When you're ready to take control.™

MasterConsole IP

MCIP18, MCIP116

User Guide

MCIP-0E-E
April 2009
255-18-0020-00

This page intentionally left blank.

Copyright and Trademark Information

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan’s reasonable control or not arising under normal operating conditions.

C US 1F61 I.T.E.
LISTED

For assistance in the North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see **Appendix A: Specifications**).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Contents

Figures

This page is intentionally left blank.

Chapter 1: Introduction

MasterConsole IP Overview

Raritan's keyboard/video/mouse (KVM) switches are engineered to provide reliable, cost-effective, central control of multiple computers. This eliminates the cost and clutter of unnecessary equipment, reclaims space, and improves productivity for a host of applications.

MasterConsole IP (MCIP) enables control of 8 to 16 computers from a single keyboard, monitor, and mouse. The MasterConsole IP user interface provides simple on-screen control and system management. Raritan's unique emulation technology dedicates a keyboard/mouse emulator for each computer to ensure that each computer always 'sees' its own keyboard and mouse. This means smooth, flawless switching and operation, even when computers are running the most demanding operating systems.

MCIP defines a new class of remote KVM access devices. It combines an 8-port or 16-port KVM switch with digital remote KVM access via IP networks and comprehensive system management. Remote access and control software runs on the MCIP embedded processors only but not on mission-critical servers, so that there is no interference with server operation.

MCIP offers convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. MCIP provides a non-intrusive solution for remote access and control.

Product Photo

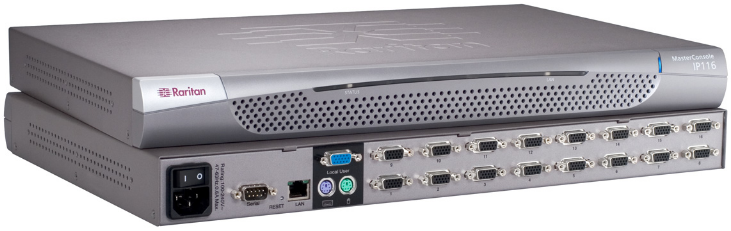


Figure 1 MCIP 116 Unit

Product Features

- MCIP Models available in 8-port and 16-port models
- KVM (keyboard, video, mouse) remote access over IP
- "Keep-alive" emulation ensures non-stop computer operation in the event of power loss to the switch
- High-resolution video – 1600 x 1200 (Remote is not recommended)
- Tangle-proof, double-shielded coaxial cable in lengths from 2 to 30 feet
- On-screen user interface for simple control and system management
- Provision to mix any brand PCs, Macs USB, & Sun USB. Note: SUN & MAC can be supported by connecting APSUSB
- Name assignment availability for quick identification and selection
- Operation from hot-keys with on-screen menus
- AutoScan function to view other computers at variable rates
- AutoSkip function provided to bypass inactive channels
- Password Security to ensure authorized access to computers

Chapter 2: Installation

Getting Started

MasterConsole IP is designed for quick, easy installation and operation:

1. Physically configure MCIP.
2. Install MCIP and connect computers.
3. Configure MCIP software.
4. Assign computer names and set channel-specific scan rates for attached computers.
5. Turn ON security and change passwords to restrict access to computers connected to MCIP.
6. Operate using On-Screen User Interface.
7. Install optional Cat5 Reach for remote console or satellite unit.

Quick-Start Operation

After you connect computers to the MCIP unit, explore operation with the default names and parameters.

You may operate using the On-Screen User Interface (OSUI). To activate the OSUI, press the **Left Ctrl** key on your keyboard three times rapidly. The Selection Menu appears. Use the ↑ (up arrow) and ↓ (down arrow) keys to highlight the desired channel (computer) and press the **Enter** key OR press the computer's Key number, listed in the left-hand column on your screen. To select another computer, re-activate the OSUI and reselect.

Configuration

MCIP can be configured only in a single configuration, and only computers can be connected to a single MasterConsole IP unit. Configure up 8 computers using an MCIP18 model, and up to 16 computers using an MCIP116 model.

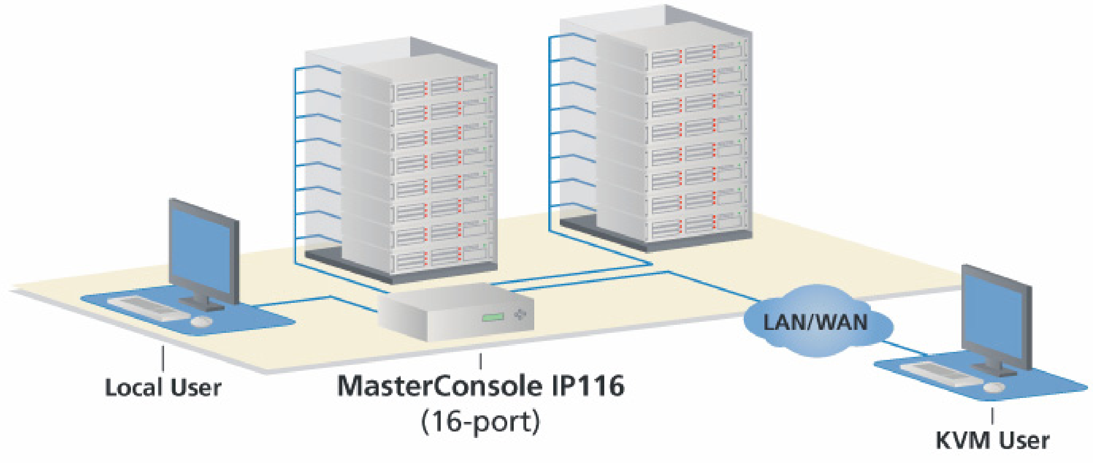


Figure 2 One-Tier Configuration

Installation

1. Power OFF all computers to be connected to MCIP.
2. Plug a keyboard, monitor, and mouse into the keyboard, monitor, and mouse ports on the rear panel of the MCIP.

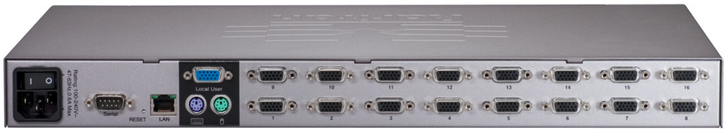


Figure 3 MCIP Rear Panel

3. Power ON MCIP.
4. Using an MCIP cable (CMCIP20, 40, or 90), plug the 15-pin connector into one of the numbered channels on the MCIP rear panel.
5. Plug the cable's other connectors into the computer's keyboard, monitor, and mouse ports.
6. Power ON the connected computer.
7. Select the connected computer using the On-Screen User Interface (please see **Chapter 3: Operations** for instructions). Verify that the monitor attached to MCIP displays the video for the connected computer. Use the keyboard and mouse attached to MCIP to verify that they operate the connected computer.

Figure 4 MCIP Front Panel Channel Lights

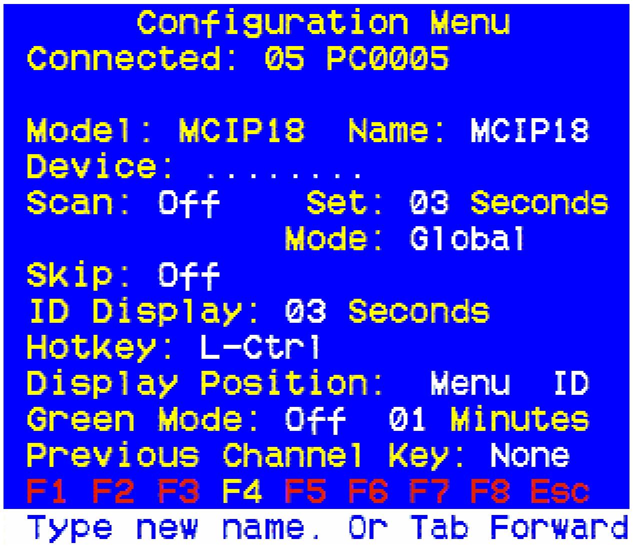
8. Repeat steps 4 through 7 to connect the remaining computers.

Chapter 3: Operation

Use the Configuration Menu is to specify your MCIP configuration and to set or change operation parameters.

1. Activate the On-Screen User Interface (**OSUI**) by pressing the Hot Key (default: **Left CTRL** key on keyboard) three times rapidly. When the OSUI appears, press **F4** to access the Configuration Menu.

__Note__: Currently, Hotkey function is not enabled for further change.



```
      Configuration Menu
 Connected: 05 PC0005

 Model: MCIP18   Name: MCIP18
 Device: ........
 Scan: Off     Set: 03 Seconds
              Mode: Global
 Skip: Off
 ID Display: 03 Seconds
 Hotkey: L-Ctrl
 Display Position:  Menu  ID
 Green Mode: Off  01 Minutes
 Previous Channel Key: None
 F1 F2 F3 F4 F5 F6 F7 F8 Esc
 Type new name. Or Tab Forward
```

Figure 5 Configuration Menu

a. The **Connected** field displays the Channel ID and Name of the currently selected computer.

b. The **Model** field displays the model number of this MasterConsole unit.

2. Use the **Tab** (forward)/**Shift** + **Tab** (backward) keys to highlight the desired field and make your changes as follows:

a. To change **Name** (default is the unit's model number): Move to **Name** and type a name up to seven characters. This field is used for identification purposes only.

b. To turn AutoScan ON/OFF (default is OFF): Move to **Scan** and press the ↑ / ↓ keys to toggle. If you exit the OSUI with AutoScan ON, MCIP will scan according to the currently set mode (Individual/Global) and scan rate.

- To change the Global Scan Rate (default is 3 seconds): Move to **Set** and type a number from 01 to 99, or press the ↑ / ↓ keys to specify the Scan Rate (in seconds) for Global AutoScan.
- To change AutoScan mode (default setting is Global): Move to **Mode** and press the ↑ / ↓ keys to toggle between Global and Individual.

c. To turn AutoSkip ON/OFF (default is OFF): Move to **Skip** and press the ↑ / ↓ keys to toggle. With AutoSkip ON, only active channels can be selected.

d. To change the ID Display time interval (default is 3 seconds): Move to **ID Display** and type a number from 01 to 99, or press the ↑ / ↓ keys to specify the interval (in seconds) you want the Channel ID and Name to display when each computer is selected. Type 99 if you want the Channel ID and Name to display continuously.

e. Green mode is disabled.

f. Previous channel key function is disabled.

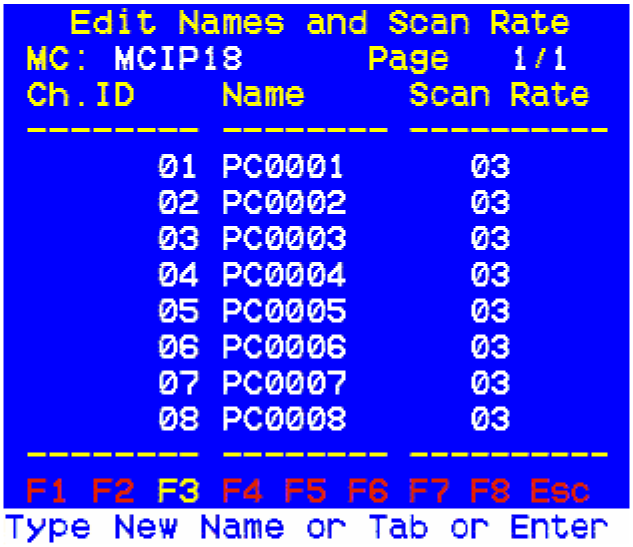
Note: *Both Green mode and Previous Channel Key functions are disabled, and no further changes to their default values can be made..*

3. To exit the Configuration Menu, press a Function key on your keyboard to access a different menu, as displayed along the bottom of the menu screen. Press **Esc** to exit the OSUI and return to normal computer operation. Any changes made in the Configuration Menu are automatically saved.

Assigning Names and Scan Rates

Assign meaningful names to easily identify and select connected computers. By default, the channel name is PC00nn (where **nn** is the Channel ID Number) and the Channel-Specific Scan Rate is 3 seconds.

1. Activate the OSUI by pressing the Hot Key (default: **Left CTRL**) three times rapidly. When it appears, press **F3** to access the Edit Names and Scan Rate menu.



```
   Edit Names and Scan Rate
MC: MCIP18        Page   1/1
Ch.ID      Name      Scan Rate
--------- --------- ----------
       01 PC0001        03
       02 PC0002        03
       03 PC0003        03
       04 PC0004        03
       05 PC0005        03
       06 PC0006        03
       07 PC0007        03
       08 PC0008        03
--------- --------- ----------
F1 F2 F3 F4 F5 F6 F7 F8 Esc
Type New Name or Tab or Enter
```

Figure 6 Edit Names and Scan Rate Menu (One-Tier)

2. Use the **Tab**, **Shift+Tab** or ↑ / ↓ keys to move the cursor to the line you want to edit. Use ← / → to move within a line.
   a. To change the **Name**: Type up to eight characters without spaces.
   b. To change the Channel-Specific **Scan Rate** (default is 3 seconds): Type a number from 00 to 99 (seconds). When the AutoScan Mode in the Configuration Menu is set to Individual, these Channel-Specific Scan Rates are enabled. If the AutoScan mode is set to Global, the global value will be used.
3. When you move to a different page or exit this Menu, you are prompted to save your changes. Press **Y** to save.
4. To exit the Edit Names and Scan Rate Menu, press a Function key on your keyboard to access a different menu, as displayed along the bottom of the menu screen, or press **Esc** to return to the Selection Menu.

Note*: If your MCIP unit is a 16-channel model, MCIP116, use the* ***Page Up*** */* ***Page Down*** *keys on your keyboard to view the next or previous screen of eight channels.*

Using MasterConsole IP Security Feature

Restrict access to MCIP by turning security ON or OFF in the Administration Menu. Up to six passwords can be defined in the Administration Menu – one Administration Password and five User Passwords.

If security is ON and the system is idle (no keyboard or mouse activity for a time interval set by the user [default: 15 minutes]), the next user to access MCIP must enter a user password to establish access.

By default, MasterConsole IP operates with security OFF.

Passwords

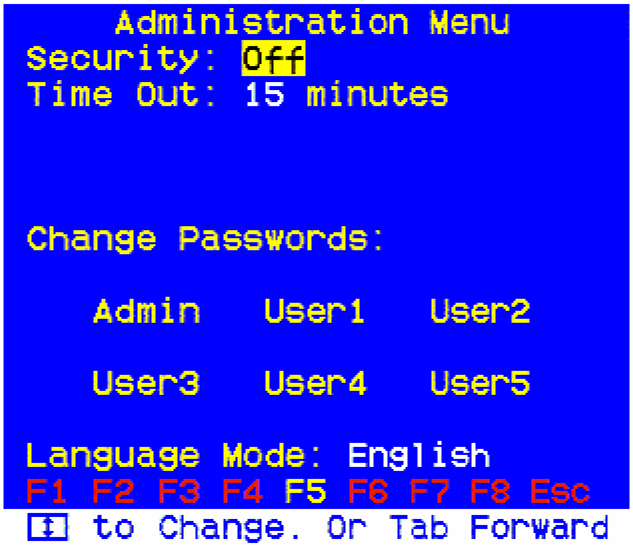
Only the Administrator's password provides access to the Administration Menu, accessed to turn security ON or OFF and to change passwords. Raritan recommends that administrators record and store passwords where they will be handy to you and other authorized users.

MasterConsole IP is delivered with system default passwords. They are:

USER	PASSWORD
Administrator	raritan
User 1	111
User 2	222
User 3	333
User 4	444
User 5	555

Turning Security ON / OFF and Changing Passwords

1. Activate the OSUI by pressing the Hot Key three times rapidly. When it appears, press **F5** to access the Administration Password prompt.
2. Type the Administration Password and press **Enter**. The Administration Menu appears.



```
     Administration Menu
Security: Off
Time Out: 15 minutes



Change Passwords:

    Admin    User1    User2

    User3    User4    User5

Language Mode: English
F1 F2 F3 F4 F5 F6 F7 F8 Esc
⇕ to Change. Or Tab Forward
```

Figure 7 Administration Menu

3. Press **Tab** or **Shift+Tab** to move the cursor forward or back to the desired field and make your changes as follows:

a. To turn Security ON/OFF (default is OFF): Press the ↑ / ↓ keys to toggle.

b. To change Security activation delay time (default is 15 minutes). Move to the **Time Out** field, then type a number from 01 to 99, or use the ↑ / ↓ keys to specify a time interval. If the system will remains inactive (no keyboard or mouse operation) for this time interval, the next user is required to enter a password to access the MasterConsole IP.

c. To change the Administration Password: Move to **Change Passwords**, where Admin will be highlighted. Press the **Enter** key and type a new password (up to eight alphanumeric characters, no spaces). Press **Enter**. Confirm the password by retyping it. Press **Enter**.

Important: Note down the new Administration Password and keep it in a safe place. If you forget this password, there is no other way to retrieve or reset it. When this occurs, contact your dealer or Raritan Technical Support.

d. To change a User Password, press the **Tab** key to highlight the desired **User#** field. Press **Enter**. Type a new password (up to eight alphanumeric characters, no spaces). Press **Enter**. Confirm the password by typing it again. Press **Enter**. Repeat this process for the remaining four Users, pressing the **Tab** key to move from one User field to the next. You can specify up to five User Passwords.

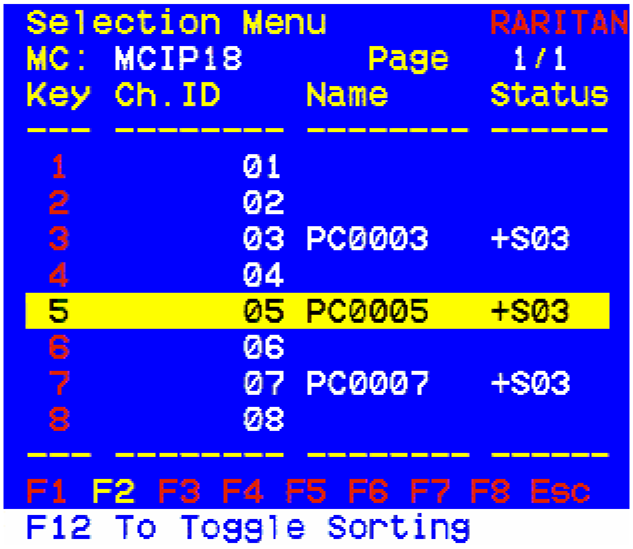
e. To change the type of keyboard, press the **Tab** key to highlight **Language Mode** field. Press ↑ / ↓ to select English, German, or French.

4. To exit the Administration Menu, press a Function key on your keyboard to access a different menu, as displayed along the bottom of the menu screen. Press **Esc** to exit the OSUI and return to normal computer operation.

Using the On-Screen User Interface (OSUI)

Selecting a Computer

1. Activate the OSUI by pressing the Hot Key three times rapidly. To switch the channel you are viewing, press [**Left CTRL**] two times, then press *N*, where *N* is the channel number you want to see. The Selection Menu appears.



```
Selection Menu      RARITAN
MC: MCIP18     Page  1/1
Key Ch.ID     Name     Status
--- -------- -------- ------
 1        01
 2        02
 3        03 PC0003   +S03
 4        04
 5        05 PC0005   +S03
 6        06
 7        07 PC0007   +S03
 8        08
--- -------- -------- ------
F1 F2 F3 F4 F5 F6 F7 F8 Esc
F12 To Toggle Sorting
```

Figure 8 Selection Menu (One-Tier, sorted by Channel ID)

2. Channels are listed either numerically by **Channel ID** or alphabetically by **Name** (default: sort numerically by Channel ID). Press **F12** to toggle between numerical and alphabetical sorting.

3. The Selection Menu displays a maximum of eight channels at a time.

a. The **Status** column shows each channel's activity and Channel-Specific Scan Rate. A "+" in the first column indicates a device is connected and powered ON, while a blank indicates the device is powered OFF or there is no device connected. "Snn" indicates the Channel-Specific Scan Rate of nn seconds. (default is 3 seconds).

b. As the computer status changes (active/inactive), the MCIP updates the Status column periodically. To enable a user to see the new status immediately, activate the OSUI and press F8-Upgrade Computer Status. The MCIP will scan the channels and update the computer status and then return to the previous menu.

c. For any inactive channel, the ID bar will display only the channel ID and not the name field, when sorted by channel and will not display anything when sorted by name-F12 toggle.

d. The non-displayed names are still available in the MCIP internal database and can be edited with the F3 function.

4. To select a computer:

    - Use the **Page Up** / **Page Down** or ↑ / ↓ keys to highlight the desired computer and press **Enter**

OR

    - When the Selection Menu is sorted by Channel ID, press the desired computer's Key number (shown in the left-hand column);

OR

    - When the Selection Menu is sorted by name (arranged alphabetically), use the **Page Up** / **Page Down** or ↑ / ↓ keys, or type the first character(s) of the desired Name to quickly jump to the Name that most closely matches what you type. To back up a character, press the **Backspace** key. Highlight the desired computer, and press **Enter**.

a. When you select a computer, you automatically return to normal computer operation at the selected computer.

b. The Channel ID and Name will be displayed on the monitor for the time interval specified in the Configuration Menu.

c. Press **Home** at any time to return to the first page of the Configuration Menu (for 16-channel.

Activating AutoScan

1. Activate the OSUI by pressing the Hot Key three times rapidly. Press the **F6** Key.
2. On the front panel of the MCIP unit, a green light next to the **Scan** button will illuminate.
3. The unit will scan according to parameters set in the Configuration Menu.

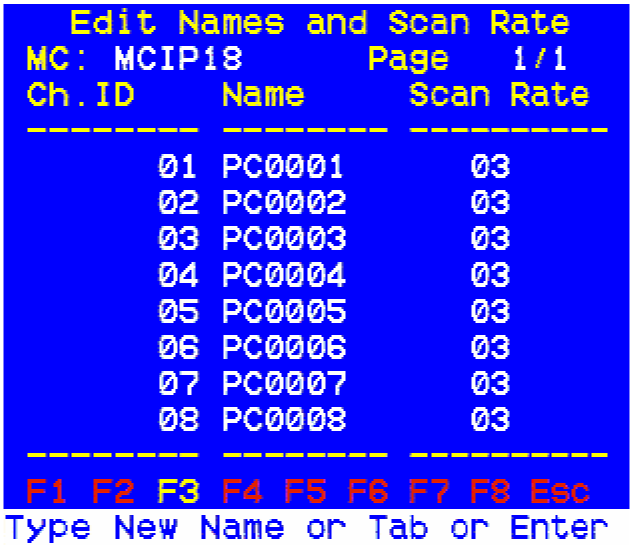
Assigning Names and Scan Rates

When you specify non-computer devices (MasterConsole units) connected to base MCIP channels, these devices are assigned default names in the base MCIP Selection Menu.

Because computers can be connected to each channel of an MCIP unit, a page is automatically created for the MCIP in the Selection Menu, listing Channel IDs with default names for each channel. These names may be changed using the Edit Names and Scan Rate Menu.

To change Names and/or Channel-Specific Scan Rates:

1. Activate the OSUI by pressing the Hot Key three times rapidly. When it appears, press **F3** to access the Edit Names and Scan Rate Menu.



```
   Edit Names and Scan Rate
MC: MCIP18        Page   1/1
Ch.ID      Name       Scan Rate
--------- -------- ----------
       01 PC0001       03
       02 PC0002       03
       03 PC0003       03
       04 PC0004       03
       05 PC0005       03
       06 PC0006       03
       07 PC0007       03
       08 PC0008       03
--------- -------- ----------
F1 F2 F3 F4 F5 F6 F7 F8 Esc
Type New Name or Tab or Enter
```

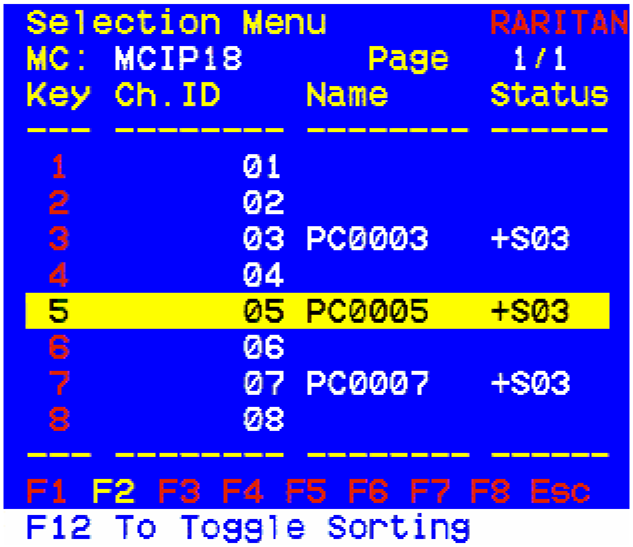
Figure 9 Edit Names and Scan Rate Menu (Base MasterConsole IP)

2. Use the **Tab**, **Shift-Tab** or ↑ / ↓ keys to move the cursor to the line you want to edit. Use ← / → to move within a line.
   a. To change the Name of any computer connected to the base unit, type up to eight alphanumeric characters (no spaces).
   b. To change the Channel-Specific scan Rate for any highlighted channel (default is 3 seconds): Type a number from 00 to 99 (in seconds). When the AutoScan Mode in the Configuration Menu is set to Individual, these Channel-Specific Scan Rates are enabled. If the AutoScan mode is set to Global, the global scan rate will be used.
3. When you move to a different page or exit this menu, you are prompted to save your changes. Press **Y** to save.
4. To exit the Edit Names and Scan Rate Menu: Press any Menu F (Function) key to go to another menu, or press **Esc** to return to the Selection Menu.

MasterConsole IP Operation

Selecting a Computer

1. Activate the OSUI by pressing the Hot Key three times rapidly. The Selection Menu appears.



```
Selection Menu        RARITAN
MC: MCIP18       Page   1/1
Key Ch.ID     Name      Status
--- --------- --------- ------
 1         01
 2         02
 3         03 PC0003    +S03
 4         04
 5         05 PC0005    +S03
 6         06
 7         07 PC0007    +S03
 8         08
--- --------- --------- ------
F1 F2 F3 F4 F5 F6 F7 F8 Esc
F12 To Toggle Sorting
```

Figure 10 Selection Menu

2. The Selection Menu lists channels sorted either numerically by Channel ID or alphabetically by Name. Default: by Channel ID. Press **F12** to toggle.
   a. The Selection Menu displays a maximum of eight channels at a time.
   b. The Status column shows each channel's activity and Channel-Specific Scan Rate. A "+"in the base unit's Selection Menu indicates the device is connected and powered ON, while a blank indicates the device is powered OFF, or there is no device connected.. Snn indicates the individual Scan Rate of nn seconds.
   c. As the computer status changes (active/inactive), MCIP updates the Status column periodically. To enable a user to see the new status immediately, activate the OSUI and press F8-Upgrade Computer Status. MCIP will scan the channels and update the computer status and then return to the previous menu.
   d. For any inactive channel, the ID bar will display only the channel ID and not the name field, when sorted by channel and will not display anything when sorted by name-F12 toggle.
   e. The non-displayed names are still available in the MCIP internal database and can be edited with the F3 function.
3. To select a computer:
   - Use the **Page Up** / **Page Down** or ↑ / ↓ keys to scroll to the desired computer and press Enter

OR

   - When the Selection Menu is sorted by Channel ID, press the desired computer's Key number (in the left-hand column)

OR

   a. When the Selection Menu is sorted by name, use the **Page Up** / **Page Down** or ↑ / ↓ keys, or type the first character(s) of the desired Name to quickly jump to a Name that most closely matches what you type. To back up a character, press the **Backspace** key. Highlight the desired computer, and press **Enter**.
   b. When you select a computer, you automatically return to normal computer operation at the selected computer.

c. The Channel ID and Name will display on the monitor for the time interval specified in the Configuration Menu.

d. Press **Home** at any time to return to the first channel on the first page of the Selection Menu. Press **End** at any time to advance to the last channel on the last page of the Selection Menu.

Chapter 4: Remote Management and Operation

Initial Configuration

MCIP comes pre-configured with the values shown below, and its communication interfaces are based on TCP/IP. You must perform an initial IP configuration to access MCIP for the first time.

PARAMETER	VALUE
IP auto configuration	DHCP
IP address	192.168.1.22
Netmask	255.255.255.0
Gateway	None
IP access	Disabled
LAN interface speed	Auto
LAN interface duplex mode	Auto

Initial Configuration via DHCP Server

By default, MCIP will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address, and net mask.

Before you connect the MCIP unit to your local subnet, complete the corresponding configuration of your DHCP server. Raritan recommends that you configure a fixed IP assignment to the MAC address of MCIP. The MAC address is located on the outside of the shipping box and on the bottom of the MCIP unit. If the DHCP connection fails on boot up, MCIP will not have an IPv4 address.

Initial Configuration via Serial Interface

MCIP has a serial line interface on its front panel. The connector is compliant to RS 232 serial line standard. The serial interface must be configured with the parameters listed below.

PARAMETER	VALUE
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

To configure MCIP via the serial interface:

1. Power OFF the MCIP unit, then power ON again to reset.
2. Press the **ESC** key on your keyboard. Device information and a prompt appear.
3. Type **config** and press the **Enter** key. After a few seconds, lines appear.
4. Type the answers as the questions appear, or press **Enter** to use the default value (shown here in brackets).

```
    IP auto configuration (none/dhcp/bootp) [dhcp]:
```

```
IP [192.168.1.22]:
NetMask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:
```

- **IP auto configuration:** With this option you can specify whether MCIP should fetch it's network settings from a DHCP or BOOTP server. For DHCP you have to enter dhcp And for BOOTP supply bootp accordingly. If you specify none then IP auto configuration is disabled and you will subsequently be asked for the following network settings.
- **IP address:** The IP address the MCIP should use. This option is only available if IP auto configuration is disabled.
- **Subnet mask:** The mask of the connected IP subnet. This option is only available if IP auto configuration is disabled.
- **Gateway address:** The IP address of the default router of the connected IP subnet. If you have no default router, you may enter 0.0.0.0. This option is only available if IP auto configuration is disabled.

There may be default values which are enclosed in brackets. If you want to use the default value of an option then you just need to press the Enter key.

You will be asked if the values are correct and get a chance to correct them. After confirming, MCIP performs a reset.

Logging In

In your Web browser, type the MCIP address you configured during installation. For instance, type the following in the address line of your browser when establishing an unsecured connection:

```
http://192.168.1.22/
```

When using a secure connection type:

```
https://192.168.1.22/
```

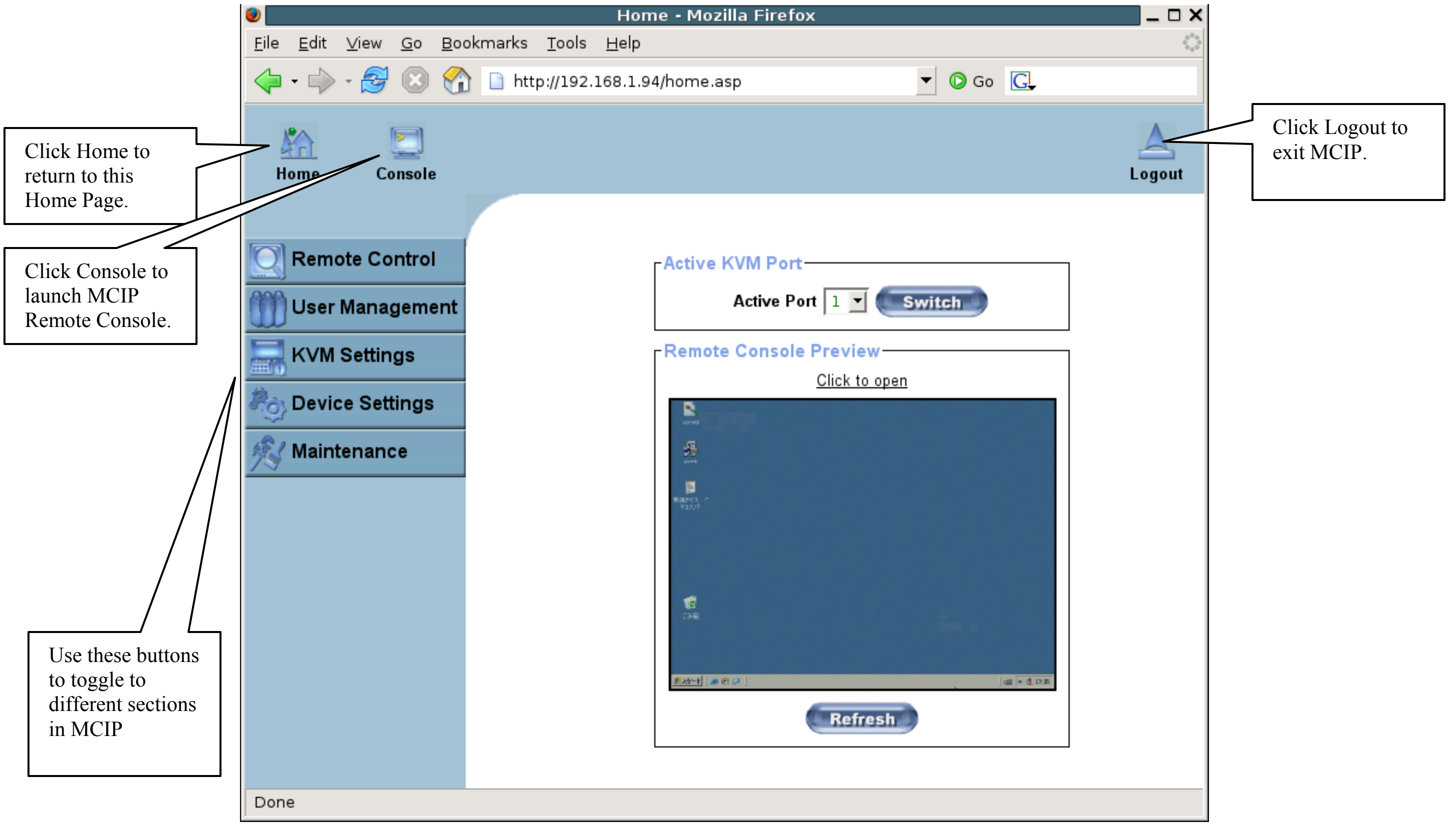
The MCIP login page appears. MCIP has a built-in "**super user**" who has all administrative permissions for the MCIP unit. The **super user** login is **admin** and the password is **raritan**. Both Login and Password are case-sensitive.

Please note that super user **admin** cannot log on via the serial interface of MCIP. Your web browser must accept cookies or you will be unable to log in.

Note: *Please change the super user password,* ***raritan,*** *immediately after you have installed and accessed your MCIP for the first time. Leaving this password can be a severe security risk.*

Navigation

Upon successful login, the MCIP Home appears.



http://192.168.1.94/home.asp

Active Port 1

Done

Click Home to return to this Home Page.

Click Console to launch MCIP Remote Console.

Use these buttons to toggle to different sections in MCIP

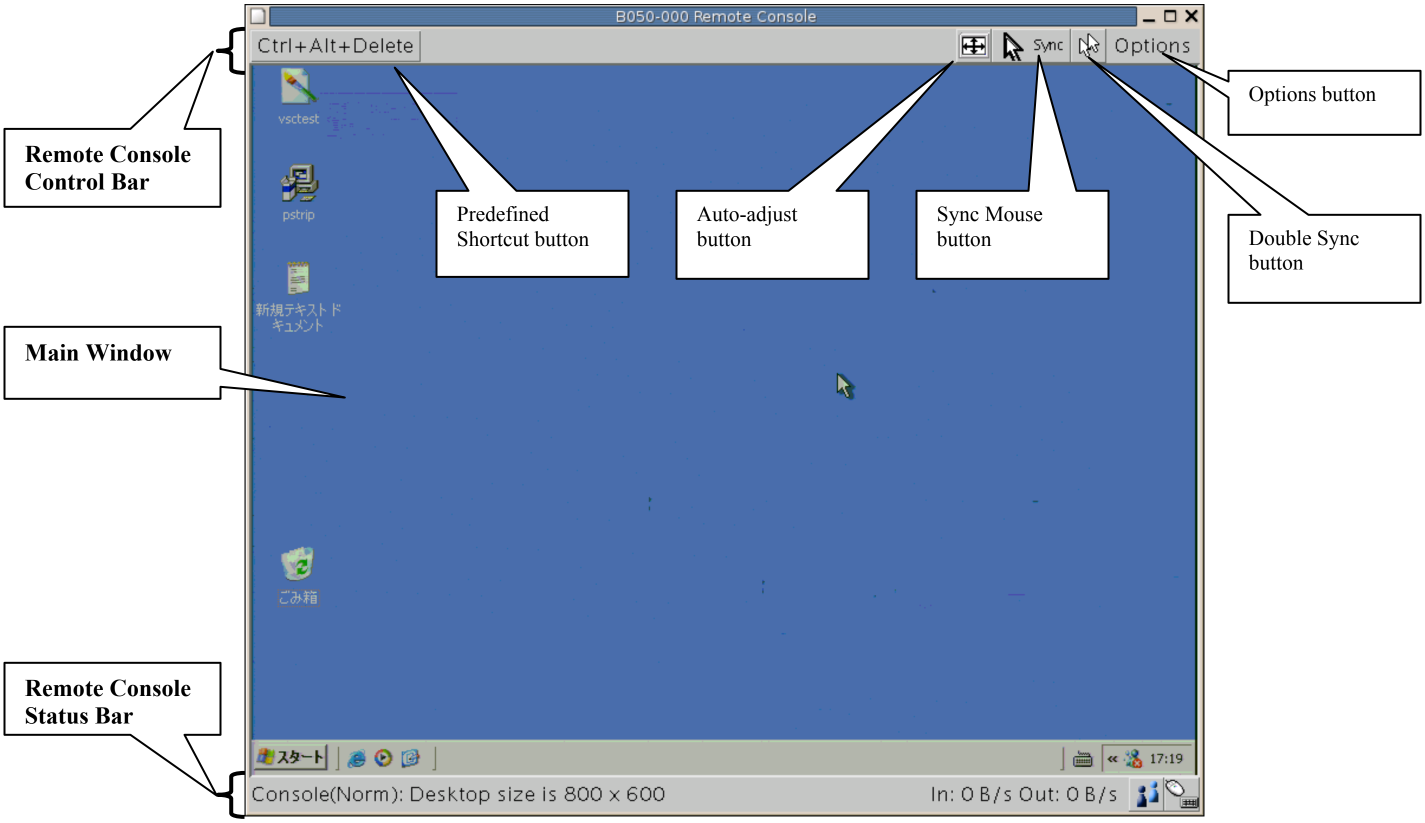
Click Logout to exit MCIP.

Figure 11 MCIP Home Page

If there is no activity for 30 minutes, you will be logged out of MCIP automatically. Press any key or move your mouse to return to the Login screen if this occurs.

The Remote Console

The Remote Console is the redirected screen, keyboard, and mouse of the remote host system that MCIP controls.



Console(Norm): Desktop size is 800 x 600

In: 0 B/s Out: 0 B/s

Figure 12 Remote Console Screen

Remote Console is a Java Applet that tries to establish its own TCP connection to the MCIP. The protocol run over this connection is neither HTTP nor HTTPS, but Remote Frame Buffer Protocol, or RFB.

Currently, RFB tries to establish a connection to port 443. Your local network environment must allow this connection to be made, that is, your firewall and – in case you have a private internal network – your Network Address Translation (NAT) settings must be configured accordingly. If the MCIP unit is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the according connection. This is because today's web proxies are not capable of relaying the RFB protocol. In case of problems, please consult your network administrator to provide an appropriate network environment.

Main Window

Activating Remote Console opens a new window that displays the screen content of your host system. The Remote Console behaves exactly as if you were sitting directly in front of the screen of your remote system, meaning you can use the keyboard and mouse normally to work in the remote system. There will be a slight delay in reacting to commands and actions, depending on your connection bandwidth.

Remote keyboard usage may be incorrect, as your local keyboard changes its keyboard layout according to the remote host system. For example, if you use a German administration system and your host system uses a US English keyboard layout, special keys on the German keyboard will not work as expected, but will instead act as they would on the US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window attempts to show the remote screen at optimal size, so it adapts its size automatically to the size of the remote screen. You can resize the Remote Console window locally as needed. Unlike the remote host system, your local Remote Console window is just one window among many. In order for the keyboard and mouse to function, the Remote Console window must be the active window on your monitor.

Remote Console Control Bar

The elements in the Remote Console Control Bar allow you to change or view the status of the Remote Console settings.

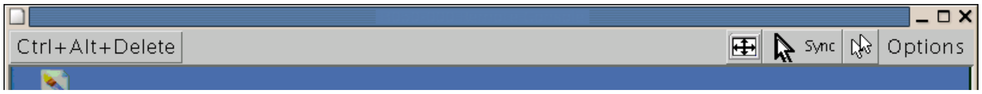


Figure 13 Remote Console Control Bar

Predefined Shortcut: This button exists only for the super user; other users can configure their own shortcuts (please see **Chapter 6: KVM Settings** for additional information).

Auto-adjust: If the video quality is poor or distorted, press this button and wait a few seconds while MCIP adjusts for the best possible video quality.

Sync Mouse: Click to synchronize local mouse pointer with remote mouse.

Double Sync: Click to toggle from Single Mouse Mode (viewing remote mouse only) and the Double Mouse Mode (where you can view both remote and local mouse icons). Single mouse mode is only available if using SUN JVM 1.4 or higher.

Options: Click to activate the Options menu.

Options Menu

When you click **Options** in the Control Bar, a drop-down menu appears.

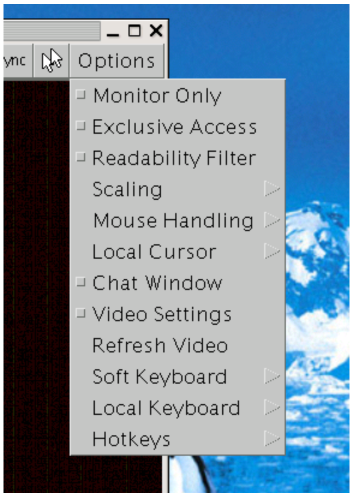


Figure 14 Options Menu

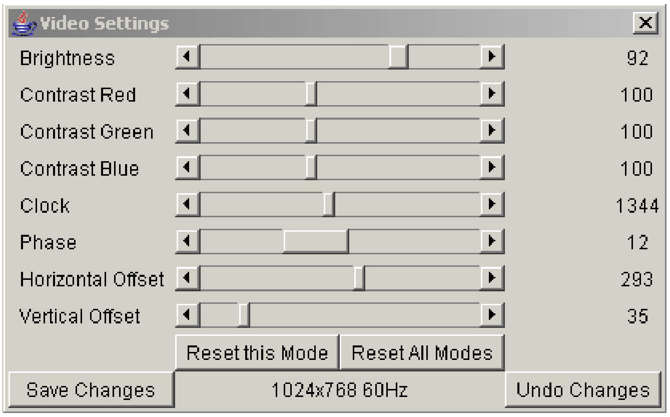
- **Monitor Only** – toggles the MCIP between no remote console interaction and remote monitoring.
- **Exclusive Access** – users with the appropriate permissions can close all other users on the Remote Console at that time. No user can open the Remote Console while this user is active until this user disables Exclusive Access or logs off. Changing access is visible in the status line (please see Remote Console Status Line section, below, for additional information).
- **Readability Filter** – toggles the Readability Filter on / off. If Readability Filter is ON in scaling mode, it will preserve most of the screen details, even if the image is scaled down. Please note that this option is available only with JVM 1.4 or higher.
- **Scaling** – allows scaling up to the size of the Remote Console screen. You can still use both keyboard and mouse, but the scaling algorithm may not preserve all display details.
- **Mouse Handling** – select an option for synchronizing local mouse and remote mouse:
  - **Fast Sync** – used to correct a temporary but fixed skew.
  - **Intelligent Sync** – used if Fast Sync does not work or if the mouse settings have been changed on the host system. Please note that Intelligent Sync takes longer than Fast Sync, and requires a correctly adjusted screen. Use the auto adjustment function or the manual correction in the Video Settings panel to adjust.
- **Mouse Mode** – choose Single Mouse Mode or Double Mouse Mode.
- **Local Cursor** – choose from different icons for the local mouse pointer. The icon selected will be saved for this user and activated every time this user opens Remote Console. The icon list depends on the JVM version (JVM version 1.2 or higher offers a full list).
- **Chat Window** – MCIP Remote Console features a Chat Window that allows communication among all users logged into the same card. This feature is useful for discussing problems or answering questions among all users.

  Chat Window Components include:

  - **Title Bar** – displays the MCIP address
  - **Chat Area** – read-only text area that displays messages
  - **Identity Label** – displays the identity string; the first part of the string is the user's ID, the second part is the hostname of the client system, and the last part (in parentheses) is the user name
  - **Chat Line** – an editable text line where you type a new message; once finished, press Enter to broadcast the message to all connected users. If a user does not have the chat window open, it will launch automatically and display the new message. There is no option to direct a message to a particular user only.

- – Chat has no message history, that is, messages are received only after opening Remote Console. Messages sent previously to login will not appear to a user who opens Remote Console afterward they are broadcast.

- **Video Settings –** activates the Video Settings panel for adjusting MCIP video settings. MCIP allows you to adjust video settings in two ways: via the HTML front end, or via Remote Console, as illustrated here.
  - – **Video Settings via Remote Console**: click and drag the blocks from left to right to adjust each field value (or click on the left and right arrow buttons)



Brightness	92
Contrast Red	100
Contrast Green	100
Contrast Blue	100
Clock	1344
Phase	12
Horizontal Offset	293
Vertical Offset	35

1024x768 60Hz

Figure 15 Video Settings Panel

- **Brightness:** Controls the brightness of the picture.
- **Contrast (Red, Green, Blue):** Controls the color contrast of the picture.
- **Clock:** Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values; default settings in conjunction with the auto adjustment procedure should be adequate for all common configurations. To achieve a better picture quality you may try to change this setting together with the sampling phase, below.
- **Phase:** Defines the phase for video sampling, used to control the display quality together with the setting for clock, above.
- **Horizontal Offset:** Move the picture horizontally to the left or right.
- **Vertical Offset:** Move the picture vertically up or down.
- **Reset this Mode:** Select a mode in the window and click on this button to reset that mode's settings to factory default.
- **Reset all Modes:** Click on this button to reset all modes in this window to factory default.
- **Save changes:** Click on this button to save changes permanently.
- **Undo Changes:** Click on this button to restore the previously-saved settings.
- **Refresh Video:** Click on this button to refresh the video using new settings.

- **Soft Keyboard**
  - **Show** – activates the Soft Keyboard; if your host system runs a different language and country mapping than your administration machine, you should activate Soft Keyboard.
  - **Mapping** – select language and country mapping for Soft Keyboard.

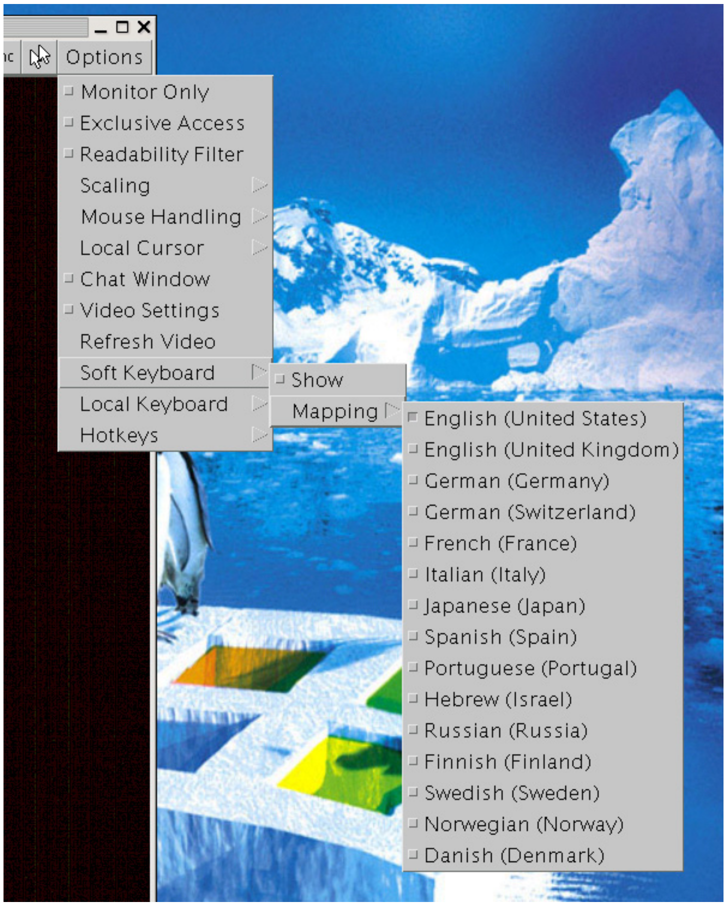
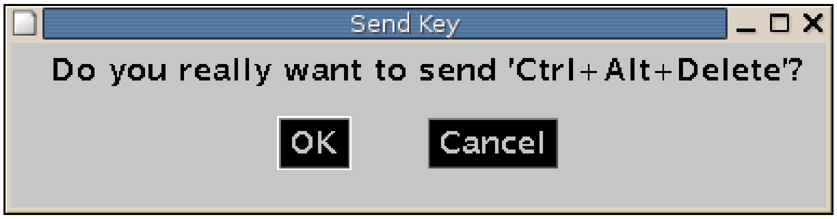


Figure 16 Soft Keyboard Mapping Menu

- **Local Keyboard** – use to change the language mapping of your browser machine that is running Remote Console. Remote Console chooses the correct mapping automatically, but sometimes cannot, depending on the JVM version and your browser settings. For example, is a German localized system that uses a US-English keyboard mapping – in this case, you must change the Local Keyboard setting to the correct language manually.
- **Hot Keys** – launches a list of factory-set default Hot Key commands. Click on an entry to send the command to the host system. A confirmation window appears to confirm the Send. Click **OK** to send the command or click **Cancel** to exit the window without sending.

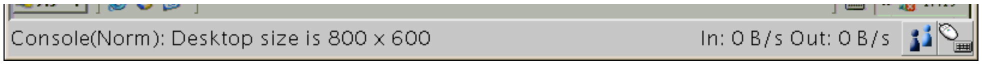

Send Key

Do you really want to send 'Ctrl+Alt+Delete'?

Figure 17 Remote Console Confirmation Dialog

Remote Console Status Bar

The Status Bar shows console and connection state



Console(Norm): Desktop size is 800 x 600

In: 0 B/s Out: 0 B/s

Figure 18 Remote Console Status Bar

Screen Size – Remote screen size appears at the very left of the Status Bar. The value in parentheses indicates the connection to the Remote Console: **Norm:** a standard connection without encryption; **SSL:** a secure connection using SSL.

Network Traffic – On the right of the Status Bar, the incoming (**In**) and outgoing (**Out**) network traffic is displayed in kilobytes per second (B/s). If compressed encoding is enabled, a value in parentheses states displays the compressed transfer rate.

Access State – Icons display Remote Console's access state.

👤	A single user is connected to the Remote Console.
👥	More than one user is connected to the Remote Console.
✗👥	You have exclusive access to Remote Console. No other user can access the remote host via Remote Console unless you disable this option.
👥✗	Another remote user has exclusive access to Remote Console. You cannot access the remote host via Remote Console unless the other user disables this option.

Monitor Only – The icon on the far right of the Status Bar displays Monitor Only settings (for use when you need to view the monitor without using the keyboard or the mouse).

🖱⌨	Monitor Only is disabled.
🚫⌨	Monitor Only is enabled. Please see **Remote Console Control Bar** later in this chapter for additional information.

Remote Management Settings

Remote Control

KVM Console

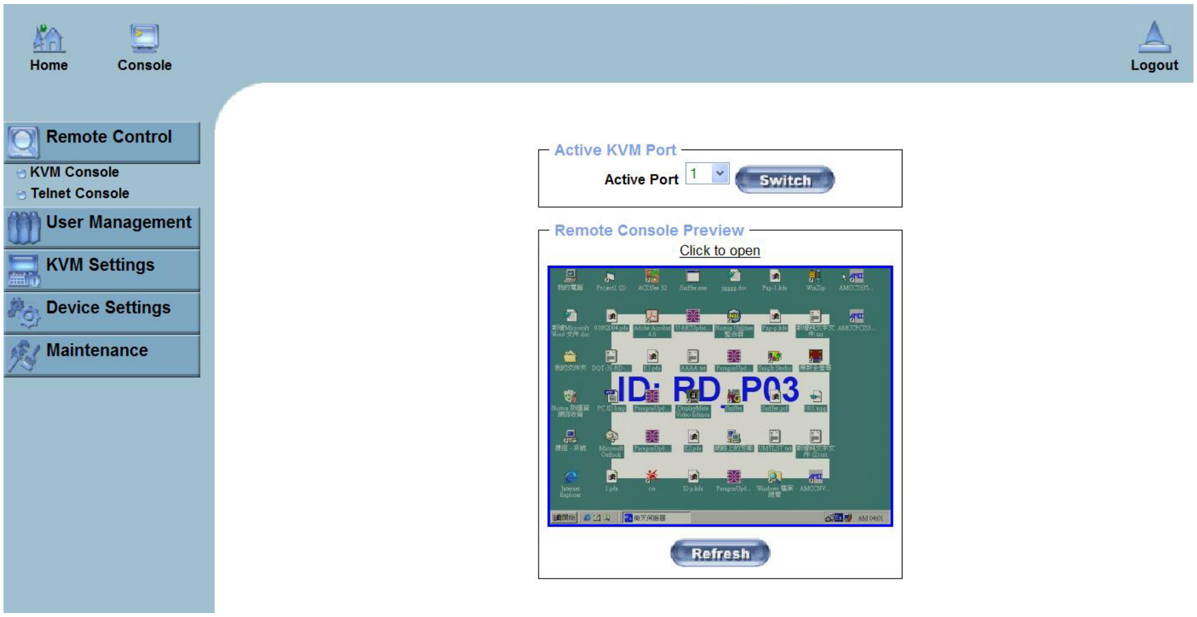
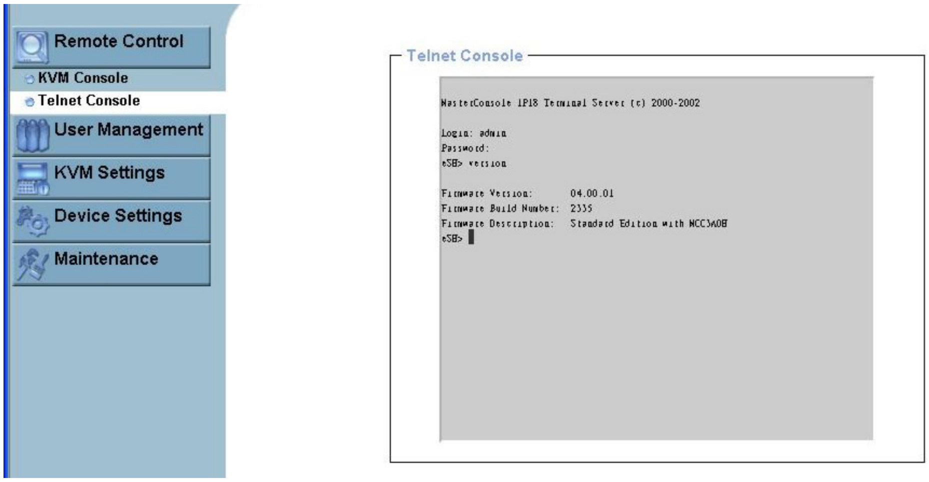


Figure 19 KVM Console Screen

In the **Active KVM Port** panel, click on the drop-down **Active Port** arrow to select the active port. Click **Switch** to change.

In the **Remote Console Preview** panel, click on the **Click to open** link to open the KVM console. Click **Refresh** to refresh the link.

Telnet Console



```
MasterConsole IP18 Terminal Server (c) 2000-2002

Login: admin
Password:
eSB> version

Firmware Version:        04.00.01
Firmware Build Number:   2335
Firmware Description:    Standard Edition with NCC3A0B
eSB> █
```

Figure 20 Telnet Console Screen

MCIP firmware features a Telnet gateway that enables you to connect to MCIP via a standard Telnet client. Use a terminal program such as xterm, TeraTerm or Putty to connect to MCIP.

If you prefer, issue the Telnet command on a command line or by using the **Run** command from the Windows Start Menu. At the command prompt, type the following sequence:

```
telnet 192.168.1.22
```

and replace the IP address given here with the IP address assigned to the MCIP unit. Type the user name and password to log into the device. Once logged into the MCIP, a command line appears and you can issue management commands.

Generally speaking, the Telnet interface supports two operation modes: command line mode and terminal mode. Command line mode is used to control or display parameters, and in terminal mode, the pass-through access to serial port 1 is activated (if serial settings were made accordingly). All input is redirected to the device on serial port #1 and its responses appear in Telnet interface. Type the following commands to view:

Help displays a list of possible commands

Cls clears the screen

Quit exits the current session and disconnects from the client

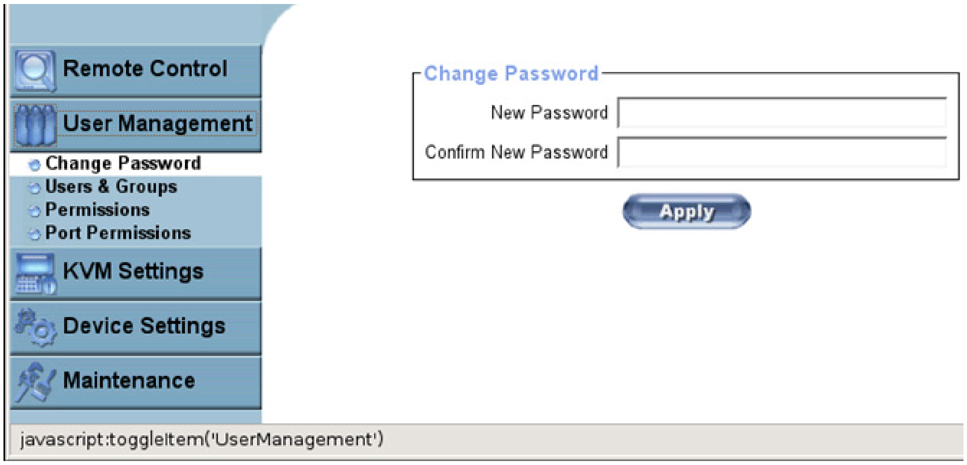
Version displays release information

Terminal starts the terminal pass-through mode for serial port #1.

Pressing the key combination **esc exit** switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for pass-through access.

User Management

Change Password



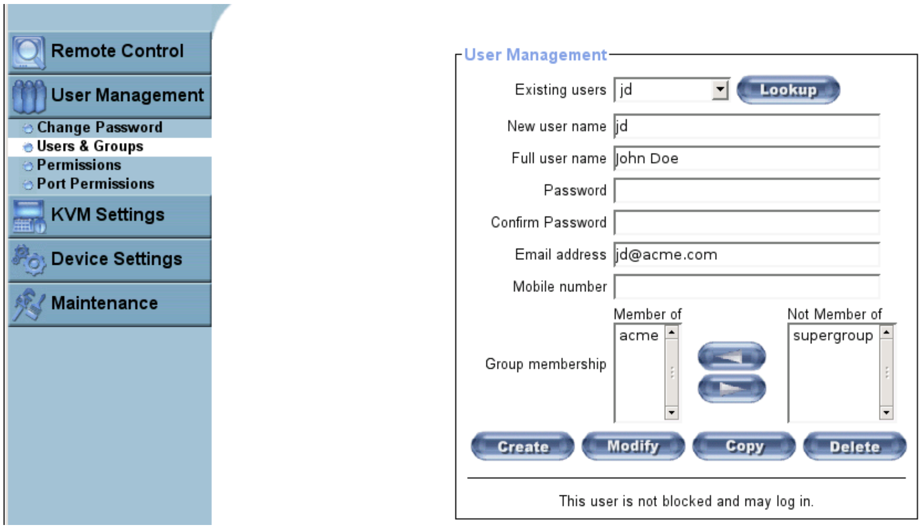
New Password
Confirm New Password

javascript:toggleItem('UserManagement')

Figure 21 Change Password Screen

In the **Change Password** panel, type your new password in the **New Password** field.
Retype the password in the **Confirm New Password** field.
Click **Apply** to change your password.

Users and Groups



Existing users jd
New user name jd
Full user name John Doe
Password
Confirm Password
Email address jd@acme.com
Mobile number
Group membership
Member of: acme
Not Member of: supergroup

This user is not blocked and may log in.

Figure 22 Users & Groups Screen

User and Group management in MCIP is based on configurable users and groups, which may be granted different permissions. Each MCIP unit is pre-configured with a Supervisor User ("super user") called **admin,** which uses the password **raritan**. For security reasons, Raritan recommends you change the super user's password, **raritan**, immediately after you have accessed your MCIP.

The **User Management** panel helps you add, edit, copy, and delete users.

To add new users:

New user name: Type an abbreviation or nickname for the new user.

Full user name: Type the new user's full name.

Password: Type the new user's password (must be at least four characters).

Confirm Password: Retype the password just entered.

Email address: Type the new user's email address (not required).

Mobile number: Type the new user's mobile telephone number (not required).

Group membership: Users can be members of one or more groups. Select entries in the **Member of** or **Not Member of** lists and use the right or left arrow buttons to personalize this user's memberships.

Click **Create** to add the new user.

***Note:** The limit of user profiles is 150. No more than 25 users should be logged into the MCIP unit at one time.*

To edit existing users:

Click on the drop-down **Existing users** arrow and choose a user from the list. Click **Lookup** to view this user's data.

Edit the user's data.

Click **Modify** to update the existing user's data.

To copy an existing user's data for a new user:

Click on the drop-down **Existing users** arrow and choose a user from the list. Click **Lookup** to view this user's data.

Click **Copy** to create a new profile with this user's data.

Change the data fields to personalize this data for the new user.

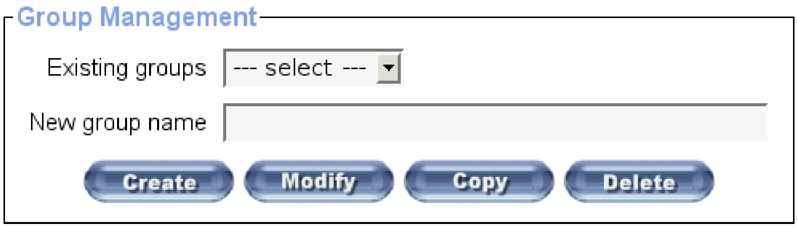
To delete an existing user:

Click on the drop-down **Existing users** arrow and choose a user from the list. Click **Lookup** to view this user's data.

Click **Delete** to delete this user.

***Note:** The super user **admin** can be renamed, but not deleted.*

Group Management



Group Management

Existing groups: --- select ---

New group name:

Figure 23 Group Management Screen

The **Group Management** panel helps you add, edit, copy, and delete groups.

To add a new group:

Type the new group's name in the **New group name** field.

Click **Create**.

To edit an existing group's name:

Click on the drop-down **Existing group** arrow and choose a group from the list.

Click **Modify** to edit the group name.

To delete a group:

Click on the drop-down **Existing group** arrow and choose a group from the list.

Click **Delete** to delete the group.

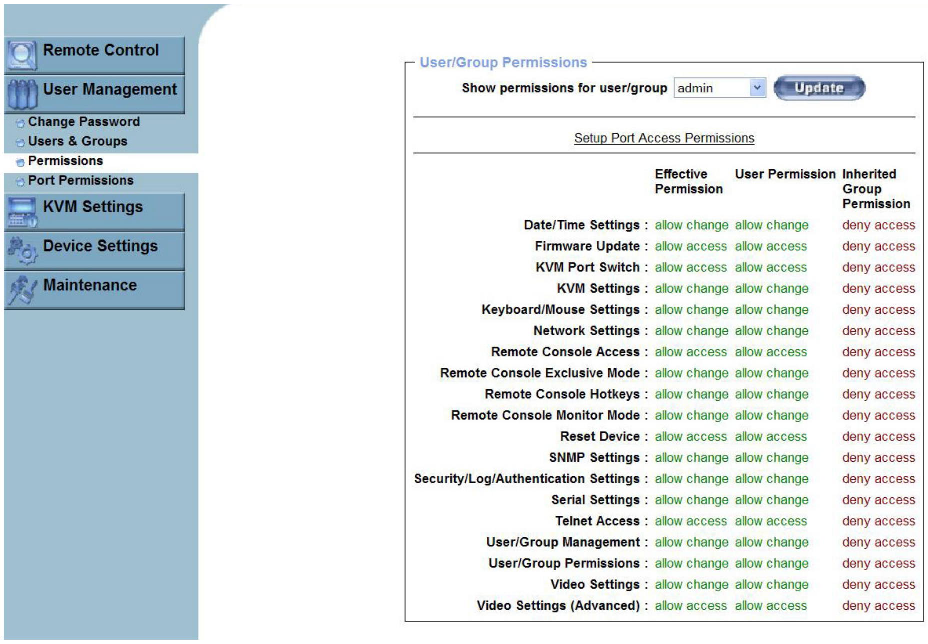
To copy an existing group's data for a new group:

Click on the drop-down **Existing group** arrow and choose a group from the list.

Click **Copy** to create a new group with this group's data.

Change the **New group name** field to personalize this data for the new group. Properties and permissions of the selected group will be copied to the newly created group.

Permissions



User/Group Permissions

Show permissions for user/group: admin

	Effective Permission	User Permission	Inherited Group Permission
Date/Time Settings :	allow change	allow change	deny access
Firmware Update :	allow access	allow access	deny access
KVM Port Switch :	allow access	allow access	deny access
KVM Settings :	allow change	allow change	deny access
Keyboard/Mouse Settings :	allow change	allow change	deny access
Network Settings :	allow change	allow change	deny access
Remote Console Access :	allow access	allow access	deny access
Remote Console Exclusive Mode :	allow change	allow change	deny access
Remote Console Hotkeys :	allow change	allow change	deny access
Remote Console Monitor Mode :	allow change	allow change	deny access
Reset Device :	allow access	allow access	deny access
SNMP Settings :	allow change	allow change	deny access
Security/Log/Authentication Settings :	allow change	allow change	deny access
Serial Settings :	allow change	allow change	deny access
Telnet Access :	allow access	allow access	deny access
User/Group Management :	allow change	allow change	deny access
User/Group Permissions :	allow change	allow change	deny access
Video Settings :	allow change	allow change	deny access
Video Settings (Advanced) :	allow access	allow access	deny access

Figure 24 User/Groups Permission Screen

Use the **User/Group Permissions** panel to change permissions of users and groups.

Each user or group in MCIP is assigned a set of permissions, used to authorize access to certain MCIP functions. By default, the super user **admin** has all permissions (this cannot be changed). New users and groups have no permissions until you set them. However, if a group exists, a user assigned to that group inherits that group's permissions.

There is a parent/child relationship among users and groups, which determines who can change rights. The user who creates another user is the 'parent' of that new user, and therefore has the right to change that user's permissions. In general, a user has the right to change another user's or group's permissions if that user holds a higher (older) position in ancestry. The super user **admin** has rights to change every user and every group permission.

Please note that a user cannot give more permission than that user actually has, for example, if a user does not have permission to change network settings, that user cannot grant the right "change network settings" to another user further down in the ancestry order. However, a user can *reduce* the permissions of descendant users.

To change user or group permissions:

Click on the **Show permissions for user/group** drop-down arrow and choose a user or group from the list. The list displays only users and groups you have rights to change.

Click **Update** to view permissions for the selected user/group. The columns in the list display rights depending on the user/group selected and your permissions to change.

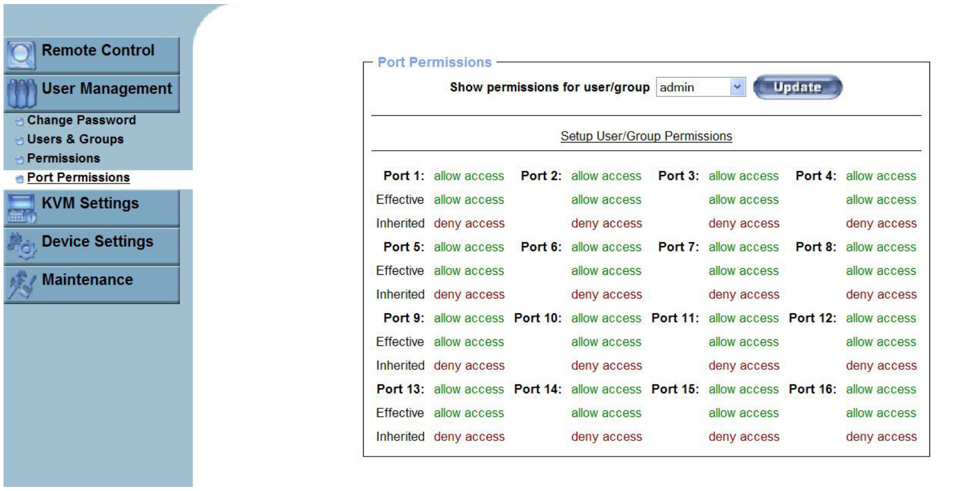
- **Effective Permission:** Permission that determines if a user may access a specific MCIP function.
- **User Permission:** Permission for the currently selected user/group; if the selected user has equal rights to you, you can only view the value; if the selected user has fewer rights, a selection box allows you to change the value.
- **Inherited Group Permission:** Permission value inherited from group(s) to which the selected user belongs (this column does not appear if a group is selected).
  - **deny access** – The selected user cannot use this function.
  - **allow view** – The selected user can view the entry.
  - **deny change** – The selected user cannot change the entry's settings.

- **allow access** – The selected user can use this function.
- **group setting** – No specific permission, uses the permissions inherited from the group(s) to which the user belongs (default: **deny access**).

To change port permissions:

Click on the **<u>Setup Port Access Permissions</u>** link (please see the section **Port Permissions,** that follows, for additional information).

Port Permissions



Port Permissions

Show permissions for user/group: admin

Setup User/Group Permissions

Port 1:	allow access	Port 2:	allow access	Port 3:	allow access	Port 4:	allow access
Effective	allow access		allow access		allow access		allow access
Inherited	deny access		deny access		deny access		deny access
Port 5:	allow access	Port 6:	allow access	Port 7:	allow access	Port 8:	allow access
Effective	allow access		allow access		allow access		allow access
Inherited	deny access		deny access		deny access		deny access
Port 9:	allow access	Port 10:	allow access	Port 11:	allow access	Port 12:	allow access
Effective	allow access		allow access		allow access		allow access
Inherited	deny access		deny access		deny access		deny access
Port 13:	allow access	Port 14:	allow access	Port 15:	allow access	Port 16:	allow access
Effective	allow access		allow access		allow access		allow access
Inherited	deny access		deny access		deny access		deny access

Figure 25 Port Permissions Screen

Use the Port Permission settings to limit viewing of KVM ports. Port permissions function similarly to User/Group permissions (see previous section), in that each user or group in MCIP is assigned permissions that authorize access to certain ports. By default, the super user **admin** has permission to all ports (cannot be changed). New users and groups have no permissions until you set them, and users assigned to a specific group inherit that group's permissions.

Again, there is a parent/child relationship with port access rights; you can change another user's or group's access permissions if you hold higher permissions. The super user **admin** has rights to change all users and every group permissions.

To view access permissions for a certain user or group, click on the **Show permission for user/group** drop-down arrow and choose the user or group from the list.

Click **Update**.

Non-accessible ports are displayed in red font, accessible ports are displayed in green.

Click on the **<u>Setup User/Group Permissions</u>** link to change permissions for the user or group displayed (please see the section Permissions, previously, for additional information).

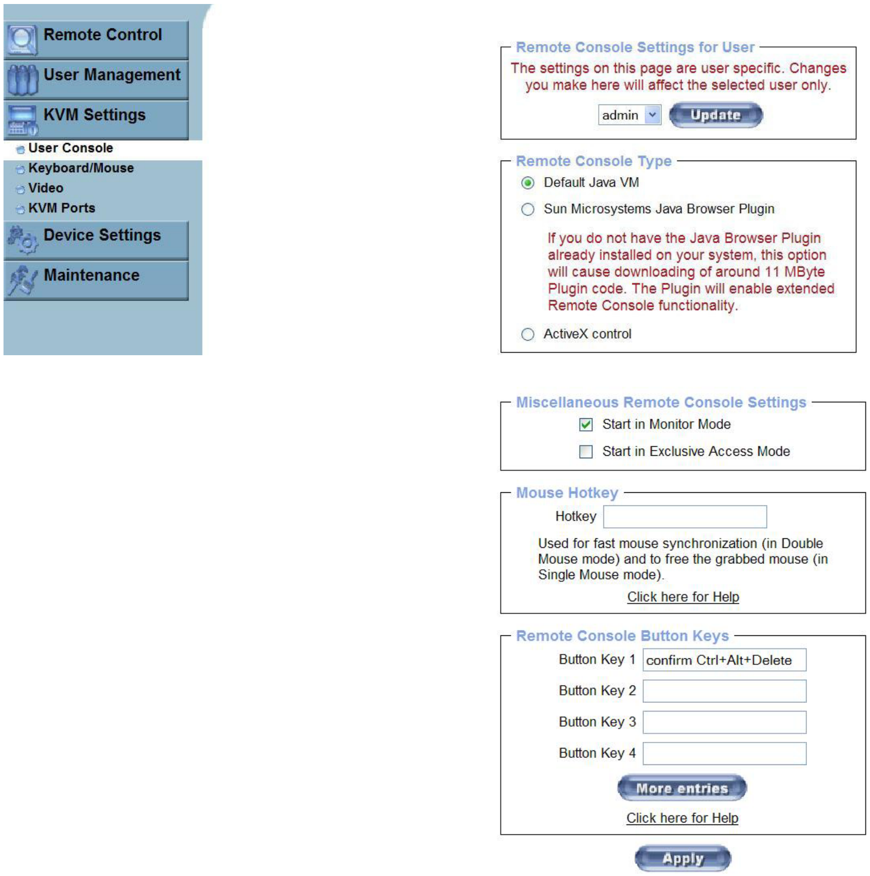
Click **Apply** to apply your changes.

Important: If you do not have permissions to a certain port, you cannot switch to it. If you attempt to switch to a non-accessible port, you will be automatically disconnected.

KVM Settings

User Console

User Console settings are user-specific: a super user can customize these settings for each individual user, and changing settings for one user does not affect settings for any other user.



Remote Console Settings for User

The settings on this page are user specific. Changes you make here will affect the selected user only.

admin

Remote Console Type

● Default Java VM

○ Sun Microsystems Java Browser Plugin

If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.

○ ActiveX control

Miscellaneous Remote Console Settings

☑ Start in Monitor Mode

□ Start in Exclusive Access Mode

Mouse Hotkey

Hotkey

Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).

Click here for Help

Remote Console Button Keys

Button Key 1: confirm Ctrl+Alt+Delete

Button Key 2:

Button Key 3:

Button Key 4:

Click here for Help

Figure 26 User Console Screen

In the **Remote Console Settings for User** panel, click on the drop-down arrow and choose the user whose settings you want to change from the list.

Click **Update**.

Note: *If you do not have the necessary access rights for this task, those of administrator or super user, you cannot change any user's settings.*

In the **Remote Console Type** panel, click on the radio button before the Remote Console Viewer to use:

- **Default Java VM (Virtual Machine):** This option uses the default JVM in your web browser; it can be Microsoft JVM for Internet Explorer or Sun JVM, if configured this way (use of the Sun JVM may also be forced, see below).
- **Sun Microsystems Java Browser Plugin:** This option instructs your system's web browser to use the Sun JVM. If you select this option and the appropriate Java plug-in is not yet installed on your system, it can be downloaded and installed automatically with an installation wizard (download volume is 11 Mbytes).
- **ActiveX control:** This option instructs the web browser to use the KVM Vision Viewer (an application available separately) ActiveX-control. This option works only with Microsoft Internet Explorer on Win32 Systems. Please contact Raritan for more information.

Note: In order for "ActiveX control" option to work, KVM Vision Viewer needs to be installed for using KVM Remote Access with MCIP.

In the **Miscellaneous Remote Console Settings** panel, click on the checkbox before **Start in Monitor Mode** to set the initial value for monitor mode. By default, monitor mode is disabled. If you enable it, the Remote Console window will be started in a read-only mode.

Click on the checkbox before **Start in Exclusive Access Mode** to enable exclusive access mode immediately upon Remote Console startup. This will log off any other users on Remote Console at that time. No other user can access Remote Console while you have this feature enabled.

In the **Mouse Hot Key** panel, you can specify a Hot Key combination to start the mouse synchronization process (when used in Remote Console) or to leave single mouse mode.

In the **Remote Console Button Keys** panel, specify keystrokes or key combinations for use on the remote system that cannot be generated locally. If the local system is operating with a different keyboard, a necessary key might be missing, or if the local system is unconditionally catching this keystroke already, you can assign a shortcut button to a keystroke command. Typical examples include [**CTRL+ALT+DELETE**] on Windows and DOS, or [**CTRL+BACKSPACE**] on Linux.

The syntax to define a new Button Key:

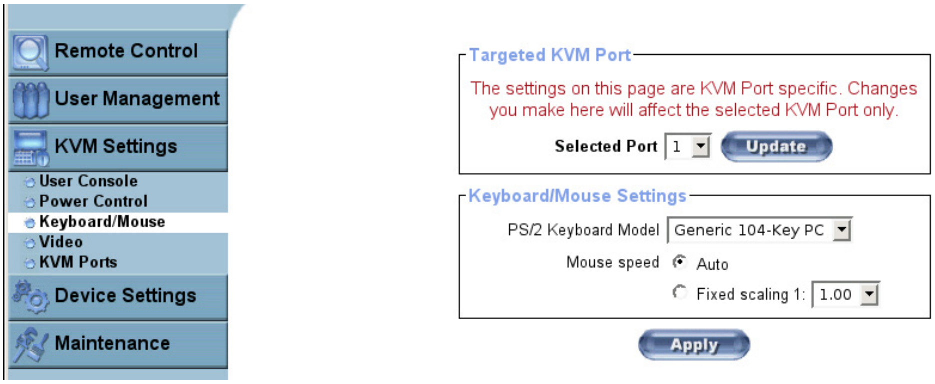
[confirm] <keycode>[+|-[*]<keycode>]*

confirm requests confirmation via dialog box before the key strokes are sent to the remote host.

keycode is the key to be sent to the remote host. Multiple key codes can be concatenated with a plus or minus sign: the plus sign builds key combinations, and all keys will be pressed until a minus sign or the end of the combination. In this case, all pressed keys will be released in reversed sequence. The minus sign builds single, separate key presses and key releases. The asterisk inserts a 100 millisecond pause between strokes. Please see the appendices for key codes and aliases recognized by MCIP.

If you require additional button keys, click **More entries** for additional entry fields. Click on the **Click here for Help** link for more on-line assistance when entering Button Keys.

Keyboard/Mouse



Targeted KVM Port

The settings on this page are KVM Port specific. Changes you make here will affect the selected KVM Port only.

Selected Port: 1

Keyboard/Mouse Settings

PS/2 Keyboard Model: Generic 104-Key PC

Mouse speed: ● Auto

○ Fixed scaling 1: 1.00

Figure 27 Keyboard/Mouse Settings Screen

In the **Targeted KVM Port** panel, click on the **Selected Port** drop-down arrow and choose the desired port from the list.

Click **Update** to select the port.

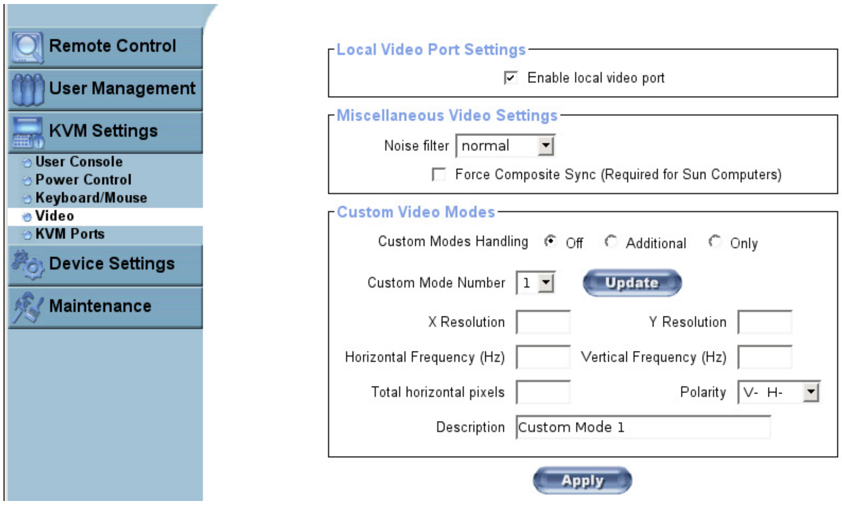
In the **Keyboard/Mouse Settings panel**, click on the **PS/2 Keyboard Model** drop-down arrow and choose a keyboard layout from the list. Generic 101-Key PC indicates a standard keyboard layout, Generic 104-Key PC indicates a standard keyboard layout extended by three additional Windows keys, Generic 106-Key PC indicates a Japanese keyboard, and Apple Macintosh indicates the Apple Macintosh keyboard.

Click on one of the **Mouse Speed** radio buttons to choose your mouse speed.

- **Auto:** Select **Auto** if the host system's mouse settings use an additional acceleration setting. MCIP tries to detect the acceleration and speed of the mouse during the mouse sync process.
- **Fixed scaling:** Select **Fixed scaling** and click on the drop-down arrow to choose a direct translation of mouse movements between the local and the remote pointer. You can also set a fixed scaling that dictates how much the remote mouse pointer moves when the local mouse pointer is moved one pixel. This option works only when the mouse settings on the host are linear, that is, if there is no mouse acceleration involved.

Click **Apply** to apply your changes.

Video



Local Video Port Settings

☑ Enable local video port

Miscellaneous Video Settings

Noise filter: normal

□ Force Composite Sync (Required for Sun Computers)

Custom Video Modes

Custom Modes Handling ● Off ○ Additional ○ Only

Custom Mode Number: 1

X Resolution: Y Resolution:

Horizontal Frequency (Hz): Vertical Frequency (Hz):

Total horizontal pixels: Polarity: V- H-

Description: Custom Mode 1

Figure 28Video Settings Screen

In the **Local Video Port Settings** panel, click on the **Enable local video port** checkbox to indicate if the local video output of the MCIP is active and passing through the incoming signal from the host system.

In the **Miscellaneous Video Settings** panel, click on the **Noise filter** drop-down arrow and select an option from the list. The Noise filter you select defines how MCIP reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). The default setting is Normal, which is suitable for most situations.

Click on the **Force Composite Sync (Required for Sun Computers)** checkbox to support signal transmission from a Sun machine. If this box is not checked, the picture of the remote console will not be visible.

In the **Custom Video Modes** panel, you can add video modes to the MCIP that are not recognized using the factory settings. This can be useful when using special mode lines in an X-Window configuration on the host or with uncommon hosts or operating systems.

Important: Please note that this panel should be filled in only by users with advanced video knowledge. Changing factory defaults on the MCIP unit can adversely affect correct video transmission.

Click on one of the **Custom Modes Handling** radio buttons. **Off** disables custom modes, **Additional** adds modes in addition to the standard video resolutions, and **Only** indicates exclusive modes. If you select **Only,** you can force a special video mode for the MCIP.

Click on the **Custom Mode Number** drop-down arrow and choose a number from the list. The maximum number of custom video resolutions is four (**4**).

Click **Update** to adjust the number of custom modes.

Fill in the fields to change parameters for the selected video mode:

X Resolution: Visible number of horizontal pixels.

Y Resolution: Visible number of vertical pixels.

Horizontal Frequency (Hz): The horizontal (line) frequency in Hz.

Vertical Frequency (Hz): The vertical (refresh) frequency in Hz.

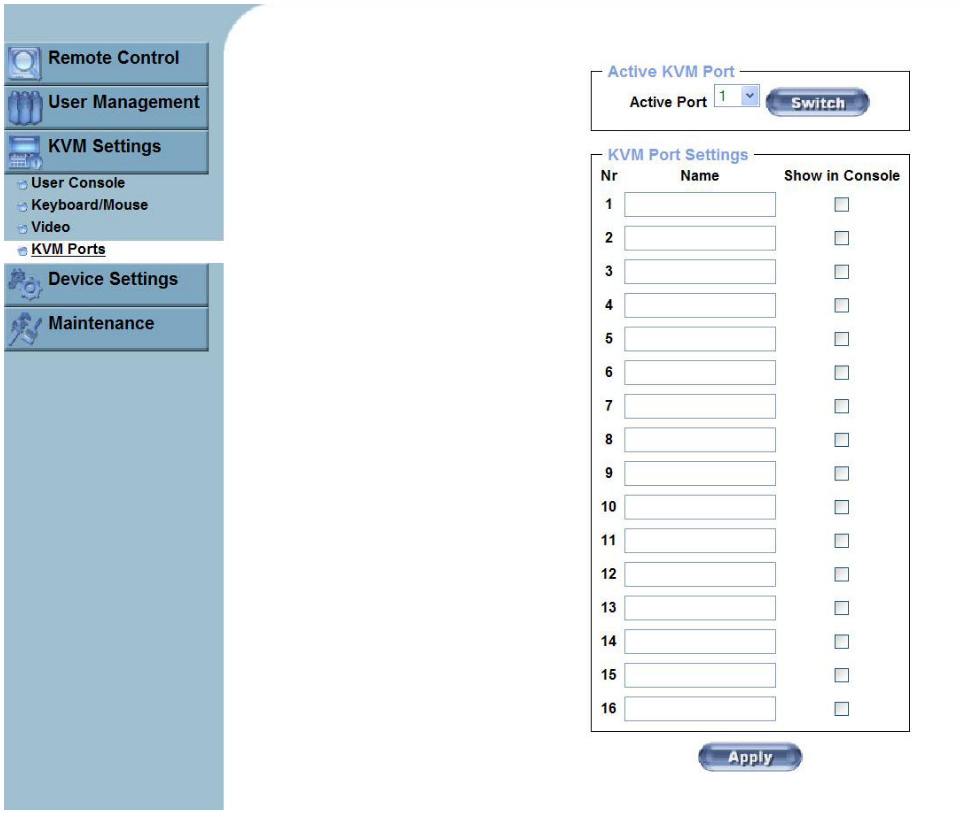
Total horizontal pixels: The total amount of pixels per line, including the non-visible and blanking area.

Polarity: The polarity (positive/negative) of the synchronization signals (V is vertical, H is horizontal).

Description: Provide a mode name that will appear in the Remote Console when this custom mode is activated.

Click **Apply** to apply your changes.

KVM Ports



Active KVM Port

Active Port 1

KVM Port Settings

Nr	Name	Show in Console
1		☐
2		☐
3		☐
4		☐
5		☐
6		☐
7		☐
8		☐
9		☐
10		☐
11		☐
12		☐
13		☐
14		☐
15		☐
16		☐

Figure 29 KVM Port Settings Screen

In the **Active KVM Port** panel, click on the Active Port drop-down arrow and choose a KVM port from the list.

Click **Switch** to activate the KVM port.

In the **KVM Port Settings** panel, specify the settings for each port.

Nr: The number of the port.

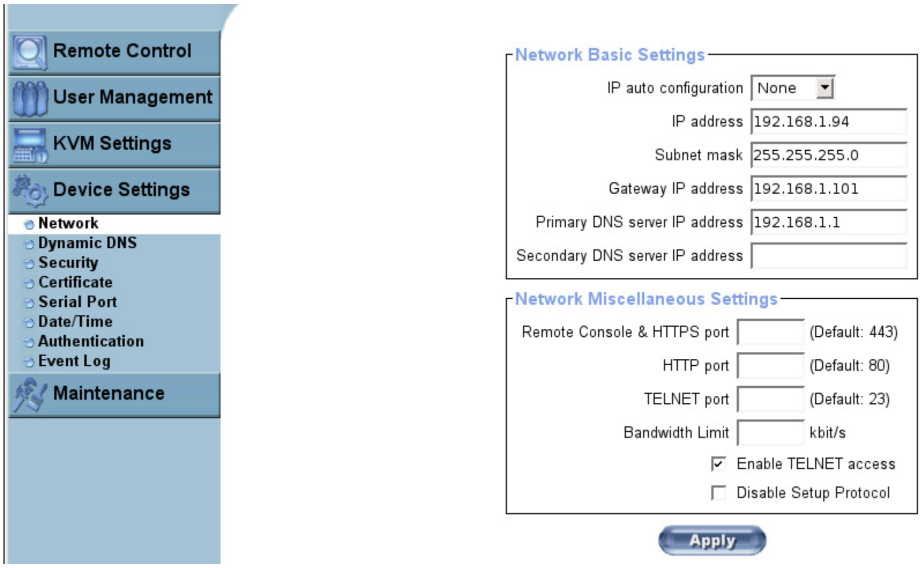
Name: The name or a description of the computer/network that is accessible using this port.

Show in Console: If checked, the port name, above, will be visible in the Remote Console.

Click **Apply** to apply your changes.

Device Settings

Network



Network Basic Settings

IP auto configuration	None
IP address	192.168.1.94
Subnet mask	255.255.255.0
Gateway IP address	192.168.1.101
Primary DNS server IP address	192.168.1.1
Secondary DNS server IP address	

Network Miscellaneous Settings

Remote Console & HTTPS port		(Default: 443)
HTTP port		(Default: 80)
TELNET port		(Default: 23)
Bandwidth Limit		kbit/s

☑ Enable TELNET access

☐ Disable Setup Protocol

Figure 30 Network Settings Screen

Network settings allow you to change network-related parameters. Changes are applied immediately. The initial IP configuration in the Network Basic Settings panel is usually completed directly on the host system using the Initial Configuration settings in the table at the beginning of this chapter. Changing the MCIP network settings could result in breaking your connection. If you change settings remotely, ensure that all the values are correct so that you can still access MCIP.

In the **Network Basic Settings** panel, click on the **IP auto configuration** drop-down arrow and choose how MCIP retrieves its network settings from a DHCP or BOOTP server. If you choose **none,** IP auto configuration is disabled.

Type the IP address in the **IP address** field.

Type the net mask of the local network in the **Subnet Mask** field.

If you want the MCIP unit to be accessible from networks other than local, type the local network router IP address in the **Gateway IP address** field.

Type the IP address of the primary Domain Name Server in the **Primary DNS Server IP Address** field. This field is optional, but MCIP will not be able to perform name resolution if you do not supply an address.

Type the IP address of the secondary Domain Name Server in the **Secondary DNS Server IP Address** field. It will be used if the Primary DNS Server cannot be contacted.

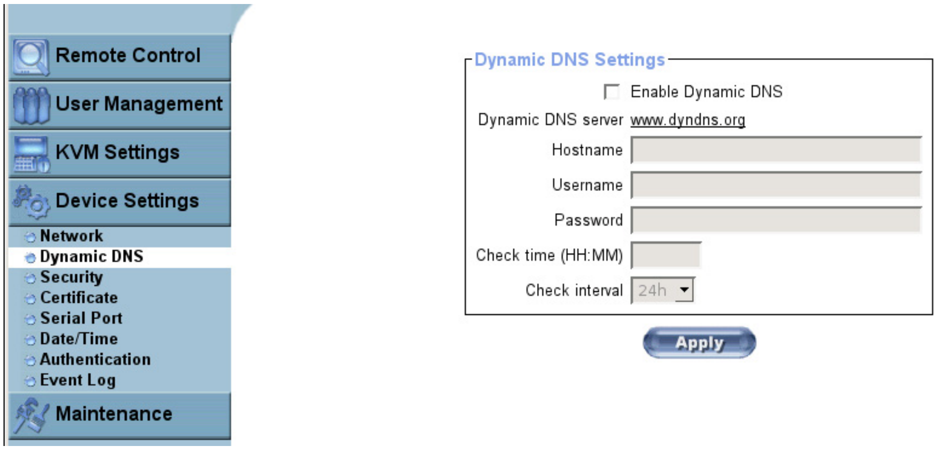
In the **Network Miscellaneous Settings** panel, fill in the **Remote Console & HTTPS port, HTTP port,** and **TELNET port.** If these fields are left empty, the default port will be used.

Type the maximum network traffic generated through the MCIP Ethernet device value in Kbit/second in the **Bandwidth Limit** field.

Click on the checkbox before **Enable Telnet access** to allow access to MCIP using the Telnet gateway.

Clear the checkbox before **Disable Setup Protocol** to exclude MCIP from the setup protocol.

Dynamic DNS



Dynamic DNS Settings

□ Enable Dynamic DNS

Dynamic DNS server www.dyndns.org

Check interval 24h

Figure 31 Dynamic DNS Settings Screen

MCIP is accessible via the DSL router that that is dynamically assigned by the provider. Because an administrator may not know the IP address assigned by the provider, MCIP connects to a special dynamic DNS server, where it registers its IP address. As an administrator, you may contact this server and pick up the same IP address. You must register an MCIP unit to work with the Dynamic DNS Server and assign it a specific hostname. You will get user name (or nick-name) and a password to continue registration. This information, along with the hostname, is required to determine the IP address of the registered MCIP.

To enable Dynamic DNS:

- Ensure that the MCIP unit's LAN interface is properly configured.
- Enter all Dynamic DNS Settings as described below.
- Enable Dynamic DNS.

In the **Dynamic DNS Settings** panel, click on the checkbox before **Enable Dynamic DNS** (please remember that you must have a configured DNS server IP address).

The **Dynamic DNS server** is the server with which MCIP registers itself at regular intervals. The default setting **dyndns.org** is supported currently.

Type the hostname of the MCIP that is provided by the Dynamic DNS Server in the **Hostname** field. Use the entire name including the domain, for example, testserver.dyndns.org, not just the actual hostname.

Type the registered username you used during your manual registration with the Dynamic DNS Server in the **Username** field. Spaces are not permitted.

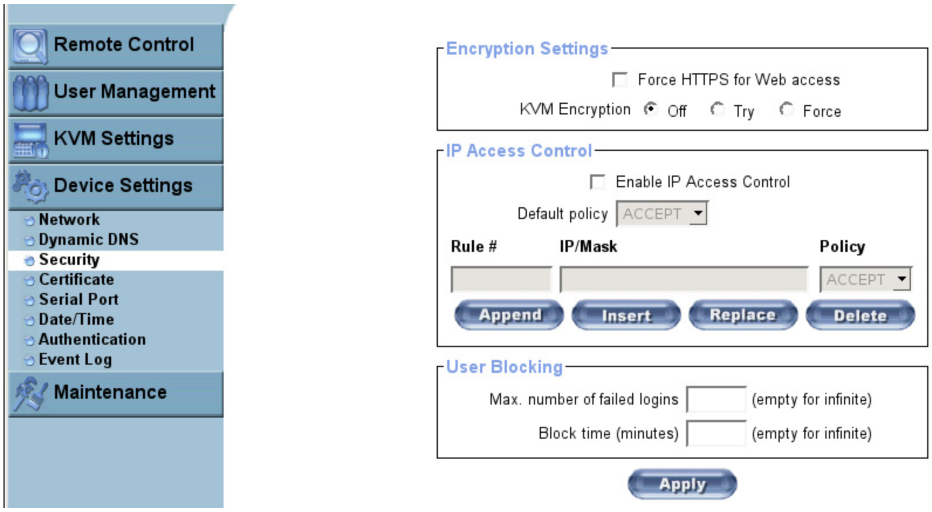
Type the password you used during your manual registration with the Dynamic DNS Server in the **Password** field.

Type the time in HH:MM format at which the MCIP card registers itself with the Dynamic DNS server in the **Check time** field (please use military time format, or the 24-hour clock; for example, type 8:30 a.m. as 0830; type 6:45 p.m. as 18:45).

Click on the **Check interval** drop-down arrow to choose the frequency for MCIP to report to the Dynamic DNS server.

Note: *MCIP has an internal independent real-time clock. Ensure that the MCIP unit's time setting is correct by configuring a time server (please see the section Date and Time for additional information)*

Security



Encryption Settings

□ Force HTTPS for Web access

KVM Encryption ● Off ○ Try ○ Force

IP Access Control

□ Enable IP Access Control

Default policy ACCEPT

Rule #	IP/Mask	Policy
		ACCEPT

User Blocking

Max. number of failed logins (empty for infinite)

Block time (minutes) (empty for infinite)

Figure 32 Security Settings Screen

In the **Encryption Settings** panel, click on the checkbox before **Force HTTPS for Web access** to enable access to the Web front-end only if using an HTTPS connection. If enabled, MCIP will not check the HTTP port for incoming connections.

Please see the section **Certificate,** later in this chapter, for additional information on creating your own SSL certificate for identifying MCIP.

Click on one of the **KVM encryption** radio buttons to control the encryption of the RFB protocol. Remote Console uses the RFB (remote framebuffer) protocol to transmit screen data to the administrator machine and transmit keyboard and mouse data back to the host.

- **Off:** No encryption will be used.
- **Try:** The applet will attempt an encrypted connection. If the connection fails, it will attempt an unencrypted connection.
- **Force:** The applet will attempt an encrypted connection. If connection fails, an error message appears.

In the **IP Access Control** panel, set settings related to IP access control used to limit the access to specific clients. These clients are identified by their IP addresses. The IP access control settings apply only to the LAN interface only.

Click on the checkbox before **Enable IP Access Control** to enables access control based on IP source addresses.

Click on the **Default policy** drop-down arrow and choose to **ACCEPT** or **DROP** incoming IP packets that do not match any configured rules.

Click on the **Policy** drop-down arrow to indicate what to do with matching packets; choose **ACCEPT** or **DROP**.

Rule #: Assign a number to the rule you are configuring. When appending a new rule, this field is ignored.

IP/Mask: Type the IP address or address range to which this rule applies.

Examples:

Typing **192.168.1.22/32** matches the IP Address 192.168.1.22

Typing **192.168.1.0/24** matches all IP packets with source addresses from 192.168.1.0 to 192.168.1.255

Typing **0.0.0.0/0** matches any IP packet

To edit a rule:

Type the Rule #.

Click **Append**.

Edit the IP/Mask or Policy as needed.

Click **Apply.**

To add a new rule:

Type a Rule #, an IP/Mask, and select the Policy.

Click **Insert**.

To replace a rule:

Type the Rule #, the IP/Mask and set the policy.

Click **Replace.**

To delete a rule:

Type the Rule #.

Click **Delete.**

Important: If you set Default policy to DROP and have no ACCEPT rules configured, access to the Web front-end via LAN is completely disabled. To enable access, change security settings via modem or by temporarily disabling IP access control with the initial configuration procedure (as listed in the table at the beginning of this chapter).

Note: *The order of rules is important. Rules are checked in ascending order until a rule matches, and all rules below the matching one are ignored. The Default policy applies if no matching rule is located.*

In the **User Blocking** panel, set a blocking mechanism that allows you to block certain users after a certain number of failed logins, that is, if they use incorrect user names or passwords, and set the duration of the block.

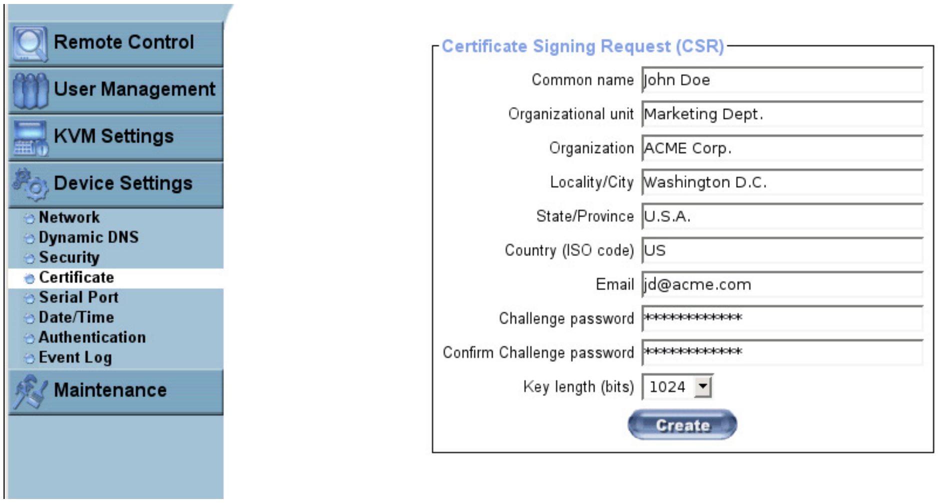
Type the number of attempts a user can make in the **Maximum number of failed logins** field. Leave this field empty to disable the user blocking feature.

Type the time (in minutes) the user is blocked after exceeding the maximum number of failed login attempts in the **Block time (minutes)** field. Leave this field empty to block a user for an infinite amount of time (or until the user is manually unblocked).

To unblock users:

- A parent user can access the User Management settings for this user and click Unblock (please see the section **User Management**, earlier in this chapter).
- Use the serial console (as used for the initial configuration – see table at the start of this chapter) and log on as the user **unblock**. Enter the super user password and unblock the user when MCIP displays a list of blocked users.

Certificate



Certificate Signing Request (CSR)

Common name	John Doe
Organizational unit	Marketing Dept.
Organization	ACME Corp.
Locality/City	Washington D.C.
State/Province	U.S.A.
Country (ISO code)	US
Email	jd@acme.com
Challenge password	************
Confirm Challenge password	************
Key length (bits)	1024

Figure 33 Certificate Settings Screen

MCIP uses the Secure Socket Layer (SSL) protocol for encrypted network traffic between itself and connected clients. While establishing the connection, MCIP exposes its identity to the client using a cryptographic certificate. Upon delivery, this certificate and underlying secret key will not match the network configuration applied to MCIP by its user. The certificate's underlying secret key is also used for securing the SSL handshake. This is a security risk, but you can generate and install a new base 64 x.509 certificate unique for your particular MCIP.

To do so, command MCIP to generate a new cryptographic key and associated Certificate Signing Request (CSR) to be certified by a certification authority (CA). A certification authority verifies your (your system's) identity and issues you a SSL certificate. To create and install an SSL certificate for the MCIP, please follow the steps outlined below.

In the **Certificate Signing Request** panel, fill in the data indicated.

Type the MCIP unit's network name (once installed in your network) in the **Common name** field. This is usually the FQDN (fully qualified domain name), and is identical to the name used to access MCIP with a web browser (without the http:// prefix). If the name here and the actual network name differ, the browser will pop up a security warning when the MCIP is accessed using HTTPS.

Type the department to which MCIP belongs in the **Organizational unit** field.

Type the name of the organization (company) to which the MCIP belongs in the **Organization** field.

Type the city in which the organization is located in the **Locality/City** field.

Type the state or province in which the organization is located in the **State/Province** field.

Type the country in which the organization is located in the **Country (ISO code)** field. Use the two-letter ISO code, for example, US for the U.S. or DE for Germany.

Some certification authorities require a challenge password to authorize later changes on the certificate. Type a password of at least four characters in the **Challenge password** field.

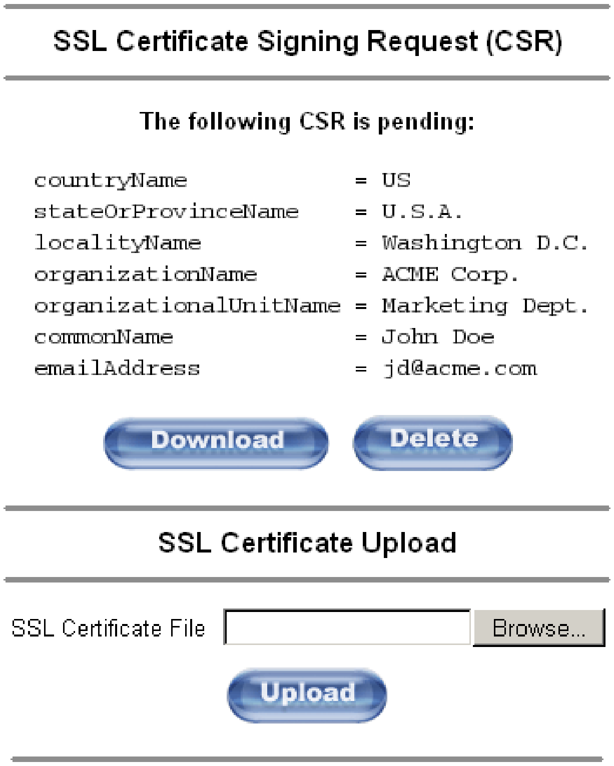
Retype the challenge password in the **Confirm Challenge password** field for confirmation.

Type a contact person's email address in the **Email** field. The contact person is a person responsible for the MCIP and its security.

Click on the **Key length** drop-down arrow and choose the length of the generated key (in bits). A key length of 1024 Bits should suffice in most cases; longer keys can result in slower response time during connection establishment.

Click **Create.**

When the **SSL Certificate Signing Request** screen appears, click **Download.**



SSL Certificate Signing Request (CSR)

The following CSR is pending:

```
countryName                = US
stateOrProvinceName        = U.S.A.
localityName               = Washington D.C.
organizationName           = ACME Corp.
organizationalUnitName     = Marketing Dept.
commonName                 = John Doe
emailAddress               = jd@acme.com
```

SSL Certificate Upload

SSL Certificate File

Figure 34 SSL Certificate Signing Request Screen

Send the saved CSR to a CA for certification. You must follow an authentication process according to the CA you select.

When you receive the SSL Certificate file from the CA, save it on your system.

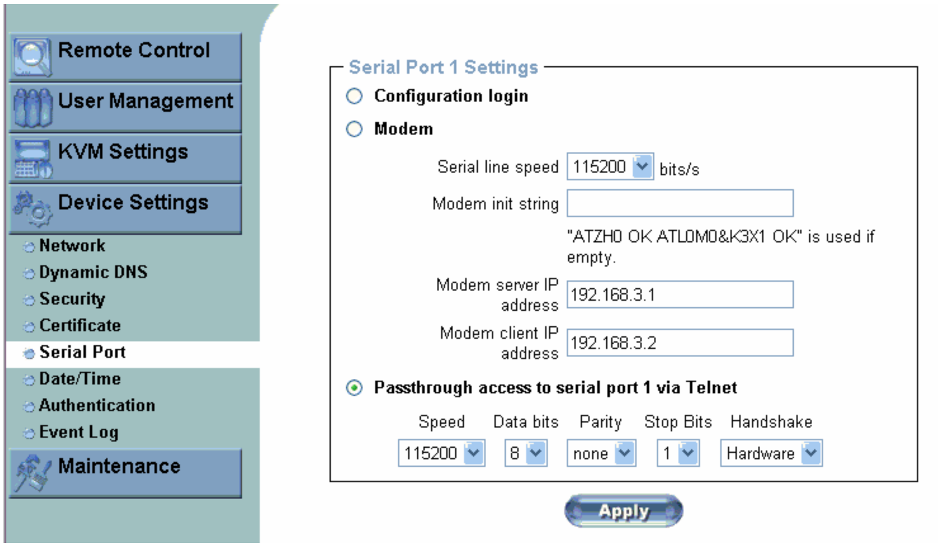
Return the **SSL Certificate Signing Request** screen and click **Browse** to locate the SSL Certificate file that you just saved on your system.

Click **Upload.**

Note: *If you delete the CSR on your system, there is no way to retrieve it, and you must repeat this process.*

Once you have completed this process, your MCIP has its own certificate that it will use for identification with connecting clients.

Serial Port



Serial Port 1 Settings

○ Configuration login

○ Modem

Serial line speed 115200 bits/s

Modem init string

"ATZH0 OK ATL0M0&K3X1 OK" is used if empty.

Modem server IP address 192.168.3.1

Modem client IP address 192.168.3.2

● Passthrough access to serial port 1 via Telnet

Speed	Data bits	Parity	Stop Bits	Handshake
115200	8	none	1	Hardware

Figure 35 Serial Port Settings Screen

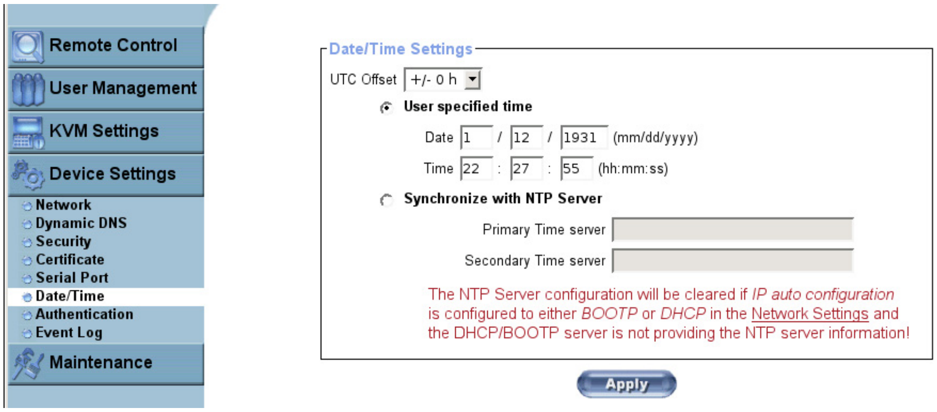
Use the Serial Port settings screen to specify the device connected to the serial port and how to use it.

In the **Serial Port 1 Settings** panel, click on the radio button before the option that best fits the connected device.

- **Configuration login:** Do not use the serial port for any special function, use it only for the initial configuration.
- **Modem:** The MCIP offers remote access using a telephone line, in addition to the standard access over the built-in Ethernet adapter. The modem must be connected to the MCIP unit's serial interface. Connecting to MCIP via telephone means building up a dedicated point-to-point connection from your console computer to the MCIP. In other words, the MCIP acts as an Internet Service Provider (ISP) into which you can dial. The connection is established using Point-to-Point Protocol (PPP). Before connecting to the MCIP unit, ensure you have configured your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection which defaults to the right settings like PPP.
  - **Serial line speed:** The speed with which the MCIP is communicating with the modem. Most of all modems available today will support the default value of 115.200 bps. In case you are using an old modem and discovering problems try to lower this speed.
  - **Modem init string:** The initialization string used by the MCIP to initialize the modem. The de- fault value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.
  - **Modem server IP address:** This IP address will be assigned to the MCIP itself during the PPP hand- shake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP set- tings of the MCIP and your console computer. The default value will work in most cases.
  - **Modem client IP address:** This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure that it is not interfering with the IP settings of the MCIP and your console computer. The default value will work in most cases.

- **Passthrough access to serial port 1 via Telnet:** Select this option to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port from the drop-down menus and use the Telnet Console or a standard Telnet client to connect to the MCIP.

Date and Time



Date/Time Settings

UTC Offset +/- 0 h

● User specified time

Date 1 / 12 / 1931 (mm/dd/yyyy)

Time 22 : 27 : 55 (hh:mm:ss)

○ Synchronize with NTP Server

Primary Time server

Secondary Time server

The NTP Server configuration will be cleared if *IP auto configuration* is configured to either *BOOTP* or *DHCP* in the Network Settings and the DHCP/BOOTP server is not providing the NTP server information!

Figure 36 Date/Time Settings Screen

Use this screen to set up the MCIP unit's internal clock. You can choose to adjust the clock manually or use an automated NTP time server.

Click on the radio button before your preference.

User specified time: Type the date in mm/dd/yy format and the time in hh:mm:ss format (please use military time format, or the 24-hour clock: for example, type 8:30 a.m. as 0830; type 6:45 p.m. as 18:45).

Click **Apply.**

Note: *If you choose to adjust the time yourself, you may have to readjust time if the MCIP ever loses power for more than a few minutes.*

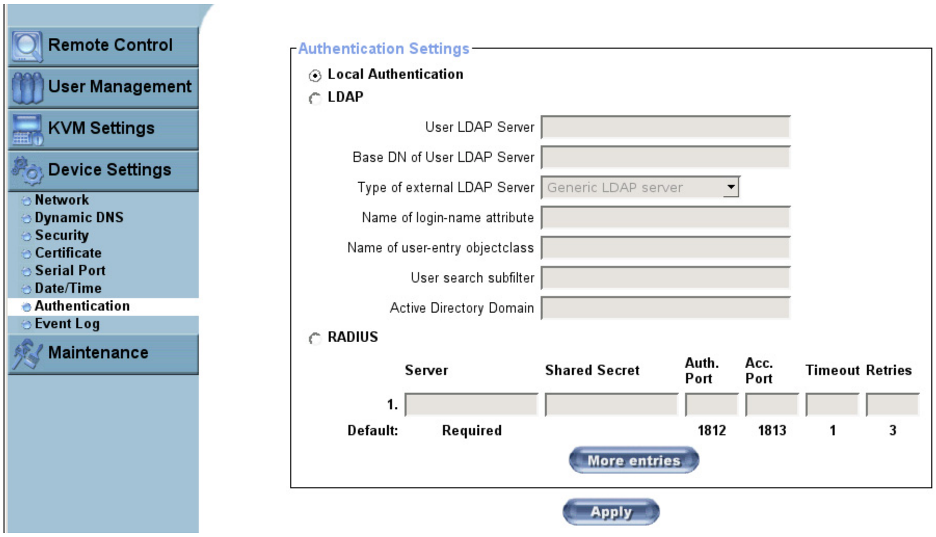
Synchronize with NTP Server: Type the address of a server to synchronize the internal clock automatically to the current UTC time in the **Primary Time** server field.

Click **Apply.**

Click on the **UTC Offset** drop-down arrow to advance or delay your timing for any reason.

Note: *There is currently no way to adjust the daylight saving time automatically; manually adjust the* ***UTC offset*** *twice a year to adhere to the daylight savings rules of your country.*

Authentication



Authentication Settings

● Local Authentication

○ LDAP

User LDAP Server

Base DN of User LDAP Server

Type of external LDAP Server: Generic LDAP server

Name of login-name attribute

Name of user-entry objectclass

User search subfilter

Active Directory Domain

○ RADIUS

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.						
Default:	Required		1812	1813	1	3

Figure 37 Authentication Settings

You can use local authentication with MCIP, or store information in a central LDAP directory or in a RADIUS server. If using LDAP or RADIUS, specify Authentication information here.

LDAP:

Type the name or IP address of the LDAP server containing all the user entries in the **User LDAP Server** field. If you use a name, you must configure a DNS server in the network settings.

Type the distinguished name (DN) where the directory tree starts in the user LDAP server in the **Base DN of User LDAP Server** field.

Click on the **Type of external LDAP Server** drop-down arrow and choose the type of external LDAP server. This is necessary, as some server types require special handling, and the default values for the LDAP scheme are set appropriately. Choose **Generic LDAP Server**, **Novell Directory Service,** and **Microsoft Active Directory**. If you have neither a Novell Directory Service nor a Microsoft Active Directory, choose **Generic LDAP Server** and edit the LDAP scheme (see below).

Type the name of the attribute containing the unique login name of a user in the **Name of login-name attribute** field. Leave this field empty to use the default value (the default depends on the selected LDAP server type).

Type the object class that identifies a user in the LDAP directory in the **Name of user-entry object class** field. Leave this field empty to use the default value (the default depends on the selected LDAP server type).

Type a subfilter to refine the search for users known to the MCIP in the **User search subfilter** field.

Type the active directory domain configured in the Microsoft Active Directory server in the **Active Directory Domain** field. This option is valid only if you have chosen Microsoft Active Directory as the LDAP server type.

RADIUS (Remote Authentication Dial In User Service):

RADIUS is a protocol specified by the Internet Engineering Task Force (IETF) working group. There are two specifications that make up the RADIUS protocol suite: Authentication and Accounting. These specifications aim to centralize authentication, configuration, and accounting for dial-in services to an independent server. The RADIUS protocol exists in several implementations, such as freeRADIUS, open-RADIUS, or RADIUS on UNIX systems. The

RADIUS protocol itself is well specified and tested. Currently, Raritan does not support challenge/response. An Access Challenge response is seen and evaluated as an Access Reject.

To access a remote device using the RADIUS protocol you must first log on, then specify your username and password. The RADIUS server reads your input data (Authentication) and the MCIP looks for your profile (Authorization). The profile defines (or limits) your actions. If the server finds no profile matching your username and password, your access via RADIUS is refused. In terms of the remote activity mechanism, login via RADIUS works similar to the Remote Console. If there is no activity for half an hour your connection to the MCIP will be interrupted and closed.

Type either the IP address or the hostname of the RADIUS Server to be connected in the **Server** field. If you use a name, you must configure a DNS server in the network settings.

Type a text string that serves as a password between the RADIUS client and RADIUS server in the **Shared Secret** field. In this case the MCIP serves as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify message integrity. Use any standard alphanumeric and special characters, up to 128 characters in length containing upper- and lowercase letters and symbols.

Note: Shared Secrets serve as the values for RADIUS server and MCIP to communicate with each other during authentication.

Type the port to which the RADIUS server listens for authentication requests in the **Authentication Port** field (default: 1812).

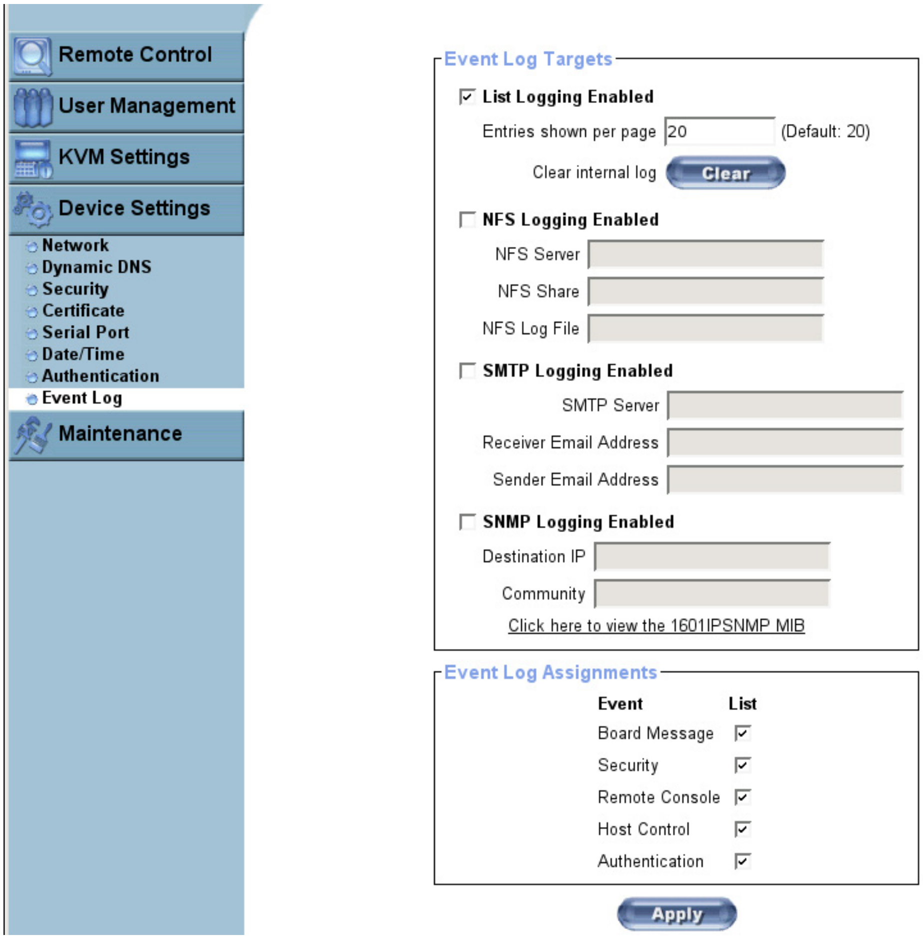
Type the port to which the RADIUS server listens for accounting requests in the **Accounting Port** field (default: 1813).

Type the request time-to-live (in seconds) in the **Timeout** field (default: 1). Time-to-live is the duration you must wait for the completion of the request. If the request job is not completed within this interval, it is cancelled.

Type the number of retries if a request cannot be completed in the **Retries** field (default: 3).

Note: Username and password information on LDAP/RADIUS server MUST also be created on MCIP unit for authentication to process.

Event Log



Event Log Targets

☑ List Logging Enabled

Entries shown per page 20 (Default: 20)

Clear internal log [Clear]

□ NFS Logging Enabled

NFS Server

NFS Share

NFS Log File

□ SMTP Logging Enabled

SMTP Server

Receiver Email Address

Sender Email Address

□ SNMP Logging Enabled

Destination IP

Community

Click here to view the 1601IPSNMP MIB

Event Log Assignments

Event	List
Board Message	☑
Security	☑
Remote Console	☑
Host Control	☑
Authentication	☑

[Apply]

Figure 38 Event Log Screen

In Event Log Targets panel, choose how many log entries are shown on each page and clear log files. Events such as login failures or firmware updates are logged to logging destinations. Each event belongs to an event group that can be activated separately. A common way to log events is to use the internal log list of the MCIP. Click on one of the radio buttons to select how to log events in MCIP.

- **List logging enabled:** View MCIP's internal log list by clicking **Maintenance** in the left navigation panel, and then clicking **Event Log.** Because the MCIP unit's system memory is used to save information, the maximum number of possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one automatically.

***Note:** If the **Reset** button on the HTML front-end is used to restart the MCIP, all logging information is saved permanently and is available after MCIP has been restarted. If the MCIP loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the log methods described below.*

- **NFS Logging enabled:** Define a NFS server where a directory or a static link has to be exported to, in order to write all logging data to a file that is located there. To write logging data from more than one MCIP devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press **Apply**, the NFS share will be mounted immediately. That means the NFS share and the NFS server must be filled with valid sources or you will get an error message.

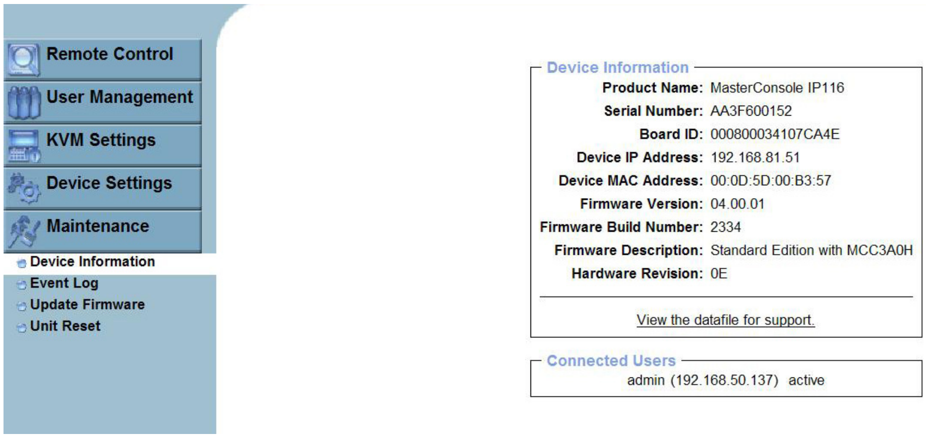
***Note:** In contrast to the internal log file on the MCIP , the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete or move it occasionally.*

- **SMTP Logging enabled:** With this option the MCIP is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server that has to be reachable from the MCIP device and that needs no authentication at all (<serverip>:<port>).
- **SNMP Logging enabled:** If this is activated, the MCIP sends a SNMP trap to a specified destination IP ad- dress, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps any SNMP trap listener may be used.

In the **Event Log Assignments** panel, choose which actions of the MCIP will be saved in the log file. Click on the desired checkbox(es) and click **Apply** to confirm your selection.

Maintenance

Device Information



Device Information

Product Name: MasterConsole IP116
Serial Number: AA3F600152
Board ID: 000800034107CA4E
Device IP Address: 192.168.81.51
Device MAC Address: 00:0D:5D:00:B3:57
Firmware Version: 04.00.01
Firmware Build Number: 2334
Firmware Description: Standard Edition with MCC3A0H
Hardware Revision: 0E

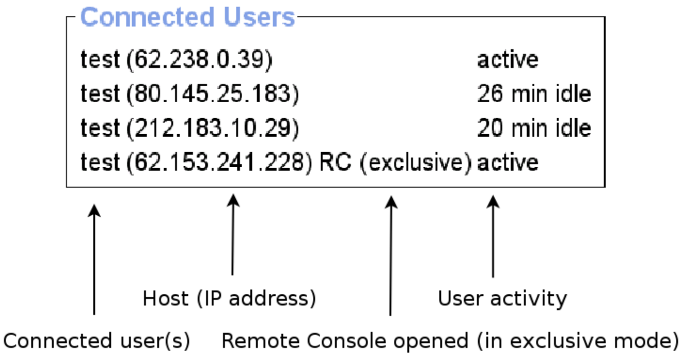
View the datafile for support.

Connected Users

admin (192.168.50.137) active

Figure 39 Device Information Screen

The Device Information screen summarizes MCIP information. The specific support information in the data file can be used in the event of a system problem and sent to Raritan so that we can better assist you.



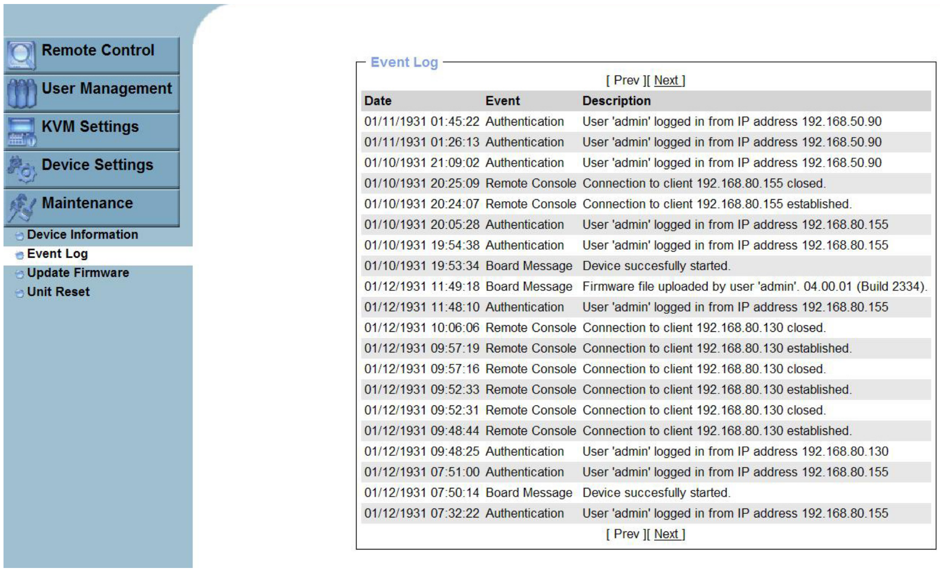
Connected Users

test (62.238.0.39) active
test (80.145.25.183) 26 min idle
test (212.183.10.29) 20 min idle
test (62.153.241.228) RC (exclusive) active

Figure 40 Connected Users Screen

The Connected Users screen displays MCIP activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. "RC" means that the Remote Console is open. If the Remote Console is opened in "exclusive mode" the term **Exclusive Mode** is added. For more information about this option see the Section called Remote Console Control Bar in Chapter 5. To display the user activity the last column contains either the term "active" for an active user or "20 min idle" for a user who is inactive for a certain amount of time.

Event Log



Date	Event	Description
01/11/1931 01:45:22	Authentication	User 'admin' logged in from IP address 192.168.50.90
01/11/1931 01:26:13	Authentication	User 'admin' logged in from IP address 192.168.50.90
01/10/1931 21:09:02	Authentication	User 'admin' logged in from IP address 192.168.50.90
01/10/1931 20:25:09	Remote Console	Connection to client 192.168.80.155 closed.
01/10/1931 20:24:07	Remote Console	Connection to client 192.168.80.155 established.
01/10/1931 20:05:28	Authentication	User 'admin' logged in from IP address 192.168.80.155
01/10/1931 19:54:38	Authentication	User 'admin' logged in from IP address 192.168.80.155
01/10/1931 19:53:34	Board Message	Device succesfully started.
01/12/1931 11:49:18	Board Message	Firmware file uploaded by user 'admin'. 04.00.01 (Build 2334).
01/12/1931 11:48:10	Authentication	User 'admin' logged in from IP address 192.168.80.155
01/12/1931 10:06:06	Remote Console	Connection to client 192.168.80.130 closed.
01/12/1931 09:57:19	Remote Console	Connection to client 192.168.80.130 established.
01/12/1931 09:57:16	Remote Console	Connection to client 192.168.80.130 closed.
01/12/1931 09:52:33	Remote Console	Connection to client 192.168.80.130 established.
01/12/1931 09:52:31	Remote Console	Connection to client 192.168.80.130 closed.
01/12/1931 09:48:44	Remote Console	Connection to client 192.168.80.130 established.
01/12/1931 09:48:25	Authentication	User 'admin' logged in from IP address 192.168.80.130
01/12/1931 07:51:00	Authentication	User 'admin' logged in from IP address 192.168.80.155
01/12/1931 07:50:14	Board Message	Device succesfully started.
01/12/1931 07:32:22	Authentication	User 'admin' logged in from IP address 192.168.80.155

Figure 41 Event Log Screen

The Event Log includes events stored by MCIP. Event date, name, and a description with issuing IP address are saved and listed.

Click on the **Prev** and **Next** links to browse from page to page within the list.

Update Firmware

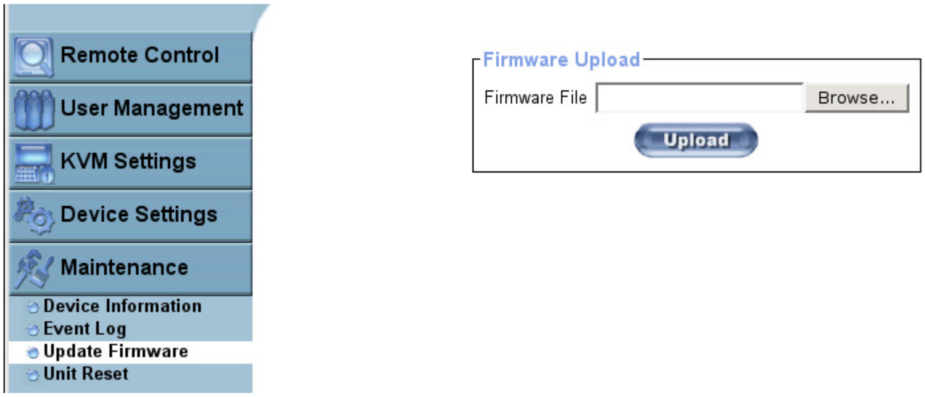


Figure 42 Update Firmware Screen

MCIP is a standalone computer that runs on firmware, which Raritan updates periodically to add new functionality or special features. A firmware update is a binary file sent to you via email or which you can download from the Raritan Website. If the firmware file is compressed (file suffix **.zip**), you must unzip it before updating (in a Windows OS, use WinZip from http://www.winzip.com/ for decompression; other operating systems may provide a proprietary unzip program). Before you update the firmware, ensure that the new (uncompressed) firmware file is accessible on the system that you use for connecting to MCIP.

To update firmware:

- In the **Firmware Upload** panel, click **Browse** to locate the firmware file on your local system and click **Upload.** Once the firmware file is uploaded, it is verified as a valid firmware file and for transmission errors. If MCIP locates an error, the upload is aborted and the current firmware is maintained.

- The **Update Firmware** panel appears, displaying the version number of your current firmware and the version number of the new firmware. Press **Update** to update the new firmware.

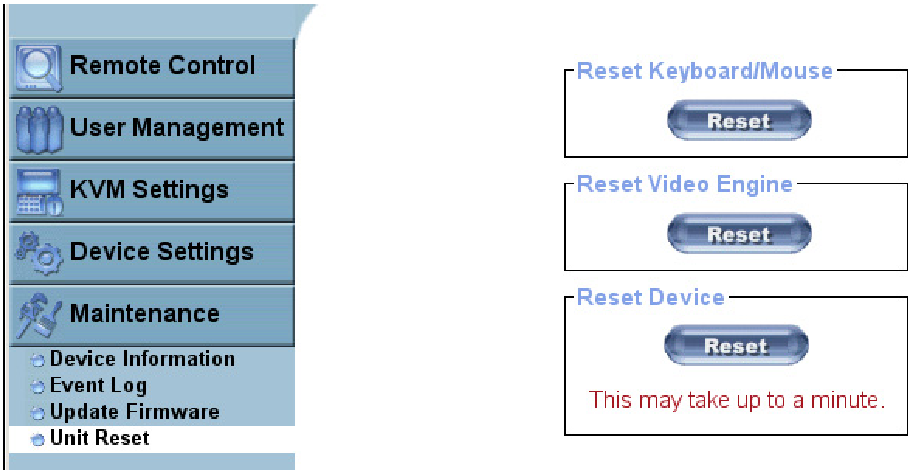
Note: *This process takes a few minutes. It is **not reversible.** Please ensure that the MCIP unit's power supply will not be interrupted during the update process; power interruption may render the MCIP unit unusable.*

- After the firmware version is updated, MCIP automatically resets. After about one minute the Login page appears, and you must log onto MCIP to resume work and reset the MCIP card (see next section).

Note: *Raritan recommends that only experienced users perform firmware updates to ensure a successful update.*

Important: Ensure that the MCIP unit's power supply will not be interrupted during firmware update.

Unit Reset



This may take up to a minute.

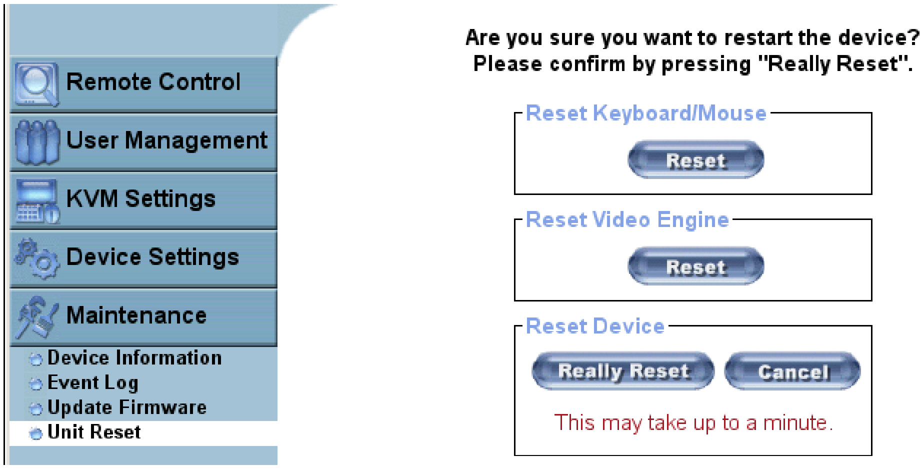
Figure 43 Unit Reset Screen

The unit reset panels allow you to reset specific parts of the MCIP unit, including keyboard and mouse, the video engine, and the MCIP itself.

You must reset the MCIP card to activate newly updated firmware. Resetting the card closes all current connections to the administration console and to the Remote Console and lasts 30-60 seconds. Resetting sub-devices takes only a few seconds and does not close any connections.

To reset any of the displayed devices, click **Reset.**

If you choose to reset the MCIP Device, MCIP confirms your choice.



Are you sure you want to restart the device?
Please confirm by pressing "Really Reset".

This may take up to a minute.

Figure 44 Unit Reset Confirmation Screen

Click **Really Reset** to reset the MCIP card.

Note: *The Reset hole in the rear panel does not reset but restart the unit.*

Appendix A: Specifications

The MCIP unit must be operated only with the provided power supply. Use of other power supplies voids the product liability of the manufacturer. If the power supply shows a malfunction, do not open it; contact Raritan Technical Support immediately for a replacement.

The power cord of the power supply is the point of junction to the supply network AC 230 V. The power supply and socket should be easily accessible in case it is necessary to disconnect them.

MCIP Video Modes (Remote User)

SCREEN RESOLUTION	REFRESH RATES (HZ)
640x350	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60, 85
1280x1024	60, 75, 85
1600x1200	60, 65, 70, 75(local port only)
2048x1536	85 (local port only)
Screen Resolution	Refresh Rates (Hz)

Main Unit

Model

MCIP18 (8–channel model):

17.28”(W) x 11”(D) x 1.71”(H) 3.46 kg (7.62 lbs.)

MCIP116 (16–channel model):

17.28”(W) x 11”(D) x 1.71”(H) 3.66 kg (8.07 lbs.)

Power:

100V/240V~

47 - 63Hz

0.6A

Operating Temperature:

0–40°C (32–104°F)

MCIP Cables:

Part No.	Length	Connectors
CMCIP20	6.56’ (2M)	HD15(M) to HD15(M), 2x mini-DIN6(M)
CMCIP40	13.12’ (4M)	HD15(M) to HD15(M), 2x mini-DIN6(M)
CMCIP90	29.52’ (9M)	HD15(M) to HD15(M), 2x mini-DIN6(M)

Appendix B: System Default Settings

FUNCTION	SETTING
Administration Password (super user 'admin')	raritan (case sensitive)
AutoScan	OFF
AutoScan mode	Global
AutoSkip	OFF
Channel-Specific Scan Rate	3 seconds
Global Scan Rate	3 seconds
Hot Key	L-Ctrl L-Ctrl L-Ctrl
ID Display Interval	3 seconds
MasterConsole IP unit configuration	First tier
PowerSave	OFF
Security	OFF
Security activation delay time	15 minutes
Selection Menu sorting	Channel ID
Language Mode	English
User password	User 1-111
	User 2-222
	User 3-333
	User 4-444

Appendix C: On-Screen User Interface Function Keys

PRESS...	WHEN YOU WANT TO...
F1	Go to the Help Menu; get a list of all the Function keys
F2	Go to the Selection Menu; view the list of channels or select a channel
F3	Go to the Edit Names and Scan Rate Menu; change channel Names or Individual Scan Rates
F4	Go to the Configuration Menu; change operating parameters (on-screen user interface, Menu position, ID position, Global / Individual Scanning, AutoScan OFF/ON, scan rate, AutoSkip OFF/ON, Hot Key, duration of ID display)
F5	Go to the Administration Menu; turn Security ON/OFF, change User Passwords
F6	Exit On-Screen User Interface and turn ON AutoScan
Alt + F6	Exit On-Screen User Interface and turn OFF AutoScan
F7	Exit On-Screen User Interface and turn ON AutoSkip
F8	Upgrade PC Status
Alt + F7	Exit On-Screen User Interface and turn OFF AutoSkip
F12	Toggle Selection Menu sorting (by Name or Channel ID)
Esc	Exit on-screen user interface and return to normal computer operation at the last channel selected. If SCAN is set ON, the system will AutoScan according to parameters set in the Configuration Menu

Appendix D: MCIP Configurations

Programming MCIP at Power Up

MCIP Product Design Background and Considerations

- User connection and operation of MCIP is through the unit's local KVM port (marked Keyboard, Monitor, Mouse – Din 6F,HD15F, Din 6F) on the back panel of each MCIP.
- For operation, a console-keyboard, monitor and mouse-plugs into the local KVM port. MCIP includes integrated On-Screen User Interface for switching and other operations.
- The On-Screen User Interface is activated through a console keyboard and facilitates operation of MCIP with on-screen menus and commands.

Appendix E: Glossary and Acronyms

Glossary

TERM	DEFINITION
Administration Menu	Used to restrict access to MCIP; toggle Security ON/OFF and to change Administrator's Password and up to five User Passwords.
Administration Password	The only Password with access to the Administration Menu, through the Administration password prompt.
AutoScan	When activated, MCIP automatically cycles through channels, displaying each computer's video for a specified period.
AutoSkip	When activated, channel selection is restricted to active channels.
Base Unit	MCIP unit
Channel	The 15-pin connector by which a device is connected to MCIP.
	Active: A channel is active when a powered ON device is connected to it.
	Inactive: A channel is inactive when there is no device connected to it, or if the connected device is powered OFF.
Channel ID	The specific Channel number to which a device is connected.
Configuration	One-Tier: Computers are connected to a single MCIP unit.
Configuration Menu	Used to specify MCIP configuration and operation parameters.
Edit Names and Scan Rate Menu	Channel-Specific Scan Rates.
Hot Key	Used to activate On-Screen User Interface. (To activate On-Screen User Interface, press the hot-key 3 times rap
ID Display	The display shown on the monitor to identify the currently selected channel
Key	Left-hand column in the Selection Menu; lists the key numbers (a sequence of numbers) for the channels listed on that page. To quickly select a channel, press its Key number when the Selection Menu is displayed.
KVM Port	The Keyboard, Monitor, and Mouse connectors on the back of the MCIP unit.
Menu	An On-Screen User Interface display.
Menu F Keys	Function keys used to access On-Screen User Interface menus while On-Screen User Interface is activated.
Mode	Field in the Configuration Menu; can be set to either Global or Individual. See also Scan Rate.
Name	A user-assigned label (up to eight characters) for a device connected to a MCIP channel.
On-Screen User Interface (OSUI)	Series of Menus displayed on the monitor that can be used, through keystrokes, to operate MCIP. All keystrokes are captured and interpreted as MCIP commands.
PowerSave	Allows a properly equipped monitor to operate in low-energy mode.
Scan	Front panel button and On-Screen User Interface function used to activate AutoScan.

TERM	DEFINITION
Scan Rate	The duration (in seconds) a channel's computer is to remain displayed on the monitor when AutoScan is activated.
	Global Scan Rate: Scan rate is the same for all computers, if the Mode field in the Configuration Menu is set to Global.
	Channel-Specific (Individual) Scan Rate:: Scan rate specified for each computer during the Scan cycle, if the Mode field in the Configuration Menu is set to Individual. Channel-specific scan rates can be set in the Edit Names and Scan Rate Menu.
Security	When activated, and the system remains idle for a period of time, the next user must enter an authorized User Password to establish access.
Selection Menu	Used to select a computer.
Sorting	Order of the channels listed in Selection Menu; either by Channel ID or by Name.
Time Out	The length of time that the system can remain idle (that is, since the last keyboard/mouse) before the next user must enter an authorized User Password to establish access.
User Password	Enables access to the system after Time Out.

Acronyms

ACPI	Advanced Configuration and Power Interface A specification that enables the operating system to implement power management and system configuration.
ATX	Advanced Technology Extended A particular specification that covers the style of motherboards and enclosure introduced by Intel in 1995.
DHCP	Dynamic Host Configuration Protocol A protocol for dynamically assigning IP configurations to host names, especially used in a local network.
DNS	Domain Name System: protocol used to locate computers on the Internet by name.
FAQ	Frequently Asked Questions
HTTP	Hypertext Transfer Protocol: One of the protocols used for communication between single computers, especially between web browsers and web servers.
HTTPS	Hyper Text Transfer Protocol Secure: secure version of HTTP.
LED	Light Emitting Diode A semiconductor device that emits incoherent monochromatic light when electrically biased in the forward direction.
PS/2	Personal System/2: IBM's second generation of personal computers, which was released to the public in 1987. Today, PS/2 is known as a device interface for mouse and keyboard.
SNMP	Simple Network Management Protocol: A widely used network monitoring and control protocol.
SSL	Secure Socket Layer: An encryption technology for the Internet used to provide secured data trans- missions.
SVGA	Super Video Graphics Array: A refinement of the Video Graphics Array (VGA) that provides increased pitch and resolution performance.
UTP	Unshielded Twisted Pair A cable with two conductors twisted as a pair and bundled within the same outer PVC covering.
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy, for secure encrypted connections between wireless devices

Appendix F: Troubleshooting

PROBLEM	SOLUTION
No power.	a. Check power cord. b. Make sure power switch is turned ON. c. Check cable connection from PC to MCIP.
No video display for one or all computers.	a. Check video cable's connection to the PC. b. Check the monitor and PC: Turn off power to MCIP and the PCs. Connect the monitor to the PC directly, boot the PC, and make sure the monitor has the proper display. If it does not, the problem is either with your PC, or the monitor is not compatible with your PC. If it does display, continue to Troubleshooting #3.
The monitor cannot correctly display the video output from some of the PCs.	a. The monitor probably does not match the video outputs. If the monitor is a single mode type VGA, all PCs must have the same type of video output. b. (Note: this problem occurs most often with some IBM PS/2s and IBM 63xx, 85xx, and 95xx monitors.) The intelligent type display card outputs video signals based on the monitor ID-pin setting in the connector of the monitor cable. If the ID-pin setting is correct, the monitor at MCIP may have no display, become monochrome instead of color, or become unstable. If this is the case, you will need to provide a proper ID-pattern to the display card.
All PCs powered up without keyboard error, but the keyboard at MasterConsole IP has no control (cannot input to any PC).	a. Make sure the keyboard is connected firmly into MCIP. Disconnect and reconnect keyboard. b. Replace keyboard. (MCIP allows hot re-connection of keyboard at its Keyboard port.)
Repeated "KB ERROR" at power-up of PC.	a. The keyboard cable from the PC to MCIP is loose. Secure the connection and power up the PC again. b. If the problem occurs after MCIP has been installed for a period of time, and occurs on PCs that have previously worked with MCIP, then some components are out of order. Verify that the PC works with the keyboard when connected directly.
After a period of trouble-free operation, the keyboard attached to MasterConsole IP locks (unable to input keystrokes) when a particular PC is selected, but works normally when other PCs are selected.	a. The most likely cause of the problem is either a voltage "spike" (increase) or a "brown out" (decrease) in the power supply, which would cause the microprocessors in MCIP to malfunction. A short-term solution to the problem is to try to recover operation by turning the MCIP power switch off and on. Then, if necessary, restart all PCs. The long-term method of avoiding this problem is to power MCIP from a UPS. b. Check keyboard connection.

PROBLEM	SOLUTION
Repeated "MOUSE INSTALLATION FAILURE" at power-up of PC.	a. The mouse cable from the PC to MCIP is loose. Secure the connection and power up again. b. If the problem only occurs to new PCs which are being added to the system, the firmware in the KVM (MCIP internal mouse emulator) may need to be upgraded to a later version to be compatible with newer PCs.
After a period of trouble-free operation, the mouse attached to MasterConsole IP locks (unable to control mouse functions) when a particular PC is selected, but works normally when other PCs are selected.	a. Try to identify if the problem is originating from the PC by reconnecting the PC to a different channel with a different cable. Then power up the PC. If the problem is not with the cable or with the specific channel, then connect the mouse directly to the PC. If the problem persists, then the PC's mouse port is out of order. b. If the problem occurs after MCIP has been installed for a period of time, and occurs to PCs that have previously worked with MCIP, then some components are out of order.
Unit does not operate in On-Screen User Interface.	Replace keyboard. On-Screen User Interface works only with PS/2 or extended AT style keyboards.
Unable to select channel.	Scan function is active; press the Scan button once to toggle Scan OFF so the light next to the button is off.
Password lost (how to reset)	**Local passwords –** When this occurs, contact Raritan Technical Support and send the device to Raritan for resolving the issue. **Remote passwords –** Reset the unit via serial interface. (See Initial Configuration via Serial Interface section for details).

Initial IP Configuration

Initially the MCIP network interface is configured with the parameters shown:

PARAMETER	VALUE
IP auto configuration	DHCP
IP address	192.168.1.22
Netmask	255.255.255.0
Gateway	None
IP access	Disabled

If this initial configuration doesn't meet your local requirements, you need to do the initial IP configuration.

Use one of the following ways:

Connect the enclosed NULL modem cable to the serial interface on the MCIP rear side. The serial interface needs to be adjusted with the parameters below:

PARAMETER	VALUE
IP auto configuration	DHCP
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

Use a terminal software (e.g. hyperterm or minicom) to connect to MCIP. Reset MCIP and immediately press ESC. You will see some device information and an ' = ' prompt. Enter the command 'config' and press **Enter**. After waiting a few moments, configure IP auto configuration, IP address, net mask and default gateway. Pressing **Enter** without entering values does not change settings. The gateway value must be set to 0.0.0.0 (for no gateway) or any other value. You will be asked if the values are correct and get a chance to correct them. After confirming, MCIP performs a reset.

Use a crossover Ethernet cable to connect MCIP to your configuring computer back to back. Set the IP address of this computer to 192.168.1.1 and use the web interface with the initial IP configuration.

Web interface

MCIP may be accessed using a standard Web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of MCIP into your Web browser. Initially there is only one user configured who has unrestricted access to all MCIP features:

Login name: super; Password MCIP

Please login and change the password immediately according to your own policies.

The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system to which MCIP is attached. The Web browser which is used for accessing MCIP has to supply a Java Runtime Environment version 1.1 or higher. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. Open the console by choosing the appropriate link in the navigation frame of the HTML front end.

There are some options to choose from, the important ones are the following:

Auto Adjust Button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while MCIP tries to adjust itself for the best possible video quality.

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general there is no need to change mouse settings on the host.

Video Settings in Options Menu

This opens a new window with elements to control the MCIP Video Settings. You can change some values, for instance, related to brightness and contrast of the picture displayed, which may improve the video quality.

Appendix G: MCIP Video Modes

The table below lists video modes supported by MCIP. Avoid using custom video settings with MCIP, as the unit may not detect them.

RESOLUTION (X,Y)	REFRESH RATES (HZ)
640x350	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85, 90, 100, 120
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85, 90, 100
832x624	75
1024x768	60, 70, 72, 75, 85, 90, 100
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60, 85
1280x1024	60, 75, 85
1600x1200	60, 65, 70, 75(local port only)

Appendix H: FAQs

QUESTION / PROBLEM	ANSWER / STATEMENT
The remote mouse does not work or is not synchronous	Ensure the mouse settings in MCIP match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly
The video quality is bad / the picture is grainy	Try to correct the brightness and contrast settings until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.
Login on MCIP fails	Ensure the correct combination of username and password was used. On delivery, the user super has the password **pass**. Your browser must be configured to accept cookies.
The Remote Console window cannot connect to the MCIP	A firewall may be preventing access to the Remote Console. Ensure the TCP port numbers 443 and 80 are open for incoming TCP connection establishments.
No connection can be established to the MCIP	Check whether the network connection is working in general (ping the IP address of the MCIP). If not, check network hardware. Make sure MCIP powered ON. Check whether the IP address of MCIP and all other IP related settings are correct. Verify that all the IP infrastructure of your LAN are correctly configured. Ensure ping functioning.
Special key combinations, for example, ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.	You must define a Button Key in the Remote Console settings.
In the browser the MCIP pages are inconsistent or chaotic	Ensure your browser cache settings are feasible; for example, ensure cache settings being are not set to "never check for newer pages" or similar, otherwise MCIP pages may be loaded from your browser cache and not from the card.
Windows XP does not awake from standby mode	This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.
Using MacOS X, an HTTPS connection fails	You must install the certificate using our certificate installer, as outlined in chapter 4.
Cannot upload the signed certificate in MacOS X	If an internal error occurs while uploading the signed certificate, change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to “plain text” and the checkbox “use for outgoing” is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).
Every time I open a dialog box with buttons, the mouse pointers are no longer synchronized.	Disable the setting “Automatically move mouse pointer to the default button of dialog boxes” in the mouse settings of your operating system.

QUESTION / PROBLEM	ANSWER / STATEMENT

Remote Console doesn't open with Opera in Linux	Some versions of Opera do not grant enough permissions if the signature of the ap- plet cannot be verified. To solve the problem, add the lines
	grant codeBase "nn.pp.rc.RemoteConsoleApplet" {
	permission java.lang.RuntimePermission "accessClassInPackage.sun.*";
	to the java policy file of opera (e.g. /usr/share/opera/java/opera.policy).

Remote console is unable to connect and displays a timeout error.	Check your hardware. If there is a proxy server between the MCIP and your host, then you may not be able to transfer the video data using RFB. Establish a direct connection between the MCIP and the client. Furthermore, check the settings of the MCIP and choose a different server port used for RFB transfer. If you use a firewall then check the according port for accepting connections. You may restrict these connections for the IP addresses used by the MCIP and your client.
For SUN computers a USB keyboard does not work.	The MCIP emulates a USB keyboard. If you attach a USB keyboard to your host two keyboards are detected. It cannot be predicted which one of these comes first and you will be able to work with. SUN supports only one USB keyboard.
Text modes are distorted and/or flicker but graphics modes work fine.	This is a known but currently unsolvable problem. It happens only if a fixed monitor resolution of 1280x1024 or higher is selected. As a workaround you may select a smaller resolution. The resolution 1280x768/60Hz is affected partially only so it is worth a try.
The local monitor displays video data but the remote screen remains blank.	If the Remote Console is connected (look at the status line of the Remote Console) you should verify that the flat panel interface is not switched off by the video driver of your operating system.
No local monitor is connected but the remote screen remains blank.	If the Remote Console is connected (look at the status line of the Remote Console) you should verify that the Monitor Dongle is connected to the VGA socket on the port replicator. This is a connector shipped with your MCIP. If it was not connected you should fix this and reboot the server afterwards.

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 8 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5994
Email: support.japan@raritan.com

Europe

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com