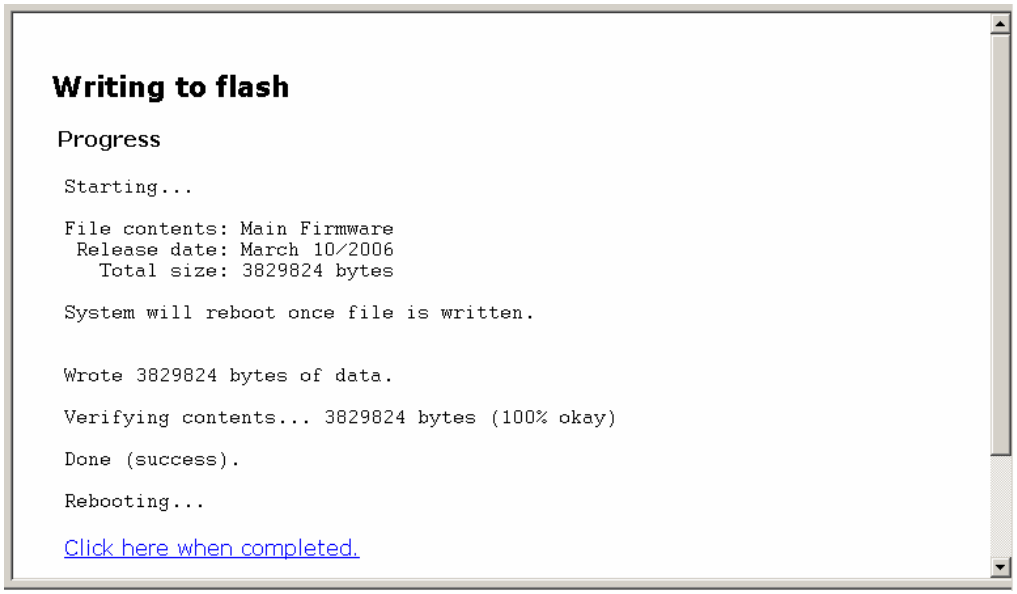




Click the [Browse…] button, select the file to be uploaded and click [Upload firmware]. The writing starts as follows.



When finished writing, the following screen is displayed.



Click [Click here when completed]. Return to the [Flash/Firmware Management] page and click the [Reboot Myself] button.

CAUTION

There is a risk of device failure if the process is cut off during writing to flash memories. Make sure not to power off the device until the firmware updating is successfully completed.

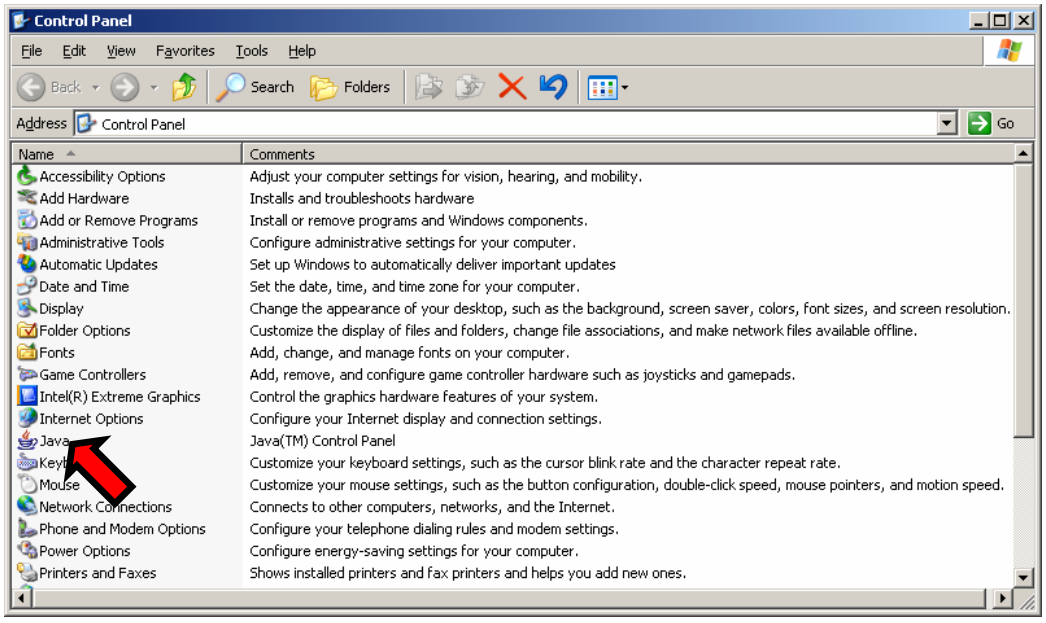
Wait at least 1 minute before stopping the uploading process (or evaluate whether the uploading process is not working) after clicking the [Upload firmware] button. It is necessary to reboot this product for upgrade. Log on again after rebooting and confirm that the system is upgraded with firmware version information.

For the upload file providing, we will offer consultation separately.

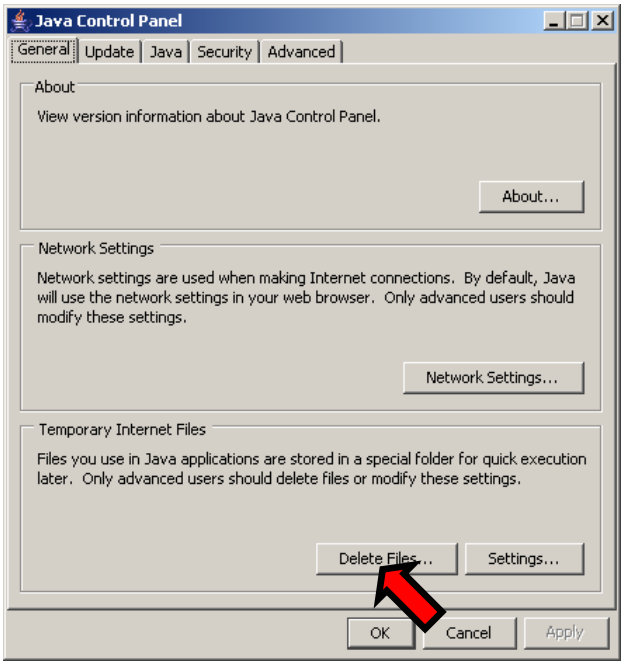
Cautions After the Uploading

It is necessary to clear the old Java Plug-in caches in client PC side after the firmware uploading. If not, the old Java Plug-in activated and firmware uploading is not reflected.
The following is the example of the cache clearing method for Windows 2000.

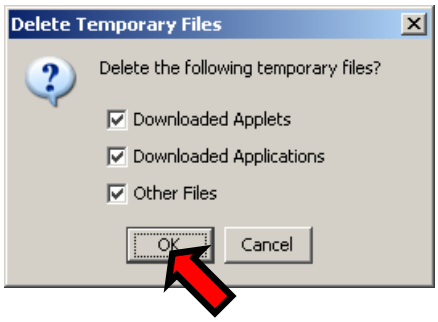
1. Click [Start] → [Setting] → and open Java in the [Control Panel] window.



2. The following [Java Control Panel] window is displayed. Click the [Delete Files…] button.



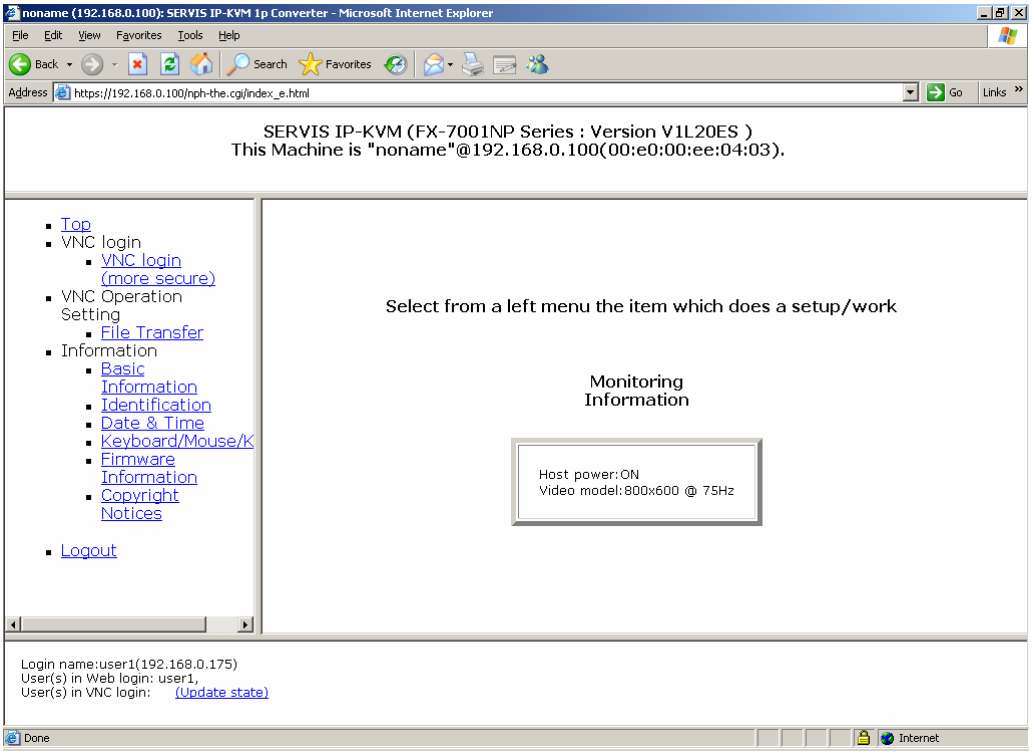
3. The confirmation dialogue is displayed. Click the [OK] button.



Then Java caches are cleared.
And the Java VNC connection is activated with the uploaded firmware.

3.7. Operation for General User

The following web page is displayed when logging on as a general user.
General users are not authorized to change settings and can confirm only the item displayed on below.
However, general users can use it about the virtual disk function.



Each item displayed in the menu selecting area is the same as the administrators.

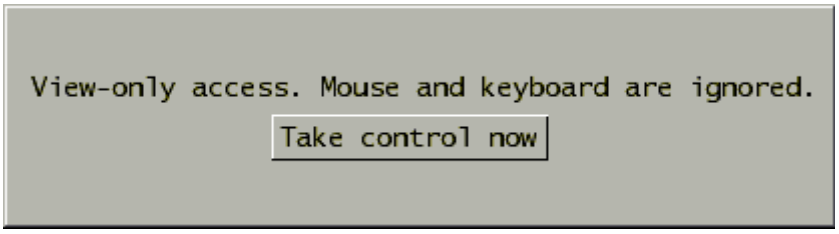
3.8. Concurrent Connection of Network Users

Up to 5 users are able to log on to this product and perform VNC connection to the server concurrently.
The first user connected to VNC obtains operation authority.

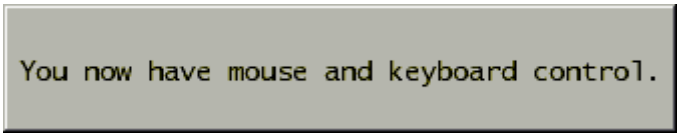
Behavior of unauthorized network users depends on [Access Sharing Policy] setting.
📖 Refer to 3.3.1.3 Access Sharing Policy (page 79)

If you connected to the VNC but don't have operating authority, all buttons besides [Video-Reset] and [Menu] button are displayed in gray. (Monitoring mode)

Even if you move the mouse on to the host server in monitoring mode, the cursor does not move. The mouse clicked or some key entered in this mode, the following window displayed.

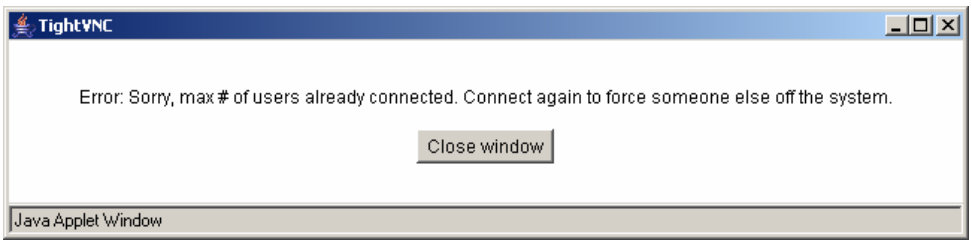


Click the [Take control now] button, the following window is displayed and you can obtain the operating authorities. It enables you to operate the host server using the keyboard and mouse.



All buttons in the VNC menu bar are displayed.

Up to 5 users are able to connect to VNC via the network. If there are already 5 users connecting to VNC, the following dialogue box is displayed and connection is impossible.



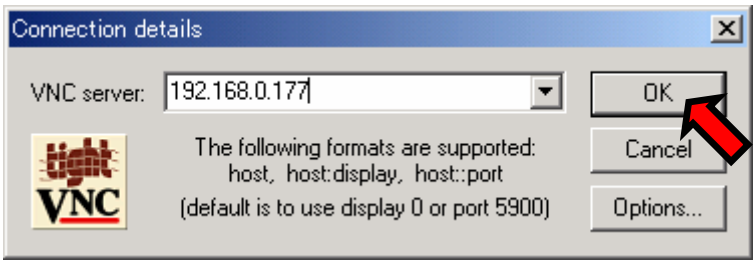
3.9. Operation by VNC Software

The system of this product supports the following VNC software.
The Access method using TightVNC is shown below.

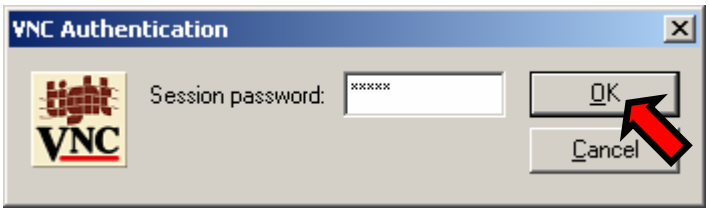
Procedure

1. Install TightVNC to the terminal PC in the network and execute the vncviewer.exe.
   Download TightVNC: http://www.tightvnc.com/download.html

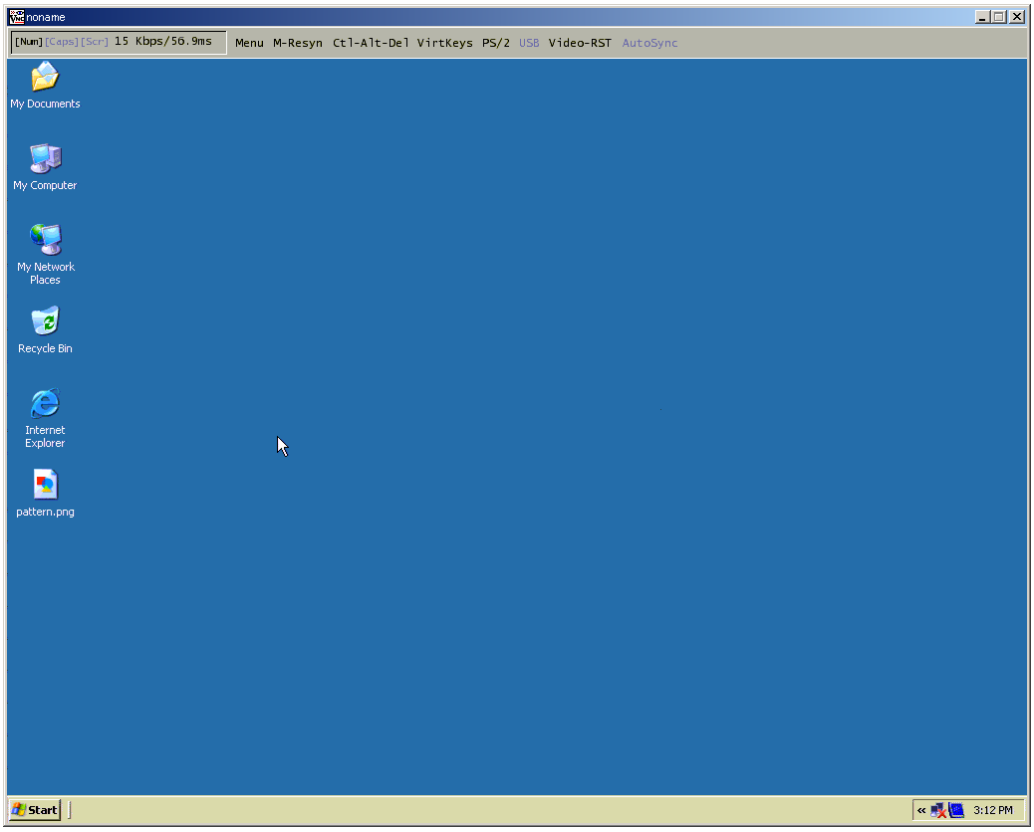
2. Enter the IP address of this product and click the [OK] button.



3. Enter administrator password (default: admin) and click the [OK] button.



4. The following Viewer is started.



Operating method for the menu bar is the same as Java VNC.
📖 Refer to 2.5.2 VNC Menu (page 32)

Chapter 4 - Specifications

This chapter provides the specifications, operating conditions and detailed information about this product.

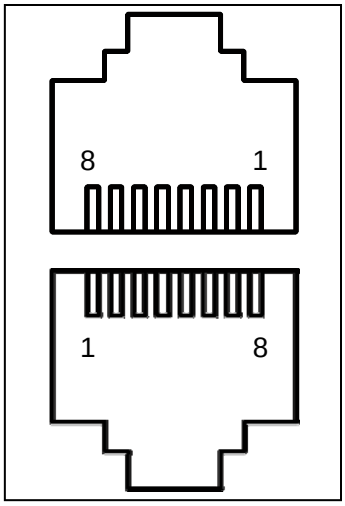
Contents

4.1. Product Specifications

Items		
Product Name		SERVIS IP-KVM 1p Converter
Model Number		FX-7001NP
Number of Managing Server		1
Number of Concurrent Connections		Network Connection: 5 users (Only 1 user is allowed to operate). Local: 1 user (Local user controls exclusively)
CPU	Type	32bit CPU
	Clock	200MHz
Memory	Main	32MB
Ethernet	Type	10BASE-T, 100BASE-TX
	Supported Protocol	IP, ICMP, TCP, UDP, FTP, DHCP, VNC, VNCS (ssh tunneled VNC), HTTP, HTTPS, SYSLOG, DNS, SSL, SSH
	Security	SSL (RC4, MD5), SSH, Firewall
Console	Type	Signal Standard: RS-232C
	Supported Speed	115.2kbps
Connector	Ethernet	RJ45 x 1
	Console	RJ45 x 1
	Local	D-sub15 x 1 mini-DIN6 x. 2
	Server	D-sub15 x 1 mini-DIN8 x 1 USB × 1
	Power	DC5V Power Adapter x 2 (Redundant power supply supported).
Supported Video Resolution (Server)		640 x 480 (60Hz, 72Hz, 75Hz, 85Hz) 800 x 600 (60Hz, 72Hz, 75Hz, 85Hz) 1024 x 768 (60Hz, 70Hz, 75Hz, 85Hz) 1152 x 864 (75Hz) 1280 x 960 (60Hz, 85Hz) 1280 x1024 (60Hz, 75Hz, 85Hz) 1600 x 1200 (60Hz, 75Hz, 85Hz)
Virtual Storage (USB disk)		1.44M floppy disk 8MB RAM disk CD-ROM (iso files)
Rack Mount		Supports 1U kit (parallel configurations of 2 devices are available).
Configuration		Metal case, black coating
Power Supply	Input Rating	DC5V
	Power Consumption	DC5V, 2A
Dimensions	W x D x H [mm]	193 x 124 x 40
Weight	[g]	785 (The main device only)

4.2. RJ45 Connector Signal Assign

Console Port



Ethernet Port

Terminal Number	Console	Ethernet
1	RTS	TX+
2	NC	TX-
3	TxD	RX+
4	GND	NC
5	GND	NC
6	RxD	RX-
7	NC	NC
8	CTS	NC

4.3. Operational Environment

Items	
Ambient Temperature	While operating: 0 to 40°C While being stored: -20 to 60°C
Ambient Humidity	While operating: 10 to 80% RH (no condensation) While being stored: 5 to 90% RH (no condensation) Temperature conditions: For 40°C or under, maximum 90% RH : For 40 to 60°C, inversely proportional until 50% RH
Vibration Resistance	JIS C 0040 (10 to 55 to 10Hz/min, 1.5mm)
Shock Resistance	JIS C 0041 (10G to 11ms)
Conformance	FCC class B, VCCI, cTUVus, CE
Electrostatic Resistance	Testing Standard : IEC61000-4-2 Body : Contact - At least ±6 kV : Air - At least ±8 kV RJ45 signal line : Contact - At least ±2 kV : Air - At least ±2 kV

4.4. Optional Accessories

Name	Model Number	Note
Composite cable for server connection (2m)	NC70005-2001RS	
USB cable (2m)	NC70002-2001RS	
RJ45–D-Sub 9-pin Cross Conversion Adapter	FP-AD009RJX	One adapter is attached.
RJ45–D-Sub 25-pin Cross Conversion Adapter	FP-AD025RJX	One adapter is attached.
AC Cable for USA	NC14004-B077	
AC Cable for EUROPE	NC14004-B078	
AC Cable for UK	NC14004-B079	

MEMO

Chapter 5 - Troubleshooting

This chapter provides problem-solving method that may occur when using this product.

Contents

5.1. Troubleshooting

This section provides examples of possible problems and methods for solving while using this product.

5.1.1 LED Confirmation

- **Did you check LEDs at front/rear of this product?**

  Check LEDs at front/rear of this product if trouble occurs. By using LEDs, it is possible to monitor power supplies and network problems.
  📖 Refer to 1.3.1 Rear (page 4)
  📖 Refer to 1.3.2 Front (page 6)

Section	LED	Status	Problem Solving
1	Power LED	**Off**	Power adapter might be disconnected. Connect the power adapter.
2	Ethernet Link LED	**Off**	Ethernet port link is not established. Check the connection with network devices such as router and hubs etc.
3	Ethernet Act LED	**Off**	This LED blinks when network access to this product is occurred. If access failure occurs, the LED turns off.

5.1.2 Cannot Power On the Device

- **Is the power adapter connected?**

  Make sure to use the provided power adapter.

- **Is power being supplied to the outlet?**

5.1.3 Cannot Access the Serial Console

- **Is the serial connection setting correct?**

  Make sure to set emulator application (Tera Term, etc.) connection as follows.

Conditions for Communication	Value
Baud Rate	115200bps
Data Length	8bit
Parity	none
Stop Bit	1bit

- **Are you using the correct conversion adapters and cables?**

  Check the conversion adapters (D-sub–RJ45, etc.) and cables being used support serial console COM port. Optional conversion adapters are available.
  🕮 Refer to 1.5.4 Serial Console Connection (page 12)

5.1.4 Cannot Operate the Device Locally

- **Are the video monitor, keyboard and mouse correctly connected?**

  Make sure that they are connected to the local port.
  🕮 Refer to 1.5.2 Connection to the Host Server (page 10)

5.1.5 Cannot Access the Web page

- **Is the UTP cable shorter than specified limits?**

  The 10BASE-T and 100BASE-TX cable length must be shorter than 100m. Make sure they are no longer than that.

- **Is the cable correctly connected?**

  Make sure that the Cat5 cable is connected to the Ethernet port.
  🕮 Refer to 1.5.2 Connection to the Host Server (page 10)

  If the network link is established, the LED in front of the device is on.

- **Is the network device power on?**

- **Is the IP address specified?**

  Check the specified IP address using the serial console.
  If not, specify the IP address using serial console.
  📖 Refer to 2.2 Set the IP Address (For Initial Installation) (page 15)

5.1.6 Cannot Login to the Setting Page

- **Is Cookie enabled?**

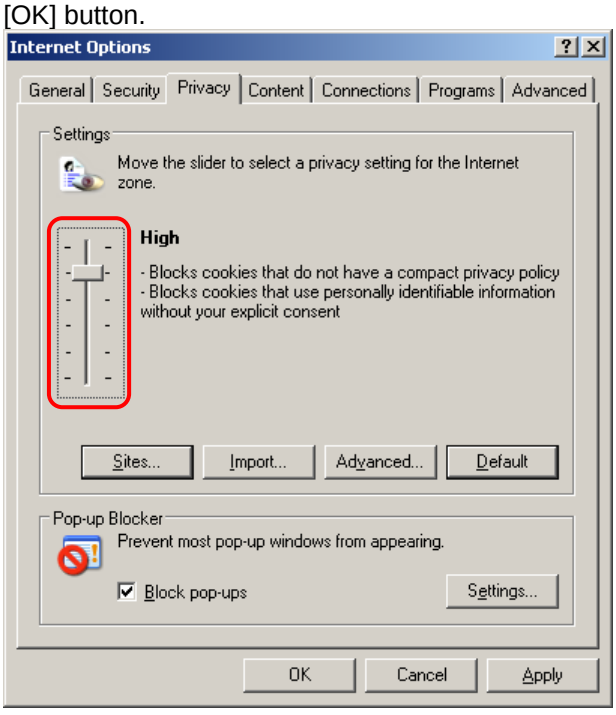
  If you disabled cookie in the browser such as Internet Explorer, Mozilla, Firefox, Opera, and Netscape, you cannot login to the setting page.

  Cookie setting method is described below.

For Internet Explorer 6.0

Click [Tools] menu → [Internet Options] and the following dialogue box is displayed.Click [Privacy] tab and move the slider to setup of cookie in the dialogue box.

Move the slider except for the setting of "Block All Cookies" and click [OK] button.



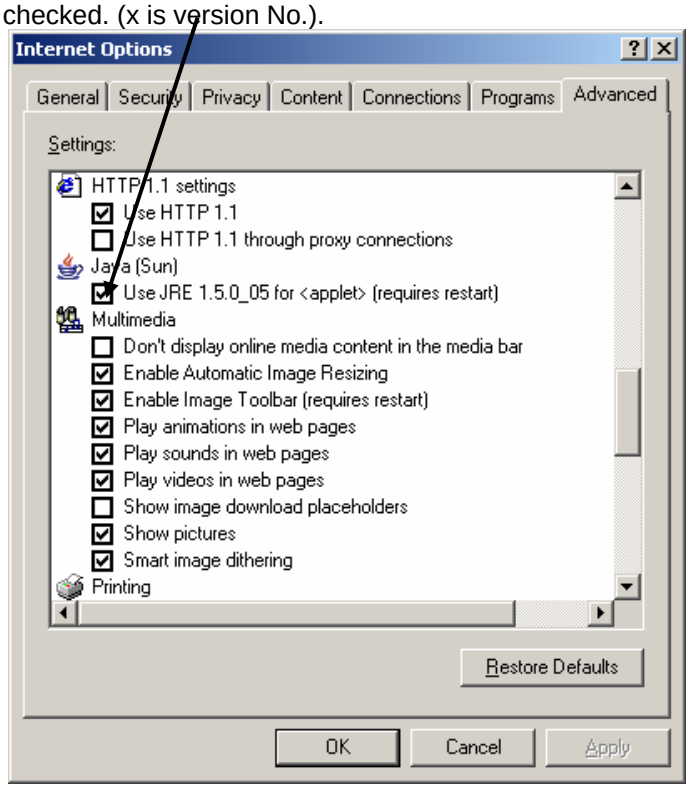
5.1.7 VNC Connection is not Performed

- **Is the Java applet installed?**

  If the VNC connection is not performed from the web page, make sure that the Sun Java applet is installed in the remote terminal unit.

For Internet Explorer 6.0

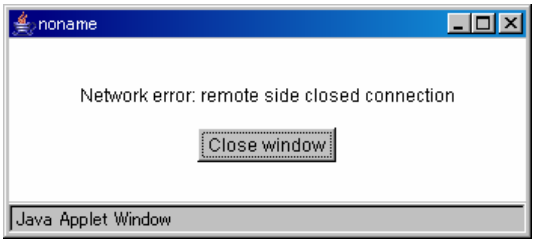
Click [Tools] menu → [Internet Options] → [Advanced] tab to confirm that Java Sun [Use JRE 1.x.x_xx for <applet> (requires restart)] is checked. (x is version No.).



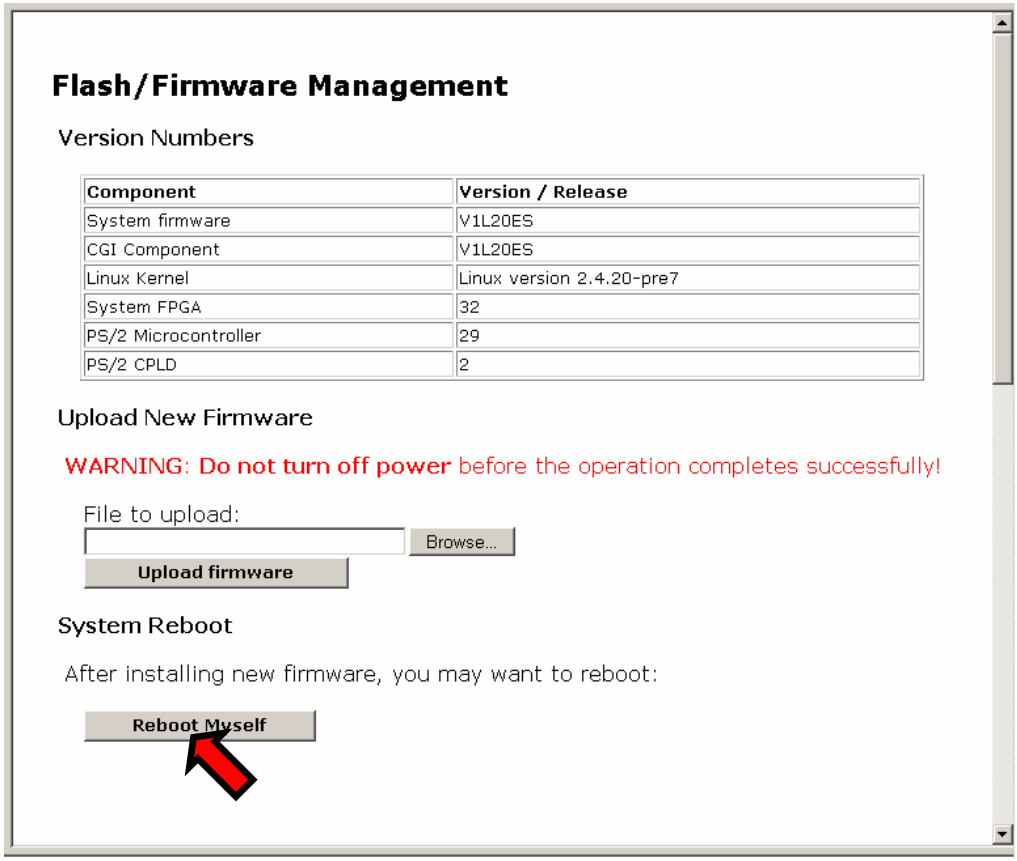
If not installed, download the Java applet from the following web site and install it.
http://www.java.com/ (Download page for the Sun Microsystems and Java software).

- **Network Error is Displayed**

If the following error is displayed and the VNC window closes every time the VNC connection is performed, reset (disconnect and reconnect the power adapter) this product.



If you connected via the network, click the [Reboot Myself] button in the firmware management page.

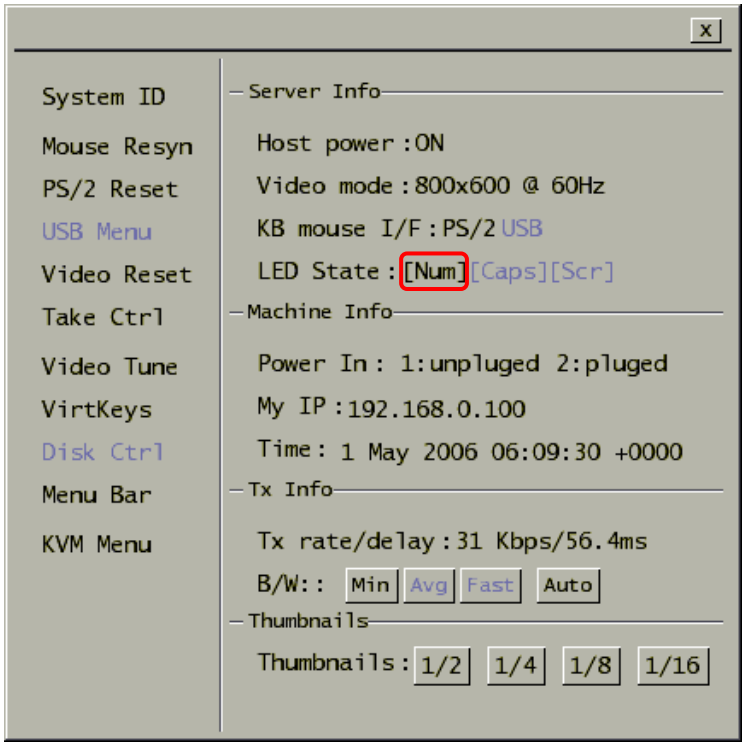


After rebooting, log on to the device from the web page again and perform the VNC connection.

5.1.8 The Numeric Keypad Does Not Work Properly

- **Are the NumLock LEDs in the remote terminal and VNC screen in the same status?**

  If the NumLock LED status in the VNC menu window is not same as that in the remote terminal unit, the Numeric Keypad does not work properly.



  Click NumLock once out of the VNC screen to conform the setting.

5.1.9 The Mouse Does Not Work

- **Perform [PS/2 Reset] or [USB Replug].**

  If the USB keyboard/mouse is disabled (connecting PS/2 status), click the [PS/2 Reset] button in the VNC menu window to reset PS/2 emulation.
  📖 Refer to 2.5.3 Menu Window (page 34)

  If the USB keyboard/mouse is enabled, click the [USB Menu] button in the VNC menu window and display the USB Menu window. Click the [do] button in the USB Replug and disconnect and reconnect the USB connection.
  📖 Refer to 2.5.9 USB Setting Window (page 47)

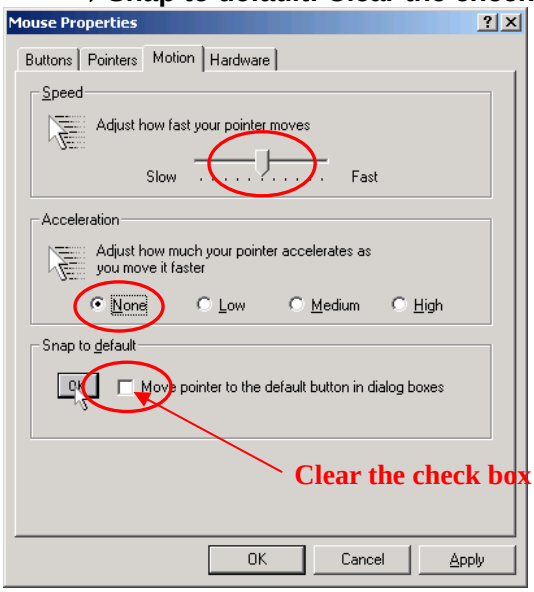
5.1.10 Mouse Cursor is Not Move Coinstantaneously

- **Are the [Acceleration] settings and the [Move to Default Button] settings for the host server mouse disabled?**

  To align the remote terminal and host server cursors, disable [Acceleration] and the [Move to Default Button] settings.

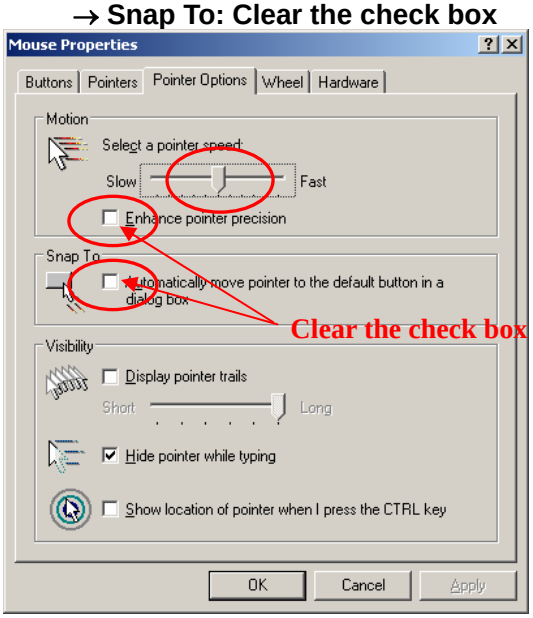
➢ For Windows OS based host servers
Click [Control Panel] - [Mouse] and display the mouse properties.
For Windows 2000

→ **Speed: Middle, Aceleration: None**
→ **Snap to default: Clear the check box**



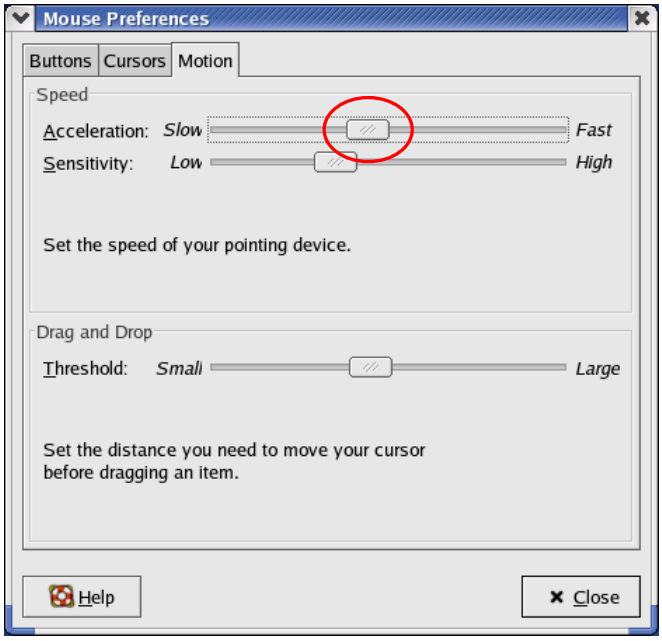
For Windows XP and Windows Server 2003

→ **Motion: Middle,**
Enhance Pointer precision: Clear the check box
→ **Snap To: Clear the check box**



➢ For RedHat Linux (GNOME) Based Host Server.
Click [Preferences] - [Mouse] and display the mouse preferences.

→ Aceleration: Middle (For slowish side)



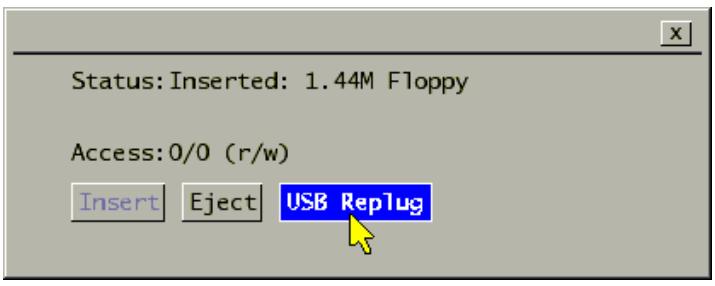
- **If the PS/2 keyboard/mouse is enabled.**

  When the PS/2 keyboard/mouse is enabled and the host server is Windows OS based, before log in the mouse cursor will not align.

5.1.11 Fail to Recognize the Virtual Disks

- **Perform USB Replug**

  If the access error occurred in VNC screen click [Menu] and [Disk Ctrl] button in the VNC menu bar to display disk operating window, click [USB Replug] button. After that operation, click the [Insert] button and check whether the host server recognizes the virtual disk.



5.1.12 Host Server Mouse Moves Slow

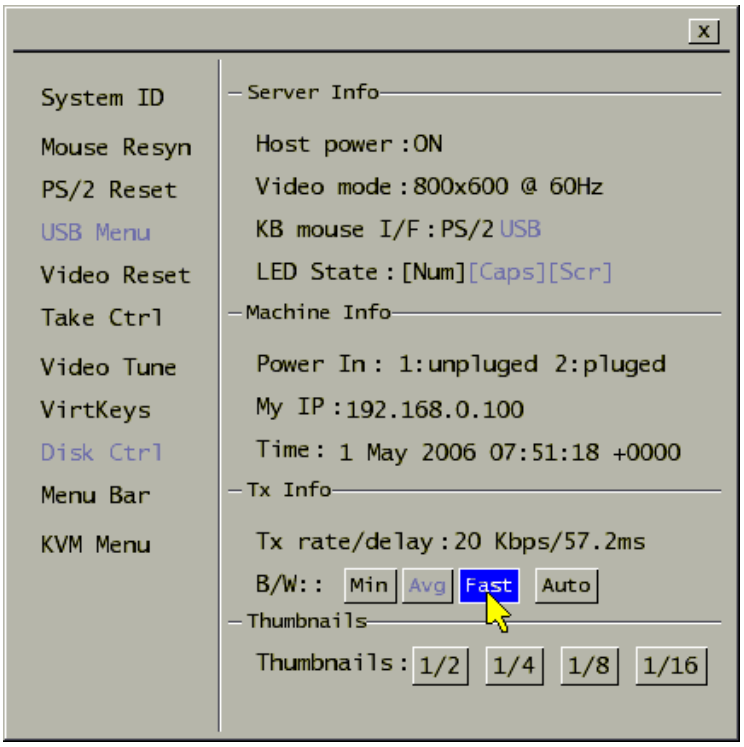
- **Adjust the transmission capacity in the band width setting**

  Click [Menu] button in the VNC menu bar to display the menu window. Click the B/W: button and perform the band width setting.

  Each setting button corresponds to the following value.

  [Min]: Specify the capacity of transmission to below 700kbps.
  [Avg]: Specify the capacity of transmission to below 4Mbps.
  [Fast]: Specify the capacity of transmission to below 12Mbps.
  [Auto]: This product sets the value automatically.

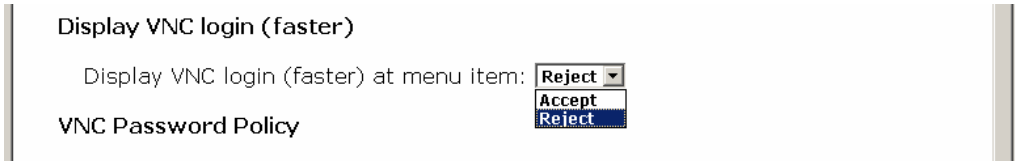
  If you feel the host server display speed is slow from mouse pointer movements, specify the value as [Avg] or [Fast].



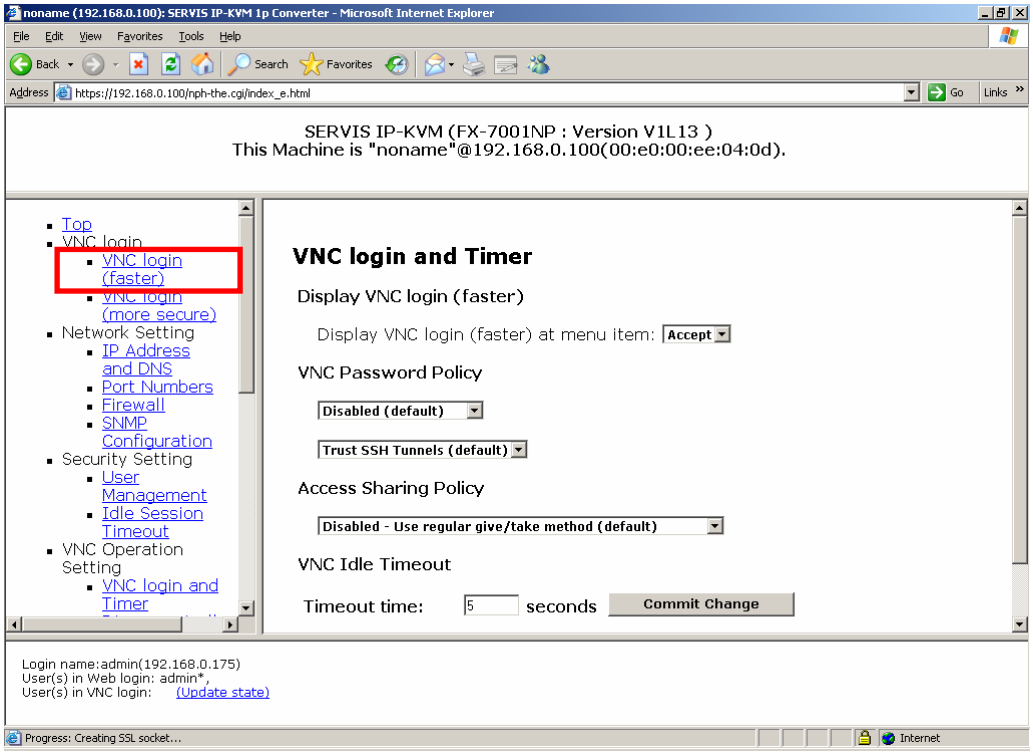
- **Perform VNC login (faster)**

  Unencrypted VNC connection improves the processing speed.

  Click [VNC login and Timer] → [Display VNC login (faster)] and “Accept “in [Display VNC login (faster) at menu item].



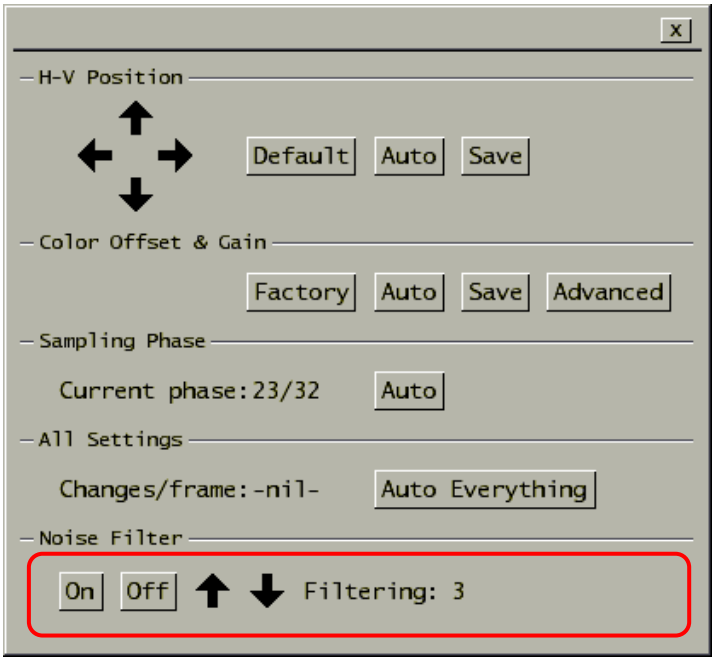
The item "VNC login (faster)" is displayed after selecting "Accept" as below.



Click “VNC login (faster)” to connect VNC without encryption.
Keep in mind are inferior in respect of security.

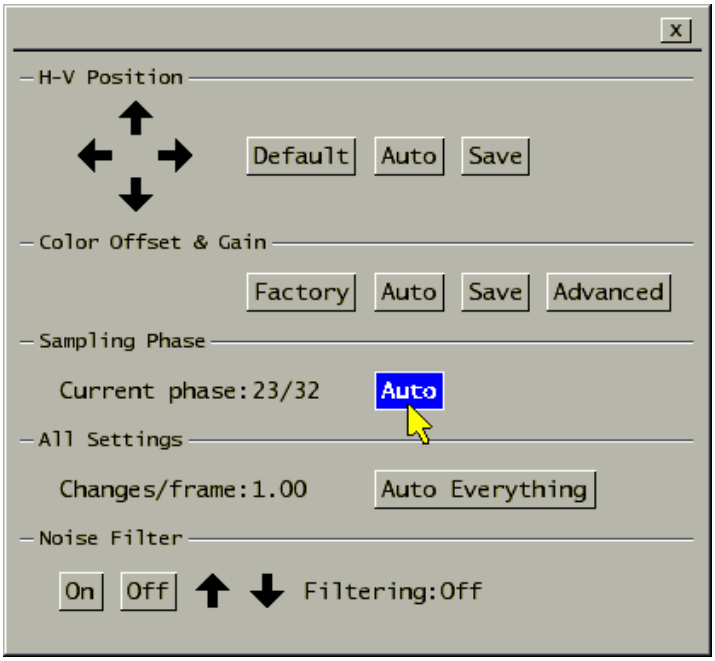
- **Specify the noise filter setting.**

  Image data transmitted from host server includes noise. It increases the volume of transmit data and operation may be delayed.
  Click the [On] button of the Noise Filter setting in the Video Tune window.
  Specify the value between 1 and 31 for transmission rates.
  ↑: Increase the filtering value, ↓: Decrease the filtering value

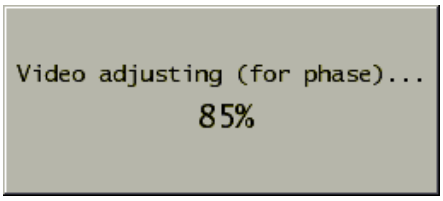


- **Perform auto-setting for the Sampling Phase**

  Auto setting of the Sampling Phase improves the processing speed.



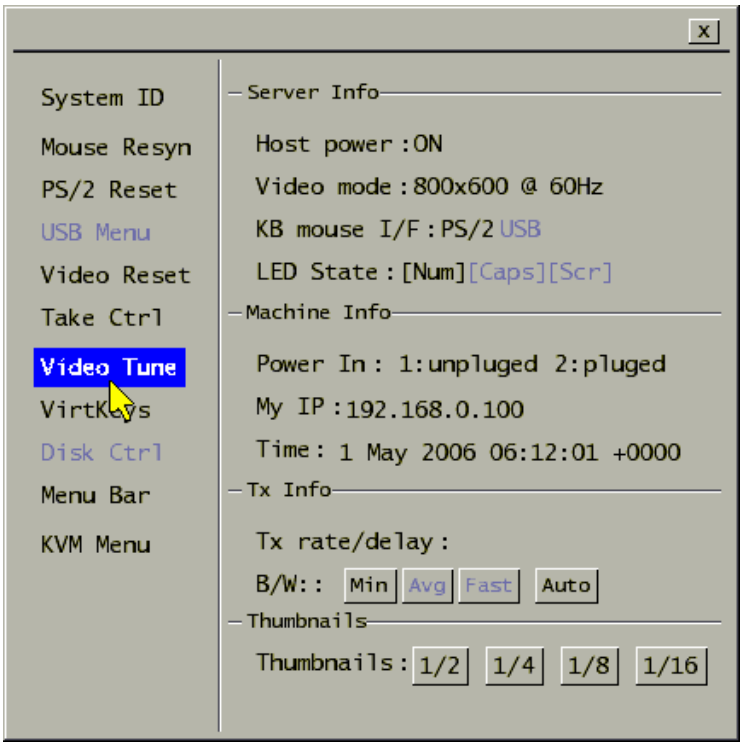
  The following dialogue box is displayed and auto-setting is performed.



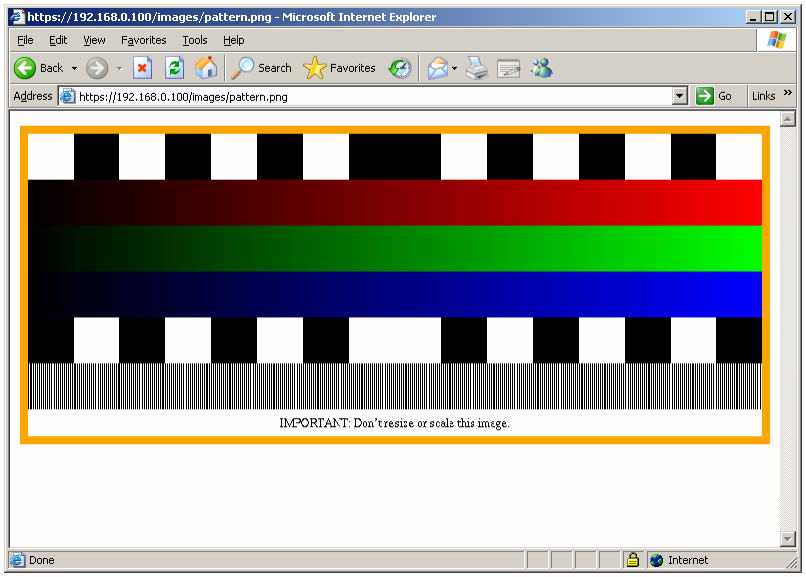
5.1.13 Increase Image Quality

- **Perform auto-setting of Video Tune.**

Optimize the image quality to improve processing speed.
Click the [Menu] button in the VNC menu bar to display menu window. Click the [Video Tune] button and the Video Tune window is displayed.

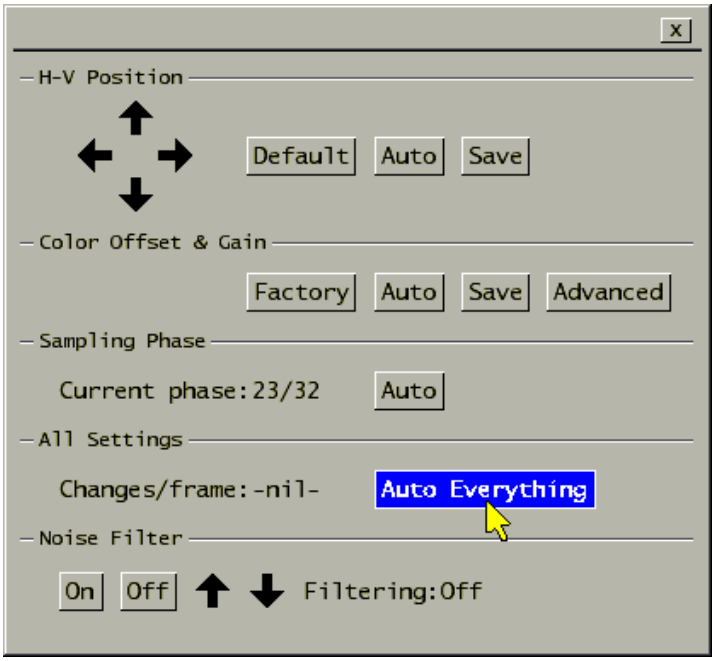


Display the following test pattern on the host server.

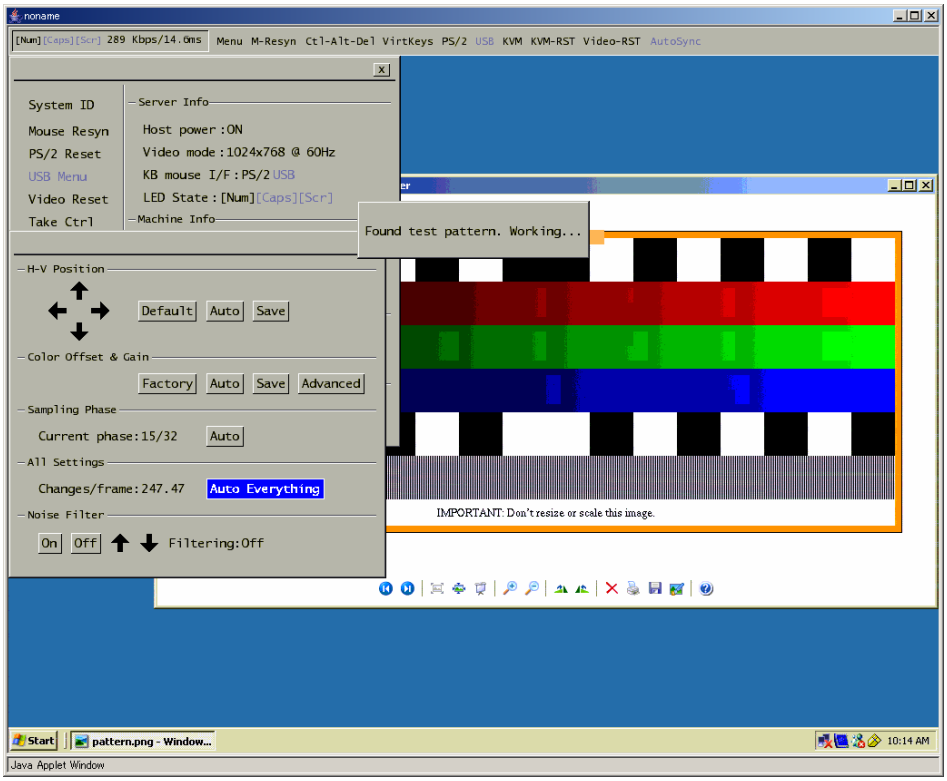


Obtain the test pattern for Video Tunes from the URL below.
Then prepare this pattern in the host server.
https://IP address for this product/images/pattern.png

Click the [Auto Everything] button in the All Setting item of the video tune window.



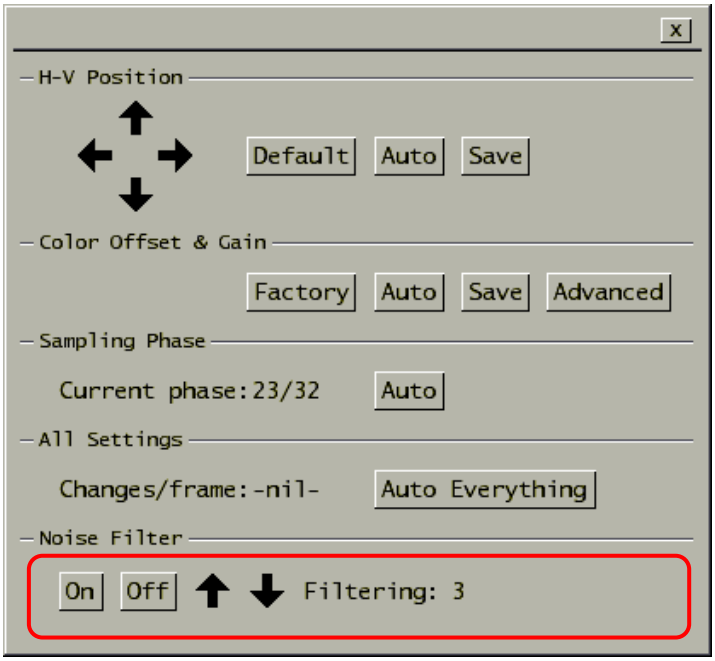
[Found test pattern. Working...] dialogue box is displayed during the auto-setting as follows. The setting takes about 20 seconds.



Click [Save] button after the [Auto Everything].

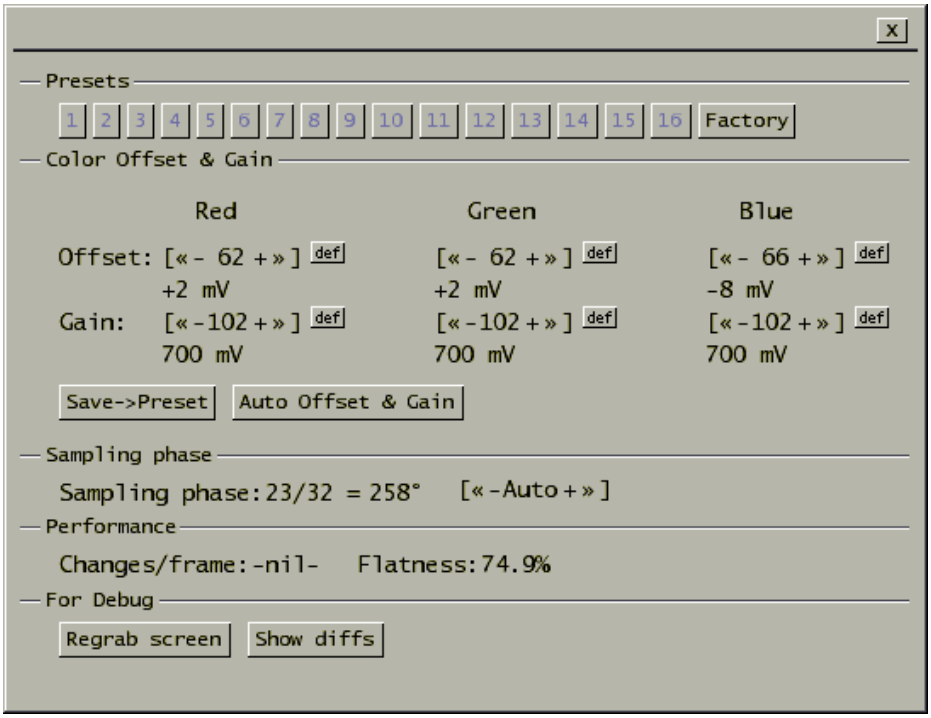
- **Specify the noise filter setting**

  Image data transmitted from the host server includes noise. It increases the volume of transmit data and operation may be delayed.
  Click the [On] button of the Noise Filter setting in the Video Tune window. Specify the value between 1 and 31 for transmission rate.
  ↑: Increase the filtering value, ↓: Decrease the filtering value



- **Tune the Offset and Gain value**

Click the [Menu] button in the VNC menu bar to display the menu window. Click [Video Tune] → [Advanced] button, tune Red, Green and Blue offset and Gain value in the following window.



Click the following symbols to change the value.

Symbol	Setting value
«	Decrease the setting value (-10)
-	Decrease the setting value (-1)
»	Increase the setting value (+10)
+	Increase the setting value (+1)
[	Offset: The value is set to 0. Gain: The value is set to 0.
]	Offset: The value is set to 127. Gain: The value is set to 255.

Adjust the Red, Green and Blue Offset and Gain value with monitoring the display.

Click the [Save->Preset] button to save the new setting. After the [Save->Preset] button is displayed in gray, click any number button of 1 to 16. The new setting saved in that number.

5.1.14 Specify a Notebook Computer as Host Server

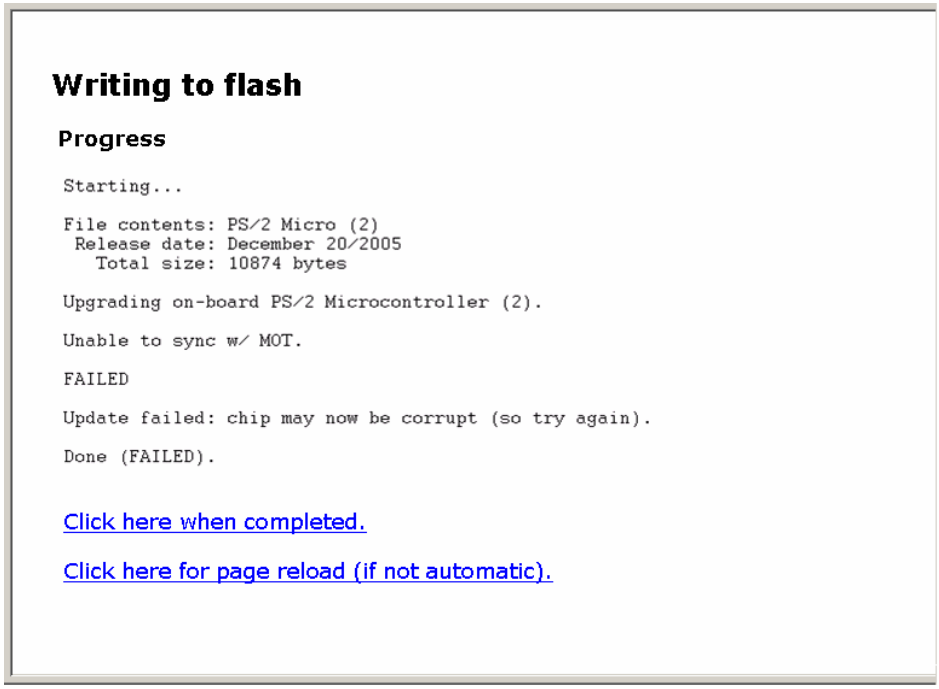
- **Check specifications for the external video output**

  Enable the use of the external video output to use a notebook computer as a host server.
  Some notebook computers do not support the external video output in any mode.
  Refer to the user's manual for the notebook computer.

5.1.15 Error during the Firmware Uploading

- **If this product does not start up, disconnect the connector once**

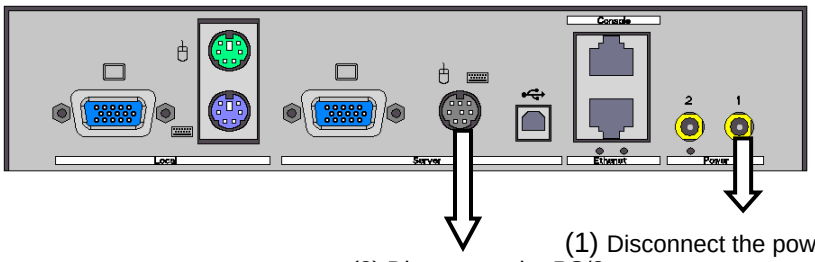
  When the [FAILED] message is displayed as follows while firmware is uploading in [Flash/Firmware Management] of the web page, this product may not be started up.



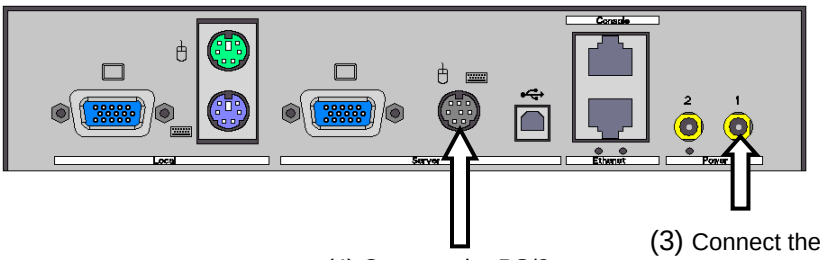
  Perform following recovery method in such a case.

Recovery Method

Disconnect the power adapter and PS/2 connecter from the server.
And then reconnect the power adapter and PS/2 connecter to the server in this order.



(1) Disconnect the power adapter
(2) Disconnect the PS/2 connecter



(3) Connect the power adapter
(4) Connect the PS/2 connecter

Connect to the host server from the remote terminal and make sure that the keyboard and mouse work properly.

If the product does not operate properly after using these recovery methods, please contact Fujitsu Comportment Customer Service and Support Center.
📖 Refer to 5.2 Technical Support (page 162)

5.2. Technical Support

< Inquiry about our products>

FUJITSU COMPONENT LIMITED
Marketing Department
TEL: 81-3-5449-7006, Fax: 81-3-5449-2626

E-mail: promothq@fcl.fujitsu.com
URL: http://www.fcl.fujitsu.com/en/

< Inquiry about repairs and failures>

FUJITSU COMPONENT LIMITED Customer Service & Support Center
TEL: 0120-810225 *Contact by mobile phones, automobile telephones and PHSs are supported.
E-mail: servis-center@fcl.fujitsu.com
Business Hours: 9:00 - 12:00, 13:00 - 17:00
(Every day except Saturdays, Sundays and public holidays.)