Digi CM and Passport Troubleshooting Guide

<table>
<thead>
<tr>
<th>Figures</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2-1: Digi CM Factory Reset Button</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2-2: Digi Passport Factory Reset Button</td>
<td>5</td>
</tr>
<tr>
<td>Figure 3-1: Digi Passport Ethernet LED</td>
<td>8</td>
</tr>
<tr>
<td>Figure 3-2: Digi CM IP Configuration Menu</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3-3: Digi CM Save and Apply Changes</td>
<td>9</td>
</tr>
<tr>
<td>Figure 4-1: Cisco/Sun RJ45 Console Cable</td>
<td>10</td>
</tr>
<tr>
<td>Figure 4-2: DB-9 Female Console (DTE device) Adapter</td>
<td>11</td>
</tr>
<tr>
<td>Figure 4-3: DB-25 Female Console (DTE device) Adapter</td>
<td>11</td>
</tr>
<tr>
<td>Figure 4-4: DB-9 Male Modem (DCE device) Adapter</td>
<td>12</td>
</tr>
<tr>
<td>Figure 4-5: DB-25 Male Modem (DCE device) Adapter</td>
<td>12</td>
</tr>
<tr>
<td>Figure 4-6: Digi Passport Kill Serial Connection</td>
<td>13</td>
</tr>
<tr>
<td>Figure 4-7: Digi CM Kill Serial Connection</td>
<td>13</td>
</tr>
<tr>
<td>Figure 4-8: Digi CM Reset Serial Port</td>
<td>14</td>
</tr>
<tr>
<td>Figure 4-9: Digi Passport Reset Serial Port</td>
<td>14</td>
</tr>
<tr>
<td>Figure 4-10: RJ45 Loopback Plug Pinout</td>
<td>15</td>
</tr>
<tr>
<td>Figure 4-11: Console Server Configuration</td>
<td>15</td>
</tr>
<tr>
<td>Figure 4-12: Telnet Session Screen</td>
<td>16</td>
</tr>
<tr>
<td>Figure 5-1: Java Control Panel</td>
<td>17</td>
</tr>
<tr>
<td>Figure 6-1: Digi CM Web Server Inactivity Timeout</td>
<td>18</td>
</tr>
<tr>
<td>Figure 6-2: Digi Passport Serial Inactivity Timeout</td>
<td>18</td>
</tr>
<tr>
<td>Figure 6-3: Digi CM Port Access Menu Inactivity Timeout</td>
<td>19</td>
</tr>
<tr>
<td>Figure 6-4: Digi Passport CLI Configuration Menu Inactivity Timeout</td>
<td>19</td>
</tr>
<tr>
<td>Figure 7-1: Digi CM Web Server Authentication</td>
<td>20</td>
</tr>
<tr>
<td>Figure 7-2: Digi CM Port Access Menu Authentication</td>
<td>20</td>
</tr>
<tr>
<td>Figure 7-3: Digi Passport Serial Authentication</td>
<td>21</td>
</tr>
<tr>
<td>Figure 7-4: Digi Passport CLI Authentication</td>
<td>21</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 Digi CM and Passport Troubleshooting Guide
This guide is designed to assist in troubleshooting common problems/questions with Digi CM and Passport products.

This application note applies to the following models:
Model: Digi CM (all models) & Digi Passport (all models)

1.2 Corrections
Requests for corrections or amendments to this guide are welcome and should be addressed to Digi Technical Support.

1.3 Version

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

2 FAILURE TO BOOT/CORRUPTION

2.1 Device Fails to Boot/Ready LED not Illuminated
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. The arrow points to the reset button’s location in the figures below:

Figure 2-1: Digi CM Factory Reset Button
If the Digi CM or Passport units still fail to boot up, the following recovery procedure should be followed:

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.

5. Choose Firmware upgrade by entering 3. This will bring up the Firmware Upgrade menu.

6. Enter the information for the first menu items:
Digi CM and Passport Troubleshooting Guide

- 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: 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.

8. When the upgrade process is complete, choose ESC to return to the main menu.

9. Choose Exit and boot from flash.

If this procedure fails to recover the unit, an RMA should be pursued.

2.2 Configuration Destroyed or Corrupt

In the event 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.
5. Choose Firmware upgrade by entering 3. This will bring up the Firmware Upgrade menu.

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: 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.

8. When the upgrade process is complete, choose ESC to return to the main menu.

9. Choose Exit and boot from flash.

If this procedure fails to recover the unit, an RMA should be pursued.

### 3 NETWORK COMMUNICATION ISSUES

#### 3.1 No Network Connectivity

The following troubleshooting steps should be performed when 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 192.168.1.100
```

The IP address of 192.168.1.100 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) Login as root (default password: dbps) and type `configmenu` at the prompt.

c) Select menu item 1 for Network configuration and item number 1 again for IP configuration. Configure the network settings as appropriate for the local network:
Digi CM and Passport Troubleshooting Guide

Figure 3-2: Digi CM IP Configuration Menu


Figure 3-3: Digi CM Save and Apply Changes

d) Save and apply the settings from the main menu:

e) If it is still not possible to ping the unit, please refer to the factory reset procedure from section 1 (pages 4 and 5).
This section outlines steps to take if there is a lack of communication on one or more serial ports by first confirming the proper cabling is in place and then testing the serial hardware integrity with a loopback test.

4.1 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:

<table>
<thead>
<tr>
<th>Signal</th>
<th>Passport Pin</th>
<th>Cisco Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTS</td>
<td>1</td>
<td>1</td>
<td>RTS</td>
</tr>
<tr>
<td>DSR</td>
<td>2</td>
<td>2</td>
<td>DTR</td>
</tr>
<tr>
<td>RXD</td>
<td>3</td>
<td>3</td>
<td>TXD</td>
</tr>
<tr>
<td>GND</td>
<td>4</td>
<td>4</td>
<td>GND</td>
</tr>
<tr>
<td>GND/DCD</td>
<td>5</td>
<td>5</td>
<td>GND</td>
</tr>
<tr>
<td>TXD</td>
<td>6</td>
<td>6</td>
<td>RXD</td>
</tr>
<tr>
<td>DTR</td>
<td>7</td>
<td>7</td>
<td>DSR</td>
</tr>
<tr>
<td>RTS</td>
<td>8</td>
<td>8</td>
<td>CTS</td>
</tr>
</tbody>
</table>

Figure 4-1: Cisco/Sun RJ45 Console Cable

4.2 Cable Pinouts for Connecting DB9 and DB25 Consoles and Modems

The following diagrams 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.
Figure 4-2: DB-9 Female Console (DTE device) Adapter

![DB-9 Female Console Adapter](image)

<table>
<thead>
<tr>
<th>RJ-45</th>
<th>DB-9F Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CTS Connected to 7 RTS</td>
</tr>
<tr>
<td>2</td>
<td>DSR Connected to 4 DTR</td>
</tr>
<tr>
<td>3</td>
<td>RxD Connected to 3 TxD</td>
</tr>
<tr>
<td>4</td>
<td>GND Connected to 5 GND</td>
</tr>
<tr>
<td>5</td>
<td>DCD Connected to 2 RXD</td>
</tr>
<tr>
<td>6</td>
<td>DTR Connected to 1 DCD</td>
</tr>
<tr>
<td>7</td>
<td>RTS Connected to 8 CTS</td>
</tr>
</tbody>
</table>

Figure 4-3: DB-25 Female Console (DTE device) Adapter

![DB-25 Female Console Adapter](image)

<table>
<thead>
<tr>
<th>RJ-45</th>
<th>DB-25M Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CTS Connected to 4 RTS</td>
</tr>
<tr>
<td>2</td>
<td>DSR Connected to 20 DTR</td>
</tr>
<tr>
<td>3</td>
<td>RxD Connected to 2 TxD</td>
</tr>
<tr>
<td>4</td>
<td>GND Connected to 7 GND</td>
</tr>
<tr>
<td>5</td>
<td>DCD Connected to 3 RXD</td>
</tr>
<tr>
<td>6</td>
<td>DTR Connected to 6 DCD</td>
</tr>
<tr>
<td>7</td>
<td>RTS Connected to 5 CTS</td>
</tr>
</tbody>
</table>

Page | 11
4.3 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. Navigate to the device web interface, and login as root.

2. Go to the **Serial port > Connection** menu and click on the desired port number (for the Digi Passport, you will click on the **Port user management** option).

3. Place a check mark in the box preceding the connection and click **Kill**.

Digi Passport web interface example:
Figure 4-6: Digi Passport Kill Serial Connection

Digi CM web interface example:

Figure 4-7: Digi CM Kill Serial Connection

4.4 Reset Serial Port

1. Digi CM Port Reset

To reset a port from the web interface of the Digi CM, select **Serial port > Configuration >** (port#) > **Reset:**
To reset port 5 from the command (root) prompt of the Digi CM:

```
# portreset 5
```

2. Digi Passport Port Reset

To reset a port from the web interface of the Digi CM, select **Serial port > Configuration > (port#) > Port management > Reset**.

To reset port number 5 from the command (root) prompt of the Digi Passport:

```
# portset reset 5
```
4.5 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.

![RJ45 Loopback Plug Pinout](image)

**Figure 4-10: RJ45 Loopback Plug Pinout**

2. Navigate to the Digi CM device from your web browser by typing in the IP address of the unit (depending on your security settings, you may be required to precede this with https:// rather than http://), login as root (default password: dbps).

3. Under the Serial port configuration, ensure the Host Mode is set to Console Server, there is a Listening Port entered and the protocol is set to Telnet. For example:

![Console Server Configuration](image)

**Figure 4-11: Console Server Configuration**
Digi CM and Passport Troubleshooting Guide

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. When prompted, login as root (default password: dbps). For example:

   Figure 4-12: Telnet Session Screen

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 the word "quit" at the telnet prompt.

7. Loopback testing failure typically points to a hardware issue with the serial port. Digi Technical Support should be contacted for possible product repair arrangements
5 JAVA SUPPORT

5.1 Java Support with Web Browsers

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.

- 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. To do so:

1. Go to Control Panel – Java – Security
2. Add the HTTP and HTTPS addresses to the exception list. As shown below:

![Java Control Panel](image)

Figure 5-1: Java Control Panel
6 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.

6.1 Web Server Inactivity Timeout

The web server inactivity timer can be configured from the web interface under Network > Web server configuration:

![Digi CM Web Server Inactivity Timeout](image1)

Figure 6-1: Digi CM Web Server Inactivity Timeout

6.2 Serial Port Inactivity Timeout

The serial port inactivity timeout timer can be configured from the web interface under Serial port > Configuration > (port#) > Host mode configuration > Inactivity timeout:

![Digi Passport Serial Inactivity Timeout](image2)

Figure 6-2: Digi Passport Serial Inactivity Timeout
Digi CM and Passport Troubleshooting Guide

6.3 Port Access Menu Inactivity Timeout

The port access menu inactivity timeout setting can be applied from the web interface under Serial port > Configuration > Port Access menu configuration > Port access menu inactivity timeout:

![Figure 6-3: Digi CM Port Access Menu Inactivity Timeout](image)

6.4 CLI Configuration Menu Inactivity Timeout (Digi Passport only)

The command line interface configuration menu inactivity timeout setting can be configured from the web interface under System administration > CLI configuration > Timeout for CLI configuration menu:

![Figure 6-4: Digi Passport CLI Configuration Menu Inactivity Timeout](image)
7 AUTHENTICATION CONFIGURATION

7.1 Web Server Authentication

The web server authentication configuration can be applied from the web interface under Network > Web server configuration > Authentication method:

![Figure 7-1: Digi CM Web Server Authentication](image)

7.2 Port Access Menu Authentication

Authentication for the port access menu can be configured from the web interface under Serial ports > Port access menu configuration > Port access menu authentication method:

![Figure 7-2: Digi CM Port Access Menu Authentication](image)
7.3 Direct Serial Port Authentication

Serial port authentication can be configured from the web interface under **Serial port > (port#) > Authentication**:

![Figure 7-3: Digi Passport Serial Authentication](image)

7.4 Command Line (CLI) Authentication

The CLI authentication can be configured from the web interface under **Administration > CLI configuration**:

![Figure 7-4: Digi Passport CLI Authentication](image)
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.

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