Digi CM

8-port, 16-port, 32-port, and 48-port

User Guide

Revision history—90000301-88

Revision	Date	Description
L	October 2024	Updated contact information for Digi Technical Support.
K	December 2021	Updated format. Included translated safety warnings.
J	January 2020	Updated to document unique passwords printed on manufacturing label.
H	August 2018	Added certification in French. Added power and ground information for CM 48. Updated the template.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Technical support

Digi Technical Support: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, visit us at www.digi.com/support.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi CM, 90000301-88 K) in the subject line of your email.

Contents

Configure ports

Alerts and notifications

User administration

Configure security and authentication

Custom and default menus

Microsoft SAC support

Configure Virtual KVM

Rackable Systems management card

Dial-in modem access

Power Controller

Post clustering

System administration

Command line interface

Configuration menu

Hardware information

Certifications

Safety warnings

Digi CM User Guide

This manual offers information on the Digi CM 4-port, 8-port, 16-port, 32-port, and 48-port models.

Feature overview

With the model number/code/name, administrators can securely monitor and control servers, routers, switches, and other network devices from anywhere on the corporate TCP/IP network, over the Internet, or through dial-up modem connections, even when the server is unavailable through the network.

The Product Name employs SSHv2 encryption, to keep server access passwords safe from hackers, and supports all popular SSH clients, as well as secure access from any Java-enabled browser. It is the first console server to provide a secure graphical user interface for easy out-of-band management of Microsoft Windows Server 2003 systems. It connects to serial console ports using standard CAT5 cables, eliminating the hassles of custom cabling. In addition, the Product Name offers a PCMCIA card slot, for adding dialup modems or wireless network cards. Flash memory cards can be used to save port logs and backup configuration files.

The Product Name is available in 8-, 16-, 32- and 48-port models, in a 1U rackmount form factor.

Feature summary

Category	Feature
Security	▪ SSH v2 server and client ▪ SSL ▪ IP Filtering ▪ Central access to security parameters via the Security Profile including network, port, and password securities.
Authentication	▪ TACACS+ ▪ RADIUSLDAP ▪ Custom PAM modules ▪ Kerberos ▪ User access per port ▪ Local user database

Category	Feature
Management	■ Command line ■ WEB --HTTP/HTTPS ■ SNMP ■ Custom applications ■ Port Triggers and Alerts ■ Multi level menus ■ Advanced Device Discovery Protocol (ADDP) for locating the device on the network ■ Integrated power management and control
Data Capture	■ Local port logging ■ External logging (syslog, NFS, PC card)
Port Access	■ Telnet/SSH ■ Reverse Telnet/SSH ■ HTTP/HTTPS ■ Port escape menu
PC Card Support	■ CompactFlash memory card ■ Wireless LAN adapter (802.11b) ■ Ethernet LAN adapter ■ PSTN/CDMA modem card ■ See the Digi CM data sheet for more information.
Other features	■ RealPort ■ Solaris Ready ■ Multiple users per port ■ Remote ports ■ Access lists per port ■ Flash upgradeable ■ SSH sessions simultaneously on all ports ■ Secure Clustering - Single IP for multiple Digi CM devices ■ IP addresses per port ■ Find Me locator light (Digi CM 48-port)

User groups

The Digi CM unit comes with four built-in user groups pre-defined by roles or access levels. The following table lists the four user groups, their access rights, and default user names. The Digi CM unit supports access lists for user privileges. These lists can contain multiple users and define specific port rights. If e.g. you have multiple people responsible for the Sun Servers in your company and you want to give them identical access rights you can create a "Sun-admin" access list. Assign this access list rights to every port that is attached to a Sun Server and add all the Sun administrators to the "Sun-admin" Access List.

Group	Access Privileges		Configuration Privileges		Defaults	
------------	Ports	Command Line	Ports	System	Login	Password
Root	yes	yes	yes	yes	root	*
System Admin	yes	yes (read only)	yes	yes	admin	admin
Port Admin	yes	no	yes	no	-	-
User	yes	no	no	no	-	-

*The default password for **root** is printed on the device label. If a password is not on the label, the default password is **dbps**. If neither default password works, the password may have been updated. Check with your system administrator.

Root and admin usernames and passwords

The Digi CM unit comes with two default users; root and system admin. The user names of the the Digi CM unit are case sensitive

User name	Default password
root	The default password for **root** is printed on the device label. If a password is not on the label, the default password is **dbps**. If neither default password works, the password may have been updated. Check with your system administrator.
admin	admin

Adding port administrators and users

The system administrator and root user can add port administrators and additional users easily with the web interface by choosing **System administration** > **User administration** > **Add user**.

Access lists

Multiple users can be defined within Access lists with access privileges or restrictions to the ports. See Add an Access List to the Digi CM Unit for more information.

Digi CM configuration methods

This section discusses the three ways to configure the Digi CM unit using the web interface, configuration menu, or command line interface.

Web interface

The web interface provides an easy way to configure the Digi CM unit. The root user and system administrator can configure all features through the web. Port administrators can configure ports, including port clustering, but cannot modify system settings. No other users can use the web interface for configuration.

There are two ways to access the web interface.

- ■ ADDP (Advanced Device Discovery Protocol)

   This device discovery tool allows you to find, configure and launch your web configuration and management interface. Find your device and double click it to access the web interface, or select your device and click Configure network settings (on the left navigation bar).

- ■ Directly entering the IP address

   You can enter the IP address directly into the URL address bar of your browser. (Of course, the IP address must already be set up)

Access the web interface from one of the previous methods. The following page is displayed after login.

Configuration menu

The root user and system administrator have full access to the configuration menu from a Telnet or SSH session or a serial connection through the console

port. Functionality is similar to the web interface, with the exception of custom menus, which can be created only from the web interface. The configuration menu is presented to system administrators automatically. Root users access the menu by entering the command **configmenu**. Port administrators can access this menu but can modify serial port configuration only. No other users can access this menu.

```
Telnet 192.168.1.80                                                    _ □ ×

Welcome to Digi CM 8 configuration page
Current time : 10/20/2004 18:10:43    F/W REV.    : v1.6.0rc3
Serial No.   : V32730356              MAC Address : 00-40-9d-23-21-df
IP mode      : Static IP              IP Address  : 192.168.1.80

Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
<ENTER> Refresh
----->
```

Command line interface

The command line interface can be accessed from a Telnet or SSH session or from the console port. The root user always has access to this interface. The system administrator can be granted read-only permission as well. No other users can access the command line interface.

Digi CM ports access methods

There are multiple ways to access the native serial ports on the Digi CM unit:

- Web interface access menu
- Port Access Menu
- Direct port access
- Custom menus
- Port Access Menu
- SNMP

Web interface access menu

The web interface menu provides easy and convenient access to ports. All users can access the menu by entering the Digi CM unit IP address or host name in a web browser's URL window.

To access a port from the web interface, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Click **Serial port** > **Connection**.
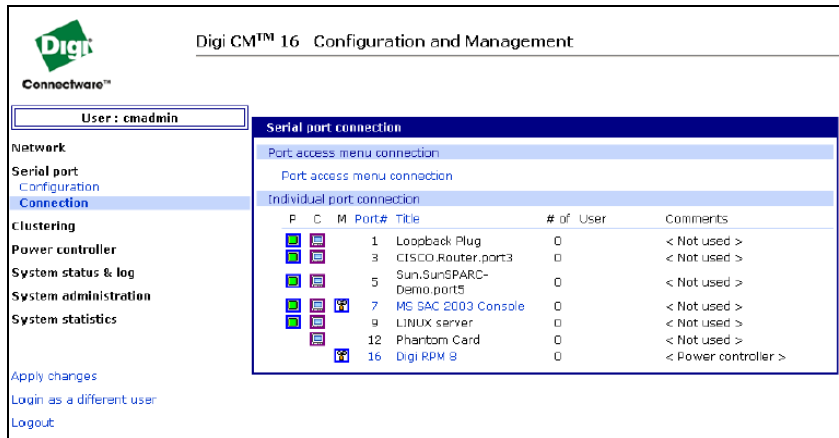
- The **P (Power)** column allows you to control power of the attached devices, if a Remote Power Management unit is attached and you have appropriate rights.

- The **M (Manage)** column offers web based management for Windows Server 2003, Remote Power Management units or Rackable Systems Management Card.

- The **# of User** column shows how many users are actually connected to the port and the username of the read/write user.

If you are conducting a special task through the console port, like BIOS upgrade and should not be interrupted, you can notify other users by entering a comment upon connect. This comment is shown here.Select a port by clicking the icon in the C (Console) column.

A Java applet or Telnet window opens with a login prompt.
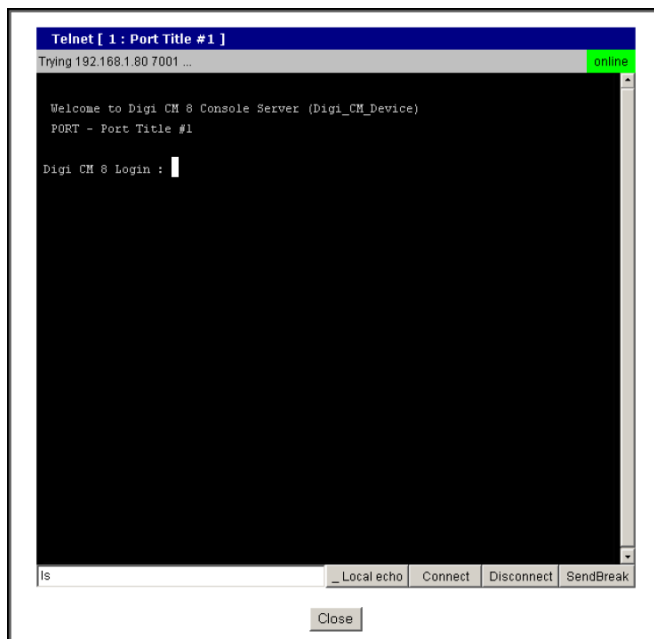
Port Access Menu

The Port Access Menu provides access to ports. It is accessible to all users through the web interface, Telnet and SSH sessions, and remote modem access.The information that follows shows you how to access this menu.

Access Type	Permissions	Procedure
Web interface	Any user can use this method.	1. Access the web interface 2. Choose Serial port > Connection > Port access menu connection 3. Log in
Telnet	Any user can use this method.	1. Telnet to the Digi CM unit specifying its IP address and port 7000. (7000 is the default socket port for both Telnet and SSH) Example: `telnet 192.168.15.7 7000` 2. Log in
Command line	Root	From the command line, issue the portaccessmenu command. Example: `portaccessmenu` **telnet http://digicm.digi.com**

Here is a screenshot of the Port access menu.

```
Welcome to Digi CM 32 Console Server

Digi CM 32 Login : root
Digi CM 32 Password : ****

==================================================================
Port#        Port Title          Mode    Port#        Port Title          Mode
==================================================================
1        Port Title #1          [CS]    2        Port Title #2          TS
3        Port Title #3          DI      4        Port Title #4          DI
5        Port Title #5          CS      6        Port Title #6          CS
7        Port Title #7          CS      8        Port Title #8          CS
9        Port Title #9          CS      10       Port Title #10         CS
11       Port Title #11         CS      12       Port Title #12         CS
13       Port Title #13         CS      14       Port Title #14         CS
15       Port Title #15         CS      16       Port Title #16         CS
17       Port Title #17         CS      18       Port Title #18         CS
19       Port Title #19         CS      20       Port Title #20         CS
21       Port Title #21         CS      22       Port Title #22         CS
23       Port Title #23         CS      24       Port Title #24         CS
25       Port Title #25         CS      26       Port Title #26         CS
27       Port Title #27         CS      28       Port Title #28         CS
29       Port Title #29         CS      30       Port Title #30         CS
31       Port Title #31         CS      32       Port Title #32         CS


 Enter the serial port ( 1-32 , others for exit ) :
```

Direct port access

Connect directly to a properly configured port through a Telnet or SSH session. Configuration requirements include setting the Host Mode to Console Server Mode and the Protocol to either Telnet or SSH. Ports, by default are set to Console Server Mode and Telnet. Use the following information to make a Telnet or SSH connection to a port.

Note The example assumes that the Listening TCP port is 7003, the default for port 3.

Type	Command syntax	Example: Connection to port 3
Telnet	telnet *ip-address tcp-port* where: *ip-address* is the Digi CM unit's IP address *tcp-port* is the Listening TCP port for a port	telnet 192.168.15.7 7003 (7000 is the default socket port for both Telnet and SSH)
SSH	ssh *user-name@ip-address tcp-port* where: *user-name* is a user's name *ip-address* is the Digi CM unit's IP address *tcp-port* is the Listening TCP port for a port	ssh admin@ 192.168.15.7 -p 7003 (7000 is the default socket port for both Telnet and SSH) http:// digicm.digi.comconnect.asp?t=CISCO.Router.port3
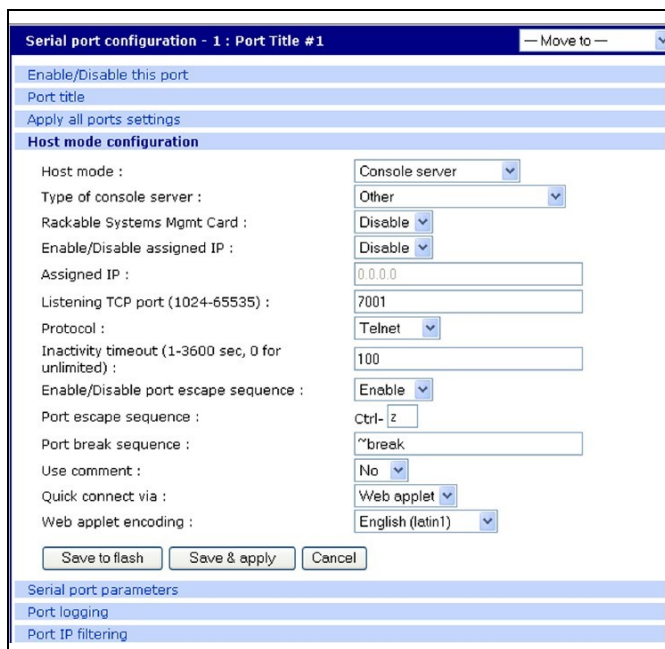
Custom menus

Custom menus are created by either root or the system administrator to limit your access to specific ports. For more information, see Make custom menus.

Port escape menu

Port escape is the ability to escape from a port without disconnecting. Port escape is available in main sessions as well as sniff sessions. Every connection method accommodates port escape. You configure the escape sequence per port. Follow the procedure to configure the port escape sequence.

1. **Serial Port** > **Configuration** > Select the port number or All.
2. **Host mode configuration** > Port escape sequence - enter a letter for the Port escape sequence.
3. Click **Save to flash** and continue with other configurations or click Save & apply for the changes to take effect.

To open a sniff session:

1. Click **Serial port** > **Connection**.

2. Select the port you want to access.

3. Log in with your user name and password.

4. Enter the letter of the port escape sequence.

Description of fields: Port escape

The following table describes the fields and the operations for the port escape feature. You will only see the fields allowed for your permissions.

Escape Sequence Ctrl+	Description of action	Occurrence
m	take over main session (read/write)	only presented to users with read/ write access upon entering a session
s	enter as a slave session (read only)	only presented to users with read/ write access upon entering a session
b	send break	not functional for sniff users
l	show last 100 lines of log buffer	must enable logging for this option
d	disconnect a sniff session	only functional to admin
a	send message to port user (s)	not available to sniff users
r	reboot device using power-switch	only if power management is available on this port
p	power device on/off	(show only on or off) only if power management is available on this port
x	close current connection to port	closes the current connection to port

Note By entering the port escape sequence twice, it is directly transmitted (once) to the connected device. If the escape sequence is entered twice within 1/2 second, the menu will not open.

SNMP

An SNMP MIB to configure the Digi CM unit is available to be downloaded from digi.com/support.

Save and apply changes

In the web interface, you can save and apply configuration changes in two ways. With the one-step method, you choose **Save & apply** and changes are saved and applied (take effect) immediately. With the two-step method, you choose **Save to flash**, which immediately saves changes but the changes do not take effect until you choose **Apply changes**. The following topics describe how to do each of these operations.

One step: Save and apply changes

To save and apply changes immediately, choose the **Save & apply** button.

Two step: Save to flash and then apply changes

To save multiple changes but apply changes once, do the following:

1. Choose the **Save to flash** button.

2. When you finish changing the configuration, choose the **Apply changes** link, which is located on the left navigation menu; or the **Save & apply** button at the bottom of the page.

For more details about Automatic Device Recognition, see Configure Automatic Device Recognitiion.

Port 3 shows a real world example of a detected device.

Automatic Device Recognition also monitors each of the configured serial ports. This allows you to receive an e-mail or SNMP trap if there is a change in the expected response from the device connected to the serial port. If the device goes down or is disconnected for any reason, you are notified.

Locator light

The Digi CM 48-port unit has a locater light on the front panel labeled Find Me. All other Digi CM units flash the serial port lights to indicate where the device is found.

If you access the web interface, log in to the Digi CM unit, and scroll down the page, you will find additional links.

1. Click **Start device locating**. A confirmation dialog displays.

2. Click **okay** and the Digi CM unit Find Me light will blink (other Digi CM models blink all LEDs).

3. To turn off the locater light, click **Stop device locating**.

Get started

Introduction

This section covers basic configuration topics. Included is information on assigning IP settings, enabling secure access with the web interface, accessing the unit through SSH, and adding or removing users.

Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

Assign IP settings from the console port

The following steps use the console port to assign IP settings.
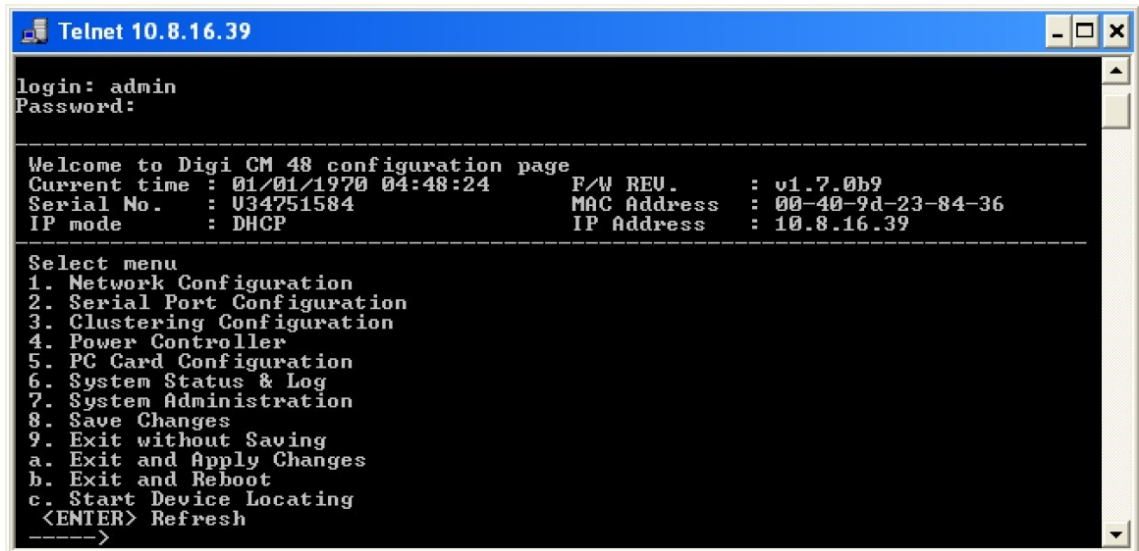
Note The default IP address is 192.168.161.5.

1. Connect the console port on the rear panel of the Digi CM unit to a serial port on a workstation using the Ethernet console cable and the appropriate console adapter packaged with the the Digi CM unit. The arrow in the following graphic points to the console port.
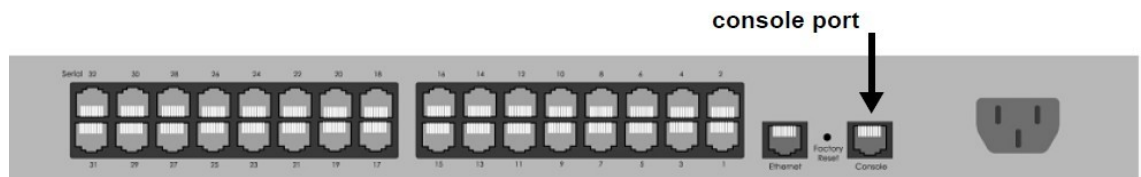
CM 32 back panel shown

2. Configure a terminal emulation program, such as HyperTerminal, using the following settings:
   - bps = 9600
   - data bits = 8
   - parity = none
   - stop bits = 1
   - flow control = none
3. Establish a connection to the console port and press Enter to get a command prompt.
4. At the login prompt, log in as **admin**. The default password for admin is **admin**. The Configuration menu appears.

5. Enter the number for Network Configuration.

6. Enter the number for IP configuration.

7. Enter the appropriate parameters for the IP settings.

8. Press ESC when done to return to the main configuration menu.

9. Enter the number to exit and apply changes. Changes are saved and applied immediately. There is no need to reboot.

Configure for SSH

The Port Access Menu and individual ports can be configured for SSH.

Note The Digi CM unit supports Blowfish and 3DES encryption methods for SSH.

1. Configure the Port Access Menu for SSH
2. Configure a port for SSH

Configure the Port Access Menu for SSH

1. Access the web interface and log in as root, admin, or a member of the port administration group.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under **Serial port** > **Configuration** > **Port access menu configuration**. The Port access configuration menu appears.

3. Select SSH as the Port access menu protocol.

   Note Log in on port access requires logging in twice (once for access to the port and once for port access menu) when enabled. Disabled allows one log in directly to the port.

4. Click **Save & apply**.

Configure a port for SSH

1. Access the web interface and log in as root, admin, or a member of the port administration group.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under **Serial port** > **Configuration**.
3. Click **Host mode configuration**.
4. Specify SSH as the Protocol as shown in the following screenshot.
5. Click **Save & apply**.

Add, edit, and remove users

The root user and system administrator can add, remove, or edit users from the web interface.

1. Access the web interface and log in as root or admin.

2. Under the **System administration** heading click **Users administration**.

3. Select **Add**, **Edit**, or **Remove**.
    -   **Add**: Assign a user name, user group, password, and shell.
    -   **Edit**: Change user group, password, or their shell
    -   **Remove: Remove a user from the system**

4. Click **Save & apply**.

Note The root and admin users cannot be removed from the system.

For more information about configuring access rights for specific users see Configure user access privileges.

About shell options

The shell program selection determines the interface you see when establishing a Telnet or SSH session with the Digi CM unit.

User Group	Shell Program Options
root	command line
system admin	command line, configuration menu, port access menu, custom menus
port admin	configuration menu, port access menu, custom menus
user	port access menu, custom menus

Install and configure PC cards

This section includes information on adding and configuring PC cards for the Digi CM unit. PC card devices that can be added to the the Digi CM unit include a serial modem, compact-flash card, wireless LAN card, and a network LAN card.

Compatible PC cards

All compact-flash cards work with the Digi CM unit, but not all serial modem, wireless LAN, or regular LAN cards do. To see a list of compatible cards that have been tested with the Digi CM unit, visit the Digi support site.

Add a compact flash card

A PC card slot is located on the front panel of the Digi CM unit. The arrow in the following graphic indicates the PC card slot.

Digi CM 32 shown

To install and configure the compact-flash card on the Digi CM unit, do the following.

1. Insert the card into the PC card slot.
2. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

3. Under the **PC card** heading click **Configuration**.

Note Always select the **Stop card service** button and **Save & apply** before removing the PC card.

4. Click **Configure the detected card**. The following fields appear on the configuration page:

    - **ATA/IDE Fixed Disk Card configuration**
    - **Total data size to be used** - Enter the amount of memory you want to assign to the compact- flash card for configuration files.
    - **Delete all files in ATA/IDE Fixed Disk Card** - Select the **Delete** button to clear the compact-flash card of all files.
    - **Format ATA/IDE Fixed Disk Card** - The options are EXT2 or FAT formats. Select the format option and then select the **Format** button.

5. Enter the appropriate parameters on the configuration page.

6. Click **Save to flash** or **Save & apply**.

Add a network card

To install and configure a network card on the Digi CM unit, do the following.

1. Insert the card into the PC slot.
2. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

3. Under the **PC card** heading, click **Configuration**.

   Note The card is automatically discovered and a configuration menu is displayed.

4. Enter the appropriate parameters in the configuration menu.
5. Click **Save & apply**.

Note If DHCP is active the IP address will appear after the configuration is saved and applied.

Add a wireless LAN card

To install and configure a wireless LAN card on the Digi CM unit, do the following.

1. Insert the card into the PC slot.
2. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

3. Under the **PC card** heading, click **Configuration**.

   Note The card is automatically discovered and a configuration menu is displayed.

4. Click **Configure the detected** card.

5. Enter the appropriate parameters in the configuration menu.

   WEP is the acronym for Wired Equivalent Privacy and is a security protocol for wireless LANs using encryption to protect data transfers. If you are unsure of the settings for the wireless card, see your network administrator.

   - **SSID** - Set Service Identifier and is the name of the wireless LAN network
   - **Use WEP key** - Enable or disable the WEP key
   - **WEP mode** - Encrypted or unencrypted
   - **WEP key length** - The options are 40 or 128 bits if the WEP key is enabled
   - **WEP key string** - Refer to the wireless network administrator for the wireless encryption key string

6. Click **Save to flash**.

Add a serial modem

The modem must first be inserted and installed on your system before it can be used. To configure the modem do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. From the menu click **Configuration** under the **PC card** heading.

   Note The card is automatically discovered and a configuration menu is displayed.

   PC card configuration

   Currently configured PC card

Card type :	None

   PC card service

   [Configure the detected card]   [Stop card service]

   Detected PC card

Card type :	Serial Modem Card
Model :	Zoom PCMCIA V92 DataFax

   New PC card is detected.

   [Save to flash]   [Save & apply]   [Cancel]

3. Click **Configure the detected card**.
4. Edit any appropriate parameters.
5. Click **Save & apply**.

   PC card configuration

   Currently configured PC card

Card type :	Serial Modem Card Serial Modem Card
Model :	Zoom PCMCIA V92 DataFax

   Serial Modem Card configuration

Init string :	q1e0s0=2
Inactivity timeout (1-3600 sec, 0 for unlimited) :	0

   PC card service

   [Configure the detected card]   [Stop card service]

   Detected PC card

Card type :	Serial Modem Card
Model :	Zoom PCMCIA V92 DataFax

   Card service is successfully configured. Save the PC card service configurations.

   [Save to flash]   [Save & apply]   [Cancel]

System status and port logging

The Digi CM unit provides four options for saving system and port logs:

- A syslog server
- An NFS server
- A compact-flash card
- The Digi CM unit s memory

When memory is selected as the storage location, log files are saved to volatile memory, meaning files are lost when the power is turned off. To use a syslog server, an NFS server, or a compact-flash card, you must first enable the devices and enter the required information. Compact-flash cards must be installed before they can be enabled and configured for logging purposes.

System logs track events such as logins, authentication failures, system configuration changes, and more. Port logs, on the other hand, document the data flow through the serial ports. This chapter outlines locations for viewing the system and port logs.

System status & log

For basic system information click **System status & log**. The parameters for the system status are described in the following list.

System Information

- **Model No.** - Identification of Digi device
- **Serial No.** - Serial number of product
- **F/W Rev.** - Revision number of firmware
- **B/L Ver**. - Bootloader version
- **MAC address** - MAC address of Digi device
- **Uptime** - Amount of time since last reboot
- **Current time** - Time based on time set for Digi device
- **System logging** - Status of system logging either Enabled or Disabled
- **Send system log by email** - Condition for notification:
- **PC card type** - Description of PC card if configured
- **PC card model** - Model of PC card if configured
- **Power status** - Dual power (1 - Normal , 2 - Normal)

IP Information

- **IP mode** - Method for setting IP address either Static, DHCP, PPPoE, or Disable
- **IP expiration** - When the IP address will expire
- **IP address** - Actual IP address
- **Subnet mask** - Address of the Subnet mask
- **Gateway** - Address of the Gateway
- **Receive/Transmit errors** - Number of errors from receiving or transmitting
- **Primary DNS** - IP address of the primary DNS
- **Secondary DNS** - IP address of the secondary DNS

Enable the log storage location

Enable an NFS server

You can save log data to an NFS server, but the NFS server must be configured with read and write privileges. To use an NFS server, you must specify the NFS server's IP address and its mounting path. Encrypted NFS is using a SSH connection to tunnel all data. To enable the NFS server for port or system logging, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the Network heading, click **NFS server configuration**.
   - **NFS service** - Enabled or disabled.
   - **Primary NFS server name** - IP address of NFS server or
   - **Mounting path on primary NFS server** - Directory to primary NFS server
   - **Primary NFS timeout** - Interval in seconds before timeout (5-3600)
   - **Primary NFS mount retrying interval** - Interval in second between attempts to connect (5- 3600)
   - **Enable/Disable encrypted primary NFS server** - If server supports encrypted NFS server
   - **Encrypted primary NFS server user** - User name of server
   - **Encryped primary NFS server password** - Password
   - **Secondary NFS service** - Enabled or Disabled
   - **Secondary NFS server name** - Name of server
   - **Mounting path on secondary NFS server** - Directory to server
   - **Secondary NFS timeout (sec, 5-3600)** - Timeout in seconds
   - **Secondary NFS mount retrying interval (sec, 5-3600)** - Retry interval in seconds
   - **Enable/Disable encrypted secondary NFS server** - If secondary server supports encrypted NFS server
   - **Encrypted secondary NFS server user** - User name

- **Encrypted secondary NFS server password** - Password
- **Confirm secondary NFS server password** - Repeat password

3. Choose **Enabled**.

4. Enter the IP address of the primary and secondary (if applicable) NFS server and the mounting path of each.

5. Click **Save & apply**.

Alert for NFS server disconnect

You can also set up an email alert and/or an SNMP trap configuration for an NFS server disconnect. To configure this feature, use this procedure.

1. Farther down the **NFS Configuration** screen, at the **Email alert configuration**, select **Enable**.

2. Enter the **Title** for the email and the **Recipient's email address**.

3. For an **SNMP trap configuration** select **Enable NFS disconnection trap**.

4. Select **Enable** for **Use global SNMP configuration**.

5. Enter the IP information for **Trap receiver settings**.

6. Click **Save & apply**.

Enable SYSLOG server

To enable the Digi CM unit for system or port logging on a syslog server:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Network** heading, click **SYSLOG server configuration**.

3. Choose **Enable**.

4. Enter the IP address of the primary and secondary (if applicable) syslog server, and select the syslog facility from the drop down menu.

5. Click **Save & apply**.

Enable a compact-flash card

The compact-flash card must be installed and configured on the Digi CM unit before it can be used for system logging or storing the Digi CM unit's configuration information. When storing log files to an external flash card, the size of the available storage is dependent on both the size of the card and the port counts of the Digi CM unit used. The maximum settings for log file sizes are listed in the following table. See also Add a compact flash card.

Total flash card size	Digi CM	System log	Port log (per port)	Total memory used
32	8	4.6	3.1M	29m
	16	4.6	1.53M	
	32	4.6	762K	
	48	4.6	500K	
64	8	9.2	6.2M	58M
	16	9.2	3.1M	
	32	9.2	1.53M	
	48	9.2	1.02M	
128	8	18.4	12.3M	118M
	16	18.4	6.2M	
	32	18.4	3.1M	
	48	18.4	2.0M	
256	8	36.8	24.6M	236M
	16	36.8	12.3M	
	32	36.8	6.2M	
	38	36.8	4.1M	

Enable the Digi CM Unit's memory

The Digi CM unit s memory is already enabled for port logging and needs to be configured only for system logs or port logs. When storing log files to the Digi CM unit's local memory, a total of 3.5M is available. The amount of memory per serial port is dependent on the port count of the Digi CM unit used. The log file sizes shown in the following table are maximum settings. See also Configure system logging.

Digi CM	System log	Port log (per port)	Total memory used
8	300K	400K	3.5M
16		200K	
32		100K	
48		66K	

Configure system logging

To configure the Digi CM unit for system logging, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under **System status & log**, click **System logging**.

3. Choose **Enabled** for **System logging** and the log buffer size.

4. From the **System log storage** location, choose the location from the drop down menu. The choices are dependent on what you have enabled and/or installed. The Digi CM unit 's memory choice is always available.

   - **System logging** - Enable or Disable
   - **System log storage location** - Memory or NFS server
   - **System log to SYSLOG server** - Enable to store system logs to a SYSLOG server
   - **System log buffer size (KB, 300 max)** - Log buffer size in KB
   - **Automatic backup on mounting** - This parameter defines the action taken if a NFS partition of a CF card or NFS server is mounted or re-mounted.
     - **Enable**: rename the existing log file by adding a -xx with xx being a incremented number.
     - **Disable**: keep writing to the existing log file.
   - **Send system log by Email**
   - **Number of log messages to send in an email (1-100)** - Number of messages
   - **System log recipient's mail address** - Email address for log recipient

5. Choose to enable or disable email alerts and the number of log messages to send. The default value is 5 seconds for the delay in log email messages.

6. Enter the contact email address.

7. Click **Save & apply**.

View system logs

The system logs can be viewed from the web interface on the System logging page or from the location where they have been saved. The following table lists the file locations of the system logs.

System Logfile Log storage	File location
Digi memory	/tmp/logs
Compact-flash card	/mnt/flash/logs
Syslog server	must be viewed on the syslog server
NFS server	/mnt/nfs/logs

Configure port logging

If a serial port is configured for console server mode, the port logging feature can be enabled. Port logging allows you to save serial data to the memory of the Digi CM unit, a compact-flash card, a syslog server, or to an NFS server. If the memory is used for port logging, all data is cleared when the system's power is turned off.

You can also define alarm keywords for each serial port and send email alerts or SNMP traps to enable unattended serial data monitoring. The following steps configure a serial port for port logging in console server mode.

1. Access the web interface.

Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

---

2. Under the **Serial port** heading, click **Configuration**.

3. Choose All or the Individual port, and then **Port logging**.

4. Configure the settings:

    Logging direction - Specify what to log:

    - Server – only server output,
    - User – only user output,
    - Both with/without arrows – server and user output with/without directional arrows.
    - Default: server output.

    Security advice: When logging user output passwords will be saved into the log file!

    Port log to SYSLOG server - Enable to store port logs to a SYSLOG server

    Port logging filename - Options are to specify your own or use the port title for the port log filename

Show last 10 lines of a log upon connect -Show previous last 10 lines of log when connecting to this port

Strip the ^M from SYSLOG -For logging to a SYSLOG server, strip out all ^M

Automatic backup on mounting - This parameter defines the action taken if a NFS partition of a CF card is mounted or re-mounted.

■ Enable: rename the existing log file by adding a -xx with xx being an incremented number.

■ Disable: keep writing to the existing log file.

Monitoring interval -The frequency in seconds to update the port log

5. Click **Save & apply**.

Note When port logging is enabled, a Port Event Handling page is available to create alarm keywords and send alerts. See Alerts and notifications for more information.

```
Serial port parameters
Port logging
    Port logging :                               Enable  ▾
    Logging direction :                          Server output        ▾
    Port log storage location :                  Memory  ▾
    Port log to SYSLOG server :                  Disable ▾
    Port log buffer size (KB, 3150 max.)         50
    Port logging filename :                      Specify below ▾
    (null as default file name[portXXdata])      port1data
    Time stamp to port log :                     Enable  ▾
    Show last 10 lines of a log upon connect :   Enable  ▾
    Strip the ^M from SYSLOG :                   Disable ▾
    Automatic backup on mounting :               Enable  ▾
    Monitoring interval (sec, 5-3600) :          5

    [ Save to flash ]  [ Save & apply ]  [ Cancel ]

    Port log :
    ┌─────────────────────────────────────────┐
    │                                          │
    │                                          │
    │                                          │
    └─────────────────────────────────────────┘

    [ Clear ] [ Refresh ]
Port IP filtering
Authentication
```

View port logs

The port logs can be viewed from the web interface on the Port logging page or from the location where they have been saved. The following table lists the file locations of the system logs.

Port logfile Log storage	File location
Digi memory	/tmp/port#data
Compact-flash card	/mnt/flash/port#data
Syslog server	must be viewed on the syslog server
NFS server	/mnt/nfs/port#data

To view the port logs on the NFS server for port number 5, enter the following command:

```
more /mnt/nfs/port5data
```

Partial logfiles can also be viewed on the web interface by going to **Serial port** > **Configuration** > select a port # you want to view > P**ort logging**.

Configure ports

This section provides information on configuring serial ports. Key port configuration attributes include whether or not the port is enabled or disabled, the host mode, which defines a type of communication between the port and a remote host, the protocol, authentication, user access restrictions, and serial communication attributes. It also covers remote port support.

Enable and disable the ports

All serial ports may be enabled or disabled individually or as a group from the web interface.

1. Click **Serial port** > **Configuration** > **Port number** or **all**

2. Select **Enable** or **Disable** from the drop-down menu.

3. Click **Save to flash** and continue with other configurations or click **Save & apply**.

Serial port configuration - 1 : Port Title #1	— Move to —
Enable/Disable this port	
Enable/Disable this port :	Enable
RealPort support :	Disable
Save to flash Save & apply Cancel	
Reset this port :	Reset
Set this port as factory default :	Set
Port title	
Apply all ports settings	
Host mode configuration	
Serial port parameters	
Port logging	
Port IP filtering	
Authentication	
User access control	
Alert configuration	

RealPort support

RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host and allows applications to talk to devices across a network as though the devices were directly attached to the host. In actuality, the devices are connected to a Digi device server or terminal server somewhere on the network.

RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput.

When you use RealPort (configured on a per port basis) the Digi CM unit functionality is unavailable. That is to say that the Digi CM unit can be used for console management or for RealPort COM re-direction but not both. An example of RealPort use would be remote kernal debugging of Microsoft Windows Servers. To enable RealPort use the following procedure.

Note RealPort does not support authentication and user rights are not validated.

1. To enable RealPort click **Serial port** > **Configuration** > Port number.

2. Select **Enable this port** from the drop-down menu.

3. Select **Enable RealPort support** from the drop-down menu.

4. Click **Save to flash** and continue with other configurations or click **Save & apply**.

Resetting ports

The Digi CM unit allows you to restart all processes associated with a port and to disconnect all sessions.

To reset an individual port:

1. Click **Serial port** > **Configuration** > **Port number**.
2. Click **Reset this port: Reset**.

Reset individual port settings

Individual ports can be reverted to factory defaults.

1. Click **Serial port** > **Configuration** > **Port number**.
2. Click **Set this port as factory default: Set**.

Port title

The Digi CM unit offers multiple ways to configure the port title; both manually and automatically. The default is set to "Port Title # xx" with xx being the port-number.

Automatic Device Recognition allows the Digi CM unit to evaluate the attached devices and populate the port title. Additionally the Digi CM unit can generate a SNMP trap or send an email in case the response of the device changes or it stops responding.

Active detect

If **Active detect** is selected, a configurable probe string (carriage return =0x0d by default) is sent to the console port and the response is saved to a file at /var/run/systemrep_raw.portxx with xx being the port number.

This file is parsed using a script /tmp/cnf/active_detect and the operating system and device name are written to files: /var/run/HostnamePortxx and /var/run/OSPortxx.

The commands to parse the system response are user customizable, so if a device is not recognized immediately by the Digi CM unit, add a rule to the file.

Passive detect

If **Passive detect** is selected, no probe string is sent to the attached device but the port buffer is analyzed.

The script /tmp/cnf/passive_detect is executed and the results are saved to files: /var/run/HostnamePortxx and /var/run/OSPortxx.

After editing the scripts as either active_detect or passive_detect, save them to flash using the saveconf command so they are not lost after a reboot.

Configure Automatic Device Recognitiion

Configure a serial port for Automatic Device Recognition.

1. Access the web interface.

    Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial Port** heading, click **Configuration**.

3. Choose All or an Individual port > **Serial port parameters**.

4. Edit the fields as they apply to your configuration.

5. Click **Save & apply**.

Field	Description
Automatic detection	Enable or disable automatic detection of devices. **Use detected port title** - Enable if you want the Digi CM unit to automatically use the results of the detection mechanism to populate the port title. Disable if you want the default port title. If you choose Disable, you can still use the alarm feature.
Port title	Manually entered or automatically populated title of the port. The Digi CM unit allows access to a port by using only the number of the port title, making it unnecessary to know the serial port number. The default is set to "Port Title xx" with xx being the port number. The default is set to "Port Title xx" with xx being the port number.
Probe string	The probe string is an ASCII string that is sent to the device. Special characters are coded in hexadecimal values like:
	CR \x0d
	LF \x0a
	ESC \x1B
	Examples are:
	Parse string — output
	root\x0d\x0a — root<CR><LF>
	\x1Btest\x0d — <ESC>test<CR>
	\x1b\x20test\x0D — <ESC><Space>test<CR>
	\x1B\x20\x74\x65\x73\x74\x0d — <ESC><Space>test<CR>
Detected OS	Displays the result of the Active or Passive detection process.
Device detection method	If Active is selected a probe string is periodically sent to the device and the response is analyzed. If Passive is selected, the port logging is parsed to determine the device name and the OS.
Detection initiation	Active only if automatic detection is Enabled. Periodically or If new device is detected are the choices in the drop down menu. If Periodically is selected, the probe string is sent once every n minutes to the device while no connection is active to the serial port. When a new device is detected is selected, the probe string is only sent if a change on the DSR signal on the serial port is detected. Normally a device will activate the DSR signal if the serial port becomes active.
Detection delay	The delay before the first active detect process is started and between active detections.

Apply all ports settings

The Digi CM unit supports managing all ports simultaneously. If changes are made to the page "all ports", they are automatically applied to all ports. You can choose to exclude ports from this feature.

To enable/disable this feature for a port:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial Port** heading, click **Configuration**.

3. Choose an individual port > **Apply Port Settings**.

4. Select **Enable** or **Disable** from the drop down menu.

5. Click **Save to flash** and continue with other configurations or click **Save & apply**.

Note When changing a parameter for all ports, all settings of the complete page are applied to all ports.

Host mode configuration

The Digi CM unit provides four modes of communication between serial devices and remote hosts. Console server, terminal server, dial-in modem, and dial-in terminal server. These are described in the following sections.

Console server mode

Configuring a serial port as a console server creates a TCP socket on the Digi CM unit that listens for a Telnet or SSH client connection. When you connect to the TCP socket, you have access to the device attached to the serial port as though the device were connected directly to the network.

RawTCP is also supported with the Console Server Mode.
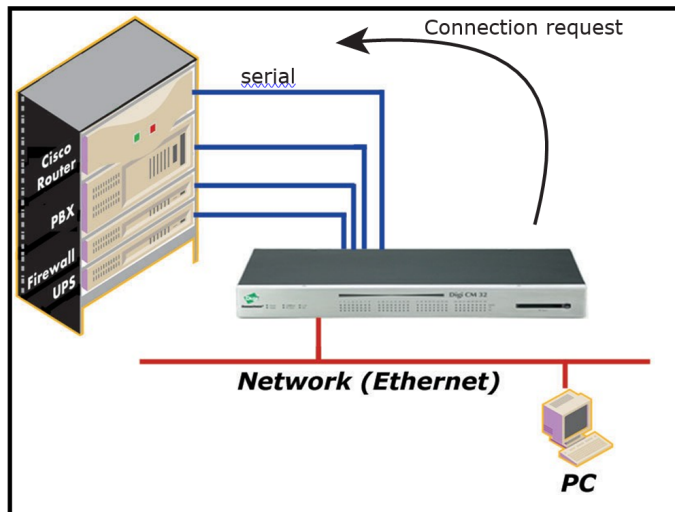
Terminal server mode

In terminal server mode, the Digi CM unit's serial port is configured to wait for data from the device connected to the port. If data is detected, the Digi CM unit starts a TCP session as a Telnet or SSH client to a pre-defined server. The server must be defined by you before the port can be configured for a Telnet or SSH client. This mode is used when you want to access servers on the network from a serial terminal. RawTCP is also supported with the Terminal Server Mode.
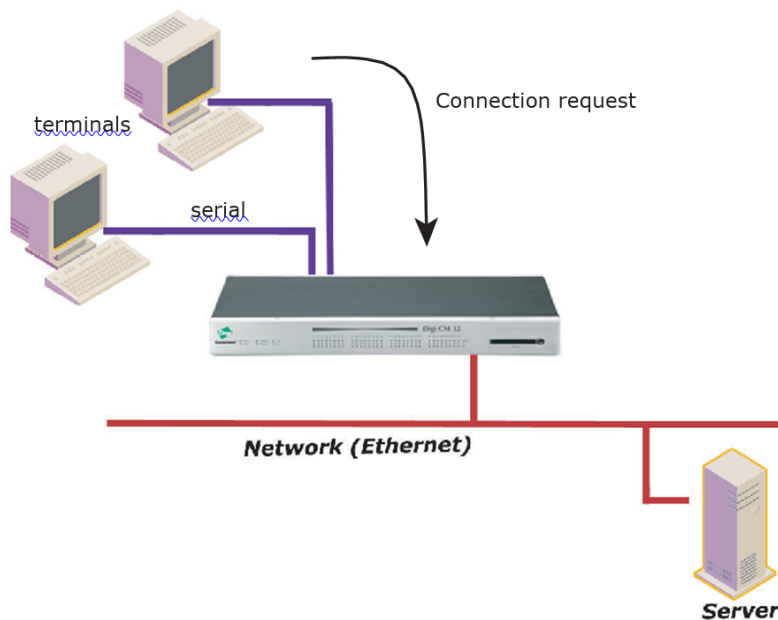
Dial-In modem mode

In this mode, the Digi CM unit assumes an external modem is attached to the serial port and is waiting for a dial-in connection from a remote site. When a user dials-in using a terminal application, the Digi CM unit accepts the connection and displays the appropriate prompt or menu for you that logged in.

Example: User 'root' would see the command line interface (CLI), whereas the user 'admin' would see the config menu or CLI depending on the shell for that user.
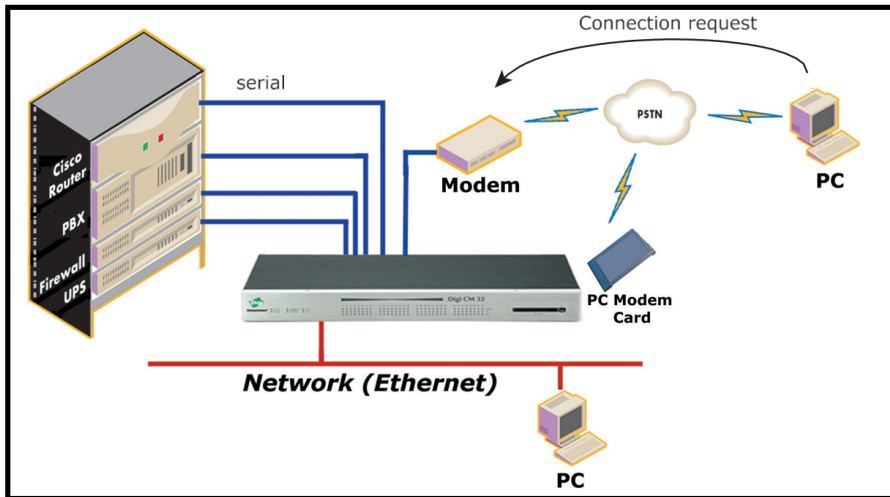
Dial-In terminal server

Dial-in terminal server mode is a combination of the terminal server mode and the dial-in modem mode. In the dial-in terminal server mode, the Digi CM unit assumes the serial port is connected to an external modem and is waiting for a dial-in connection from a remote site. When you dial-in using terminal applications, the Digi CM unit accepts the connection as a Telnet or SSH client to a pre-defined server. This mode is most frequently used when you want to use modems to access servers on a network.
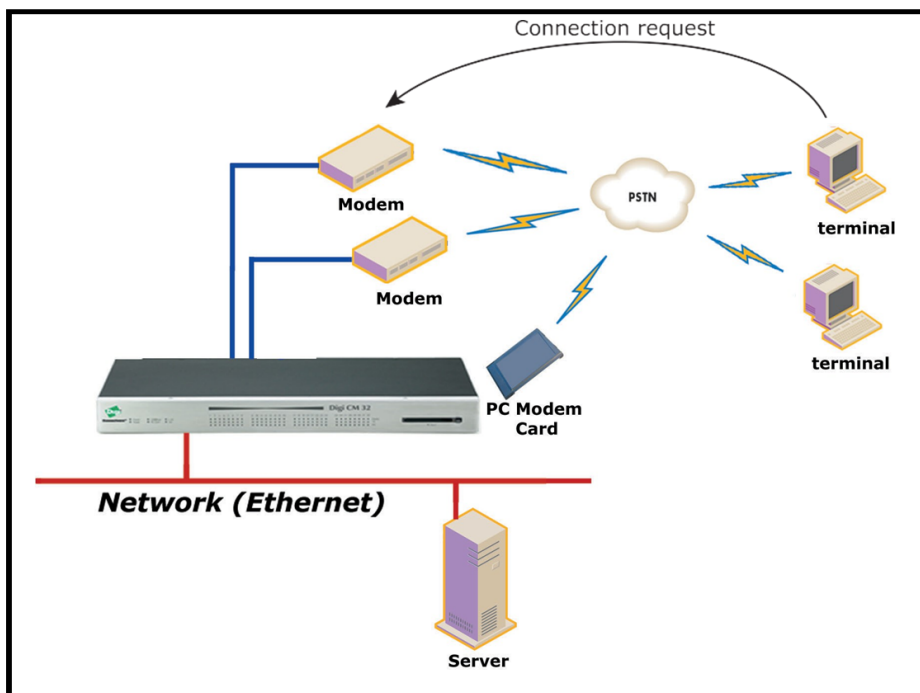
Configure host mode

To configure a serial port for host mode, enter the values in the applicable fields. To access the Host mode configuration screen, do the following:

1. Access the web interface.

    Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial Port** heading, click **Configuration**.

3. Choose All or an Individual port > **Host mode configuration**.

4. Fill in the highlighted fields as they apply to your configuration.

5. Click **Save & apply**.

Serial port configuration - All ports : Port Title	— Move to —
Enable/Disable this port	
Port title	
Host mode configuration	

Host mode :	Console server
Type of console server :	Other
Rackable Systems Mgmt Card :	Disable
Enable/Disable assigned IP :	Disable
Assigned IP :	0.0.0.0
Listening TCP port (1024-65535) :	7001
Protocol :	SSH
Inactivity timeout (1-3600 sec, 0 for unlimited) :	100
Enable/Disable port escape sequence :	Enable
Port escape sequence :	Ctrl- z
Port break sequence :	~break
Use comment :	No
Quick connect via :	Web applet
Web applet encoding :	English (latin1)

Save to flash   Save & apply   Cancel

Serial port parameters
Port logging
Port IP filtering
Authentication
User access control
Alert configuration

Field	Description
Host mode	The options are console server mode, terminal server mode, dial-in modem mode, and dial-in terminal server mode.

Field	Description
Type of console server	The options are MS SAC - English and MS SAC - International which you use to provide a graphic user interface to the Windows Server 2003 Special Administration Console (see Microsoft SAC support) and Other, which you use in all other cases.
Rackable Systems Mgmt Card	Enable to use Rackable Management card.
Enable/Disable assigned IP	Determines whether an IP address will be assigned to the port. The default is Disabled.
Assigned IP	Also known as alternate IP, this field assigns an IP address to the port, enabling you to Telnet directly to the serial port using an IP address (without having to specify a TCP port).
Listening TCP port	This is the TCP port you will specify when connecting directly to the port using Telnet or SSH.
Protocol	The options are SSH, RawTCP, and Telnet. Inactivity timeout - In seconds, the time set for inactivity to trigger an action. Setting the timeout to 0 (zero) means no timeout.
Enable/Disable port escape sequence	Allows the port escape sequence to function.
Port escape sequence	The key combination to initiate port escape.
Port break sequence	The sequence of characters that sends a break character to a device.
Use comment	Determines whether a port user is prompted to add a comment each time the port is accessed.
Quick connect via	Determines method for connecting to a port when in console server mode. Available with Telnet.
Web applet encoding	Supported languages for Java terminal.

Supported protocols

In configuring a serial port, you have three protocol options. The three protocols available are: RawTCP, SSH, and Telnet. Choose SSH as the protocol when logging in from an SSH client program to access a port. Choose RawTCP when connecting directly to a TCP socket. Choose Telnet when logging in from a Telnet client program and accessing the ports. Use the Host mode configuration page in the web interface to select the correct protocol.

Serial port parameters

In attaching a serial device to the Digi CM unit's serial port, the port parameters must match. The serial ports by default are enabled, meaning you have full access to the port. To configure the port

parameters for the Digi CM unit, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

   ---

2. Under the **Serial Port** heading, click **Configuration**.
3. Choose All or an Individual port > **Serial port parameters**.
4. Fill in the serial port parameters. The following are the defaults: bps=9600, data bits=8, parity=none, stop bits=1, flow control=none, and DTR behavior=High when open.
5. Click **Save & apply**.

DTR behavior

DTR can be set on the serial port to one of three settings: always high, always low, or High when open. Setting the DTR to High when open keeps the DTR high if a TCP connection is established. The DTR setting cannot be set by you when the host mode is configured for dial-in modem or dial-in terminal server mode.

Inter-character timeout

This setting is only available when the host mode protocol is set for RawTCP. The parameter sets the time value for the Digi CM unit to transfer data stored in the buffer. The Digi CM unit transfers data when the buffer is full using the TCP/IP protocol. However, if it is not full, the Digi CM unit will also transfer data dependent on the timeout value selected.

Specialty Use of Port: When data is processed in chunks

Some applications are written to process only chunks of data rather than continuous streams of data. The Digi CM unit supports "chunking" holding back data from the serial device to the application on the network until it detects a delimiter - at which point it sends the data to the application.

To configure a port for this mode:

1. Open a web connection to the Digi CM unit.
2. Click **Serial Port** > **Configuration**.
3. Select **All ports to configure**.
4. Click **Host Mode configuration**.
5. Select **Serial port parameters**.
6. Configure the delimiter and supporting settings. Descriptions of the options follow.

- **Enable/Disable delimiter** - Allows delimiter to function.
- **Delimiter** - Define the sequence that should be received before forwarding the data to the application
- **Delimiter option** - with delimiters - sends the delimiter as part of the data to the application without delimiters - remove the delimiter before sending the data to the application
- **Inter character time-out timeout** - In msec (1-10000) If no delimiter is detected the data is delivered after this timeout has elapsed.

Remote ports

The Digi CM unit supports remote ports. Remote ports are any type of port that can be accessed using Telnet or SSH protocol. Types of ports include ports that are provided using PortServer Terminals Servers or Sun ILOM ports. This feature establishes the Digi CM unit as the central access system for any kind of text based out-of-band management. Using the Digi CM unit as a central access system has multiple advantages:

- Central point of access
- Central user authentication
- Capturing of every user transaction on the remote system
- Keyword monitoring and alarm while connection is up

Configure remote ports

To configure a remote port use the following procedure.

1. Access the Digi CM unit's web interface.
2. Under the **Serial Port** heading click **Configuration**.
3. Scroll down the page to the section called **Remote port configuration**.
4. Enter the port title and click **Add**. A confirmation dialog displays.
5. Click the port title to access the configuration menus.
6. Select **Remote port parameters**.
7. Enter the IP address, port number, and protocol to use.
8. Confirm you selections by clicking **Save & apply**. A confirmation dialog displays to confirm the successful execution.

Note If you want to use a Digi PortServer TS 2 as remote device you would configure: IP address as assigned, IP port 2001 for port 1 or 2002 for port 2 and telnet or 2501/ 2502 when using SSH as protocol.

All other settings of the remote port are equivalent to the settings of a local serial port.

Access a remote port

You can connect to a remote port using the web, Telnet or SSH client. You can also use the port access menu or a custom menu to simplify navigation.

Method	Description
Web Access	Click **Serial ports** > **Connection** > Port number. Remote ports are sorted below the physical serial ports as V1...
Telnet	Telnet to the IP and the port number (the specific port number is defined on the 'Host mode configuration' page). `telnet 143.191.3.9 7051`
SSH to the port number	SSH to the IP and the port number (the specific port number is defined on the 'Host mode configuration' page).

Method	Description

SSH to the port name	SSH to the IP and the port number (the specific port number is defined on the 'Host mode configuration' page).
	`Ssh user-name:'t=port-title'@ip-Address`
	`Ssh sunadmin:'t=Switch3level':@MainDigi`
	You can access a remote port just like any local port: directly using the portnumber.

The parameters of the remote port are equivalent to regular serial ports. Enter any additional parameters for the remote and click **Save & apply** or **Apply all changes**.

Alerts and notifications

The Digi CM unit can be configured for system alerts and notifications. It sends email messages when the number of system log messages reaches a certain value or when an alarm message is detected in the serial port data. The Digi CM unit uses SMTP (Simple Mail Transfer Protocol) for sending the notifications. To use SMTP, the system administrator must configure a valid SMTP server for sending the emails. The Digi CM unit supports three types of SMTP servers: SMTP server without authentication, SMTP server with authentication, and POP before SMTP.

The Digi CM unit also supports SNMP (Simple Network Management Protocol), a protocol used to manage a network and monitor devices on a network. System and port alerts can also be sent using SNMP traps. The Digi CM unit supports both versions 1 and 2 of the SNMP protocol. The main function of SNMP on the Digi CM unit is to allow a system administrator to query remote devices for information.
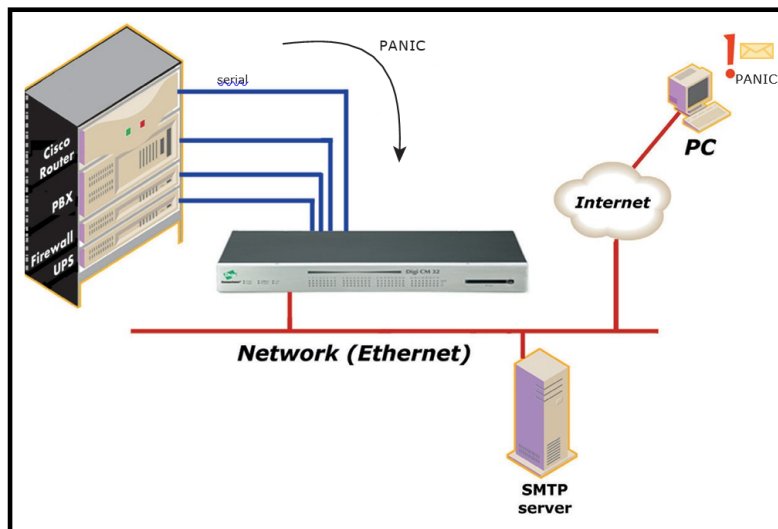
Configuring SMTP alerts

Most SMTP servers check the sender's email address with the host domain name to verify the address as authentic. Consequently, when assigning an email address for the device email address, any arbitrary username with the registered hostname may be used. An example is username@company.com.

To configure the Digi CM unit for SMTP alerts, the following parameters are required:

- **SMTP server** - Use either the hostname or the IP address.
- **Device mail address** - Specify the sender's email address for the log and alarm delivery.
- **SMTP mode** - Specify the type of SMTP server to use.
- **Username and password** - These fields are required for POP before SMTP and SMTP with authentication servers.

To configure SMTP alerts on the Digi CM unit, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Network** heading, choose **SMTP configuration**.

3. Fill in the required fields. SMTP with authentication and POP before SMTP require usernames and passwords.

4. Click **Save & apply**.

SNMP information

Applications such as NMS (Network Management System) or an SNMP browser can exchange information with the Digi CM unit and control actions to the unit. The protocol functions defined for SNMP includes GET, SET, GET-Next, GET-Bulk, and TRAP. Below are the definitions of the protocol functions found in SNMP. Authentication, power on, and link up traps are supported.

Protocol	Function
GET	Queries a device for more information
SET	Makes changes to a device's state

Protocol	Function
GET-Next	After an initial GET query, goes to the next value
GET-Bulk	Retrieves tables of information and security functions
TRAP	Notifies a system administrator of a significant event

Traps

There are additional traps that can be set at the port level. The following table shows where the trap is under **Serial port** > **Configuration** on the web interface, trap name, configure options, and the trap functions. The MIBs for login traps can be found at http://ftp.digi.com/support/utilities/digicm/.

Trap Location	Trap Name	Function
Port access menu	Port login trap	Notify about any login action to the port access menu (succeed and fail)
Alert configuration	Port login trap	Notify about login to this specific port (succeed and fail) (only available if host mode is set to "Console server")
Alert configuration	Device connection trap	Notify about a change of the DTR signal line (only available if host mode is set to "Console server")
Alert configuration	Active detection trap	Notify about changes in the device's response to the probe string (see also Web interface, only available if host mode is set to "Console server")
Alert configuration	Dial-in modem test trap	Notify about modem test (succeed and fail) (only available if host mode is set to "Dial-in modem")
Port event handling	Keyword notification trap	Notify about the occurrence of a keyword in the port log (only available if host mode is set to "Console server")

Configure SNMP

To configure the Digi CM unit for SNMP do the following:

1. Access the Digi CM unit's web interface.
2. Under the **Network** heading, choose **SNMP configuration**.
3. Fill in information for the MIB-II system objects section and choose Yes under EnableAuthenTrap. The fields are described in the following section:
   - **sysContact** - Identity of the contact person managing the MIB-II system.
   - **sysName** - The name identifying the system. By convention, this is the fully qualified domain name of the Digi CM unit. An example is: DigiPassport@companyname.com.
   - **sysLocation** - The physical location of the unit such as Room 264 or Engineering Lab.

- **sysService (Read only)** - A series of values, separated by commas, indicating the set of services the system provides. By default, the Digi CM unit only supports Application (7) service level.
- **EnablePowerOnTrap** - Determines whether the SNMP agent generates a trap each time the Digi CM unit is started.
- **EnableAuthenTrap** - Indicates whether the SNMP agent process is permitted to generate authentication failure traps.
- **EnableLinkUpTrap** - Determines whether the SNMP agent generates a trap each time the network connection comes up.
- **EnableLoginTrap** - Determines whether the SNMP agent generates a trap for each login.

Note Trap values override all other configuration information, meaning all other authentication failure traps can be disabled with this setting.

4. Enter Access control settings based on the following field descriptions:
    - **IP Address** - Defines what applications can access the Digi CM unit's SNMP agent to exchange information and control actions. If no IP addresses are listed, any application can access the SNMP agent.
    - **Community** - The options are public or private.
    - **Permissions** - The options are Read only or Read/Write.
5. Enter Trap receiver settings based on the following field descriptions:
    - **IP Address** - Enter the IP address of the device receiving the trap alerts.
    - **Community** - The options are public or private.
    - **Version** - Choose the SNMP version, either version 1 or version 2c.
6. Click **Save & apply**.

Manage the SNMP protocol

The Digi CM unit 's SNMP protocol can be managed using an NMS or SNMP browser. However, before the NMS or SNMP browser can access the data, the Access control settings must list the IP address of the host from which the browser is executed. See the preceding graphic for details.

Configure port event handling

Once an SMTP or SNMP server has been configured, it can be used to send port-related alerts and notifications. The following describes how to configure a port for port event handling.

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Choose **Serial port** > **Configuration**.
3. Choose a port to configure and then **Port logging**.
4. Select **Enable**.

5. Choose **Save & apply**.

6. Choose **Port event handling**. The following page appears.

7. Select an action and enter the keyword for the port event handling.

8. Enable Email notification.

> **Note** It is assumed that SMTP is configured first. If not, see Configuring SMTP alerts.

9. Enter the **Title of Email** (subject line).

10. For **Case sensitive**, choose **Enable** or **Disable**.

11. Enter the email recipient's address.

12. Enable SNMP trap notification.

13. Enter the title of the trap.

14. Choose either to use the global SNMP settings by enabling **Use global SNMP configuration** or specify special settings for this port.

15. Enter the IP address of the trap receiver.

16. Enter the SNMP community.

17. Select the version.

18. Complete configuration and then choose **Save & apply**.

> **Note** Key word is any text string that will trigger an alert when it traverses the serial port.

Configure alerts for Automatic Device Recognition (ADR)

Before configuring the alerts for Automatic Device Recognition, be sure you have configured the port for ADR as described in Configure Automatic Device Recognitiion.

1. Access the web interface.

> **Note** Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial Por**t heading, click **Configuration**.

3. Choose All or an Individual port > **Alert Configuration**.

4. Follow the Email Alert steps to configure the email alert or follow the SMTP Notification to configure SMTP.
    - Email Alert
      a. Enable **Email Alert for active detection**.
      b. For **Title of Email**, enter the email subject line.
      c. Enter Name and email address where the email should be sent.
    - SMTP Notification
      a. Enable "Active detection trap".
      b. Configure the trap receiver by one of the following two ways:
          - Enter **Use global SNMP configuration**.
          - Enter the IP address of the trap receiver, the SNMP trap community, and select the version

5. Complete configuration and choose **Save & apply**.

User administration

Required privileges

Only root and admin can administer users. The root user has unlimited administration privileges. Admin can view and change all attributes except those that belong to the root user.

There are several ways to manage users. A user can be added, edited, or removed. Multiple users can be managed in Groups or Access lists. The difference between Groups and Access lists are that Groups are established in the operating system on the Digi CM unit and privileges are predefined such as Root or Admin and are used most often for configuration. Access lists allow access to the ports and are created by defining the privileges of the lists. Access Lists manage rights of multiple users at the same time. Multiple users with the same rights are associated with an access list. This allows the administrator to simplify the overall administrative process.

Maintain users

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under **System administration**, choose **Users administration**. The following screen appears.

   Note The username on the Digi CM unit is case sensitive.

3. Do one of the following:

To...	Do the following....
Add a user	■ Click **Add**. ■ Fill in the attribute fields. See Add an Access List to the Digi CM Unit for information on attribute fields. ■ Click **Add**.
Edit a user	■ Click on the username. ■ Fill in the attribute fields. See the table that follows for information on attribute fields. ■ Click **Submit**.
Remove a user	■ Check the box that corresponds to the user you want to remove. ■ Click **Remove**. ■ Choose **OK** at the prompt.
Create an Access list	■ Under System Administration, click **Access List**. ■ Enter the name of the **Access List** and click **Add**. ■ Click on the access list name to add users. ■ Add the users to the access list. **Note** The name field in the **Access list** allows you to add users that are not locally configured on the Digi CM unit but use a centralized authentication method like RADIUS, LDAP etc. To change the privileges of an Access list, see Change the privileges of an access list.

4. Click **Apply Changes**.

Add an Access List to the Digi CM Unit

1. Access the web interface of the Digi CM unit.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under System Configuration choose **Access Lists**.

3. Enter the access list name into the edit-box and click **[ADD]**.

4. A pop-up windows will appear confirming the successful addition of an access list.

5. You can add users to the access list.

   a. Click the name of the access list. A configuration window displays.

   b. Add one user at a time to the list.

      i. Enter the name into the edit-box.

      ii. Click **[ADD]**.

⚠ **CAUTION!** Spelling is not verified against the local user database. This allows you to add externally configured users that only exist in the RADISU, LDAP or other central databases.

After an access list has been added to the system, port rights can be associated with it. See Configure security and authentication.

The following table describes the user fields.

Field	Description
User name	Name for the user, which must be between 3 and 29 characters and cannot include colons (:), less than or greater than signs (< >), ampersand (&), spaces, or quotation marks. The at sign @ and period . are acceptable. The username on the Digi CM unit is case sensitive.
Select group	Group to which the user is assigned. Groups include Root, System Admin, Port Admin and User. See User groups for more information.
Password	Password to assign to the user. This must conform to the rules stipulated above for a user name.
Confirm Password	Confirms the password.
Shell program	Interface presented to the user when he/she logs on to the system from a Telnet or SSH connection.
SSH public key authentication	Alternative method of identifying yourself to a login server. More secure than just a password.
SSH public key to use	Current public file key or create a new public file key.

Field	Description
Select new SSH public key version	SSH1 only supports one type of key SSH2 supports both RSA and DSA key types
Select new SSH public key file	Location for the SSH public key file

Configure security and authentication

The Digi CM unit provides four methods for controlling access to the network and the devices on the network:

- Restricting or permitting IP filtering

  This method allows or prevents users with specific IP addresses from accessing devices or serial ports on the network. IP filtering can be permitted or restricted for all ports globally or per port.

- Restricting or permitting specific users

  You easily can add users to or remove them from a list of restricted or permitted users list.

- Enabling sniff session access

  This method allows multiple users to access a single port.

- Using a central point (System administration > Security profile) where you establish security parameters per network, port, or password.

The Digi CM unit supports several authentication methods, including:

- Local
- RADIUS
- TACACS+
- LDAP
- Kerberos: The Kerberos module is not part of the normal firmware because of memory constraints. You can download the module from digi.com and place onto /usr2/ if required. To copy files to /usr2/, use a scp tool such as WinSCP.
- Custom PAM. You can configure authentication so that a secondary method is attempted if the primary method fails.

Configure network IP filtering

The Digi CM unit offers built-in firewall functionality to limit TCP/IP traffic to and from certain networks, TCP ports, and interfaces. The functionality implemented is based on the Linux tool IP tables.

The next scenario shows that access to the device connected to the Digi CM is allowed only on the .1 subnet. The device at 192.168.1.108 can access the device connected to the Digi CM because it is in the range allowed by the IP Filter rule.

Filter IP: 192.168.1.0
Filter Mask: 255.255.255.0
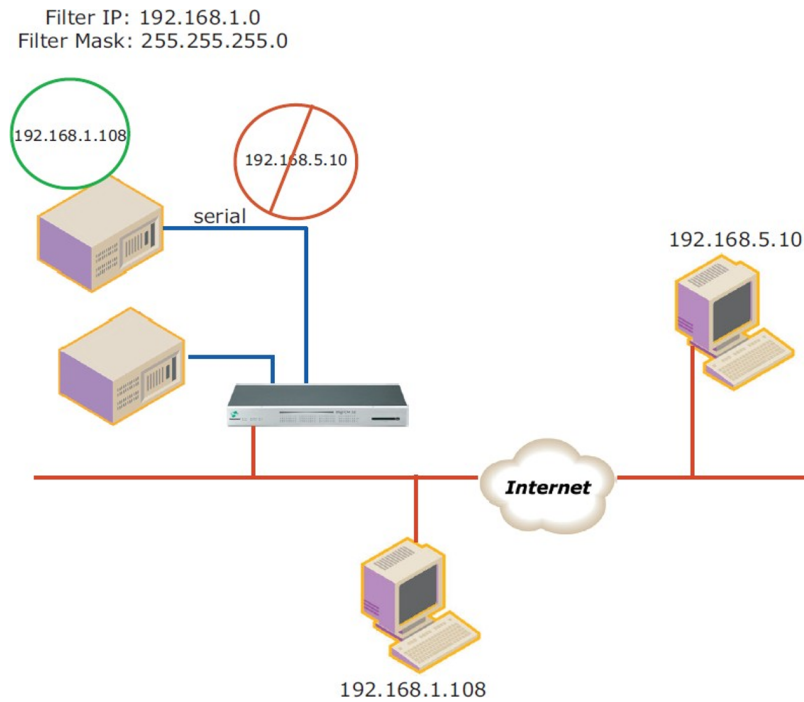
It is also possible to enable or disable specific services of the Digi CM unit by creating IP Filtering rules:

- Telnet console (TCP/IP port 23)
- SSH console (TCP/IP port 22)
- Web configuration (TCP/IP port 80)

The fields are described next:

Interface - The name of the network interface through which a packet is received. The name can be one of these values:

- eth0: the default Ethernet interface of the Digi CM unit
- eth1: the secondary interface added by using a PC card or wireless card
- all: both interfaces

Option - Determines that the rule will be applied to the IP address/Mask specified or its inverse; that is, the rule will be applied to all except those specified.

- Normal: applied to the hosts that are included
- Invert: applied to the hosts that are excluded

IP address/Mask - Specifies the host range by entering base host IP address followed by "/" and subnet mask. The host range can be one of the following scenarios by changing the value:

- Only one host of a specific IP address
- Hosts on a specific subnet
- Any host

Specified host range	Input format
Any host	0.0.0.0/0.0.0.0
192.168.1.120	192.168.1.120/255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0/255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0/255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0/255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128/255.255.255.128

Protocol - The protocol that is being accepted on or dropped from the port:

- TCP
- UDP
- ICMP

Port - A TCP/IP port on the Digi CM unit that other hosts try to access. You can specify either one port, using a single value, or a range of ports in this form

`: port1:port2`

where

`port1` defines the lowest port and `port2` the highest port.

Chain rule - Determines whether access from the hosts is allowed:

- ACCEPT: Access allowed
- DROP: Access not allowed

To add a new IP filtering rule, enter the values for the parameters and click the **Add** button on the right side of the table.

To remove a rule, click the **Remove** button.

After you finish editing the table, save the settings to flash:

- To save your changes, use the **Save to flash** button.
- To save and apply your changes, use the **Save & apply** button.

Be aware that you must apply the changes to make them active. This screen shows five established IP rules.

This table describes the rules.

Rule	Description
#1	Defines SSH access to the Digi CM unit (port 22). ■ The Normal option specifies that the rule applies to all addresses listed. ■ The rule says to Accept traffic from these addresses for Port 22.
#2	Defines Telnet access to the Digi CM unit (port23). ■ The Invert option specifies that the rule applies to all addresses except those listed. ■ The rule says to Drop traffic from all addresses not listed.
#3	Define access to the Digi CM unit using HTTP (port 80). ■ Rule 3 blocks all traffic. ■ Rule 4 allows access from IP address 192.168.1.0. ■ Rule 5 allows access from IP address 192.168.2.0.

Allowable Hosts	Input format Base hose IP address	Subnet Mask
Any host	0.0.0.0	0.0.0.0
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 ~ 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 ~ 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 ~ 192.168.1.254	192.168.1.128	255.255.255.128

Configure User Access Control

Another method for controlling access to the serial ports on the Digi CM unit is the User Access Control configuration. You can set up this configuration either globally (using the All Ports option) or per port.

It is not necessary to have users added to the system to assign rights. However, for the permissions or restrictions to be enforced, the username must match exactly. The username is case sensitive, and the application does not recognize misspellings.

To add users, click on "System administration > Users administration". For details about adding users, see User administration.

Note Users do not need to be authenticated locally; they can be users on any configured authentication server.

Using Access lists, you can add rights to a single user or to multiple users at the same time. In addition, you can group multiple users and assign one, some, or all these rights:

- Port access rights
- Port monitor rights
- Power management rights to an access list. For more information, see Create an Access list.

This scenario shows a configuration with a restricted user: Joe does not have access to the Sun server, while Mike does.
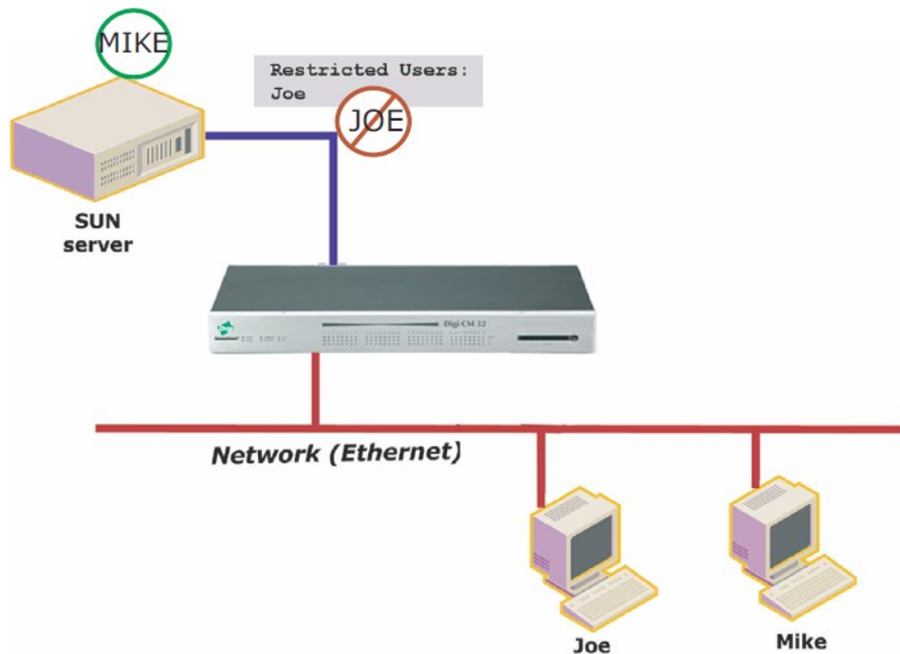
Your strategy for assigning rights to a port can include:

- Allowing <<Everyone>> access to a port and then restricting access to certain users -or-
- Specifying each individual user and their specific rights to a port.
- Adding a user to an established group (Access list) with preconfigured rights to a port.

If you check <<Everyone>>, all users, whether they are configured locally or are using a remote authentication (such as LDAP or Kerberos), have access to this port.

If you do not check <<Everyone>>, no users are allowed to access this port unless they are individually listed.

When you enter usernames for access permissions or restrictions, you must enter the username exactly as the username on the remote authentication server or configured locally. The username is case-sensitive.

In the next example, three users are configured on the Digi CM unit: Jeff, Tim and Paul. To give Tim and Paul read/write access and power access to this port, you could either:

- Grant rights to Paul and Tim
- Restrict Jeff's rights
- Add users to an Access list (in this example. sun-users) found under System administration > Access list. For more information, see Add an Access List to the Digi CM Unit.

Configure user access privileges

To configure user access privileges:

1. Select **Serial Port Configuration** > **All Ports** (or Port #)
2. Click **User access mode**.
3. Enter the users and their privileges, and click **Add user**.

Restrict a user's privileges

To restrict user access:

1. Under **Port configuration** > **User access control**.

2. Enter privileges for **<<Everyone>>**.

3. Enter restricted user's name, for example: **Jeff**

4. Enter the privileges this user has. Notice that **<<Everyone>>** has more access than **Jeff** does.

Note The usernames and passwords on the Digi CM unit are case-sensitive. Notice **<<Everyone>>** has access to Port, Monitor, and Power, while **Jeff** has access to only Monitor, with no Port or Power access.

Change the privileges of an access list

1. On the same screen shown in the previous procedure, select an access list from the drop-down box.

2. Click **Add access**, and then click **Save & apply**. When you add the access list, it will include Paul and Tim.

In this screen, the "sun-users" Access group has access to Port, Monitor, and Power, while any other users (**<<Everyone>>**) do not have access.

Types of users	Access types	How to permit or restrict
Only specific users have access "Permitted Users"	Access type is unchecked for Everyone (meaning All other users) does not have access	By listing specific users and checking the access types - (Permitting them access)
All users have access except for a few "Restricted Users"	Everyone has access to everything by checking the access types. If an access type is unchecked, all users are restricted from that access type.	By listing users and unchecking the access type they are restricted from using

Sniff Session

A sniff session enables multiple users to access a single serial port for viewing the data stream. Anyone who is registered for a sniff session can access a specific serial port —even if someone else is using the port. The Digi CM unit supports multiple concurrent sniff sessions.
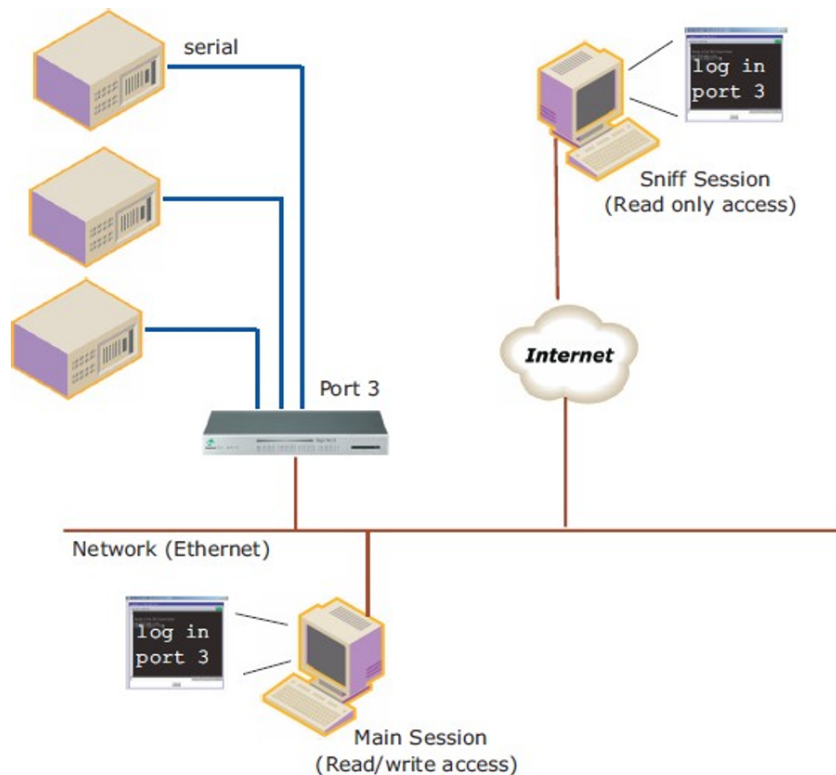
Sniff session mode has four options: disabled, input, output, and both. You configure the sniff session modes per port from the serial port configuration page.

Enable/Disable sniff mode

- **Disabled**: No one can enter a sniff session after the first user logs on.
- **Enabled**: Allows all users with access the following options in sniff mode: Sniff session display mode
- **server output**: View all data to a serial port from a remote connection
- **user input**: View all data from a serial port to a remote connection
- **both**: See all data transmitted or received through a serial port

Display data direction arrows

- **Enable/Disable**: Displays arrows to indicate the direction of data to or from the server. When the second user accesses the port, the global "Port escape menu" is displayed. See Port escape menu.

Permit monitor only mode

- **Enable**: A user with "Monitor" permissions can only connect to the port in read only mode any time.
- **Disable**: A user with "Monitor" permissions can connect if a read/write user has a connection to the port. A read-only session is automatically disconnected if the main user (read/write session) disconnects from the port.

Security Profile

The Security Profile tab, available under System Administration > Security Profile, provides a centralized access for enforcing site-appropriate, minimum security parameters on the CM. These are the available control mechanisms:

- System Security
- Password Security (Force heightened)

System security

SNMP

The CM allows you to use Get and Set commands for easy remote configuration and monitoring. You can configure Get and Set individually using the Network > SNMP Configuration interface.

This option gives you a simple method for globally disabling any SNMP queries. (Traps always can be sent if they are configured). In the Default configuration, SNMP is disabled.

Discovery (ADDP)

Enables/disables the discovery protocol. While this is convenient for initial discovery of units on the network, this service is often disabled when the system is ready for production, unless the system is deployed on a controlled LAN.

Telnet

Disabled by default, this feature can be enabled afterward if the customer does not plan to use network security.

SSH

Usually remains enabled; in some environments, however, access is allowed only by a totally out-of-band connection (hard-wired serial, dial-up modem, or both). In such situations, the Ethernet connection is used only for reports and alerts.

SSHv1

SSHv1 (Secure Shell Version 1). SSHv1 uses server and host keys to authenticate systems. This service is disabled by default.

HTTP

Enables/disables access to the Digi CM using the Web interface. By default, HTTP is redirected to HTTPS.

HTTPS

Enables/disables access to the Digi CM using the Web interface. This service is enabled by default. If, however, the unit will be deployed outside a controlled LAN, HTTPS is often disabled to limit the number of services available.

All Ports

Enables/disables access to all ports using any protocol.

Set all ports to

Specifies the protocol to be used on all ports. The default is Telnet.

Stealth Mode

Makes the Digi CM "invisible" on the network and exposes only ports that are used to provide access. In Stealth Mode, the CM does not reply to pings or traceroutes and does not respond to communication attempts on unused TCP/UDP sockets.

Password security

To enhance password security, you can use these settings:

- **Minimum password length**: Allows passwords that are 3 to 255 characters long; also allows spaces in passwords

- **Maximum password age**: Specified in days. To disable this setting, enter 0.

- **Enforce password complexity**: Cannot include all or part of a user's account name. Passwords must be at least eight characters long. If you enable Minimum Password Length, passwords can be 8-255 characters long and must include three of these four categories of characters:
  - English uppercase characters (A-Z)
  - English lowercase characters (a-z)
  - Base 10 digits (0-9)
  - Non-alphabetic characters (!, $, #, %, and so on)

- **Enforce password history**: Cannot reuse the last nine passwords

Authentication

The Digi CM unit supports multiple methods of user authentication, including local, TACACS+, RADIUS, RADIUS Down-Local, LDAP, Kerberos, and Custom PAM. The authentication protocol you use depends on your environment.
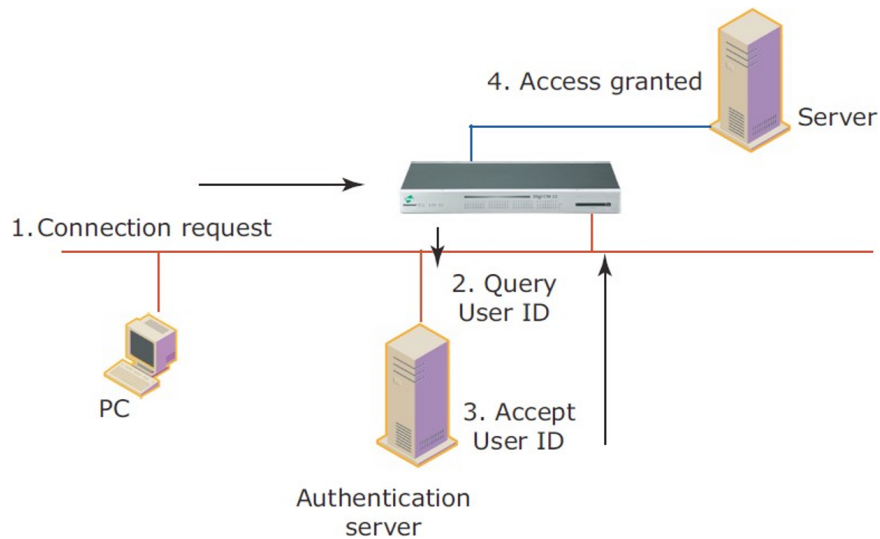
Configure authentication methods for port access

You can choose between having a single authentication method, such as RADIUS, or an authentication method where a Local authentication service is used in addition to the RADIUS, LDAP, TACACS+ server, or Kerberos. These options are listed when you configure the Digi CM unit for authentication. To configure the Digi CM unit for authentication, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial port** heading, choose **Configuration**.
3. Choose All or an Individual port > Authentication.
4. From the drop-down menu, choose an authentication method. A configuration screen for the authentication method you choose is displayed. This figure displays the options for setting up a RADIUS server as the primary authentication server and Local authentication if the primary authentication method fails.

> **Note** Remote authentication to Port access menu can be obtained from **Serial port** > **Configuration** > **Port access Menu**.

5. Fill in the applicable fields.

6. Choose **Save & apply changes**.

Configure authentication for the web server

1. Access the web interface.

> **Note** Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Choose **Network** > **Web server configuration**. This screen opens.

3. Choose an authentication method and then click **Save & apply**.

When you are using remote authentication for the web server, such as RADIUS, RADIUS Down-local, TACACS+, LDAP, Kerberos, or Custom PAM, you must also be added to the local database. The user password must be different from local authentication; otherwise, the CM will authenticate against the local database instead of the remote one. For details, see User administration.

When your password is approved by the authentication server, the Digi CM unit uses the local permission rights to provide access privileges for you to ports and the configuration.

LDAP authentication

The Digi CM unit supports authenticating against an LDAP-based database, including LDAP systems running on Linux servers as well as Microsoft Active Directory together with the LDAP gateway ADAM (Active Directory Application Mode).

If the Digi CM unit authenticates against an LDAP directory, all users must be configured in one container. The Digi CM unit will extend the username using the LDAP search base and authenticate the user.

In the next example, the domain is called dilbert.com, the LDAP server is at 10.1.1.1, and all users with access to the Digi CM unit are located in the container: USA Users

Configure the LDAP authentication as shown here:

```
Authentication method: LDAP server
First LDAP Server 10.1.1.1
```
Second LDAP Server
```
LDAP search base: ou=users,ou=usa,dc=dilbert,dc=com
Domain name for active directory:
```
If your LDAP database resides on a Microsoft system you also have to configure the Domain name for the active directory (dilbert.com in the above example).

Do not use this setting if you are using a non-Microsoft system as it changes the LDAP to comply with Microsoft syntax.

Custom PAM module

The Digi CM unit supports custom PAM modules for remote authentication. This allows you to create your own authentication schema or use any other third party PAM module. The module must o be compiled for the Digi CM unit's environment.

Digi offers an SDK for the Digi CM family.

To download the SDK, contact Digi technical support at www.digi.com/support.

1. Place the custom PAM modules onto: /usr/2 on the Digi CM unit.

2. Use an scp client (like WinSCP) to copy data to the /usr2 directory, or download the ftp client for the Digi CM unit from support.digi.com.

3. Make sure the module is flagged to be executable (chmod 755 ...)

   Note To activate the custom PAM module it has to be configured in the custom file located in /etc/ pam.d

4. Create a file called: /etc/pam.d/custom and add these lines:

```
auth required /usr2/my_pam _auth.so
session required /usr2/my_pam_ auth.so
```
(with the my_pam_auth.so being the "custom pam" module's name)

To keep this file permanently copy it to /usr2 and add a line to /usr2/rc.user.
```
Cp /usr2/custom /etc/pam.d/
```

Example of an rc.user file
```
#!/bin/bash #
# rc.user : Sample script file for running user programs at boot time
#
#PATH=/bin:/usr/bin:/sbin:/usr/sbin
# Add shell command to  execute  from  here cp /usr2/custom /etc/pamd/
exit 0
```

Custom and default menus

The Digi CM unit has several default menus for easy configuration and access by different users. Depending on access privileges, the menus available are the Web Interface, Configuration Menu, and Port Access Menu. A Custom Menu feature for creating menus is also available through the web interface.

The Custom Menu feature enables system administrators to create menus for specific users; in other words, system administrators can create a customized interface to selected ports. Custom menus can only be configured via the web however, they can only be accessed via the shell (command line).

Make custom menus

Before making custom menus, plan the kind of menus and menu items you want available to your users. A good plan would include the following:

1. Add users to the system.
2. Create a menu name with sort and display features.
3. Add menu items and submenus to the new menu.
4. Assign users to the menus.

Add users

You cannot assign users to a menu until you have added users to the system. To add users, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Choose **System administration** > **Users administration** > **Add**.

3. Enter the **User name** and **User group** from the drop down menu. Select **Custom menu** from the drop down menu for the **Shell program**.

4. Click **Add** to add the user.
5. Continue to add users as needed.

Note You do not need to **Save to flash** or **Apply changes** to add users.

Create menu names

To make a custom menu, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. **Custom Menu** > **Configuration**.
3. Enter the Menu Name to assign and click the Add Menu button. The menu is added.
4. Click the hyperlink to the menu you just created.
5. From the drop down menu, select the way to Sort and Display items.

Custom Menu - Menu Name: command

Menu Configuration

Menu Title: [The Command Menu]

Sort Items: [By Key ▼]

Display Items: [Automatic ▼]

[Save to flash]   [Cancel]

Menu Items

Submenus

6. Click **Save & apply**.

7. Repeat as required to create additional menus.

Add menu items

Once you have defined a menu name and added users, you can then add menu items. To add menu items, do the following:

1. **Custom Menu** > **Configuration** > Menu Name hyperlink for the menu you want to configure.

2. Choose **Menu Items** > **Add Item**. The following screen appears.

Custom Menu - Menu Name: Master - Item Configuration

Key: [b ▼]   Label: [   ]

○ Create new submenu
   Submenu Name: [   ]
◉ Go to an existing submenu
   Submenu Name: [▼]
○ Connect to serial port
   Serial Port: [1 ▼]
○ Connect to clustered serial port
   Clustered Slave: [▼]
   Serial Port: [1 ▼]
○ Telnet to a remote host
   Remote Host: [   ]
   Remote Port: [23   ]
○ SSH (Secure Shell) to a remote host
   Remote Host: [   ]
   Remote User: [   ]
○ Execute a custom command
   Custom Command: [   ]

[Apply] [Cancel]

3. Fill in the desired parameters. The parameters are:

   ▪ **Key** - Assign any letter or number except a value already used by another menu item.

   ▪ **Label** - Assign a label or name for the menu item.

- **Create new submenu** - Assign a name for a new submenu that this menu item will be assigned or linked to.
- **Go to existing submenu** - Choose an existing submenu from the drop down menu that this menu item will be assigned or linked to.
- **Connect to serial port** - Connects you to a specified port.
- **Connect to clustered serial port** - Connects you to a clustered port.
- **Telnet to a remote host** - Enter a remote host's IP address or hostname.
- **SSH (Secure Shell) to a remote host** - Enter the hostname or IP address of a remote host and the remote username.
- **Execute a custom command** - Enter a customized command that is any valid command on the command line with acceptable user privileges.

4. Choose **Apply**.
5. Repeat this procedure to add more menu items.

Note To add or configure submenus, select the Submenus hyperlink on the Menu Configuration page.

Assign users to a menu

Once a menu has been created, users can be assigned to the menu by doing the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. **Configuration > Custom Menu > Menu Users**. A list of available users is displayed.

Custom Menu Configuration	
Custom Menus	
Menu Users	
User Name	Assigned Menu
nicholas	defaultmenu ▾
root	command ▾
Note: You must add a user to the system in the Users administration page.	
Save to flash Cancel	
Menu Configuration	

3. Choose a menu for a user by selecting a menu from the drop down Assigned Menu list.
4. Choose **Save & apply**.

Default menu: Port Access menu

The Port Access menu is a flat (one level) menu showing all ports, port titles and the mode of each port.

Using the Port Access menu you have a complete overview of all ports and can initiate a connection to any of them.

When you choose to connect to a specific port, you are prompted again for the username and password.

```
[Digi_CM_Device]
===============================================================================
Port#        Port Title        Mode   Port#         Port Title        Mode
===============================================================================
1       Port Title #1           CS      2       Port Title #2           CS
3       Port Title #3           CS      4       Port Title #4           CS
5       Port Title #5           CS      6       Port Title #6           CS
7       Port Title #7           CS      8       Port Title #8           CS

 Enter command (1-8 serial port, P passwd, others for exit)
 ------>
```

There are multiple ways to access the Port Access menu:

- Assigned IP address. See Configure host mode.
- TCP/IP port 7000
- TCP/IP port 22 or 23 if the "Shell program" is set to "port access menu" for this specific user. See User administration.
- By calling "portaccessmenu" from the command line

The Port Access menu allows simple access to each port.

By typing the number of the port to connect to, the Digi CM unit initiates a connection to this port using the appropriate protocol (Telnet of SSH).

You can also change your own password by using the "P" Key.

If the Digi CM unit is configured to be the master in a master-slave scenario, the "S" key will bring up a list of all slaves. Selecting a slave will then spawn a connection to the Port Access Menu of the slave.

When using a Digi CM 48, not all ports can be displayed on one screen. Ports 33-48 can be viewed after hitting the <Enter> key.

Microsoft SAC support

About the Digi CM Unit's support for Microsoft Windows Server 2003

The Digi CM unit provides a browser-based user interface to Microsoft's text-based Special Administration Console (SAC), an integral part of Windows Server 2003 Emergency Management Services (EMS). Both the English and Japanese versions of SAC are now supported. When a server running Windows Server 2003 is connected to the Digi CM unit's serial port, key SAC functions-- normally accessed from the command line--are available from a graphical user interface (GUI). SAC features accessible from this interface include:

- Reset and shutdown
- Show performance values like memory utilization
- Show and configure IP settings per interface
- Show the process list and kill processes

Note While the EMS port is available at all times using Telnet or SSH, the special GUI is available only while SAC is active.
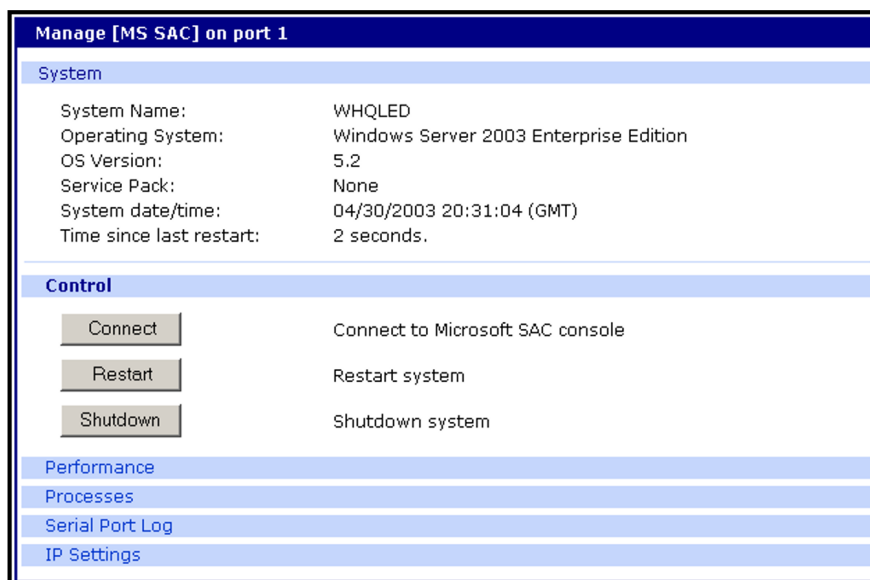
Setup overview

Setup for the Digi CM unit SAC support is a three-step process:

1. Set up the Windows Server 2003 for SAC support. To do this, ensure that the COM port used for console traffic is properly set up. This includes designating a COM port for console communication and setting the port speed (baud) appropriately. See Set up the Windows Server 2003 port.

2. Cable the console port on the Windows Server 2003 to the Digi CM unit's port. See About serial port cabling.

3. Set up the Digi CM unit for SAC support. See Set up the Digi CM Unit for SAC support.

Set up the Windows Server 2003 port

1. Sign on to the Windows Server 2003 as the administrator.

2. Access the command line.

3. Use the bootcfg command to redirect console traffic to the correct COM port. The following is the command syntax and an example. See the Microsoft documentation for additional information on the SAC feature.

Command syntax

```
bootcfg /ems on /port com# /id # /baud 115200
```

where:

- `com#` is the COM port to which console traffic will be redirected.
- `#` is the is the number of the boot entry.
- The port speed is set to the recommended rate, although you can use any rate supported by Windows Server 2003.

Command example

In this example, console output is redirected to COM 2, the boot entry is specified as 1, and the port speed set to 115200.

```
bootcfg /ems on /port com2 /id 1 /baud 115200
```

Set up the Digi CM Unit for SAC support

To set up a serial port to provide access to the Windows Server 2003 console port, do the following:

1. Access the web interface.

    Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Choose **Serial port** > **Configuration**.

3. Choose a port.

4. Choose **Host mode configuration.** The **Host mode configuration** page appears.

5. Set the **Host mode** to **Console server** and the **Type of console server** to MS SAC -English (or Japanese) console as shown in the following figure.

6. Set other fields as appropriate.

7. Click **Save & apply**.

8. Configure serial port communication settings, by doing the following:

    a. Choose Serial port parameters from the menu.

    b. Adjust settings as required. This includes ensuring that the Baud rate matches the setting on the Windows Server 2003 serial port and Flow control is set to None. Ignore the DTR behavior field.

    c. Click **Save & apply**.

Access the Windows Server 2003 Console port from the Digi CM Unit's GUI

To access the Windows Server 2003 console port, do the following:

1. Access the web interface.

    Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Choose **Serial port** > **Connection**. A screen similar to the following appears.

3. Click on the **title** of the port to which the Windows Server 2003 console port is connected. A screen similar to the following appears.

   Note If support for "Windows Server 2003" and "Rackable Systems Management Card" is selected a menu will appear and you must choose between the two functions.

4. Use the Digi CM unit's GUI to perform SAC functions. The following table describes attributes of the controls on the GUI.

Field	Description
Connect	Connects to the SAC console port via the command line interface.
Restart	Reboots the Microsoft Server 2003.
Shutdown	Shuts down the Microsoft Server 2003. Caution! This switches off the server and you can no longer access it remotely.

Field	Description
Performance	Provides access to Microsoft Server 2003 status information.
Process	Provides access to the process list, which allows you to view and kill active processes.
Serial Port Log	Provides access to port logging information.
IP Settings	Provides access to IP settings, enabling you to verify and change settings.

Configure Virtual KVM

Introduction

The Digi CM unit provides a method for gaining access to the graphical interface of a system using the network. Using this method, Virtual KVM, you specify a connection method and IP address to use to reach the system.

Supported methods include:

- Microsoft Remote Desktop Protocol
- VNC
- XManager for X Window System
- A user-defined option

An example configuration

This diagram shows the Digi CM managing a Linux SuSE 9.2 system, a Windows 2003 system, and an HPUX system.

Virtual KVM protocols

This table lists the Virtual KVM protocols and the client software with which each protocol has been tested.

Virtual KVM protocols	Tested client software
Remote Desktop	Windows 2000, XP, 2003 Remote Desktop Client Linux: rdesktop

Virtual KVM protocols	Tested client software
VNC	Windows: tightVNC, realVNC, UltraVNC Linux: vncviewer
X Window System	Windows: Xmanager Linux/Unix: X Window System

The rest of this section describes how to set up Virtual KVM with each of the supported methods and connect to a system through Virtual KVM.

Use Virtual KVM with Remote Desktop

This section describes how to:

- Configure Virtual KVM with Remote Desktop
- Connect to a system through Virtual KVM using Remote Desktop protocol

Configure Virtual KVM with Remote Desktop

To set up Virtual KVM with Remote Desktop protocol, follow this procedure:

1. Access the Digi Passport Web interface and log in.

2. Choose **Serial Port** > **Configuration**. This window opens:

3. Choose the port you want to configure, and then select the Virtual KVM tab. (In this example, port 1 is selected.) A window similar to this one opens, showing the serial port number and title.
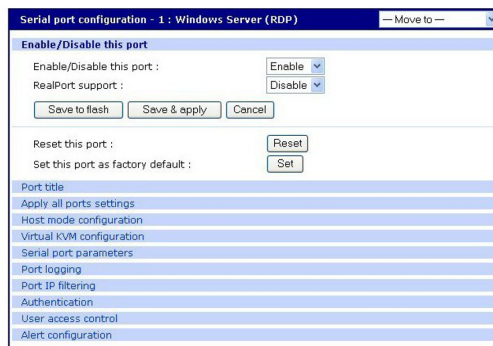
4. Click Virtual KVM configuration. This window opens:
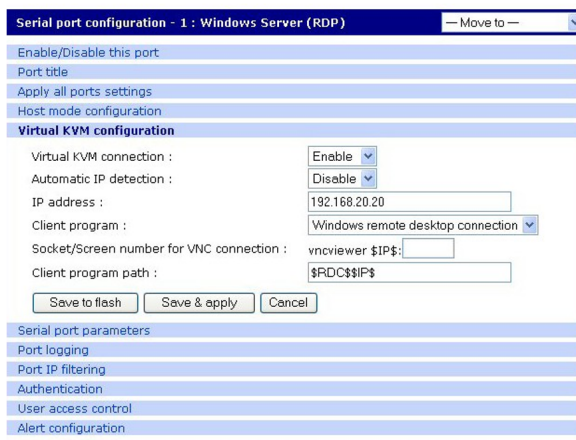
5. From the drop-down list next to **Virtual KVM configuration**, select **Enable**.

6. Then, from the **Client program** drop-down list, select **Windows remote desktop connection**.

7. If you are not using IP automatic detection, enter the IP address.

8. Click the **Save & Apply** button.

Note If you are using Remote Desktop configuration and you want to use automatic IP address detection, configure the host mode for the port to MS SAC console before you configure the Virtual KVM feature for the port. For more information, see Set up the Digi CM Unit for SAC support.

Connect to a system through Virtual KVM using Remote Desktop protocol

When you connect through the Connection window, and a Virtual KVM connection is configured, you now see:

- The terminal monitor button, which connects to the raw ASCII SAC console
- A mouse button (next to the monitor icon), which connects to the Virtual KVM graphical

interface

- The manage button, which connects to the SAC GUI screen

To connect through Virtual KVM using Remote Desktop, follow these steps:

1. Click on the mouse icon.

2. Click **OK** in each of the three Java confirmation request windows. The applet first checks whether the optional Virtual KVM Assistant is installed on the system. Then:

   - If the applet is installed, it starts Virtual KVM Assistant to manage the connection.

   - If the applet is not installed, the attempt to launch the Virtual KVM assistant fails, and the applet tries to launch the connection directly.

   - If the Virtual KVM Assistant is not installed, a message indicates that the first connection attempt failed. A second message indicates that the second connection attempt succeeded. This is normal behavior if the applet does not find the Virtual KVM Assistant. For more information, see Virtual KVM Assistant.

     The application starts and you see a message that the connection succeeded:
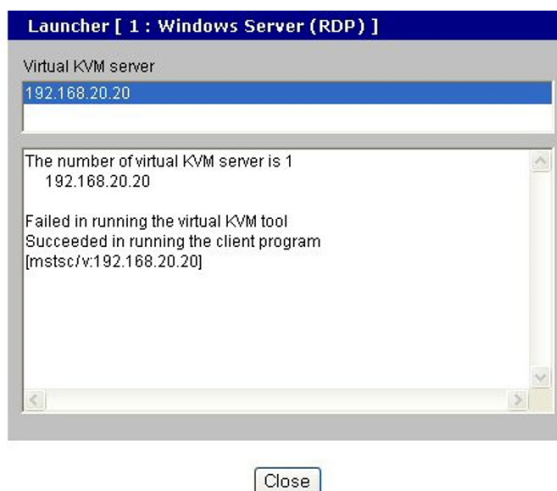
3. A login screen displays. Enter your user name and password, and then click **OK**.

    If the application does not start, check to make sure that the application is in the search path on your server. See Install programs for Virtual KVM.

Use Virtual KVM with VNC protocol

This section describes how to:

- Configure Virtual KVM with VNC protocol
- Connect to a system through Virtual KVM using VNC

Configure Virtual KVM with VNC protocol

To configure Virtual KVM with VNC protocol, follow this procedure:

1. Access the Digi Passport Web interface and log in.

2. Choose **Serial Port** > **Configuration**. This window opens:

Serial port configuration						
Port access menu configuration						
Port access menu configuration						
All port configuration						
Port#	Title	Mode	Base address	Port	Proto	Serial-settings
All	Port Title	CS	0.0.0.0	7001	Telnet	9600-N-8-1-No
Individual port configuration						
Port#	Title	Mode	Dest/AssignedIP	Port	Proto	Serial-settings
1	Windows Server (RDP)	CS	0.0.0.0	7001	Telnet	9600-N-8-1-No
2	Linux Server (VNC)	CS	0.0.0.0	7002	Telnet	9600-N-8-1-No
3	HPUX (XManager)	CS	0.0.0.0	7003	Telnet	9600-N-8-1-No
4	Port Title #4	CS	0.0.0.0	7004	Telnet	9600-N-8-1-No
5	Port Title #5	CS	0.0.0.0	7005	Telnet	9600-N-8-1-No
6	Port Title #6	CS	0.0.0.0	7006	Telnet	9600-N-8-1-No
7	Port Title #7	CS	0.0.0.0	7007	Telnet	9600-N-8-1-No
8	Port Title #8	CS	0.0.0.0	7008	Telnet	9600-N-8-1-No
9	Port Title #9	CS	0.0.0.0	7009	Telnet	9600-N-8-1-No
10	Port Title #10	CS	0.0.0.0	7010	Telnet	115200-N-8-1-No
11	Port Title #11	CS	0.0.0.0	7011	Telnet	9600-N-8-1-No
12	Port Title #12	CS	0.0.0.0	7012	Telnet	9600-N-8-1-No
13	Port Title #13	CS	0.0.0.0	7013	Telnet	9600-N-8-1-No
Remote port configuration						
☐	Title	Mode	Assigned IP	Port	Proto	Remote-settings
	No remote port found…					

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

Remote port title : [   ]   [Add]

3. Double-click the port you want to configure. A window similar to this one opens, showing the serial port number and title:

4. Select the **Virtual KVM** tab.

5. From the **Virtual KVM connection** drop-down list, select **Enable**.

6. Then, from the **Client program** drop-down list, choose the **VNC Client program**.

7. Adjust the **VNC socket/screen number**, if necessary. The default is 1.

8. Click **Save & Apply**.

Connect to a system through Virtual KVM using VNC

When you connect through the Connection window, and a Virtual KVM connection is configured, you now see:

- The terminal monitor button, which connects to the serial console
- A mouse button (next to the monitor icon), which connects to the Virtual KVM graphical interface.

To connect through Virtual KVM using VNC:

1. Click on the mouse button.

2. Click OK in each of the three Java confirmation request windows. The applet first checks whether the optional Virtual KVM Assistant is installed on the system:

   - If the applet is installed, it starts Virtual KVM Assistant to manage the connection.

   - If the applet is not installed, the attempt to launch the Virtual KVM assistant fails, and the applet tries to launch the connection directly.

   - If the Virtual KVM Assistant is not installed, a message indicates that the first connection attempt failed, and then another message indicates that the second connection attempt succeeded. This is normal behavior if the applet does not find the Virtual KVM assistant.

   The application starts, and you see a message that the connection succeeded:

3. The Virtual KVM VNC Connection opens. Enter your user name and password, and click **Login**.

   If the application does not start, check to make sure that the application is in the search path on your server. See Install programs for Virtual KVM.

Use Virtual KVM with X Window System Protocol and XManager software

This section describes how to:

- Configure Virtual KVM with X Window System Protocol and XManager Software
- Connect to a system through Virtual KVM using Xmanager

Configure Virtual KVM with X Window System Protocol and XManager Software

To set up Virtual KVM with X Window System Protocol and XManager Software, follow this procedure.

1. Access the Digi Passport Web interface and log in.

2. Choose **Serial Port** > **Configuration**. The following window displays:

Serial port configuration

Port access menu configuration

Port access menu configuration

All port configuration

Port#	Title	Mode	Base address	Port	Proto	Serial-settings
All	Port Title	CS	0.0.0.0	7001	Telnet	9600-N-8-1-No

Individual port configuration

Port#	Title	Mode	Dest/AssignedIP	Port	Proto	Serial-settings
1	Windows Server (RDP)	CS	0.0.0.0	7001	Telnet	9600-N-8-1-No
2	Linux Server (VNC)	CS	0.0.0.0	7002	Telnet	9600-N-8-1-No
3	HPUX (XManager)	CS	0.0.0.0	7003	Telnet	9600-N-8-1-No
4	Port Title #4	CS	0.0.0.0	7004	Telnet	9600-N-8-1-No
5	Port Title #5	CS	0.0.0.0	7005	Telnet	9600-N-8-1-No
6	Port Title #6	CS	0.0.0.0	7006	Telnet	9600-N-8-1-No
7	Port Title #7	CS	0.0.0.0	7007	Telnet	9600-N-8-1-No
8	Port Title #8	CS	0.0.0.0	7008	Telnet	9600-N-8-1-No
9	Port Title #9	CS	0.0.0.0	7009	Telnet	9600-N-8-1-No
10	Port Title #10	CS	0.0.0.0	7010	Telnet	115200-N-8-1-No
11	Port Title #11	CS	0.0.0.0	7011	Telnet	9600-N-8-1-No
12	Port Title #12	CS	0.0.0.0	7012	Telnet	9600-N-8-1-No
13	Port Title #13	CS	0.0.0.0	7013	Telnet	9600-N-8-1-No

Remote port configuration

☐	Title	Mode	Assigned IP	Port	Proto	Remote-settings
	No remote port found...					

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

Remote port title : [_____]   [Add]

3. Choose the port you want to configure. A window similar to this one opens, showing the serial port number and title:

4. Choose **Virtual KVM configuration**.

5. From the **Virtual KVM connection** drop-down list, select **Enable**. Then, from the **Client program** drop-down list, choose the **Xmanager program**.

6. Click **Save & Apply**.

Connect to a system through Virtual KVM using Xmanager

When you connect through the Connection window, and a Virtual KVM connection is configured, you now see:

- The terminal monitor button, which connects to the serial console
- A mouse button (next to the monitor icon), which connects to the Virtual KVM graphical interface.

To connect through Virtual KVM using X Window System Protocol and XManager Software:

1. Click on the mouse icon.

2. Click **OK** for each of the three Java requests in pop-up windows.

   The applet first checks to see if the optional Virtual KVM Assistant is installed on the system:

   - If the applet is installed, it starts Virtual KVM Assistant to manage the connection.
   - If the applet is not installed, the attempt to launch the Virtual KVM assistant will fail, and the applet tries to launch the connection directly.
   - If the Virtual KVM Assistant is not installed, a message indicates that the first connection attempt failed, and then another message indicates that the second connection attempt succeeded. This is normal behavior if the applet does not find the Virtual KVM assistant. For more information, see Virtual KVM Assistant.

3. The application starts, and you see a message that the connection succeeded:
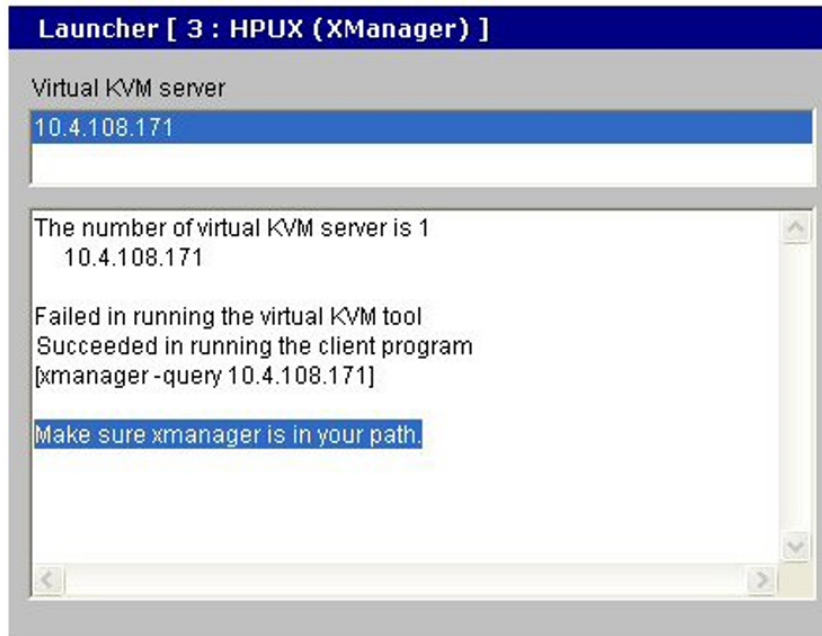
4. The Virtual KVM VNC Connection comes up:

5. Enter your user name and password, and click **OK**.

6. If the application does not start, check to make sure that the application is in the search path on your server. See Install programs for Virtual KVM.

Virtual KVM Assistant

Digi provides an optional tool, Virtual KVM Assistant, that can be loaded on a Windows or Linux system.

When the Virtual KVM Assistant is loaded, it registers itself with the browser so it can manage requested connections. It creates a drop-down list of the available Virtual KVM sessions and provides a floating dashboard, shown here:

The floating dashboard allows fast access, without going through the Web UI, to the:

- Serial Console
- Serial Console Log
- Power Controller, if it is configured

How the Virtual KVM Assistant works

Users access the remote desktop of Windows Servers using the Passport web page.

Virtual KVM Assistant appears on the screen:

Serial Console
Console Log
Power Control
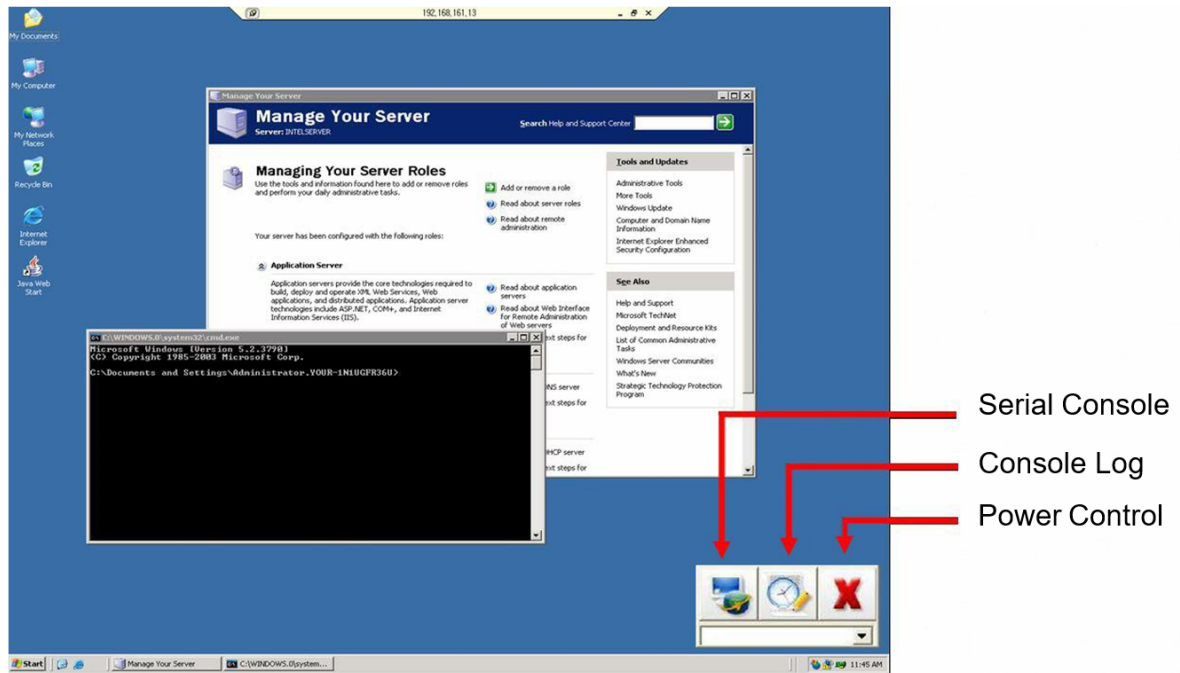
To switch between multiple connections, choose the item from the drop-down list.

To view the console logs, connect to the serial console, or cycle the power, use the buttons on the dashboard.

User client PC platforms supported

- Windows XP/2000/NT
- Linux

Users need to download the program to use it. The Digi Passport java applet automatically detects the program if it is present and in your path.

Install programs for Virtual KVM

Virtual KVM relies on software installed on the client system to provide access to the target system. This section is for troubleshooting common issues that may come up as you use Virtual KVM.

- Because the Virtual KVM is launched by a Java applet, you must have Java installed on your Workstation and in your browser.

- Regardless of the software package you use, make sure that the server has support for that package enabled.

Remote desktop protocol

Software needed

Remote Desktop Client software is provided as part of the standard installation of Windows for Windows 2000, 2003, and XP systems. Generally, there are no issues, because it is installed in the windows\system32\ directory. A Remote Desktop Client program is standard in major Linux distributions and is available as an open source package that can be installed if it's not already present. Make sure the Remote Desktop Client is in your user path on your Linux/Unix server.

Usage notes

You can perform applications management and most diagnostics from the standard Remote Desktop connection. On Windows Server 2003, however, note that there are actually two different types of connection – one for general access and one to take over the primary VGA data stream.

Some applications may require access to the VGA data. Windows systems prior to Server 2003 provide the VGA facility on the standard data stream.

To get to the VGA video stream, do either of these steps:

Install additional software (tsmmc.msc) on your XP system

At the command line, change the command in Virtual KVM from:

`$RDC$`

to:

`tsmmc.msc`

The VGA video stream is available for WinXP in the Win 2K3 administrative service pack for Win2K3, on the Windows Server 2003 CD, or online from:

microsoft.com/en-us/download/details.aspx?id=6315

Standard remote desktop connection

Make a standard remote desktop connection to the W2k3 server and then run the tsmmc command remotely on the target W2k3 server. The advantage of this method is that it doesn't require any additional software to be loaded onto Windows systems, and it works equally well with Remote Desktop Client from Linux and Unix workstations.

To reach the VGA data stream from within an existing RDP connection:

1. Log in with RDP.
2. Choose Start ☺ Programs ☺ Administrative Tools ☺ Remote Desktops.
3. Under Console Root, right-click on Remote Desktops ☺ Add New Connection ☺ Use IP Address 127.0.0.1.
4. Right-click on 127.0.0.1 ☺ New Window From Here ☺ Log In.

To enable Remote Desktop on your Windows Server 2003 System, choose

My Computer > Right Click > Properties > Remote > Enable Remote Desktop on this Computer.

VNC Viewer

Client software needed

Windows:

- TightVNC from tightvnc.com
- RealVNC software from realvnc.com
- UltraVNC from uvnc.com

Linux:

- vncviewer from the VNC client software package for your distribution.

Make sure that vncviewer is installed into a folder in your standard Windows or Linux/Unix path. On Windows systems, as a secondary option, you can copy the vncviewer.exe file to your c:\windows directory.

Usage notes

Follow the distribution-specific instructions for enabling VNC support on your Unix or Linux Server.

Xmanager

Client software needed

The Xmanager software is available for free 30 day evaluation download from netsarang.com/download/main.html

Usage notes

Install the client software in a directory in the PATH of the Windows system; otherwise, you must update path to include the base directory for the Xmanager software.

Make sure that X Window System is configured to allow for remote connections from your Client workstation's IP address.

Full documentation of Xmanager capabilities is included with the evaluation download.

Rackable Systems management card

Rackable Systems manufactures a management card that is built into some of their servers. It interfaces between the Digi CM unit and the server's serial port. In normal mode, it allows transparent communication between the Digi CM unit and the server. After detecting an escape sequence, it allows you to control functions from the server independently of the main processor. The controllable functions are listed below:

- Switching power on or off
- Rebooting
- Turning the status LED on or off
- Programming the LCD panel
- Reading the temperature from inside the server
- Setting the power on delay

The Digi CM unit offers a graphical web based user interface to manage the Rackable Systems Management Card.

Follow all of these steps to configure this feature.

Set up the Digi CM unit to support the Rackable Systems management card

To set up the serial port to provide access to the Rackable Systems Management console, do the following:

1. Access the Digi CM unit's web interface.
2. Under the **Serial Port** heading choose **Configuration**.
3. Choose a port.
4. Choose **Host mode configuration**. The Host mode configuration page appears.
5. Set the **Host mode** to Console server.
6. Set the **Rackable Systems Mgmt Card support** to **Enable**.
7. Click **Save & apply**.

Configure Serial Port Communication settings

1. Choose **Serial port parameters** from the menu.
2. Adjust the settings as required. The defaults for the Rackable Systems Management Card are identical to these of the Digi CM unit:
   - **Baud rate**: 9600
   - **Data bits**: 8
   - **Parity**: None
   - **Stop bits**: 1
   - **Flow control**: None
   - **DTR behavior**: High when open
3. Click **Save & apply**.

Assign a port name

1. Choose port title from the menu.
2. Enter a port title.
3. Click **Save & apply**.

Access the Rackable Systems Management Card from the Digi CM Unit's User Interface

1. Access the Digi CM unit's web interface.
2. Under the **Serial Port** heading choose **Connection**. A screen similar to the following appears.

3. Click on the icon in the M (Manage) column or on the title of the port to which the Rackable Server is connected. A screen similar to the following appears.

4. Use the Digi CM unit's user interface to perform Rackable Systems Management Card functions. The following describes attributes of the user interface controls.

Field	Description
Control	
Power status	The first column shows the current state. Three buttons are available to initiate an action to either, power on, power off or restart the server. Dependant on the current status Power on or Power off is disabled.
Reboot	Reboot the Rackable Server by sending a 500ms reset signal to the server.
Connect	Spawn the Java Telnet applet or the local Telnet/SSH application to connect directly to the port.
LED Mgmt	
LED Management	To control the LED in the front of the Rackable Server. The first columns shows the current status of the LED. Three buttons are available to select the activity of the status LED: turn on, turn off and blinking. Either of these buttons is disabled.
LCD Mgmt	
Currently displayed message	Shows the message that is currently displayed on the LCD display.

Field	Description
Erase	This function clears the LCD display. The saved message stays saved to flash.
Save	Save currently displayed message to flash memory.
Show saved LCD message upon startup	The first columns shows the current status: Yes or No. This parameter defines which message is displayed upon startup of the server, either the saved message or the standard: "Rackable Systems Phantom Vx.xx".
Contrast	Set a contrast for the LCD panel. The default is 50, the range is 0 – 100.
Phantom Properties	
Temperature	Indicates current temperature inside the Rackable Systems Server.
Power delay	Time in seconds before the server starts up after applying power (0-98 seconds, 99 means no power on delay).
Power sense	The power sense option toggles between sensing server power on the reset header or on the J7 connector. Most applications will use the "Reset" option. This option should be set before shipping from Rackable Systems, but may need to be reset if somehow changed after shipping.
Communication settings Baud Rate	Configure the baud rate used to communicate with the Rackable Systems Management Card. For this change to become effective reset or power-cycle the Management card, and be sure to switch the port settings in the Digi CM unit's port settings.

Dial-in modem access

The Digi CM unit supports dial-in connections from remote sites for out-of-band access. In this configuration, the Digi CM unit has serial ports configured for external modems and waits for dial-in connections from remote sites. If you dial-in using a terminal application, the Digi CM unit accepts the connection and displays a menu of available serials ports. In a dial-in terminal server mode, the Digi CM unit makes a TCP connection with either a Telnet or SSH client to a pre-defined server.

RawTCP is also an option for dial-in users.

For more information on the different types of Host mode configuration, see Host mode configuration.
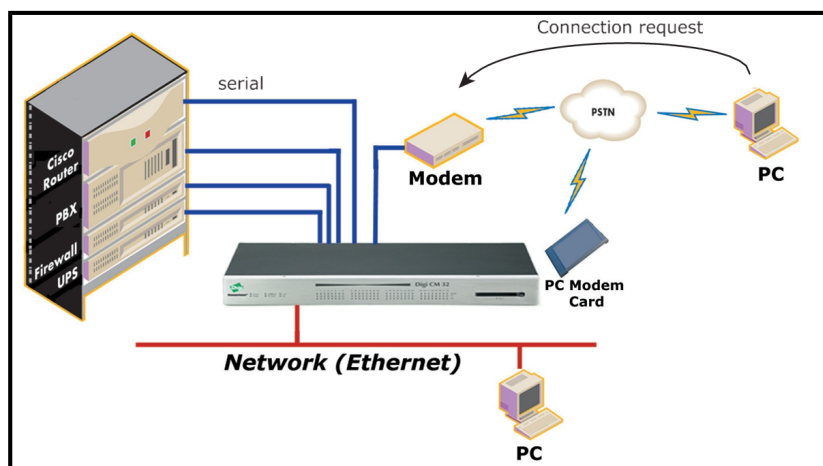
Configure for dial-in modem access

To configure a serial port for a dial-in modem, enter the values for these fields: Host mode, Modem init string, and Inactivity timeout. To access the Host mode configuration screen, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial port** heading, choose **Configuration**.
3. Choose a specific port under Individual port configuration and then choose **Host mode configuration**.
4. Select Dial-in modem for the Host mode in the drop down menu.

5. Fill in the appropriate fields as they apply to your configuration.
6. Click **Save & apply**.

Field	Description
Modem init string	The default modem init string is q1e0s0=2. The init string sets the modem to quiet mode, echo off, and Auto Answer on two rings. The modem init string is used for initializing an external modem attached to the Digi CM unit's serial port. See your modem user manual for more information.
Callback	For security reasons, the callback feature can be activated. If callback is enabled, the Digi CM unit does not accept any incoming calls. After the incoming call is rejected, a callback is initiated to the phone number configured in the "Dial-in modem callback phone number".

Field	Description

Modem test	To ensure the proper functionality of the modem, the Digi CM unit has the ability to test the modem connection in a configurable interval.
	
	Enable/Disable dial-in modem test : `Enable`
	Dial-in modem test phone number : `1234444567`
	Dial-in modem test interval : every `24` hour(s)
	
	The modem test allows you to specify a phone number and an interval.
	After the system has booted, the interval has elapsed, and the modem is not in use, the specified dial number is called. The modem trains and receives a login prompt from the other side (normally another Digi CM unit)
	If the login-in prompt (login:) is detected the line is disconnected again and the modem test is considered successful.
	Two ports can call each other using this modem test procedure. Please be aware that the tests will fail if the other modem is in use.
	There are multiple ways to review the information about the mode test:
	• syslog in the Digi CM unit
	In this example a modem connected to port 16 is calling another modem connected to port 15. Any errors occurring are captured in the syslog file as well.
	`07-16-2004 12:45:01 > Port #16 - Modem Test started. Calling to 1234444567.`
	`07-16-2004 12:45:22 > Modem connected through Port #15`
	`07-16-2004 12:45:22 > Port #16 - Modem Test succeeded`
	
	• Email-based notification
	The **Alert configuration** dialog of the port configuration, contains multiple settings.
	Email alert configuration
	The title of the e-mail and the address can be configured.
	To be able to configure e-mail notifications, a primary SMTP server has to be configured under **Network > SMTP** configuration.
	SNMP configuration
	It is also possible to receive notifications using SNMP traps.
	When using SNMP traps the global settings for IP address, Community and Version can be used, or specified separately.
	The Trap MIB can be downloaded from support.digi.com (select your product and go to Diagnostics, Utilities and MIBs).

Add a PC modem

A PC card slot is provided on the front panel of the Digi CM unit. The following graphic has an arrow that indicates the PC card slot.

PC card slot

Digi CM 32 shown
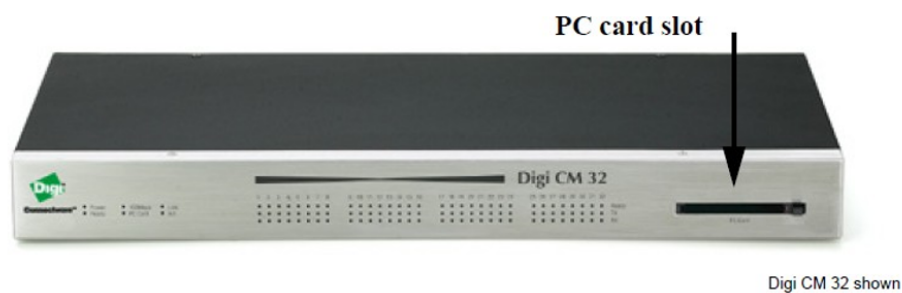
To install and configure the PC modem on the Digi CM unit, do the following.

1. Insert the card into the PC slot located on the front of the device.

2. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

3. From the menu, choose **Configuration** under the **PC card** heading.

4. Choose **Discover a new card**. The Digi CM unit searches for a PC card and displays a configuration menu.

5. Enter the appropriate parameters in the configuration menu.

6. Click **Save & apply**.

Configure for Dial-In Terminal Server access
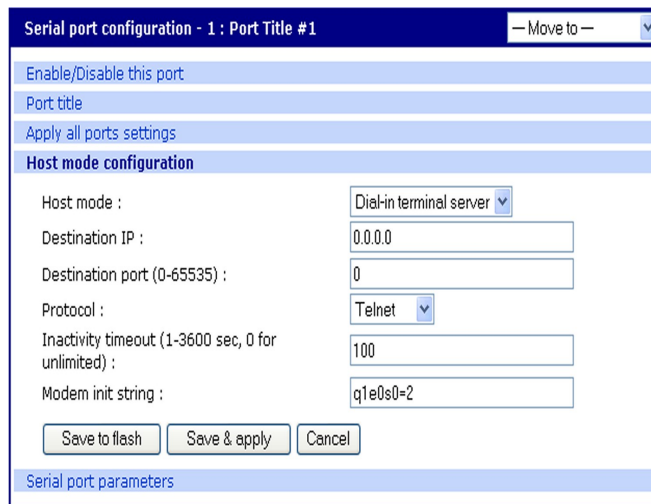
The host mode Dial-In Terminal Server is identical to the host mode Terminal Server but allows you to configure a modem init string. In this mode an incoming modem connection is automatically connected to an IP address.

To configure a serial port for a dial-in terminal server access, enter the values for these fields: Host mode, Destination IP, Base Port, Protocol, Inactivity timeout, and Modem init string. To access the Host mode configuration screen, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **Serial port** heading, choose **Configuration**.

3. Choose a specific port under Individual port configuration and then choose **Host mode configuration**.

4. Select **Dial-in terminal server** for the **Host mode** from the drop down menu.

5. Fill in the appropriate fields as they apply to your configuration.

6. Click **Save & apply**.

- **Destination IP**: The IP address of the system that you will be automatically connected to when you access the port.

- **Destination port**: The TCP port that will be used when the port you accessed is automatically connected to a system on the network.

- **Protocol**: The protocol that will be used to establish the connection to Destination IP: port. The options are SSH, RawTCP, and Telnet.

- **Inactivity timeout**: The timeout length ranges from 1 to 3600 seconds; 0 is unlimited timeout.

- **Modem init string**: Use the default string or enter your own string.

Power Controller

The Power Controller feature allows the administrators of the Digi CM unit to use console management to control power functions. Power control consists of three basic functions: on, off, and reboot (power cycle). There are two typical scenarios when using a power controller. The simplest scenario is a non-serial device connected to a power controller (for example, an environmental sensor controller or a tape backup device). The power controller is configured and accessed through the Digi CM unit.

This illustration shows the power controller configured through the Digi CM unit for non-serial devices.
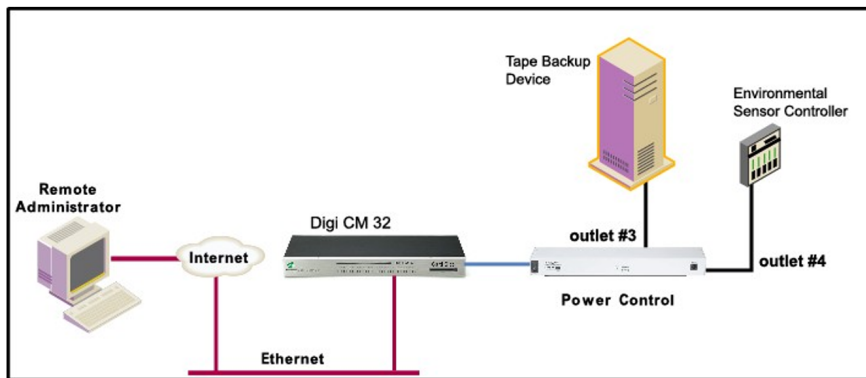
The second scenario is a serial device (such as a router or server) managed through a port on the Digi CM unit with its power supply mapped through the power control feature. After configuration is complete, you need only reference the console management port on the Digi CM unit to also manage power. The Power Controller feature handles the relationship of a specific outlet to a serial device as if the power supply was also connected to the same port as the serial device. In other words, you don't need to see the physical connection or remember which outlet controls a specific serial device after configuration - the Digi CM unit does that for you.

The following illustration shows a Sun server configured through a serial port connection on the Digi CM 32.
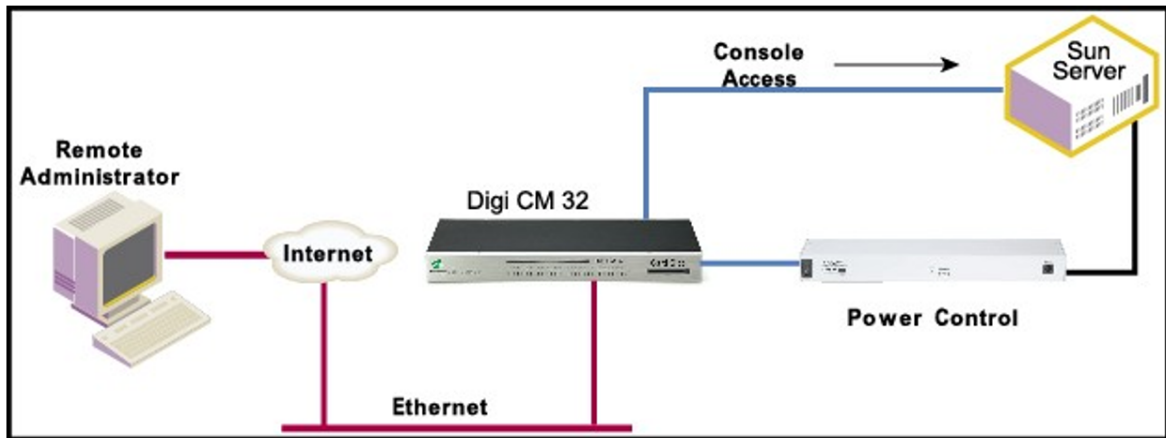
Install Power Controller

To connect the Digi RPM power controller to the Digi CM unit use the straight-thru cable provided with the Digi RPM unit. Plug one side into the "Console" port of the Digi RPM unit and the other into any port of the Digi CM unit. If you plan to connect multiple power controllers, set up all of them as described before proceeding. For details on how to configure the Digi RPM unit for cascading refer to Cascade multiple Digi RPM units.

If you are using any other manufacturer of power controllers, please refer to About serial port cabling for more information.

Before proceeding, plug the power controller into an appropriate power source and turn it on.

Note The DIP switches on the Digi RPM unit are used for cascading. Make sure that the dip switches of the first unit are set to off. For more information about cascading refer to Cascade multiple Digi RPM units.

Configure Power Controller

Only system administrators can add a power controller although authorized users may reconfigure outlets or serial ports.

Configure the serial port parameters to match the Power Controller

1. Log in to the Digi CM unit.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Click **Serial port > Configuration**.
3. Select the port number of the serial port you want to connect to the power controller.
4. Select the **Serial port parameters**:
   - **Baud rate**: 9600
   - **Data bits**: 8
   - **Parity**: None

- **Stop bits**: 1
- **Flow control**: None
- **DTR behavior**: High when open

5. Click **Save & apply**.
6. Continue by adding the power controller. See Add the Power Controller.

Add the Power Controller

1. Login to the Digi CM unit.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Click **Power Controller > Configuration**.

3. Select the port number of the serial port you want have connected to the power controller(s), the manufacturer of the power controller, and the number of units to be cascaded (1 means that one unit will be connected (no cascading)).

   Note The number of cascaded units cannot be changed later, so make sure you have all power controllers connected before proceeding.

   The default title is the manufacturer brand and the port number it is connected to. You have the ability to change this title in step 5 if needed.

4. Click **Add controller**.
5. After the controller is detected automatically, you can correct the number of ports if necessary or edit the port title.
6. Click **Save & apply**.
7. Continue by setting the alarms and thresholds.

Set alarms and thresholds

Power Controller allows administrators to set an alert via email notification or an SNMP trap when environmental conditions exceed specifications.

1. Under **Power Controller** click **Alarms & thresholds**.

2. Enter the appropriate parameters. Select the condition(s) for an alert and enter the information for the alert (email, SNMP trap, or select both).

   Note If multiple power management units are cascaded, the alarm threshold is set for the sum of all outlets.

   Note To set up an email alert it is assumed that the mail server has already been set up. If not, go to Configuring SMTP alerts. If the SMTP server is not set up, the E-mail option will not be available.

3. Click **Save & apply**.

4. Continue by configuring the outlets

Outlet configuration

The following procedure allows you to setup the power supplied to your device from the power controller.

1. From **Power controller**, click **Outlets**.

2. Click the outlet number to configure.

3. Select the serial port number that controls the device connected to the Digi CM unit (if any). If
    the port number has a title, it will appear.

    > **Note** If you want to add a title or change the existing title, go to **Serial port > Configuration**
    > and select the port number that you want to add or change the title. Enter the title and click
    > **Save & apply**. Go back to **Power Controller > Configuration > Title > Outlets** and select the
    > outlet you are configuring to continue.

4. If you are not selecting a serial port number, you can modify a user's access on this screen.
    Enter the User Access Control parameters. See User access for Power Controller.

5. Click Save to flash and repeat steps 2- 4 for each outlet you want to configure.

6. Click **Save & apply**.

Power controller configuration - DIGI RPM on Port 8

Power controller
Alarms & thresholds
Outlets

Outlet	Port	Title	Unit#	Outlet#
1	1	Sun Server	0	1
2	2	Sun Server	0	2

Serial port :   1

Move to serial port configuration to change [title] or [power access]

Outlet title :   Sun Server

User access control :

User	Power access	Action
<<Everyone>>	☑	
Gilligan	☑	Remove
	☑	Add

Save to flash   Save & apply   Cancel

3	None	None	0	3
4	None	None	0	4
5	None	None	0	5
6	None	None	0	6
7	None	None	0	7
8	None	None	0	8

> **Note** The screen above shows that serial port one on the Digi CM unit is connected to a Sun Server that is supplied power from outlets 1 and 2 on the power controller. In the example above, Gilligan has access to the power outlets.

7. To select the parameters for the User Access Control, click the User Access link. You may grant specific users permission to access an outlet or restrict access for specific users from an outlet. For more information see User access for Power Controller.

User access for Power Controller

The Digi CM unit can be configured to allow all users or specific users access to the power controller feature as well as restricting specific users to the power controller feature. User Access is configured on an outlet by outlet basis.

> **Note** User Access to a serial device that is connected to the power controller in configured under **Serial Port > Configuration > Port # > User Access**.

Configure to allow specific users access

To configure the Digi CM unit for specific users, you must deselect <<Everyone's>> access and add the specific user and access as in the following steps.

1. Log in to the Digi CM unit.

> **Note** Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Click **Power Controller > Configuration > Outlets > Select** the outlet # to configure.
3. Select the port to configure to the outlet. If it is a non-serial device select None.

4. Edit the outlet title. If there is a serial port, the port title will appear and cannot be edited from this screen.

5. Click **Save & apply**.

6. Under **Everyone** uncheck the **Access** type and click **Save to flash**.

7. Enter the user that will have access and check the Access type.

Note Port is access to the port. Monitor is access to sniff. Power is access to the power management.

---

8. Click **Save to flash**. Repeat steps 7 and 8 for additional users.

9. Click **Save & apply** after all users have been entered.

Note The screen above shows outlets 1 & 2 control power to the Sun Server configured on port 1 of the Digi CM unit. Outlets 3 and 4 are not serial devices. Gilligan has been designated the specific user to control outlet # 3.

Configure to restrict specific users

To restrict specific users, you must select access for << Everyone>> and add the restricted user by deselecting his or her access.

1. Log in to the Digi CM unit.

Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

---

2. Click **Power Controller > Configuration > Outlets > Select** the outlet # to configure.

3. Select the port to configure to the outlet. If it is a non-serial device select None.

4. Edit the outlet title. If there is a serial port, the port title will appear and cannot be edited from this screen.

5. Click **Save & apply**.

6. Check **Everyone** and click **Save to flash**.

7. Enter the username that will NOT have access, uncheck the Access types that are restricted, and click Add.

   Note Port is access to the port. Monitor is access to sniff. Power is access to the power management.

8. Click **Save to flash** and repeat steps 7 and 8 for additional users.

9. When all users have been added, click **Save & apply**.

Note Gilligan does not have access to Outlet # 4.

Power Controller management

The Power Controller Management option allows you to change outlet settings or get a quick update of the power controller status.

1. Under **Power Control** click **Management**.

Power controller management

Power controller

Port#	Manufacturer	Title	Outlets	Status
8	DIGI RPM	DIGI RPM on Port 8	8	Connected

The Power controller management screen gives a quick view of all the power controllers and the current status of the connection. The Port # and Manufacturer fields are a link to the specific power controller statistic page, which displays information for the power controller. If the status is 'Disconnected' the links are inactive.

2. Click either the Port # or the power controller title.

Power controller management - DIGI RPM on Port 8

Power controller

Model :	RPM8
Alarm threshold :	30.0 amps
Temperature :	86.0 °F (30.0 °C)
Circuit breaker :	Good
RMS voltage :	120.0 volts
RMS current :	0.0 amps
Max current detected :	0.0 amps [Clear]

Outlets

The Power controller statistics screen appears to show the **Alarm threshold**, **Current temp**, **Circuit breaker condition**, **RMS voltage**, **RMS current**, and **Max current detected**.

The **Clear** button will reset the Max current detected to 0.0 amps. From this screen click Outlets.

3. Select the outlet number that you would like to manage.

Note The screen below shows that all the outlets are powered On and outlet 3 is Rebooting, therefore the Backup Tape Device is power cycling.

Power controller management - DIGI RPM on Port 8

Power controller

Outlets

	Outlet	Port	Title	Unit#	Outlet#
ON	1	1	Sun Server	0	1
ON	2	2	Sun Server Backup	0	2
Rebooting	3	None	Backup Tape Device	0	3
			[Power on] [Power off] [Reboot]		
ON	4	None	Environmental Sensor	0	4
ON	5	None	None	0	5
ON	6	None	None	0	6
ON	7	None	None	0	7
ON	8	None	None	0	8

4. Click **Power on**, **Power off**, or **Reboot** depending on what you want the outlet to do.

Cascade multiple Digi RPM units

The Digi RPM power controllers can be cascaded when used with the Digi CM unit.

The DIP switches on the front panel of the Digi RPM allow configuring unique identities (ID) to the Digi RPMs so they can be identified. In a cascaded environment each unit has to be configured to a unique ID.

To cascade the Digi RPM units, connect a serial port of the Digi CM unit to the Console Port of the first Digi RPM unit using a straight-thru cable. Connect the "Cascade" Port of the first Digi RPM unit to the "Console" Port of the second.

Following an example of two cascaded Digi RPM units connected to a Digi CM unit.S Please note that the ID for the first unit is set to 0 and for the second unit it is set to 1.
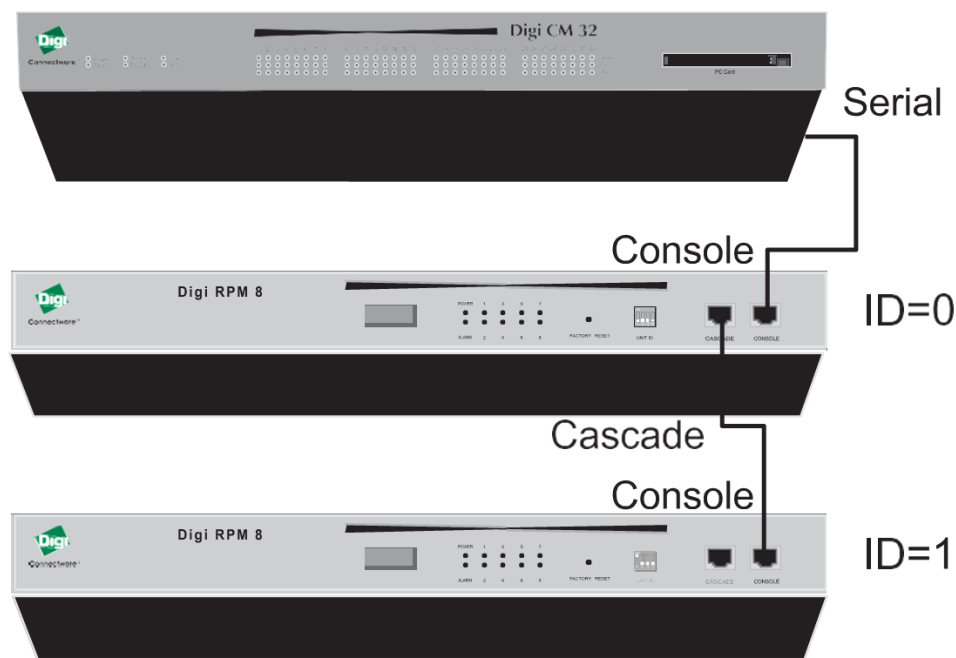
The following table shows all possible IDs that can be configured on the Digi RPM. unit.

Unit ID Switch Configuration

ON 1 2 3 4 — Unit ID 0
ON 1 2 3 4 — Unit ID 1
ON 1 2 3 4 — Unit ID 2
ON 1 2 3 4 — Unit ID 3

ON 1 2 3 4 — Unit ID 4
ON 1 2 3 4 — Unit ID 5
ON 1 2 3 4 — Unit ID 6
ON 1 2 3 4 — Unit ID 7

ON 1 2 3 4 — Unit ID 8
ON 1 2 3 4 — Unit ID 9
ON 1 2 3 4 — Unit ID 10
ON 1 2 3 4 — Unit ID 11

ON 1 2 3 4 — Unit ID 12
ON 1 2 3 4 — Unit ID 13
ON 1 2 3 4 — Unit ID 14
ON 1 2 3 4 — Unit ID 15
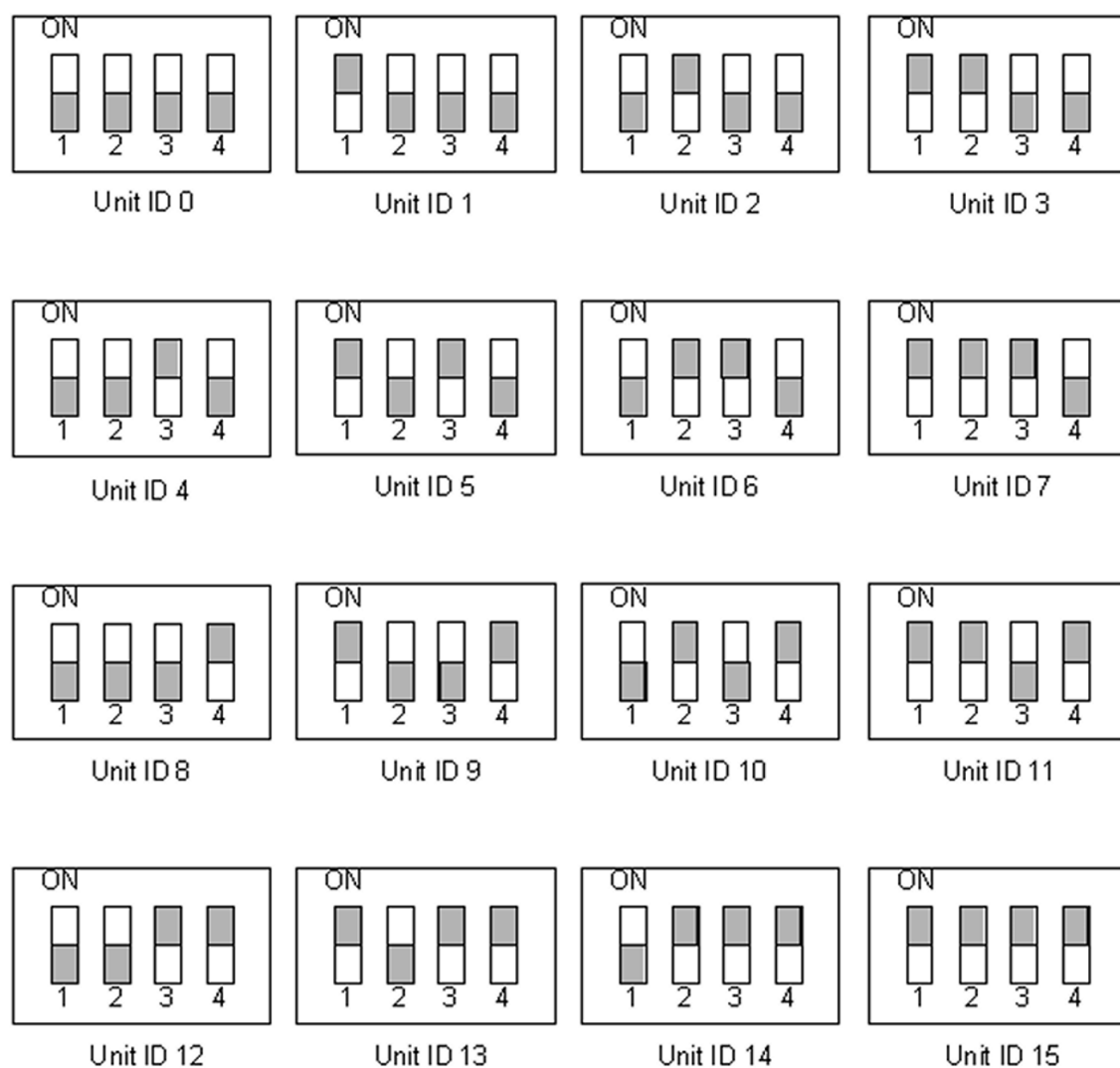
Post clustering

Port clustering is the ability to manage many serial ports on one or multiple slave devices from one master device using a single IP address. For instance, the Digi CM unit can manage up to 16 slave devices or a maximum 816 serial ports with one Master device. Ports can be configured either collectively or individually depending on user preference. Each master and slave device is configured separately; they cannot be configured from one master console.

A secondary IP address can be specified to put all slaves on a private network. The secondary IP option can be found under **Network > IP configuration**.

To set up the Digi CM unit for port clustering you will need to:

- Configure all the Digi CM serial ports.
- Assign one Digi CM unit as the master clustering device; all other Digi CM units default to slave devices.
- Import slave configuration to the Digi CM unit's master device.
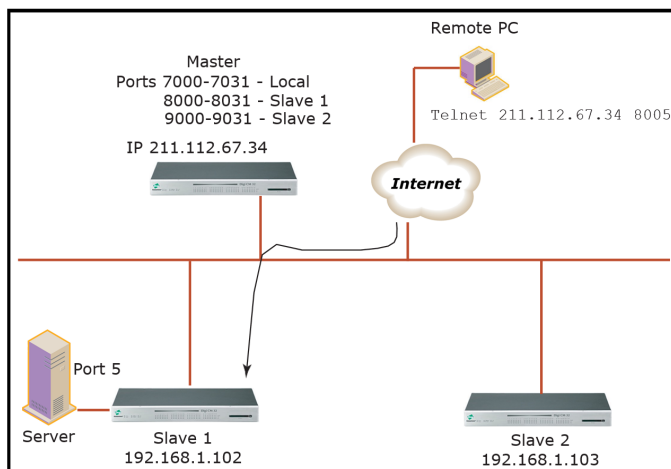
Assign master clustering mode

To assign a Digi CM unit as the master cluster device, do the following:

1. Access the Digi CM unit through the web interface. This Digi CM unit needs to be the unit you want as the Master.
2. Under the **Clustering** heading, choose **Configuration**.

3. Choose **Master** from the drop down menu. Subsequent units will be configured in Slave mode by default.

4. Choose **Save & apply**.

Configure clients to join a cluster

Digi CM units can be configured as basic slaves without any additional configuration. Two additional settings, however, enhance the clustering capability.

- **Authentication mode**: Local authentication is the slave independently authenticating all port access. Master authentication is the master performs port authentication. Users do NOT need to be defined on the slave unit. Password verification will be done by the master unit.

- **Update Master on Changes:** Automatically updates port name changes, port settings, and user permission settings to the master unit. Generally, Update Master on changes should be yes.

Select the appropriate settings then click **Save & apply**.

Advanced clustering configuration

To refine a cluster environment, use the following parameters for advanced configuration of a cluster. To access the Advanced menu follow the proceedure listed below.

1. Select **Clustering > Configuration > Master > Save & apply**.
2. Select the port number > **Enable > Save & apply**.

3. Select **Advanced** from the **Clustering >Master** mode.

- **Enable**: This shows whether the port is enabled or disabled. All ports are enabled by default.

- **Slave unit address**: IP address of slave.

- **No. of ports**: Number of ports on slave.

- **Slave authentication mode**: To specify if your database is controlled by the master unit, or locally by the slaves themselves.

- **Update Master on Changes**: Automatically updates port name changes, port settings, and user permission settings to the master unit. Generally, Update Master on changes should be yes.

- **Connect to slave unit to change configuration**: A quick access method to connect to the slave.

- **Source port**: This is the port number that you would access to get to the slave on the master unit. The first slave port defaults to 7100 for the port access menu and the port numbers increase according to the number of ports on the Digi CM unit.

- **Destination port**: The destination port is the corresponding port number on the slave unit. On a 32-port slave unit, the destination port numbers range from 7001 to 7032.

- **Protocol**: The four options are N/A (not available), SSH, Telnet, and RawTCP.

- **Base source port**: If you choose not to use AutoConfig, you can set these ports manually. Base source port is the first port number on a master unit. By default the base source port on the master unit is 7001. The base source ports extend the master's ports via the slave ports. For example, starting the base source port number with 7101 results in a 32-port unit being numbered from 7101 to 7082. Port number 7100 is the port access menu of the slave. If you configure the device manually, the port access menu must also be configured separately.

- **Base destination port**: The physical port numbers of the slave device.

Note However, you can change the base source port number to another number and the rest of the ports on the unit will be sequentially numbered from the base source port.

Access the cluster ports

You can connect to the slave port using the web, Telnet or SSH client. You can access the port access menu or custom menu of each slave device or connect directly to each slave port.

Web Access

1. Click **Clustering > Connection** > Port number.
2. Log in to the port.
3. Enter the port escape sequence (listed on page).

Telnet

1. Telnet to the IP and the port number of the device.

   ```
   telnet 143.191.3.9 7101
   ```

2. Login.
3. Enter the port escape sequence (listed on page).

SSH

1. Click on the port with SSH protocol
2. Login.

3. Enter the port escape sequence (listed on the page). Depending on your access rights you can sniff (read only) or monitor (read/write), or manage power of the ports.

System administration

This section describes how to perform tasks performed either by root or the system administrator. These tasks fall under the general heading of system administration and include firmware upgrades, saving configurations, resetting the unit to defaults, and disaster recovery procedures.

Upgrade the firmware

The web interface allows you to download the latest firmware version to the Digi CM unit. The latest firmware can be found at:

https://www.digi.com/products/consoleservers/digicm#productsupport

To upgrade the firmware:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. Under the **System administration** heading, choose **Firmware upgrade**.
3. Select Local machine or CF card (if configured).
4. Choose the **Browse** button and locate the firmware download.
5. Choose **Upgrade**. The Digi CM unit will automatically reboot when the upgrade is complete.

Note Do not power cycle the unit for five minutes after the firmware upgrade is completed, as the unit is writing the firmware to flash!

Configure management

Configuration management allows you to save all or parts of your configuration. You can also establish the time frame to save the configuration either periodically or 10 minutes after the latest changes. The Digi CM unit saves all configurations when the **Save & apply** button is used or the **Apply changes** link is used. These configurations are saved to the local Digi CM unit in /tmp/cnf directory by default. Manage these configurations by exporting the files to your location of choice.

1. Click S**ystem administration > Configuration management**. The **Configuration management** screen appears.

2. Under **Configuration Export**, select the file locations that you wish to save enter a name and click **Export**.

Save the configuration automatically

Further down the screen are the options for automatically saving the configuration either periodically or 10 minutes after the latest changes. The following list contains the parameter descriptions.

- **Automatic backup option**
  - **Disable**: If you do not want to use an automatic save option.
  - **Periodic**: Used to set the save option per your time frame 10 minutes after last change - as described.

- **Location**
  - CF card, Primary NFS server, User space, Send via email: Options for where to save the configuration.

- **Encrypt**
  - **Yes**: File will be encrypted (.syscm).
  - **No**: File will not be encrypted (.tar.gz) in a tar and a gzip'd format.

- **File Name**: The name of the configuration file.

- **Backup interval**: The periodic hourly interval to back up the configuration files.

- **Recipient's email address**: The email address to send the configuration file.

To setup the automatic backup option follow the procedure.

1. Select **Periodic or 10 minutes after latest change** from the drop down menu.
2. Select the location to save the file.
3. Select **Yes** or **No** to encrypt and enter the file name.
4. Enter the number of hours for the backup interval (if periodic)
5. Enter the recipient's email address to send the configuration file (if the location is sent via email).
6. Click **Save & apply**.

Automatically upgrade the Digi CM Unit's firmware or configuration using TFTP

The Digi CM unit supports upgrading the firmware, configuration, or any other files in the file system using a TFTP-based mechanism.

During boot, the Digi CM unit can verify a "hash" file and determine if it needs to download upgrades from the TFTP server.

There are multiple ways to configure the TFTP upgrade function.

DHCP

The DHCP server can automatically assign a TFTP upgrade server and file to the Digi CM unit during boot. The options implemented are:

- (66) TFTP server address
- (67) TFTP filename (this is the filename of the hash file)

To enable DHCP firmware upgrade:

1. Click **System administration > Firmware upgrade**.
2. Set **Automatic firmware and configuration upgrade at boot time** to **Enable**.
3. Set **Use DHCP option for remote server and hash file** to **Yes**.
4. Click **Save & apply**.

The next time the Digi CM unit reboots, it will analyze the hash file and upgrade the firmware, configuration, or other files if required.

Directly configure the TFTP Server and the name of the hash file

To configure the IP address of the TFTP server and the filename of the hash file on the Digi CM unit, follow the steps below:

1. Click **System administration > Firmware upgrade**.
2. Set **Automatic firmware and configuration upgrade at boot time** to **Enable**.
3. Set **Use DHCP option for remote server and hash file** to **No**.
4. Configure the **IP address of remote server**.
5. Configure the **Hash file name**.
6. Click **Save & apply**.

The next time the Digi CM unit reboots, it will analyze the hash file and upgrade the firmware, configuration, or other files if required.

If you have trouble with the TFTP upgrade process, please verify that the hash file and the other files are accessible using TFTP.

Hash file structure

The hash file is an ASCII configuration file with one line per entry. Each entry defines one upgrade action.

There are three actions defined:

- Upgrade firmware
- Upgrade configuration
- Upgrade any file
- Execute an application.

The action is the first entry in the line and it also defines the syntax of the line. Syntax for action 1: firmware upgrade

```
<image name>,<model name>,<version>
```

```
<image name> specifying the path and the filename of the firmware on the
TFTP server
```

```
<model name> specifying the product name especially the port count e.g.
DigiCM48, DigiCM32, DigiCM16 or DigiCM8
```

This allows you to have one hash file for different models.

```
<version> the version number of the firmware
```

The Digi CM unit will download the firmware if the version number of the running firmware is different than the firmware version in the hash file (the current firmware version is saved in file / tmp/cnf/version).

Note Make sure the firmware version in the hash file matches the firmware version on the FTP directory, otherwise you will start a continuous upgrade process.

Example

```
Passport48.img,DigiPassport48,v1.6.0
```

After the firmware was upgraded the Digi CM unit boots again.

Syntax for action 2: configuration upgrade

```
<image name>,<model name>,<version>
```

```
<image name> specifying the path and the filename of the configuration
file on the TFTP server
```

```
<model name> specifying the product name especially the port count e.g.
DigiCM48, DigiCM32, DigiCM16 or DigiCM8
```

This allows you to have one hash file for different models.

```
<version> the version number of the firmware
```

The Digi CM unit will download the configuration if the version in the hash file is different from the version saved in the file /tmp/cnf/.cnfversion. This file does not exist until you do the first automatic configuration upgrade. It is also deleted if the unit is reset to factory defaults.

If the /tmp/cnf/.cnfversion file does not exist, no download will occur. The file /tmp/cnf/.cnfversion is a hidden file.

Example

```
config.tar.gz,DigiPassport48,v1.6.0
```

After the firmware configuration is upgraded the Digi CM unit boots again.

A sample hash file can be downloaded from: https://www.digi.com/products/consoleservers/ digicm#productsupport

Syntax for action 3: file upgrade

```
<file name>,<options>,<destination>
```

```
<file name> specifying the path and the filename of the file on the TFTP
server
```

```
<options>
```

```
    - F: forced copy (override existing file)
```

```
    - X: decompress
```

```
    - Z: unzip
```

```
    - U: default option for file uploading
```

```
<destination> directory on the Digi CM unit to place the file
```

These files are downloaded every time the Digi CM unit boots and there is no reboot after downloading.

Example

```
snmpd.conf,FU,/tmp/cnf
```

The file snmpd.conf is copied from the TFTP server and placed into /tmp/cnf. The file is used as is and the previous version is overwritten.

Syntax for action 4: execute a command

```
<command> <parameters>
```

```
<command> any application residing on the Digi CM unit that is
executable by root
```

```
<parameter> all parameters this application requires
```

Example

```
touch /tmp/test
```

Reset factory defaults

There are two ways to reset the unit to the factory defaults. The quickest and simplest method is to push and hold the hardware factory default reset button until the Ready light on the front panel goes out. The reset button is located on the back panel of the unit next to the Ethernet port. The arrow points to the reset button's location.

Factory reset button
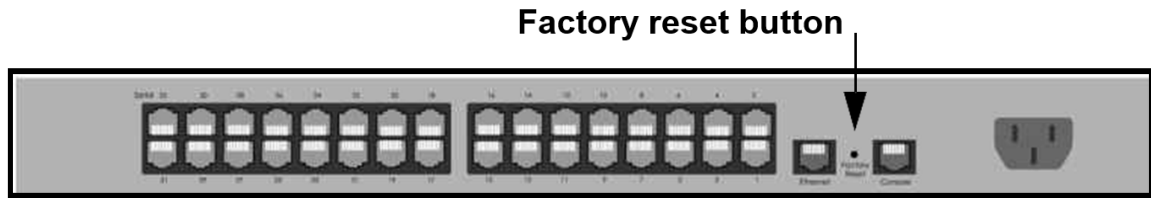
Digi CM 32 shown

The alternative method to reset the unit is through the web interface. The web interface provides the option of retaining the IP settings. To use the web interface to reset the Digi CM unit, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. **System administration > Configuration management**

3. Under **Configuration import** select **Factory default**.

4. Select the Configuration factory default options you want to restore from the checklist.

5. Click **Import**. The Digi CM unit will automatically reboot.

The following are the default values when the Digi CM unit is reset to the factory defaults.

- **Static IP Address**: 192.168.161.5
- **Port Access Menu IP Address**: 192.168.1.100
- **Port Access Menu TCP Port Number**: 7000
- **Serial Port IP Address:** 192.168.1.101-
- **Serial Port TCP Port Number**: 7001-

Set the date and time

The Digi CM unit provides two options for keeping system time. The first is by using an NTP server and the other is through an internal battery backup. To configure the Digi CM unit for date and time, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.
   ---

2. **System administration > Date and time**.

Date and time	
Use NTP :	Disable
NTP server (0.0.0.0 for Auto) :	192.168.200.100
Date [mm/dd/yyyy] :	04/28/2005
Time [hh:mm:ss] :	04:36:39
[Standard time]	
Timezone :	UTC
Time offset from UTC (UTC + [x.x]hours) :	0.0
[Daylight saving time]	
Enable/Disable daylight saving time :	Enable
Daylight saving timezone :	cms
Time offset from UTC (UTC + [x.x]hours) :	0.0
Start date [mm/dd] :	03/27
Start time [hh:mm:ss] :	02:00:00
End date [mm/dd] :	10/16
End time [hh:mm:ss] :	02:00:00

   Save to flash   Save & apply   Cancel

3. Set the time method using one of the following options.
   - **NTP server**: Choose **Enable**, and then enter the NTP server's IP address, the Time offset, and the Date and Time fields.
   - **Internal battery**: Enter the Date and Time fields only.

   Note If you change your time zone, you must go back and reconfigure your time for the time zone change to be effective.
   ---

4. Choose **Save & apply**.

Configure a host name

The system administrator can assign a Host name to the Digi CM unit. This is often helpful for administration purposes to locate a specific Digi CM unit on the network. To assign the Digi CM unit a device name, do the following:

1. Access the web interface.

   Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

2. **System administration > Device name**.
3. Enter the name you want to assign the Digi CM unit.
4. Choose **Save & apply**.

Command line interface

The Digi CM unit runs the embedded Hard Hat Linux operating system. The command line interface for configuration purposes is accessible only by the root user. The system administrator has read only privileges from the command line. By default the root user is connected to the CLI (command line interface) when accessing the Digi CM unit through Telnet or SSH. To gain access to the command prompt, the root user uses the username root and the root password. This chapter includes the Linux commands available on the embedded Linux operating system and the location of files useful to the root user for administrative purposes.

Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

Note The root user should be aware that deleting or corrupting files may prevent the Digi CM unit from booting properly. Before editing any files, be sure to back up your configuration files.

Linux commands

The purpose of this section is to list the various Linux commands available on the Digi CM unit. This is simply a listing of commands and does not detail what the commands do or give their particular parameters. If you need more information, see the man pages on a Linux system.

Two commands that are very important for saving and applying changes to the configuration files are:

- **saveconf**: The **saveconf** command saves the configuration files to flash memory.
- **applyconf**: The **applyconf** command immediately applies the configuration changes. The configuration files are located in /tmp/cnf directory.

Two system utility menus that are important for accessing and configuring the Digi CM unit and the serial ports are the portaccessmenu and configmenu.

- **portaccessmenu**: This menu allows the user to access the serial ports on the Digi CM unit.
- **configmenu**: This menu enables the system administrator to configure the Digi CM unit. It has essentially the same functionality as the web interface for configuring a unit with the exception of the ability to create custom menus.
- **portreset #**: This command allows the user to reset a specific port. It restarts all processes associated with the port.

Shell and shell utilities				
sh	ash	bash	echo	sed
env	false	grep	more	which
pwd				

File and disk utilities				
ls	cp	mv	rm	mkdir
rmdir	ln	mknod	chmod	touch
sync	gunzup	gzip	zcat	tar
dd	df	du	find	cat
vi	tail	mkdosfs	mke2fs	e2fsck
fsck	mount	unmount	scp	

System utilities				
date	free	hostname	sleep	stty
uname	reset	insmod	rmmod	lsmod
modprobe	kill	killall	ps	half
shutdown	poweroff	reboot	telnet	init
useradd	userdel	usermod	whoami	who
id	su			

Network utilities				
ifconfig	iptables	route	telnet	ftp
ssh	ping			

Important file locations

The Digi CM unit has several files that are important for administrative use. Below is a brief listing of some files that the root user or system administrator might desire to either monitor or edit.

Default script

The default script file is executed whenever the Digi CM unit is booted. The file is /usr2/rc.user and can be modified with the vi editor. The modified script becomes effective when the system is rebooted.

Booting sequence

When the Digi CM unit boots, it decompresses the /cnf/cnf.tar.gz file to /tmp/cnf/* and unmounts the /cnf file. If the configuration files are modified in the /tmp/cnf file and the configuration is saved to flash (saveconf), the unit mounts the /cnf file and compresses the /tmp/cnf/* to /cnf/cnf.tar.gz.

Config files

All config files are in /tmp/cnf and /tmp/cnf subdirectories. The following table lists the filenames and a brief description.

File name	Description
active_detect	Active auto detection of serial devices
chap-secrets	Chap authentication information when using "PPPoE"
client.pem	Web certificate
./cluster/cluster.conf	Cluster "Master" port information
./cluster/unit#.conf	Cluster "Slave" port information
.cnfversion	Version of current configuration. Used for TFTP update only
dhcpd.opt	DHCPD information
ez-ipupdate.conf	"Dynamic DNS" information for IP assigning
group	User group information
host.cnf	Host name look up order
hosts	Host name table
interfaces	Basic loopback (lo) and ethernet interface (eth0) information (IP, gateway, etc.)
krb5.conf	Kerberos information
./keywords	Keywords for alert configuration
./menu	All custom menu information, .xml files
pap-secrets	PAP auth via PPPoE
passive.detect	Passive auto detection of serial devices
passwd	User password file
./power/power.cnf	Power management configuration
pppoe.conf	Config file for PPPoE

File name	Description
redirect.cnf	Basic port and portaccessmenu config information
resolv.conf	DNS information
server.pem	Private key for SSH with key certification information
shadow	Secure password file
snmpd.conf	SNMP information
./.ssh	Directory for SSH information
system.cnf	Basic network config information (IP, gateway, etc.)
timezone	Time zone configuration
./.usracctl	Directory containing user access control information
version	Firmware version

User storage space

The Digi CM unit comes with 1 megabyte of user storage space. This storage space can be used to store custom scripts. The location is /usr2. Custom scripts such as simple commands, are simply dropped into /usr2. If a file needs to be edited, copy the file into usr2/rc.usr, kill the process, then restart the process from the new file. Scripts from the user storage may be created to run during boot after the network is up. The following are some examples of various ways to create a script stored in the user storage space.

- Saving IP tables options permanently
- Changing radius socket ports
- Limiting root access to the console on Digi CM products
- Sending a break

Example scripts

Example script: Saving IP tables options permanently

Add the following command in the '/usr2/rc.user' script file just above "exit 0". Disabling Telnet is just shown as one example.

1. Create a new script file '/usr2/run.user' that includes the commands you want.

   ```
   iptables -A INPUT -p tcp --dport 23 -j DROP
   ```
2. Run the following command to make the script executable

   ```
   chmod 755 /usr2/run.user
   ```
3. Add the following command in the '/usr2/rc.user' script, just above "exit 0"

   ```
   ln -s /usr2/run.user /etc/rc.d/rc2.d/S60runuser
   ```
4. Reboot

   ```
   reboot
   ```

Note If you factory default the unit, the '/usr2/rc.user' script file is moved to '/usr2/rc.user.old#' and the default rc.user file will be restored.

Example script: Changing radius socket ports

The radius client obtains the radius socket ports to use via the '/etc/services' file. The client only looks up the lines starting with 'radius' and 'radacct'.

1. Modify the /etc/services file as follows. Change lines starting with 'radius' and 'radacct' to the socket numbers you wish. For example:

    ```
    radius 1645/tcp
    radius 1645/ucp
    radacct 1646/tcp
    radacct 1646/ucp
    ```

2. After editing /etc/services copy it to /usr2

    ```
    cp /etc/services /usr2
    ```

3. Edit /usr2/rc.user and add the following line just above "exit 0":

    ```
    cp -a /usr2/services /etc/services
    ```

4. Reboot

    ```
    reboot
    ```

Note If you factory default the unit, the '/usr2/rc.user' script file is moved to '/usr2/rc.user.old#' and the default rc.user file will be restored.

Example script: Limiting root access to the console on Digi CM products (for SSH only)

This prevents root access from any means except physically logging in on the Digi CM console.

1. Modify '/etc/inetd.conf' and append -f /usr2/sshd_config to the sshd line.

    ```
    cp /etc/inetd.conf /usr2/inetd.conf
    ```

2. Edit '/etc/ssh/sshd_config'. Change "PermitRootLogin" to no.

    ```
    cp /etc/ssh/sshd_config /usr2
    ```

3. Add the following commands in the '/usr2/rc.user' script. Add these commands just above "exit 0":

    ```
    cp -a /usr2/inetd.conf /etc/inetd.conf while killall inetd
    2>/dev/null;
    do sleep 5; done
    /usr/sbin/inetd
    ```

4. Reboot

    ```
    reboot
    ```

Note If you factory default the unit, the '/usr2/rc.user' script file is moved to '/usr2/rc.user.old#' and the default rc.user file will be restored.

Example script: Sending a break from an existing session with the Digi CM unit from a Telnet session

If the Telnet was initiated from a UNIX command line Telnet client

Issuing the Telnet escape sequence '^]' (control-right_square_bracket) will take you to the 'telnet>' prompt.

```
telnet>send brk
```

Note Other Telnet clients often have a "send break" option.

From an ssh session

Type the [tilde-break] which is the default ssh break characters.

```
~break
```

The ssh break can changed from the Web UI or config menu under Serial ports > Configuration >

Host mode configuration > SSH break sequence

Additional binaries or applications can be added to /usr2 such as:

- crontab
- netstat
- fuser

To download these utilities go to: https://www.digi.com/products/networking/infrastructure-management/console-servers/digicm#productsupport

User administration

Add, edit or delete users with the Digi CM unit's command line interface.

Add user

Example: `useradd -d /tmp [-g groupid] [-s shellprogram] [username]`

groupid = Options are: Sys admin, Port admin, or Standard User.

> 500 = Sys admin
>
> 501 = Port admin
>
> 502 = Standard User
>
> These are the three types of groups supported by the Digi CM unit. You must use one of these.

`shellprogram` = Options are: CLI (Command Line Interface), Config menu, Port access menu, or Custom menu.

> /bin/bash = CLI

/bin/editconf = Configuration menu

/bin/vts.master = Port access menu

/bin/menu = Custom menu

These are the four types of shells supported by the Digi CM unit. You must use one of these four.

- passwd [username]
- saveconf
- applyconf

Modify user

Example: `usermod -d /tmp [-g groupid] [-s shellprogram] [username]`

Syntax is the same as it is for useradd mentioned above.

- saveconf
- applyconf

Delete user

Example: `userdel [username]`

- saveconf
- applyconf

Locator LED script

The Find Me LED on the Digi CM 48 can be deactivated and reactivated with the following file and command.

Note All other Digi CM units have the locator feature without a Find Me LED. To identify another Digi CM unit, all the LEDs blink when the feature is activated.

The file and syntax for the locator LED is `/bin/blinkled [start|stop]`

Example to stop and start locator LEDS:

```
root@mankato:~# /bin/blinkleds stop
root@mankato:~# /bin/blinkleds start
```

Configuration menu

The configuration menu presents the same functionality in configuring the Digi CM unit as does the web interface, excluding the creation of custom menus. The configuration menu is navigated by using the number representing the menu item and the ESC key to return to earlier menus. Telnet to the Digi CM unit, log in and enter configmenu to start any configuration. If you log in as admin, the configuration menu will automatically appear.

Note Initial setup is described in the Quick Start Guide included with the product packaging. A copy of this document is also available online here.

Access the configuration menu

The configuration menu is available through a Telnet or SSH session to the root user, system administrator, or port administrator. (Port administrator can only change serial port parameters.) The configuration menu enables the authorized users to configure the Digi CM unit with the same functionality as is available with the web interface. The only functionality missing from the configuration menu is the ability to create custom menus.

1. Telnet into the Digi CM unit. The root user, by default, is connected from a Telnet session to the Linux command line.
2. Enter configmenu at the command prompt. The configuration menu follows the layout of the web interface.

```
login: root
Password:
root@Digi_CM_Device:~# configmenu


-----------------------------------------------------------------------
Welcome to Digi CM 48 configuration page
Current time : 01/02/1970 04:43:01      F/W REV.    : v1.7.0b9
Serial No.   : V34751584                MAC Address : 00-40-9d-23-84-36
IP mode      : DHCP                     IP Address  : 10.8.16.39
-----------------------------------------------------------------------

Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
c. Start Device Locating
 <ENTER> Refresh
----->
```

Choices for the configuration menu are made by selecting the number of a menu item. The ESC key allows you to move back a menu each time it is selected. Sometimes only one menu item is presented; however, that single menu item has two or more options that have to be configured.

Configure SSH

1. Choose Serial Port Configuration and then an individual port number or 0 (zero) for all ports.

2. Choose Host mode configuration > Protocol > SSH.

3. Use the ESC key to return to the main configuration menu.

4. Choose **Exit** and apply changes.

Add, edit, and remove users

1. Choose System administration > User administration and then choose an operation to perform (Add, Remove, or Edit)

2. Configure the user as required.

3. Use the ESC key to return to the main configuration menu.

4. Choose Exit and apply changes.

Add and configure a PC card

To add a modem card, compact-flash card, wireless LAN card, or a network card to the Digi CM unit using the configuration menu, do the following:

1. Access the configuration menu.

2. Choose PC Card configuration.

```
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 5
-----------------------------------------------------------------------------
PC Card Configuration
-----------------------------------------------------------------------------
Currently configured PC card : <none>

Select menu
1. Change card configuration
2. Stop the card service to disable or remove card
3. Configuring a new card
 <ESC> Back, <ENTER> Refresh
-----> 3
Insert new card and then press [ENTER] key
Now configuring card type. Please wait !!!
Press [ESC] key to stop card configuring.
```

3. Configure the card by choosing Change card configuration.

   Note The system searches for the card and displays information on the product model number and type of card.

```
Currently configured PC card : <none>

Select menu
1. Change card configuration
2. Stop the card service to disable or remove card
3. Configuring a new card
 <ESC> Back, <ENTER> Refresh
-----> 3
Now configuring card type. Please wait !!!
Press [ESC] key to stop card configuring.
PC card found.
-----------------------------------------------------------------------------
PC Card Configuration
-----------------------------------------------------------------------------
Currently configured PC card : ATA/IDE Fixed Disk Card
Model : TOSHIBA THNCF064MMA
Size : 64 MB
File System : ext2

Select menu
1. Change card configuration
2. Stop the card service to disable or remove card
3. Configuring a new card
 <ESC> Back, <ENTER> Refresh
----->
```

4. Use the ESC key to back out to the main configuration menu.
5. Choose Save Changes.

Host Mode configuration

1. Access the configuration menu.
2. Choose Serial Port Configuration > an individual port number or 0 (zero) for all ports > Host Mode Configuration.

```
11 Port Title #11         CS  192.168.1.111   7011   SSH    RS232-9600-N-8-1-No
12 Port Title #12         CS  192.168.1.112   7012   SSH    RS232-9600-N-8-1-No
13 Port Title #13         CS  192.168.1.113   7013   SSH    RS232-9600-N-8-1-No
14 Port Title #14         CS  192.168.1.114   7014   SSH    RS232-9600-N-8-1-No
15 Port Title #15         CS  192.168.1.115   7015   SSH    RS232-9600-N-8-1-No
16 Port Title #16         CS  192.168.1.116   7016   SSH    RS232-9600-N-8-1-No

Enter port number to confiugre < 0 for all port configuration >
 <ESC> Back, <ENTER> Refresh
 -----> 0
------------------------------------------------------------------------------
Serial configuration --> All ports
------------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title
3. Host Mode Configuration
4. Serial Port Parameters
5. Port Logging
6. IP Filtering
7. Authentication
8. User Access Control
9. SNMP Trap Configuration
0. Port access menu configuration
 <ESC> Back, <ENTER> Refresh
 ----->
```

3. Enter the desired parameters for each menu item.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Port paramaeters

1. Access the configuration menu.

2. Choose Serial Port Configuration > an individual port number or 0 (zero) for all ports.

```
11 Port Title #11         CS  192.168.1.111   7011   SSH    RS232-9600-N-8-1-No
12 Port Title #12         CS  192.168.1.112   7012   SSH    RS232-9600-N-8-1-No
13 Port Title #13         CS  192.168.1.113   7013   SSH    RS232-9600-N-8-1-No
14 Port Title #14         CS  192.168.1.114   7014   SSH    RS232-9600-N-8-1-No
15 Port Title #15         CS  192.168.1.115   7015   SSH    RS232-9600-N-8-1-No
16 Port Title #16         CS  192.168.1.116   7016   SSH    RS232-9600-N-8-1-No

Enter port number to confiugre < 0 for all port configuration >
 <ESC> Back, <ENTER> Refresh
 -----> 0
------------------------------------------------------------------------------
Serial configuration --> All ports
------------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title
3. Host Mode Configuration
4. Serial Port Parameters
5. Port Logging
6. IP Filtering
7. Authentication
8. User Access Control
9. SNMP Trap Configuration
0. Port access menu configuration
 <ESC> Back, <ENTER> Refresh
 ----->
```

3. Enter the desired parameters for each menu item.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Port Access menu

Another default menu is the Port Access Menu, which is available to all users.

1. Access Configuration menu

2. Select Serial Port Configuration.

3. Select 0 for all ports.

4. Select Port access menu configuration.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 2
--------------------------------------------------------------------------------
Serial configuration
--------------------------------------------------------------------------------
Port#     Title        Mode Dest/AssignedIP Port    Proto   Serial-Settings
1   Port Title #1      DI   --------------- -----   ------  RS232-9600-N-8-1-No
2   Port Title #2      CS   0.0.0.0         7002    Telnet  RS232-9600-N-8-1-No
3   Port Title #3      CS   0.0.0.0         7003    Telnet  RS232-9600-N-8-1-No
4   Port Title #4      CS   0.0.0.0         7004    Telnet  RS232-9600-N-8-1-No
5   Port Title #5      CS   0.0.0.0         7005    Telnet  RS232-9600-N-8-1-No
6   Port Title #6      CS   0.0.0.0         7006    Telnet  RS232-9600-N-8-1-No
7   Port Title #7      CS   0.0.0.0         7007    Telnet  RS232-9600-N-8-1-No
8   Port Title #8      CS   0.0.0.0         7008    Telnet  RS232-9600-N-8-1-No

Enter port number to confiugre ( 0 for all port configuration )
 <ESC> Back, <ENTER> Refresh
-----> 0
--------------------------------------------------------------------------------
Serial configuration --> All ports
--------------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title
3. Host Mode Configuration
4. Serial Port Parameters
5. Port Logging
6. IP Filtering
7. Authentication
8. User Access Control
9. Alert Configuration
0. Port access menu configuration
 <ESC> Back, <ENTER> Refresh
-----> 0
```

You can access this menu through a Telnet or SSH session using the IP address of the Digi CM unit followed by the port number 7000 as in the following example:

```
telnet 192.168.100.200 7000
```

By default root is connected to the command line interface and the preceding option allows the root user access to the port access menu.

System logging

System logging is a two part process. First, the device being used to record the system logs must be configured. Secondly, system logging must be configured for the system under System status and log. System logs can be saved to the Digi CM unit's system memory (there is no need to configure the memory), a compact-flash card, an NFS server, or a SYSLOG server.

Configure the system log device

To configure the compact-flash card for system logging, see Add a compact flash card. For an NFS or SYSLOG server, do the following:

1. Access the configuration menu.
2. Choose Network configuration > NFS or SYSLOG server configuration.

```
------------------------------------------------------------------------
Network configuration
------------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet configuration
a. TCP service configuration
 <ESC> Back, <ENTER> Refresh
------> 7_
```

3. Disable or enable the server.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Configure system logging

1. Access the configuration menu.

2. Choose System Status & log > System logging.

```
------------------------------------------------------------------------
System status & log
------------------------------------------------------------------------
Select menu
1. System status
2. System logging
3. User logged on list
 <ESC> Back, <ENTER> Refresh
------> 2
------------------------------------------------------------------------
System status & log --> System logging
------------------------------------------------------------------------
Select menu
1. Enable/Disable system logging : Enable
2. System log buffer size : 50 KB
3. System log storage location : Memory
4. Display system logs
5. Clear system logs
6. Send system log by Email : Disable
 <ESC> Back, <ENTER> Refresh
------> _
```

3. Enter the desired parameters for the menu items.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Configure SNMP

To configure SNMP from the configuration menu, do the following:

1. Access the configuration menu.

2. Choose Network Configuration > SNMP configuration.

```
Network configuration
----------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet configuration
a. TCP service configuration
 <ESC> Back, <ENTER> Refresh
-----> 2
----------------------------------------------------------------------
Network configuration --> SNMP configuration
----------------------------------------------------------------------
Select menu
1. Configure the MIB-II System objects
2. Configure the Access control settings
3. Configure the Trap receiver settings
 <ESC> Back, <ENTER> Refresh
----->
```

3. Enter the desired parameters for the menu items.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Configure SMTP

To configure SMTP from the configuration menu, do the following:

1. Access the configuration menu.

2. Choose Network configuration > SMTP configuration.


```
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet configuration
a. TCP service configuration
 <ESC> Back, <ENTER> Refresh
-----> 4
----------------------------------------------------------------------
Network configuration --> SMTP configuration
----------------------------------------------------------------------
Select menu
1. Send mail : Enable
2. SMTP server : None
3. Mode : SMTP without authentication
4. secondary SMTP server : None
5. Device mail address :
 <ESC> Back, <ENTER> Refresh
----->
```

3. Enter the desired parameters for the menu items.

4. Use the ESC key when all parameters are entered to return to the main menu.

5. Choose Save changes.

Network IP filtering

To configure the Digi CM unit for Network IP filtering, do the following:

1. Access the configuration menu.

2. Choose Network configuration > IP filtering.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
<ENTER> Refresh
-----> 1
----------------------------------------------------------------------
Network configuration
----------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet configuration
a. TCP service configuration
<ESC> Back, <ENTER> Refresh
-----> 5
----------------------------------------------------------------------
Network configuration --> IP filtering
----------------------------------------------------------------------
#  Iface  Option   IP/Mask                   Port    Command
1  all    Invert   192.168.0.0/255.255.0.0    22      DROP
2  all    Invert   192.168.0.0/255.255.0.0    23      DROP
3  all    Normal   192.168.1.0/255.255.255.0  80      ACCEPT
4  all    Normal   192.168.2.0/255.255.255.0  80      ACCEPT
5  all    Normal   0.0.0.0/0.0.0.0            80      DROP
6  all    Normal   192.168.1.0/255.255.255.0  443     ACCEPT
7  all    Invert   192.168.2.0/255.255.255.0  443     DROP

a. Telnet Console     : Enabled
b. SSH Console        : Enabled
c. Web Configuration  : HTTP Disabled : HTTPS Enabled

1. Add a Rule
2. Remove a Rule
3. Edit a Rule
<ESC> Back, <ENTER> Refresh
----->
```

3. Choose a menu item and enter the desired parameters for the menu items.

4. Use the ESC key to return to the main menu.

5. Choose Save changes.

Port IP filtering

To configure the Digi CM unit for Port IP filtering, do the following:

1. Access the configuration menu.

2. Choose Serial port configuration.

3. Choose an individual port number or 0 (zero) for all ports > IP filtering.

```
11 Port Title #11        CS  192.168.1.111   7011  Telnet RS232-9600-N-8-1-No
12 Port Title #12        CS  192.168.1.112   7012  Telnet RS232-9600-N-8-1-No
13 Port Title #13        CS  192.168.1.113   7013  Telnet RS232-9600-N-8-1-No
14 Port Title #14        CS  192.168.1.114   7014  Telnet RS232-9600-N-8-1-No
15 Port Title #15        CS  192.168.1.115   7015  Telnet RS232-9600-N-8-1-No
16 Port Title #16        CS  192.168.1.116   7016  Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
 <ESC> Back, <ENTER> Refresh
 -----> 0
------------------------------------------------------------------------
 Serial configuration --> All ports
------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. SNMP Trap Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
  -----> 6
```

4. Choose a menu item and enter the desired parameters for the menu items.

5. Use the ESC key when all parameters are entered to return to the main menu.

6. Choose Save changes.

Sniff sessions

To configure a port or all ports for sniff users, do the following:

1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number or 0 (zero) for all ports > User access control.
4. Choose User Access Control.
5. Choose Enable/Disable Sniff Mode.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
----> 2
--------------------------------------------------------------------------------
Serial configuration
--------------------------------------------------------------------------------
Port#      Title         Mode Dest/AssignedIP Port   Proto   Serial-Settings
1   Port Title #1         DI   --------      ----  ------  RS232-9600-N-8-1-No
2   Port Title #2         CS   0.0.0.0        7002  Telnet  RS232-9600-N-8-1-No
3   Port Title #3         CS   0.0.0.0        7003  Telnet  RS232-9600-N-8-1-No
4   Port Title #4         CS   0.0.0.0        7004  Telnet  RS232-9600-N-8-1-No
5   Port Title #5         CS   0.0.0.0        7005  Telnet  RS232-9600-N-8-1-No
6   Port Title #6         CS   0.0.0.0        7006  Telnet  RS232-9600-N-8-1-No
7   Port Title #7         CS   0.0.0.0        7007  Telnet  RS232-9600-N-8-1-No
8   Port Title #8         CS   0.0.0.0        7008  Telnet  RS232-9600-N-8-1-No

Enter port number to confiugre < 0 for all port configuration >
 <ESC> Back, <ENTER> Refresh
----> 0
--------------------------------------------------------------------------------
Serial configuration --> All ports
--------------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title
3. Host Mode Configuration
4. Serial Port Parameters
5. Port Logging
6. IP Filtering
7. Authentication
8. User Access Control
9. Alert Configuration
0. Port access menu configuration
 <ESC> Back, <ENTER> Refresh
----> 8
--------------------------------------------------------------------------------
Serial configuration --> All ports --> User access control
--------------------------------------------------------------------------------
1. User Permissions
2. Enable/Disable Sniff Mode : Disable
 <ESC> Back, <ENTER> Refresh
----> 2
Select enable/disable sniff mode < 1 = Enable, 2 = Disable > :
```

6. Choose a menu item and enter the desired parameters.
7. Use the ESC key when all parameters are entered to return to the main menu.
8. Choose Save changes.

For information on entering a sniff session, see the next section, View a sniff session.

View a sniff session

A sniff user enters a sniff session by starting a Telnet session on a specified port. In the following example, a sniff user telnets to port 7 of the Digi CM unit. From the command prompt enter the following command:

```
telnet 192.168.100.42 7007
```

1. Log in and enter your password.
2. Enter the port escape sequence.

```
Port Menu:

b      send break
d      disconnect a sniff session
a      send message to port user

x      close current connection to port
```

When sniff users login to a port from a Telnet session, a sniff session menu is displayed with your permitted options. The first user (with port access rights) to login to the port is in the main session.

```
Port Menu:

<Port Title #1> <Port 1> is being used by <Gilligan>
The <Skipper> is connected in monitoring mode.

m      take over main session
s      enter as a slave session

d      disconnect a sniff session
a      send message to port user

x      close current connection to port
```

The next user (with port access rights) to enter the port will be given the option to take over the main session. This user is given the option to take over the main session by either terminating the first user or switching the first user to sniff (read only).

```
Port Menu:

<Port Title #7> <Port 7> is being used by <Gilligan>
The <Skipper> is connected in monitoring mode.

m      take over main session
s      enter as a slave session

l      show last 100 lines of log buffer
d      disconnect a sniff session
a      send message to port user

x      close current connection to port

Take over master session and
t      terminate session of main session
s      switch main session to sniff mode
```

Field descriptions for sniff sessions

Escape sequence Ctrl+	Description of action	Occurrence
m	take over main session (read/write)	only presented to users with read/write access upon entering a session
s	enter as a slave session (read only)	only presented to users with read/write access upon entering a session
b	send break	not functional for sniff users

Escape sequence Ctrl+	Description of action	Occurrence
l	show last 100 lines of log buffer	must enable logging for this option
d	disconnect a sniff session	only functional to admin
a	send message to port user(s)	not available to sniff users
r	reboot device using power-switch	only if power management is available on this port
p	power device on/off	(show only on or off) only if power management is available on this port
x	close current connection to port	closes the sniff session connection

Authentication

1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number or 0 (zero) for all ports > Authentication.
4. Choose Authentication type.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 2
--------------------------------------------------------------------------------
Serial configuration
--------------------------------------------------------------------------------
Port#      Title        Mode Dest/AssignedIP Port   Proto    Serial-Settings
1   Port Title #1        DI   --------------- -----  ------   RS232-9600-N-8-1-No
2   Port Title #2        CS   0.0.0.0         7002   Telnet   RS232-9600-N-8-1-No
3   Port Title #3        CS   0.0.0.0         7003   Telnet   RS232-9600-N-8-1-No
4   Port Title #4        CS   0.0.0.0         7004   Telnet   RS232-9600-N-8-1-No
5   Port Title #5        CS   0.0.0.0         7005   Telnet   RS232-9600-N-8-1-No
6   Port Title #6        CS   0.0.0.0         7006   Telnet   RS232-9600-N-8-1-No
7   Port Title #7        CS   0.0.0.0         7007   Telnet   RS232-9600-N-8-1-No
8   Port Title #8        CS   0.0.0.0         7008   Telnet   RS232-9600-N-8-1-No

Enter port number to confiugre ( 0 for all port configuration )
 <ESC> Back, <ENTER> Refresh
-----> 0
--------------------------------------------------------------------------------
Serial configuration --> All ports
--------------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title
3. Host Mode Configuration
4. Serial Port Parameters
5. Port Logging
6. IP Filtering
7. Authentication
8. User Access Control
9. Alert Configuration
0. Port access menu configuration
 <ESC> Back, <ENTER> Refresh
-----> 7
--------------------------------------------------------------------------------
Serial configuration --> All ports --> Authentication
--------------------------------------------------------------------------------
1. Authenticaton Type : Local
 <ESC> Back, <ENTER> Refresh
-----> 1
Select authentication type.
  0 = None,   1 = RADIUS,   2 = Local, 3 = RADIUS-Local, 4 = Local-RADIUS
  5 = TACACS+,   6 = TACACS+-Local,   7 = Local-TACACS+
  8 = LDAP,      9 = LDAP-Local,      10 = Local-LDAP
  11 = Kerberos, 12 = Kerberos-Local, 13 = Local-Kerberos
  14 = RADIUS Down-Local
----->
```

5. Use the ESC key to return to the main menu.

6. Choose Save changes.

Upload server certificate

To upload your own certificate, you can use one of following two methods,

1. Use Upload Server Certificate menu.

Note This menu is displayed only when you run configmenu on the serial console of the Digi CM unit. (configmenu run on CLI via Telnet or SHI will not display this menu)

---

2. Copy your own server.pem file to /tmp/cnf/ using scp.

Note Do not forget to run saveconf command in CLI if you want to keep this change permanently.

You can use your own certificate for your Digi CM unit after replacing the original server.pem on /tmp/cnf/ with your server.pem. The following procedure is to import an SSL certificate for the HTTPS interface.

OpenSSL (SSLeay) Simple CA Usage - Install Openssl

1. Download latest openssl package

2. Install openssl package

```
# cd  /work/
#  tar  -xvzf  openssl-0.9.7c.tar.gz # cd openssl-0.9.7c
# cd openssl-0.9.7c
#   ./config
# make
# make  test
# make  install
```

Make Root CA (Certificate Authority for self-signed)

1. Edit openssl configuration file

   ```
   # vi /usr/share/ssl/openssl.cnf
   ```

Note Modify [req_distinguished_name] section of "openssl.cnf" Please refer to sample openssl.conf file(openssl.conf.digi). Modify [req_attributes] section of "openssl.cnf"

challengePassword_min =0

challengePassword_max =0

2. Make self-signed Root CA(Certificate Authority)

   ```
   # cd /work/openssl-0.9.7c/ # mkdir CA
   # cd CA
   # sh /usr/local/ssl/misc/CA.sh -newca
   CA certificate filename (or enter to create)
   ; (Press Enter to use default value)
   Making CA certificate ...
   ; openssl is called here as follow from CA.sh
   ; openssl req -new -x509 -keyout ./demoCA/private/./cakey.pem \
   ; -out ./demoCA/./cacert.pem -days 365
   ```

3. Use configuration from

   ```
   /usr/local/ssl/lib/ssleay.cnf
   ```

4. Generate a 1024 bit RSA private key.

   ```
   ........++++++
   ....................++++++
   ```

5. Write new private key to './demoCA/private/./cakey.pem'

6. Enter PEM pass phrase:

   ```
   ; CA Password (Enter passsword and remember this) Verify password -
   Enter PEM pass phrase: ; CA Password
   ```

Note The following information will be incorporated into your certificate.

You will enter text for a field call Distinguished Name or a DN. Although there are many fields, some can be left blank, use a default, or enter '.' and the field will be left blank.

```
----- ; CA's Information
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Your-State]: Minnesota
Locality Name (eg, city) []: Minneapolis
Organization Name (eg, company): Digi International Organizational
Unit Name (eg, section) [](Enter) Common Name (eg, YOUR name) []:
Bob Alou
Email Address []:(Enter)
#
```

7. Verify the CA key file(demoCA/private/cakey.pem) and CA certificate (demoCA/cacert.pem) is generated

```
# ls demoCA/
                    cacert.pem certs crl index.txt newcerts
                    private serial
# ls demoCA/private
                     cakey.pem
```

Make a certificate request

To make new certificates, you should make a certificate request first.

1. Enter the following

   ```
   # cd /work/openssl-0.9.7c/CA
   ```

2. Run the following commands:

   ```
   # openssl genrsa -out key.pem 1024
   ```
   ```
   # openssl req -new -key key.pem -out req.pem
   ```
   ```
   It is assumed that you are using sample configuration file -
   "openssl.conf.digi" )
   ```

3. Use configuration from /usr/share/ssl/openssl.cnf

   ```
   You are about to be asked to enter information that will be
   incorporated into your certificate request.
   ```
   ```
   What you are about to enter is what is called a Distinguished Name
   or a DN.
   ```
   ```
   There are quite a few fields but you can leave some blank For some
   fields there will be a default value,
   ```
   ```
   If you enter '.', the field will be left blank.
   ```

Note The following information will be incorporated into your certificate.

You will enter text for a field call Distinguished Name or a DN. You may enter a default or '.' to leave the field blank.

```
----- ; CA's Information
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Your-State]: Minnesota
```

```
Locality Name (eg, city) []: Minneapolis
Organization Name (eg, company): Digi International
Organizational Unit Name (eg, section) [](Enter)
Common Name (eg, YOUR name or your server's hostname) []: Digi CM
Email Address []:(Enter)
```

Enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []:(Press Enter - Do not enter any other
characters)
An optional company name []:(Press Enter - Do not enter any other
characters)
```

Sign a certificate request

1. To sign a certificate request, enter the following:

```
# cd /work/openssl-0.9.7c/CA # cp req.pem newreq.pem
# sh /usr/local/ssl/misc/CA.sh -sign
Use configuration from /usr/share/ssl/openssl.cnf
```

2. Enter PEM pass phrase:

   `CA Password` (Enter CA Password from Make Root CA (Certificate Authority for self-signed).)

3. Check that the request matches the signature.

```
Signature ok
The Subjects Distinguished Name is as follows countryName
:PRINTABLE:'US' stateOrProvinceName :PRINTABLE:'Minnesota'
localityName :PRINTABLE:'Minneapolis' organizationName
:PRINTABLE:'Digi International' commonName :PRINTABLE:'Digi CM'
Certificate is to be certified until Oct 6 09:39:59 2013 GMT (3653
days) Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y Write out
database with 1 new entries
Data Base Updated Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Digi International,
CN=Digi International
Validity
Not Before: Oct 6 09:39:59 2003 GMT
Not After : Oct 6 09:39:59 2013 GMT
Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International,
CN=Digi CM
Subject Public Key Info:
Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit)
```

```
....
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
```

4. Verify signed certificate(newcert.pem) is generated.

```
# ls
demoCA key.pem newcert.pem newreq.pem req.pem
```

Make certificate for the Digi CM Unit

1. Removing headings in newcert.pem file

```
# cd /work/openssl-0.9.7c/CA
# cp newcert.pem server.pem
# vi server.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Digi International,
CN=Digi CM
ValidityNot Before: Oct 6 09:39:59 2003 GMT
Not After : Oct 6 09:39:59 2013 GMT
Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International,
CN=Digi CM
Subject Public Key Info:
Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit)
....
== Removing above lines ===
-----BEGIN CERTIFICATE-----
....
-----END CERTIFICATE-----
```

2. Concatenating key.pem file to server.pem

```
# cat key.pem >> server.pem
```

Dial-in modem access

Individual serial ports on the Digi CM unit can be configured for dial-in modem access. To use dial-in modem mode, an external modem is first attached to a serial port and then the serial port is configured for dial-in modem access. In the illustration below, port 7 is configured for a dial-in modem.

To configure a serial port for a dial-in modem, do the following:

1. Access the configuration menu.
2. Choose Serial Port Configuration.
3. Choose an individual port number and then Host Mode Configuration.
4. Select Host mode and then Dial-in modem.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 2
------------------------------------------------------------------------
Serial configuration
------------------------------------------------------------------------
Port#    Title       Mode Dest/AssignedIP Port   Proto   Serial-Settings
1  Port Title #1      TS   0.0.0.0          0    Telnet RS232-9600-N-8-1-No
2  Port Title #2      CS   0.0.0.0         7002  Telnet RS232-9600-N-8-1-No
3  Port Title #3      CS   0.0.0.0         7003  Telnet RS232-9600-N-8-1-No
4  Port Title #4      CS   0.0.0.0         7004  Telnet RS232-9600-N-8-1-No
5  Port Title #5      CS   0.0.0.0         7005  Telnet RS232-9600-N-8-1-No
6  Port Title #6      CS   0.0.0.0         7006  Telnet RS232-9600-N-8-1-No
7  Port Title #7      CS   0.0.0.0         7007  Telnet RS232-9600-N-8-1-No
8  Port Title #8      CS   0.0.0.0         7008  Telnet RS232-9600-N-8-1-No

Enter port number to confiugre ( 0 for all port configuration )
 <ESC> Back, <ENTER> Refresh
-----> 1
------------------------------------------------------------------------
Serial configuration --> port #1
------------------------------------------------------------------------
1. Enable/Disable Port : Enable
2. Port Title : Port Title #1
3. Host Mode Configuration
4. Serial Port Parameters
5. Authentication
0. Apply all ports setting : Enable
a. Port Management
 <ESC> Back, <ENTER> Refresh
-----> 3
------------------------------------------------------------------------
Serial configuration --> Port#1 --> Host mode configuration
------------------------------------------------------------------------
Select menu
1. Host mode : Terminal Server
2. Terminal Server Option : Shell Program
3. Shell Program Path :
 <ESC> Back, <ENTER> Refresh
-----> 1
Select Host mode :
   1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
   4 = Dial-In Terminal Server
-----> 3
```

5. Use the ESC key to return to the main menu.
6. Choose Save changes.

Dial-in terminal server access

Individual serial ports on the Digi CM unit can be configured for a dial-in terminal server access. To use dial-in terminal server access, an external modem is first attached to a serial port on the Digi CM unit and then the serial port is configured for dial-in terminal server mode. In the illustration below, port 7 is configured for dial-in terminal server mode.

In terminal server mode, you are connected directly to a server.

To configure a serial port for a dial-in terminal server, do the following:

1. Access the configuration menu.
2. Choose Serial port configuration.
3. Choose an individual port number and then Host Mode Configuration.

```
Select menu
1. Host mode : Dial-in modem
2. Inactivity timeout : 100 sec
3. Modem init string : q1e0s0=2
 <ESC> Back, <ENTER> Refresh
-----> 1
Select Host mode :
    1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
    4 = Dial-In Termimal Server
-----> 1
```

4. Choose Dial-in Terminal Server and configure the other configuration parameters.

5. Use the ESC key to return to the main menu.

6. Choose Save changes.

Clustering

DBy default clustered slave devices are configured using the Telnet protocol and port parameters of the following: bps=9600, data bits=8, parity=none, stop bits=1, flow control=none. When the master device autoconfigures a slave device, it simply imports the information from the slave unit. If you want other protocols or other port parameters, you should configure your slave unit first with those parameters before autoconfiguring.

Before you start this configuration procedure, the slave units should already be configured unless you want them set to the default values. To set up the Digi CM unit for clustering, do the following:

1. Access the configuration menu.

2. Choose Clustering configuration > Unit position.

3. Assign the unit as the master device. A new screen is displayed.

```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 3
-------------------------------------------------------------------
Clustering Configuration
-------------------------------------------------------------------
Select menu
 0. Unit position : Master

 1. ---------------         2. ---------------
 3. ---------------         4. ---------------
 5. ---------------         6. ---------------
 7. ---------------         8. ---------------
 9. ---------------        10. ---------------
11. ---------------        12. ---------------
13. ---------------        14. ---------------
15. ---------------        16. ---------------
 <ESC> Back, <ENTER> Refresh
----->
```

4. Enter the number 1 for the first slave unit.

5. Choose Enable/Disable unit clustering > Enable.

```
------------------------------------------------------------------------
Clustering configuration --> Unit #1
------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Disable
 <ESC> Back, <ENTER> Refresh
-----> 1
Select unit clustering option ( 1 = Enable, 2 = Disable) : 1_
```

6. Enter the values for Slave Unit IP, No. of ports, and Port configuration.

7. Select the port number to configure or 0 for all ports.

```
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : None
3. No. of Ports : 0
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 2
Enter slave unit IP : 143.191.4.101
------------------------------------------------------------------------
Clustering configuration --> Unit #2
------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : 143.191.4.101
3. No. of Ports : 0
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 3
Enter no. of ports ( 1 = 4, 2 = 8, 3 = 16, 4 = 32, 5 = 48 ) : 4
------------------------------------------------------------------------
Clustering configuration --> Unit #2
------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : 143.191.4.101
3. No. of Ports : 32
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 4
------------------------------------------------------------------------
Clustering configuration --> Unit #2
------------------------------------------------------------------------
Port#  S. Port  D. Port  Enb  Proto    Port#  S. Port  D. Port  Enb  Proto
   1        0        0    D   UNKNOW       2        0        0    D   UNKNOW
   3        0        0    D   UNKNOW       4        0        0    D   UNKNOW
   5        0        0    D   UNKNOW       6        0        0    D   UNKNOW
   7        0        0    D   UNKNOW       8        0        0    D   UNKNOW
   9        0        0    D   UNKNOW      10        0        0    D   UNKNOW
  11        0        0    D   UNKNOW      12        0        0    D   UNKNOW
  13        0        0    D   UNKNOW      14        0        0    D   UNKNOW
  15        0        0    D   UNKNOW      16        0        0    D   UNKNOW
  17        0        0    D   UNKNOW      18        0        0    D   UNKNOW
  19        0        0    D   UNKNOW      20        0        0    D   UNKNOW
  21        0        0    D   UNKNOW      22        0        0    D   UNKNOW
  23        0        0    D   UNKNOW      24        0        0    D   UNKNOW
  25        0        0    D   UNKNOW      26        0        0    D   UNKNOW
  27        0        0    D   UNKNOW      28        0        0    D   UNKNOW
  29        0        0    D   UNKNOW      30        0        0    D   UNKNOW
  31        0        0    D   UNKNOW      32        0        0    D   UNKNOW

Enter port number to confiugre ( 0 for all port configuration )
-----> 0_
```

8. Select Enable configuration

9. Select Auto Configuration

10. Choose Exit and apply changes.

Firmware upgrade

Before upgrading firmware from the configuration menu you should have:

- Downloaded the firmware to a system on the same subnet

- Set up a terminal emulation program that supports Zmodem transfer protocol To upgrade the firmware with the configuration menu, do the following:

1. Access the configuration menu.

2. Choose System administration.

```
System Administration
--------------------------------------------------------------------------
Select menu
1. User administration
2. Device name : Digi_CM_Device
3. Date and time
4. Configuration management
5. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
-----> 5

*** Firmware upgrade will RESTART your device. ***
Do you want to start firmware upgrade ? (y/n) : _
```

3. Choose Firmware upgrade. Enter y for Yes when asked if you want to upgrade the firmware.

If the firmware upgrade is successful, the Digi CM unit will reboot automatically. If a **Firmware upgrade failed!** warning appears, do not reboot the unit but repeat the upgrade process.

Restore factory defaults

You have two choices to restore the unit to its factory defaults. The options are restoring all factory defaults or restoring all factory defaults except IP settings. To restore your unit to the factory defaults, do the following:

1. Access the configuration menu.
2. Choose System administration.
3. Select Configuration import.
4. Select Location.

```
System Administration
--------------------------------------------------------------------------
Select menu
1. User administration
2. Device name : Digi_CM_Device
3. Date and time
4. Configuration management
5. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
-----> 4
--------------------------------------------------------------------------
System Administration --> Configuration Management
--------------------------------------------------------------------------
Select menu
1. Configuration export
2. Configuration import
 <ESC> Back, <ENTER> Refresh
-----> 2
--------------------------------------------------------------------------
System Administration --> Configuration Management --> Configuration import
--------------------------------------------------------------------------
Select menu
1. Location : None
2. Filename : None
3. Encrypt  : Yes
4. Configuration Selection (Press A-E to select each option
   A. [X] System configuration
   B. [X] Serial port configuration
   C. [X] Clustering configuration
   D. [X] System user configuration
   E. [X] Custom menu
 <ESC> Back, <ENTER> Refresh
-----> 1
Select location.
( 1 = CF Card ,
  2 = Primary NFS ,
  3 = User Space (/usr2),
  4 = Local Machine,
  5 = Factory Default )
----->_
```

5. Select Factory Default.

The system will restore factory defaults, and the unit will automatically reboot.

> **Note** Use System Administration to save your configuration in case you need to reload it later or onto another system. See Add and configure a PC card for more information.

Set date and time

Date and time on the Digi CM unit can either be kept internally or by an NTP server. To set the parameters for date and time on the Digi CM unit, do the following:

1. Access the configuration menu.
2. Choose System administration.
3. Choose Date and Time.
4. Enter the desired parameters.
5. Choose Save changes.

Access the Boot Loader program

The Boot Loader program can be accessed during the boot process. The main function of the program is to provide a backup means for restoring the firmware if the Digi CM unit will no longer boot. It also provides a hardware testing module that detects and tests hardware components on the unit.

To access the Boot Loader program, do the following:

1. Connect the Ethernet cable from the console port on the rear panel of the Digi CM unit to a serial port on a workstation. Use the Ethernet cable packaged with the Digi CM unit and attach the DB-9 adapter. The arrow in the following graphic points to the Console Port.
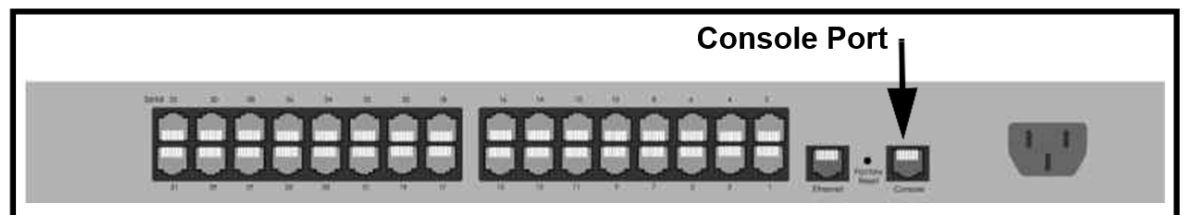
2. Set up a terminal emulation program, such as HyperTerminal, using the following port parameters: bps=9600, data bits=8, parity=none, stop bits=1, and flow control=none.
3. Turn the power on to the unit.
4. Press ESC within 3 seconds of booting the unit to get Boot Loader menu.

Hardware test menu

The Boot Loader program provides a hardware test for detecting and testing hardware components on the Digi CM unit. From the Boot Loader menu, choose the number 3 to access the Hardware test. Options for several components appear.

Disaster recovery

The Digi CM unit provides a disaster recovery procedure in the event the configuration data is destroyed or corrupted. The Digi CM unit automatically restores a corrupted configuration file system to the factory default settings. However, if the Digi CM unit fails to boot in spite of being reset to the factory default settings, the firmware can be restored by using the Boot Loader program.

To restore the Digi CM unit to the factory default configuration settings, you will need to use a TFTP or BOOTP server. To use the Boot Loader program to flash new firmware, do the following:

1. Connect the console port on the rear panel of the Digi CM unit to a serial port on a workstation. Use an Ethernet cable with a DB-9 adapter.

2. Set up a terminal emulation program such as HyperTerminal. Use the following port parameters: bps=9600, data bits=8, parity=none, stop bits=1, flow control=none

3. Reboot or power on the Digi CM unit.

4. Press the ESC key within three seconds of applying power to the device. The following screen appears.

```
Bootloader(48port) 1.1.1 (Jun  2 2004 - 15:07:26)

CPU      :  XPC855xxZPnnD4 (65 MHz)
DRAM     :  256 MB
FLASH    :  32 MB
PC CARD  :  No card
EEPROM   :  A Type exist
Ethernet :  AUTO-NEGOTIATION
Autoboot Start:  0
--------------------------------------------------------------------------
 Welcome to Boot Loader Configuration page
--------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Oct 29 2004 - 10:54:22 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.5.3.1]
 4. Exit and boot from flash
 5. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->  _
```

5. Choose Firmware upgrade by entering 3. The following screen appears.

```
 -----> 3
--------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------
 Select menu
 1. Protocol [BOOTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [cm48.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select protocol ( 1 = BOOTP, 2 = TFTP) : 2
--------------------------------------------------------------------------
 Firmware upgrade
--------------------------------------------------------------------------
 Select menu
 1. Protocol [TFTP]
 2. IP address assigned to Ethernet interface [192.168.161.5]
 3. Server's IP address [192.168.0.128]
 4. Firmware File Name [cm48.bin]
 5. Start firmware upgrade
  <ESC> Back, <ENTER> Refresh
 ----->
```

6. Enter the information for the first menu items.

   ■ Protocol: The choices are BOOTP or TFTP

   ■ IP address assigned: Enter the IP address of the Digi CM unit

   ■ Server's IP address: The IP address of the BOOTP or TFTP server

   ■ Firmware File Name: The filename for the firmware

   Note Use the ESC key to back up to earlier menu screens.

7. Choose Start firmware upgrade. The firmware upgrade will take several minutes to process. This will factory default the unit.

8. When the upgrade process is complete, choose ESC to return to the main menu.

9. Choose Exit and boot from flash.

Hardware information

This section provides information on Digi CM hardware. Among the topics covered are the hardware specifications, LED descriptions, pinouts for the Ethernet cable, pinouts for the cable adapters, and rack mounting specifications.

Hardware specifications

Dig CM 48

Attribute	Value AC Powered	Value DC Powered
Operating temperature	40°F to 120°F (5°C to 50°C)	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing	10% to 90% non-condensing
Power supply	Internal, 100 -240VAC, 50/60 Hz, 1.2A (max)	Internal, 36 - 72 Vdc, 1.2A (max)
Power consumption	0.37A / 120VAC, 45W (typical), 150W (max)	0.4A / 48Vdc, 19W (typical), 40W (max)
Fuse (internal)	FUSE (Type L) AC250V, 2A	Fuse (Type L) 250V, 5A
Operating system	Linux Hard Hat embedded	Linux Hard Hat embedded
SDRAM	256 megabytes	256 megabytes
Flash memory	16 megabytes	16 megabytes
Dimensions: unpackaged	17.5" x 10.0" x 1.75" (44.5 x 25.4 x 4.5 cm)	17.5" x 10.0" x 1.75" (44.5 x 25.4 x 4.5 cm)
Weight: unpackaged	6.5 lbs (2.95 kg)	6.7 lbs (3.05 kg)
Weight: packaged	9.95 lbs (4.51 kg)	10.2 lbs (4.61 kg)

Digi CM 16 and Digi CM 32

Attribute	Value AC Powered	Value DC Powered
Operating temperature	40°F to 120°F (5°C to 50°C)	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing	10% to 90% non-condensing
Power supply	Internal, 100 -240VAC, 50/60 Hz, 1.2A (max)	Internal, 36 - 72 Vdc, 1.2A (max)
Power consumption	0.1A /120VAC (type), 12W (typical), 40W (max)	0.25A /48Vdc, 12W (typical), 40W (max)
Fuse (internal)	FUSE (Type L) AC250V, 2A	
Operating system	Linux Hard Hat embedded	Linux Hard Hat embedded
SDRAM	64 megabytes	64 megabytes
Flash memory	8 megabytes	8 megabytes
Dimensions: unpackaged	17" x 8.5" x 1.75" (431.8 cm x 215.9 cm x 44.5 cm)	17" x 8.5" x 1.75" (431.8 cm x 215.9 cm x 44.5 cm)
Weight: unpackaged	5.8 lbs (2.63 kilograms)	5.8 lbs (2.63 kilograms)
Weight: packaged	8.6 lbs (3.9 kilograms)	8.6 lbs (3.9 kilograms)

Digi CM 8 AC Powered

Attribute	Value
Operating temperature	40°F to 120°F (5°C to 50°C)
Storage temperature	-20°F to 140°F (-29°C to 60°C)
Humidity	10% to 90% non-condensing
Power supply	External, 100 - 240VAC, 50/60 Hz, 1.0A (max)
Power consumption	AC input: 0.05A /120VAC, 6W (typical), 12W (max) DC input: 0.8A/5VAC, 4.5 W (typical), 8W (max)
Operating system	Linux Hard Hat embedded
SDRAM	64 megabytes

Attribute	Value
Flash memory	8 megabytes
Dimensions	9.5" x 6.25" x 1.25" (241.3 cm 158.75 x 31.75 cm)
Weight	2.5 lbs (1.13 kilograms)

LED indicators

Use the LED indicators to confirm your attachment to the network and that the Digi CM unit is able to send and receive data.

LED		Function
System	Power	On when power is supplied
	Ready	On when system is ready to run
	PC	On when a PC device is running
Ethernet	100 Mbps	On when 100Base-TX connection is detected
	LINK	On when connected to an Ethernet network
	Act	Blinks when there is activity on the Ethernet
Serial port*	In use	On when the serial port is ready to run
	Rx/Tx	Blinks when there is traffic on the serial port
*Not available on the Digi CM 48		

About serial port cabling

The Digi CM unit simplifies cabling. The RJ-45 8-pin configuration matches all SUN and Cisco RJ-45 console port configurations, enabling CAT 5 cabling without pinout concerns. Three DB-25 and one DB-9 adapters come in the package. A DB-25 male, a DB-25 female, and a DB-9 adapter support console management applications. A DB-25 male adapter provides a modem connection. See the cable adapter information that follows later in this chapter.

Note The cable length restrictions common to RS-232 cables apply to the Digi CM serial cable as well.

Serial port pinouts

The Digi CM unit uses an RJ-45 connector for serial ports. Pin assignments are listed in the following table.

Pin	Description
1	CTS
2	DSR

Pin	Description
3	RxD
4	GND
5	DCD **Note** Inbound signal can also be used as a second ground.
6	TxD
7	DTR
8	RTS

Cable adapters

The Digi CM unit comes with four cable adapters. The following illustrations show cable adapter pin outs. Additional adapters can be purchased from Digi in quantities of 8.

DB-25 Male console adapter

Digi 8-pack reorder P/N 76000672
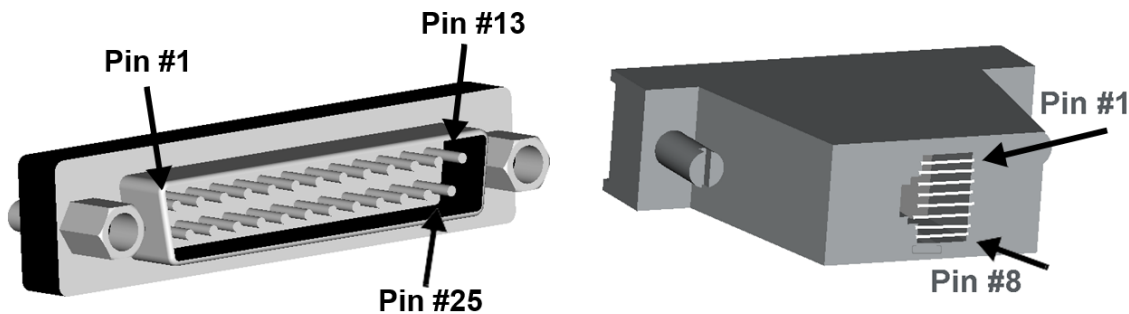
DB-25 Male to RJ-45 connector pin assignments

RJ-45	Signal		DB-25M	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTR
5	DCD			
3	RxD	Connected to	2	TxD
4	GNS	Connected to	7	GND
6	TxD	Connected to	3	RxD

RJ-45	Signal		DB-25M	Signal
7	DTR	Connected to	6	DCD
			8	DSR
8	RTS	Connected to	5	CTS

DB-9 Female console adapter

Digi 8-pack reorder P/N 76000671
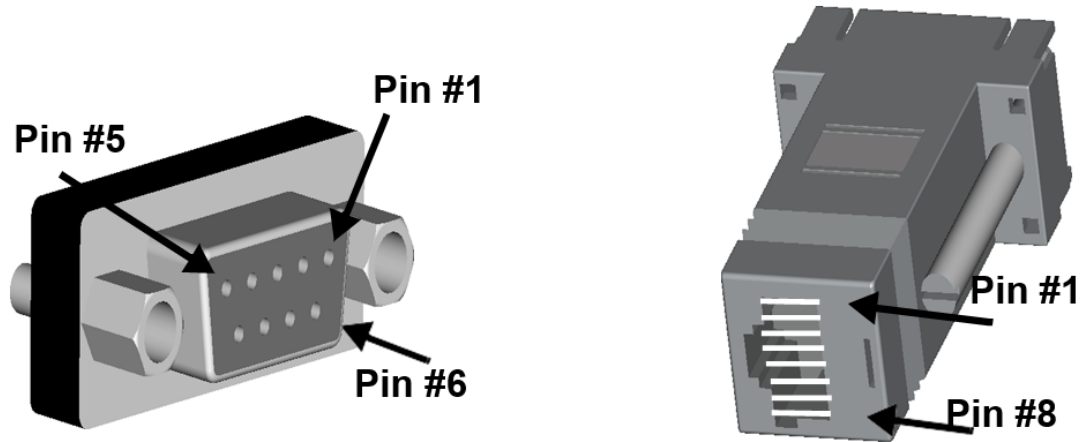
DB-9 Female to RJ-45 pin assignments

RJ-45	Signal		DB-9F	Signal
1	CTS	Connected to	7	RTS
2	DSR	Connected to	4	DTR
5	DCD			
3	RxD	Connected to	3	TxD
4	GNS	Connected to	5	GND
6	TxD	Connected to	2	RxD
7	DTR	Connected to	1	DCD
			6	DSR
8	RTS	Connected to	8	CTS

DB-25 Female console adapter

Digi 8-pack reorder P/N 76000673
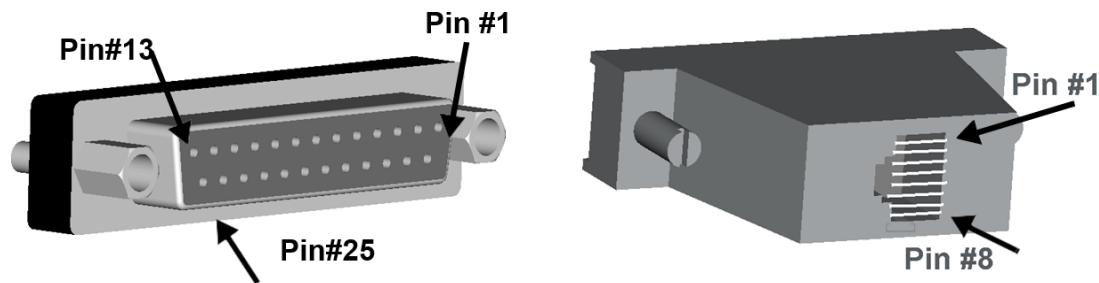
DB-25 Female to RJ-45 pin assignments

RJ-45	Signal			DB-25M	Signal
1	CTS	Connected to		4	RTS
2	DSR	Connected to		20	DTR
5	DCD				
3	RxD	Connected to		2	TxD
4	GND	Connected to		7	GND
6	TxD	Connected to		3	RxD
7	DTR	Connected to		6	DCD
				8	DSR
8	RTS	Connected to		5	CTS

DB-25 Male modem adapter

Digi 8-pack reorder P/N 76000670
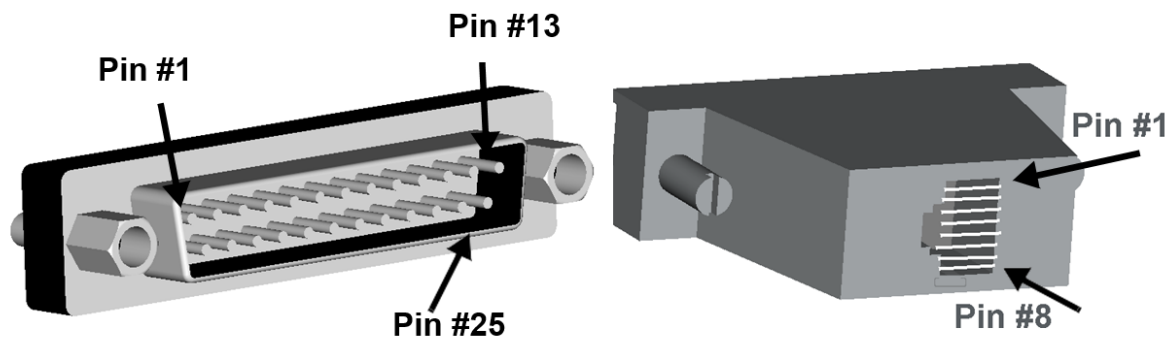
DB-25 Male modem to RJ-45 pin assignment

RJ-45	Signal		DB-25M	Signal
1	CTS	Connected to	5	CTS
2	DSR	Connected to	6	DSR
3	RxD	Connected to	3	RXD
4	GND	Connected to	7	GND
5	DCD	Connected to	8	DCD
6	TxD	Connected to	2	TxD
7	DTR	Connected to	20	DTR
8	RTS	Connected to	4	RTS

DB-9 Male modem adapter

Digi 8-pack reorder P/N 76000702

Note Available but not included
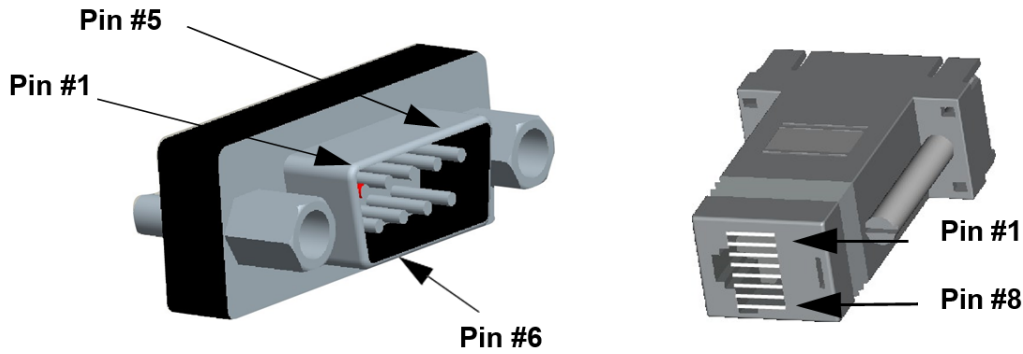
DB-9 Male Modem to RJ-45 Pin Assignment

RJ-45	Signal		DB-29M	Signal
1	CTS	Connected to	8	CTS
2	DSR	Connected to	6	DSR
3	RxD	Connected to	2	RXD
4	GND	Connected to	5	GND
5	DCD	Connected to	1	DCD
6	TxD	Connected to	3	TxD
7	DTR	Connected to	4	DTR
8	RTS	Connected to	7	RTS

Ethernet pinouts

The Digi CM unit uses a standard Ethernet connector, that is a shielded and compliant with AT&T 258 specifications.
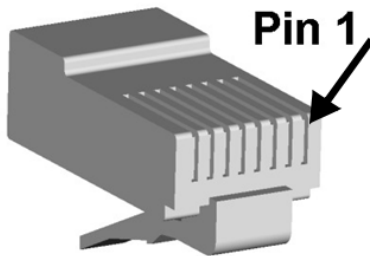
Pin	Description
1	TX+
2	TX-
3	Rx+
4	NC
5	NC
6	RX-
7	NC
8	NC

Rack mounting installation

1. Attach enclosed bracket ears to rack as shown in illustration.
2. Follow safety precautions when placing the Digi CM unit on the rack.

Note Rack shown in illustration is not included with the Digi CM unit.
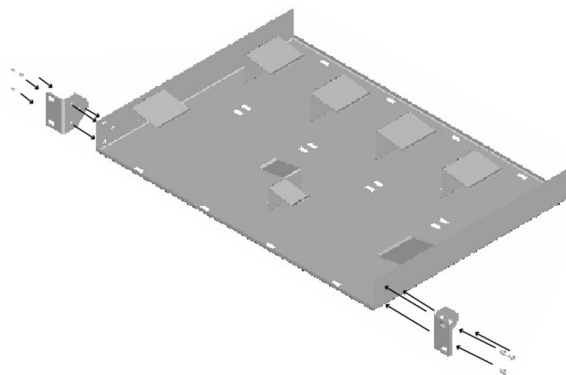
Rack mounting safety precautions

- Distribute weight evenly in the rack to avoid overloading.
- Ensure proper ventilation with at least 12 inches (30 centimeters) of clearance on all sides.
- Check equipment nameplate ratings before connecting to the supply circuit to avoid overloads that may damage over-current protection devices and supply wiring.
- Maintain reliable earthing for rack-mounting equipment, especially for supply connections.
- Install equipment in Restricted Access Areas only (dedicated equipment rooms/closets) in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
- Connect equipment to a DC supply source (reliably earthed) that is electrically isolated from the AC source.
- Directly connect the equipment chassis to the DC supply system-grounding electrode conductor or a bonding jumper from a grounding terminal bar (or bus) that is connected to the DC supply system grounding electrode conductor.
- Contain equipment that has a connection between the grounded conductor of the same DC supply circuit, the grounding conductor, and also the point of grounding of the DC system in the same immediate area. Do not ground the equipment elsewhere.
- Locate the DC supply source within the same premises as the equipment.
- Route away and secure all DC input wiring from sharp edges to prevent chaffing as well as provide strain relief.
- Provide a readily accessible disconnect device and protective device a fixed wiring for a DC power supply suitable for the specified rated voltage and current. Disconnect and protective devices to be rated 2A Amps maximum.

Certifications

Safety

- US: UL1950
- Canada: CSA 22.2 No. 60950
- Europe: EN60950 (CB Scheme Report)

This equipment is not suitable for use in locations where children are likely to be present.

Warning to service personel

⚠️ CAUTION DOUBLE POLE/NEUTRAL FUSING.

Working the Digi CM unit

⚠️ Do not attempt to service the Digi CM unit yourself, except when following the instructions from Technical Support personnel. In such a case, first perform the following actions:

- Turn off the Digi CM unit.
- Ground yourself by touching an unpainted metal surface at the back of the equipment before touching anything inside your equipment.

Replacing the battery

A coin-cell battery maintains date and time information. If you have to repeatedly reset time and date information after turning on the Digi CM unit, replace the battery.

⚠️ **CAUTION!** A new battery can explode if it is incorrectly installed. Replace the 3 Volt CR2032 battery only with the same or equivalent type recommended by the battery manufacturer. Discard used batteries according to the battery manufacturer's instructions.

Remplacer la batterie

Une pile bouton maintient les informations de date et d'heure. Si vous devez réinitialiser à plusieurs reprises les informations d'heure et de date après avoir allumé l'unité Digi CM, remplacez la batterie.

⚠ ATTENTION! Une nouvelle batterie peut exploser si elle est mal installée. Remplace le Pile 3 volts CR2032 uniquement du même type ou d'un type équivalent recommandé par le fabricant de la batterie. Jetez les batteries usagées en fonction de la batterie instruction du fabricant.

Rack mounting installation considerations

For a rack setup with forced air, the device can run 0-55° C with no extra space above or below the device (default design of the Digi CM Rack provides 1/16" = 2mm between devices).

For a rack setup with no forced air, make sure that the air in-between devices does not get warmer than 55°C by the following measures:

- Providing space between the devices, or controlling the ambient temperature on the rack.
- Distribute weight evenly in the rack to avoid overloading.
- Check equipment nameplate ratings before connecting to the supply circuit to avoid overloads that may damage over-current protection devices and supply wiring.
- Maintain reliable earthing for rack-mounting equipment, especially for supply connections.

Environmental considerations and cautions

The following is a list of environmental considerations that will ensure safe and efficient operation of the Digi CM unit:

- Do not position the Digi CM unit near high-powered radio transmitters or electrical equipment, such as electrical motors or air conditioners. Interference from electrical equipment can cause intermittent failures.
- Avoid exceeding the maximum cabling distances discussed in the online cable guide.
- Do not install the Digi CM unit in areas where condensation, water, or other liquids may be present. These may cause safety hazards and equipment failure.

For DC powered equipment:

- Install equipment in Restricted Access Areas only (dedicated equipment rooms/closets) in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
- Connect equipment to a DC supply source (reliably earthed) that is electrically isolated from the AC source.
- Directly connect the equipment chassis to the DC supply system grounding electrode conductor or a bonding jumper from a grounding terminal bar (or bus) that is connected to the DC supply system grounding electrode conductor.
- Contain equipment that has a connection between the grounded conductor of the same DC supply circuit, the grounding conductor, and also the point of grounding of the DC system in the same immediate area. Do not ground the equipment elsewhere.

- Locate the DC supply source within the same premises as the equipment.
- Route away and secure all DC input wiring from sharp edges to prevent chaffing as well as provide strain relief.
- Provide a readily accessible disconnect device and protective device a fixed wiring for a DC power supply suitable for the specified rated voltage and current. Disconnect and protective devices to be rated 2A maximum.

Note The Digi CM unit is intended to connect to networking devices. Do not attempt connecting to a telephone line.

Safety instructions

⚠️ Do not operate the Digi CM unit with the cover removed.

- To avoid shorting out the Digi CM unit when disconnecting the network cable, first unplug the cable from the equipment and then from the network jack. When reconnecting a network cable to the equipment, first plug the cable into the network jack and then into the equipment.
- To help prevent electric shock, plug the Digi CM unit into a properly grounded power source. The cable is equipped with 3-prong plug to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from the cable. If you have to use an extension cable, use a 3- wire cable with properly grounded plugs.
- To help protect the Digi CM unit from transients in electrical power, use a surge suppressor, line conditioner, or a continuous-protected (a power supply that cannot be interrupted) power supply.
- Be sure that nothing rests on the Digi CM unit cables and that the cables are not located where they can be stepped on or tripped over.
- Do not spill food or liquids on the Digi CM unit. If it gets wet, contact Technical Support.
- Do not push objects into the openings of the Digi CM unit. Doing so can cause fire or electric shock by shorting out interior components.
- Keep the Digi CM unit away from heat sources and do not block cooling vents.

Power and ground - Digi CM 48 single and dual power

This Console Management Server shall be connected to main socket outlet with a protective earthing connection.

Rated a.c. voltage	100-240 V a.c.
Rated frequency	50-60 Hz
Rated current	0.37 A

Protective earth; protective ground, IEC 60417-5019 (2006-08)	

Emissions

- US: FCC part 15, Class A
- Canada: ICES 003 Class A
- Europe: EN55022
- Japan: VCCI
- Australia: AS3548

Immunity

Europe:

- EN55024:1998
- EN61000-3-2: 2000
- EN61000-3-3: 1998

Solaris ready

All Digi CM products are Solaris Ready certified. This certification identifies these products have met the stringent testing requirements for system compatibility, inter operability, ease-of-installation, functionality, and network interpretability as defined and controlled by Sun Microsystems.

Safety warnings

English
Bulgarian--български
Croatian--Hrvatski
French--Français
Greek--Ελληνικά
Hungarian--Magyar
Italian--Italiano
Latvian--Latvietis
Lithuanian--Lietuvis
Polish--Polskie
Portuguese--Português
Slovak--Slovák
Slovenian--Esloveno
Spanish--Español

English

⚠ Risk of explosion if battery is replaced by incorrect battery type or if the battery is installed incorrectly. Dispose of used batteries according to the instructions.

⚠ Caution: Double pole/Neutral fusing.

Bulgarian--български

⚠ Риск от експлозия, ако батерията бъде заменена от неправилен тип батерия или ако батерията е инсталирана неправилно. Изхвърлете използваните батерии в съответствие с инструкциите.

⚠ Внимание: Двуполюсен / неутрален фюзинг.

Croatian--Hrvatski

⚠ Opasnost od eksplozije ako je baterija zamijenjena pogrešnim tipom baterije ili ako je baterija pogrešno instalirana. Bacite istrošene baterije prema uputama.

⚠ Oprez: Dvopolno / neutralno stapanje.

French--Français

⚠ Risque d'explosion si la batterie est remplacée par un type de batterie incorrect ou si la batterie est mal installée. Jetez les piles usagées conformément aux instructions.

⚠ Attention : Fusible bipolaire/neutre.

Greek--Ελληνικά

Κίνδυνος έκρηξης εάν η μπαταρία αντικατασταθεί από λανθασμένο τύπο μπαταρίας ή εάν η μπαταρία δεν έχει εγκατασταθεί σωστά. Απορρίψτε τις χρησιμοποιημένες μπαταρίες σύμφωνα με τις οδηγίες.

Προσοχή: Διπλός πόλος / Ουδέτερη τήξη.

Hungarian--Magyar

Robbanásveszély, ha az elemet nem megfelelő típusú elemre cserélik, vagy ha az akkumulátort helytelenül helyezik be. A használt elemeket az utasításoknak megfelelően dobja ki.

Vigyázat: kettős pólusú / semleges olvadás.

Italian--Italiano

Rischio di esplosione se la batteria viene sostituita con un tipo di batteria errato o se la batteria è installata in modo errato. Smaltire le batterie usate secondo le istruzioni.

Attenzione: fusione bipolare/neutra.

Latvian--Latvietis

Eksplozijas risks, ja akumulatoru aizstāj ar nepareizu akumulatora tipu vai nepareizi ievietots akumulators. Iznīciniet izlietotās baterijas saskaņā ar instrukcijām.

Uzmanību: dubultpola / neitrāla kausēšana.

Lithuanian--Lietuvis

⚠ Sprogimo pavojus, jei baterija pakeičiama netinkamu akumuliatoriaus tipu arba neteisingai įdėta. Panaudotas baterijas išmeskite pagal instrukcijas.

⚠ Dėmesio: dvigubas polius / neutralus lydymas.

Polish--Polskie

⚠ Ryzyko wybuchu w przypadku wymiany baterii na baterię niewłaściwego typu lub nieprawidłowego zainstalowania baterii. Zużyte baterie należy utylizować zgodnie z instrukcjami.

⚠ Uwaga: bezpiecznik dwubiegunowy/neutralny.

Portuguese--Português

⚠ Há risco de explosão se a bateria for substituída por um tipo incorreto de bateria ou se a bateria for instalada incorretamente. Descarte as baterias usadas de acordo com as instruções.

⚠ Cuidado: Fusão de pólo duplo / neutro.

Slovak--Slovák

⚠ Ak je batéria vymenená za nesprávny typ alebo je batéria vložená nesprávne, hrozí nebezpečenstvo výbuchu. Použité batérie zlikvidujte podľa pokynov.

⚠ Pozor: Dvojpólová / neutrálna poistka.

Slovenian--Esloveno

Nevarnost eksplozije, če baterijo zamenjate z nepravilno vrsto baterije ali če je baterija nepravilno nameščena. Odslužene baterije zavrzite v skladu z navodili.

Pozor: Dvopol / nevtralno varovanje.

Spanish--Español

Riesgo de explosión si la batería se reemplaza por un tipo de batería incorrecto o si la batería se instala incorrectamente. Deseche las baterías usadas de acuerdo con las instrucciones.

Precaución: Fusible bipolar / neutro.