DVI KVM over IP
RCM101D

User Manual

www.aten.com

EMC Information

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT: 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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Warning: Operation of this equipment in a residential environment could cause radio interference.

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

KCC Statement

유선 제품용 / A 급 기기 (업무용 방송 통신 기기)

이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정 외의 지역에서 사용하는 것을 목적으로 합니다 .

RoHS

This product is RoHS compliant.

User Information

Online Registration

Be sure to register your product at our online support center:

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-400-810-0-810
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988 1-949-428-1111

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Package Contents

The RCM101D package consists of:

- 1 RCM101D DVI KVM over IP
- 1 Custom KVM Cable Set
- 1 USB 2.0 Virtual Media Cable
- 1 Power Adapter
- 1 Mounting Kit

Check to make sure that all the components are present and that nothing got damaged in shipping. If you encounter a problem, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit, and/or any of the devices connected to it.

Features may have been added to the RCM101D since this manual was published. Please visit our website to download the most up-to-date version.

Manual Date: 2020-01-17

Contents

1. Introduction

2. Hardware Setup

3. Browser Login

4. Configuration

5. The Windows Client Viewer

6. Local Console

7. The Log File

8. The Log Server

Appendix

About this Manual

This User Manual is provided to help you get the most from your system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the RCM101D system. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup, describes how to set up your installation. Diagrams showing the necessary steps are provided.

Chapter 3, Browser Login, describes how to log into the RCM101D with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 4, Configuration, explains the administrative procedures that are employed to configure the RCM101D's working environment.

Chapter 5, The Windows Client Viewer, explains how to connect to the RCM101D with the Windows Client software, and describes how to use the OSD to access and control the computers connected to the switch.

Chapter 6, AP Operation, describes how to operate the RCM101D using Windows and Java Client application programs, rather than with the browser method.

Chapter 6, Local Console, describes the use of the RCM101D from the local console and mini USB ports for console functionality.

Chapter 7, The Log File, shows how to use the log file utility to view the events that take place on the RCM101D.

Chapter 8, The Log Server, explains how to install and configure the Log Server.

An *Appendix*, provides specifications and other technical information regarding the RCM101D.

Conventions

This manual uses the following conventions:

Monospaced — Indicates text that you should key in.

[ ] — Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].

1. — Numbered lists represent procedures with sequential steps.

♦ — Bullet lists provide information, but do not involve sequential steps.

→ — Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.

⚠ — Indicates critical information.

Product Information

For information about all ATEN products and how they can help you connect without limits, visit ATEN on the Web or contact an ATEN Authorized Reseller. Visit ATEN on the Web for a list of locations and telephone numbers:

International	http://www.aten.com
North America	http://www.aten-usa.com

This Page Intentionally Left Blank

Chapter 1
Introduction

Overview

The RCM101D is a cost-efficient over-IP device that provides secure KVM (keyboard, video and mouse) server management over an IP network. It allows operators to monitor and access their computers at BIOS-level from remote locations using a web GUI, a browser-based Windows or Java client, or a Windows or Java based application program. It also allows the IP address to be easily configured from the local console.

The RCM101D supports redundant Network Internet Card (NIC) to ensure connectivity. It connects to the Internet using industry standard Cat 5e/6 cables, then uses a custom KVM cable to connect to a local KVM switch or server. It is compatible with ATEN DVI KVM switches and LCD consoles, such as the CS1768 and CL6700.

Because the RCM101D uses TCP/IP for its communications protocol, the server or KVM switch to which it is connected can be accessed from any computer on the Internet – whether that computer is located down the hall, down the street, or half-way around the world. Operators at remote locations connect to the RCM101D via its IP address. Once a connection has been established and authorization granted, the remote computer can exchange keyboard, video and mouse signals with the server (or servers on a KVM switch installation), as if an administrator were physically present and working on the equipment directly. For security, the RCM101D can pair with the Access Control Box to locally enable or disable the aforementioned remote control privilege.

The RCM101D supports Panel Array for monitoring all machines with multiple RCM products and supports advanced and exclusive RCM and OCR API (DLL) interfaces with various function integrated for easy management.

A mini USB port in the rear panel serves as a Virtual Media USB port, as well as a Laptop USB Console (LUC) port. No additional monitor, keyboard or mouse is required on the local site during routine maintenance – simply use a laptop that utilizes the LUC feature to access a computer on-site for easy management.

The RCM101D's Virtual Media function allows a user to perform diagnostic testing, file transfer, and OS/application patches from a remote console. There is no need to physically load a CD directly to the server to perform data-related tasks – conveniently and efficiently troubleshoot and resolve problems at the BIOS level from anywhere.

The RCM101D functions as a Virtual Remote Desktop. A client software for viewing remote consoles allows access to, and control of, the connected servers. Once an operator successfully connects and logs in, his screen displays what is running on the remote unit attached to the RCM101D and he can control it from his console just as if he were there.

The Log Server records the events that take place on selected RCM101D units for the administrator to analyze.

The RCM101D's firmware can be upgraded over the Internet. You can stay current with the latest functionality improvements by downloading firmware update files from our website as they become available, and then using the utility to quickly and conveniently perform the upgrade.

ATEN capitalizes on providing affordable and durable Over-IP server management solutions and ensures that each piece of equipment is worth the investment with their dependability and operational efficiency. ATEN guarantees that your RCM101D investment is protected and delivers continuous quality performance.

Features and Benefits

The features and benefits provided by a RCM101D deployment are described in the following table:

Features	Benefits
Advanced Security	◆ Advanced security features include password protection – whereby a valid username and password must be given before the client software will run – and advanced encryption technologies, such as secure TLS 1.2 and RSA 2048-bit certificates. ◆ Flexible encryption design allows users to choose any combination of 56-bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent keyboard/mouse/video and virtual media data encryption. ◆ Support for IP/MAC Filter ◆ Private CA ◆ Supports Access Control Box – enable/disable remote control privilege
External Authentication Support	In addition to its own security protection, the RCM101D allows you to set up log in authentication and authorization management from external sources such as RADIUS, LDAP, LDAPS, and MS Active Directory.
Multi-Users / Multi-Logins	The RCM101D supports up to 64 user accounts, and allows up to 32 concurrent user logins for single-bus access.
Port Share Mode	The RCM101D allows multiple users to gain access to a server simultaneously.
Serial Interface	◆ Serial console management – serial terminal access. Access the server connected to RCM101D via a built-in serial viewer, or via third party software (such as PuTTY) for Telnet and SSH sessions. ◆ Out of Band Support – via dial up modem support. Access the RCM101D through its RS-232 port using a dial-up connection.
Message Board	A message board – similar to an Internet chat program – allows users to communicate with each other, and provides mechanisms for a user to take exclusive control of the KVM functions.
Event Logging	Record the events that take place on the RCM101D and write them to the log server. Administrators and users can search for events containing specific words or strings and retrieve them according to date and order of significance.
Panel Array	Monitors all machines for operators with multiple RCM products.

Features	Benefits
Exclusive Interface Support	Supports exclusive integrated RCM API (DLL) interface with various function for system integrators
Upgradeable Firmware over the Internet	No need to add yet another cable to your installation – stay current with the latest functionality improvements and updates, all over the Internet.
Redundant LAN using one IPMAC address	Supports Network Interface Card (NIC) with backup function. Once the primary network connection fails, the RCM101D switches to another network connection automatically. This ensures connectivity and uptime.
Mouse DynaSync	No need to re-sync your mouse – Mouse DynaSync provides automatic locked-in syncing of the remote and local mouse pointers – eliminating the need to constantly re-sync the two movements. Your local console mouse movement becomes the remote unit’s mouse movement.
Superior Video	With its enhanced fps throughput for crisp responsive video display, the RCM101D offers resolutions of up to 1920 x 1200 @ 60Hz; vibrant 30-bit color depth and gray level control for rich remote session display.
Full-Screen or Sizable Remote Desktop Window	Get a full screen even if your monitor’s resolution is lower than the remote computer’s resolution. In full-screen mode the remote desktop display scales to the user’s monitor display size. Supports up to 1920 x 1200 @ 60Hz; 24-bit color depth and gray level control for remote sessions.
DDNS	Allows the mapping of a dynamic IP address assigned by a DHCP server to a host name.
End session	Administrators can terminate running sessions, especially when doing maintenance, to prevent unexpected device operations.
Multi-Keyboard Language Support / On-Screen Keyboard	The RCM101D supports multiple keyboard language input – such as English, French, German, Italian, Spanish, Japanese, Korean, and Traditional Chinese. There is no need to have a separate keyboard for each language – you can input key data in any of these languages with the RCM101D's convenient on-screen keyboard.
Virtual Media	USB 1.1 and 2.0 devices (Floppy drives, CD-ROMs, Flash drives, etc.), folders, and image files on a user’s local system, appear and act as if they were installed on the remote server, for ease and convenience when performing software installation and system updates across the entire installation.
Console access right management	The RCM101D prioritizes the local console operation. When the RCM101D is powered on, the Console Lock Switch prevents remote users from operating the device. Local/Remote Share Mode – conveniently grants shared or exclusive console privilege.
External control port	Using an external control port, the RCM101D sends a signal to trigger an alarm (light) or accepts a signal to lock the console.

Features	Benefits
ATEN PadClient Support	A mobile app for iPad to remotely and securely access computers connected to the KVM over IP switch.

System Requirements

Remote User Computers

Remote user computers (also referred to as client computers) are the ones the users log into the switch with from remote locations over the Internet. The following equipment must be installed on these computers:

- The computers used to access the switch have at least a P III 1 GHz processor, with their screen resolution set to 1024 x 768. It is recommended that your PC has P IV 2 GHz and at least 1 Gb of RAM.
- Browsers must support TLS 1.2 encryption.
- A network transfer speed of at least 128 kbps is required.
- For the *Log Server*, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.

Servers

Servers are the computers connected to the switch via KVM Cables. The following equipment must be installed on these servers:

- For USB KVM Cable Connections: a Type A USB port and USB host controller
- For virtual media connection, an extra Type A USB and USB host controller.

Cables

- A custom USB KVM cable set to link the RCM101D to a server or KVM switch are provided with this package.
- Custom KVM cable sets are available in various lengths, as shown in the table below:

Cable Type	Length	CS Part Number
USB	1.8 m	2L-7D02U / 2L-7D02UI
	3.0 m	2L-7D03U / 2L-7D03UI
	5.0 m	2L-7D05U

To purchase additional cable sets, contact your dealer.

- One custom Console cable set to link the RCM101D to a local console is provided with this package.
- A RJ45-to-serial adapter (SA0142) cable for use with the *Virtual Media* function or Laptop USB Console function (see *Virtual Media Port*, page 12; or see *Local Console*, page 93) is provided with this package.
- Cat 5e/6 or higher Ethernet cable (not provided with this package), should be used to connect the RCM101D to the LAN, WAN, or Internet.

Video

Only the following **non-interlaced** video signals are supported:

Resolution	Refresh Rates
640 x 480	60, 72, 75
720 x 400	70
800 x 600	56, 60, 72, 75, 85
1024 x 768	60, 70, 75, 85
1152 x 864	60, 70, 75, 85
1280 x 720	60
1280 x 1024	60, 70, 75, 85
1600 x 1200	60
1680 x 1050	60
1920 x 1200	60

Operating Systems

- Supported operating systems for remote user computers that log into the RCM101D include Windows 2000 or later, and other systems capable of running Sun's Java Runtime Environment (JRE) 6, Update 3, or higher (Linux, Mac, Sun, etc.).
- Supported operating systems for servers that connect to the RCM101D are shown in the table, below:

OS		Version
Windows		2000 or later
Linux	RedHat	7.1 or later
	Fedora	Core 5 or later
	SuSE	9.0 or later
	Mandriva (Mandrake)	9.0 or later
UNIX	AIX	4.3 or later
	FreeBSD	3.51 or later
	Sun	Solaris 8 or later
Novell	Netware	5.0 or later
Mac		OS 9 or later
DOS		6.2 or later

Browsers

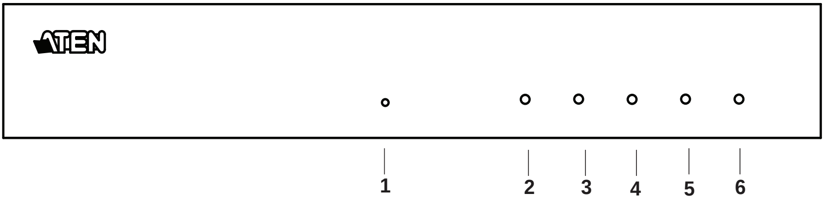
Supported browsers for users that log into the RCM101D include the following:

Browser		Version
Internet Explorer		6 or later
Chrome		8.0 or later
Firefox	Windows	3.5 or later
	Linux	3.0 or later
Safari	Windows	4.0 or later
	Mac	3.1 or later
Opera		10,0 or later
Mozilla	Windows	1.7 or later
	Sun	1.7 or later
Netscape		9.0 or later

* See *Mac Systems*, page 129, for further information regarding Safari.

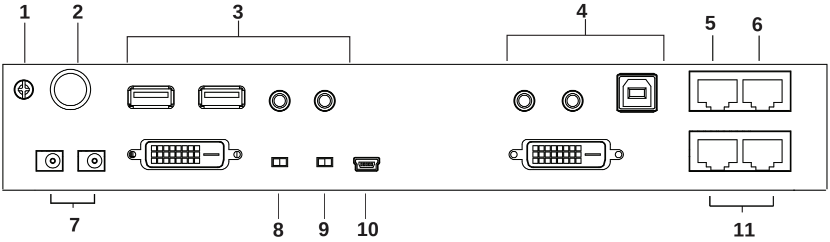
Components

Front View



No.	Component	Description
1	Reset button	Press the Reset button for more than three (3) seconds to revert to factory settings.
2	LAN 2 10/100/ 1000 LED	Lights ORANGE to indicate that the RCM101D is transmitting at 10 Mbps on this port. Lights ORANGE + GREEN to indicate that the RCM101D is transmitting at 100 Mbps on this port. Lights GREEN to indicate that the RCM101D is transmitting at 1000 Mbps on this port.
3	Remote Login LED	Lights are off when there is no active remote connection. Flashes GREEN at steady intervals to indicate that a Client program has logged into the RCM101D from the remote console.
4	LAN 1 10/100/ 1000 LED	Lights ORANGE to indicate that the RCM101D is transmitting at 10 Mbps on this port. Lights ORANGE + GREEN to indicate that the RCM101D is transmitting at 100 Mbps on this port. Lights GREEN to indicate that the RCM101D is transmitting at 1000 Mbps on this port.
5	Console Lock LED	Lights steady GREEN to indicate that another access mode is operating, depending on the active configuration.
6	Power LED	Lights GREEN when the RCM101D is powered up.

Rear View



No.	Component	Description
1	Grounding Terminal	The wire used to ground the unit connects here.
2	Control Port	This port only connects to an optional control box that requires a separate purchase.
3	Local Console Port	Connect the cable for the local console (USB keyboard, DVI monitor, USB mouse, microphone and speakers) to this port. Each connector is color coded and marked with an appropriate icon.
4	PC/KVM Port	Use the KVM cable provided with this package that links the RCM101D to your PC / Server for this port. Connect the DVI video display, keyboard/mouse, microphone and speakers to the server or KVM switch that you are installing. Each connector is color coded and marked with an appropriate icon.
5	PON Port	Use a RJ45-to-Serial adapter (SA0142) cable to connect this port to PN0108.
6	Serial Port	Use a RJ45-to-Serial adapter (SA0142) cable to connect this port to another network device, such as a modem.
7	Power Jacks	Plug the power adapter provided with this package into an AC power source, then plug the power adapter cable into any power jack. Plug another power adapter into an AC power source, then plug the power cable into the other RCM101D power jack. **Note:** Dual power operation is optional – the second power source is for back-up; a second power adapter requires a separate purchase.
8	Console Lock Switch	Use this switch to lock the console so that remote access is disabled (view only) and only the local console can operate the RCM101D. When set to unlock, the RCM101D grants access depending on the configuration stored.

9	Virtual Media / Laptop USB Console (LUC) Switch	Use this switch to select how the mini USB port operates, whether as a Virtual Media port or a Laptop USB Console port.
10	Virtual Media Port / Laptop USB Console (LUC) Port	When the *Virtual Media / Laptop USB Console (LUC) Switch* is set to Virtual Media, use the USB 2.0 cable provided with this package to connect a USB port on the server to the RCM101D's Virtual Media port. See *Virtual Media*, page 83, for details. When the switch is set to LUC, connect the laptop’s USB to this port. See *Local Console*, page 93.
11	LAN Ports	Connect a Cat 5e/6 network cable to these ports for uplink connection.

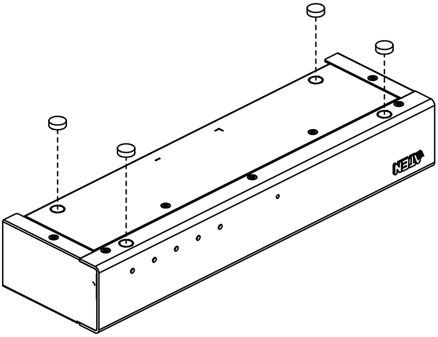
Chapter 2
Hardware Setup

1. Important safety information regarding the placement of this device is provided on page 107. Please review it before proceeding.
2. Make sure that the power to any device that you connect to the installation has been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.
3. Any installation that does not follow the instructions in this guide may be hazardous.
4. The power source for this product is intended to be supplied by a power adapter only, not a DC mains.

Stacking and Rack Mounting

Stacking

The RCM101D can be placed on any appropriate level surface that can safely support its weight plus the weight of its attached cables. To place or stack the RCM101D, remove the backing material from the bottom of the rubber feet that came with this package, and stick them onto the switch's bottom panel at the corners, as shown in the diagram below

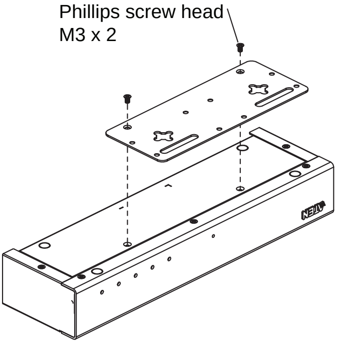


Note: To ensure adequate ventilation, allow at least 5.1 cm on each side, and 12.7cm at the back for power cord and cable clearance.

Rack / Wall Mounting

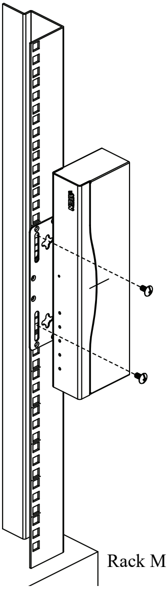
The RCM101D can be installed in most standard 19" (1U) racks or mounted to a wall. To rack mount the unit or attach the unit to the wall, do the following:

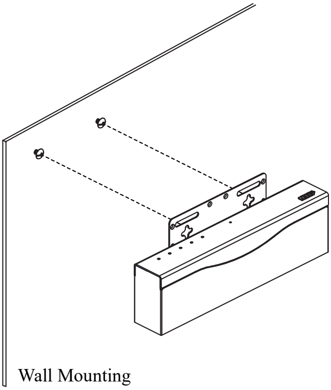
1. Use the screws supplied with your rack mounting kit to attach the mounting brackets to each side of the device:



2. If rack mounting, position the device in the rack and align the holes in the mounting brackets with the hole in the rack. If wall mounting, position the unit to a desired position on the wall.

3. Screw the mounting brackets to the rack or to a wall.


Rack Mounting


Wall Mounting

Note: Cage nuts are provided for racks that are not prethreaded.

Installation

To install the RCM101D, refer to the installation diagrams on the following pages (the numbers correspond to the numbers of the steps), and do the following:

1. Plug your USB keyboard, mouse, DVI monitor, speakers and microphone into the local console port section located on the RCM101D unit's rear panel.
2. Use the KVM cable provided with the package to connect the RCM101D's PC/KVM Port to the keyboard, video, mouse, speakers and microphone ports of the server or KVM switch that you are installing.
3. (Optional) If you want to use the virtual media function, use the USB 2.0 cable provided with the package to connect a USB port on the server to the RCM101D's Virtual Media port.
4. (Optional) If you want to use a Laptop USB Console, connect the laptop's USB to this port.

Note: Check that the Select Switch for the Virtual Media/Laptop USB Console ports is in the right position.

5. Plug a network cable into the RCM101D's LAN port 1
6. (Optional) Plug a second network cable into the RCM101D's LAN port 2.

Note: Dual LAN operation is optional.

7. (Optional) If you are using a PON device (PN108), connect it to the PON port with RJ45-to-serial adapters (SA0142).

Note: Serial adapters require a separate purchase.

8. (Optional) If you are using other serial devices, such as a standard modem, connect it to the Serial port with RJ45-to-serial adapters (SA0142)

Note: Serial adapters require a separate purchase.

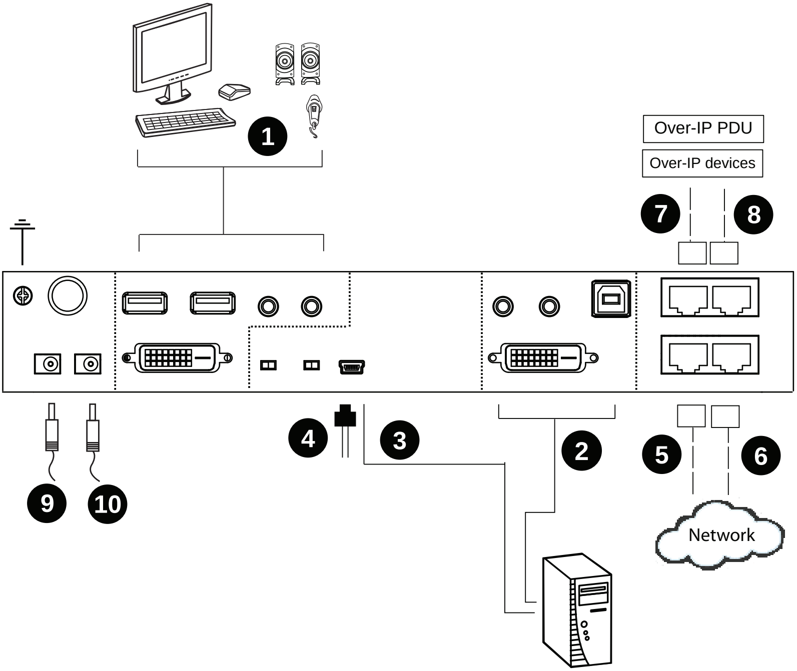
9. Plug the power adapter provided with this package into an AC power source, then plug the power adapter cable into one of the RCM101D's power jacks.

10. (Optional) Plug another power adapter into an AC power source, then plug the power cable into the other RCM101D power jack.

Note: Dual power operation is optional – the second power source is for back-up; a second power adapter requires a separate purchase

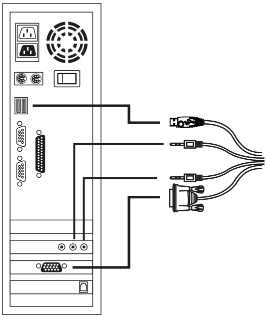
11. Power on the RCM101D, then power on the server/KVM switch.

Note: For safety reasons, we suggest you ground the switch using a grounding wire.



2

DVI KVM Cable Connection



This Page Intentionally Left Blank

Chapter 3
Browser Login

The RCM101D can be accessed either from an Internet type browser or via the following methods:

- Windows Client (see *The Windows Client Viewer*, page 63);
- Laptop USB Console (LUC) port; and
- Local Console (see *Local Console*, page 93)

The next several chapters describe browser-based operations.

Logging In

To operate the RCM101D from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the RCM101D you want to access in the browser's URL location bar.

   The default IP address for non-DHCP environment is 192.168.0.60.

   Note: 1. For security purposes, a login string may have been set by the administrator. If so, you must include a forward slash and the login string along with the IP address when you log in. For example:

   ```
   192.168.0.100/RCM101D
   ```

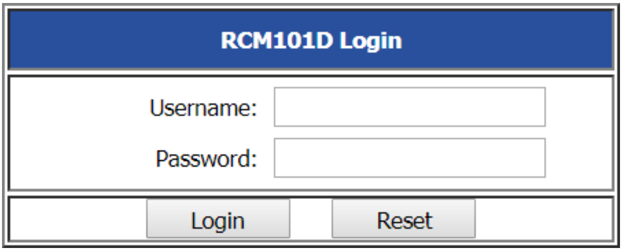
   If you don't know the IP address and login string, ask your Administrator.

   2. If you are the administrator, and are logging in for the first time, the various ways to determine the RCM101D's IP address are described in the Appendix on page 111.

2. A **Security Alert** screen (or dialog box) appears. Accept the certificate – it can be trusted. (See *Trusted Certificates*, page 121, for details.) If a second certificate appears, accept it as well.

Note: The **Security Alert** screen’s appearance varies depending on the browser version.

The RCM101D login page appears:



3. Provide a valid **Username** and **Password** (set by the RCM101D administrator), then click **Login** to continue.

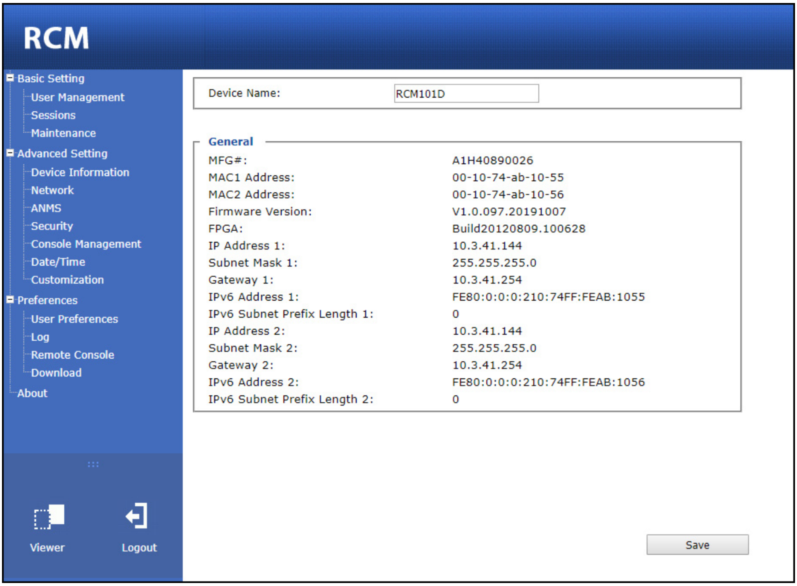
4. For security purposes, the system will prompt you to change the login password. The password must be different from your login password.

Note: 1. If you are the administrator and are logging in for the first time, use the default Username: *administrator*; and the default Password: *password*.

2. If you supplied an invalid login, the authentication routine will return this message: *Invalid Username or Password. Please try again.* If you see this message, log in again being careful with the Username and Password.

Main Screen

After you have successfully logged in, the RCM101D Main screen appears:



Device Name:	RCM101D

General

MFG#:	A1H40890026
MAC1 Address:	00-10-74-ab-10-55
MAC2 Address:	00-10-74-ab-10-56
Firmware Version:	V1.0.097.20191007
FPGA:	Build20120809.100628
IP Address 1:	10.3.41.144
Subnet Mask 1:	255.255.255.0
Gateway 1:	10.3.41.254
IPv6 Address 1:	FE80:0:0:0:210:74FF:FEAB:1055
IPv6 Subnet Prefix Length 1:	0
IP Address 2:	10.3.41.144
Subnet Mask 2:	255.255.255.0
Gateway 2:	10.3.41.254
IPv6 Address 2:	FE80:0:0:0:210:74FF:FEAB:1056
IPv6 Subnet Prefix Length 2:	0

The Main screen consists of the user menu in the left panel, with a *Viewer* icon (to launch the Java or WinClient Viewer) as well as a *Logout* icon displayed in the bottom of the menu.

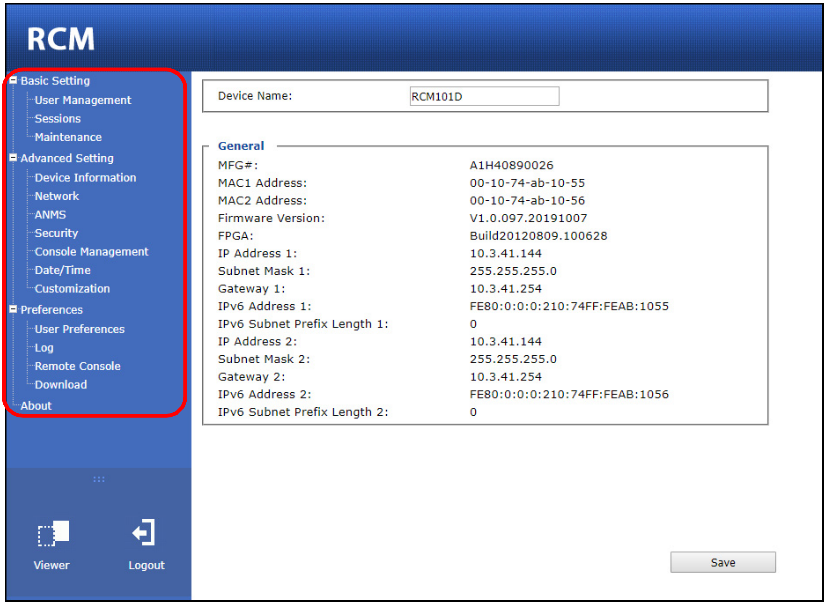
Note: If a user does not have permission to perform a particular activity, the menu option for that activity does not appear. See *Download*, page 62, for permission details.

This Page Intentionally Left Blank

Chapter 4
Configuration

Introduction

The administration utilities, represented by the links and icons located at the left panel of the RCM101D web page, are used to configure the RCM101D's operating environment. This chapter discusses each of them in turn.



Device Name: RCM101D

General

MFG#:	A1H40890026
MAC1 Address:	00-10-74-ab-10-55
MAC2 Address:	00-10-74-ab-10-56
Firmware Version:	V1.0.097.20191007
FPGA:	Build20120809.100628
IP Address 1:	10.3.41.144
Subnet Mask 1:	255.255.255.0
Gateway 1:	10.3.41.254
IPv6 Address 1:	FE80:0:0:0:210:74FF:FEAB:1055
IPv6 Subnet Prefix Length 1:	0
IP Address 2:	10.3.41.144
Subnet Mask 2:	255.255.255.0
Gateway 2:	10.3.41.254
IPv6 Address 2:	FE80:0:0:0:210:74FF:FEAB:1056
IPv6 Subnet Prefix Length 2:	0

Note: 1. As you make your configuration changes in each dialog box, click **Save** to apply the settings.

2. Some configuration changes only take effect after a RCM101D reset. To have the changes take effect, log out and then log back in again.

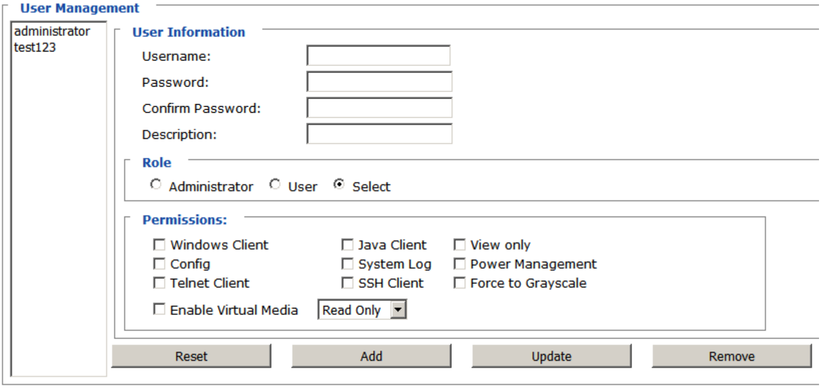
3. If you don't have configuration privileges (see *User Management*, page 24), the Administration configuration dialogs are not available.

Basic Setting

The following sections describe the screens under *Basic Setting*, which enable users to view or edit user information and device settings, including sessions, firmware version, configuration backup/restore and EDID. Click the **User Management**, **Sessions** and **Maintenance** links in the left panel menu to view the screens.

User Management

The User Management screen allows you to add, edit or remove user accounts to the RCM101D, as well as modify the role and permissions of each account:



administrator
test123

Username:
Password:
Confirm Password:
Description:

Role

○ Administrator ○ User ● Select

Permissions:

□ Windows Client □ Java Client □ View only
□ Config □ System Log □ Power Management
□ Telnet Client □ SSH Client □ Force to Grayscale
□ Enable Virtual Media Read Only

- **Username:** This is the user name of the account.
- **Password / Confirm Password:** Enter a new password if you are changing it. Re-enter the new password to confirm it.
- **Description:** Enter a descriptive word or phrase to describe the account.

Role

This allows the administrator to select which permissions the account will be allowed.

- **Administrator**: Gives the user Administrator level access to the RCM101D. All permissions (except *View Only*) are granted (see permissions below).
- **User**: Gives the user User level access to the RCM101D. Windows Client, Power Manager, and Java Client permissions are granted (see permissions below).

- **Select**: This allows you to manually select the access rights of the user by selecting them in the *Permissions* section.

Permissions

Click to place/remove a check mark next to an item to grant/withhold access to that aspect of the RCM101D's operation.

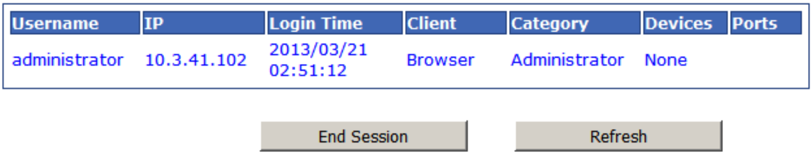
- **Windows Client**: Checking this allows a user to access the RCM101D via the Windows Client software.
- **Config:** Checking this allows the user to set up and modify the RCM101D's operating environment.
- **Telnet**: Checking this allows a user to access the RCM101D via the network protocol of the same name.
- **Enable Virtual Media**: Checking this allows a user to utilize the RCM101D's Virtual Media capabilities (see *Virtual Media*, page 83 for details). User the drop down menu to select whether the user has **Read/ Write**, or **Read Only** permission.
- **Java Client**: The related function is reserved.
- **System Log**: Checking this allows a user to view the contents of the log file.
- **SSH Client**: Checking this allows a user to access the RCM101D via SSH sessions.
- **View Only**: Checking this restricts a user from configuring the RCM101D.
- **Power Management**: Checking this gives a user privileges to access the Power on the Net™ device being implemented on the RCM101D.
- **Force to Grayscale**: Checking this renders the remote display to be in grayscale. This can speed up I/O transfer in low bandwidth situations.

After filling out the fields, click the action you want the RCM101D to apply:

- *Reset* - Click this to clear the fields.
- *Add* - Click this to add the new account to the RCM101D.
- *Update* - Click this to update the settings of an existing account.
- *Remove* - Click this to remove the selected account.

Sessions

The Sessions screen lets the administrator see at a glance all the users currently logged into the RCM101D, and provides information about each of their sessions.



Username	IP	Login Time	Client	Category	Devices	Ports
administrator	10.3.41.102	2013/03/21 02:51:12	Browser	Administrator	None	

The meanings of the headings at the top of the page are fairly straightforward.

- The *IP* heading refers to the IP address that the user has logged in from.
- The *Client* heading refers to the means the user employed to connect to the RCM101D (Browser, WinClient AP, JavaClient AP, etc.).
- The *Category* heading lists the type of user who has logged in: Admin (Administrator), User, or Select. (See *Download*, page 64 for details about user types.)

This screen also gives the administrator the option of forcing a user logout by selecting the user and clicking **End Session**.

Click **Refresh** to update the screen.

Maintenance

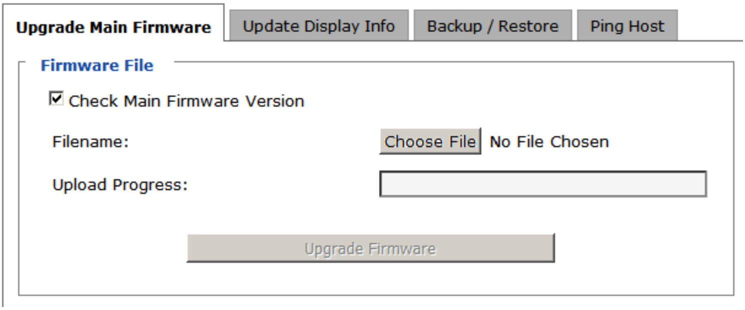
The Maintenance screen allows the Administrator to upgrade the RCM101D's firmware, view the monitor's EDID, backup/restore the RCM101D's configuration settings and ping an IP address.

Upgrade Main Firmware

As new versions of the RCM101D firmware become available, they can be downloaded from our website. Check the website regularly to find the latest information and packages.

To upgrade the firmware, do the following:

1. Download the new firmware file to your computer.
2. Open your browser; log in to the RCM101D; and click *Maintenance* in the left panel menu to bring up the *Firmware File* dialog box as follows:



☑ Check Main Firmware Version

Filename: No File Chosen

Upload Progress:

3. Click **Choose File**; navigate to the directory that the new firmware file is in and select the file.
4. Click the **Upgrade Firmware** button.

   If **Check Firmware Version** is enabled, when you perform an upgrade the current firmware level is compared with that of the upgrade file. If the current version is higher than the upgrade version, a message appears informing you of the fact and the procedure stops.

Note: If you want to install an older firmware version, you must uncheck the **Check Firmware Version** checkbox before clicking **Upgrade Firmware**.

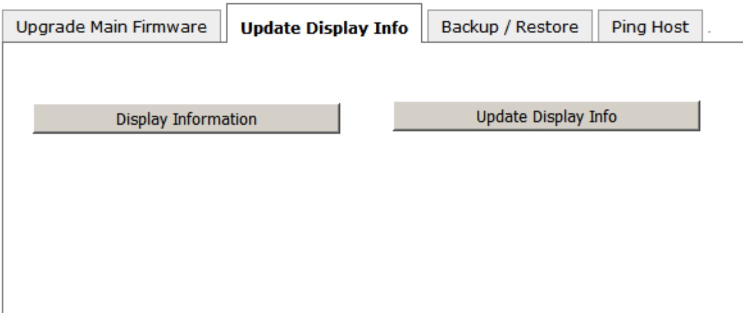
5. After the upload completes, a message appears on the screen to inform you that the operations succeeded. Click **Logout** at the bottom left of the Main web page.

6. In the screen that comes up click **Yes** to confirm that you want to exit and reset the RCM101D.

Note: You will need to wait a bit before logging back in.

Update Display Info

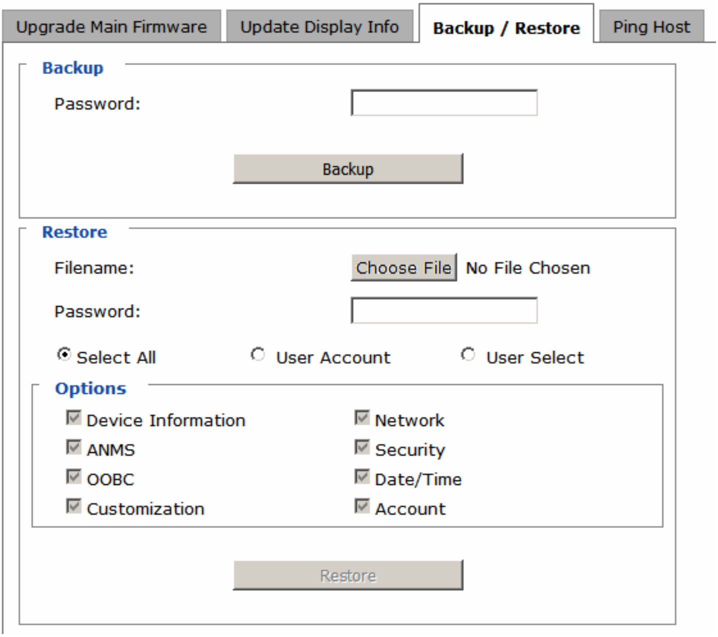
The Update Display Info section displays the EDID (Extended Display Identification Data) of the local monitor:



Click *Display Information* to view the EDID of the attached monitor. If you changed the monitor, click *Update Display Info* to get the EDID of the newly attached monitor.

Backup / Restore

The Backup / Restore screen gives you the ability to back up the RCM101D's configuration and user profile information. Backed up User Account and Configuration information can be restored with the *Restore* section. Information currently configured on the RCM101D will be replaced with the information that you restore.



Backup

Password:

Restore

Filename: No File Chosen

Password:

● Select All ○ User Account ○ User Select

Options

☑ Device Information ☑ Network
☑ ANMS ☑ Security
☑ OOBC ☑ Date/Time
☑ Customization ☑ Account

To perform a backup, do the following:

1. (Optional) In the *Password* field, key in a password for the file.

   Note: If you set a password, make a note of it, since you will need it to be able to perform restore operations with the file.

2. Click **Backup**.

3. When the browser asks what you want to do with the file, select *Save to disk*; then save it in a convenient location.

Note: The RCM101D saves all its backup files as *sysconfig.cfg*. If you want to save more than one backup file, simply rename the file to something convenient when you save it.

To restore a previous backup, do the following:

1. If a password was set when the backup was made, key the same password that you used to save the backup file in the *Password* field. If a password was not set, you can leave this field blank.
2. Click **Choose File**; navigate to the file and select it.

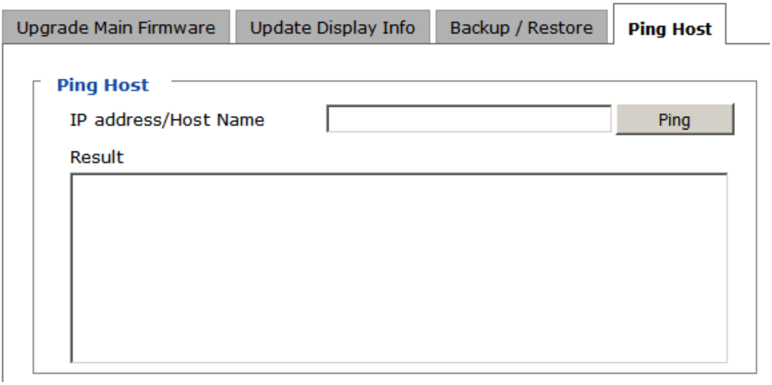
Note: If you renamed the file, you can leave the new name. There is no need to return it to its original name.

3. Select which parts of the backup you wish to restore:
   - Select the *All* to restore both User Account and all Configuration information
   - Select the *User Account* radio button to only restore User Account information
   - Select the *User Select* radio button to choose which parts of the backed up information you wish to restore, then click the checkboxes to select/deselect the restore elements.
4. When you have made your selections, click **Restore**.

   After the file is restored, a message appears to inform you that the procedure succeeded.

Ping Host

The Ping Host section enables you to ping an IP address. Enter the IP address/ Hostname then click *Ping*.



You can also enter Commands in the IP address/Host Name text bar.

Command: tc help

Result: Receive help information for commands.

Command: tc get

Result: Get current configuration.

Command: tc enablesslv2 [options]

Result:

0 - disable SSLv2

1 - enable SSLv2

Command: tc enablerc4 [options]

Result:

0 - disable RC4 cipher

1 - enable RC4 cipher

Command: tc setsslcipher [options]

0 - uses LOW, MEDIUM and HIGH ciphers

1 - uses MEDIUM and HIGH ciphers

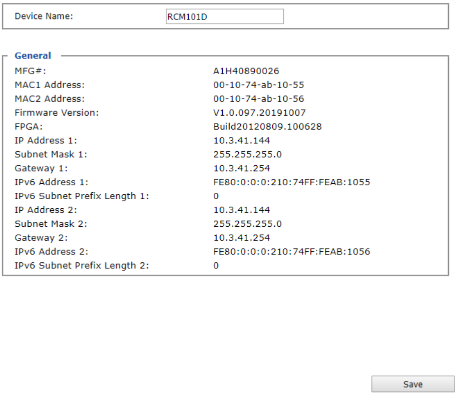
2 - uses HIGH ciphers only

Advanced Setting

The following sections describe the administration utilities covered under *Advanced Setting*, including the **Device Information**, **Network**, **ANMS**, **Security, Console Management**, **Date/Time, Customization** screens.

Device Information

The Device Information screen provides information about the RCM101D's status. You can change the device name in this screen.



Device Name: RCM101D

General

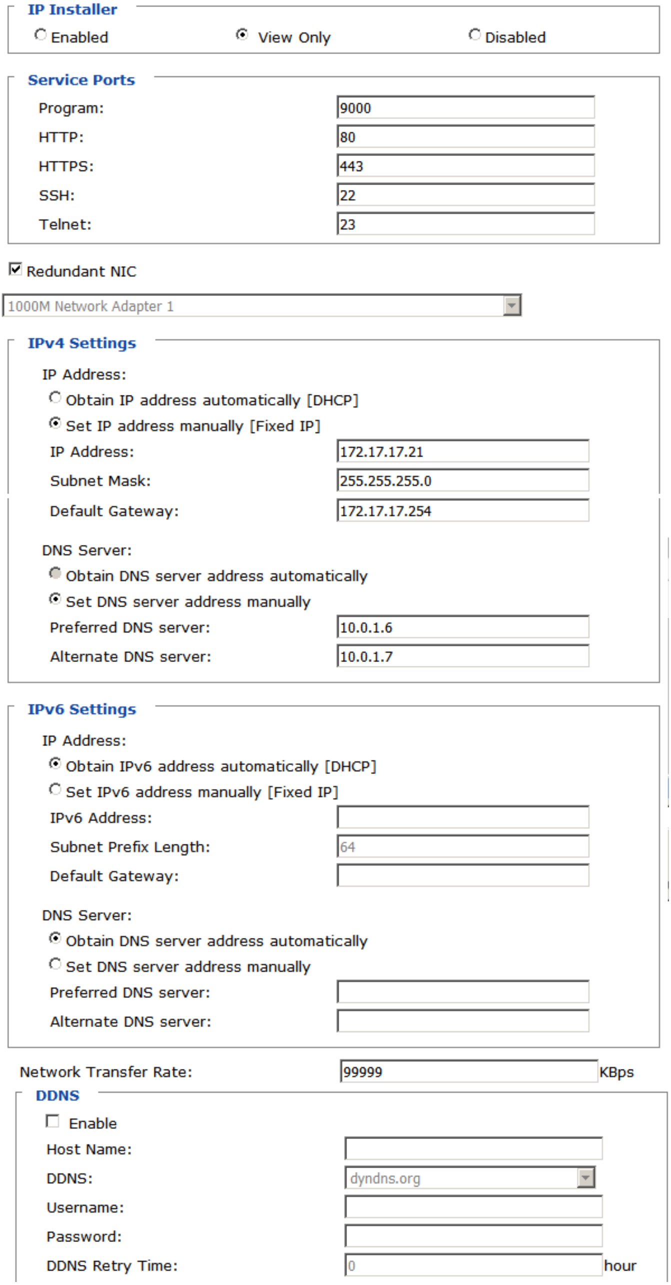
MFG#:	A1H40890026
MAC1 Address:	00-10-74-ab-10-55
MAC2 Address:	00-10-74-ab-10-56
Firmware Version:	V1.0.097.20191007
FPGA:	Build20120809.100628
IP Address 1:	10.3.41.144
Subnet Mask 1:	255.255.255.0
Gateway 1:	10.3.41.254
IPv6 Address 1:	FE80:0:0:0:210:74FF:FEAB:1055
IPv6 Subnet Prefix Length 1:	0
IP Address 2:	10.3.41.144
Subnet Mask 2:	255.255.255.0
Gateway 2:	10.3.41.254
IPv6 Address 2:	FE80:0:0:0:210:74FF:FEAB:1056
IPv6 Subnet Prefix Length 2:	0

General

- **Device Name**: To make it easier to manage installations that have more than one RCM101D, each one can be given a name. Enter a name (16 characters max.) for the RCM101D then click **Save**.
- **MAC (1, 2) Address**: The RCM101D's MAC Address displays here.
- **Firmware Version / FPGA**: Indicates the RCM101D's current firmware version level and build. New versions of the RCM101D's firmware can be downloaded from our website as they become available (see *Upgrade Main Firmware*, page 27). You can reference this number to see if there are newer versions available on the website.
- **IP Address**: Displays the RCM101D’s Internet Protocol Version 4 (32 bit) address (in the legacy format).
- **Subnet Mask**: This is the subnet mask for the IP connection.
- **Gateway**: This is the RCM101D’s gateway address.
- **IPV6 Address / IPv6 Subnet Prefix Length**: Displays the RCM101D’s Internet Protocol Version 6 (128 bit) address (in the new format). See *IPv6*, page 117 for details.

Network

The Network screen is used to specify the RCM101D's network environment.



IP Installer

○ Enabled ● View Only ○ Disabled

Service Ports

Program:	9000
HTTP:	80
HTTPS:	443
SSH:	22
Telnet:	23

☑ Redundant NIC

1000M Network Adapter 1

IPv4 Settings

IP Address:

○ Obtain IP address automatically [DHCP]

● Set IP address manually [Fixed IP]

IP Address:	172.17.17.21
Subnet Mask:	255.255.255.0
Default Gateway:	172.17.17.254

DNS Server:

○ Obtain DNS server address automatically

● Set DNS server address manually

Preferred DNS server:	10.0.1.6
Alternate DNS server:	10.0.1.7

IPv6 Settings

IP Address:

● Obtain IPv6 address automatically [DHCP]

○ Set IPv6 address manually [Fixed IP]

IPv6 Address:	
Subnet Prefix Length:	64
Default Gateway:	

DNS Server:

● Obtain DNS server address automatically

○ Set DNS server address manually

Preferred DNS server:	
Alternate DNS server:	

Network Transfer Rate: 99999 KBps

DDNS

☐ Enable

Host Name:	
DDNS:	dyndns.org
Username:	
Password:	
DDNS Retry Time:	0 hour

IP Installer

The IP Installer is an external Windows-based utility for assigning IP addresses to the RCM101D. Click one of the radio buttons to select *Enabled, View Only, or Disabled* for the IP Installer utility. See p. 113 for IP Installer details.

Note: 1. If you select *View Only*, you will be able to see the RCM101D in the IP Installer's Device List, but you will not be able to change the IP address.

2. For security, we strongly recommend that you set this to *View Only* or *Disabled* after using it.

Service Ports

Specify the ports that the RCM101D uses for various network services.

- **Program**: This is the port number for connecting to the RCM101D from the Windows Client and Java Applet Viewers, and from the Windows and Java Client AP programs. The default is 9000.
- **HTTP**: The port number for a browser login. The default is 80.
- **HTTPS**: The port number for a secure browser login. The default is 443.
- **SSH**: The port number for a secure shell login. The default is 22.
- **Telnet**: The port number for a secure console login. The default is 23.

Note: 1. Valid entries for all of the Service Ports are from 1–65535.

2. The service ports cannot have the same value. You must set a different value for each one.

3. If there is no firewall (on an Intranet, for example), it does not matter what these numbers are set to, since they have no effect.

If a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). If a port other than the default is set, users must specify the port number as part of the IP address when they log in. If not, an invalid port number (or no port number) is specified, the RCM101D will not be found.

Redundant NIC

A Redundant NIC ensures that the RCM101D is always online by switching to another network adapter in case the primary connection fails.

- Check *Redundant NIC* if you are using the secondary LAN port for a second IP address.
- If you are using the secondary LAN port for a second IP address, leave Redundant NIC unchecked. Use the drop-down menu and select 1000M Network Adapter 2, then set the IP and DNS addresses for it.

IPv4 Settings

The RCM101D can either have its IP address assigned dynamically at bootup (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the **Obtain an IP address automatically**, radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Set IP address manually**, radio button and fill in the IP address.

Note: 1. If you choose *Obtain IP address automatically*, when the switch starts up it waits to get its IP address from the DHCP server. If it has not obtained the address after one minute, it automatically reverts to its factory default IP address, 192.168.0.60.

2. If the RCM101D is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, you can use the IP installer. See *IP Address Determination*, page 111, for information.

The RCM101D can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically**, radio button.
- To specify a fixed address, select the **Use the following DNS server address**, radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

IPv6 Settings

The RCM101D can either have its IPv6 address assigned dynamically at bootup (DHCP), or it can be given a fixed IPv6 address.

- For dynamic IP address assignment, select the **Obtain an IPv6 address automatically**, radio button. (This is the default setting.)
- To specify a fixed IP address, select the **Set IPv6 address manually**, radio button and fill in the IP address.

The RCM101D can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic DNS Server address assignment, select the **Obtain DNS server address automatically**, radio button.
- To specify a fixed address, select the **Use the following DNS server address**, radio button and fill in the required information.

Note: Specifying at the alternate DNS Server address is optional.

Network Transfer Rate

This setting allows you to tailor the size of the data transfer stream to match network traffic conditions by setting the rate at which the RCM101D transfers data to remote computers. The range is from 4–99999 Kilobytes per second (KBps).

DDNS

DDNS maps a dynamic IP address assigned by a DHCP server to a host name. The RCM101D can update the DDNS server with its IP address at certain time intervals. To enable the DDNS capability for the RCM101D, do the following:

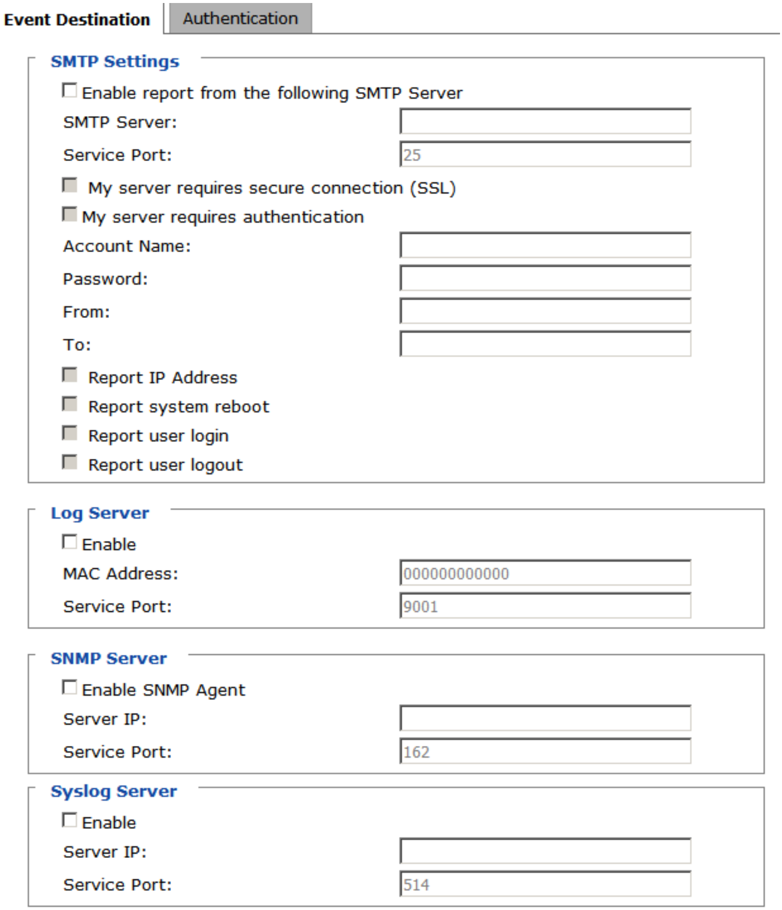
1. Check **Enable**.
2. Enter the hostname that you registered with your DDNS service provider.
3. Drop down the list to select the DDNS service you are registered with.
4. Key in the Username and Password that authenticates you with your DDNS service.
5. In the DDNS Retry Time field, key in how many hours the RCM101D waits before updating the DDNS server.

ANMS

The Advanced Network Management Settings screen allows you to set up login authentication and authorization management from external sources. It is divided into several sections, each of which is described in the sections that follow.

Event Destination

This section lets you configure the SMTP, log server, SNMP and syslog server settings.



SMTP Settings

☐ Enable report from the following SMTP Server

SMTP Server:

Service Port: 25

☐ My server requires secure connection (SSL)

☐ My server requires authentication

Account Name:

Password:

From:

To:

☐ Report IP Address

☐ Report system reboot

☐ Report user login

☐ Report user logout

Log Server

☐ Enable

MAC Address: 000000000000

Service Port: 9001

SNMP Server

☐ Enable SNMP Agent

Server IP:

Service Port: 162

Syslog Server

☐ Enable

Server IP:

Service Port: 514

SMTP Settings

To have the RCM101D email reports from the SMTP server to you, do the following:

1. Check **Enable report from the following SMTP server**, and key in the IP address and service port of your SMTP server.
2. If you're connecting to a secure server, check **My server requires secure connection (SSL)**.
3. If your server requires authentication, put a check in the **My server requires authentication** checkbox, and key in the appropriate account information in the **Account Name** and **Password** fields.
4. Key in the email address of where the report is being sent from in the **From** field.

Note: Only one email address is allowed in the *From* field, and it cannot exceed 64 English alphanumeric character.

5. Key in the email address (addresses) of where you want the SMTP reports sent to in the **To** field.

Note: If you are sending the report to more than one email address, separate the addresses with a semicolon. The total cannot exceed 256 English alphanumeric character.

6. Put a check on the kind of information that you want to be included in the report email:
   - Report IP Address
   - Report system reboot
   - Report user login
   - Report user logout

Log Server

Important transactions that occur on the RCM101D, such as logins and internal status messages, are kept in an automatically generated log file

- Specify the MAC address of the computer that the Log Server runs on in the *MAC address* field.
- Specify the port used by the computer that the Log Server runs on to listen for log details in the *Port* field. The valid port range is 1–65535. The default port number is 9001.

Note: The port number must different than the one used for the *Program* port (see *Service Ports*, page 35).

See Chapter 8, *The Log Server*, for details on setting up the log server. The *Log File* is discussed on page 97.

SNMP Server

To be notified of SNMP trap events, do the following:

1. Check *Enable SNMP Agent*.
2. Key in the IP address and the port number of the computer to be notified of SNMP trap events. The valid port range is 1-65535. Default is 162.

Note: The following SNMP trap events are sent: *System Power On, Login Failure,* and *System Reset.*

Syslog Server

To record all the events that take place on the RCM101D and write them to a Syslog server, do the following:

1. Check **Enable**.
2. Key in the IP address and the port number of the Syslog server. The valid port range is 1-65535. Default is 514.

Authentication

The RCM101D allows log in authentication and authorization through external programs.

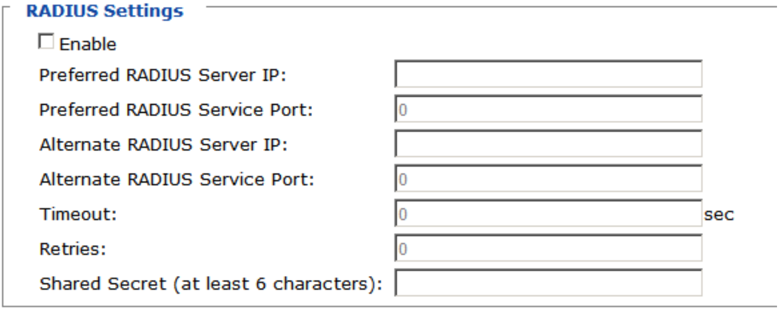
This screen lets you configure the RADIUS and LDAP settings.

If you want to use a RADIUS or LDAP instead of the RCM101D device authentication, check **Disable Device Authentication**. Selecting this option will disable login authentication locally on the RCM101D.

If the third party authentication server/external program you are using fails to authenticate and you cannot log on to the RCM101D, you can enable local authentication through the local console. See page 112 for details on how to use the local console to enable authentication on the RCM101D.

RADIUS Settings

To allow authentication and authorization for the RCM101D through a RADIUS server, do the following:



RADIUS Settings

☐ Enable

Preferred RADIUS Server IP:	
Preferred RADIUS Service Port:	0
Alternate RADIUS Server IP:	
Alternate RADIUS Service Port:	0
Timeout:	0 sec
Retries:	0
Shared Secret (at least 6 characters):	

1. Check **Enable**.

2. Fill in the IP addresses and service port numbers for the Preferred and Alternate RADIUS servers.

3. In the *Timeout* field, set the time in seconds that the RCM101D waits for a RADIUS server reply before it times out.

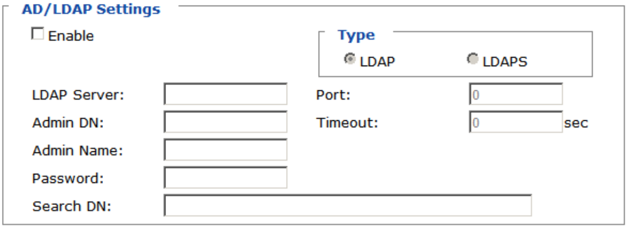
4. In the *Retries* field, set the number of allowed RADIUS retries.

5. In the **Shared Secret** field, key in the character string that you want to use for authentication between the RCM101D and the RADIUS Server.

LDAP Settings

To allow authentication and authorization via LDAP or LDAPS, the Active Directory's LDAP Schema must be extended so that an extended attribute name for the RCM101D – RCM101D-*userProfile* – is added as an optional attribute to the person class.

In order to configure the LDAP server, you will have to complete the following procedures: 1) Install the Windows Server Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema. Refer to the *LDAP Server Configuration Example* for further information, please see the ATEN website at www.aten.com and navigate to the Download page.



AD/LDAP Settings

□ Enable

Type

● LDAP ○ LDAPS

LDAP Server:		Port:	0
Admin DN:		Timeout:	0 sec
Admin Name:			
Password:			
Search DN:			

To allow authentication and authorization for the RCM101D via LDAP / LDAPS, refer to the information in the following table.

Item	Action
Enable	Put a check in the *Enable* checkbox to allow LDAP / LDAPS authentication and authorization.
LDAP / LDAPS	Click a radio button to specify whether to use LDAP or LDAPS.
LDAP Server Port	Fill in the IP address and port number for the LDAP or LDAPS server. For LDAP, the default port number is 389; for LDAPS, the default port number is 636.
Timeout (seconds)	Set the time in seconds that the RCM101D waits for an LDAP or LDAPS server reply before it times out.
Admin DN	Consult the LDAP / LDAPS administrator to ascertain the appropriate entry for this field. For example, the entry might look like this: cn=LDAPAdmin,ou=rcm101d,dc=aten,dc=com
Admin Name	Key in the Group Name for RCM101D administrator users.
Password	Key in the LDAP administrator's password.
Search DN	Set the distinguished name of the search base. This is the domain name where the search starts for user names. If *Enable Authorization is not checked, this field must include the entry where* the RCM101D *Admin Group is created.* Consult the LDAP / LDAPS administrator to ascertain the appropriate value.

The Permission Attribute Value (for RADIUS and LDAP)

The attribute value for *permission* is made up of two parts: 1) the IP address of the RCM101D a user will access; and 2) a string that indicates the access rights the user has on the RCM101D at that IP address. For example:

```
192.168.0.80&c,w,j;192.168.0.188&v,l
```

The makeup of the permission entry is as follows:

- An ampersand (&) connects the RCM101D*'s IP* with the access rights string.
- The access rights string is made up of various combinations of the following characters: c w j p l v s. The characters can be entered in upper or lower case. See *Permitted String Characters* table below.
- The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- If a user has access rights to more than one RCM101D*,* each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.
- Use the following keyword for Radius and LDAP setting: **su/[username]** – the username must be a real user account that exists in the system.
- LDAP should use **RCM101D-userProfile**, or can waive this. The login name must exist in the local account.

Permission String Characters

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java applet.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
M	Allows the user to use the Virtual Media function – Read / Write

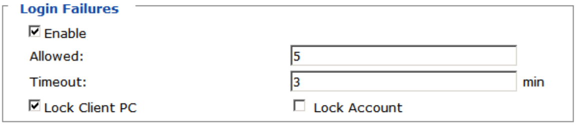
Note: *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.

Security

The Security screen controls access to the RCM101D, and lets you configure the login failure policies, login string, security settings, and so on.

Login Failures

For increased security, the Login Failures section allows administrators to set policies governing what happens when a user fails to log in successfully.



Login Failures

☑ Enable

Allowed: 5

Timeout: 3 min

☑ Lock Client PC □ Lock Account

The meanings of the entries are explained below.

- Login Fail Policy: Select the login failure policy that the RCM101D applies.

  Lock Client PC – If this is enabled, after the allowed number of failures have been exceeded, the computer attempting to log in is automatically locked out. No logins from that computer will be accepted. The default is enabled. This function relates to the client computer's IP. If the IP is changed, the computer will no longer be locked out.

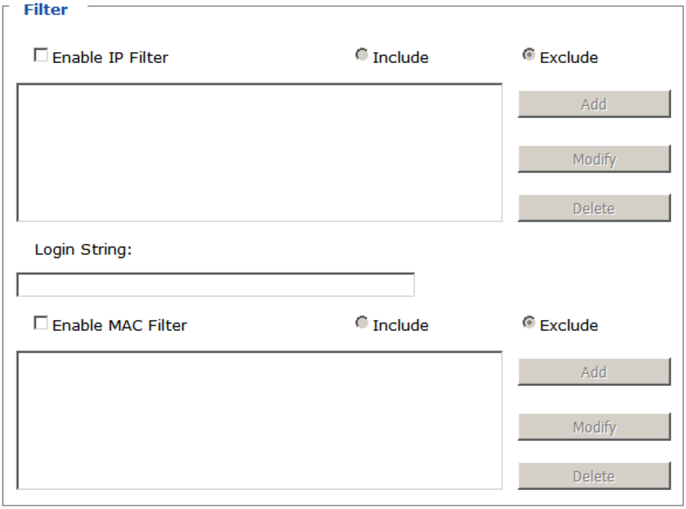
  Lock Account – If this is enabled, after the allowed number of failures have been exceeded, the user attempting to log in is automatically locked out. No logins from the username and password that have failed will be accepted. The default is enabled.

- **Allowed** - Sets the number of consecutive failed login attempts that are permitted from a remote computer. The default is 5 times.
- **Timeout** - Sets the amount of time (in minutes) that a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures. The default is 3 minutes.

Note: If you don't enable **Login Failures**, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, we recommend that you enable this function and enable the lockout policies.

Filter

IP and MAC Filters control access to the RCM101D based on the IP and/or MAC addresses of the computers attempting to connect. A maximum of 100 IP filters and 100 MAC filters are allowed. If any filters have been configured, they appear in the IP Filter and/or MAC Filter list boxes.



Filter

☐ Enable IP Filter ○ Include ● Exclude

Login String:

☐ Enable MAC Filter ○ Include ● Exclude

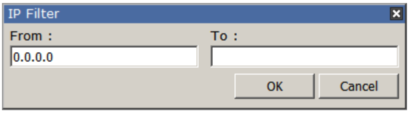
To enable IP and/or MAC filtering, put a check mark in the *IP Filter Enable* and/or *MAC Filter Enable* checkbox.

- If the **Include** button is checked, all the addresses within the filter range are allowed access; all other addresses are denied access.
- If the **Exclude** button is checked, all the addresses within the filter range are denied access; all other addresses are allowed access.

Adding Filters

To add an IP filter, do the following:

1. Click **Add**. Key in the IP address range you want to filter, and click **OK**:



IP Filter

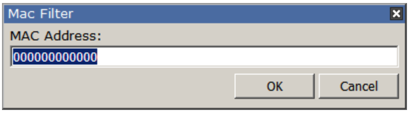
From : 0.0.0.0

To :

2. Repeat these steps for any additional IP addresses you want to filter.

To add a MAC filter, do the following:

1. Click **Add**. A dialog box similar to the one below appears:



2. Specify the MAC address in the dialog box, then click **OK**.
3. Repeat these steps for any additional MAC addresses you want to filter.

Note: If there is a conflict between an IP filter and a MAC filter – for example, where a computer's IP address is allowed by the IP filter but it's MAC address is excluded by the MAC filter – then that computer's access is blocked. In other words, if either filter blocks a computer, then the computer is blocked, no matter what the other filter is set to.

Modifying Filters
To modify a filter, select it in the IP Filter or MAC Filter list box and click **Modify**. The Modify dialog box is similar to the Add dialog box. When it comes up, simply delete the old address(es) and replace it with the new one(s).

Deleting Filters
To delete a filter, select it in the IP Filter or MAC Filter list box and click **Delete**.

The Filter section also lets administrators specify a *Login String* that users must include (in addition to the IP address) when they access the RCM101D with a browser. For example:

```
192.168.0.126/RCM101D
```

- The following characters are allowed:
  0–9 a–z A–Z ~ ! @ $ ^ & * ( ) _ + ‘ - = [ ] { } ; ’ < > , . |
- The following characters are not allowed:
  - % ” : / ? # \ [Space]
  - Compound characters (É Ç ñ ... etc.)

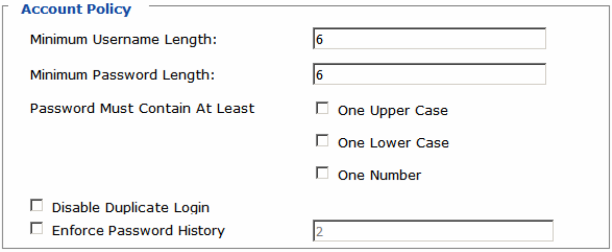
Note: 1. There must be a forward slash between the IP address and the string.

2. If no login string is specified here, anyone will be able to access the RCM101D login page using the IP address alone. This makes your installation less secure.

For security purposes, we recommend that you change this string occasionally.

Account Policy

Set the parameters for the username and password.



Account Policy

Minimum Username Length: 6

Minimum Password Length: 6

Password Must Contain At Least
□ One Upper Case
□ One Lower Case
□ One Number

□ Disable Duplicate Login

□ Enforce Password History 2

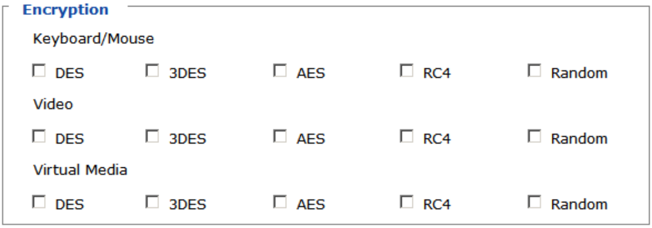
- Minimum Username Length: Enter the minimum number (0 - 16) of characters required for a username (default is 6).
- Minimum Password Length: Enter the minimum number (0 - 16) of characters required for a password (default is 6).
- Check whether the password must contain at least: *One Upper Case*, *One Lower Case*; and/or *One Number* character.

Note: This policy only affects user accounts created after this policy has been enabled, as well as password changes to existing user accounts.

- Check *Disable Duplicate Login* to ensure that only one session for each user account is active. This prevents users from logging in with the same account at the same time.
- To prevent users from using the same password when they are required to recreate their passwords, you can check *Enforce Password History*. In the field, enter the number of password changes that must occur before a previous password can be used a second time.

Encryption

These flexible encryption alternatives for keyboard/mouse, video, and virtual media data let you choose any combination of DES; 3DES; AES; RC4; or a Random cycle of any or all of them.



Encryption

Keyboard/Mouse
□ DES □ 3DES □ AES □ RC4 □ Random

Video
□ DES □ 3DES □ AES □ RC4 □ Random

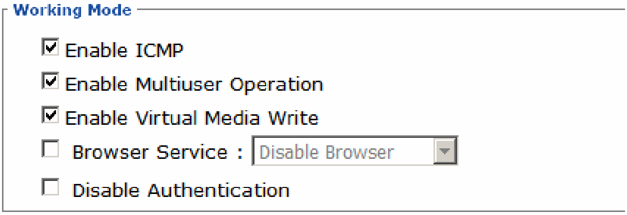
Virtual Media
□ DES □ 3DES □ AES □ RC4 □ Random

Enabling encryption will affect system performance – no encryption offers the best performance; the greater the encryption, the greater the adverse effect. If you enable encryption, the performance considerations (going from best to worst) are as follows:

- RC4 offers the least performance impact; DES is next; then 3DES or AES
- The RC4 + DES combination offers the least impact of any combination

Working Mode

Use this section to set the working mode parameters.



Working Mode

☑ Enable ICMP

☑ Enable Multiuser Operation

☑ Enable Virtual Media Write

□ Browser Service : Disable Browser

□ Disable Authentication

- *Enable ICMP* so that the RCM101D can be pinged. If it is not enabled, the device cannot be pinged. The default is **Enabled**.
- *Enable Multiuser Operation* to permit more than one user to log into the RCM101D at the same time. The default is **Enabled**.
- *Enable Virtual Media Write* allows redirected virtual media devices on a user's system to send data to a remote server, as well as being able to have data from the remote server written to them. The default is **Enabled**.
- *Browser Service* allows the administrator to limit the scope of browser access to the RCM101D. Put a check in the checkbox to enable this function, then select the browser limitation in the drop down list box. Choices are explained in the following table:

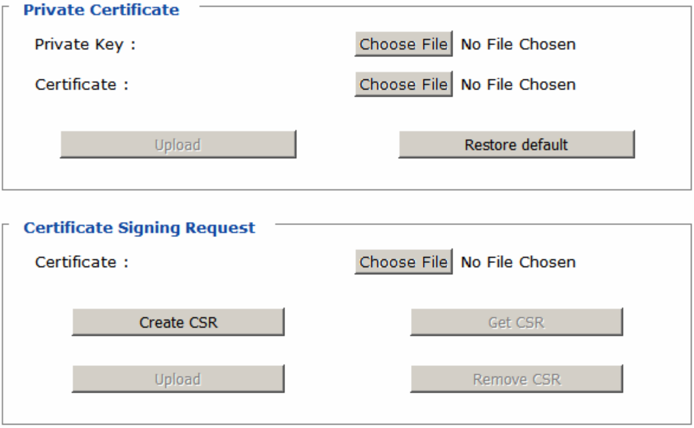
Item	Explanation
Disable Browser	If this is selected, the RCM101D cannot be accessed via a browser. It can only be accessed from the windows client viewer (see *The Windows Client Viewer*, page 63).
Disable HTTP	If this is selected, the RCM101D can be accessed via a browser, but not from an ordinary (HTTP) login connection – it can only be accessed over a secure HTTPS (SSL) connection.
Disable HTTPS (SSL)	If this is selected, the RCM101D can be accessed via a browser over an ordinary (HTTP) login connection, but not via a secure HTTPS (SSL) connection.

- If *Disable Authentication* is checked, no authentication procedures are used to check users attempting to log in. Users gain Administrator access to the RCM101D switch simply by entering combination of username and password.

Note: Enabling this setting creates an extremely dangerous result as far as security goes, and should only be used under very special circumstances.

Private Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the Private Certificate section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.



There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

Generating a Self-Signed Certificate
If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 125 for details about using OpenSSL to generate your own private key and SSL certificate.

Obtaining a CA Signed SSL Server Certificate
For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After

the CA sends you the certificate, save it to a convenient location on your computer.

Importing the Private Certificate
To import the private certificate, do the following:

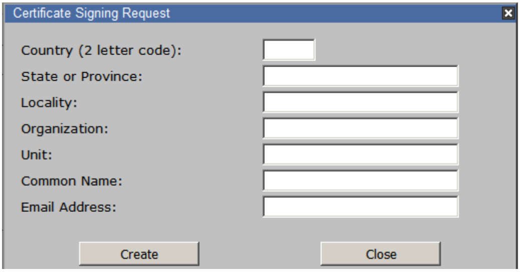
1. Click **Browse** to the right of **Private Key**; browse to where your private encryption key file is located; and select it.
2. Click **Browse** to the right of **Certificate**; browse to where your certificate file is located; and select it.
3. Click **Upload** to complete the procedure.

Note: Both the private encryption key and the signed certificate must be imported at the same time.

Certificate Signing Request

The Certificate Signing Request (CSR) section provides an automated way of obtaining and installing a CA signed SSL server certificate.
To perform this operation do the following:

1. Click **Create CSR**. The following dialog box appears:



Certificate Signing Request

Country (2 letter code):

State or Province:

Locality:

Organization:

Unit:

Common Name:

Email Address:

2. Fill in the form – with entries that are valid for your site – according to the example information in the following table:

Information	Example
Country (2 letter code)	TW
State or Province	Taiwan
Locality	Taipei
Organization	Your Company, Ltd.
Unit	Techdoc Department

Information	Example
Common Name	mycompany.com This must be the exact domain name of the site that you want the certificate to be valid for. If the site's domain name is *www.mycompany.com*, and you only specify *mycompany.com*, the certificate will not be valid.
Email Address	administrator@yourcompany.com

3. After filling in the form (all fields are required), click **Create**.

   A self-signed certificate based on the information you just provided is now stored on the RCM101D.

4. Click **Get CSR**, and save the certificate file (*csr.cer*) to a convenient location on your computer

   This is the file that you give to the third party CA to apply for their signed SSL certificate.

5. After the CA sends you the certificate, save it to a convenient location on your computer. Click **Browse** to locate the file; then click **Upload** to store it on the RCM101D.

Note: When you upload the file, the RCM101D checks the file to make sure the specified information still matches. If it does, the file is accepted; if not, it is rejected.

If you want to remove the certificate (to replace it with a new one because of a domain name change, for example), simply click **Remove CSR**.

Console Management

This section discusses methods of opening the RCM101D console via OOBC or serial connection.

OOBC

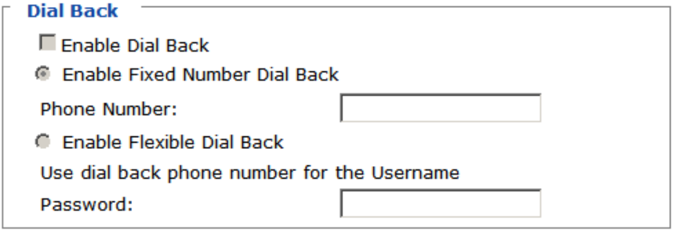
In case the RCM101D cannot be accessed with the usual LAN-based methods, it can be accessed via the switch's modem port. To enable support for PPP (modem) operation, click to put a checkmark in the *Enable Out of Band Access* checkbox.

PPP Settings

When you enable Out of Band Access, the *Enable Dial Back*, and *Enable Dial Out* functions become available, as described in the sections that follow.

Dial Back

As an added security feature, if this function is enabled, the switch disconnects the calls that dial in to it, and dials back to one of the entries specified below:



Dial Back

□ Enable Dial Back

● Enable Fixed Number Dial Back

Phone Number:

○ Enable Flexible Dial Back

Use dial back phone number for the Username

Password:

- **Enable Fixed Number Dial Back**: If *Fixed Number Dial Back* is enabled, when there is an incoming call, the RCM101D hangs up the modem and dials back to the modem whose phone number is specified in the Phone Number field.

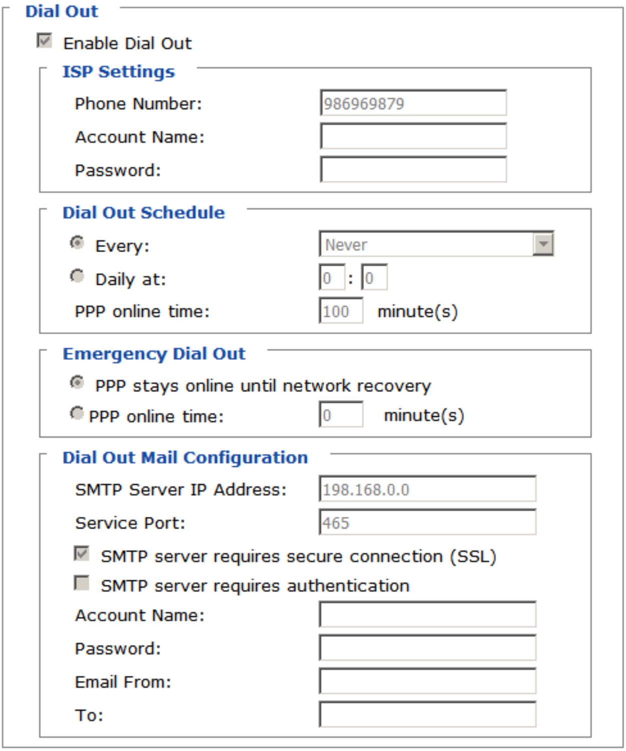
  Key the phone number of the modem that you want the RCM101D to dial back to in the *Phone Number* field.

- **Enable Flexible Dial Back:** If *Flexible Dial Back* is enabled, the modem that the RCM101D dials back to doesn't have to be fixed. It can dial back to any modem that is convenient for the user, as follows:

  1. Key the password that the users must specify in the *Password* field.
  2. When connecting to the RCM101D's modem, users specify the phone number of the modem that they want the RCM101D to dial back to as their Username, and specify the password set in the *Password* field for their password.

Dial Out

For the dial out function, you must establish an account with an Internet Service Provider, and use a modem to dial up to your ISP account. An explanation of the Enable Dial Out items is given in the table below:



Dial Out

☑ Enable Dial Out

ISP Settings

Phone Number: 986969879

Account Name:

Password:

Dial Out Schedule

● Every: Never

○ Daily at: 0 : 0

PPP online time: 100 minute(s)

Emergency Dial Out

● PPP stays online until network recovery

○ PPP online time: 0 minute(s)

Dial Out Mail Configuration

SMTP Server IP Address: 198.168.0.0

Service Port: 465

☑ SMTP server requires secure connection (SSL)

☐ SMTP server requires authentication

Account Name:

Password:

Email From:

To:

- **ISP Settings**: Specify the telephone number, account name (username), and password that you use to connect to your ISP.
- **Dial Out Schedule:** This entry sets up the times you want the RCM101D to dial out over the ISP connection. *Every* provides a listing of fixed times from every hour to every four hours.
  - If you select *Every two hours* (for example), the RCM101D will start dialing out every two hours beginning at 00:00.
  - If you don't want the RCM101D to dial out on a fixed schedule, select **Never** from the list.
- *Daily at* will dial out once a day at a specified time. Use the hh:mm format to specify the time.

- *PPP online time* specifies how long you want the ISP connection to last before terminating the session and hanging up the modem. A setting of zero means it is always on line.
- **Emergency Dial Out:** If the RCM101D gets disconnected from the network, or the network goes down, this function puts the switch on line via the ISP dial up connection.
  - If you choose *PPP stays online until network recovery*, the PPP connection to the ISP will last until the network comes back up or the switch reconnects to it.
  - If you choose *PPP online time*, the connection to the ISP will terminate after the amount of time that you specify is up. A setting of zero means it is always on line.
- **Dial Out Mail Configuration**: This section provides email notification of problems that occur on the devices connected to the RCM101D's ports.

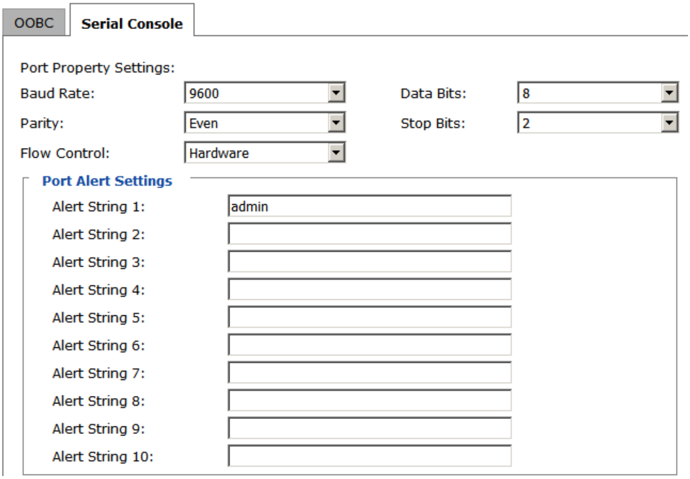
Note: This email notification differs from the one configured under *SMTP Settings* in that it uses the ISP mail server rather than the internal company’s mail server.

  - Key in the IPv4 address, IPv6 address, or domain name of your SMTP server in the *SMTP Server IP Address* field, and enter the corresponding port in the *Service Port* field.
  - If your server requires a secure SSL connection, put a check in the *SMTP server requires secure connection (SSL)* checkbox
  - If your server requires authentication, put a check in the *SMTP server requires authentication* checkbox, then key in the appropriate account name and password in the fields, below.
  - Key in the email address of the person responsible for the SMTP server (or some other equally responsible administrator), in the Email From field.
  - Key in the email address (addresses) of where you want the report sent to in the *To* field. If you are sending the report to more than one email address, separate the addresses with a comma or a semicolon.

When you have finished making your settings on this page, click **Save**.

Serial Console

To configure the RCM101D to interact with the connected serial device, you need to set its parameters to match the parameters of the device in the *Port Property Settings*.



Port Property Settings:

Baud Rate: 9600

Data Bits: 8

Parity: Even

Stop Bits: 2

Flow Control: Hardware

Port Alert Settings

Alert String 1: admin

Alert String 2:

Alert String 3:

Alert String 4:

Alert String 5:

Alert String 6:

Alert String 7:

Alert String 8:

Alert String 9:

Alert String 10:

Select the values that match the ones used by the connected serial console device. The port property settings that the RCM101D supports are as follows:

- **Baud Rate**: This sets the port's data transfer speed. Choices are from 300–38400 (drop down the list to see them all). Set this to match the baud rate setting of the serial console device. Default is 9600 (which is a basic setting for many serial console devices).
- **Data Bits**: This sets the number of bits used to transmit one character of data. Choices are: 7 and 8. Set this to match the data bit setting of the serial console device. Default is 8 (which is the default for the majority of serial console devices).
- **Parity**: This bit checks the integrity of the transmitted data. Choices are: None; Odd; Even. Set this to match the parity setting of the serial console device. Default is None.
- **Stop Bits**: This indicates that a character has been transmitted. Set this to match the stop bit setting of the serial console device. Choices are: 1 and 2. Default is 1 (which is the default for the majority of serial console devices).
- **Flow Control:** This allows you to choose how the data flow will be controlled. Choices are: None, Hardware, and XON/XOFF. Set this to match the flow control setting of the serial console device. Default is None.

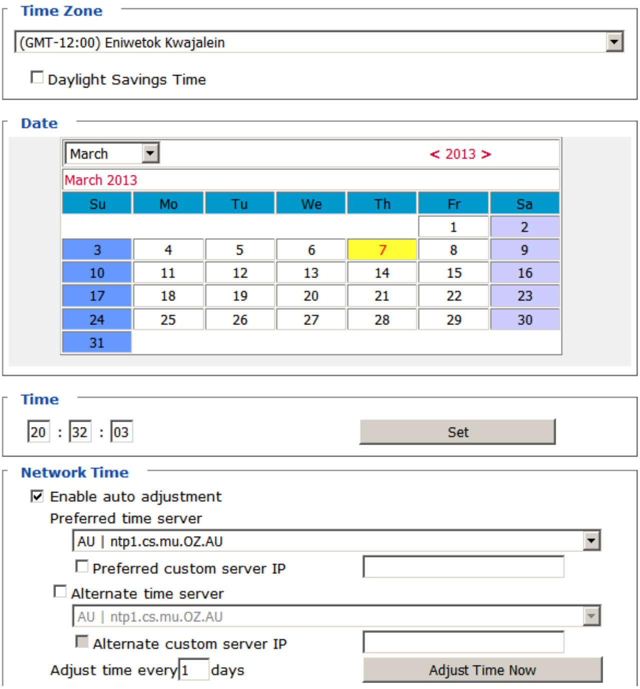
Note: None is only supported for baud rates of 9600 and lower. For baud rates greater than 9600, you must choose Hardware or XON/XOFF.

- **Port Alert Properties**: You can specify up to 10 types of events (e.g., Power On). Enter them in the provided *Alert String* (1 - 10) fields.

When you have finished making your selections, click **Save**.

Date/Time

The Date/Time dialog page sets the RCM101D time parameters:



Time Zone

(GMT-12:00) Eniwetok Kwajalein

□ Daylight Savings Time

Date

March < 2013 >

March 2013

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Time

20 : 32 : 03

Network Time

☑ Enable auto adjustment

Preferred time server

AU | ntp1.cs.mu.OZ.AU

□ Preferred custom server IP

□ Alternate time server

AU | ntp1.cs.mu.OZ.AU

□ Alternate custom server IP

Adjust time every 1 days

Set the parameters according to the information below.

Time Zone

- To establish the time zone that the RCM101D is located in, drop down the **Time Zone** list and choose the city that most closely corresponds to where it is at.
- If your country or region employs Daylight Saving Time (Summer Time), check the corresponding checkbox.

Date / Time

- Select the month from the drop-down list-box.
- Click < or > to move backward or forward by one year increments.
- In the calendar, click on the day.
- To set the time, key in the numbers using the 24 hour HH:MM:SS format.
- Click **Set** to save your settings.

Network Time

To have the time automatically synchronized to a network time server, do the following:

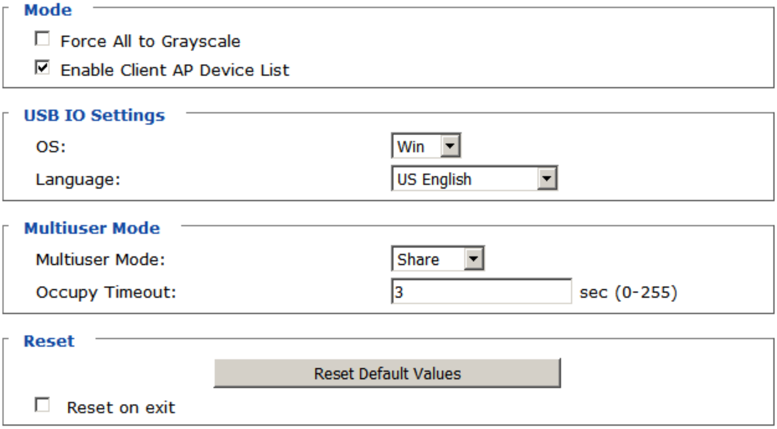
1. Check the *Enable auto adjustment* checkbox.
2. Drop down the time server list to select your preferred time server

   – or –

   Check the *Preferred custom server IP* checkbox, and key in the IP address of the time server of your choice.
3. If you want to configure an alternate time server, check the *Alternate time server* checkbox, and repeat step 2 for the alternate time server entries.
4. Key in your choice for the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

Customization

Use this section to edit the device settings.



Mode

□ Force All to Grayscale

☑ Enable Client AP Device List

USB IO Settings

OS: Win

Language: US English

Multiuser Mode

Multiuser Mode: Share

Occupy Timeout: 3 sec (0-255)

Reset

□ Reset on exit

- If *Force All to Grayscale* is enabled, the remote displays of all devices connected to the RCM101D are changed to grayscale. This can speed up I/O transfer in low bandwidth situations.
- If *Enable Client AP Device List* is enabled, the switch appears in the Server List when using the WinClient (see *The Windows Client Viewer*, page 63). If this option is not enabled, the switch can still be connected to, but its name will not appear in the Server List.
- **OS**: Specifies the operating system that the server on the connected port is using. Choices are Win, Mac, Sun, and Other. The default is Win.
- **Language**: Specifies the OS language being used by the server on the connected port. Drop down the list to see the available choices. The default is English US.
- **Multiuser Mode:** Defines how a port is to be accessed when multiple users have logged on, as follows:
  - *Exclusive*: The first user to switch to the port has exclusive control over the port. No other users can view the port.
  - *Occupy*: The first user to switch to the port has control over the port. However, additional users may view the port's video display.
  - *Share*: Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically. Under these circumstances, users can take advantage of the Message Board, which allows a user to take control of the keyboard and mouse or keyboard, mouse, and video of a Share port (see *The Message Board*, page 81).

- **Occupy Timeout**: If there is no user input for the amount of time specified here, the control privilege is released and transferred to the next user who moves the mouse or uses the keyboard.
- **Reset**: After making any network changes, be sure *Reset on exit* has been enabled (there is a check in the checkbox), before logging out. This allows network changes to take effect without having to power the switch off and on.

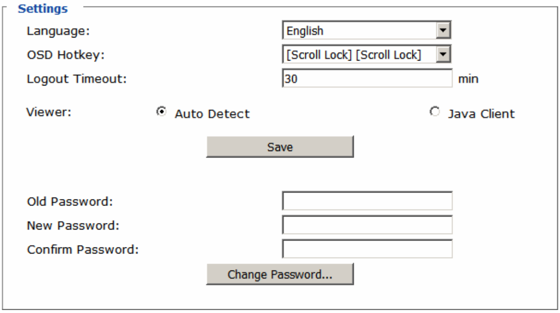
  Click *Reset Default Values* to use the default factory settings of the RCM101D.

Preferences

The following sections describe the administration utilities covered on this section, including the **User Preferences**, **Log**, **Remote Console** and **Download** screens. You can find the links to these screens under *Preferences* in the left panel menu.

User Preferences

The *User Preferences* screen allows the user to set the device password, as well as device parameters including the Language, OSD Hotkey, Logout Timeout and the Viewer.



Settings

Language: English

OSD Hotkey: [Scroll Lock] [Scroll Lock]

Logout Timeout: 30 min

Viewer: ● Auto Detect ○ Java Client

Old Password:

New Password:

Confirm Password:

Settings

Set device parameters using the following fields:

- **Language:** Selects the language that the interface displays in. Drop down the list to make your selection.

  Selecting **Auto** causes the RCM101D to display the pages in the same language to which the browser is set.

  If your browser is set to a non-supported language, the RCM101D looks to what your server's operating system is set to. If the operating system is set to a supported language it will use that language to display its pages. If the operating system is set to a non-supported language, the RCM101D defaults to English. After making your choice, click **Save**.

- **OSD Hotkey:** Select the keyboard combination to call the OSD function.
- **Logout Timeout**: Set how many minutes the RCM101D allows a user session to last before terminating the session.
- **Viewer**: Choose the viewer you would like to use when viewing the remote server's display. This is set to **Auto Detect** by default, which opens the WinClient for Windows systems.

Password

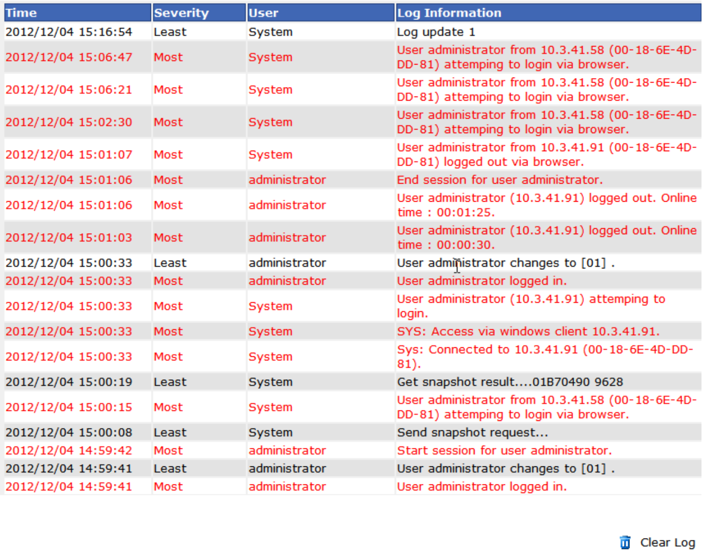
Change your password using the following fields:

- **Old Password:** Key in the old password.
- **New Password:** Key in the new password.
- **Confirm Password:** Key in the exact same characters to verify you have entered the correct new password

Click **Change Password** to apply your settings**.**

Logs

The RCM101D logs all the events that take place on it. Following a reset, it writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the center left of the page. A screen similar to the one below appears:



Time	Severity	User	Log Information
2012/12/04 15:16:54	Least	System	Log update 1
2012/12/04 15:06:47	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attemping to login via browser.
2012/12/04 15:06:21	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attemping to login via browser.
2012/12/04 15:02:30	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attemping to login via browser.
2012/12/04 15:01:07	Most	System	User administrator from 10.3.41.91 (00-18-6E-4D-DD-81) logged out via browser.
2012/12/04 15:01:06	Most	administrator	End session for user administrator.
2012/12/04 15:01:06	Most	administrator	User administrator (10.3.41.91) logged out. Online time : 00:01:25.
2012/12/04 15:01:03	Most	administrator	User administrator (10.3.41.91) logged out. Online time : 00:00:30.
2012/12/04 15:00:33	Least	administrator	User administrator changes to [01] .
2012/12/04 15:00:33	Most	administrator	User administrator logged in.
2012/12/04 15:00:33	Most	System	User administrator (10.3.41.91) attemping to login.
2012/12/04 15:00:33	Most	System	SYS: Access via windows client 10.3.41.91.
2012/12/04 15:00:33	Most	System	Sys: Connected to 10.3.41.91 (00-18-6E-4D-DD-81).
2012/12/04 15:00:19	Least	System	Get snapshot result....01B70490 9628
2012/12/04 15:00:15	Most	System	User administrator from 10.3.41.58 (00-18-6E-4D-DD-81) attemping to login via browser.
2012/12/04 15:00:08	Least	System	Send snapshot request...
2012/12/04 14:59:42	Most	administrator	Start session for user administrator.
2012/12/04 14:59:41	Least	administrator	User administrator changes to [01] .
2012/12/04 14:59:41	Most	administrator	User administrator logged in.

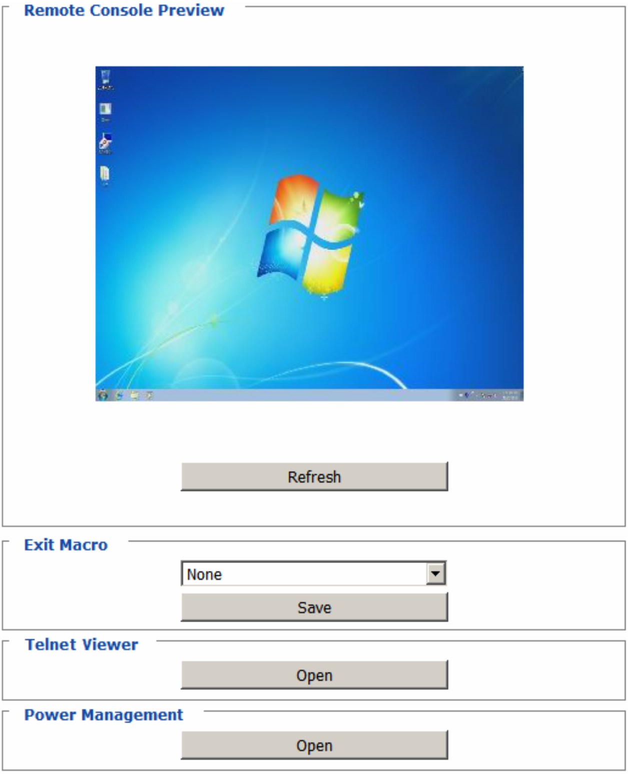
A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded.

Note: To maintain and view a record of all the events that take place (not just the most recent 512), set up the Log Server AP program. see *The Log Server*, page 99.

To clear the log file, click on the *Clear Log* icon at the lower right of the page.

Remote Console

The preview in this screen shows a snapshot of the server's display as follows:



Clicking *Refresh* updates the snapshot of the remote display.

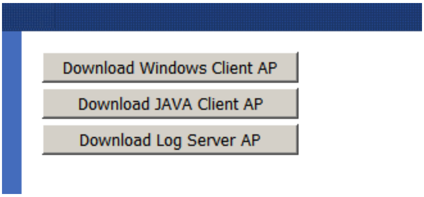
- Select the *Exit Macro* you would like to use and click **Save**.
- Telnet Viewer: Click **Open** to access the server connected to RCM101D via a built-in serial viewer for Telnet sessions.
- To configure the PN0108 (a Power Over the NET™ device), click *Open Power Management.* When connection between the devices is established, you can only use the RCM101D's IP address to access the configuration screens of the PN0108. Clicking this button opens the login page of the device.

Note: 1. Connection to the PN0108 or a Power Over the NET™ (PON) device can only be viewed and managed through the browser configuration screens; these screens are not available via the Windows or Java application (AP) programs.

2. Refer to ATEN's PN0108 User Manual (or a compatible PON device's manual) for details on editing the power management configuration screens.

Download

The Download page lets you download the standalone *Windows Client AP*, *Java client AP* and *Log Server AP*. For performance stability, if you wish to access the server, download the Windows Client Viewer from your ATEN dealer.

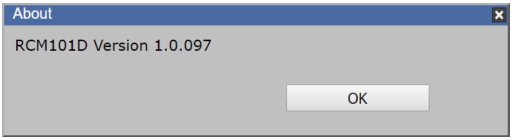


1. Click the button of the AP you want to download.
2. Follow the on-screen instructions to complete the installation and have the program icon placed on your desktop.

- For more information on the *Windows Client Viewer*, refer to *The Windows Client Viewer* on page 63.
- For details on the *Log Server AP*, refer to Chapter 8 on page 99.

About

Click *About* to see the current firmware version and copyright information of your RCM101D.



RCM101D Version 1.0.097

Logout

Click the Logout icon when you are done configuring the RCM101D's operating environment. This logs you out of the RCM101D GUI.

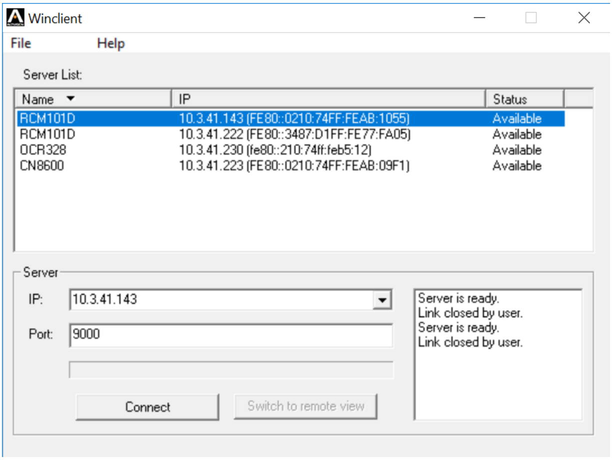
Chapter 5

The Windows Client Viewer

Starting Up

The RCM101D has a standalone windows application that opens a window on the user's desktop containing the remote server's (RCM unit) display. Follow the steps below to reach the remote server's display.

1. Download the Windows Client Viewer (hereafter abbreviated as "Winclient") from your ATEN supplier.
2. Go to the Winclient folder, locate and execute the *WinClient.exe* file. A Winclient connection window will appear as shown:



Server List:

Name	IP	Status
RCM101D	10.3.41.143 (FE80::0210:74FF:FEAB:1055)	Available
RCM101D	10.3.41.222 (FE80::3487:D1FF:FE77:FA05)	Available
OCR328	10.3.41.230 (fe80::210:74ff:feb5:12)	Available
CN8600	10.3.41.223 (FE80::0210:74FF:FEAB:09F1)	Available

IP: 10.3.41.143

Port: 9000

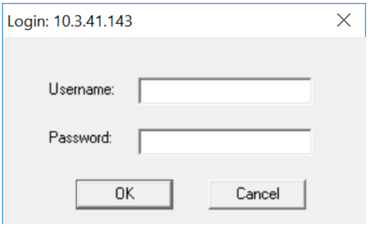
```
Server is ready.
Link closed by user.
Server is ready.
Link closed by user.
```

This window helps you select and connect to the correct server. A description of the components in the window is given in the following table:

Item	Description
Server List	Every time the Winclient is executed, it searches the user's local LAN segment for RCM101D units, and lists the found units in this box. If you want to connect to one of these units, click to select it and click **Connect**. When you have finished with your session, click **Disconnect**.

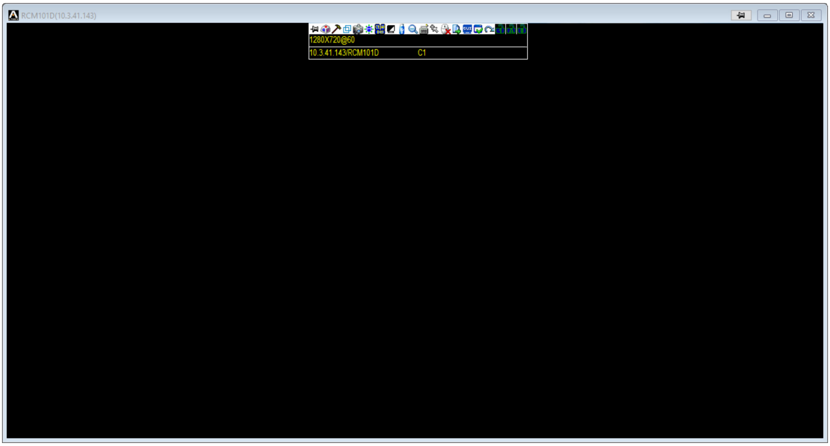
Server	Use this section if you wish to connect to a RCM101D at a remote location. Enter the IP address and the port of the unit and click **Connect**. If you don't know the Port number, contact the Administrator.
Connect / Disconnect	The button **Connect** starts the connection to the desired RCM101D. The system will prompt you to enter a username and password. Refer to step 3 below for more information. Once connected, the button becomes **Disconnect**, which you can use to disconnect from the unit.
Switch to remote view	When connected to the desired RCM101D, click this button to switch to the remote view.

3. When you click **Connect**, the system will prompt you to enter a username and password as shown:



The default username is *administrator* and password is *password*. Click **OK** to continue.

4. When you are connected, the remote server's display appears as a window on your desktop:



Navigation

You can work on the remote system via the screen display on your monitor just as if it were your local system.

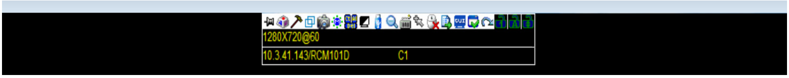
- You can maximize the window, drag the borders to resize the window; or use the scrollbars to move around the screen.
- You can switch between your local and remote programs with [Alt + Tab].

Note: 1. Due to net lag, there might be a slight delay before your keystrokes show up. You may also have to wait a bit for the remote mouse to catch up to your local mouse before you click.

2. Due to net lag, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

The WinClient Control Panel

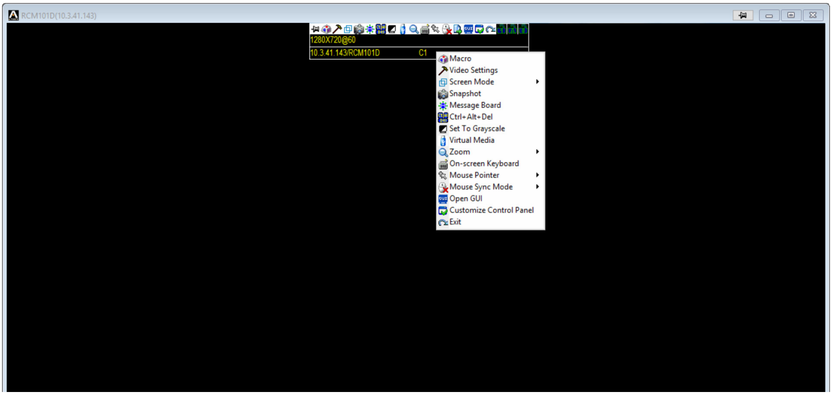
The WinClient control panel is hidden at the upper or lower center of the screen (the default is up). It becomes visible when you move the mouse pointer over it:



Note: 1. The above image shows the complete Control Panel. The icons that appear can be customized. See *Control Panel Configuration*, page 91, for details.

2. To move the Control Panel to a different location on the screen, place the mouse pointer over the text bar area, then click and drag.

- By default, the upper text row shows the video resolution of the remote display. As the mouse pointer moves over the icons in the icon bar, however, the information in the upper text row changes to describe the icon's function. In addition, if a message from another user is entered in the message board, and you have not opened the message board in your session, the message will appear in the upper row.
- The lower row shows the IP address of the device you are accessing on the left of the row. The center of the row indicates which bus the user is on (the number before the slash) and the total number of users on that bus (the number behind the slash).
- Right clicking in the text row area brings up a menu-style version of the control panel. In addition, it allows you to select options for the *Screen Mode*, *Zoom*, *Mouse Pointer*, *Mouse Sync Mode* and *Macro List* as shown by the triangles (pointing to the right) behind these options. These will be discussed in the sections that follow.



Control Panel Functions

The Control Panel functions are described in the table below.

Icon	Function
📌	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
🎲	Click to bring up the Macros dialog box (see page 69 for details).
🔨	Click to bring up the Video Options dialog box. Right-click to perform a quick Auto Sync (see *Video Settings*, page 77, for details).
⧉	Toggles the display between *Full Screen Mode* and *Windowed Mode*.
📷	Click to take a snapshot (screen capture) of the remote display. See *Snapshot*, page 92, for details on configuring the Snapshot parameters.
💬	Click to bring up the Message Board (see *The Message Board*, page 81).
Ct Al Del	Click to send a *Ctrl+Alt+Del* signal to the remote system.
◩	Click to toggle the remote display between color and grayscale.
💾	Click to bring up the *Virtual Media* dialog box. The icon changes when a virtual media device is started on the port. See *Virtual Media*, page 83, for specific details. **Note:** This icon displays in gray when the function is disabled or not available to the user.
🔍	Click to zoom the remote display window. **Note:** This feature is only available in windowed mode (Full Screen Mode is off). See *Zoom*, page 86 for details.
⌨	Click to bring up the on-screen keyboard (see *The On-Screen Keyboard*, page 87).

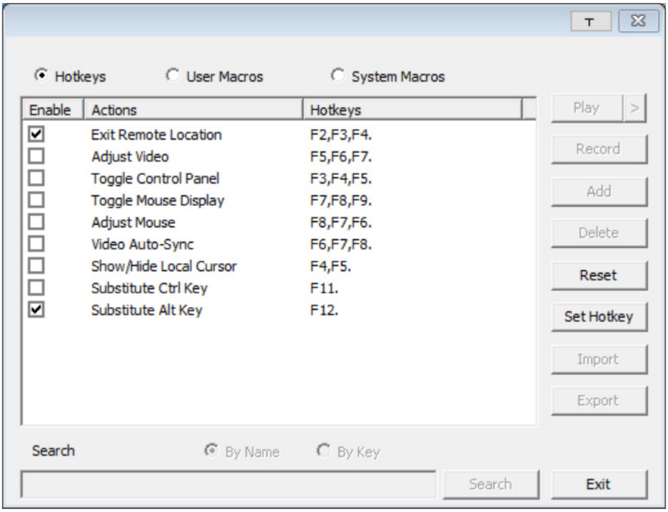
Icon	Function
	Click to select the mouse pointer type. **Note:** This icon changes depending on which mouse pointer type is selected (see *Mouse Pointer Type*, page 88).
	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is *Automatic*, a green √ appears on the icon. ◆ When the selection is *Manual*, a red X appears on the icon. See *Mouse Sync Mode*, page 88 for a complete explanation of this feature.
GUI	Under an accessed port, click to recall the GUI.
	Click to display a drop-down Macro List of *User* macros. Access and run macros more conveniently rather than using the Macros dialog box (see the *Macros* icon in the table above, and the *Macros* section on page 69).
	Click to bring up the Control Panel Configuration dialog box. See *Control Panel Configuration*, page 91, for details on configuring the Control Panel.
	Click to exit the remote view and go back to the web browser Main Page.
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is *On*, the LED is bright green and the lock hasp is closed. ◆ When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. **Note:** These icons and your local keyboard icons are in sync. Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.

Macros

The Macros icon provides access to three functions found in the Macros dialog box: Hotkeys, User Macros, and System Macros. Each of these functions is described in the following sections.

Hotkeys

Various actions corresponding to clicking the Control Panel icons, can be accomplished directly from the keyboard with hotkeys. Selecting the Hotkeys radio button lets you configure which hotkeys perform the actions. The actions are listed to the left; their hotkeys are shown to the right. Use the checkbox to the left of an action's name to enable or disable its hotkey.



● Hotkeys ○ User Macros ○ System Macros

Enable	Actions	Hotkeys
☑	Exit Remote Location	F2,F3,F4.
□	Adjust Video	F5,F6,F7.
□	Toggle Control Panel	F3,F4,F5.
□	Toggle Mouse Display	F7,F8,F9.
□	Adjust Mouse	F8,F7,F6.
□	Video Auto-Sync	F6,F7,F8.
□	Show/Hide Local Cursor	F4,F5.
□	Substitute Ctrl Key	F11.
☑	Substitute Alt Key	F12.

Search ● By Name ○ By Key

If you find the default Hotkey combinations inconvenient, you can reconfigure them as follows:

1. Highlight an *Action*, then click **Set Hotkey**.
2. Press your selected Function keys (one at a time). The key names appear in the **Hotkeys** field as you press them.
   - You can use the same function keys for more than one action, as long as the key sequence is not the same.
   - To cancel setting a hotkey value, click **Cancel**; to clear an action's Hotkeys field, click **Clear**.
3. When you have finished keying in your sequence, click **Save**.

To reset all the hotkeys to their default values, click **Reset**.

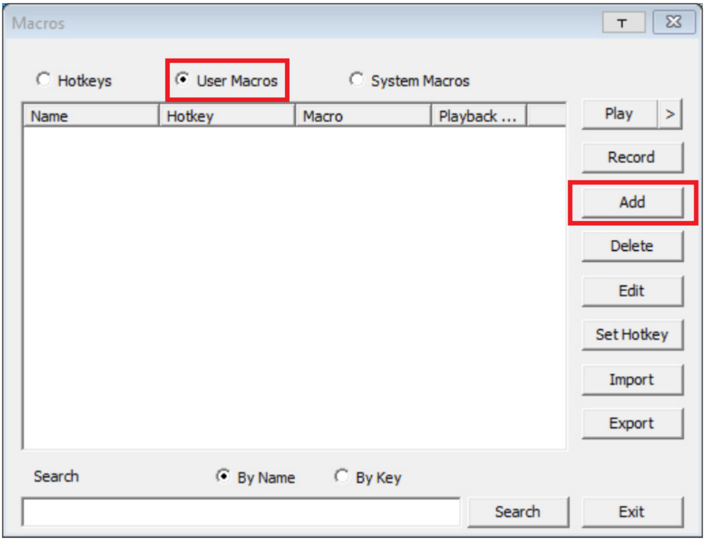
An explanation of the Hotkey actions is given in the table below:

Action	Explanation
Exit remote location	Exits the remote view and goes back to the web browser Main Page. This is equivalent to clicking the *Exit* icon on the Control Panel. The default keys are F2, F3, F4.
Adjust Video	Brings up the *Video Settings* dialog box. This is equivalent to clicking the *Video Settings* icon on the Control Panel. The default keys are F5, F6, F7.
Toggle control panel	Toggles the Control Panel **Off** and **On**. The default keys are F3, F4, F5.
Toggle mouse display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely noticeable tiny circle, which can be ignored. Since this function is a toggle, use the hotkeys again to bring the mouse display back to its original configuration. This is equivalent to selecting the *Dot* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F7, F8, F9. **Note:** The Java Control Panel does not have this feature.
Adjust mouse	This synchronizes the local and remote mouse movements. The default keys are F8, F7, F6.
Video auto-sync	This combination performs an auto-sync operation. It is equivalent to clicking the *Video Autosync* icon on the Control Panel. The default keys are F6, F7, F8.
Show/Hide Local Cursor	Toggles the display of your local mouse pointer off and on. This is equivalent to selecting the *Null* pointer type from the *Mouse Pointer* icon on the Control Panel. The default keys are F4,F5.
Substitute Ctrl key	If your local computer captures Ctrl key combinations, preventing them from being sent to the remote system, you can implement their effects on the remote system by specifying a function key to substitute for the Ctrl key. If you substitute the F11 key, for example, pressing [F11 + 5] would appear to the remote system as [Ctrl + 5]. The default key is F11.
Substitute Alt key	Although all other keyboard input is captured and sent to the remote system, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, another key may be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del]. The default key is F11.

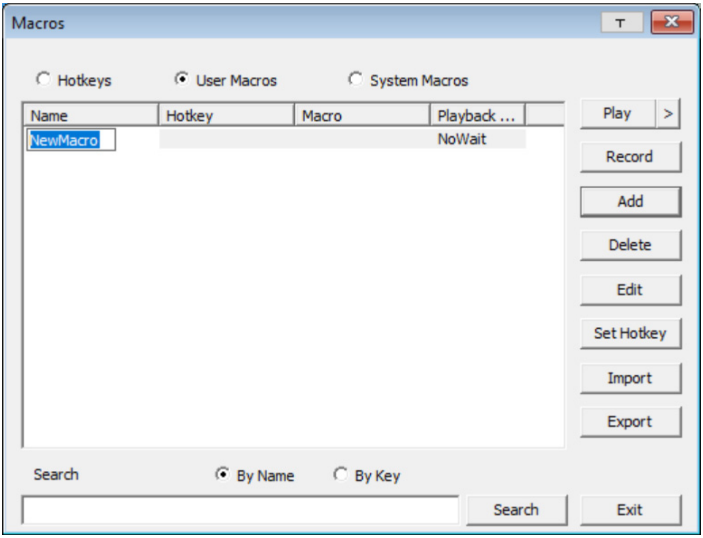
User Macros

User Macros are used to perform specific actions on the remote server. To create the macro, do the following:

1. Select the *User Macros* radio button, then click **Add**.



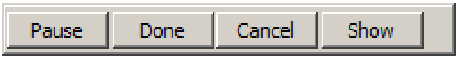
2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



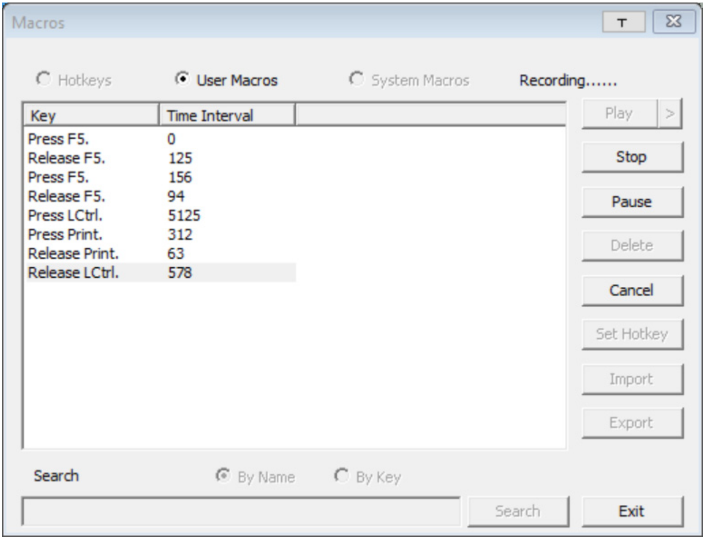
Name	Hotkey	Macro	Playback ...
NewMacro			NoWait

3. Click **Record**.

   The dialog box disappears, and a small panel appears at the top left of the screen:



4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes:



○ Hotkeys ● User Macros ○ System Macros Recording......

Key	Time Interval
Press F5.	0
Release F5.	125
Press F5.	156
Release F5.	94
Press LCtrl.	5125
Press Print.	312
Release Print.	63
Release LCtrl.	578

● By Name ○ By Key

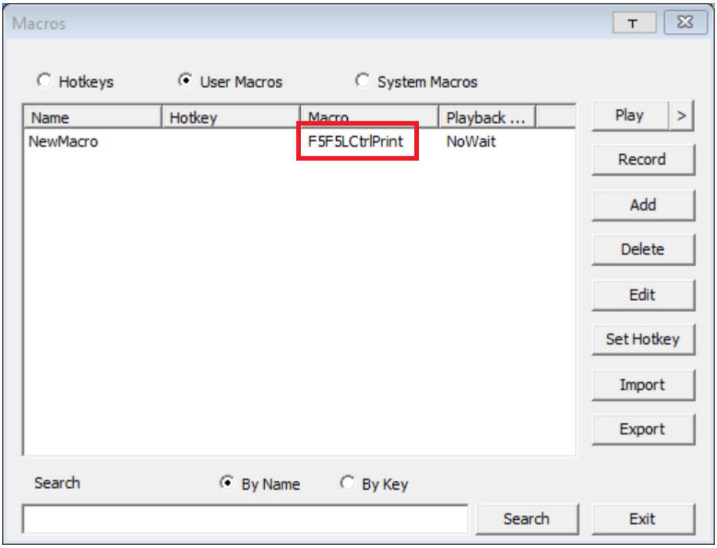
   - Clicking **Cancel** cancels all keystrokes.
   - When you have finished, click **Stop**. This is the equivalent of clicking *Done* in Step 5.

Note: 1. Case is not considered – typing **A** or **a** has the same effect.

2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.

4. If you haven't brought up the Show dialog, click **Done** when you have finished recording your macro. You return to the **Macros** dialog box shown in Step 1:



○ Hotkeys ● User Macros ○ System Macros

Name	Hotkey	Macro	Playback ...
NewMacro		F5F5LCtrlPrint	NoWait

Search ● By Name ○ By Key

5. You can give each macro a set of hotkeys, as illustrated in *Hotkeys*, page 69.

6. You can also assign the playback mode and select either **Play Without Wait** (*Nowait)* or **Play with Time Control**.

If you run the macro from this dialog box, you have the option of specifying how the macro runs.

- If you choose *Play Without Wait*, the macro runs the key presses one after another with no time delay between them.
- If you choose *Play With Time Control*, the macro waits for the amount of time between key presses that you took when you created it. Click on the arrow next to *Play* to make your choice.
- If you click *Play* without opening the list, the macro runs with the default choice. The default choice (*NoWait* or *TimeCtrl*), is shown in the *Playback* column.

7. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.

8. Repeat the procedure for any other macros you wish to create.

After creating your macros, you can run them in any of three ways:

1. By using the hotkey (if one was assigned).
2. By opening this dialog box and clicking **Play**.

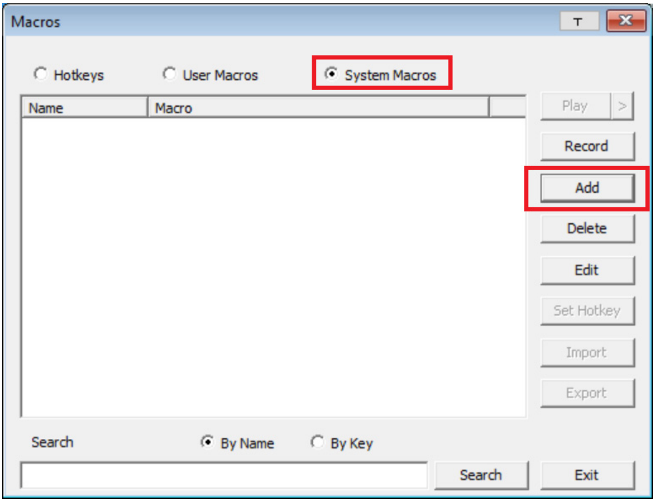
Note: User Macros are stored on the Local Client computer of each user. Therefore there is no limitation on the of number of macros, the size of the macro names, or makeup of the hotkey combinations that invoke them.

Search, at the bottom of the dialog box, lets you filter the list of macros that appear in the large upper panel for you to play or edit. Click a radio button to choose whether you want to search by name or by key; key in a string for the search; then click **Search**. All instances that match your search string appear in the upper panel.

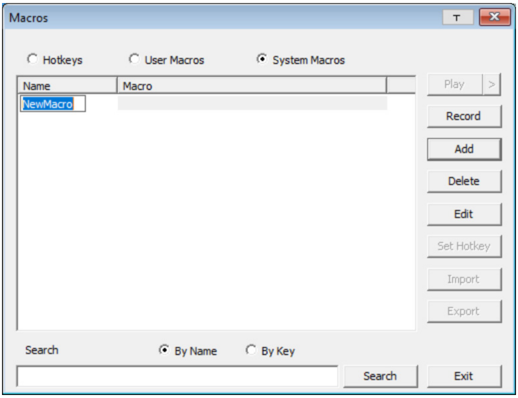
System Macros

System Macros are used to create exit macros for when you close a session. For example, as an added measure of security, you could create a macro that sends the Winkey-L combination which would cause the remote device's log in page to come up the next time the device was accessed. To create the macro, do the following:

1. Select *System Macros*, then click **Add**.

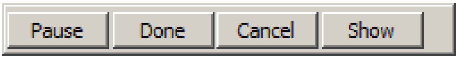


2. In the dialog box that comes up, replace the “New Macro” text with a name of your choice for the macro:



3. Click **Record**.

   The dialog box disappears, and a small panel appears at the top left of the screen:



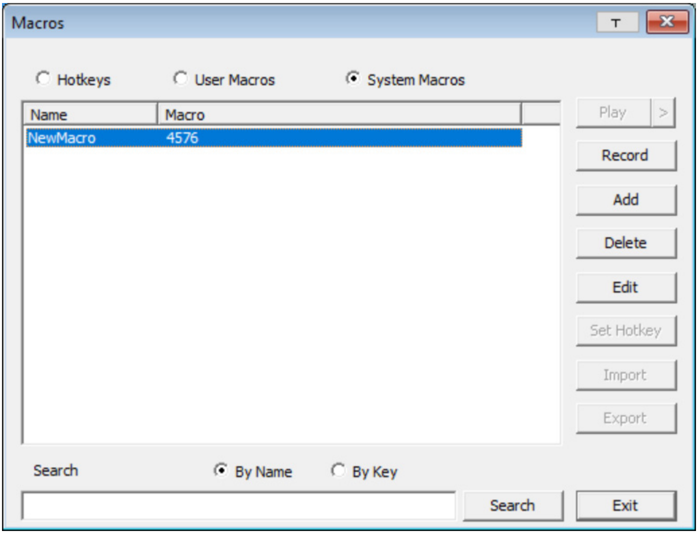
4. Press the keys for the macro.
   - To pause macro recording, click **Pause**. To resume, click **Pause** again.
   - Clicking **Show** brings up a dialog box that lists each keystroke that you make, together with the amount of time each one takes (see page 75).

Note: 1. Case is not considered – typing **A** or **a** has the same effect.

2. When recording the macro the focus must be on the remote screen. It cannot be in the macro dialog box.

3. Only the default keyboard characters may be used. Alternate characters cannot be used. For example, if the keyboard is Traditional Chinese and default character is **A** the alternate Chinese character obtained via keyboard switching is not recorded.

4. If you haven't brought up the **Show** dialog, click **Done** when you have finished recording your macro. You return to the Macros dialog box with your system macro key presses displayed in the Macro column:



○ Hotkeys ○ User Macros ● System Macros

Name	Macro
NewMacro	4576

Search ● By Name ○ By Key

5. If you want to change any of the keystrokes, select the macro and click **Edit**. This brings up a dialog box similar to the one for Show. You can change the content of your keystrokes, change their order, etc.

6. Repeat the procedure for any other macros you wish to create.

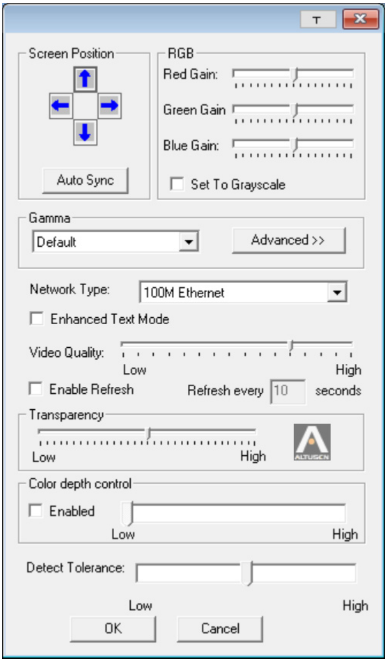
Once the system macros have been created, you can choose to run any one them upon logging out of the RCM101D (see *Customization*, page 59 for details).

Note: 1. Information about the Search function is given on page 74.

2. Systems macros are stored on the RCM101D, therefore macro names may not exceed 64 English alphanumeric character, and hotkey combinations may not exceed 256 Bytes (each key usually takes 3–5 Bytes).

Video Settings

The *Video Settings* dialog box allows you to adjust the placement and picture quality of the remote screen display on your monitor.



Gamma: Default

Network Type: 100M Ethernet

Refresh every 10 seconds

The adjustment options are as follows:

Option	Usage
T	Click this to control the transparency of the Video Settings dialog box.
Screen Position	Adjust the horizontal and vertical position of the remote server window by clicking the arrow buttons.
Auto Sync	Click Auto Sync to have the vertical and horizontal offset values of the remote screen detected and automatically synchronized with the local screen. **Note:** 1. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. 2. This function works best with a bright screen. 3. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually.

Option	Usage
RGB	Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When an RGB value is increased, the RGB component of the image is correspondingly increased. If you enable *Set to Grayscale*, the remote video display is changed to grayscale.
Gamma	This section allows you to adjust the video display's gamma level. If default gamma level is not ideal, you can click the drop-down menu for a list of preset gamma levels and select from it. There are ten preset and four user-defined levels to choose from. To define the user-defined levels, click the **Advanced** button. This function is discussed in detail in the next section.
Performance	Select the type of internet connection that exists between the Local Client computer and the RCM101D. The RCM101D will use that selection to automatically adjust the *Video Quality* and *Detect Tolerance* settings to optimize the quality of the video display. Since network conditions vary, if none of the pre-set choices seem to work well, you can select *Customize* and use the **Video Quality** and **Detect Tolerance** slider bars to adjust the settings to suit your conditions.
Enhanced Text Mode	Check this to solve video display problems related to video screen resolution that affect some interface systems (e.g., Sun Blade 1000 servers).
Video Quality	Drag the slider bar to adjust the overall Video Quality. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely effect response time.
Enable Refresh	The system can redraw the screen every 1 to 99 seconds, eliminating unwanted artifacts from the screen. Select **Enable Refresh** and enter a number from 1 through 99. The system will redraw the screen at the interval you specify. This feature is disabled by default. Check the checkbox next to *Enable Refresh* to enable this feature. **Note:** 1. The system starts counting the time interval when mouse movement stops. 2. Enabling this feature increases the volume of video data transmitted over the network. The lower the number specified, the more often the video data is transmitted. Setting too low a value may adversely affect overall operating responsiveness.
Transparency	Adjusts the transparency of the toolbar that comes up when the GUI hotkey ([Scroll Lock][Scroll Lock], for example) is invoked. Slide the bar until the display in the example window is to your liking.

Option	Usage
Color Depth Control	This setting determines the richness of the video display by adjusting the amount of color information.
Detect Tolerance	This setting also relates to video quality. It governs detecting or ignoring pixel changes. A high setting can result in a lower quality display due to less data transfer. A lower setting will result in better video quality, but setting the threshold too low may allow too much data to be transferred, negatively impacting network performance.

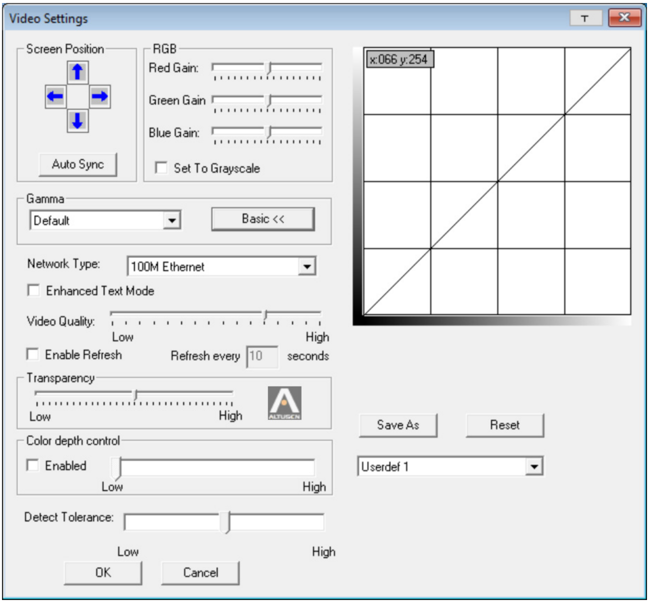
Click **OK** to save your changes and close the dialog box.

Click **Cancel** to abandon your changes and close the dialog box.

Gamma Adjustment

If it is necessary to correct the gamma level for the remote video display, use the Gamma function of the Video Adjustment dialog box.

For greater control, clicking the **Advanced** button brings up the following dialog box:



Video Settings

Gamma: Default

Network Type: 100M Ethernet

☐ Enhanced Text Mode

☐ Enable Refresh   Refresh every 10 seconds

☐ Set To Grayscale

Color depth control: ☐ Enabled

x:066 y:254

Userdef 1

This section allows you to adjust the video display's gamma level.

Click and drag the diagonal line at as many points as you wish to achieve the display output you desire.

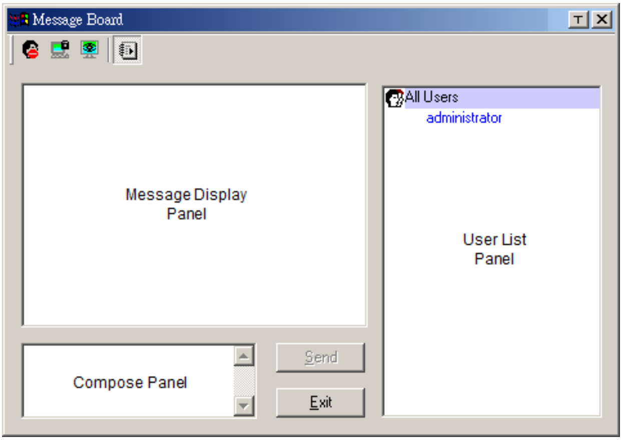
If a gamma level is desirable, click **Save As** to save the current configuration as one of the four user-defined configurations. Saved configurations can be recalled from the list box at a future time.

Click **Reset** to abandon any changes and return the gamma line to its original diagonal position.

Note: For best results, change the gamma while viewing a remote computer.

The Message Board

To alleviate the possibility of access conflicts resulting from multiple user logins, the RCM101D provides a message board that allows users to communicate with each other:



Buttons on the Top

The buttons on the top are toggles. Their actions are described in the table below:

Button	Action
	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The button is shadowed when Chat is disabled. The icon displays next to the user's name in the User List panel when the user has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When a port is set to *Occupy* mode (see *Working Mode*, page 49), you can use this button to occupy the KVM. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The button is shadowed when the KVM is occupied. The icon displays next to the user's name in the User List panel when the user has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When a port is set to *Occupy* mode (see *Working Mode*, page 49), you can use this button to occupy the KM. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed when the KM is occupied. The icon displays next to the user's name in the User List panel when the user has occupied the KM.
	Show/Hide User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.

Message Display Panel

Messages that users post to the board - as well as system messages - display in this panel. If you disable Chat, however, messages that get posted to the board won't appear.

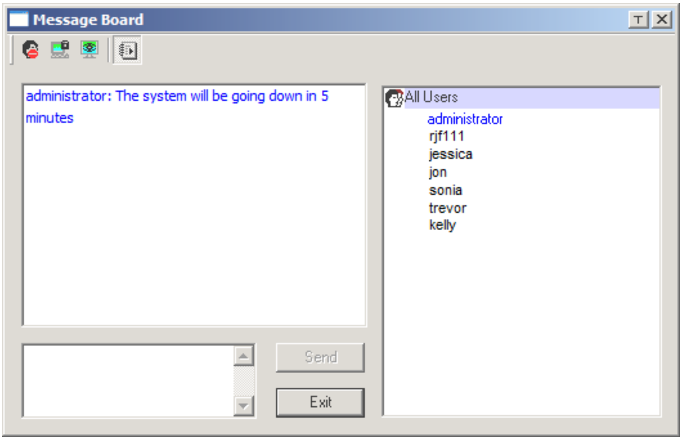
Compose Panel

Key in the messages that you want to post to the board in this panel. Click **Send**, or press [**Enter**] to post the message to the board.

User List Panel

The names of all the logged in users are listed in this panel.

- Your name appears in blue; other users' names appear in black.
- By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- If a user's name is selected, and you want to post a message to all users, select **All Users** before sending your message.
- If a user has disabled Chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.



administrator: The system will be going down in 5 minutes

Virtual Media

The *Virtual Media* feature allows a drive, folder, image file, or removable disk on a local client computer to appear and act as if it were installed on the remote server. Virtual Media also supports a smart card reader function that allows a reader plugged into a local client computer to appear as if it were plugged into the remote server.

Virtual Media Icons

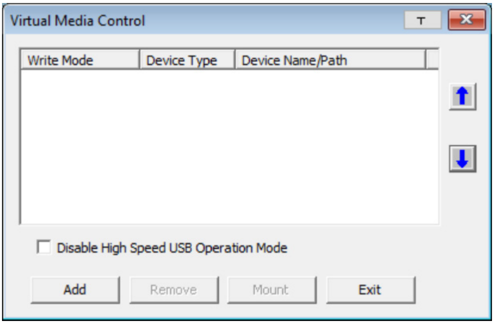
The *Virtual Media* icon on the **WinClient Control Panel** changes to indicate whether the virtual media function is available, or if a virtual media device has already been mounted on the remote server, as shown in the table below:

Icon	Function
	The icon displays in gray to indicate that the virtual media function is disabled or not available.
	The icon displays in blue to indicate that the virtual media function is available. Click the icon to bring up the virtual media dialog box.
	The icon displays in blue with a red **X** to indicate that a virtual media device has been mounted on the remote server. Click the icon to unmount all redirected devices.

Virtual Media Redirection

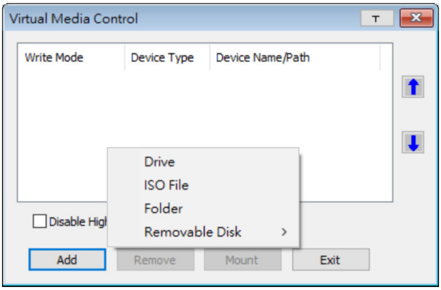
To implement the virtual media redirection feature, do the following:

1. Click the Virtual Media icon to bring up the *Virtual Media* dialog box:



□ Disable High Speed USB Operation Mode

2. Click **Add**, then select the media source.



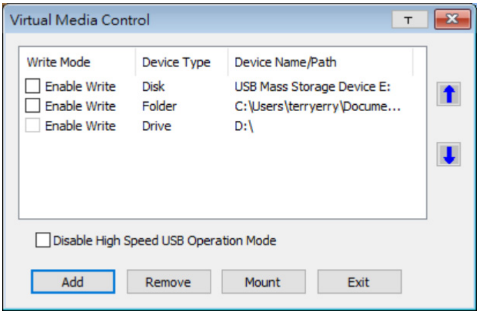
Depending on your selection, additional dialog boxes appear enabling you to select the drive, file, folder, or removable disk you desire. See *Virtual Media Support*, page 133 for details about mounting these media types.

3. If your device only supports full speed USB, check the *Disable High Speed USB Operation Mode* checkbox.

4. To add additional media sources, repeat the steps above. There is no limit to how many media sources you can add.

   The system recognizes up to three virtual media sources and the top three in the list are the ones that are selected. Virtual Media and Smart Card Readers (see *Smart Card Reader* on page 86) can be mounted at the same time. To rearrange the selection order, highlight the device you want to move, then click the **Up** or **Down** Arrow button to promote or demote it in the list.

5. *Read* refers to the redirected device being able to send data to the remote server; *Write* refers to the redirected device being able to have data from the remote server written to it. The default is for **Write** to not be enabled (Read only). If you want the redirected device to be writable as well as readable, click to put a check in the *Enable Write* checkbox:


Virtual Media Control

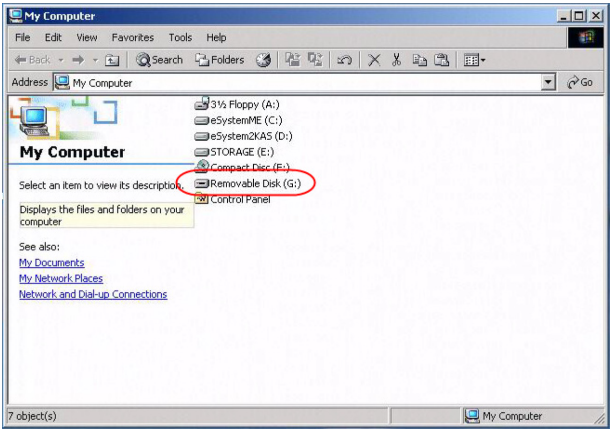
Write Mode	Device Type	Device Name/Path
□ Enable Write	Disk	USB Mass Storage Device E:
□ Enable Write	Folder	C:\Users\terryerry\Docume...
□ Enable Write	Drive	D:\

□ Disable High Speed USB Operation Mode

Note: 1. If a redirected device cannot be written to, or if a user does not have write permissions, it appears in gray and cannot be selected.

2. See *Virtual Media Support*, page 133, for a list of supported virtual media types.

6. To remove an entry from the list, highlight it and click **Remove**.
7. After you have made your media source selections, click **Mount**. The dialog box closes. The virtual media devices that you have selected are redirected to the remote system, where they show up as drives, files and folders on the remote system's file system.



Select an item to view its description.

Displays the files and folders on your computer

7 object(s)

Once mounted, you can treat the virtual media as if they were really on the remote server – drag and drop files to/from them; open files on the remote system for editing and save them to the redirected media, etc.

Files that you save to the redirected media, will actually be saved on your local system. Files that you drag from the redirected media will actually come from your local system.

8. To end the redirection, bring up the *Control Panel* and click on the *Virtual Media* icon. All mounted devices are automatically unmounted.

Smart Card Reader

Note: This feature is only available when using the *WinClient Viewer* or the *Windows Client AP*.

The smart card reader function allows a reader plugged into a local client computer's USB port to be redirected, and appear as if it were plugged into the remote server. One purpose of smart cards (Common Access Cards, for example) is to allow authentication to the remote server from the local client.

When a smart card reader is connected to the local client computer, an entry for it appears when you click **Add** in the **Virtual Media** dialog box.

Note: If you mount a smart card reader, you cannot mount any other virtual media device. If any virtual media devices are already mounted, you must unmount them before you can mount the smart card reader.

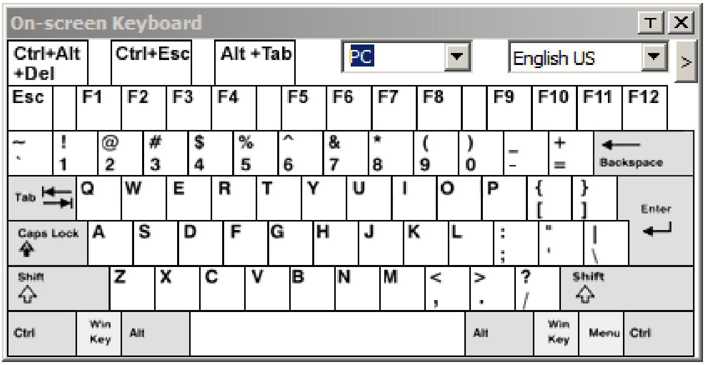
Zoom

The *Zoom* icon controls the zoom factor for the remote view window. Settings are as follows:

Setting	Description
100%	Sizes and displays the remote view window at 100%.
75%	Sizes and displays the remote view window at 75%.
50%	Sizes and displays the remote view window at 50%.
25%	Sizes and displays the remote view window at 25%.
1:1	Sizes and displays the remote view window at 100%. The difference between this setting and the 100% setting is that when the remote view window is resized its contents don't resize – they remain at the size they were. To see any objects that are outside of the viewing area move the mouse to the window edge, to have the screen scroll.

The On-Screen Keyboard

The RCM101D supports an on-screen keyboard, available in multiple languages, with all the standard keys for each supported language. Click this icon to pop up the on-screen keyboard:

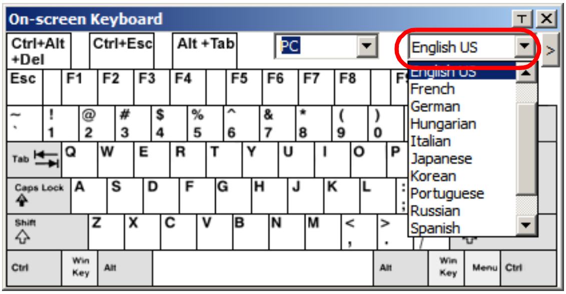

On-screen Keyboard
Ctrl+Alt +Del
Ctrl+Esc
Alt +Tab
PC
English US
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12
~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Backspace
Tab Q W E R T Y U I O P { [}] Enter
Caps Lock A S D F G H J K L : ; " ' | \
Shift Z X C V B N M < , > . ? / Shift
Ctrl Win Key Alt Alt Win Key Menu Ctrl

One of the major advantages of the on-screen keyboard is that if the keyboard languages of the remote and local systems are not the same, you do not have to change the configuration settings for either system. The user just has to bring up the on-screen keyboard; select the language used by the computer on the port he is accessing; and use the on-screen keyboard to communicate with it.

Note: You must use your mouse to click on the keys. You cannot use your actual keyboard.

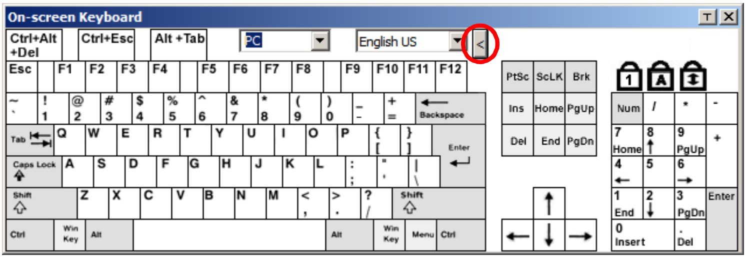
To change languages, do the following:

1. Click the down arrow next to the currently selected language to drop down the language list.



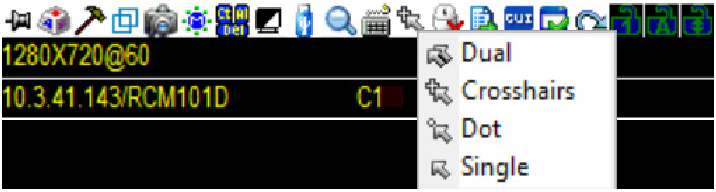
2. Select the new language from the list.

To display/hide the expanded keyboard keys, click the arrow to the right of the language list arrow.



Mouse Pointer Type

The RCM101D offers a number of mouse pointer options when working in the remote display. Click this icon to select the type that you would like to work with:



Note: The icon on the Control Panel changes to match your choice.

Mouse Sync Mode

Clicking this icon selects whether synchronization of the local and remote mouse pointers is accomplished either automatically or manually.

The icon on the toolbar indicates the synchronization mode status as follows:

Icon	Function
✓	The green check mark indicates that Mouse DynaSync is **enabled**. This is the default setting when Mouse DynaSync is available.
✗	The red X indicates that Mouse DynaSync is **disabled** and is on manual sync mode.

When *Mouse DynaSync is available,* clicking the icon toggles its status between enabled and /disabled. If you choose to disable Mouse DynaSync mode, you must use the manual syncing procedures described in the next section.

Automatic Mouse Synchronization (DynaSync)

Mouse DynaSync provides automatic locked-in synching of the remote and local mouse pointers – eliminating the need to constantly resync the two movements.

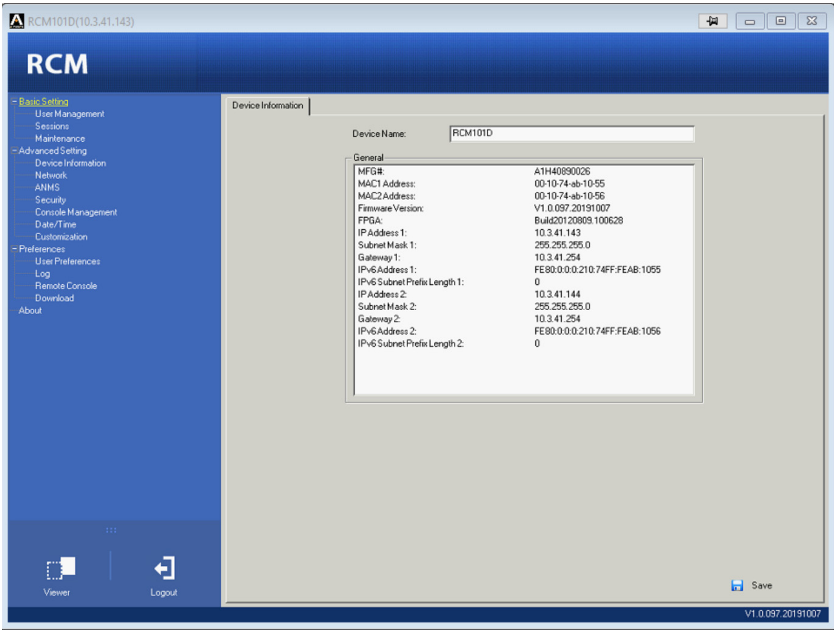
Manual Mouse Synchronization

If you are using Manual mouse synchronization instead of automatic DynaSync and the local mouse pointer goes out of sync with the remote system's mouse pointer, there are a number of methods to bring them back into sync:

1. Perform a video and mouse auto sync by clicking the *Video Settings* icon on the Control Panel (see page 77).
2. Perform an **Auto Sync** with the Video Adjustment function (see *Video Settings*, page 77, for details).
3. Invoke the **Adjust Mouse** function with the *Adjust Mouse* hotkeys (see *Adjust mouse*, page 70, for details).
4. Move the pointer into all 4 corners of the screen (in any order).
5. Drag the Control Panel to a different position on the screen.
6. Set the mouse speed and acceleration for each problematic computer attached to the switch. See *Additional Mouse Synchronization Procedures*, page 130, for instructions.

Open GUI

Clicking the *Open GUI* icon brings up a window that allows you to configure the RCM101D via viewer-based GUI with the web browser administrative functionalities:



Device Name: RCM101D

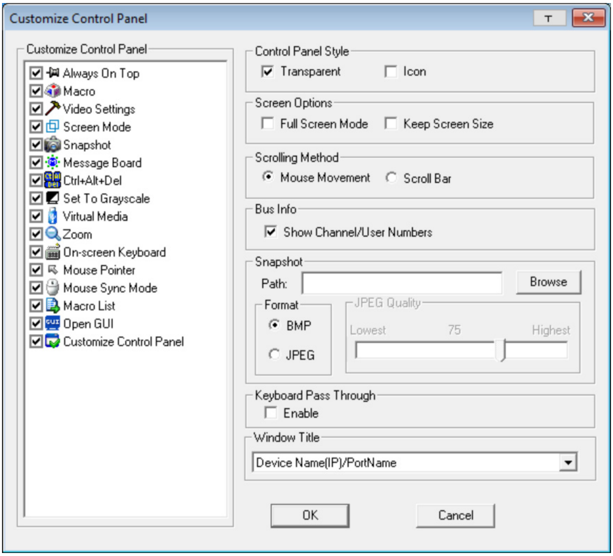
General

MFG#:	A1H40890026
MAC1 Address:	00-10-74-ab-10-55
MAC2 Address:	00-10-74-ab-10-56
Firmware Version:	V1.0.097.20191007
FPGA:	Build20120809.100628
IP Address 1:	10.3.41.143
Subnet Mask 1:	255.255.255.0
Gateway 1:	10.3.41.254
IPv6 Address 1:	FE80:0:0:0:210:74FF:FEAB:1055
IPv6 Subnet Prefix Length 1:	0
IP Address 2:	10.3.41.144
Subnet Mask 2:	255.255.255.0
Gateway 2:	10.3.41.254
IPv6 Address 2:	FE80:0:0:0:210:74FF:FEAB:1056
IPv6 Subnet Prefix Length 2:	0

The Administrator Utility is essentially the same as the browser-based version. See Chapter 4, *Configuration* for information on these pages.

Control Panel Configuration

Clicking the *Customize Control Panel* icon brings up a dialog box that allows you to configure the items that appear on the Control Panel, as well as its graphical settings:



Customize Control Panel

Customize Control Panel
- ☑ Always On Top
- ☑ Macro
- ☑ Video Settings
- ☑ Screen Mode
- ☑ Snapshot
- ☑ Message Board
- ☑ Ctrl+Alt+Del
- ☑ Set To Grayscale
- ☑ Virtual Media
- ☑ Zoom
- ☑ On-screen Keyboard
- ☑ Mouse Pointer
- ☑ Mouse Sync Mode
- ☑ Macro List
- ☑ Open GUI
- ☑ Customize Control Panel

Control Panel Style: ☑ Transparent ☐ Icon

Screen Options: ☐ Full Screen Mode ☐ Keep Screen Size

Scrolling Method: ● Mouse Movement ○ Scroll Bar

Bus Info: ☑ Show Channel/User Numbers

Snapshot
Path:
Format: ● BMP ○ JPEG
JPEG Quality: Lowest 75 Highest

Keyboard Pass Through: ☐ Enable

Window Title: Device Name(IP)/PortName

The dialog box is organized into five main sections as described in the table below:

Item	Description
Customize Control Panel	Allows you to select which icons display in the Control Panel
Control Panel Style	◆ Enabling *Transparent* makes the Control Panel semi-transparent, so that you can see through it to the display underneath. ◆ Enabling *Icon* causes the Control Panel to display as an icon until you mouse over it. When you mouse over the icon, the full panel comes up.

Item	Description
Screen Options	◆ If **Full Screen Mode** is enabled, the remote display fills the entire screen. ◆ If **Full Screen Mode** is not enabled, the remote display appears as a window on the client desktop. If the remote screen is larger than what is able to fit in the window, scroll bars will appear. ◆ If **Keep Screen Size** is enabled, the remote screen is not resized. ◆ If the remote resolution is smaller than that of the client monitor, its display appears like a window centered on the screen. ◆ If the remote resolution is larger than that of the client monitor, its display is scaled to the client monitor size. ◆ If **Keep Screen Size** is not enabled, the remote screen is resized to fit the client monitor's resolution.
Scrolling Method	In cases where the remote screen display is larger than your monitor, you can choose how to scroll to the areas that are off-screen. ◆ If you select *Mouse Movement*, the screen will scroll when you move the mouse pointer to your screen border. ◆ If you select *Scroll Bars*, scroll bars appear around the screen borders that you can use to scroll to the off-screen areas.
Bus Info	If *Bus Info* is enabled, the number of the bus you are on, as well as the total number of users on the bus, displays on the bottom row center of the Control Panel as follows: Bus No./Total Users. (See the Control Panel diagram on page 66 for an example.)
Snapshot	These settings let the user configure the RCM101D's screen capture parameters (see the *Snapshot* description under *The WinClient Control Panel*, page 66): ◆ Path lets you select a directory that the captured screens automatically get saved to. Click **Browse**; navigate to the directory of your choice; then click **OK**. If you don't specify a directory here, the snapshot is saved to your desktop. ◆ Click a radio button to choose whether you want the captured screen to be saved as a BMP or a JPEG (JPG) file. ◆ If you choose JPEG, you can select the quality of the captured file with the slider bar. The higher the quality, the better looking the image, but the larger the file size.
Keyboard Pass Through	When this is enabled, the Alt-Tab key press is passed to the remote server and affects that server. If it is not enabled, Alt-Tab acts on your local client computer.
Window Title	For the drop-down menu, you can choose how much information is displayed for the remote server.

Chapter 6
Local Console

The RCM101D can be accessed directly from a local console's keyboard/ mouse/monitor or via a laptop application (AP) program at the local site.

Console Lock Switch

The switch on the RCM101D rear panel lets you select how the mini USB port operates.

Set the switch to LUC to use the mini USB port as a Laptop USB Console port. This lets you conveniently configure the RCM101D directly at the local site simply by connecting a laptop to the port. With the laptop, you can then access and edit the RCM101D application. See p. 94 for more details on how to use the Laptop USB Console feature.

Note: You can also set the mini USB port so that it functions as a Virtual Media port. See p. 83 for more details.

Local Console

Use the keyboard, mouse and monitor to directly access and operate the local console port. The RCM101D is able to split the signal to both the local and remote consoles.

- The local console has priority by default. Refer to **Console Lock Switch** on page 11.
- To configure concurrent usage for the local console user and remote console user(s), refer to **Multiuser Mode** on page 59.

Message Tag

When a remote user logs on to the RCM101D, a message tag displays in the local console. This serves as a reminder to the local user that operations may be affected. Close the message tag by pressing the ESC key.

If the local user does not want operations to be disrupted, make sure the **Console Lock Switch** is locked to the local console. The message tag does not appear in this case.

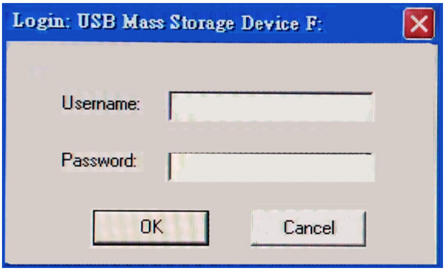
Laptop USB Console

To use the mini USB port for Laptop USB Console (LUC) operations, set the switch at the rear panel of the RCM101D to **LUC**.

Note: The LUC function only works for Windows systems.

The laptop application (AP) program for operating the LUC is built into the RCM101D's firmware and does not require a download. To access the switch, do the following:

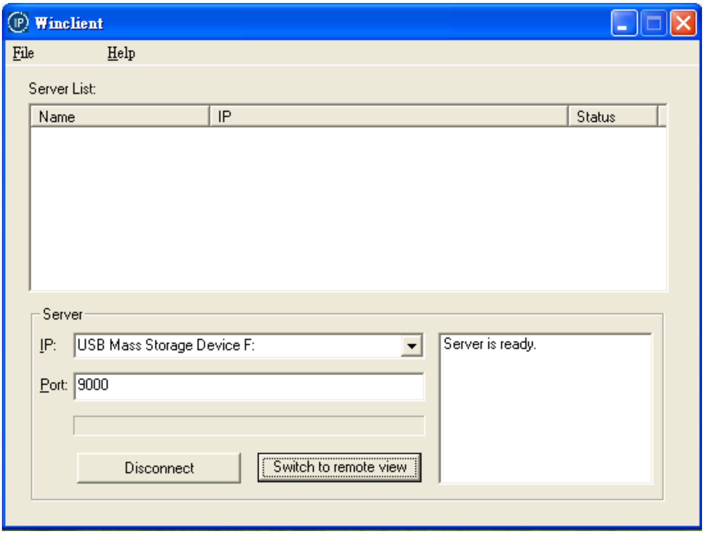
1. Use the USB 2.0 cable (A-type to mini USB) included in the package to connect your laptop to the RCM101D's mini USB port, located on the unit's rear panel (see *Installation*, page 15).
2. The RCM101D appears as a virtual drive in the laptop's file system. Locate the Laptop AP on the virtual CD ROM and double-click the icon. The login screen appears.



3. At the login screen, key in your valid Username and Password, then click **Login. Once you** have logged in successfully, the **Remote View** button becomes active.
4. Click **Remote View** to bring up the Laptop Console Main Page.

Laptop USB Console Main Page

After connecting a laptop to the RCM101D's Laptop port, logging in, and opening the AP, the Laptop Console main page appears.



IP: USB Mass Storage Device F:

Port: 9000

Server is ready.

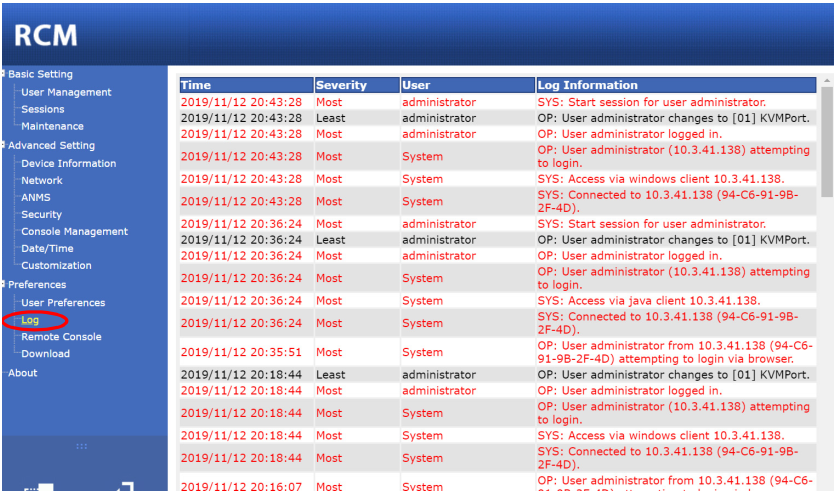
The Laptop Console Main Page is similar to the Web Browser and WinClient Main Pages. Refer to the *The Windows Client Viewer* on page 63 throughout the rest of the manual regarding operations.

This Page Intentionally Left Blank

Chapter 7
The Log File

The Log File Screen

The RCM101D logs all the events that take place on it. Following a reset, it writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the center left of the page. A screen similar to the one below appears:



Time	Severity	User	Log Information
2019/11/12 20:43:28	Most	administrator	SYS: Start session for user administrator.
2019/11/12 20:43:28	Least	administrator	OP: User administrator changes to [01] KVMPort.
2019/11/12 20:43:28	Most	administrator	OP: User administrator logged in.
2019/11/12 20:43:28	Most	System	OP: User administrator (10.3.41.138) attempting to login.
2019/11/12 20:43:28	Most	System	SYS: Access via windows client 10.3.41.138.
2019/11/12 20:43:28	Most	System	SYS: Connected to 10.3.41.138 (94-C6-91-9B-2F-4D).
2019/11/12 20:36:24	Most	administrator	SYS: Start session for user administrator.
2019/11/12 20:36:24	Least	administrator	OP: User administrator changes to [01] KVMPort.
2019/11/12 20:36:24	Most	administrator	OP: User administrator logged in.
2019/11/12 20:36:24	Most	System	OP: User administrator (10.3.41.138) attempting to login.
2019/11/12 20:36:24	Most	System	SYS: Access via java client 10.3.41.138.
2019/11/12 20:36:24	Most	System	SYS: Connected to 10.3.41.138 (94-C6-91-9B-2F-4D).
2019/11/12 20:35:51	Most	System	OP: User administrator from 10.3.41.138 (94-C6-91-9B-2F-4D) attempting to login via browser.
2019/11/12 20:18:44	Least	administrator	OP: User administrator changes to [01] KVMPort.
2019/11/12 20:18:44	Most	administrator	OP: User administrator logged in.
2019/11/12 20:18:44	Most	System	OP: User administrator (10.3.41.138) attempting to login.
2019/11/12 20:18:44	Most	System	SYS: Access via windows client 10.3.41.138.
2019/11/12 20:18:44	Most	System	SYS: Connected to 10.3.41.138 (94-C6-91-9B-2F-4D).
2019/11/12 20:16:07	Most	System	OP: User administrator from 10.3.41.138 (94-C6-

A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded.

Note: To maintain and view a record of all the events that take place (not just the most recent 512), set up the Log Server AP program. see *The Log Server*, page 99.

To clear the log file, click on the *Clear Log* icon at the lower right of the page.

This Page Intentionally Left Blank

Chapter 8
The Log Server

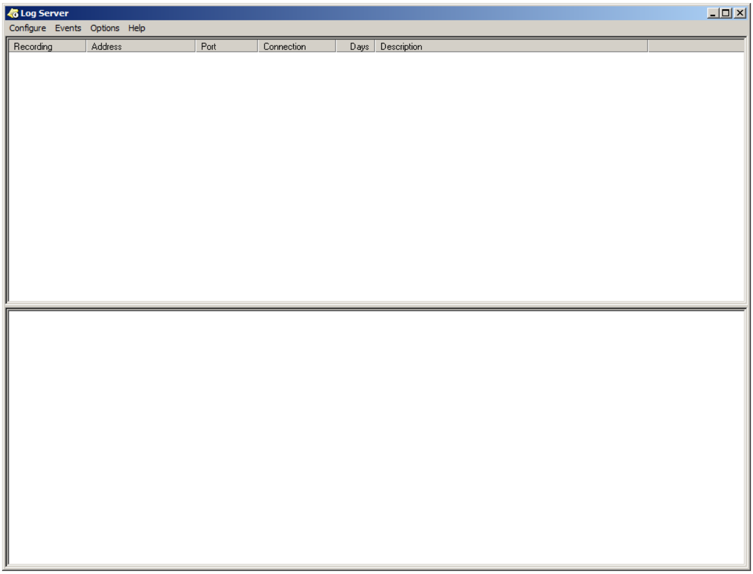
The Log Server is a Windows-based administrative utility that records all the events that take place on selected RCM101D units and writes them to a searchable database. This chapter describes how to install and configure the Log Server.

Installation

1. In the web GUI, go to the Download page. Refer to *Download*, page 64 for more details.
2. Click the **Download Log Server AP** button.
3. Follow the on-screen instructions to complete the installation and have the Log Server program icon placed on your desktop.

Starting Up

To bring up the Log Server, either double click the program icon, or key in the full path to the program on the command line. The first time you run it, a screen similar to the one below appears:



Note: 1. The MAC address of the Log Server computer must be specified in the *ANMS* settings – see *Log Server*, page 40 for details.

2. The Log Server requires the Microsoft Jet OLEDB 4.0 driver. See *The Log Server*, page 129 if the program does not start.

The screen is divided into three components:

- A *Menu Bar* at the top
- A panel that will contain a list of RCM101D units in the middle (see *The Log Server Main Screen*, page 105, for details).
- A panel that will contain an *Events List* at the bottom

Each of the components is explained in the sections that follow.

The Menu Bar

The Menu bar consists of four items:

- Configure
- Events
- Options
- Help

These are discussed in the sections that follow.

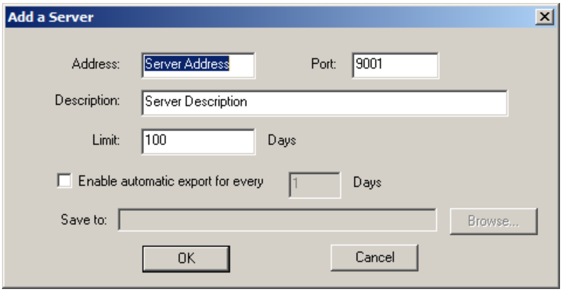
Note: If the Menu Bar appears to be disabled, click in the RCM101D List window to enable it.

Configure

The Configure menu contains three items: Add, Edit, and Delete. They are used to add new RCM101D units to the RCM101D List, edit the information for units already on the list, or delete RCM101D units from the list.

- To add a RCM101D to the RCM101D List, click **Add**.
- To edit or delete a listed RCM101D, first select the one you want in the RCM101D List window, then open this menu and click **Edit** or **Delete**.

When you choose *Add* or *Edit*, a dialog box, similar to the one below appears:



Add a Server

Address: Server Address

Port: 9001

Description: Server Description

Limit: 100 Days

□ Enable automatic export for every 1 Days

Save to:

A description of the fields is given in the table, below:

Field	Explanation
Address	This can either be the IP address of the RCM101D or its DNS name (if the network administrator has assigned it a DNS name). Key in the value specified for the RCM101D in the *ANMS* settings (see *ANMS*, page 38).
Port	Key in the port number that was specified for the Log Server's *Service Port* in the *ANMS* settings (see *Log Server*, page 40).
Description	This field is provided so that you can put in a descriptive reference for the unit to help identify it.
Limit	This specifies the number of days that an event should be kept in the Log Server's database before it expires and it is cleared out.
Enable automatic export for every (*) Days	Check this to have the server create a log file at specific intervals (in Days), and save it to your specified location. Click the **Browse...** button and navigate to the file folder where you want the log file to be stored.

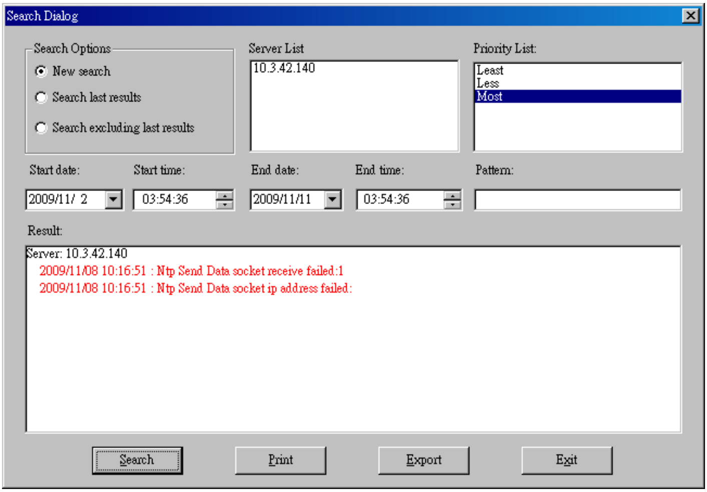
Fill in or modify the fields, then click **OK** to finish.

Events

The Events Menu has two items: *Search* and *Maintenance*.

Search

Search allows you to search for events containing specific words or strings. When you access this function, a screen similar to the one below appears:



Search Dialog

Search Options

● New search

○ Search last results

○ Search excluding last results

Server List: 10.3.42.140

Priority List: Least, Less, Most

Start date: 2009/11/ 2

Start time: 03:54:36

End date: 2009/11/11

End time: 03:54:36

Pattern:

Result:

```
Server: 10.3.42.140
  2009/11/08 10:16:51 : Ntp Send Data socket receive failed:1
  2009/11/08 10:16:51 : Ntp Send Data socket ip address failed:
```

A description of the items is given in the table below:

Item	Explanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected RCM101D.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected RCM101D *excluding* the events that resulted from the last search.
Server List	RCM101D units are listed according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority List	Sets the level for how detailed the search results display should be. *Least* is the most general; *Most* is the most specific. Least results appear in black; Less results appear in blue; Most results appear in red.

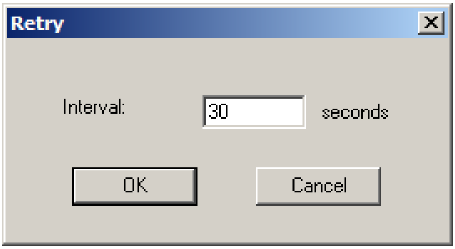
Start Date	Select the date that you want the search to start from. The format follows the YYYY/MM/DD convention, as follows: 2009/11/04
Start Time	Select the time that you want the search to start from.
End Date	Select the date that you want the search to end at.
End Time	Select the time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (*) is supported. E.g., h*ds would match *hands* and *hoods*.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results.
Export	Click this button to write the search results to a .txt file.
Exit	Click this button to exit the Search dialog box.

Maintenance

This function allows the administrator to perform manual maintenance of the database, such as erasing specified records before the expiration time that was set with the *Limit* setting of the Edit function (see page 102).

Options

Network Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect if the previous attempt to connect failed. When you click this item, a dialog box, similar to the one below appears:



Interval: 30 seconds

Key in the number of seconds, then click **OK** to finish.

Help

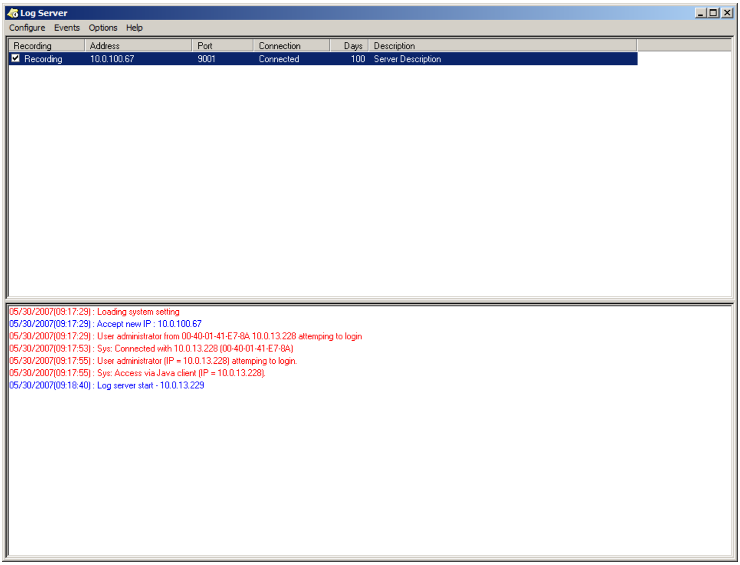
From the Help Menu, click Contents to access the online Windows Help file. The help file contains instructions about how to setup, operation and troubleshoot the Log Server.

The Log Server Main Screen

Overview

The Log Server Main Screen is divided into two main panels.

- The upper (List) panel lists the RCM101D units that have been selected for the Log Server to track (see *Configure*, page 102).
- The lower (Event) panel displays the log events for the currently selected RCM101D (the highlighted one - if there are more than one). To select a RCM101D unit in the list, simply click on it.



Recording	Address	Port	Connection	Days	Description
☑ Recording	10.0.100.67	9001	Connected	100	Server Description

```
05/30/2007(09:17:29) : Loading system setting
05/30/2007(09:17:29) : Accept new IP : 10.0.100.67
05/30/2007(09:17:29) : User administrator from 00-40-01-41-E7-8A 10.0.13.228 attemping to login
05/30/2007(09:17:53) : Sys: Connected with 10.0.13.228 (00-40-01-41-E7-8A)
05/30/2007(09:17:55) : User administrator (IP = 10.0.13.228) attemping to login.
05/30/2007(09:17:55) : Sys: Access via Java client (IP = 10.0.13.228).
05/30/2007(09:18:40) : Log server start - 10.0.13.229
```

The List Panel

The List panel contains six fields:

Field	Explanation
Recording	Determines whether the Log Server records log events for this RCM101D or not. If the Recording check box is checked, the field displays *Recording*, and log events are recorded. If the Recording check box is not checked, the field displays *Paused*, and log events are not recorded. **Note:** Even though a RCM101D is not the currently selected one, if its Recording check box is checked, the Log Server will still record its log events.
Address	This is the IP Address or DNS name that was given to the RCM101D when it was added to the Log Server (see *Configure*, page 102).
Port	This is the port number that was assigned to the RCM101D when it was added to the Log Server (see *Configure*, page 102).
Connection	If the Log Server is connected to the RCM101D, this field displays *Connected*. If it is not connected, this field displays *Waiting*. This means that the Log Server's MAC address and/or port number has not been set properly. It needs to be set in the *ANMS* settings (see page 38) and specified in the *Configure* dialog box (see *Configure*, page 102).
Days	This field displays the number of days that the RCM101D's log events are to be kept in the Log Server's database before expiration (see *Configure*, page 102).
Description	This field displays the descriptive information given for the RCM101D when it was added to the Log Server (see *Configure*, page 102).

Panel Showing Logs of the Selected

The lower panel displays the log information of the selected RCM101D. Note that if the installation contains more than one switch, even though a switch is not currently selected, if its *Recording* checkbox is checked, the Log Server records its tick information and keeps it in its database.

Appendix

Safety Instructions

General

- This product is for indoor use only.
- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- To prevent damage to your installation it is important that all devices are properly grounded.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the

extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or un-interruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Inlet power cord selection: Detachable, maximum 2.0 m long, 18 AWG, flexible cord (125V, 10A, 3C, NEMA 5-15P). Or, 0.75mm^2, 3G, flexible cord (E.g.: H05VV-F, 250V 10A).

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Make sure that all equipment used on the rack – including power strips and other electrical connectors – is properly grounded.
- Ensure that proper airflow is provided to devices in the rack.
- Ensure that the operating ambient temperature of the rack environment does not exceed the maximum ambient temperature specified for the equipment by the manufacturer
- Do not step on or stand on any device when servicing other devices in a rack.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://eservice.aten.com**
- For telephone support, see *Telephone Support*, page iv.

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://eservice.aten.com
Telephone Support		1-888-999-ATEN ext 4988 1-949-428-1111

When you contact us, please have the following information ready beforehand:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information you feel may be of help.

IP Address Determination

If you are an administrator logging in for the first time, you need to access the RCM101D in order to give it an IP address that users can connect to. There are several methods to choose from. In each case, your computer must be on the same network segment as the RCM101D. After you have connected and logged in you can give the RCM101D its fixed network address. (See *Network*, page 34.)

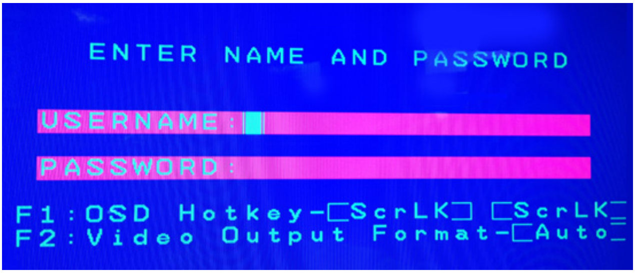
Local IP Setup

Use the local console to set the IP address. All procedures start from the OSD Main Screen.

1. To display the Main Screen, tap [Scroll Lock] twice.

Note: [Scroll Lock] is the default OSD hotkey. You can optionally change the Hotkey to the Ctrl key.

The login screen appears:



```
ENTER NAME AND PASSWORD

USERNAME :

PASSWORD :

F1 : OSD Hotkey-[ScrLK] [ScrLK]
F2 : Video Output Format-[Auto]
```

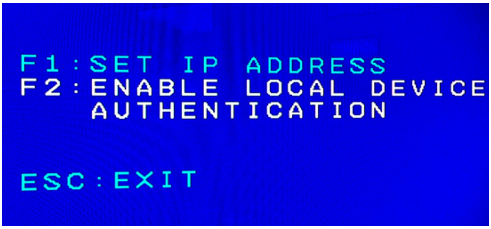
From this screen, you can select the following options:

- Press **F1** to change the hotkey for invoking the OSD screen. You can change the Hotkey to the Ctrl key instead of the Scroll lock key (shown as *ScrLK* in the screen).
- Press **F2** to select the video output format for the remote display, which includes AUTO, DVI and HDMI.

2. Enter a valid **Username** and **Password** to continue.

   The default username is *administrator*; the default password is *password.* The first time you log in, you must use these defaults. For security purposes, we strongly recommend that you change the default password to something unique.

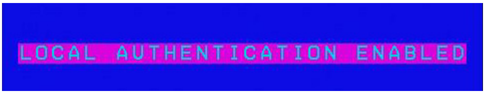
3. In the screen that appears, press **F1** to set the IP address. Proceed to step 4.



```
F1:SET IP ADDRESS
F2:ENABLE LOCAL DEVICE
   AUTHENTICATION

ESC:EXIT
```

Press **F2** to enable the RCM101D to authenticate users. The RCM101D allows authentication and authorization through external programs. If the external programs fail to authenticate and you cannot log on to the device, use the local console to transfer authentication to the RCM101D. The following message displays when the operation is successful.

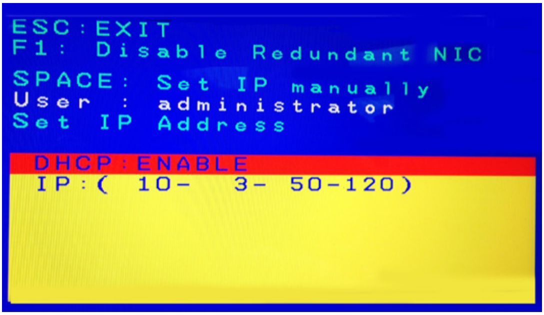


```
LOCAL AUTHENTICATION ENABLED
```

See *Authentication*, page 41 for details.

Press the **Esc** key to exit the local console.

4. When you invoke the OSD, a screen similar to the one below appears:

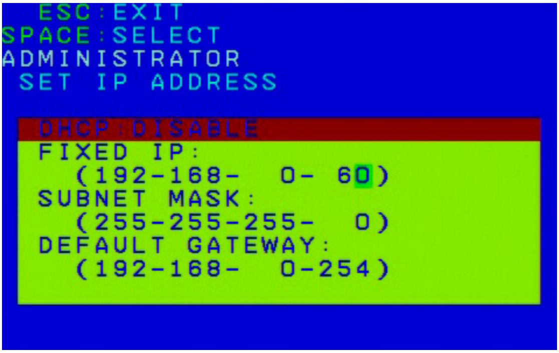


```
ESC:EXIT
F1:  Disable Redundant NIC
SPACE:  Set IP manually
User  :  administrator
Set IP Address

 DHCP:ENABLE
 IP:( 10-  3- 50-120)
```

- To move up or down through the list one screen at a time, Click the Up and Down Arrow symbols (↑↓), or use the [Pg Up] and [Pg Dn] keys.
- To select or confirm a value, press the space bar [Space].
- To dismiss the menu, and deactivate OSD, press [Esc].

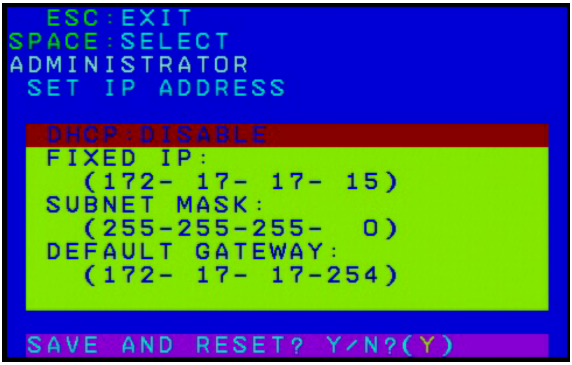
5. From the list, select **DHCP: Enable** and hit the space bar to toggle enabling or disabling the DHCP server. It should change to **DHCP: Disable** with additional fields, as follows:



```
  ESC:EXIT
SPACE:SELECT
ADMINISTRATOR
 SET IP ADDRESS

 DHCP:DISABLE
 FIXED IP:
   (192-168-  0- 60)
 SUBNET MASK:
   (255-255-255-  0)
 DEFAULT GATEWAY:
   (192-168-  0-254)
```

6. For the fields **Fixed IP**, **Subnet Mask**, and **Default Gateway**, select each choice and enter the numerical address (dotted quad address).



```
  ESC:EXIT
SPACE:SELECT
ADMINISTRATOR
 SET IP ADDRESS

 DHCP:DISABLE
 FIXED IP:
   (172- 17- 17- 15)
 SUBNET MASK:
   (255-255-255-  0)
 DEFAULT GATEWAY:
   (172- 17- 17-254)

 SAVE AND RESET? Y/N?(Y)
```

7. Go to **Save and Reset** and enter **Y** to confirm the new IP address.

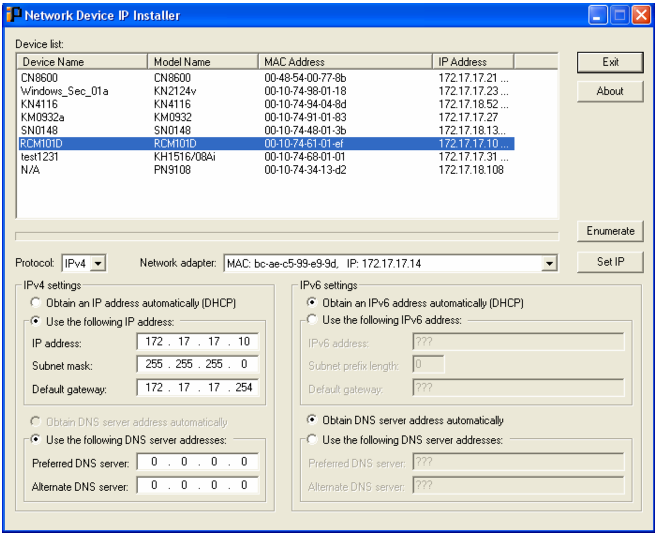
IP Installer

The IP Installer utility provides a simple method to ascertain and configure IP related settings for ATEN network enabled devices.

The utility can be obtained from the *Download* area of our website. Look under *Download - Driver & Software*, and select the model of your switch. After downloading the utility to your client computer, do the following:

1. Unzip the contents of *IPInstaller.zip* to a directory on your hard drive.

2. Double click *IPInstaller.exe,* and the following screen appears:



Device list:

Device Name	Model Name	MAC Address	IP Address
CN8600	CN8600	00-48-54-00-77-8b	172.17.17.21 ...
Windows_Sec_01a	KN2124v	00-10-74-98-01-18	172.17.17.23 ...
KN4116	KN4116	00-10-74-94-04-8d	172.17.18.52 ...
KM0932a	KM0932	00-10-74-91-01-83	172.17.17.27
SN0148	SN0148	00-10-74-48-01-3b	172.17.18.13...
RCM101D	RCM101D	00-10-74-61-01-ef	172.17.17.10 ...
test1231	KH1516/08Ai	00-10-74-68-01-01	172.17.17.31 ...
N/A	PN9108	00-10-74-34-13-d2	172.17.18.108

Protocol: IPv4   Network adapter: MAC: bc-ae-c5-99-e9-9d, IP: 172.17.17.14

IPv4 settings
○ Obtain an IP address automatically (DHCP)
● Use the following IP address:
IP address: 172 . 17 . 17 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 172 . 17 . 17 . 254
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 0 . 0 . 0 . 0
Alternate DNS server: 0 . 0 . 0 . 0

IPv6 settings
● Obtain an IPv6 address automatically (DHCP)
○ Use the following IPv6 address:
IPv6 address: ???
Subnet prefix length: 0
Default gateway: ???
● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: ???
Alternate DNS server: ???

Network Device IP Installer

The way that the IP Installer works is that it searches and lists all compatible ATEN devices on your network. You can select a model from the *Device List* and set it's IP Address settings using the options listed below, then click **Set IP** to implement the change on the device.

Device List

When the IP Installer main window comes up, the utility scans the network for devices and lists the ones it finds in the device list panel. The device list panel consists of four columns, as shown in the following table:

Heading	Details
Device Name	Displays the device name assigned to the switch.
Model Name	Displays the switches model name (RCM101D, PN9108, SN0116, etc.).
MAC Address	Displays the device's MAC address.
IP Address	Displays the device's current IP address.

Clicking **Enumerate** causes the utility to broadcast an *Enumerate* command and wait for replies from all the devices. It then refreshes the list based on the response it receives.

Protocol

Use this drop-down box to select the type of protocol **IPv4** or **IPv6**, you are using for the network adapters on your LAN.

Network Adapter

The Network Adapter selection box, located just below the Device List, pertains to computers that have more than one network adapter installed. Users can use this to select the adapter that they want Enumerate to be directed to.

Set IP

There are two methods of specifying an IP address: *Dynamic*, and *Static*:

- If you want to obtain an IP address dynamically, select *Obtain an IP address automatically (DHCP)*.
- If you want to use a static IP address, select *Specify an IP address*, then fill in the information for:
  - **IPv4**: IP Address, Subnet Mask, and Gateway.
  - **IPv6**: IPv6 Address, Subnet Prefix Length, and Default Gateway

After you have made your changes, click **Set IP** to set the IP address for the device you have selected.

Note: The screen will freeze for a moment or two until the utility has finished setting the IP.

About

Clicking the *About* button brings up a dialog box with information about the product – including the current firmware version.

Browser

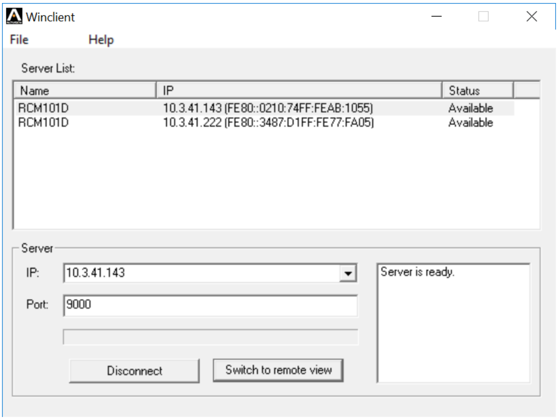
1. Set your client computer's IP address to 192.168.0.*XXX*

   Where *XXX* represents any number or numbers except 60. (192.168.0.60 is the default address of the RCM101D.)

2. Specify the switch's default IP address (192.168.0.60) in your browser, and you will be able to connect.
3. Assign a fixed IP address for the RCM101D that is suitable for the network segment that it resides on.
4. After you log out, reset your client computer's IP address to its original value.

AP Windows Client

For computers running Windows, the RCM101D's IP address can be determined with the Windows AP program (see *The Windows Client AP*, page 91). When you run the program it searches the network segment for RCM101D devices, and displays the results in a dialog box similar to the one below:



Server List:

Name	IP	Status
RCM101D	10.3.41.143 (FE80::0210:74FF:FEAB:1055)	Available
RCM101D	10.3.41.222 (FE80::3487:D1FF:FE77:FA05)	Available

IP: 10.3.41.143

Port: 9000

Server is ready.

You can now use this network address, or you can change it by logging in (clicking **Connect**), or clicking **Open GUI**, and then clicking *Network* under the Advanced Settings menu. See *Network*, page 34, for details.

IPv6

At present, the RCM101D supports two IPv6 address protocols: *Link Local IPv6 Address*, and *IPv6 Stateless Autoconfiguration*

Link Local IPv6 Address

At power on, the RCM101D is automatically configured with a Link Local IPv6 Address (for example, fe80::210:74ff:fe61:1ef). To find out what the Link Local IPv6 Address is, log in with the RCM101D's IPv4 address and click the *Basic Setting* icon. The address is displayed at the bottom of the *Basic Setting* page (see page 24).

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[fe80::2001:74ff:fe6e:59%5]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
fe80::2001:74ff:fe6e:59%5
```

for the *IP* field of the *Server* panel (see *The Windows Client Connection Screen*, page 92).

Note: 1. To log in with the Link Local IPv6 Address, the client computer must be on the same local network segment as the RCM101D

2. The %5 is the %interface used by the client computer. To see your client computer's IPv6 address: from the command line issue the following command: `ipconfig /all`. The % value appears at the end of the IPv6 address.

IPv6 Stateless Autoconfiguration

If the RCM101D's network environment contains a device (such as a router) that supports the IPv6 Stateless Autoconfiguration function, the RCM101D can obtain its prefix information from that device in order to generate its IPv6 address. For example, 2001::74ff:fe6e:59.

As above, the address is displayed at the bottom of the *Basic Setting* page.

Once you have determined what the IPv6 address is, you can use it when logging in from a browser or the Win and Java Client AP programs.

For example:

If you are logging in from a browser, you would key in

```
http://[2001::74ff:fe6e:59]
```

for the URL bar.

If you are logging in with the AP program, you would key:

```
2001::74ff:fe6e:59
```

for the *IP* field of the *Server* panel (see *The Windows Client Connection Screen*, page 92).

Port Forwarding

For devices located behind a router, port forwarding allows the router to pass data coming in over a specific port to a specific device. By setting the port forwarding parameters, you tell the router which device to send the data coming in over a particular port to.

For example, if the RCM101D connected to a particular router has an IP address of 192.168.1.180, you would log into your router's setup program and access the Port Forwarding (sometimes referred to as *Virtual Server*) configuration page. You would then specify 192.168.1.180 for the IP address and the port number you want opened for it (9000 for internet access, for example).

Since configuration setup can vary somewhat for each brand of router, refer to the router's User Manual for specific information on configuring port forwarding for it.

Keyboard Emulation

The PC compatible (101/104 key) keyboard can emulate the functions of the Sun and Mac keyboards. The emulation mappings are listed in the table below.

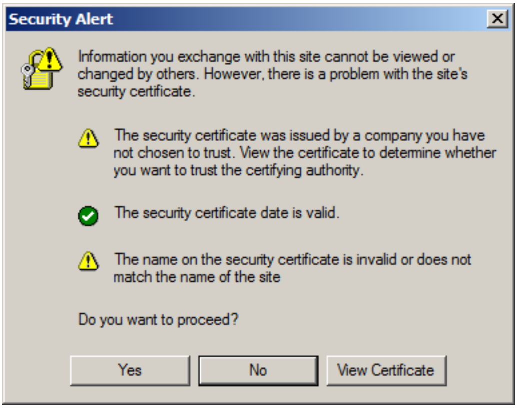
PC Keyboard	Sun Keyboard	PC Keyboard	Mac Keyboard
[Ctrl] [T]	Stop	[Shift]	Shift
[Ctrl] [F2]	Again	[Ctrl]	Ctrl
[Ctrl] [F3]	Props	⊞	⌘
[Ctrl] [F4]	Undo	[Ctrl] [1]	🔈
[Ctrl] [F5]	Front	[Ctrl] [2]	🔉
[Ctrl] [F6]	Copy	[Ctrl] [3]	🔊
[Ctrl] [F7]	Open	[Ctrl] [4]	⏏
[Ctrl] [F8]	Paste	[Alt]	Alt
[Ctrl] [F9]	Find	[Print Screen]	F13
[Ctrl] [F10]	Cut	[Scroll Lock]	F14
[Ctrl] [1]	▭ 🔇	▤	=
[Ctrl] [2]	◑ - 🔉	[Enter]	Return
[Ctrl] [3]	◑ + 🔊	[Backspace]	Delete
[Ctrl] [4]	☾	[Insert]	Help
[Ctrl] [H]	Help	[Ctrl] ⊞	F15
▤	Compose		
⊞	◆		

Note: When using key combinations, press and release the first key (Ctrl), then press and release the activation key.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

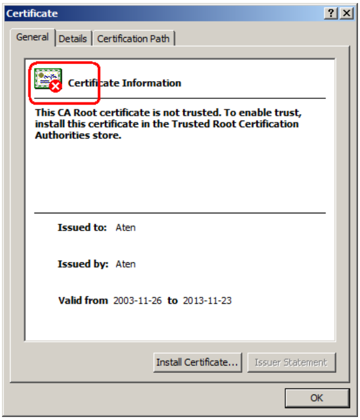
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- If you are working on a computer at another location, accept the certificate for just this session by clicking **Yes.**
- If you are working at your own computer, install the certificate on your computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Installing the Certificate

To install the certificate, do the following:

3. In the *Security Alert* dialog box, click **View Certificate.** The *Certificate Information* dialog box appears:



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Aten

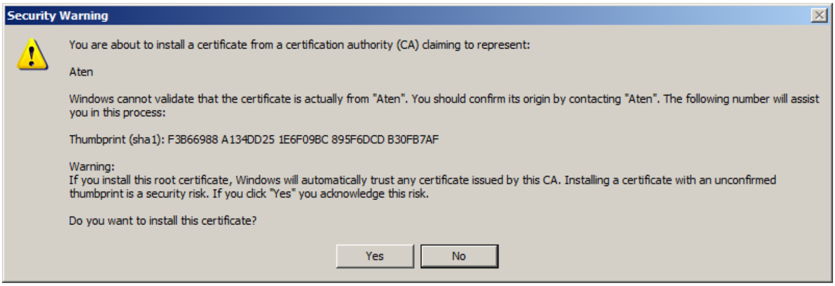
Issued by: Aten

Valid from 2003-11-26 **to** 2013-11-23

Note: There is a red and white **X** logo over the certificate to indicate that it is not trusted.

---

4. Click **Install Certificate.**
5. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
6. When the Wizard presents a caution screen:



You are about to install a certificate from a certification authority (CA) claiming to represent:

Aten

Windows cannot validate that the certificate is actually from "Aten". You should confirm its origin by contacting "Aten". The following number will assist you in this process:

Thumbprint (sha1): F3B66988 A134DD25 1E6F09BC 895F6DCD B30FB7AF

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

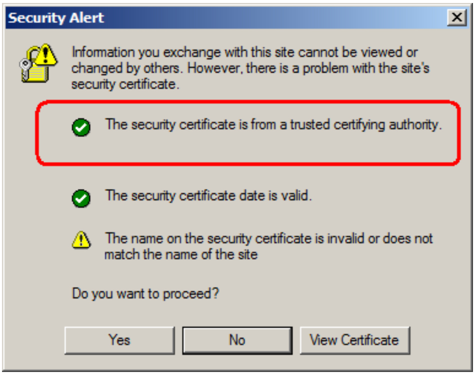
Do you want to install this certificate?

Click **Yes**.

7. Next, click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

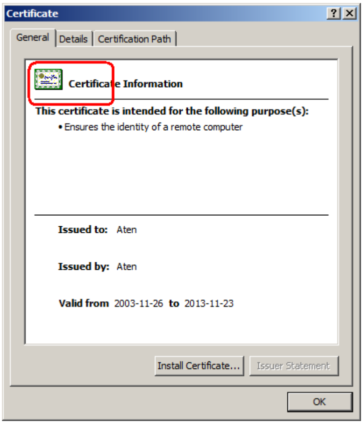
✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

When you click *View Certificate*, you can see that the red and white **X** logo is no longer present – further indication that the certificate is trusted:



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

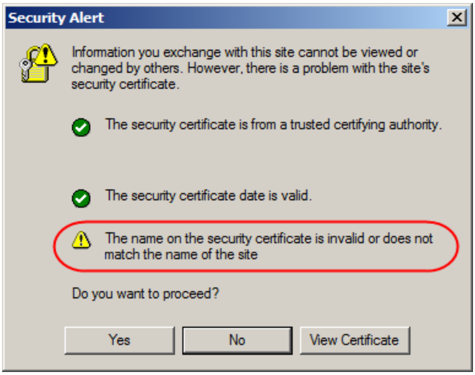
Issued to: Aten

Issued by: Aten

Valid from 2003-11-26 to 2013-11-23

Mismatch Considerations

If the site name or IP address used for generating the certificate no longer matches the current address of the RCM101D a mismatch warning occurs:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

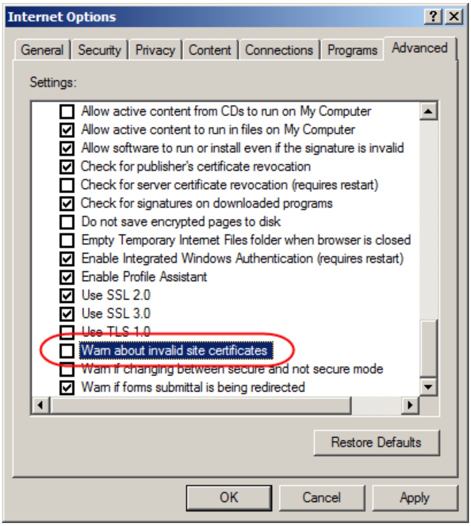
⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

You can click **Yes** to go on, or you can disable mismatch checking.

To disable mismatch checking, do the following:

1. After the page you are logging in to comes up open the browser's Tools menu; Select *Internet Options* → *Advanced*.
2. Scroll to the bottom of the list and uncheck *Warn about trusted certificates*:



Internet Options

Settings:

- □ Allow active content from CDs to run on My Computer
- ☑ Allow active content to run in files on My Computer
- ☑ Allow software to run or install even if the signature is invalid
- ☑ Check for publisher's certificate revocation
- □ Check for server certificate revocation (requires restart)
- ☑ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is closed
- ☑ Enable Integrated Windows Authentication (requires restart)
- ☑ Enable Profile Assistant
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- □ Use TLS 1.0
- □ Warn about invalid site certificates
- □ Warn if changing between secure and not secure mode
- ☑ Warn if forms submittal is being redirected

3. Click **OK**. The next time you run the browser the change will be in effect.

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at **www.openssl.org**. To create your private key and certificate do the following:

1. Go to the directory where you downloaded and extracted *openssl.exe* to.
2. Run openssl.exe with the following parameters:

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf
```

Note: 1. The command should be entered all on one line (i.e., do not press [Enter] until all the parameters have been keyed in).

2. If there are spaces in the input, surround the entry in quotes (e.g., “ATEN International”).

To avoid having to input information during key generation the following additional parameters can be used:

```
/C /ST /L /O /OU /CN /emailAddress.
```

Examples

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=yourcountry/ST=yourstateorprovince/L=yourlocationor
city/O=yourorganiztion/OU=yourorganizationalunit/
CN=yourcommonname/emailAddress=name@yourcompany.com
```

```
openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509
-keyout CA.key  -out CA.cer -config openssl.cnf -subj
/C=CA/ST=BC/L=Richmond/O="ATEN International"/OU=ATEN
/CN=ATEN/emailAddress=eservice@aten.com.tw
```

Importing the Files

After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files that you upload in the *Private Certificate* panel of the Security page (see page 50).

Troubleshooting

General Operation

Problem	Resolution
Erratic operation	The RCM101D needs to be started before the KVM switch 1. If the RCM101D is connected to a KVM switch, make sure to power it on before powering on the switch. 2. If the KVM switch was started before the RCM101D, reset or restart the KVM switch.
	The RCM101D needs to be reset (see *Upgrade Main Firmware*, page 27, point 1).
I can't access the RCM101D, even though I have specified the IP address and port number correctly.	If the RCM101D is behind a router, the router's *Port Forwarding* (also referred to as *Virtual Server*) feature must be configured. See *Port Forwarding*, page 119, for details.
Mouse pointer confusion	If you find the display of two mouse pointers (local and remote) to be confusing or annoying, you can use the *Toggle Mouse Display* function to shrink the non-functioning pointer. See page 70 for details.
Mouse movement extremely slow	There is too much data being transferred for your connection to keep up with. Lower the video quality (see *Video Settings*, page 77) so that less video data is transmitted.
Changing Mouse Sync Mode to Manual makes the RCM101D crash.	The RCM101D has not crashed. You can wait approximately 5 minutes for normal operations to resume, or you can reset the RCM101D to get it going right away (see *Upgrade Main Firmware*, page 27, point 1).
When I was in a web browser session making configuration changes, I got timed out and the settings I changed are lost.	If you do not click **Apply**, the RCM101D is not aware that you are working, and times you out. Without clicking **Apply**, none of your changes are recognized. You must click **Apply** as you go along in order to have the settings saved on the RCM101D and reset the timeout counter.
When the remote server is running Fedora the mouse pointer on the remote server does not move, whether I am accessing it from the local console or a local client computer.	If the remote server is connected with a PS/2 cable, log into the RCM101D with a browser; open a viewer; on the control panel set *Mouse DynaSync* to **Manual**. See page 88 for details.

Windows

Problem	Resolution
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	1. The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 121, for details. 2. You can eliminate this message by importing a certificate issued by a recognized third party certificate authority (see *Obtaining a CA Signed SSL Server Certificate*, page 50).
After I import the site's certificate, I still get a message warning me about the site when I log in.	Certificate security checking noticed a certificate address mismatch – however the certificate can be trusted. You can click *Continue to the website (not recommended)* to go on, or you can disable mismatch checking. See *Mismatch Considerations*, page 124 for a complete explanation of this topic.
Remote mouse pointer is out of step.	1. Check the status of the *Mouse DynaSync Mode* setting (see *Mouse Sync Mode*, page 88). If it is set to *Automatic*, change the setting to *Manual* and refer to the information provided. 2. If you are in Manual mode, use the *AutoSync* feature (see *Video Settings*, page 77), to sync the local and remote monitors. 3. If that does not resolve the problem, use the *Adjust Mouse* feature (see *Adjust mouse*, page 70) to bring the pointers back in step. 4. If the above fails to resolve the problem, refer to *Additional Mouse Synchronization Procedures*, page 130, for further steps to take.
Part of remote window is off my monitor.	Use the *AutoSync* feature (see *Video Settings*, page 77), to sync the local and remote monitors.
Virtual Media does not work.	This problem sometimes arises on older computers. Get the latest firmware version for your mainboard from the manufacturer and upgrade your mainboard firmware.
Under Virtual Media, I can mount an ISO file, but I cannot access it.	Virtual Media under the WindowsClient only supports ISO files less than 4G.Bytes. If the ISO file is 4GBytes or greater it cannot be accessed.
My anti-virus program reports that there is a Trojan after I access the RCM101D with my browser and then open the Windows Client Viewer.	The Windows Client Viewer uses an ActiveX plugin (windows.ocx) that some antivirus programs mistakenly see as a virus or trojan. We have tested our firmware extensively and found no evidence of a virus or trojan. You can add the plugin to your antivirus program's White List and use the Viewer safely. If you are reluctant to use the Windows Client Viewer, however, you can simply use the Java Client Viewer, instead.

Sun Systems

Problem	Resolution
Video display problems with HDB15 interface systems (e.g., Sun Blade 1000 servers).[1]	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to **OK mode** and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
Video display problems with 13W3 interface systems (e.g., Sun Ultra servers).*	The display resolution should be set to 1024 x 768: Under Text Mode: 1. Go to **OK mode** and issue the following commands: setenv output-device screen:r1024x768x60 reset-all Under XWindow: 1. Open a console and issue the following command: m64config -res 1024x768x60 2. Log out 3. Log in
The local and remote mouse pointers do not sync	The default configuration is for the local and remote mouse pointers to automatically sync when you connect. Automatic mouse sync only supports USB mice on Windows and Mac (G4 or higher) systems, however. You must select *Manual* as the *Mouse Sync Mode* choice, and sync the pointers manually. See *Mouse Sync Mode*, page 88 for further details.

* These solutions work for most common Sun VGA cards. If using them fails to resolve the problem, consult the Sun VGA card's manual.

Mac Systems

Problem	Resolution
The local and remote mouse pointers do not sync.	There are two USB I/O settings for the Mac: Mac 1, and Mac 2 (see *Customization*, page 59). In general, Mac 1 works with older operating system versions, whereas Mac 2 works with the newer ones. In some cases, however, the reverse is true. If you experience pointer sync problems, try selecting the other mode.
When I log in to the switch with my Safari browser, it hangs when I use the Snapshot feature.	Force close Safari, then reopen it. Don’t use the Snapshot feature in the future.
	To use the Snapshot feature with Safari, upgrade to Mac OS 10.4.11 and Safari 3.0.4.

The Log Server

Problem	Resolution
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows ME, 2000 and XP. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com/data/download.htm to retrieve the driver file: MDAC 2.7 RTM Refresh (2.70.9001.0) Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Additional Mouse Synchronization Procedures

If the mouse synchronization procedures mentioned in the manual fail to resolve mouse pointer problems for particular computers, try the following:

Windows:

Note: In order for the local and remote mice to synchronize, you must use the generic mouse driver supplied with the MS operating system. If you have a third party driver installed - such as one supplied by the mouse manufacturer - you must remove it.

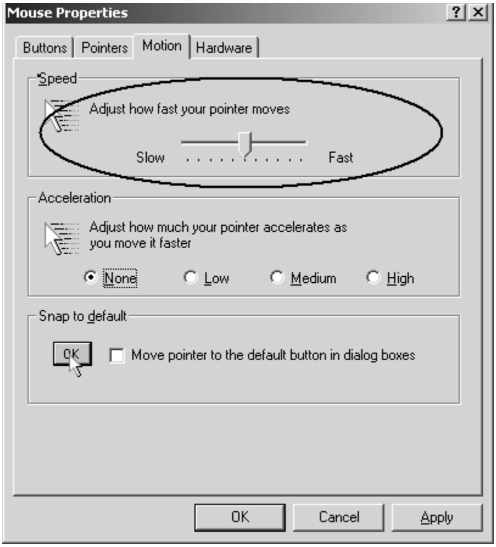
1. Windows 2000:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse → Mouse Properties)

   b) Click the *Motion* tab

   c) Set the mouse speed to the middle position (6 units in from the left)

   d) Set the mouse acceleration to *None*



Adjust how fast your pointer moves

Adjust how much your pointer accelerates as you move it faster

● None ○ Low ○ Medium ○ High

☐ Move pointer to the default button in dialog boxes

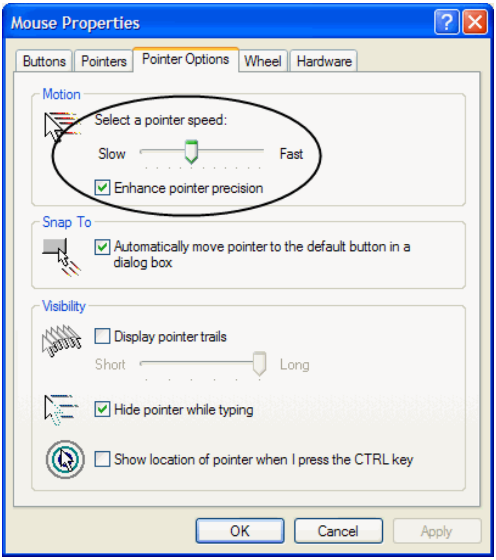
2. Windows XP / Windows Server 2003:

   a) Open the Mouse Properties dialog box (Control Panel → Mouse)

b) Click the *Pointer Options* tab

c) Set the mouse speed to the middle position (6 units in from the left)

d) Disable *Enhance Pointer Precision*



Select a pointer speed:

☑ Enhance pointer precision

☑ Automatically move pointer to the default button in a dialog box

☐ Display pointer trails

☑ Hide pointer while typing

☐ Show location of pointer when I press the CTRL key

3. Windows ME:

   Set the mouse speed to the middle position; disable mouse acceleration (click **Advanced** to get the dialog box for this).

4. Windows NT / Windows 98 / Windows 95:

   Set the mouse speed to the slowest position.

Sun / Linux

Open a terminal session and issue the following command:

Sun: `xset m 1`

Linux: `xset m 0`

```
or
xset m 1
```

(If one does not help, try the other.)

Virtual Media Support

WinClient ActiveX Viewer / WinClient AP

- IDE CDROM/DVD-ROM Drives – Read Only
- IDE Hard Drives – Read Only
- USB CDROM/DVD-ROM Drives – Read Only
- USB Hard Drives – Read/Write*
- USB Flash Drives – Read/Write*
- USB Floppy Drives – Read/Write

* These drives can be mounted either as Drives or Removable Disks (see *Virtual Media*, page 83). Mounting them as removable disks allow booting the remote server if the disk contains a bootable OS. In addition, if the disk contains more than one partition, the remote server can access all the partitions.

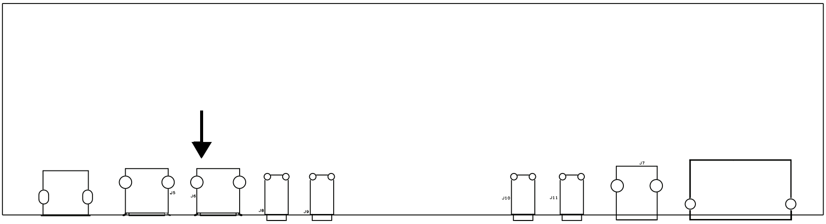
- ISO Files – Read Only
- Folders – Read/Write
- Smart Card Readers

Administrator Login Failure

If you are unable to perform an Administrator login (because the Username and Password information has become corrupted, or you have forgotten it, for example), there is a procedure you can use to clear the login information.

To clear the login information do the following:

1. Power off the RCM101D, disconnect the power cord from its inlet, and remove its housing.
2. Use a jumper cap to short the jumper on the mainboard labeled **J15**.



3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from **J15**.
6. Close the housing and power on the RCM101D.

   After you start back up, you can use the default Username and Password (see page 20, and page 93) to log in.

Specifications

Connectors			
Console Ports	KB		1 x USB Type A Female (White)
	Video		1 x DVI-D Female (White)
	Mouse		1 x USB Type A Female (White)
	Audio	Speaker	1 x 3.5mm Audio Jack Female (Green)
		Microphone	1 x 3.5mm Audio Jack Female (Pink)
KVM Ports	KB/Mouse		1 x USB Type B Female (White)
	Video		1 x DVI-D Female (White)
	Audio	Speaker	1 x 3.5mm Audio Jack Female (Green)
		Microphone	1 x 3.5mm Audio Jack Female (Pink)
LAN			2 x RJ-45 Female (Black)
Virtual Media / Laptop USB console			1 x USB Mini-B Female (Black)
Power			2 x DC Jack (Black)
PON			1 x RJ-45 Female (Black)
Serial Port			1 x RJ-45 Female (Black)
Control Port			1 x PS/2 port
Switches			
Reset			1 x Semi-recessed pushbutton (Black)
USB Function Selection			1 x Slide Switch (Black)
Console Lock			1 x Slide Switch (Black)
LEDs			
Console Status			1 (Green)
LAN 10/100/1000 Mbps			2 (Orange / Orange + Green / Green)
Remote Login			1 (Green)
Power			1 (Green)
Emulation			
Keyboard/Mouse			USB
Others			
Video			Local Console: 1920 x 1200 @ 60 Hz RB Remote: 1920 x 1200 @ 60 Hz RB
Power Consumption			DC5.3V, 5.56W, 30BTU
Environment			
Operating Temp.			0 – 50^{o} C
Storage Temp.			-20 – 60^{o} C
Humidity			0 – 80% RH, Non-condensing
Physical Properties			
Housing			Metal
Weight			0.88 kg (1.94 lb)
Dimensions (L x W x H)			26.00 x 7.64 x 4.20 cm (10.24 x 3.01 x 1.65 in.)

Limited Warranty

ATEN warrants its hardware in the country of purchase against flaws in materials and workmanship for a Warranty Period of three [3] years (warranty period may vary in certain regions/countries) commencing on the date of original purchase. This warranty period includes the LCD panel of ATEN LCD KVM switches. Select products are warranted for an additional year (see *A+ Warranty* for further details). Cables and accessories are not covered by the Standard Warranty.

What is covered by the Limited Hardware Warranty

ATEN will provide a repair service, without charge, during the Warranty Period. If a product is detective, ATEN will, at its discretion, have the option to (1) repair said product with new or repaired components, or (2) replace the entire product with an identical product or with a similar product which fulfills the same function as the defective product. Replaced products assume the warranty of the original product for the remaining period or a period of 90 days, whichever is longer. When the products or components are replaced, the replacing articles shall become customer property and the replaced articles shall become the property of ATEN.

To learn more about our warranty policies, please visit our website:

http://www.aten.com/global/en/legal/policies/warranty-policy/