



Digi CM and Passport

Troubleshooting Guide

Revision history—90002380

Revision	Date	Description
A	June 2016	Initial release.
B	January 2020	Updated and edited for unique password change.

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.

© 2019 Digi International Inc. All rights reserved.

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

Send comments

Documentation feedback: To provide feedback on this document, send your comments to techcomm@digi.com.

Customer 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, contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Contents

Introduction to Digi CM and Passport Troubleshooting Guide

Log in to the web interface on the device	5
---	---

Failure to Boot (Corruption)

Device fails to boot and the READY LED is not illuminated	6
Configuration data destroyed or corrupt	7

Network communication issues

No network connectivity	9
-------------------------------	---

Serial port communication issues

Cable pinouts for connecting to Cisco/Sun RJ45 console ports	13
Cable pinouts for connecting DB9 and DB25 consoles and modems	13
DB-9 female console (DTE device) adapter	13
DB-25 female console (DTE device) adapter	14
DB-9 male console (DCE device) adapter	14
DB-25 male console (DCE device) adapter	15
Kill serial port connection	15
Reset a serial port	17
Reset a Digi CM serial port	17
Reset a Digi Passport serial port	18
Serial loopback testing	19

Java Support

Chrome	22
Internet Explorer or Firefox and security errors	22

Inactivity timeouts

Web server inactivity timeout	23
Serial port inactivity timeout	23
Port Access menu inactivity timeout	24
CLI Configuration Menu inactivity timeout (Digi Passport ONLY)	25

Authentication configuration

Web server authentication	26
Port Access menu authentication	26
Direct serial port authentication	27
Command Line (CLI) authentication	28

Security scan vulnerabilities

Digi CM change and feature requests

Introduction to Digi CM and Passport Troubleshooting Guide

This guide contains troubleshooting information for common problems, and applies to the following models:

- Digi CM (all models)
- Digi Passport (all models)

Log in to the web interface on the device

You can use the web interface to configure the firmware on the device. You are required to log in to the web interface each time you access the interface.

1. Run the Device Discovery Utility or DPA utility.
2. Select the device from the device list.
3. Click **Open web interface**. A log in screen displays.
4. Enter the user name and password.
 - **User name:** The default user name is **root**.
 - **Password:** The unique, default password is printed on the device label. If a password is not printed on the label, the password is **dbps**. If neither password works, the password may have been updated. Contact your system administrator.
5. Click **Sign in**.

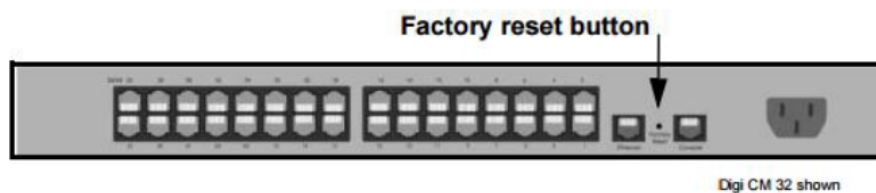
Failure to Boot (Corruption)

Device fails to boot and the READY LED is not illuminated

Reset device to factory default

The Digi CM and Passport units can be reset to factory defaults by pressing and holding the hardware factory reset button until the Ready LED on the front panel goes out.

Digi CM factory reset button:



Digi Passport factory reset button:



Follow recovery procedure

If the Digi CM or Passport units still fail to boot up, perform the recovery procedure.

1. Connect the console port on the rear panel of the Digi unit to a serial port on a workstation. Use an Ethernet cable with a DB-9 adapter (one is shipped with the product and labeled as console).

2. Set up a terminal emulation program such as HyperTerminal or PuTTY. Use the following port parameters:
 - baud = 9600
 - data bits = 8
 - parity = none
 - stop bits = 1
 - flow control = none
3. Reboot or power on the Digi unit.
4. Press the **ESC** key within three seconds of applying power to the device. The bios menu appears.

```

Press <ESC> key to enter the bios menu : 0
-----
Welcome to Bios Configuration page
-----
Select menu
1. RTC configuration
2. Hardware test
3. Firmware upgrade
4. Exit and boot from flash
5. Exit and boot from flash in emergency mode
6. Exit and reboot
<ESC> Back, <ENTER> Refresh
-----> _

```

5. Press **3: Firmware upgrade**. The **Firmware Upgrade** menu appears.
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 unit
 - **Server IP address**: The IP address of the BOOTP or TFTP server
 - **Firmware File Name**: The filename for the firmware

Note Press the **ESC** key to back up to earlier menu screens.

7. Choose **Start firmware upgrade**. The firmware upgrade will take several minutes to process.
8. When the upgrade process is complete, press **ESC** to return to the main menu.
9. Choose **Exit and boot from flash**.

If this procedure fails to recover the unit, pursue an RMA.

Configuration data destroyed or corrupt

If the configuration data is destroyed or corrupted, the Digi console server automatically restores a corrupted configuration file system to the factory default settings. However, if the Digi 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 unit to the factory default configuration settings, you will need to use a TFTP or BOOTP server to download the firmware from.

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 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 or PuTTY. Use the following port parameters:
 - baud = 9600
 - data bits = 8
 - parity = none
 - stop bits = 1
 - flow control = none
3. Reboot or power on the Digi unit.
4. Press the **ESC** key within three seconds of applying power to the device. The bios menu appears.

```
Press <ESC> key to enter the bios menu : 0
-----
Welcome to Bios Configuration page
-----
Select menu
1. RTC configuration
2. Hardware test
3. Firmware upgrade
4. Exit and boot from flash
5. Exit and boot from flash in emergency mode
6. Exit and reboot
<ESC> Back, <ENTER> Refresh
-----> _
```

5. Press **3: Firmware upgrade**. The **Firmware Upgrade** menu appears.
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 unit
 - **Server IP address**: The IP address of the BOOTP or TFTP server
 - **Firmware File Name**: The filename for the firmware

Note Press the **ESC** key to back up to earlier menu screens.

7. Choose **Start firmware upgrade**. The firmware upgrade will take several minutes to process.
8. When the upgrade process is complete, press **ESC** to return to the main menu.
9. Choose **Exit and boot from flash**.

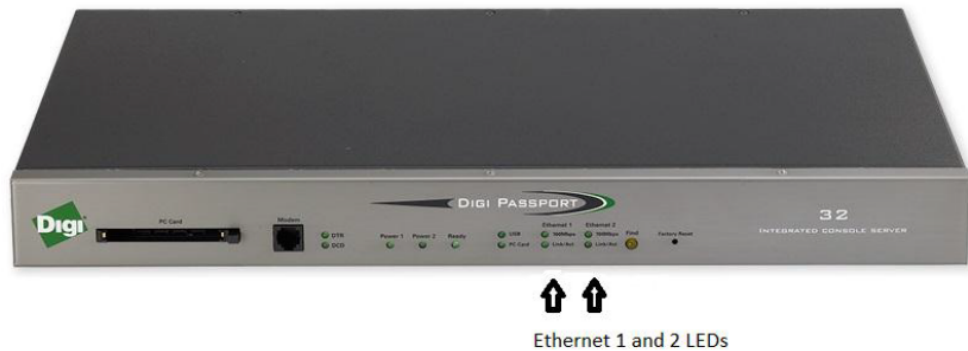
If this procedure fails to recover the unit, pursue an RMA.

Network communication issues

No network connectivity

Perform this troubleshooting process if the unit is not reachable on the network.

1. Check the LED activity for the Ethernet port. There should be a solid green for the 100Mbps LED and flashing green for the Link/Act LED.



2. Make sure you are not behind a firewall or running any third party firewall software on your PC.

3. Ping the IP address: `ping <ip address>`

Where the `<ip address>` represents the IP address assigned to the unit. If pinging the device is unsuccessful, access the unit directly from the console port to confirm the network settings.

- a. Set up a terminal emulation program, such as HyperTerminal, using the following port parameters to the console port:
 - baud = 9600
 - data bits = 8
 - parity = none
 - stop bits = 1
 - flow control = none
- b. [Log in to the web interface on the device.](#)
- c. At the prompt, type: `configmenu`
- d. In the **Configuration** menu, select menu item **1: Network configuration**.
- e. Select menu item **1: IP configuration**.
- f. Configure the network settings as appropriate for the local network.

```
-----
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
-----> 1

-----
Network configuration --> IP configuration
-----

Select menu
1. IP mode : static IP
2. IP address : 192.168.0.5
3. Subnet mask : 255.255.255.0
4. Default gateway : 192.168.0.1
5. Use Manual DNS : Enable
6. Primary DNS : 192.168.0.1
7. Secondary DNS : 8.8.8.8
8. Enable/Disable Secondary IP : Disable
<ESC> Back, <ENTER> Refresh
-----> _
```

- g. Save and apply the settings from the main menu.

```
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
----->
```

- h. If it is still not possible to ping the unit, please refer to the [factory reset procedure](#).

Serial port communication issues

Cable pinouts for connecting to Cisco/Sun RJ45 console ports	13
Cable pinouts for connecting DB9 and DB25 consoles and modems	13
Kill serial port connection	15
Reset a serial port	17
Serial loopback testing	19

Cable pinouts for connecting to Cisco/Sun RJ45 console ports

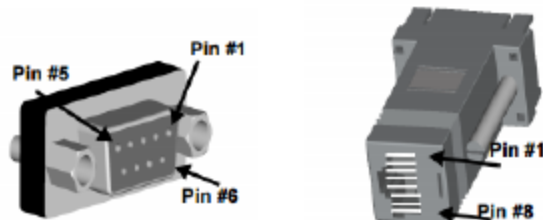
The RJ-45 8-pin configuration matches all SUN and Cisco RJ-45 console port configurations, enabling straight through CAT 5 cabling without pinout concerns.

Signal	Passport Pin	Cisco Pin	Signal
CTS	1	1	RTS
DSR	2	2	DTR
RXD	3	3	TXD
GND	4	4	GND
GND/DCD	5	5	GND
TXD	6	6	RXD
DTR	7	7	DSR
RTS	8	8	CTS

Cable pinouts for connecting DB9 and DB25 consoles and modems

The diagrams below show commonly used cabling pinouts for connecting to DB9 and DB25 style console ports and modems. Data Terminal Equipment (DTE) devices typically require cross-over or null-modem cabling pinouts where the Transmit pins are wired to Receive pins and vice versa. Common examples of DTE devices are PCs, dumb terminals and printers. Data Communication Equipment (DCE) devices use straight through cabling. Common examples of DCE devices are modems and UPS equipment.

DB-9 female console (DTE device) adapter

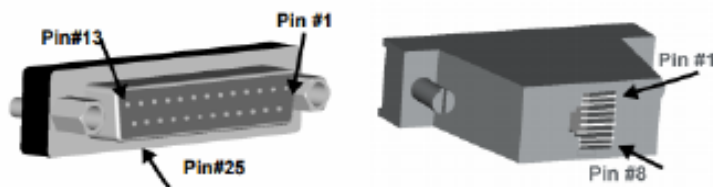


Digi 8-pack reorder PN 76000671

RJ-45	Signal	DB-9F	Signal
1	CTS	7	RTS
2	DSR	4	DTS

RJ-45	Signal	DB-9F	Signal
5	DCD	3	TxD
3	RxD	5	GND
4	GND	2	RxD
6	TxD	1	DCD
7	DTR	6	DSR
8	RTS	8	CTS

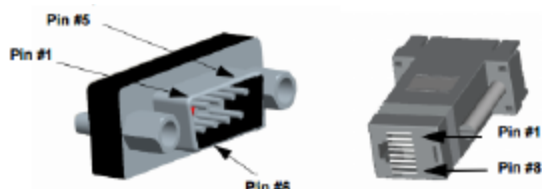
DB-25 female console (DTE device) adapter



Digi 8-pack reorder PN 76000673

RJ-45	Signal		DB-9F	Signal
1	CTS	Connected to	4	RTS
2	DSR	Connected to	20	DTS
5	DCD	Connected to	2	TxD
3	RxD	Connected to	7	GND
4	GND	Connected to	3	RxD
6	TxD	Connected to	6	DCD
7	DTR	Connected to	8	DSR
8	RTS	Connected to	5	CTS

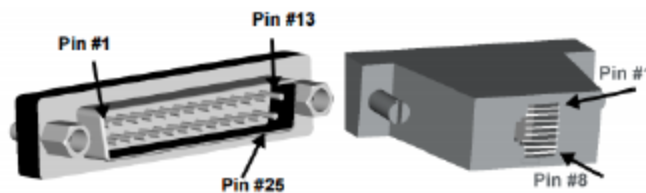
DB-9 male console (DCE device) adapter



Digi 8-pack reorder PN 76000702

RJ-45	Signal	DB-9F	Signal
1	CTS	8	CTS
2	DSR	6	DSR
3	RxD	2	RxD
4	GND	5	GND
5	DCD	1	DCD
6	TxD	3	TxD
7	DTR	4	DTR
8	RTS	7	RTS

DB-25 male console (DCE device) adapter



Digi 8-pack reorder PN 76000670

RJ-45	Signal		DB-9F	Signal
1	CTS	Connected to	5	CTS
2	DSR	Connected to	6	DSR
5	RxD	Connected to	3	RxD
3	GND	Connected to	7	GND
4	DCD	Connected to	8	DCD
6	TxD	Connected to	2	TxD
7	DTR	Connected to	20	DTR
8	RTS	Connected to	4	RTS

Kill serial port connection

In the event there is a stuck process on a port, killing the process may release the port for connection.

1. [Log in to the web interface on the device](#)
2. In the web interface, select **Serial port > Connection**.

3. Select the desired port.

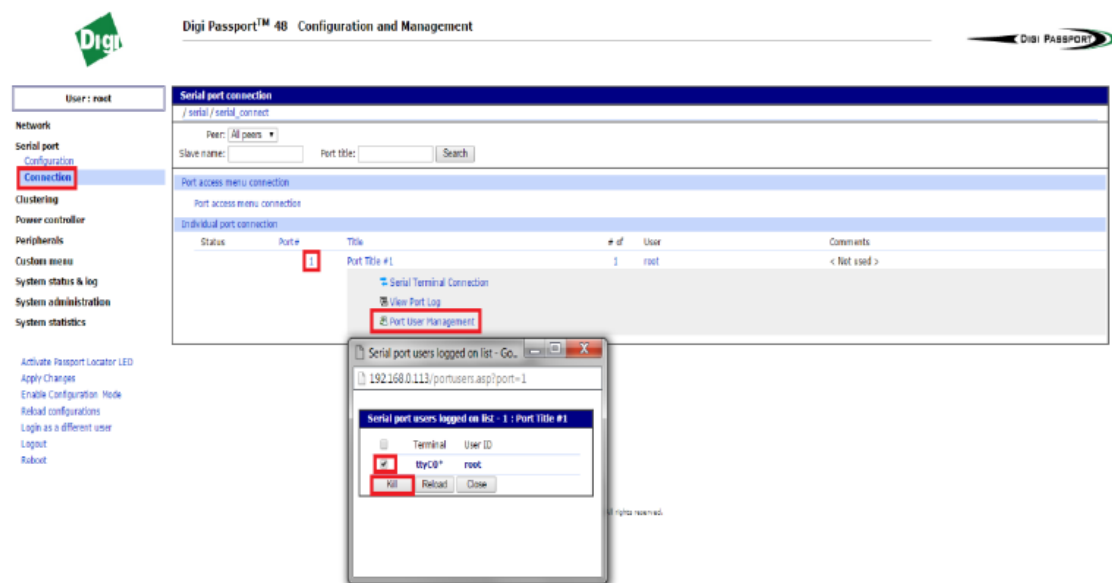
Digi Passport

- a. Click the desired port number. The **Serial port users logged on list** dialog appears.

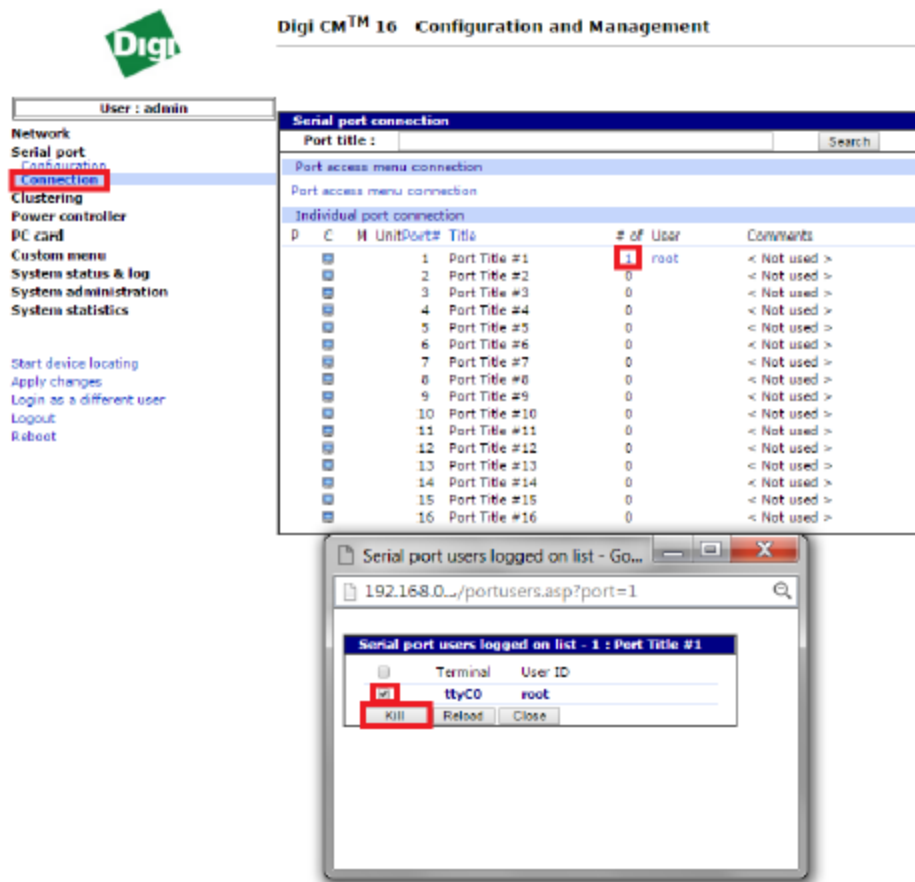
Digi CM

- a. Click the desired port number.
 - b. Click **Port User Management**. The **Serial port users logged on list** dialog appears.
4. Click the selection box in the box for the connection.
 5. Click **Kill**.

Kill connection for Digi Passport



Kill connection for Digi CM



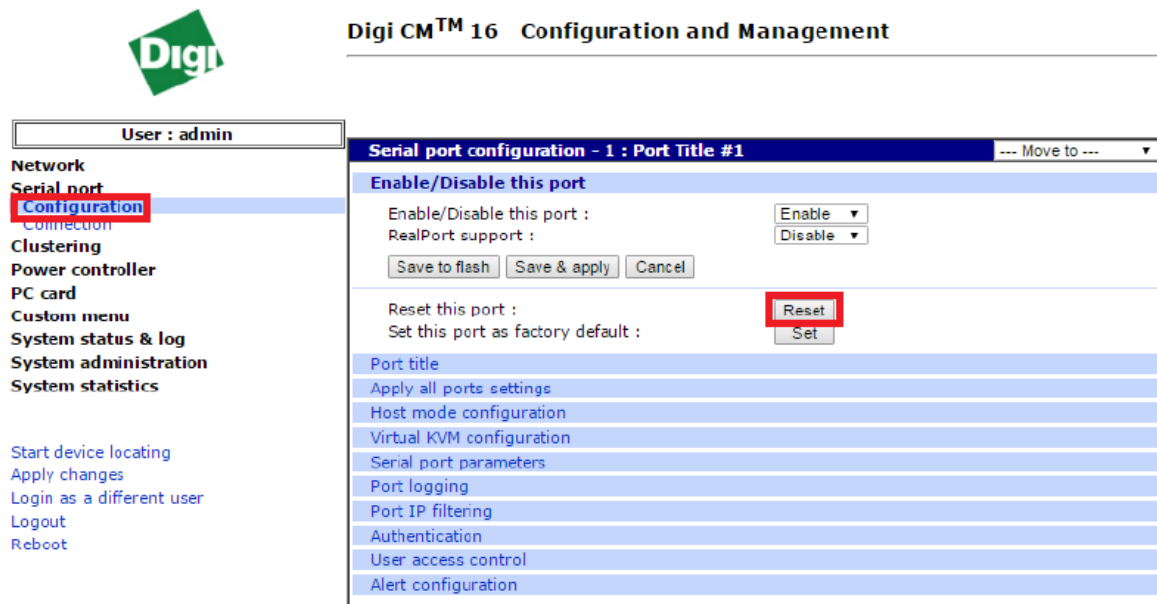
Reset a serial port

Reset a Digi CM serial port

You can reset a serial port from the web interface or the command prompt.

Web interface

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration.**
3. Select the port number.
4. Click **Reset.**



Command (root) prompt

```
# portreset <port number>
```

Where <port number> is the port number you want to reset.

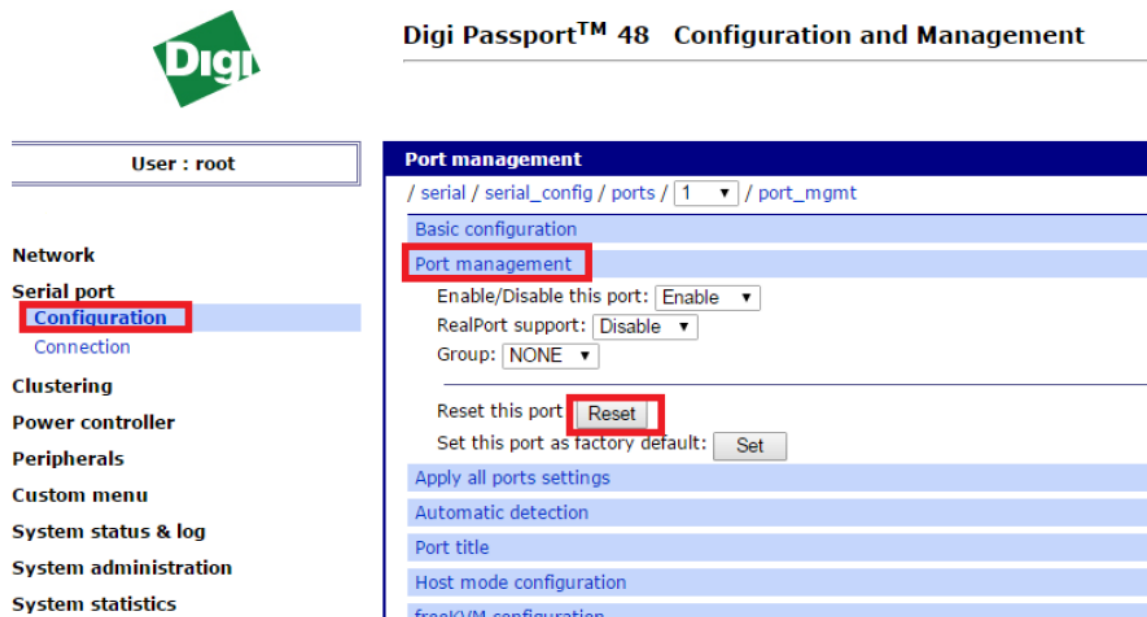
For example, if you want to reset port number 5: # portreset 5

Reset a Digi Passport serial port

You can reset a serial port from the web interface or the command prompt.

Web interface

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration**.
3. Select the port number.
4. Click **Port Management**.
5. Click **Reset**.



Command (root) prompt

```
# port reset <port number>
```

Where <port number> is the port number you want to reset.

For example, if you want to reset port number 5: # port reset 5

Serial loopback testing

If the serial cabling checks out and the above steps do not result in successful serial communication, loopback testing should be performed to check the hardware integrity.

1. Insert the loopback plug (shipped with the product) into the applicable port.

RJ-45 Loopback Plug pinout	
1 CTS	8 RTS
2 DSR and DCD	7 DTR
3 RxD	6 TxD
4 GND	4 GND

2. [Log in to the web interface on the device.](#)

3. Verify the serial port configuration for Telnet.
 - a. Click **Serial port > Configuration**.
 - b. Select the port number.
 - c. Expand **Host mode configuration** section.
 - d. Verify these settings:
 - **Host mode:** Console server
 - **Listening TCP port:** an entry should be made
 - **Protocol:** Telnet

The screenshot shows the Digi CM 48 Configuration and Management web interface. On the left, the 'Serial port Configuration' menu item is highlighted. The main panel displays the configuration for 'Serial port configuration - 1 : Port Title #1'. The 'Host mode configuration' section is expanded, showing the following settings:

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

At the bottom of the configuration section, the 'Save & apply' button is highlighted. Below this, there are links for 'Virtual KVM configuration', 'Serial port parameters', 'Port logging', 'Port event handling', 'Port IP filtering', 'Authentication', and 'User access control'.

4. From a Microsoft Windows CMD line, Unix/Linux prompt, or terminal emulator software, such as PuTTY or HyperTerminal, telnet to the IP address and the listening port number of the Digi CM unit. For example:


```
C:\> telnet 192.168.0.2 7001
```
5. You are prompted to log in.
 - **User name:** The default user name is **root**.
 - **Password:** The unique, default password is printed on the device label. If a password is not printed on the label, the password is **dbps**. If neither password works, the password may have been updated. Contact your system administrator.

6. Start typing characters on your keyboard. The characters you type should echo back and be displayed on your screen (once). If you remove the loopback plug from the port and keep typing, you should not see any data on your screen.

To disconnect from the port, issue the telnet escape sequence: `<Ctrl>]`. Enter `quit` at the telnet prompt.

7. Loopback testing failure typically points to a hardware issue with the serial port. Contact Digi Technical Support for possible product repair arrangements.

Java Support

Some pages within the web UI of the Digi CM and Digi Passport use Java, most notably, the **Serial port connection** page. The following outlines web browser compatibility and resolving Java errors.

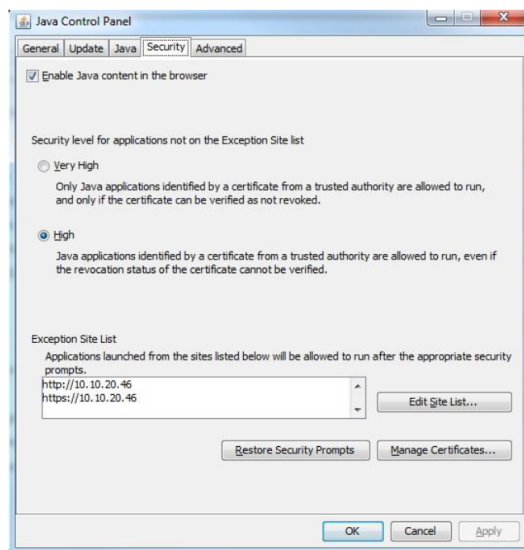
Chrome

Chrome version 45 and above no longer supports Java. If Java is required, it is suggested a different web browser is used such as Internet Explorer or Firefox.

Internet Explorer or Firefox and security errors

Due to security issues with Java you may see errors if using Internet Explorer or Firefox. This can be resolved by adding the addresses to the Java exception list. You need to add both the HTTP and HTTPS addresses.

1. Go to **Control Panel > Java > Security**.
2. Add the HTTP and HTTPS addresses to the exception list.



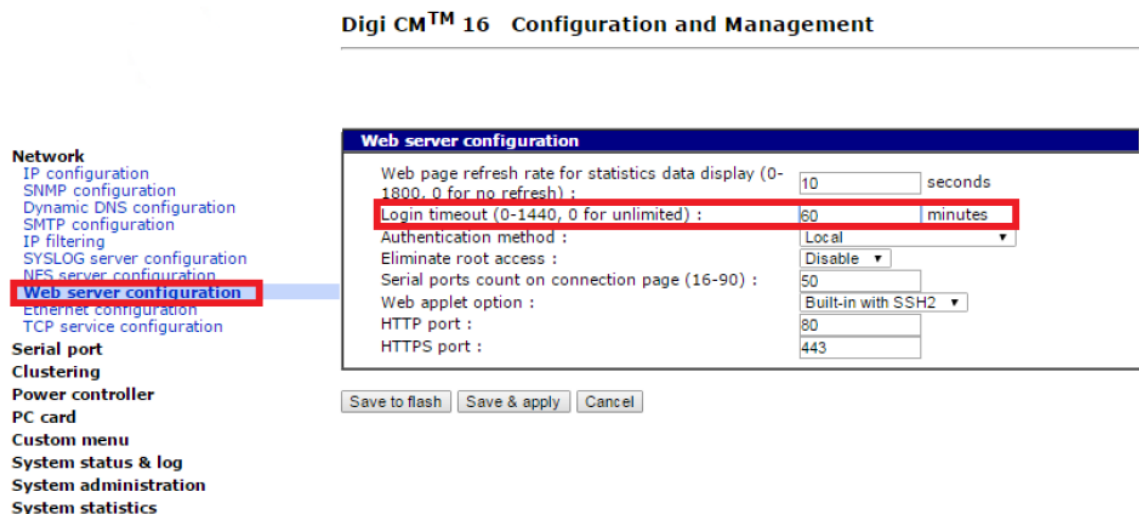
Inactivity timeouts

Configuring inactivity timeouts will timeout stale connections which can block new connection attempts. The following outlines the configuration for various inactivity timeout settings on the Digi Passport/Digi CM units.

Web server inactivity timeout

You can configure the inactivity timer for the web server.

1. [Log in to the web interface on the device.](#)
2. Select **Network > Web server configuration**. The **Web server configuration** page appears.
3. In the **Login timeout** field, configure the time for web server inactivity.



Serial port inactivity timeout

You can configure the inactivity timer for a serial port.

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration**. The **Web server configuration** page appears.
3. Select the port number.

4. Expand the **Host mode configuration** section.
5. In the **Inactivity timeout** field, configure the time limit for serial port inactivity.

User : root

Browser cannot locate Java

Network

Serial port

Configuration

Connection

Clustering

Power controller

Peripherals

Custom menu

System status & log

System administration

System statistics

Activate Passport Locator LED

Apply Changes

Enable Configuration Mode

Reload configurations

Login as a different user

Logout

Reboot

Host mode configuration

/ serial / serial_config / ports / 1 / hostmode

Basic configuration

Port management

Apply all ports settings

Automatic detection

Port title

Host mode configuration

Host mode: Console server

Type of console server: Other

Rackable System Management Card: Disable

Service processor: NONE

Enable/Disable assigned IP address: Disable

Listening TCP port (1024-65535): 7001

Protocol: Telnet

Ignore telnet negotiation at connection: Disable

Inactivity timeout (1-86400 seconds, 0 for unlimited): 100 second(s)

Display port information: Disable

Port escape sequence option: Ctrl

Port escape sequence: Ctrl- z

Port break sequence: ~break

Use comment: No

Quick connect via: Web applet

Web applet encoding: English (latin1)

Web applet size: Columns 80 Rows 24

Port Access menu inactivity timeout

You can configure the inactivity timer for the Port Access menu.

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration**. The **Port access menu configuration** page appears.
3. In the **Port access menu inactivity timeout** field, configure the time limit for Port Access menu inactivity.

Port access menu configuration

Port access menu : Enable

Port access menu port number (1024-65535) : 7000

Port access menu protocol : Telnet

Port access menu inactivity timeout (1-3600 sec, 0 for unlimited) : 100

Enable/Disable port access menu local IP : Disable

Port access menu local IP : 0.0.0.0

Port access menu quick connect via : Web applet

Port access menu web applet encoding : English (latin1)

Login on port access : Enable

Port access menu authentication method : Local

[Email alert configuration]

Enable/Disable email alert for port login : Disable

Title of email :

Recipient's email address :

[SNMP trap configuration]

Enable/Disable port login trap : Disable

Use global SNMP configuration : Disable

Trap receiver settings :

IP Address	Community	Version
0.0.0.0	public	v1
0.0.0.0	public	v1

Save to flash Save & apply Cancel

CLI Configuration Menu inactivity timeout (Digi Passport ONLY)

You can configure the inactivity timer for the command line interface configuration menu.

1. [Log in to the web interface on the device.](#)
2. Select **System administration > CLI configuration**. The **CLI configuration** page appears.
3. In the **Timeout for CLI configuration menu** field, configure the time limit for the command line interface configuration menu inactivity.

CLI configuration

/ admin / cli_conf

Authentication method: Local

Timeout for CLI configuration menu (0-1440 minutes, 0 for unlimited): 10 minutes

Use CLI authentication method for serial console access: No

Save to flash Save & apply Cancel

Authentication configuration

Web server authentication

1. [Log in to the web interface on the device.](#)
2. Select **Network > Web server configuration**. The **Web server configuration** page appears.
3. In the **Authentication method** field, select the desired option.

User : admin

Network

- IP configuration
- SNMP configuration
- Dynamic DNS configuration
- SMTP configuration
- IP filtering
- SYSLOG server configuration
- NFS server configuration
- Web server configuration**
- Ethernet configuration
- TCP service configuration

Serial port

Clustering

Power controller

PC card

Custom menu

System status & log

System administration

System statistics

Web server configuration

Web page refresh rate for statistics data display (0-1800, 0 for no refresh) : 10 seconds

Login timeout (0-1440, 0 for unlimited) : 60 minutes

Authentication method : Local

Eliminate root access : Disable

Serial ports count on connection page (16-90) : 50

Web applet option : Built-in with SSH2

HTTP port : 80

HTTPS port : 443

Save to flash Save & apply Cancel

Port Access menu authentication

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration**. The **Port access menu configuration** page appears.

3. In the **Port access menu authentication** field, select the desired option.

Port access menu configuration

Port access menu : Enable ▾

Port access menu port number (1024-65535) : 7000

Port access menu protocol : Telnet ▾

Port access menu inactivity timeout (1-3600 sec, 0 for unlimited) : 100

Enable/Disable port access menu local IP : Disable ▾

Port access menu local IP : 0.0.0.0

Port access menu quick connect via : Web applet ▾

Port access menu web applet encoding : English (latin1) ▾

Login on port access : Enable ▾

Port access menu authentication method : Local ▾

[Email alert configuration]

Enable/Disable email alert for port login : Disable ▾

Title of email :

Recipient's email address :

[SNMP trap configuration]

Enable/Disable port login trap : Disable ▾

Use global SNMP configuration : Disable ▾

Trap receiver settings :

IP Address	Community	Version
0.0.0.0	public	v1 ▾
0.0.0.0	public	v1 ▾

Save to flash Save & apply Cancel

Direct serial port authentication

1. [Log in to the web interface on the device.](#)
2. Select **Serial port > Configuration**. The **Web server configuration** page appears.
3. Select the port number.
4. Expand the **Authentication** section.

5. In the **Authentication method** field, select the desired option.

The screenshot shows a web interface with a sidebar on the left and a main content area on the right. The sidebar has a 'User : root' box at the top, followed by a red error message 'Browser cannot locate Java'. Below this is a list of menu items: Network, Serial port, Configuration (highlighted with a red box), Connection, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. At the bottom of the sidebar are links: Activate Passport Locator LED, Apply Changes, Enable Configuration Mode, and Reload configurations. The main content area has a blue header 'Authentication' with a breadcrumb path '/ serial / serial_config / ports / 1 / auth'. Below the header is a list of configuration options: Basic configuration, Port management, Apply all ports settings, Automatic detection, Port title, Host mode configuration, freeKVM configuration, Serial port parameters, Port logging, Authentication (highlighted with a red box), User access control, Alert configuration, and Copy port configuration. The 'Authentication' section has a dropdown menu for 'Authentication method' set to 'Local'. At the bottom of the main content area are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'.

Command Line (CLI) authentication

1. Log in to the web interface on the device.
2. Select **System administration > CLI configuration**. The **CLI configuration** page appears.
3. In the **Authentication method** field, select the desired option.

The screenshot shows a web interface with a sidebar on the left and a main content area on the right. The sidebar has a 'User : root' box at the top. Below this is a list of menu items: Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. Under 'System administration' are sub-items: User administration, Access lists, Change password, Device name, Date and time, Configuration management, Security profile, and Firmware upgrade. The 'CLI configuration' item is highlighted with a red box. The main content area has a blue header 'CLI configuration' with a breadcrumb path '/ admin / cli_conf'. Below the header is a dropdown menu for 'Authentication method' set to 'Local' (highlighted with a red box). Below this is a text field for 'Timeout for CLI configuration menu (0-1440 minutes, 0 for unlimited):' with the value '10' and a unit 'minutes'. Below that is a text field for 'Use CLI authentication method for serial console access:' with the value 'No'. At the bottom of the main content area are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'.

Security scan vulnerabilities

Please report any security scan vulnerabilities to [Digi Technical Support](#). It is recommended that the CVE number and the scanning software used are provided to Digi.

Digi CM change and feature requests

Due to limited space being available on the Digi CM, no new enhancements are planned. There is however, a Digi CM Utility pack, which contains cron, fuser, netstat, Kerberos, pppd, clustering utilities and all network PC Card drivers which can obtained here: [Digi CM Utility pack](#).