



Digi Passport

© Digi International Inc. 2006. All rights reserved.

Digi, Digi International, the Digi logo, Digi Passport, the Making Device Networking Easy logo, Digi One, and RealPort are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective owners.

This product contains software licensed under the GNU Public License version 2 and other open source licenses.

(<http://www.gnu.org/copyleft/gpl.html>)

An SDK for all open-source code used in this product is available free of charge from Digi International (send email to supportwizards@digicom.com) for more information.

Microsoft Windows Server 2003 is a trademark of Microsoft Corporation.

Chapter 1 Introduction

Digi Passport™ Model Support	13
Feature Overview	13
Feature Summary.....	13
User Groups	15
Root and Admin Usernames and Passwords.....	16
Adding Port Administrators and Users	16
Ways to Configure the Digi Passport	16
Web Interface	16
Configuration Menu	17
Command Line Interface	18
Ways of Accessing the Digi Passport Ports: Overview	18
Web Interface Access Menu	18
Port Access Menu.....	20
Direct Port Access.....	20
Custom Menus	21
Port Escape Menu.....	21
Description of Fields	21
SNMP	22
Saving and Applying Changes	22
One Step: Save and Apply Changes	22
Two-Step: Save to Flash and then Apply Changes	22
Automatic Device Discovery Protocol ADDP	22
Automatic Device Recognition	23
Locator Light.....	23

Chapter 2 Getting Started

Introduction.....	25
Assigning IP Settings from the Console Port	25
Configuring for SSH	26
Options	26
Configuring the Port Access Menu for SSH	26
Configuring a Port for SSH	27
Windows Configuration for PPP	28
Windows XP	28
PPP configuration using a Linux client.	28
Passport	28
Redhat 9 machine	29
Adding, Editing, and Removing Users.....	30
Procedure	30
About Shell Options	31

Chapter 3 Installing and Configuring PC Cards

Introduction.....	33
Compatible PC Cards.....	33
Adding a Compact-flash Card	33
Adding a Network Card	34
Adding a Wireless LAN Card.....	35
Adding a Serial Modem	36

Chapter 4 User Interface

Digi Passport User interface.....	39
Administering Users	40
Required Privileges	40
Procedure	40
To Add an Access List to the Digi Passport Unit	42

Chapter 5 System Status and Port Logging

Introduction.....	45
System Status & Log.....	45
System Information	45
IP Information	46
Enabling Log Storage Location	46
Enable NFS Server	46
Alert for NFS Server Disconnect	47
Enable Server	47
Enable a Compact-flash Card	49
Enable the Passport Unit's Memory	49
Configuring System Logging	50
Viewing System Logs	51
Configure Port Logging	51
Viewing Port Logs	52

Chapter 6 Configuring Ports

Introduction.....	55
Enabling and Disabling the Ports	55
RealPort Support.....	55
Resetting Ports.....	57
Reset Individual Port Settings	57
Port Title	57
Configuring Automatic Device Recognition	57
Apply all Ports Settings	59
Host Mode Configuration.....	59
Console Server Mode	60
Terminal Server Mode	60
Dial-In Modem Mode	61
Dial-In Terminal Server	61
Configuring Host Mode.....	62
Supported Protocols.....	63
Serial Port Parameters	64
DTR Behavior	64
Inter-character Timeout	64

Specialty Use of Port -When Data is Processed in Chunks	65
Remote Ports	66
Configure Remote Ports	66
Accessing a remote port	66
Chapter 7 Alerts and Notifications	
Introduction.....	69
Configuring SMTP Alerts.....	70
SNMP Information	70
Traps	71
Configuring SNMP v1 or v2.....	71
Managing the SNMP Protocol	72
Configuring Port Event Handling	76
Config Alerts for Automatic Device Recognition (ADR).....	78
Chapter 8 Intelligent Platform Management Interface	
Introduction.....	81
Procedure	81
Chapter 9 User, Security, and Authentication Configuration and Administration	
Introduction.....	89
Configuring User Access Control	89
Configure User Access Privileges	91
Restrict a User's Privileges	91
Change the Privileges of an Access List	92
Sniff Session	93
Security Profile	95
System Security	95
Password Security	96
Authentication.....	96
Configuring Authentication Methods for Port Access.....	97
Configuring Authentication for the Web Server	98
LDAP Authentication	98
Custom PAM Module	99
Samba configuration>	99
Samba server	99
Passport	99
Chapter 10 Custom and Default Menus	
Introduction.....	101
Making Custom Menus.....	101
Adding Users	101
Creating Menu Names	102
Adding Menu Items	103
Assigning Users to a Menu	104

Default Menu	104
Port Access Menu	104
Chapter 11 Microsoft SAC Support	
About the Digi Passport Unit's Support for Microsoft Windows Server 2003	107
Setup Overview	108
Setting Up the Windows Server 2003 Port.....	108
Command Syntax	108
Command Example	108
Setting Up the Digi Passport Unit for SAC Support.....	108
Accessing the Windows Server 2003 Console Port from the Digi Passport Unit's GUI	109
Chapter 12 Configuring FreeKVM	
Introduction.....	113
An Example Configuration	113
Free Protocols	113
Using FreeKVM with Remote Desktop Protocol.....	114
Configuring	114
Connecting to a system through FreeKVM using Remote Desktop Protocol	116
Using FreeKVM with VNC Protocol.....	116
Configuring	117
Connecting to a system through FreeKVM using VNC	118
Using FreeKVM with X Window System Protocol and XManager Software	119
Configuring	119
Connecting to a system through FreeKVM using Xmanager	121
Web Redirection.....	122
Installing Programs for FreeKVM	122
Remote Desktop Protocol	122
VNC Viewer	123
Xmanager	123
Chapter 13 Rackable® Systems Management Card	
Introduction.....	125
Set up	125
Setup of the Digi Passport Unit to Support the Rackable Systems Management	
Card	125
Configure Serial Port Communication Settings:	125
Assign a Port Name:	126
Accessing the Rackable Systems Management Card from the Digi Passport Unit's	
User Interface	126
Chapter 14 Configuring Remote Dial-In Access	
Introduction.....	129
Configuring for Dial-In Modem Access.....	129
Adding a PC Modem	132
Configuring for Dial-In Terminal Server Access	132
Chapter 15 Power Controller	
Introduction.....	135

Installing Power Controller	136
Configuring Power Controller	136
Configure the Serial Port Parameters to Match the Power Controller	136
Add the Power Controller	137
Serial Port info.....	137
Setting Alarms and Thresholds	138
Outlet Configuration	139
User Access for Power Controller	140
Configuring to Allow Specific Users Access	140
Configuring to Restrict Specific Users	141
Power Controller Management.....	142
Cascading Multiple Digi RPM Units.....	144

Chapter 16 Port Clustering

Introduction.....	147
Configuring Port Clustering	148
Assigning Master Clustering Mode	148
Configure Slaves to Join a Cluster	148
Advanced Clustering Configuration	149
Peer to Peer Clustering	152
Accessing the Cluster Ports	152
Clustering Peer-to-peer	152
Making up a peer_to_peer group	154
Peer to peer mode configuration	154
Peer to peer information	154
Join	155
Invite peers	157
Withdraw	159
Remove	159
Update	159
Connecting to peers	159
Link to web interface	159
Link to port access menu	159
Serial port connection page	160
Connect to a port via connect.asp	160
Connect to a port via ssh	161
Custom menu	161

Chapter 17 System Administration

Introduction.....	163
Upgrading the Firmware.....	163
Web Interface	163
Configuration Management.....	164
Automatically Saving the Configuration	164
Automatically Upgrading the Digi Passport Unit's Firmware or Configuration using TFTP	165
DHCP	166

Directly Configure the TFTP Server and the Name of the “hash” File	166
The Structure of the Hash File	166
Resetting Factory Defaults	168
Setting Date and Time.....	169
Configuring a Host Name	170

Chapter 18 Command Line Interface

Introduction.....	171
Linux Commands	171
Important File Locations	172
Default Script	172
Booting Sequence	172
Config Files	173
User Storage Space	175
Example Scripts	175
User Administration.....	177
Locator LED Script	178

Chapter 19 Configuration Menu

Introduction to the Configuration Menu	179
Accessing the Configuration Menu.....	179
Configuring SSH.....	180
Adding, Editing, and Removing Users.....	181
Adding and Configuring a PC Card	181
Host Mode Configuration.....	181
Port Parameters	182
Port Access Menu	182
System Logging.....	183
Configure the System Log Device	183
Procedure for an NFS or SYSLOG Server	184
Configure System Logging	184
Configuring SNMP.....	185
Configuring SMTP	185
Configuring Network IP Filtering.....	185
Network IP Filtering.....	189
Port IP Filtering.....	189
Sniff Sessions.....	190
Viewing A Sniff Session	191
Field Descriptions for Sniff Sessions	192
Authentication.....	193
Upload Server Certificate	194
OpenSSL (SSLeay) Simple CA Usage - Install Openssl	194
Make Root CA (Certificate Authority for Self-signed)	195
Making a Certificate Request	196
Signing a Certificate Request	197
Make Certificate for the Digi Passport Unit	198
Dial-in Modem Access.....	198
Dial-in Terminal Server Access	199
Clustering	200
Firmware Upgrade.....	201

Restoring Factory Defaults.....	202
Setting Date and Time.....	202
Accessing the Boot Loader Program.....	202
Hardware Test Menu	203
Disaster Recovery	203

Chapter 20 Hardware Information

Introduction.....	205
Hardware Specifications.....	205
Digi Passport 48	205
Digi Passport 16 and Digi Passport 32	206
Digi Passport 8 AC Powered	206
LED Indicators.....	207
About Serial Port Cabling	207
Serial Port Pinouts.....	207
Cable Adapters.....	208
DB-25 Male Console Adapter	208
DB-9 Female Console Adapter	209
DB-25 Female Console Adapter	210
DB-25 Female to RJ-45 Pin Assignments	210
DB-25 Male Modem Adapter (Digi 8-pack reorder P/N 76000670)	211
DB-25 Male Modem to RJ-45 Pin Assignment	211
DB-9 Male Modem Adapter (Digi 8-pack reorder P/N 76000702)	212
DB-9 Male Modem to RJ-45 Pin Assignment	212
Ethernet Pinouts.....	212
Rack Mounting Installation	213
Rack Mounting Safety Precautions	213

Chapter 21 Certifications

Safety	215
Working Inside the Digi Passport Unit	215
Replacing the Battery	215
Rack Mounting Installation Considerations	215
Environmental Considerations and Cautions	216
Safety Instructions	216
Emissions.....	217
Immunity.....	217
Solaris Ready.....	217

Digi Passport™ Model Support

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

Feature Overview

With the Digi Passport unit, 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 Digi Passport 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 Digi Passport unit offers a PC-Card slot for adding dialup modems, Ethernet, or wireless network cards. USB or PC-Card Flash devices can be used to save port logs and back up configurations.

The Digi Passport unit is available in 4-, 8-, 16-, 32- and 48-port models, in a 1U rack-mount form factor.

Feature Summary

Category	Feature
Security	<ul style="list-style-type: none"> • SSH v2 server and client • TLS/SSL • IP Filtering • Central access to security parameters via the Security Profile including network, port, and password securities.
Authentication	<ul style="list-style-type: none"> • TACACS+ • RADIUS • LDAP and Active Directory • Kerberos support for customized PAM Modules • User access per port • Local user database

Feature Summary

Category	Feature
Management	<ul style="list-style-type: none"> • Command line • WEB --HTTP/HTTPS • SNMPv3 • IPMI 2.0 • Custom applications • Port Triggers and Alerts • Multi level menus • Advanced Device Discovery Protocol (ADDP) for locating the device on the network • RemotePorts™ extends console management features to remote devices • Integrated power management and control in conjunction with Digi RPM power strips • Automatic Device Recognition • Perl programming and scripting • IP v4/v6 dual stack
Data Capture	<ul style="list-style-type: none"> • Local port logging • External logging (syslog, NFS, PC card, USB Flash)
Port Access	<ul style="list-style-type: none"> • Telnet/SSH • Direct SSH and Telnet to individual ports • HTTP/HTTPS • Multiple concurrent users per port • Independent IP addresses per port • Raw TCP • Port escape menu • USB Export option
freeKVM™ access	<ul style="list-style-type: none"> • Windows Remote Desktop • VNC • Xmanager (X Window System) • Web Redirection • Radmin • User defined
Expandable Capabilities	<p>CompactFlash/PC Card:</p> <ul style="list-style-type: none"> • Flash memory card • Wireless LAN adapter (802.11b) • Ethernet LAN adapter • PSTN/CDMA modem card <p>USB:</p> <ul style="list-style-type: none"> • Expandable storage to USB flash

Category	Feature
Other Features	<ul style="list-style-type: none"> • RealPort® and Encrypted RealPort support • Solaris Ready • Multiple concurrent users per port • RemotePorts™ • Access lists per port • Flash upgradeable • SSH sessions simultaneously on all ports • Secure Clustering - Single IP for multiple Digi Passport devices • Individual IP addresses per port • Automatable TFTP firmware and configuration update upon boot • RSA SecurID® support using RADIUS • Find Me locator light

User Groups

The Digi Passport unit comes with 4 built-in user groups pre-defined by roles or access levels. The following table lists the 4 user groups, their access rights, and default user names.

Group	Access Privileges		Configuration Privileges		Defaults	
	Ports	Command Line	Ports	System	Login	Password

Root	yes	yes	yes	yes	root	dbps
System Admin	yes	yes (read only)	yes	yes	admin	admin
Port Admin	yes	no	yes	no	-	-
User	yes	no	no	no	-	-

Access Lists

The Digi Passport unit supports access lists for user privileges. These lists can contain multiple users and define specific port rights. If 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, which grants access to all the ports connected to Sun servers. You can then make all the Sun administrators members of this access list. See "Create an Access list" on page 70 for more information.

Root and Admin Usernames and Passwords

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

User Name	Default Password
root	dbps
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. The admin user's password can be changed by either admin or root from within the Web interface or the Menu CLI, the root user's password must be modified from the command line using the command `passwd`.

Ways to Configure the Digi Passport

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

Web Interface

The web interface provides an easy way to configure the Digi Passport 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. Only users with port or system administrative rights can use the web interface for configuration.

The Digi Passport web interface features HTTPS for secure access.

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. ADDP will work whether or not the unit has an address assigned, and whether or not there is a DHCP server on the network, it only requires that the ADDP software is running on a computer on the same LAN segment as the Digi Passport. 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 or hostname directly into the URL address bar of your browser. (Of course, the IP address and DNS server if hostname is used, 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 by entering the command `configmenu`.

```
[root@Digi_Passport ~]# configmenu

Welcome to Digi Passport 16 configuration page
Current time   : 04/18/2006 14:21:48   F/W REV.      : v0.8.0a1
Serial No.     : pp16proto-0610-0001   MAC addr.(eth0): 00-40-9D-22-DE-60
IP addr.(eth0) : 10.4.102.55

1. Network
2. Serial port
3. Clustering
4. Power controller
5. Peripherals
6. System status & log
7. System administration
8. Stop device locating

[h]elp, [s]lave, [a]pply, e[x]it
COMMAND (Display HELP : help)>
```

Ways of Accessing the Digi Passport Ports: Overview

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 admin user can be granted read-only permission as well.

Ways of Accessing the Digi Passport Ports: Overview

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

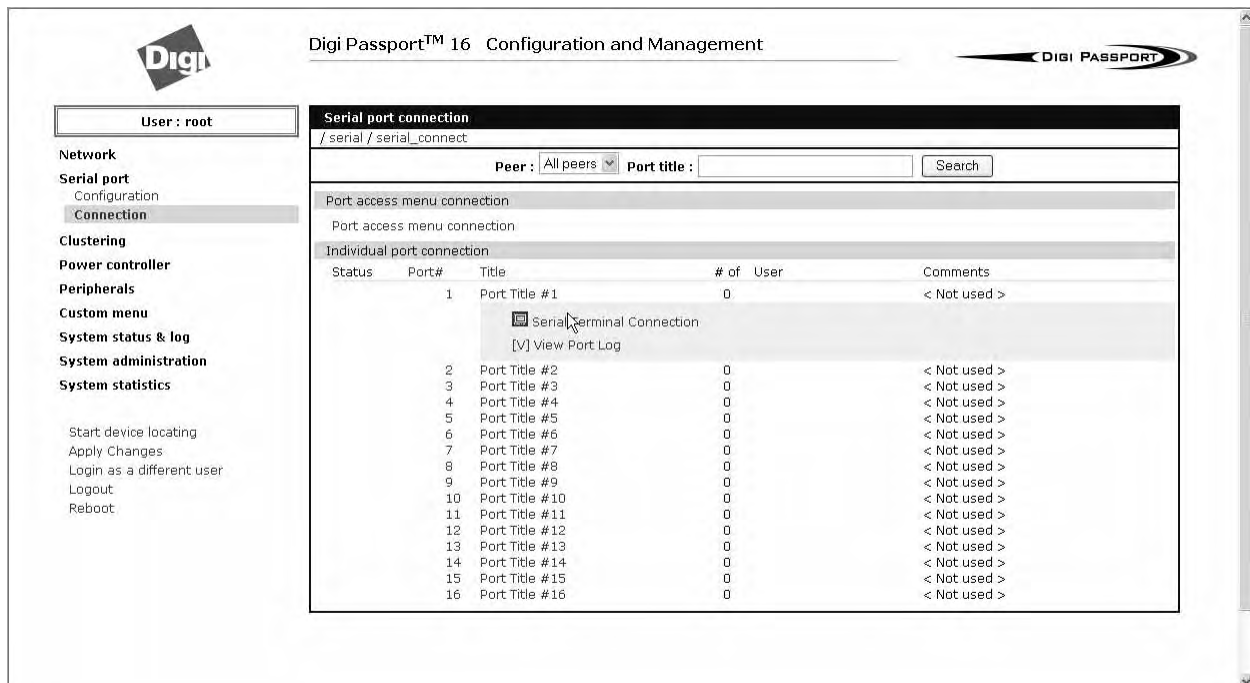
- Web Interface
- Port Access Menu
- Direct Port Access
- Custom Menus

Web Interface Access Menu

The web interface menu provides easy and convenient access to ports. All users can access the menu by entering the the Digi Passport unit IP address or host name in a web browser's URL window. You will only be able to see the ports that you are allowed to access.

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

1. Access the web interface.
2. Click **Serial port > Connection**.



The screenshot shows the web interface for a Digi Passport 16 unit. The page title is "Digi Passport™ 16 Configuration and Management". The user is logged in as "root". The navigation menu on the left includes: Network, Serial port (Configuration, Connection), Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The "Serial port" section is expanded, and the "Connection" sub-menu is selected. The main content area shows the "Serial port connection" configuration page. At the top, there is a search bar with "Peer" set to "All peers" and a "Port title" field. Below this, there are sections for "Port access menu connection" and "Individual port connection". The "Individual port connection" section contains a table with the following data:

Status	Port#	Title	# of	User	Comments
	1	Port Title #1	0		< Not used >
	2	Port Title #2	0		< Not used >
	3	Port Title #3	0		< Not used >
	4	Port Title #4	0		< Not used >
	5	Port Title #5	0		< Not used >
	6	Port Title #6	0		< Not used >
	7	Port Title #7	0		< Not used >
	8	Port Title #8	0		< Not used >
	9	Port Title #9	0		< Not used >
	10	Port Title #10	0		< Not used >
	11	Port Title #11	0		< Not used >
	12	Port Title #12	0		< Not used >
	13	Port Title #13	0		< Not used >
	14	Port Title #14	0		< Not used >
	15	Port Title #15	0		< Not used >
	16	Port Title #16	0		< Not used >

3. Select a port.

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

```
Trying 10.8.115.251 7000 online
```

```

Welcome to Digi Passport 16 Port Access Menu (Digi_Passport)

Digi Passport 16 Login : admin
Digi Passport 16 Password : *****

[Digi_Passport]
=====
Port#      Port Title      Mode  Port#      Port Title      Mode
=====
1      Port Title #1      --    2      Port Title #2      --
3      Port Title #3      --    4      Port Title #4      --
5      Port Title #5      --    6      Port Title #6      --
7      Port Title #7      --    8      Port Title #8      --
9      Port Title #9      --    10     Port Title #10     --
11     Port Title #11     --    12     Port Title #12     --
13     Port Title #13     --    14     Port Title #14     --
15     Port Title #15     --    16     Port Title #16     --

Enter command (1-16 serial port, P passwd, Q exit )
-----> █

```

ls _Local echo Connect Disconnect SendBreak

The web interface can also be configured to call a local Telnet or SSH application, see "Configuring Host Mode" on page 62.

Port Access Menu.

Access Type	Permissions	Procedure
Web interface	Any user can use this method.	<ol style="list-style-type: none"> 1. Access the web interface 2. Choose Serial port > Connection > Port access menu connection 3. Log in
Telnet/SSH	Any user can use this method.	<ol style="list-style-type: none"> 1. Telnet to the Digi Passport unit specifying its IP address and port 7000. (7000 is the default socket port for Telnet) Example: telnet 192.168.15.7 7000 2. Log in
Command line	Root	From the command line, issue the portaccessmenu or connect command. Example: portaccessmenu connect 4 to connect to port 4
Telnet/SSH	Any user	Example: telnet passportdemo.digi.com If user's shell is configured to "Port access menu", please refer to "Administering Users" on page 69.

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.

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:

Type	Command Syntax	Example: Connection to Port 3
Telnet	telnet <i>ip-address tcp-port</i> where <i>ip-address</i> is the Digi Passport unit's IP address and <i>tcp-port</i> 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 <i>user-name@ ip-address tcp-port</i> where <i>user-name</i> is a user's name, <i>ip-address</i> is the Digi Passport unit's IP address and <i>tcp-port</i> is the Listening TCP port for a port ssh <i>user-name:"p=port-number"@ip-address</i> or ssh <i>user-name:"t=port-title"@ip-address</i>	ssh admin@ 192.168.15.7 -p 7003 (7000 is the default socket port for both Telnet and SSH) ssh sunadmin:"p=25"@Digi12 ssh ciscoadmin:"t=Cisco-main"@Digi12

Type	Command Syntax	Example: Connection to Port 3
WEB	<p>http://ip-address/connect.asp?t=<i>port-title</i> http://ip-address/connect.asp?p=<i>port-number</i> where <i>ip-address</i> is the Digi Passport unit IP address or DNS name, <i>port-number</i> is the number of the serial port and <i>port title</i> is the name of the port as assigned in serial port, port title.</p>	<p>http://passportdemo.digi.com connect.asp?t=CISCO.Router.port3 (the port name is case sensitive)</p>

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

Custom Menus

Custom menus are created by either root or the system administrator to limit your access to specific ports. For more information, see "Making Custom Menus" on page 101.

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. The default is <ctrl> z.
3. Click Save to flash and continue with other configurations or click Save & apply for the changes to take effect.
4. Click Save & Apply.

The port escape menu is automatically started if there is one active session to the port established.

5. Enter the port escape sequence. (^z)

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

Description of Fields

Escape Sequence Ctrl+	Description of Action	Occurrence
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

Escape Sequence Ctrl+	Description of Action	Occurrence
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 sniff session

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 Passport unit is available on the Passport CD and can be downloaded from support.digi.com.

Note: SNMP configuration needs to be enabled in the security profile to allow use of this MIB. This is accomplished under the System Administration->Security Profile section of the configuration screen. See "Security Profile" on page 95 for more information

Saving and Applying 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:

Choose the Save to flash button.

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.)

Automatic Device Discovery Protocol ADDP

See the quick start guide that came with the device to set up the configuration. Or insert the CD and select the Device Discovery wizard. Select and click the correct device to configure.

The Device discovery wizard knows the default password for the device. It will prompt you for the password for the root user if you have changed it from the default (dbps)

Configure the IP.

Once the Digi Passport is configured with a valid IP address, you can login to the webUI with username admin, password admin.

Automatic Device Recognition

This feature allows the Digi Passport unit to automatically detect and recognize attached devices. The Digi Passport unit sends down a probe string, default is < Enter > then analyzes the response. If "Use detected port title" is enabled, it will display the detected OS, device and port number in the format:

```
CISCO.Router.port3
Sun.nemo.port5
```

To enable Automatic Device Recognition:

1. **Serial Port > Configuration >** Select the port number or All.
2. **Port title**
 - Automatic Detection** - Enable
 - Use detected port title** - Enable
 - Probe String** - \x0D (means <Enter>)
 - Device detection method** - Active
 - Detection initiation** - periodically
 - Detection delay** - every 5 minutes
3. Click Save & apply.

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.

For configuration of this alarm feature please refer to Configuring Ports Chapter 6.

Locator Light

The Digi Passport unit has two locator lights, one on each side of the unit.

Log into the WebUI as admin or root and Click Start device locating and a popup box will appear to confirm. Click okay and the Digi Passport unit Find me light will blink.

To turn off the Find me light, click Stop device locating.

Introduction

This chapter 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.

Assigning IP Settings from the Console Port

The following steps use the console port to assign IP settings to Ethernet port #1.

The default IP address is 192.168.161.5.

1. Connect the console port on the rear panel of the Digi Passport unit to a serial port on a workstation using the supplied straight-through CAT5 cable and the appropriate console adapter packaged with the the Digi Passport unit.



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.

Configuring for SSH

- At the login prompt, log in as `admin`. The default password for `admin` is `admin`.
The Configuration menu appears.
- Enter the number 1 for Network Configuration.
- Enter the number 1 to select the port for IP configuration

```
Linux 2.6.12 (Digi_Passport) <0>
Digi_Passport login: admin
Password:

Welcome to Digi Passport 48 configuration page
Current time : 04/18/2006 18:23:30 F/W REV : v0.8.0a1
Serial No. : pp16proto-0610-0001 MAC addr.(eth0): 00-40-9D-22-DE-60
IP addr.(eth0) : 10.4.102.55

1. Network
2. Serial port
3. Clustering
4. Power controller
5. Peripherals
6. System status & log
7. System administration
8. Start device locating

[help, ls, save, fa]pply, e[xf]lit
COMMAND <Display HELP : help>> 1

Network
/network

1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering configuration
6. NFS server configuration
7. Web server configuration
8. Ethernet configuration
9. TCP service configuration
10. PPP configuration
11. NIS configuration

[help, ls, save, fa]pply, e[xf]lit
COMMAND <Display HELP : help>> 1_
```

- Enter 1 for IPv4.
- Enter the appropriate parameters for the IP settings.
- Press ESC when done to return to the main configuration menu.
- Enter the number to exit and apply changes.
Changes are saved and applied immediately. There is no need to reboot.

Configuring for SSH

Accessing the Digi Passport unit's command line via SSH is enabled by default (TCP port 22).

Options

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

The the Digi Passport unit supports Blowfish and 3DES encryption methods for SSH.

Configuring the Port Access Menu for SSH

- Access the web interface.
- Log in as `root`, `admin`, or a member of the port administration group. The default password for `root` is `dbps`, and the default password for `admin` is `admin`.
- Under **Serial port > Configuration > Port access menu configuration**.
The Port access configuration menu appears.
- Select SSH as the Port access menu protocol.

User : root

Port access menu configuration
/serial / serial_config / pam

Port Access Menu:

Enable/Disable assigned IP:

Listening TCP port (1024-65535):

Protocol:

Inactivity timeout (1-3600 seconds, 0 for unlimited): second(s)

Quick connect via:

Web applet encoding:

Login on port access:

Authentication

Authentication method:

Alert configuration

Email alert configuration

Email alert for port login:

SNMP trap configuration

Port login trap:

Copyright © 1996-2006 Digi International. All rights reserved.

Note: The "Log in on port access" feature requires the user to log in twice (once for access to the port access menu and again for the specific port) when enabled. If this feature is disabled the only login challenge is to the Port Access Menu (though only permitted users will be able to successfully connect to any specific port).

5. Click Save & apply.

Configuring a Port for SSH

1. Access the web interface.
2. Log in as root, admin, or a member of the port administration group. The default password for root is `dbps`, and the default password for admin is `admin`.
3. Under **Serial port > Configuration**.
4. Select All or one individual port you want to configure for SSH.
5. Click **Host mode configuration**.
6. Specify SSH as the Protocol as shown in the following screenshot.
7. Click Save & apply. see following screenshot.

Windows Configuration for PPP

Windows XP

1. Open "Network Connections" window [Start->Control Panel->Network Connections]
2. Start New connection Wizard [File->New connection] on "Network Connections" window
3. Select "Connect to the network at my workplace" and press Next button
4. Select "Dial-up connection" and press Next button
5. Select "Dial-up connection" and press Next button
6. Enter Connection name and press Next button
7. Enter Phone number and press Next button
8. Select either "Anyone" or "My use only" for Connection Availability and press Next button
9. Click Finish button
10. . Open properties window by clicking right mouse button on the Connection just you made
11. On Security tab, check "Advanced" for Security options and press "Settings" button
12. Set each parameters on Advanced Security Settings window as follows,

. Data encryption: Optional encryption (connect even if no encryption)

Allow these protocols: Unencrypted password(PAP)/Challenge Handshake Authentication Protocol(CHAP)

And then press OK button

- 13 Check "Run script" check box, select "Generic login" and then press Edit button

- 14 Edit following lines of switch.inf file

line 72: OK=<match>"ogin:" => OK=<match>"ogin: "; insert a space character before ":"

line 80: COMMAND=<user name><cr> => COMMAND=admin<cr>

line 89: OK=<match>"assword:" => OK=<match>"password" ; insert a space character before ":"

line 97: COMMAND=<password><cr> => COMMAND=admin<cr>

and then save file.(Attached please find my switch.inf file for your reference)

- 15 Press "OK" button on Properties window

- 16 Double click Connect icon on Dial-up connection.

And enter User name and Password, and then press dial button.

PPP configuration using a Linux client.

Passport

1. [Network -> PPP configuration->Basic PPP settings]

Dynamic IP address pool for incoming connections: **Enable**

First IP address: *enter the starting address of IP pool (192.168.161.200)*

Number of address: *enter the number you want, say (10)*

Press "save to flash" button

2. [Network -> PPP configuration->incoming PPP connection]

Add user for PPP connection and set each parameters

Authentication configuration

Username: admin

Password (new): admin

Password (confirm): admin

Authentication: *CHAP/PAP*

Peer configuration

(*) Automatically assign remote IP address from IP address pool

(v) Allow client access to local network via PPP connection

(*) Automatically assign local IP address from IP address pool

Press "save to flash" button

Please specify the Password after setting all other parameters.(just before pressing "save to flash" button)

If not, Null Password can be specified while changing other parameters.(We will fix this problem in rc version)

[Peripherals->Modem configuration] (v) Enable PPP connection on the Modem

Press "save & apply" button

Redhat 9 machine

1. 1. run kppp

kppp

2. Press "Setup" button on KPPP window

3. Press "New" button on Accounts Tab on KPPP Configuration window

4. Select "Dialog Setup" on Create New Account window

5. Enter any name you want in Connection name field on Dial tab on New Account window

6. Press "Add" button on Dial tab on New Account window

6. Enter phone number of internal modem and press "OK" button

7. Select authentication as "PAP/CHAP" on Dial tab on New Account window

8. Select Dynamic IP address on IP tab on New Account window

9. Select Default gateway on Gateway tab on New Account window

Adding, Editing, and Removing Users

10. Select Automatic configuration on DNS tab on New Account window

11. Add following Login Scripts sequentially on Login Script tab on New Account window

Expect Login:

Send admin

Expect Password:

Send admin

Please note that there is a space character before ":" character in Expect case

And then press "OK" button

12. Select Device tab on KPPP Configuration window and check each parameters

You may use default values except Modem device.

Please select the device that modem is connected

Then press "OK" button

13. Select Connection name that you just configured on KPPP window

And enter Login ID and Password and check Show log window checkbox

14. Finally Press "Connect" button and you can see the login process on Login Script Debug Window

If there is any error, you can find the reason on Redhat machine by checking /var/log/messages file

After connection, please check whether there are correct PPP interfaces in Passport and Redhat machine both.

Current Passport firmware you have has a problem in using PC modem card, we will fix this problem in rc version.

PPP mode in serial port can be set in [Serial port configuration ->Host mode configuration->Host mode]

Adding, Editing, and Removing Users

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

Procedure

1. Access the web interface.
2. Log in as root or admin. The default password for root is `dbps`, and the default password for admin is `admin`.

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

The screenshot shows the 'User administration' window. At the top, there are input fields for 'User name' and 'User group' (set to 'All group'), and a 'Search' button. Below this is a table titled 'Current local users' with columns for '#', 'User name', 'User group', and 'Shell'. The table contains two entries: '1 admin System admin Configuration menu' and '2 root Root CLI'. At the bottom of the table are 'Add', 'Edit', and 'Remove' buttons.

#	User name	User group	Shell
1	admin	System admin	Configuration menu
2	root	Root	CLI

4. Select Add, Edit, Remove or click the username to edit a user.
- 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

The screenshot shows the 'Add user' dialog box. It contains several fields: 'User name' (Test), 'Select group' (User), 'Password' (empty), 'Confirm password' (empty), 'Shell program' (Custom menu), 'SSH public key authentication' (Disable), 'Select SSH Version' (SSH v2), and 'SSH public key file' (empty) with a 'Browse...' button. At the bottom are 'Add' and 'Cancel' buttons.

5. 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" on page 91.

About Shell Options

The shell program selection determines the interface you see when establishing a Telnet or SSH session or connecting via the console port with the Digi Passport 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

Adding, Editing, and Removing Users

User Group	Shell Program Options
user	port access menu, custom menus

Introduction

This chapter includes information on adding and configuring PC cards for the Digi Passport 8, 16, 32, and 48 port units. PC card devices that can be added to the the Digi Passport unit include a serial modem, compact-flash card, wireless LAN card, and a network LAN card.

Compatible PC Cards

All compact-flash, and most simple serial modem cards should work with the Digi Passport, but not all LAN, wireless LAN, or combo cards will. To see a list of compatible cards that have been tested with the Digi Passport unit, visit the Digi support site at <http://www.digi.com/passport/>.

Adding a Compact-flash Card

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



PC card slot

Digi Passport 32 shown

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

1. Insert the card into the PC card slot.
2. Access the web interface.
3. Under the **PC card** heading click **Configuration**.
4. Click Configure the detected card.

The following fields appear on the configuration page.

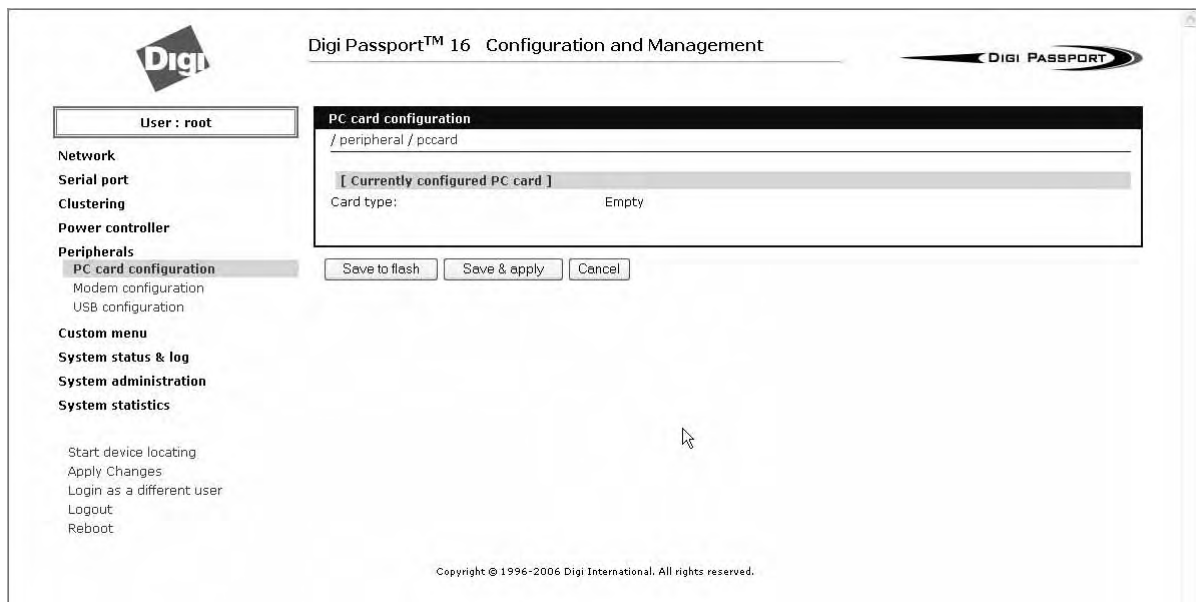
— **ATA/IDE Fixed Disk Card configuration**

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

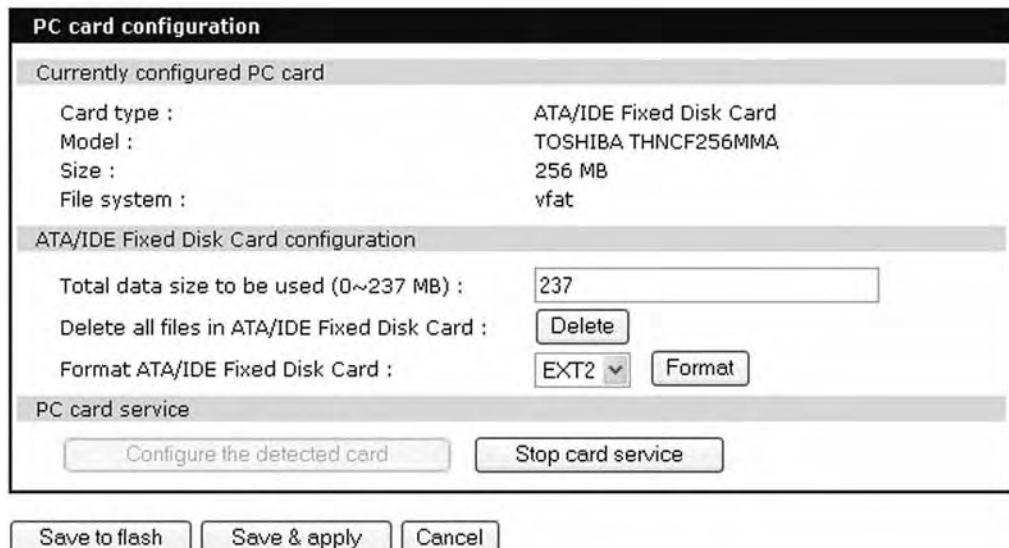
Always select the Stop card service button and Save & apply before removing the PC card.

Adding a Network Card



compact-flash card of all files.

Format ATA/IDE Fixed Disk Card. - The options are EXT2 or FAT formats. If it is necessary to format the card, 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.

Adding a Network Card

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

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

PC card configuration	
Currently configured PC card	
Card type :	Network Card
Model :	corega K.K. corega FEtherII PCC-TXD
Network configuration	
IP mode :	DHCP
IP address :	192.168.1.254
Subnet mask :	255.255.255.0
Default gateway :	192.168.1.1
Primary DNS :	204.221.114.1
Secondary DNS :	168.126.63.2
PC card service	
<input type="button" value="Configure the detected card"/> <input type="button" value="Stop card service"/>	
<input type="button" value="Save to flash"/> <input type="button" value="Save & apply"/> <input type="button" value="Cancel"/>	

5. Click Save & apply.

Note: If DHCP is active the IP address will appear after "Save & apply" is clicked.

Adding a Wireless LAN Card

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

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

Adding a Serial Modem

PC card configuration

Currently configured PC card

Card type :	Wireless Network Card
Model :	Cisco Systems 350 Series Wireless LAN Adapter

Network configuration

IP mode :	DHCP
IP address :	192.168.1.254
Subnet mask :	255.255.255.0
Default gateway :	192.168.1.1
Primary DNS :	192.168.1.1
Secondary DNS :	0.0.0.0
Reuse old IP at bootup time on DHCP failure :	Disable

Wireless network card configuration

SSID :	test
Use WEP key :	Enable
WEP mode :	Encrypt
WEP key length :	128 bits
WEP key string :	XXXXXXXXXX

PC card service

Configure the detected card Stop card service

Save to flash Save & apply Cancel

6. Click Save to flash.

Adding 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.
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.

Installing and Configuring PC Cards

PC card configuration

Currently configured PC card

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

Serial Modem Card configuration

Init string :	<input type="text" value="q1e0s0=2"/>
Inactivity timeout (1-3600 sec, 0 for unlimited) :	<input type="text" value="0"/>

PC 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.

4. Edit any appropriate parameters and Click Save & apply.

Digi Passport User interface

While the Digi Passport provides many capabilities for the Passport Administrator, the goal is to make the experience as simple as possible for the Passport User (who has other systems to worry about).

The screenshot shows the user interface for 'User: admin' on the 'Serial port connection' page. The left sidebar contains a navigation menu with categories like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area displays a table of port titles and their status.

Status	Port#	Title	# of	User	Comments
	1	Port Title #1	0		< Not used >
	2	Port Title #2	0		< Not used >
	3	Port Title #3	0		< Not used >
	4	Port Title #4	0		< Not used >
	5	Port Title #5	0		< Not used >
	6	Port Title #6	0		< Not used >
	7	Port Title #7	0		< Not used >
	8	Port Title #8	0		< Not used >
	9	Port Title #9	0		< Not used >
	10	Port Title #10	0		< Not used >
	11	Port Title #11	0		< Not used >
	12	Port Title #12	0		< Not used >
	13	Port Title #13	0		< Not used >
	14	Port Title #14	0		< Not used >
	15	Port Title #15	0		< Not used >
	16	Port Title #16	0		< Not used >

Upon login, the Passport user is presented with a page that shows the systems that they are allowed to manage or control.

The only option available under System Administration is to change their own password. They can also log in as a different user or log out of the system.

The Passport Connection page provides an iconic representation of the status of the equipment under management when you click a specific port:

The screenshot shows the user interface for 'User: root' on the 'Serial port connection' page. The left sidebar contains a navigation menu with categories like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area displays a table of port titles and their status, with a 'Serial Terminal Connection' section below the table.

Status	Port#	Title	# of	User	Comments
	1	Port Title #1	0		< Not used >
	2	Port Title #2	0		< Not used >
	3	Port Title #3	0		< Not used >
	4	Port Title #4	0		< Not used >
	5	Port Title #5	0		< Not used >
	6	Port Title #6	0		< Not used >
Serial Terminal Connection [V] View Port Log					
	7	Port Title #7	0		< Not used >
	8	Port Title #8	0		< Not used >
	9	Port Title #9	0		< Not used >
	10	Port Title #10	0		< Not used >
	11	Port Title #11	0		< Not used >
	12	Port Title #12	0		< Not used >
	13	Port Title #13	0		< Not used >
	14	Port Title #14	0		< Not used >
	15	Port Title #15	0		< Not used >
	16	Port Title #16	0		< Not used >

Administering Users

If the power to a unit is turned off, then the power warning status is indicated on the main screen.

If an event alert has been triggered, then the Alert Icon will appear.

Clicking on the System name or port number will expand the view so that all available methods of connection or management are specified. Systems can be powered on and off, a console to the serial console can be launched, and a **freeKVM** session can be initiated to the server. The port log can also be reviewed to see what event triggered the alarm.

Administering Users

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.

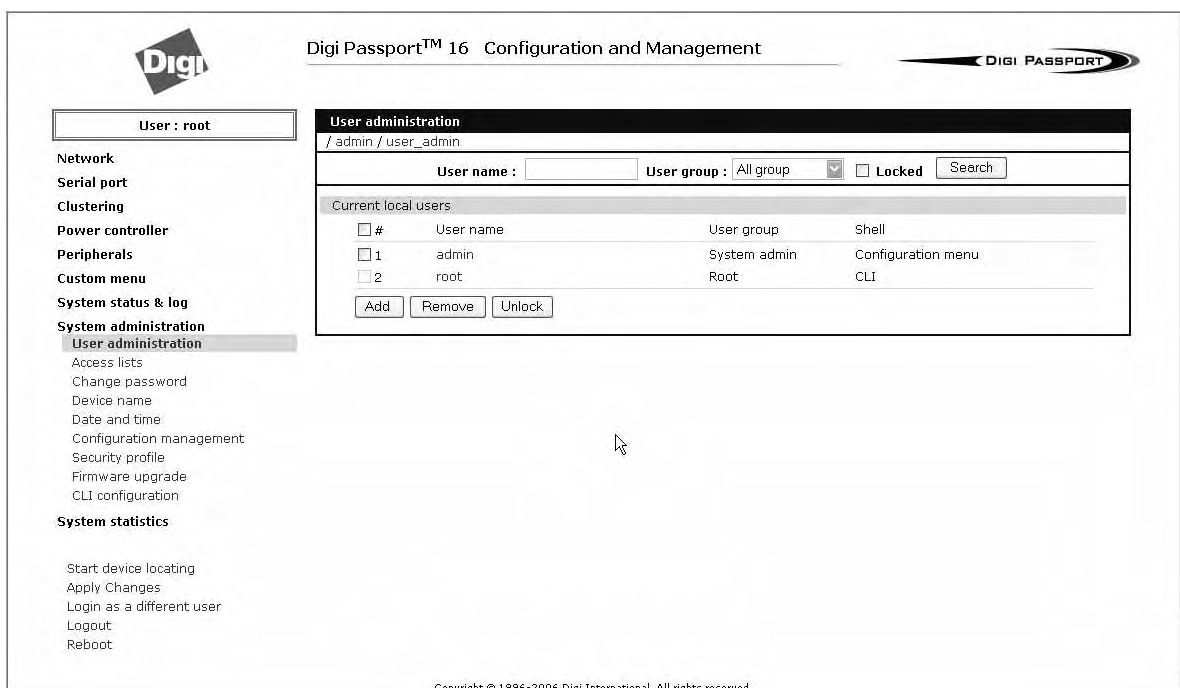
There are several ways to manage users. A user can be added, edited, or removed. Multiple users can be managed in Groups or Access lists. The difference between Groups and Access lists are that Groups define privilege levels to access or change configuration of the Passport unit itself (for Passport unit administration) while Access lists define rules for access to ports and port capabilities.

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.

Procedure

1. Access the web interface.
2. Under **System administration**, choose **User administration**.

The following screen appears.

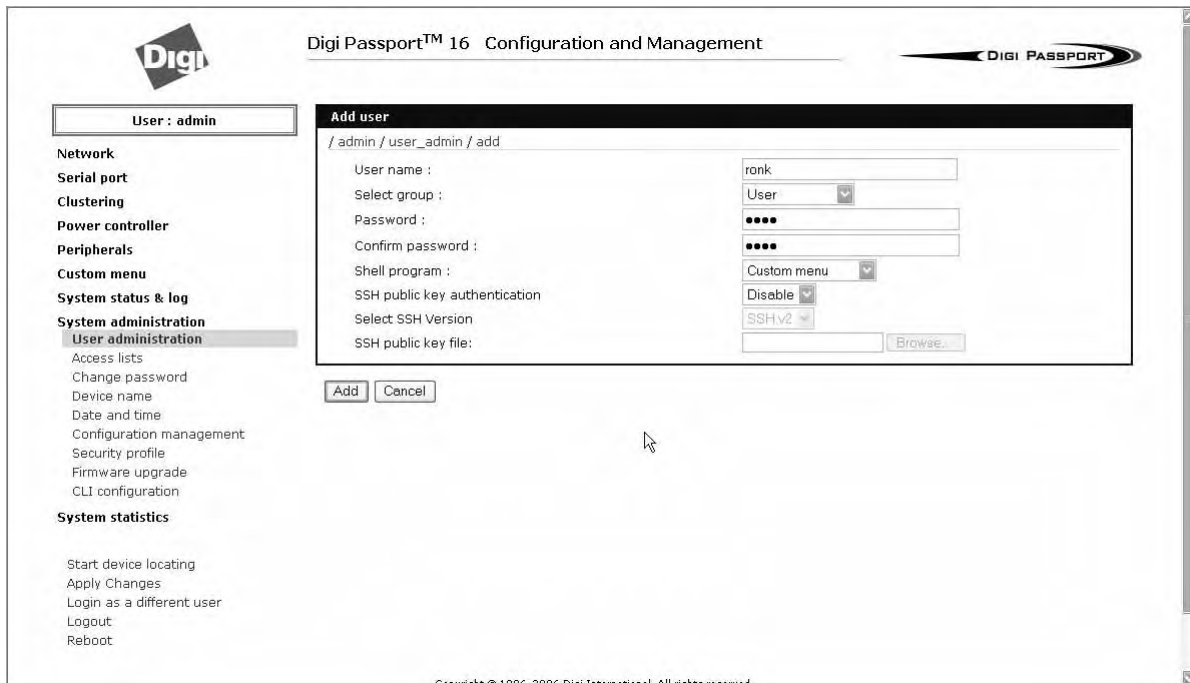


Note: Usernames on the Digi Passport unit are case sensitive.

3. Do one of the following:

To...	Do the Following...
Add a user	<ol style="list-style-type: none"> 1. Click Add. 2. Fill in the attribute fields. See the table that follows for information on attribute fields. 3. Click Add.
Edit a user	<ol style="list-style-type: none"> 1. Click on the username. 2. Fill in the attribute fields. See the table that follows for information on attribute fields. 3. Click Submit.
Remove a user	<ol style="list-style-type: none"> 1. Check the box that corresponds to the user you want to remove. 2. Click Remove. 3. Choose OK at the prompt.

To...	Do the Following...
Create an Access list	<ol style="list-style-type: none"> 1. Under System administration, click Access List. 2. Enter the name of the Access List and click Add. 3. Click on the access list name to add users 4. Add the users to the access list <p>Note: The name field in the Access list allows you to add users that are not locally configured on the Digi Passport unit but use a centralized authentication method like RADIUS, LDAP etc.</p> <p>To change the privileges of an Access list, see "Change the Privileges of an Access List" on page 92</p>



4. Click **Apply changes**.

To Add an Access List to the Digi Passport Unit

1. Access the web interface of the Digi Passport unit.
2. Under System Configuration choose **Access Lists**
3. Enter the access list name into the edit-box and click [ADD].

A pop-up windows will appear confirming the successful addition of an access list. Now you can add users to the access list by:

1. Click the name of the access list; a configuration windows will open
2. Add one user at a time to the list by:

Entering the name into the edit-box and clicking on [ADD].

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

After an access list has been added to the system, port rights can be associated with it. See chapter 8.

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 Passport 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" on page 15 for more information
Password	Password to assign to the user.
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
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

Introduction

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

- A syslog server
- An NFS server
- Removable flash storage (PC-card or USB)
- The Passport 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 flash, you must first enable the devices and/or enter the required information before you can designate them as storage locations.

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)

Enabling Log Storage Location

IP Information

IP mode - Method for setting IP address either Static, DHCP, PPPoE, or Disabled

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

Enabling Log Storage Location

Enable 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. To enable the NFS server for port or system logging, do the following:

1. Access the web interface.
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

Encrypted primary NFS server password - Password

Confirm Encrypted primary NFS server password - Repeat 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. To activate NFS logging, choose Enable.

User : root

Network

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

Serial port

Clustering

Power controller

Peripherals

Custom menu

System status & log

System administration

System statistics

- Start device locating
- Apply Changes
- Login as a different user
- Logout
- Reboot

NFS server configuration
/network/nfs

NFS service:

Primary NFS server name:

Mounting path on primary NFS server:

Primary NFS timeout (sec, 5-3600):

Primary NFS mount retrying interval (sec, 5-3600):

Enable/Disable encrypted primary NFS server:

Encrypted primary NFS server user:

Encrypted primary NFS server password (new):

Encrypted primary NFS server password (confirm):

Secondary NFS service configuration

Secondary NFS service:

Secondary NFS server name:

Mounting path on secondary NFS server:

Secondary NFS timeout (sec, 5-3600):

Secondary NFS mount retrying interval (sec, 5-3600):

Enable/Disable encrypted secondary NFS server:

Email alert configuration

Enable/Disable email alert for NFS disconnection:

SNMP trap configuration

Enable/Disable NFS disconnection trap:

Use global SNMP configuration:

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 of 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, and enter the IP information for Trap receiver settings.
5. Click Save & apply.

Enable Server

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

1. Access the web interface.

User : root

NFS server configuration
/ network / nfs

Primary NFS service configuration

NFS service:

Primary NFS server name:

Mounting path on primary NFS server:

Primary NFS timeout (sec, 5-3600):

Primary NFS mount retrying interval (sec, 5-3600):

Enable/Disable encrypted primary NFS server:

Encrypted primary NFS server user:

Encrypted primary NFS server password (new):

Encrypted primary NFS server password (confirm):

Secondary NFS service configuration

Secondary NFS service:

Secondary NFS server name:

Mounting path on secondary NFS server:

Secondary NFS timeout (sec, 5-3600):

Secondary NFS mount retrying interval (sec, 5-3600):

Enable/Disable encrypted secondary NFS server:

Email alert configuration

Enable/Disable email alert for NFS disconnection:

SNMP trap configuration

Enable/Disable NFS disconnection trap:

Use global SNMP configuration:

Save to flash Save & apply Cancel

2. Under the **Systems Status and Logging** heading, click **SYSLOG-NG 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**.

User : admin

System logging
/ system / systemlog

System log storage location:

SYSLOG facility for system logging:

System log buffer max size:

System log buffer size: KB

System log filename:

Automatic backup on mounting:

Send system log by Email:

System log view :

Clear Refresh View

Save to flash Save & apply Cancel

Enable a Compact-flash Card

The compact-flash card must be installed and configured on the Passport unit before it can be used for system logging or storing the Passport 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 count of the Passport unit used. The maximum settings for log file sizes are listed in the following table. See also Adding a Compact-flash Card on page 33.

Total Flash Card Size	Passport	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	
	48	36.8	4.1M	

Enable the Passport Unit's Memory

The Passport 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 Passport 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 Passport unit used. The log file sizes shown in the following table are maximum settings. See also Configuring System Logging on page 50.

Configuring System Logging

Passport	System Log	Port Log (per port)	Total Memory Used
8	300K	400K	3.5M
16		200K	
32		100K	
48		66K	

Configuring System Logging

To configure the Passport unit for system logging, do the following:

1. Access the web interface.
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 Passport unit's memory choice is always available.

System logging - Enable or Disable

System log storage location - Memory, Flash Media, or NFS server

System log buffer size (KB, 300 max) - Log buffer size in KB

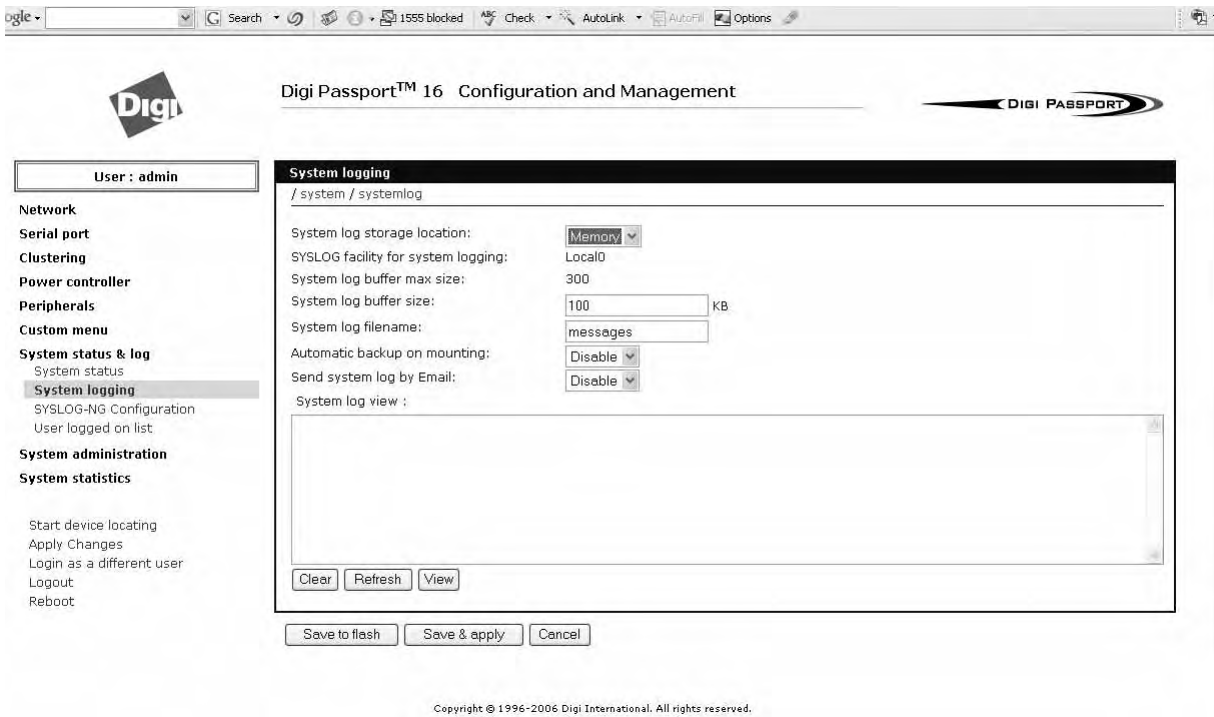
Automatic backup on mounting This parameter defines the action taken if the NFS partition or Flash media is mounted or re-mounted.

- Enable: rename the existing log file by adding a -xx with xx being a incrementing 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. Enter the contact email address.
6. Click Save & apply



Viewing 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
USB	

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 Passport unit, a compact-flash card, a syslog server, or to an NFS server. If

Configure Port Logging

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.
2. Under the **Serial port** heading, click **Configuration**.
3. Choose All or the Individual port, and then **Port logging**.

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.

4. Click Save & apply.

The screenshot displays the 'Port logging' configuration page in a web interface. The user is logged in as 'admin'. The left sidebar contains a navigation menu with categories like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled 'Port logging' and shows the configuration for port 4. The configuration options include: 'Port logging' (set to 'Enable'), 'Logging direction' (set to 'Server output'), 'Port log storage location' (set to 'Memory'), 'Port log to SYSLOG server' (set to 'Disable'), 'Port log buffer size' (set to '50 KB'), 'Port logging filename option' (set to 'Specify below'), 'Port logging filename' (set to 'port4data'), 'Time stamp to port log' (set to 'Disable'), and 'Show last 10 lines of a log upon connect' (set to 'Disable'). There are also buttons for 'Clear', 'Refresh', and 'View'.

Note: When port logging is enabled, a Port Event Handling page is available to create alarm keywords and send alerts. See Chapter Alerts and Notifications on page 69 for more information.

Viewing 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 from 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 > **Port logging**.

Introduction

This chapter 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 RemotePorts™ support.

Enabling and Disabling 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 Port Management > Enable or Disable from the drop down menu.
3. Click Save to flash and continue with other configurations or click Save & apply.

The screenshot displays the web interface for configuring a Digi Passport™ 16. The page title is "Digi Passport™ 16 Configuration and Management". The user is logged in as "admin". The left sidebar shows a navigation menu with categories: Network, Serial port (selected), Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. Under "Serial port", the "Configuration" sub-menu is active, showing options for Connection, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled "Port management" and shows the configuration for port 1. The breadcrumb path is "/ serial / serial_config / ports / 1 / port_mgmt". The "Port management" section includes:

- Enable/Disable this port: Enable (dropdown)
- RealPort support: Disable (dropdown)
- Reset this port: Reset (button)
- Set this port as factory default: Set (button)

 Below this are several expandable sections: Apply all ports settings, Automatic detection, Port title, Host mode configuration, freeKVM configuration, Serial port parameters, Port logging, Authentication, User access control, and Alert configuration. At the bottom of the configuration area are three buttons: "Save to flash", "Save & apply", and "Cancel". The footer contains the copyright notice: "Copyright © 1996-2006 Digi International. All rights reserved."

RealPort Support

The Digi supplied RealPort driver provides a logical connection from a host computer to the physical serial port on the Digi Passport, regardless of where it is located 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. Full hardware and software flow control is also included.

When you use RealPort to communicate with a serial port on the Digi Passport, the other capabilities of the Digi Passport are not available for that port. That is to say that the Digi Passport unit can be used for console management or for RealPort COM re-direction but not both at the same time. To enable RealPort use the following procedure.

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

The screenshot displays the web interface for a Digi Passport 16. The top navigation bar includes the Digi logo, the title "Digi Passport™ 16 Configuration and Management", and the "Digi PASSPORT" logo. On the left, a sidebar menu lists various system functions such as "Network", "Serial port", "Configuration", "Connection", "Clustering", "Power controller", "Peripherals", "Custom menu", "System status & log", "System administration", and "System statistics". The main content area is titled "Port management" and shows a breadcrumb path: "/ serial / serial_config / ports / 1 / port_mgmt". The configuration options include: "Enable/Disable this port:" with a dropdown menu set to "Enable"; "RealPort support:" with a dropdown menu set to "Disable"; "Reset this port:" with a "Reset" button; and "Set this port as factory default:" with a "Set" button. Below these are several expandable sections: "Apply all ports settings", "Automatic detection", "Port title", "Host mode configuration", "freeKVM configuration", "Serial port parameters", "Port logging", "Authentication", "User access control", and "Alert configuration". At the bottom of the configuration area are three buttons: "Save to flash", "Save & apply", and "Cancel". A copyright notice at the bottom reads: "Copyright © 1996-2006 Digi International. All rights reserved."

Resetting Ports

The Digi Passport 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 Passport 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 Passport unit to evaluate the attached devices and populate the port title. Additionally the Digi Passport unit can generate a SNMP trap or send an e-mail in case the response of the device changes or if it stops responding.

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`.

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`.

The commands to parse the system response are user customizable, so if a device is not recognized by the Digi Passport unit, the root user may add a rule to the appropriate file to allow it to be properly recognized.

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.

Configuring Automatic Device Recognition

Configure a serial port for Automatic Device Recognition.

1. Access the web interface.
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.

Copyright © 1996-2006 Digi International. All rights reserved.

Automatic detection - Enable or disable automatic detection of devices

Use detected port title - Enable if you want the Digi Passport 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 Passport unit allows access to a port by using only 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.

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 test\x0d	<ESC><Space>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 If 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.

5. Click Save & apply.

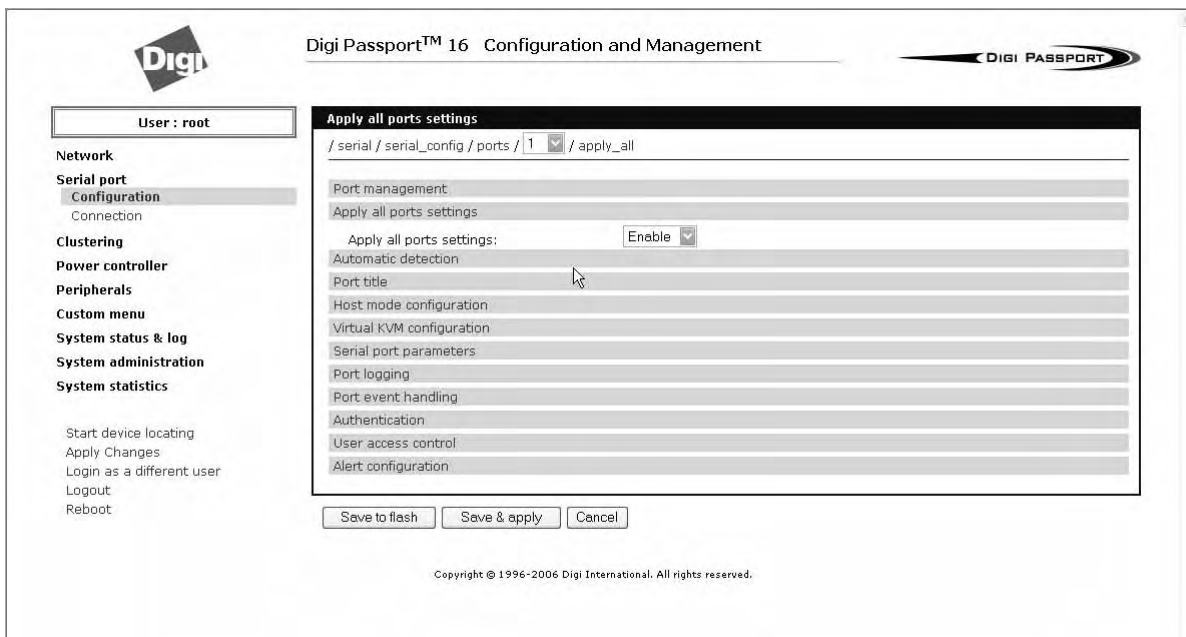
Apply all Ports Settings

The Digi Passport 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.
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.



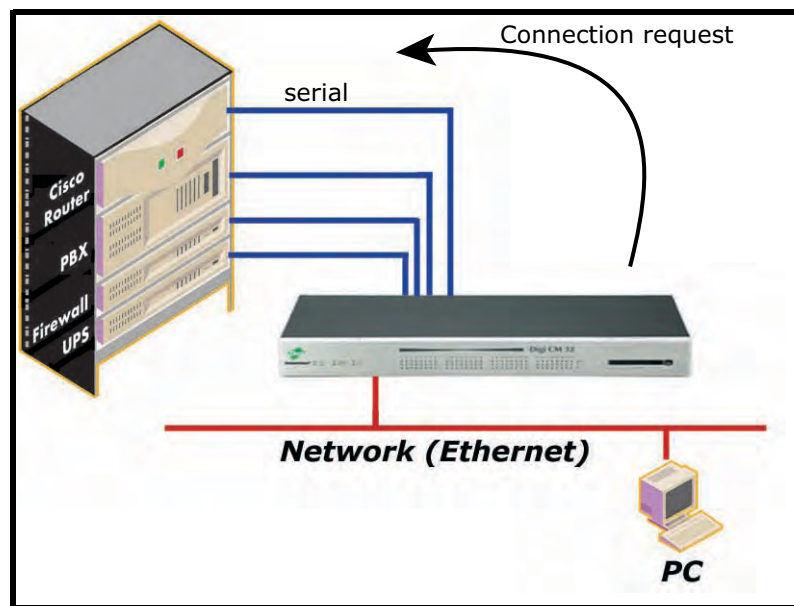
Host Mode Configuration

The Digi Passport 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.

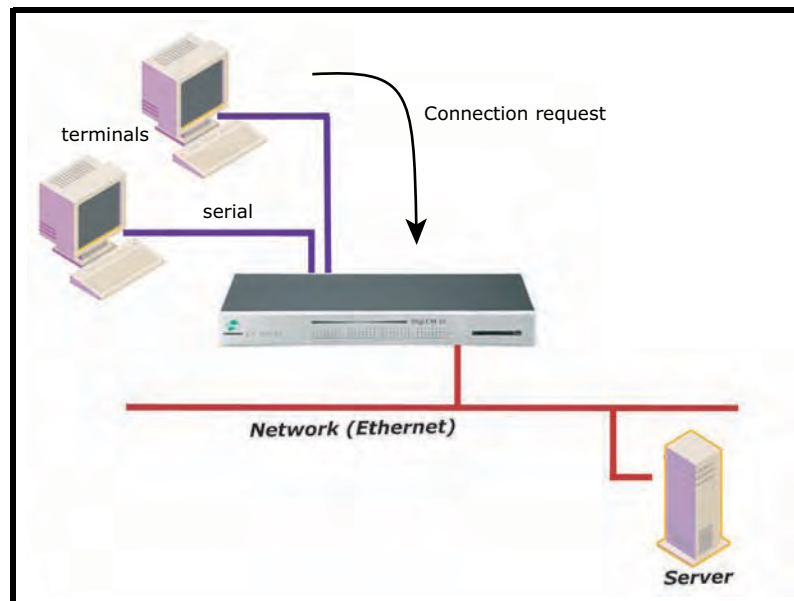
Console Server Mode

Configuring a serial port as a console server creates a TCP socket on the Digi Passport 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.



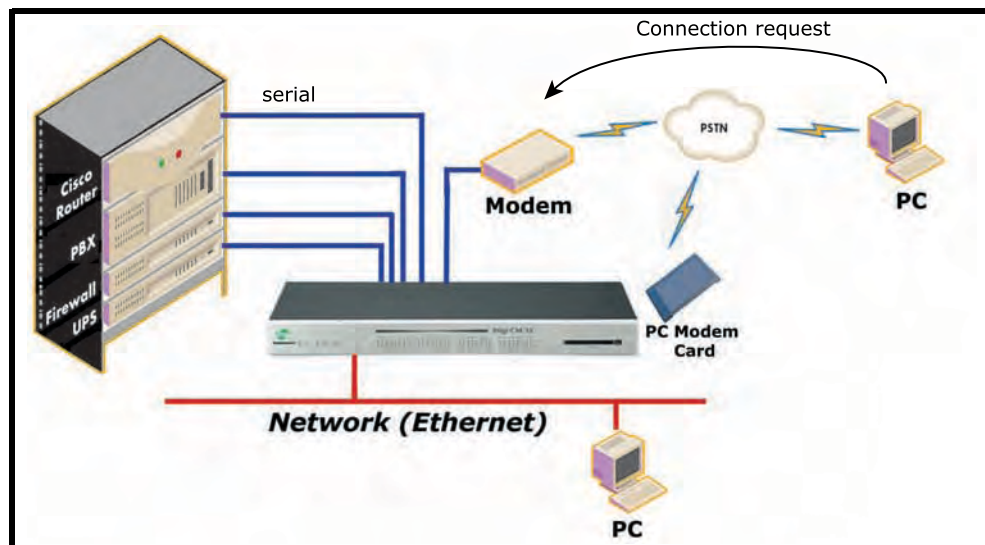
Terminal Server Mode

In terminal server mode, the Digi Passport unit's serial port is configured to wait for data from the device connected to the port. If data is detected, the Digi Passport 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.



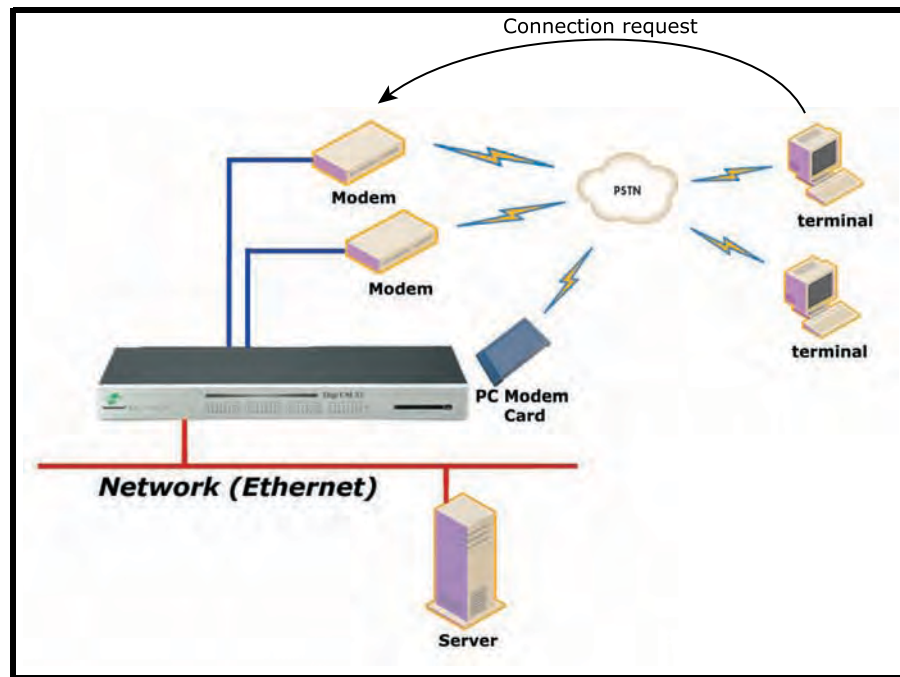
Dial-In Modem Mode

In this mode, the Digi Passport 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 Passport 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 Passport 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 Passport 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.



Configuring 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.
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.

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

Type of console server - The options are MS SAC - which you use to provide a graphic user interface to the Windows Server 2003 Special Administration Console (see "Microsoft SAC Support" on page 107) 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.

The screenshot shows the 'Host mode configuration' page in the Digi Passport 16 web interface. The breadcrumb path is '/ serial / serial_config / ports / 1 / hostmode'. The page is divided into several sections:

- Port management:** Includes 'Apply all ports settings' and 'Automatic detection' buttons.
- Host mode configuration:**
 - Host mode: Console server (dropdown)
 - Type of console server: Other (dropdown)
 - Rackable System Management Card: Disable (dropdown)
 - Enable/Disable assigned IP: Disable (dropdown)
 - Listening TCP port (1024-65535): 7001 (text input)
 - Protocol: SSH (dropdown)
 - Inactivity timeout (1-3600 sec, 0 for unlimited): 0 (text input)
 - Enable/Disable port escape sequence: Enable (dropdown)
 - Port escape sequence: Ctrl- Z (text input)
 - Port break sequence: ~break (text input)
 - Use comment: No (dropdown)
 - Quick connect via: Web applet (dropdown)
 - Web applet encoding: English (latin1) (dropdown)
- Virtual KVM configuration:** Includes 'Serial port parameters', 'Port logging', 'Port event handling', 'Authentication', 'User access control', and 'Alert configuration' sections.

At the bottom of the configuration area are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'. The footer of the page reads 'Copyright © 1996-2006 Digi International. All rights reserved.'

5. Click Save & apply.

Supported Protocols

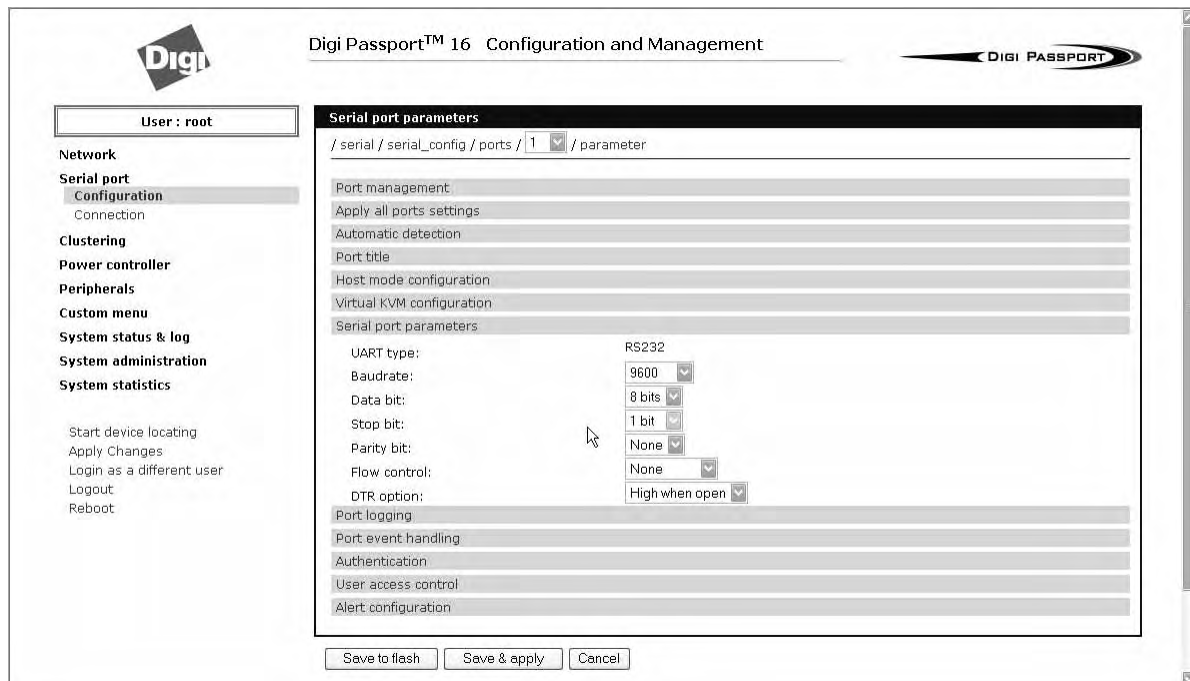
The Digi Passport unit supports the ability to choose one of three different protocol options for each port: SSH, Raw TCP, and Telnet.

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 Passport 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 Passport unit, do the following:

1. Access the web interface.
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 Passport unit to transfer data stored in the buffer. The Digi Passport unit transfers data when the buffer is full using the TCP/IP protocol. However, if it is not full, the Digi Passport 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 Passport 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 Passport unit.
2. Click Serial Port > Configuration.
3. Select All ports to configure.
4. Click Host Mode configuration.
5. Under Protocol, select RawTCP.
- 6) Select Serial port parameters

The screenshot shows the 'Serial port parameters' configuration page in the Digi Passport 16 web interface. The page is titled 'Digi Passport™ 16 Configuration and Management' and includes a navigation menu on the left with options like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled 'Serial port parameters' and shows the configuration for port 1. The 'Serial port parameters' section includes the following settings:

- UART type: RS232
- Baudrate: 9600
- Data bit: 8 bits
- Stop bit: 1 bit
- Parity bit: None
- Flow control: None
- DTR option: High when open
- Enable/Disable delimiter: Enable
- Delimiter: (empty text field)
- Delimiter option: with delimiters

At the bottom of the configuration area, there are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'. The footer of the page reads 'Copyright © 1996-2006 Digi International. All rights reserved.'

7) Configure the delimiter and supporting settings. Descriptions of the options follow.

Enable/Disable delimiter --Allows delimitator 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

Remote Ports

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 Passport unit supports RemotePorts. RemotePorts are any type of port that can be accessed using Telnet, SSH, or Raw TCP protocol. This includes connections to Digi PortServer Terminal Servers, Sun ALOM ports, and IPMI management ports. This feature establishes the Digi Passport unit as the central access system for any kind of text based out-of-band management. Using the Digi Passport 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 alarming
- Centralized access to serial-based and IPMI consoles

Remote ports also provide the additional capabilities described in the sections on Port Logging, Alerts and Notifications, and *freeKVM*

Configure Remote Ports

To configure a remote port use the following procedure.

1. Access the Digi Passport 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 pop-up window will appear to confirm the action.

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 your selections by clicking Save & apply. A pop-up window will appear 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.

Accessing 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

Web Access

Click Serial ports > **Connection** > Port number.

Remote ports are sorted below the physical serial ports as the next available port number.

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).

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:

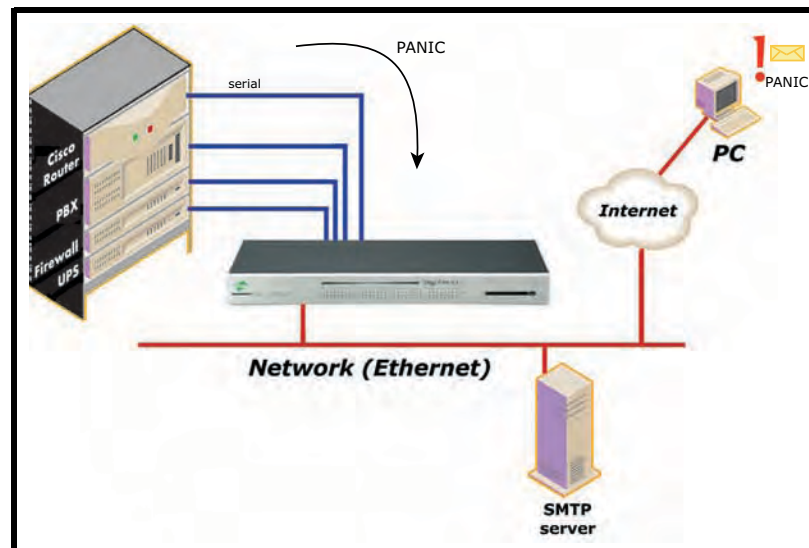
- directly using the portnumber

Note: 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.

Chapter 6**Alerts and Notifications****Introduction**

The Digi Passport 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 Passport 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 Passport unit supports three types of SMTP servers: SMTP server without authentication, SMTP server with authentication, and POP before SMTP.

The Digi Passport 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 Passport unit supports both versions 1, 2, and 3 of the SNMP protocol. The main function of SNMP on the Digi Passport 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 Passport 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 Passport unit, do the following:

1. Access the web interface.
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

The Digi Passport unit supports SNMP authentication, power on, and link up traps.

Applications such as an NMS (Network Management System) or an SNMP browser can exchange information with the Digi Passport 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, link up, login, NFS, Samba, Power Management, Power Fail and IPMI traps are supported.

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

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 "Automatic Device Discovery Protocol ADDP" on page 22, 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")

The MIBs for applicable to the Digi Passport unit can be found on the Passport CD and at <http://www.digi.com/support/> under Digi Passport utilities.

Configuring SNMP v1 or v2

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

1. Access the Digi Passport 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 Passport 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 Passport unit only supports Application (7) service level.

EnablePowerOnTrap. - Determines whether the SNMP agent generates a trap each time the Digi Passport 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.

EnableLinkDownTrap. -

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 Passport 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. The Community string can be anything but they must match what you use in your SNMP software.

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. The Community string can be anything but they must match what you use in your SNMP software.

Version - Choose the SNMP version, either version 1 or version 2c.

The screenshot displays the 'SNMP configuration' page. On the left is a navigation menu with categories like Network, Serial port, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main area is divided into several sections:

- SNMP configuration:** Fields for sysContact (adminstrator), sysName (Digi Passport), sysLocation (my location), sysService (7), and Options (Trap, Email).
- EnablePowerOnTrap/Email:** No / No
- EnableLoginTrap/Email:** No / No
- EnableLinkUpTrap/Email:** No / No
- EnableLinkDownTrap/Email:** No / No
- EnableLoginTrap/Email:** No / No

Below these are two tables for access control settings:

No.	IP address	Community	Permission
1	<input checked="" type="checkbox"/> 192.168.100.101	digipassport	Read Only
2	<input type="checkbox"/> 0.0.0.0		
3	<input type="checkbox"/> 0.0.0.0		
4	<input type="checkbox"/> 0.0.0.0		

No.	User	Security level	Auth Priv	Permission
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			

No.	IP address	Community	User	Security level	Version
1	<input type="checkbox"/> 0.0.0.0				
2	<input type="checkbox"/> 0.0.0.0				
3	<input type="checkbox"/> 0.0.0.0				
4	<input type="checkbox"/> 0.0.0.0				

6. Click Save & apply.

Managing the SNMP Protocol

The Digi Passport 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.

SNMPv3 Configuration

SNMPv3 allows for authentication and encryption thus making it more secure than SNMPv1 or SNMPv2. This section demonstrates the steps required to configure SNMPv3 access control and SNMPv3 traps.

1. Open the main SNMP configuration page.

SNMP configuration
/ network / snmp

sysContact: administrator
 sysName: Digi Passport
 sysLocation: my location
 sysService: 7
 Options: Trap Email
 EnablePowerOnTrap/Email: No No
 EnableAuthenTrap/Email: No No
 EnableLinkUpTrap/Email: No No
 EnableLinkDownTrap/Email: No No
 EnableLoginTrap/Email: No No

Access control settings (NMS)

No.	IP address	Community	Permission
1	<input checked="" type="checkbox"/> 192.168.100.101	digipassport	Read Only
2	<input type="checkbox"/> 0.0.0.0		Read Only
3	<input type="checkbox"/> 0.0.0.0		Read Only
4	<input type="checkbox"/> 0.0.0.0		Read Only

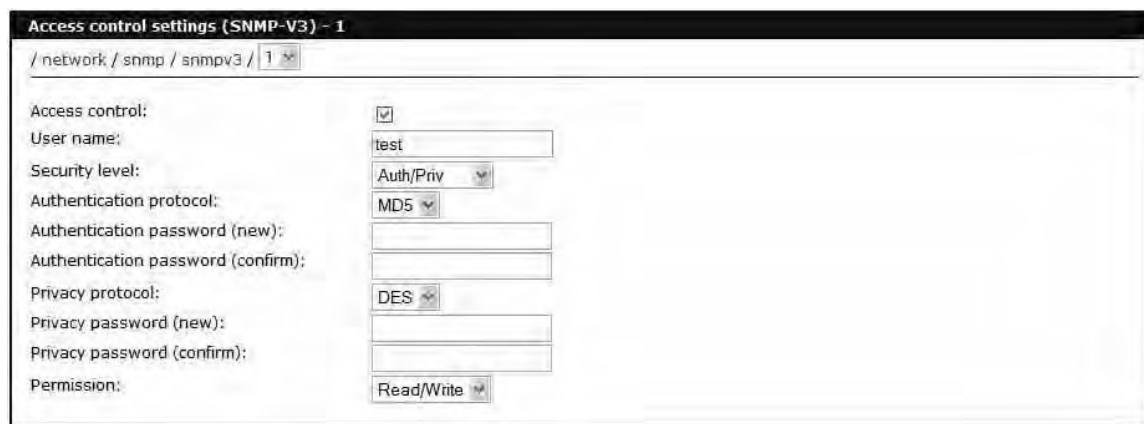
Access control settings (SNMP-V3)

No.	User	Security-level	Auth Priv	Permission
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			

Trap receiver settings

No.	IP address	Community	User	Security-level	Version
1	<input type="checkbox"/> 0.0.0.0	public	---	---	V1
2	<input type="checkbox"/> 0.0.0.0	public	---	---	V2
3	<input type="checkbox"/> 0.0.0.0	public	---	---	V3
4	<input type="checkbox"/> 0.0.0.0	public	---	---	V1

2. Next you need to add a user to the “Access control settings (SNMPv3)” section.
3. Select the number “1” and a new menu will open.



Access control settings (SNMP-V3) - 1

/ network / snmp / snmpv3 / 1

Access control:

User name: test

Security level: Auth/Priv

Authentication protocol: MD5

Authentication password (new):

Authentication password (confirm):

Privacy protocol: DES

Privacy password (new):

Privacy password (confirm):

Permission: Read/Write

4. Fill in the “User name” field, this is a user that is set up for SNMPv3 access in your SNMP browser software.
5. Select your Security level, this should match what is configured in your SNMPv3 software.
6. Select the Authentication protocol, again this must match what is configured in your SNMPv3 software.
7. Supply and confirm the password for the above user, again this must match what is configured in your SNMPv3 software.
8. Next follow the same steps as above for the Privacy protocol.
9. Finally select the appropriate permission level and Save to flash.
10. Now open the main SNMP configuration page again it should look something like this.

SNMP configuration
/ network / snmp

sysContact: administrator
 sysName: Digi Passport
 sysLocation: my location
 sysService: 7
 Options: Trap Email
 EnablePowerOnTrap/Email: Yes Yes
 EnableAuthenTrap/Email: Yes Yes
 EnableLinkUpTrap/Email: Yes Yes
 EnableLinkDownTrap/Email: Yes Yes
 EnableLoginTrap/Email: Yes Yes
 Trap event recipient's email address: jeffn@digicom

Access control settings (NMS)

No.	IP address	Community	Permission
1	<input checked="" type="checkbox"/> 192.168.100.101	digipassport	Read Only
2	<input type="checkbox"/> 0.0.0.0		Read Only
3	<input type="checkbox"/> 0.0.0.0		Read Only
4	<input type="checkbox"/> 0.0.0.0		Read Only

Access control settings (SNMP-V3)

No.	User	Security-level	Auth Priv	Permission
1	<input checked="" type="checkbox"/> test	Auth/Priv	MD5 DES	Read/Write
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			

Trap receiver settings

No.	IP address	Community	User	Security-level	Version
1	<input checked="" type="checkbox"/> 10.9.101.2	---	test	Auth/Priv	v3
2	<input type="checkbox"/> 0.0.0.0	public	---	---	v1
3	<input type="checkbox"/> 0.0.0.0	public	---	---	v2
4	<input type="checkbox"/> 0.0.0.0	public	---	---	v3

11. Next you need to configure the Trap receiver settings. Select number 1 from this section.

12. The resulting menu opens.

Trap receiver settings - 1
/ network / snmp / trap / 1

Trap receiver enable/disable:
 IP address: 0.0.0.0
 Community: public
 Version: v3

13. In this menu select the "Trap receiver enable/disable check box then select v3 from the version dropdown. The resulting menu will open.

Configuring Port Event Handling

Trap receiver settings - 1

/ network / snmp / trap / 1

Trap receiver enable/disable:

IP address: 0.0.0.0

User name:

Security level: NoAuth/NoPriv

Engine ID:

Version: v3

14. In this menu fill in the IP address of the Trap receiver.
15. Fill in the User name, this is the same user from the SNMPv3 software.
16. Select the security level and a new menu will open. It should look this.

Trap receiver settings - 1

/ network / snmp / trap / 1

Trap receiver enable/disable:

IP address: 10.9.101.2

User name: test

Security level: Auth/Priv

Authentication protocol: MD5

Authentication password (new):

Authentication password (confirm):

Privacy protocol: DES

Privacy password (new):

Privacy password (confirm):

Engine ID: 0x800x000x050x230x010

Version: v3

17. Use the same steps as in the “Access control settings” section for the Authentication and Privacy Protocols and their passwords.
18. Fill in the engine ID this is supplied by the SNMPv3 software. Make sure that you delete the spaces from the original engine ID.

Configuring 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.
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" on page 70.

9. Enter the title of the Email (subject line).
10. Enable or Disable Case sensitive.
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.

Config Alerts for Automatic Device Recognition (ADR)

The screenshot shows the Digi Passport 16 Configuration and Management web interface. The user is logged in as 'root'. The left sidebar contains a navigation menu with categories: Network, Serial port (selected), Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. Under 'Serial port', the 'Configuration' sub-menu is selected, showing options for Connection, Port management, Automatic detection, Port title, Host mode configuration, Virtual KVM configuration, Serial port parameters, Port logging, and Port event handling. The main content area is titled 'Keywords Configuration - 1' and shows the configuration for port 1. The 'Monitoring interval (sec, 5-3600):' is set to 5. The 'Keywords Configuration' section includes: Keyword: Alert; Case sensitive: Disable; Email notification: Enable; Title of email: Attention on port 1; Recipient's email address: (empty); SNMP trap notification: Enable; Title of SNMP trap: (empty); Use global SNMP configuration: Enable. At the bottom, there are buttons for 'Save to flash', 'Save & apply', and 'Cancel'.

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.

Config 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 "Configuring Automatic Device Recognition" on page 57.

1. Access the web interface.
2. Under the **Serial Port** heading, Click **Configuration**.
3. Choose All or an Individual port > **Alert Configuration**.

- Follow the Email Alert steps to configure the email alert or follow the SMTP Notification to configure SMTP.

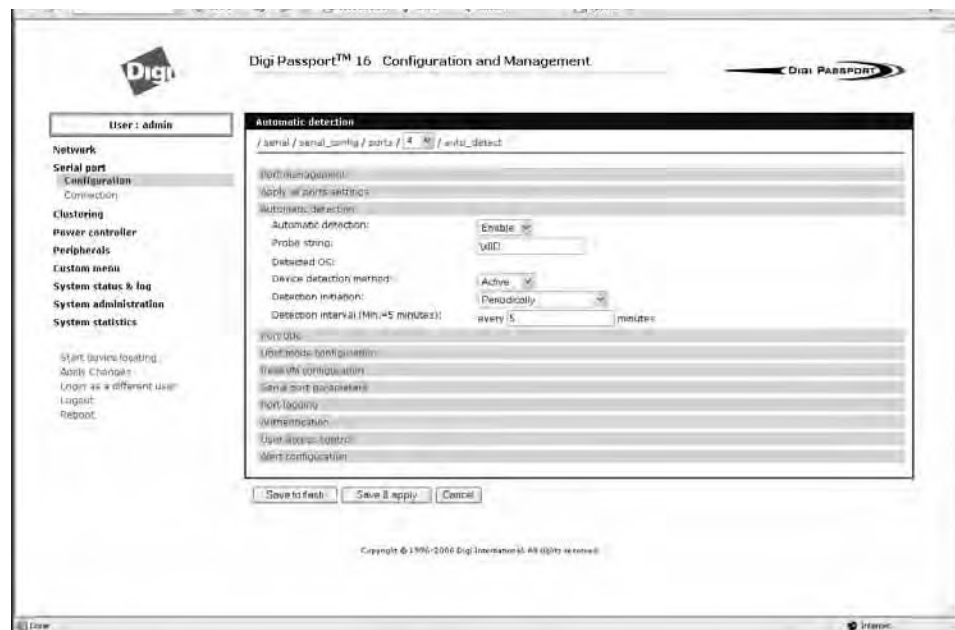
Email Alert

Enable "Email Alert for active detection"
 Enter the Title of email
 Enter Name and email address where the email should be sent.

SMTP Notification

Enable "Active detection trap"
 Configure the trap receiver by one of the following two ways:
 Enter "Use global SNMP configuration"
OR
 Enter the IP address of the trap receiver, the SNMP trap community and select the version

- Complete configuration and choose Save & apply.



Introduction

Intelligent Platform Management Interface (IPMI) is a specification for the equipment that monitors the physical environment and condition of a computer hardware server. The specification is intended to cover the regulation of temperature, voltage and power, and to ensure the proper operation of the firmware.

IPMI works with hardware servers regardless of the operating platform or other software they may run. IPMI allows an administrator to manage multiple servers from a single location by means of a user-friendly interface. Critical system events for each server can be logged. Settings for each basic input/output system (BIOS) can be monitored or changed. Servers can be remotely and independently powered on or off, rebooted, or reset as necessary.

The following instructions explain the method for configuring IPMI including SOL (Serial Over Lan) on a Remote port. Configuring IPMI on a standard serial port is identical except there is no SOL section.

Procedure

1. In the Web select Serial port configuration and then select the port that you want to configure for IPMI.
2. From the menu that opens select "Host mode configuration" from the resulting (shown below) select "Enable" for IPMI and save to flash.

The screenshot shows the 'Host mode configuration' page in a network management interface. The breadcrumb navigation at the top reads: / serial / serial_config / ports / 17 / hostmode. The page is divided into sections: 'Port management' with an 'Apply all ports settings' button, and 'Host mode configuration'. The configuration options are as follows:

Host mode:	Console server
Type of console server:	Other
Enable/Disable IPMI:	Enable
Enable/Disable assigned IP:	Disable
Listening TCP port (1024-65535):	7017
Protocol:	Telnet
Inactivity timeout (1-3600 sec, 0 for unlimited):	0
Enable/Disable port escape sequence:	Enable
Port escape sequence:	Ctrl-z
Port break sequence:	~break
Use comment:	No
Quick connect via:	Local client

3. Next select "Remote port parameters" from the main configuration page. The resulting menu will open.

The screenshot shows the 'Remote port parameters' configuration page in the IPMI interface. The breadcrumb navigation is: / serial / serial_config / ports / 17 / rport_param. The page is divided into several sections: Port management, Apply all ports settings, Port title, Host mode configuration, freeKVM configuration, and Remote port parameters. The 'Remote port parameters' section contains the following fields:

Destination IP:	<input type="text" value="71.216.228.121"/>
Destination port (0-65535):	<input type="text" value="623"/>
Protocol:	<input type="text" value="RMCP+(SOL)"/>
OEM type:	<input type="text" value="None"/>
Allow unattended continuous connection:	<input type="text" value="Disable"/>

Below the 'Remote port parameters' section are other configuration sections: Port logging, Authentication, User access control, Alert configuration, and IPMI configuration.

4. Fill in the Destination IP field with the address of the server you want to monitor. Generally this will be the address assigned to the BMC (Base-board Management Controller).
5. Fill in the Destination port, normally 623 is the port used for IPMI, but this may vary on individual servers.
6. Select the Protocol RMCP+ is the protocol used for SOL.
7. The OEM type should be set to "None" in most cases. You should only use "Intel IPMI 2.0 BMC" if your server has an actual Intel 2.0 BMC.
8. Save to Flash. Next from the main configuration page select "IPMI Configuration" and the resulting menu will open.

IPMI configuration

/ serial / serial_config / ports / 17 / ipmi

Port management

Apply all ports settings

Port title

Host mode configuration

freeKVM configuration

Remote port parameters

Port logging

Authentication

User access control

Alert configuration

IPMI configuration

Destination IP: 71.216.228.121

Destination port: 623

User name: jeffn

Password (new):

Password (confirm):

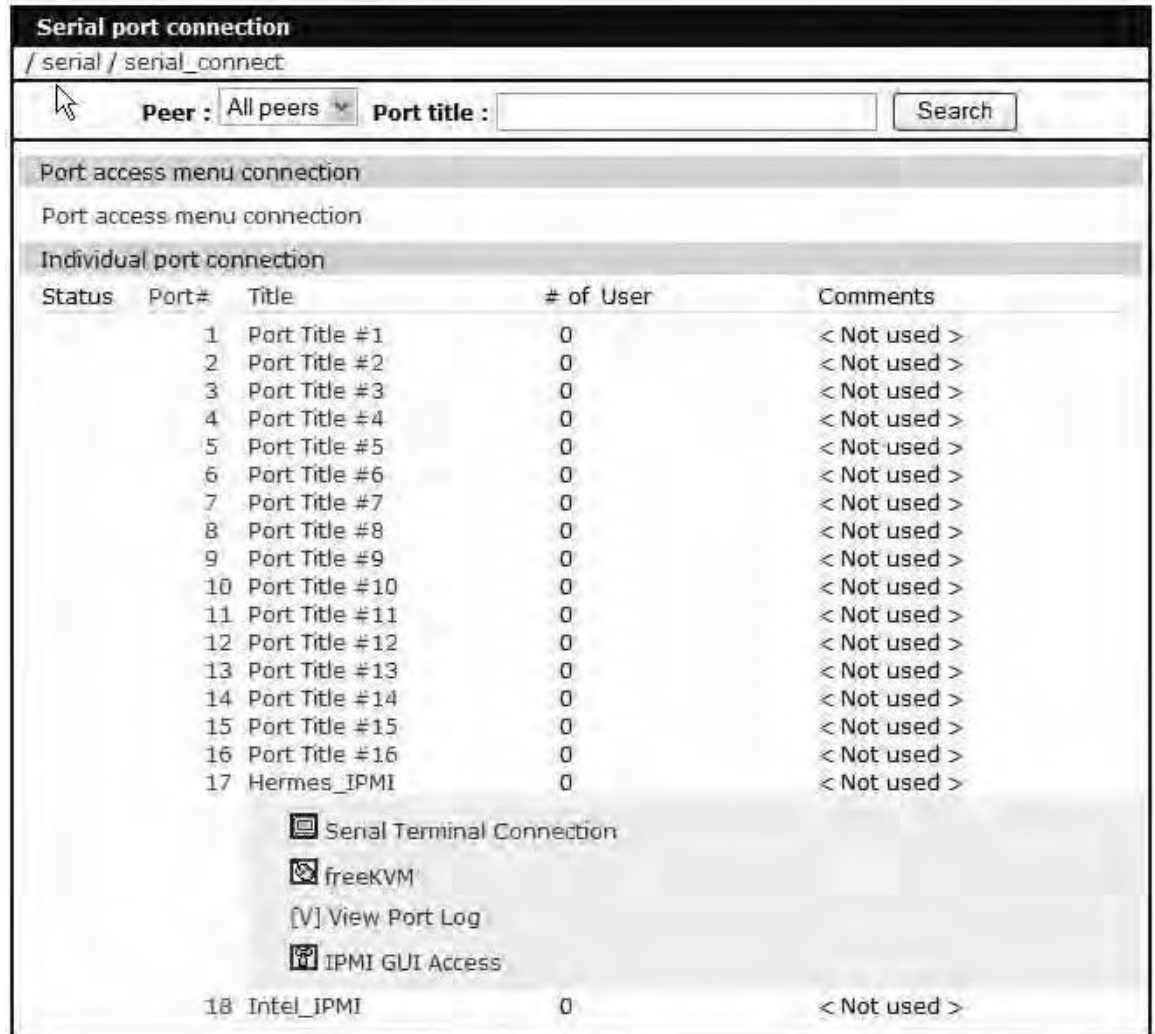
Sensor alert configuration

No.	Sensor type	Email alert	SNMP alert
		Nothing	
New	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

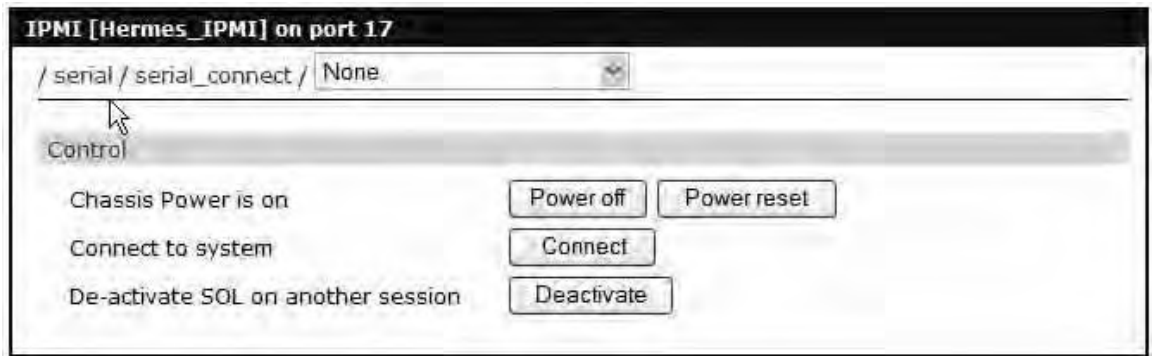
9. Fill in the Destination IP field with the address of the server you want to monitor. Generally this will be the address assigned to the BMC (Base-board Management Controller). If you are using a remote port this value will be supplied from the “Remote port parameters”.
10. Fill in the Destination port, normally 623 is the port used for IPMI, but this may vary on individual servers. If you are using a remote port this value will be supplied from the “Remote port parameters”.
11. Fill in the “User name” field. This is a user configured on the server that can access the BMC.
12. Supply and confirm the password for the above user.
13. Sensor alert configuration is where you can create a list of sensors on your server that you would like to receive notifications from.

Connecting to your server via IPMI

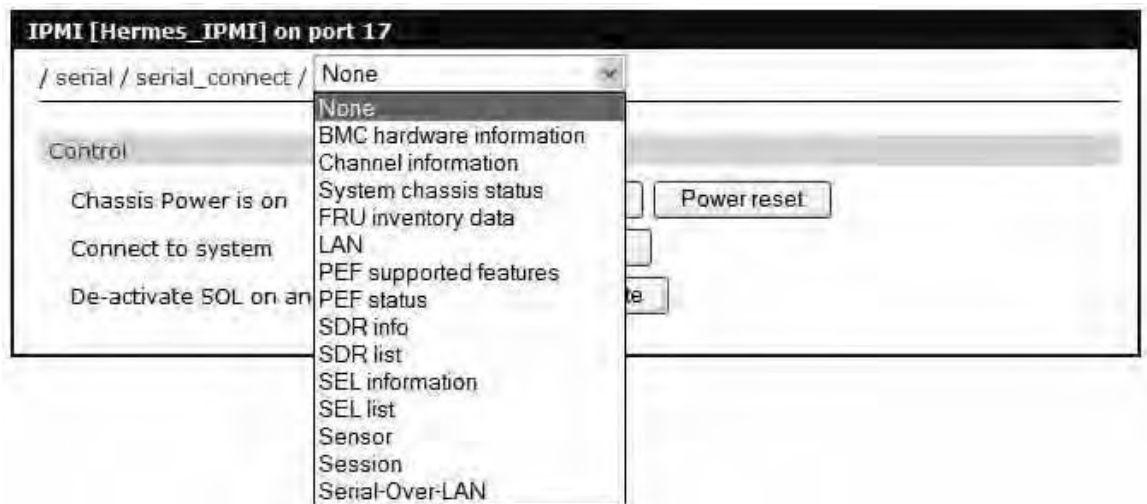
1. To connect to your server via the IPMI GUI select the serial port connection page.
2. Select the serial port that is configured for IPMI and the resulting menu will open.



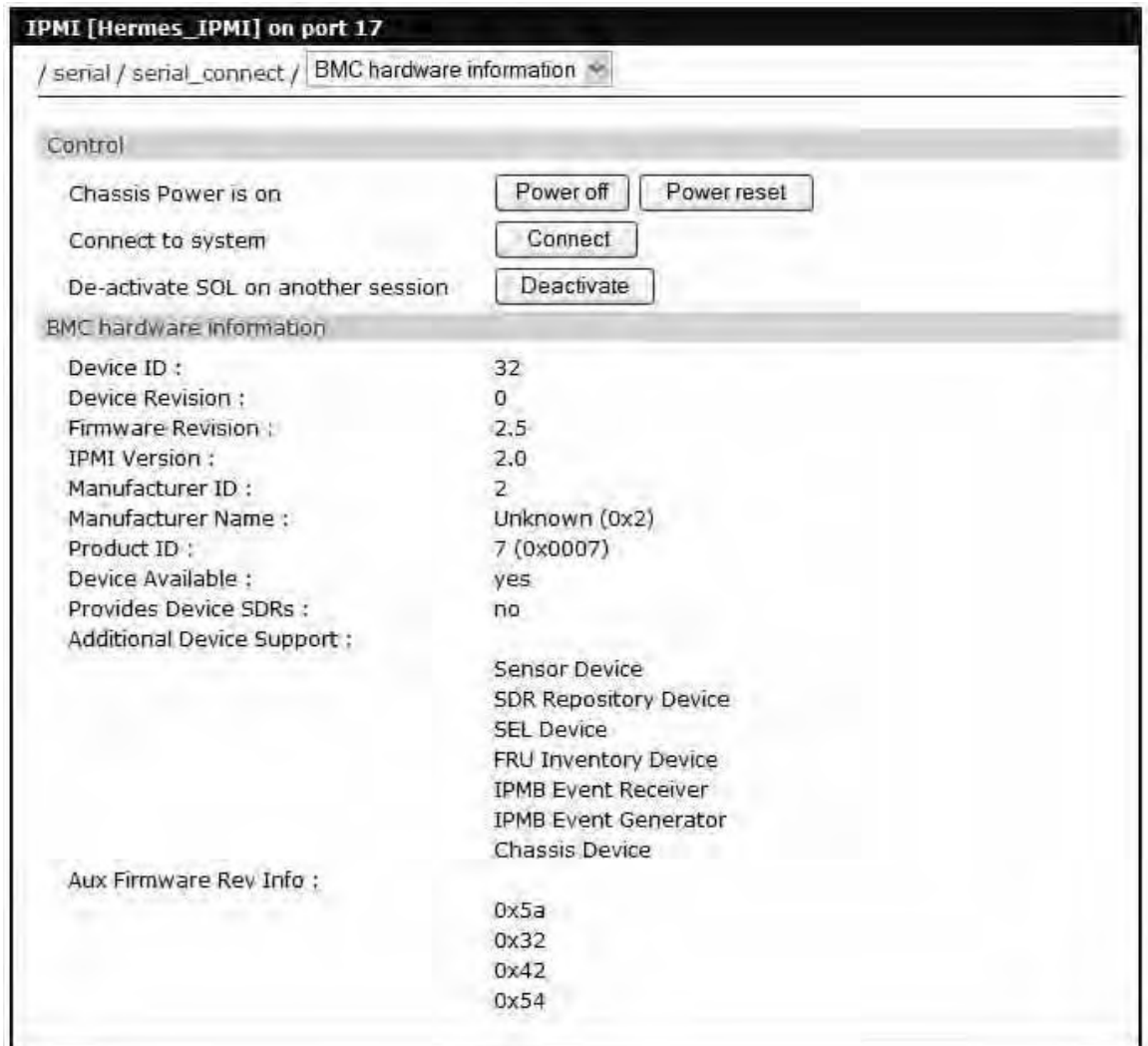
3. Select the "IPMI GUI Access" link this will connect to your server via IPMI. The resulting page will open.



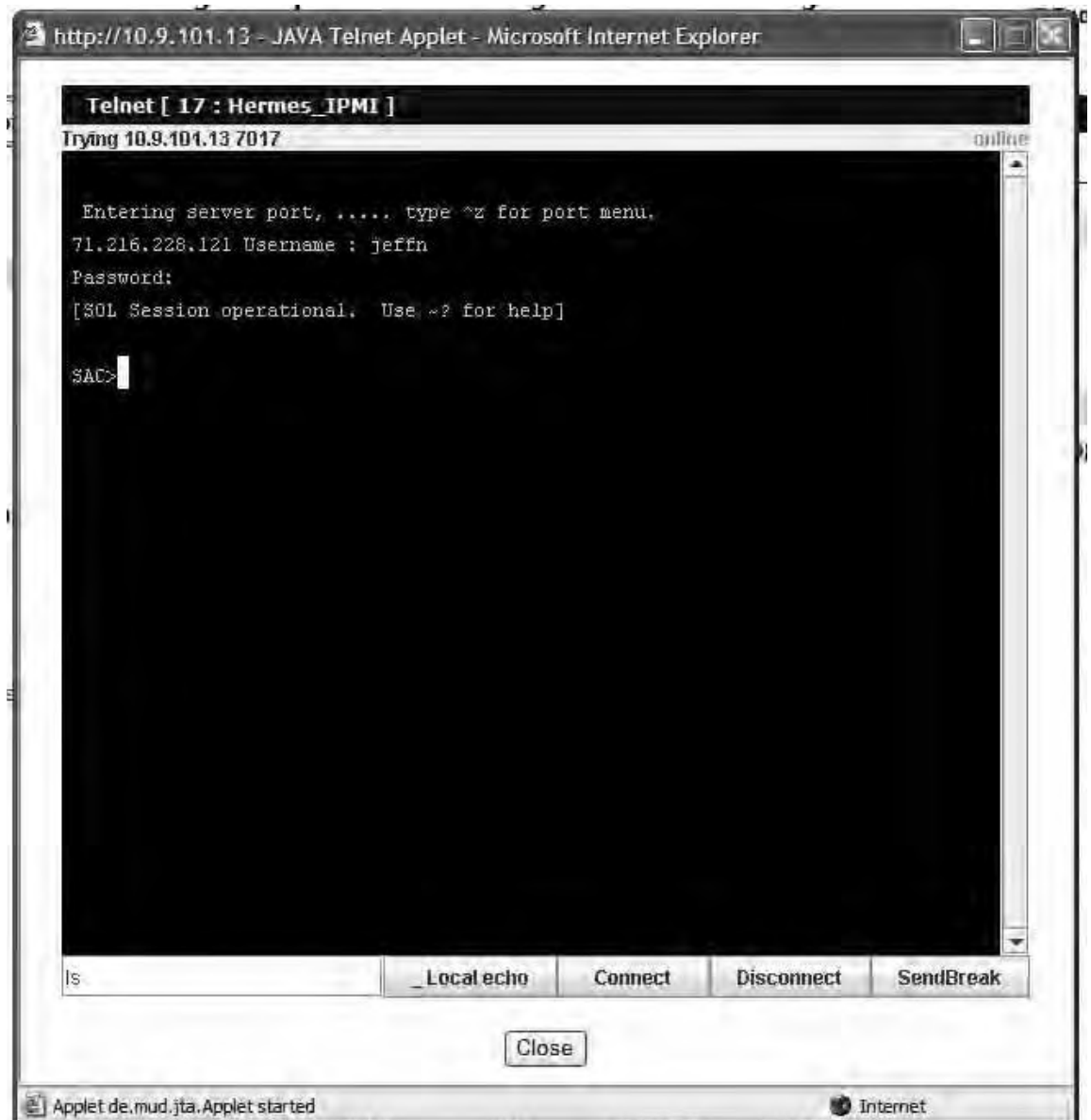
4. From this page you can choose which BMC statistics to monitor, power cycle the server or make an SOL connection to the server's console port.
5. To choose what you would like to monitor click the drop down arrow and a list will open.



6. In the example shown below we have chosen BMC hardware information. The resulting page is displayed. The information displayed on this page will vary between server manufacturers.



7. To make an SOL connection to your servers console port click the “Connect” button the resulting window will open. The example shown below is a console connection to a Windows 2003 servers SAC port.



User, Security, and Authentication Configuration and Administration

Introduction

The Digi Passport 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 Passport 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 <http://support.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.

Configuring User Access Control

Another method for controlling access to the serial ports on the Digi Passport 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

Configuring User Access Control

details about adding users, see "Administering Users" on page 69.

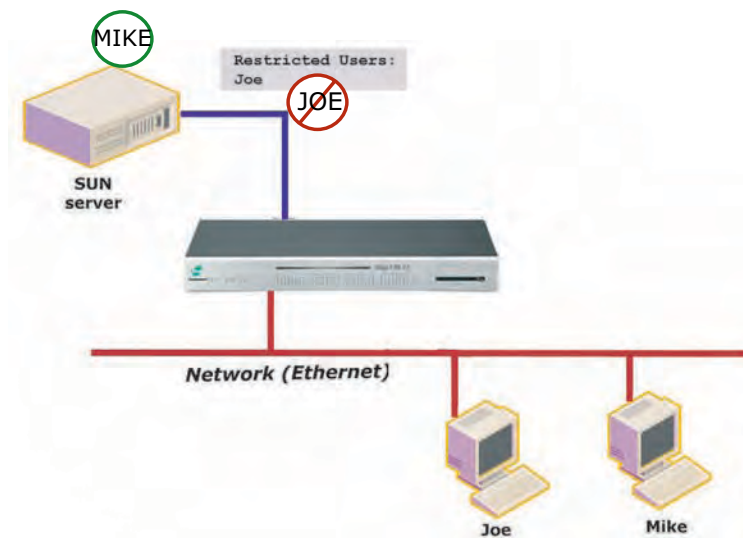
Note: Users do not need to be configured locally; they can be defined on a remote authentication server.

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" on page 70.

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.

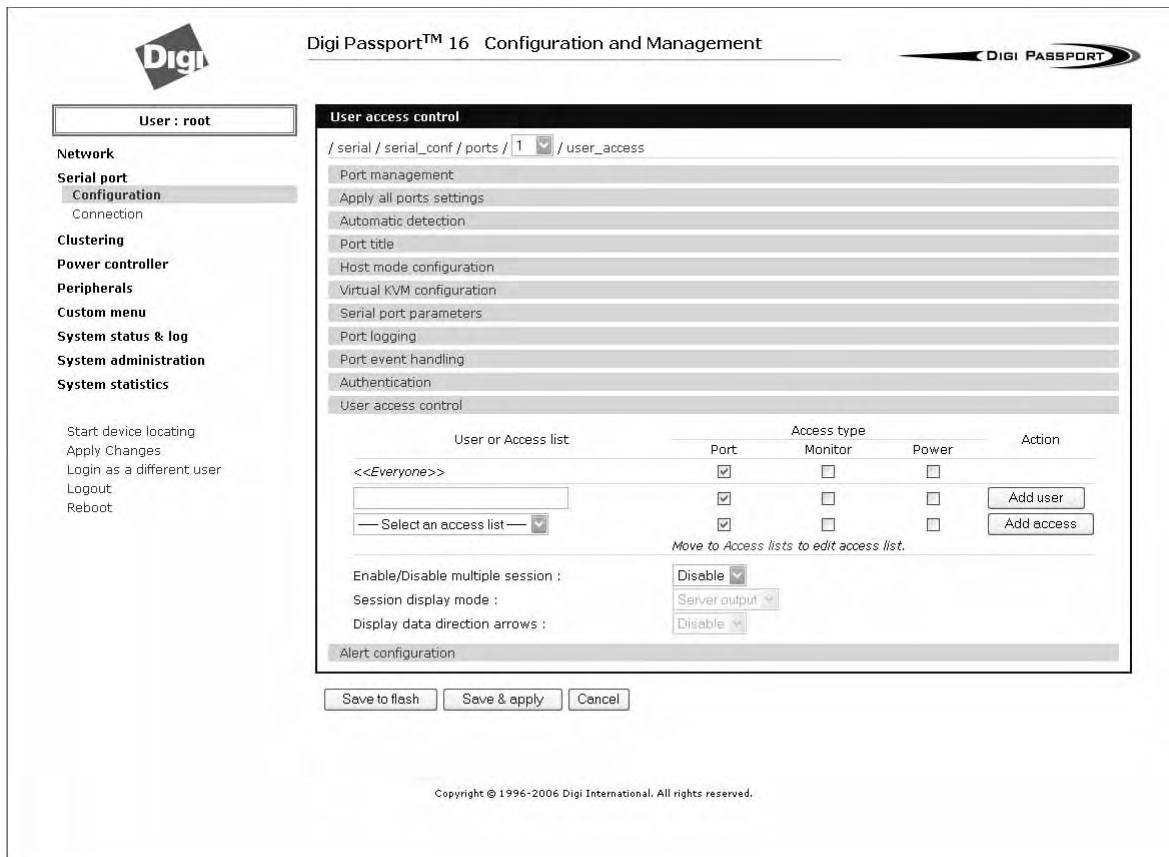
If you do not check <<Everyone>>, no users are allowed to access this port unless they are individually listed.

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

In the next example, three users are configured on the Digi Passport 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 "Create an Access list" on page 70.



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 (Here it is ronk).
4. Enter the privileges this user has. (Notice that <<Everyone>> has more access than ronk does.)

The screenshot shows the 'User access control' configuration page. The breadcrumb path is '/ serial / serial_conf / ports / 1 / user_access'. The page contains a table with the following data:

User or Access list	Access type			Action
	Port	Monitor	Power	
<<Everyone>>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ronk	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Remove
<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Add user
<input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Add access

Below the table, there are three dropdown menus for session and display settings:

- Enable/Disable multiple session : Disable
- Session display mode : Both
- Display data direction arrows : Disable

At the bottom of the page, there are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'.

Note: The usernames and passwords on the Digi Passport 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.

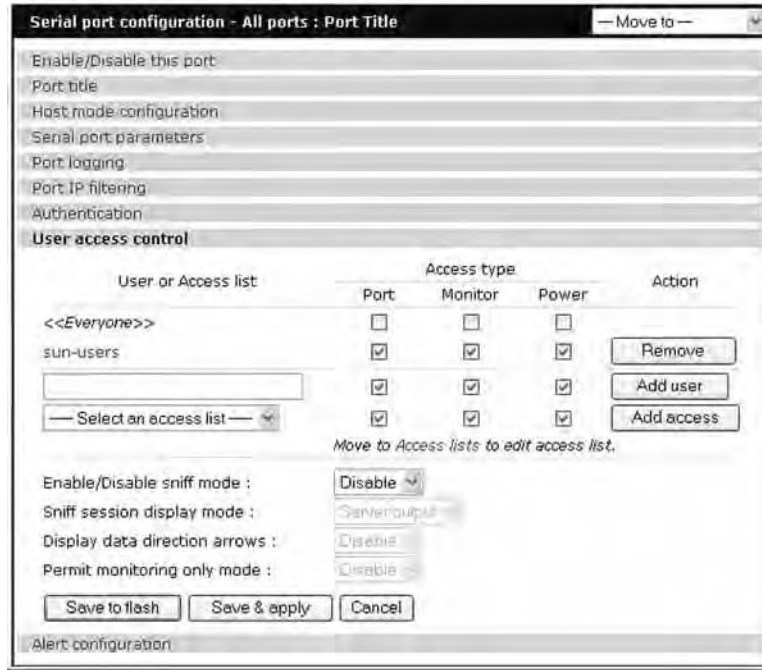
Change the Privileges of an Access List

1. On the same screen shown in the previous procedure, select an access list from the drop-down box.
2. Click the Add access button, and then click and the Save & apply button.

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.

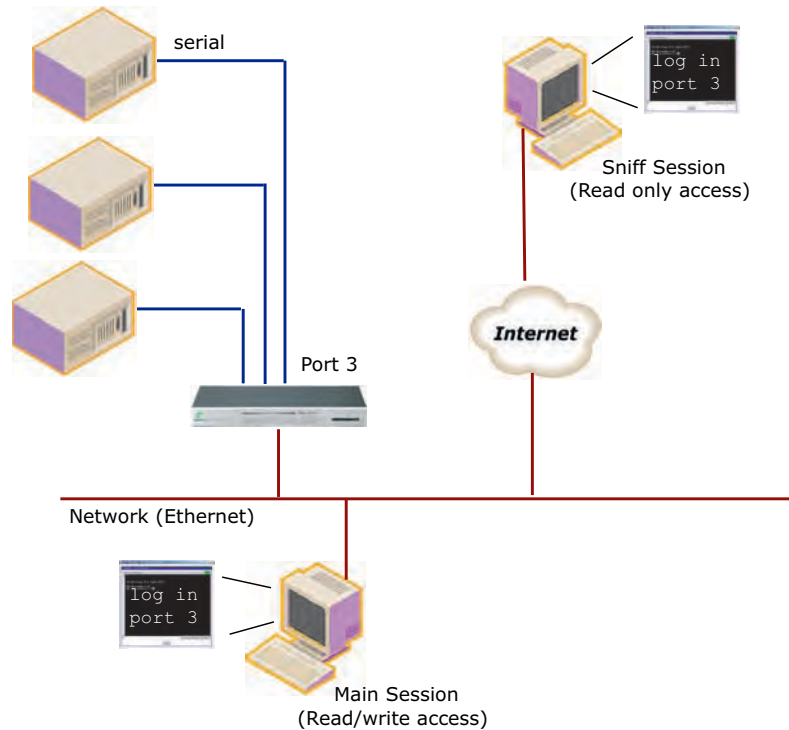
User, Security, and Authentication Configuration and Administration



Type 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 Passport 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" on page 21.

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 Passport. These are the available control mechanisms:

- System Security
- Password Security (Force heightened)

System Security

- SNMP

The Passport 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 require encrypted connections.

- 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 Passport using the Web interface. By default, HTTP is redirected to HTTPS.

- HTTPS

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

Password Security

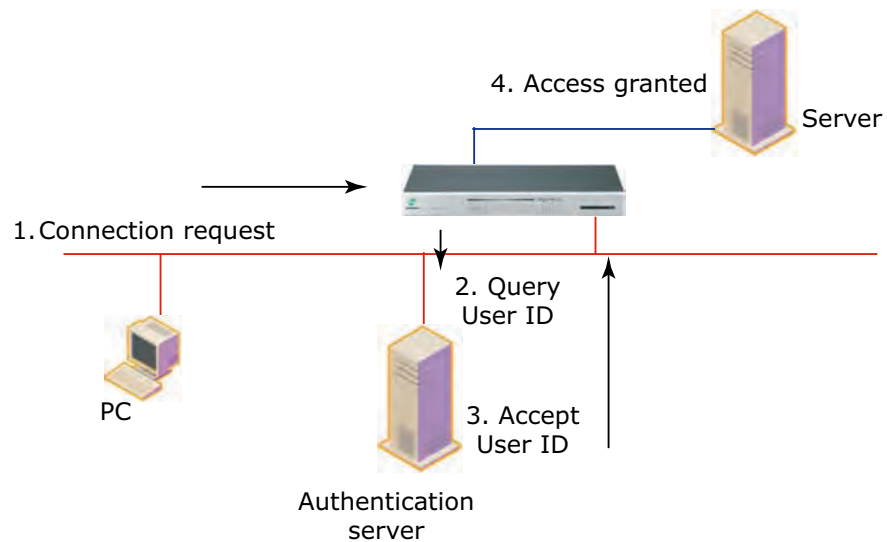
To enhance password security, you can use these settings:

- 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, or exceed Minimum password length if larger. Passwords can be up to 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 Passport 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.



Configuring Authentication Methods for Port Access

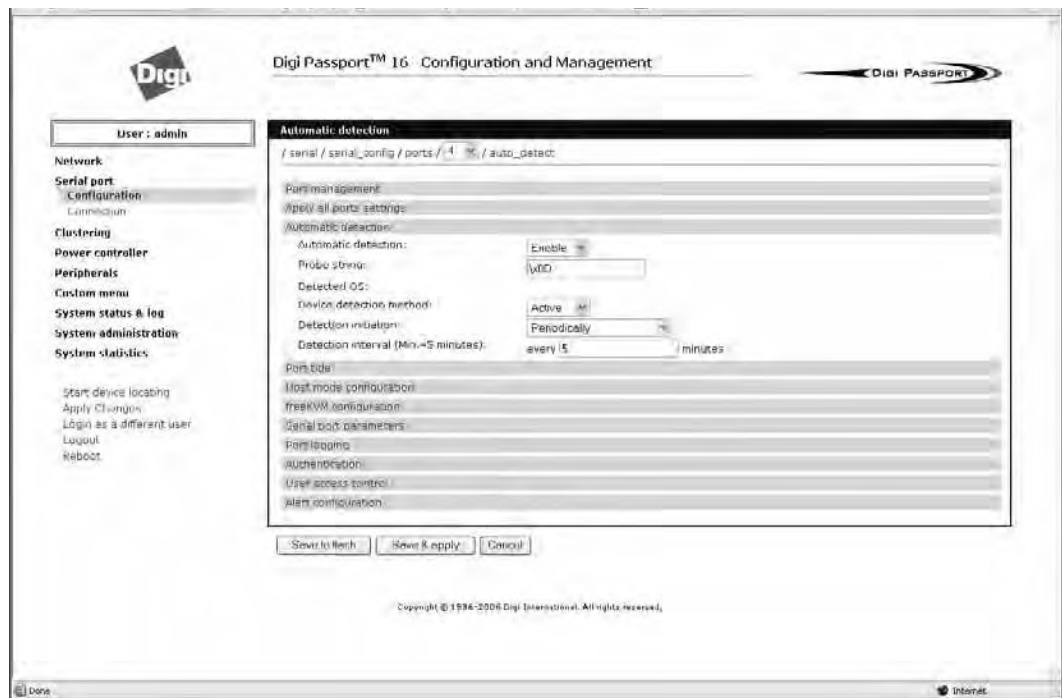
You can choose between having a single authentication method, such as RADIUS, or an authentication method where a Local authentication service is used in addition to the RADIUS, LDAP, TACACS+ server, or Kerberos. These options are listed when you configure the Digi Passport unit for authentication. To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

1. Access the web interface.
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.

Note: Under Serial port > Connection, The “# of User” column shows how many users are actually connected to the port and the username of the read/write user.



Configuring Authentication for the Web Server

1. Access the web interface.
2. Choose **Network > Web server configuration**.
This screen opens.
3. Choose an authentication method and then **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 Passport will authenticate against the local database instead of the remote one. For details, see "Administering Users" on page 69.

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

LDAP Authentication

The Digi Passport 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 Passport unit authenticates against an LDAP directory, all users must be configured in one container. The Digi Passport 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 Passport 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 Passport 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 be compiled for the Digi Passport unit's environment.

Digi offers an SDK for the Digi Passport family.

To download the SDK, contact technical support at support.wizards@digipass.com

1. Place the custom PAM modules onto: `/usr2` on the Digi Passport unit.
2. Use an scp client (like WinSCP) to copy data to the `/usr2` directory, or use scp or ftp client on the Digi Passport unit to upload the file while logged in as root.
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)

Samba configuration>

Samba server

Make a shared folder to use a Windows machine for a Samba server. For a Linux machine, run `smb service`.

Passport

[Network->Samba configuration]

Samba service: Enable

Samba configuration>

Samba server name: *IP address or Computer name of Samba server*

Mounting path on Samba server: *shared folder name* (should be started with '/'
' e.g. /share)

Samba timeout (sec, 5-3600): 5 (this is a default value)

Samba mount retrying interval (sec, 5-3600): 5 (this a default value)

Samba server user: *User name* of Samba server

Samba server password: *Password* of the user

Note: Samba directory will be mounted on /mnt/smb directory in passport.

Chapter 9**Custom and Default Menus****Introduction**

The Digi Passport 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 command line (serial, telnet, or ssh) connections.

Making 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.

Adding Users

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

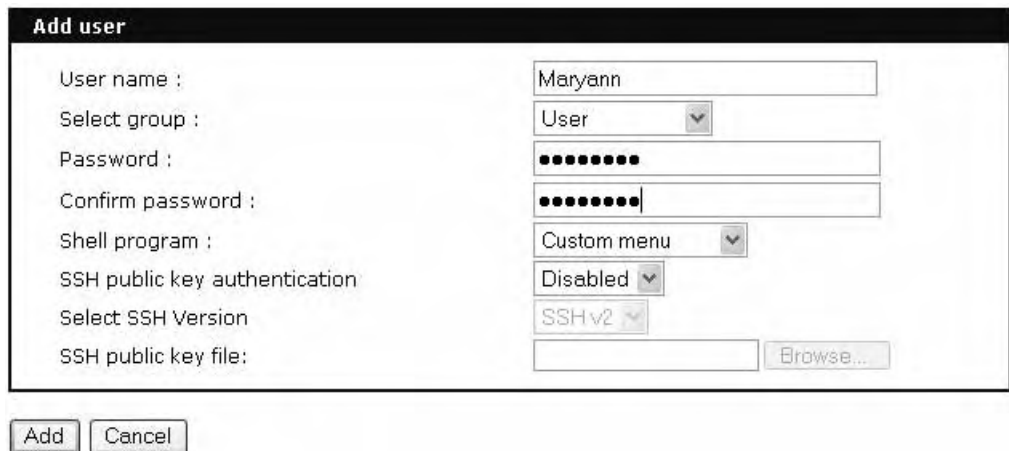
1. Access the web interface.
2. **System administration > Users administration > Add**

The screenshot shows the 'User administration' web interface. At the top, there are input fields for 'User name' and 'User group' (set to 'All group'), and a 'Search' button. Below this is a table titled 'Current local users' with columns for '#', 'User name', 'User group', and 'Shell'. The table lists four users: 1 (Gilligan, Port admin, Configuration menu), 2 (Skipper, System admin, CLI), 3 (admin, System admin, Configuration menu), and 4 (root, Root, CLI). At the bottom of the table are 'Add', 'Edit', and 'Remove' buttons.

#	User name	User group	Shell
1	Gilligan	Port admin	Configuration menu
2	Skipper	System admin	CLI
3	admin	System admin	Configuration menu
4	root	Root	CLI

Making Custom Menus

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.



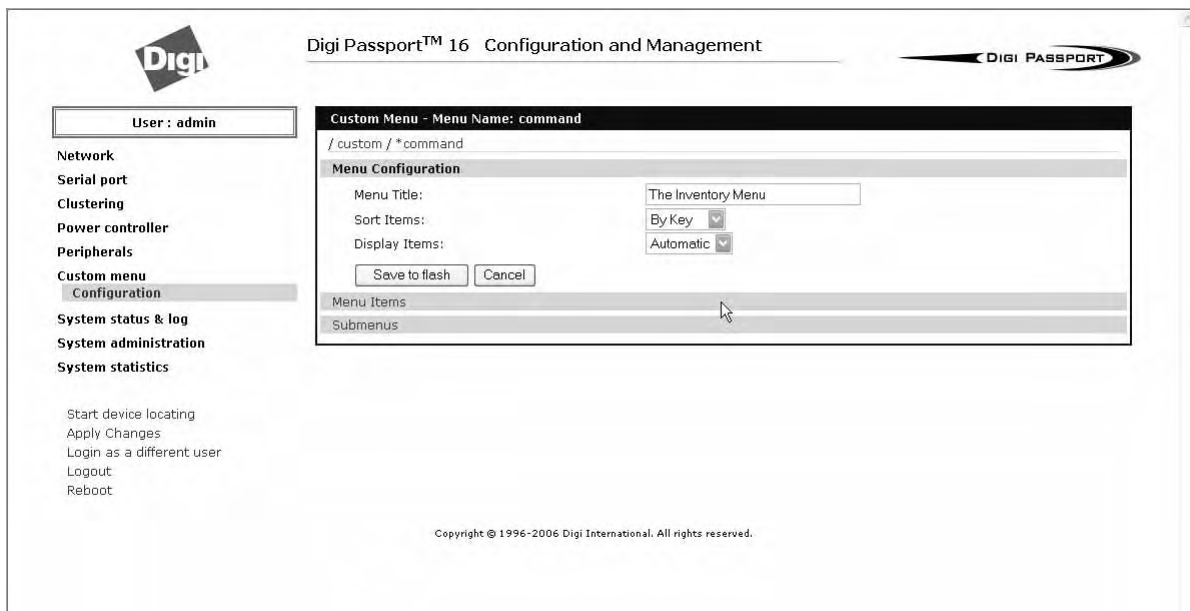
4. Click Add to add the user.
5. Continue to add users as needed.

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

Creating Menu Names

To make a custom menu, do the following:

1. Access the web interface.
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.



6. Click Save & apply.

7. Repeat as required to create additional menus.

Adding 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.

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.

Default Menu

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.

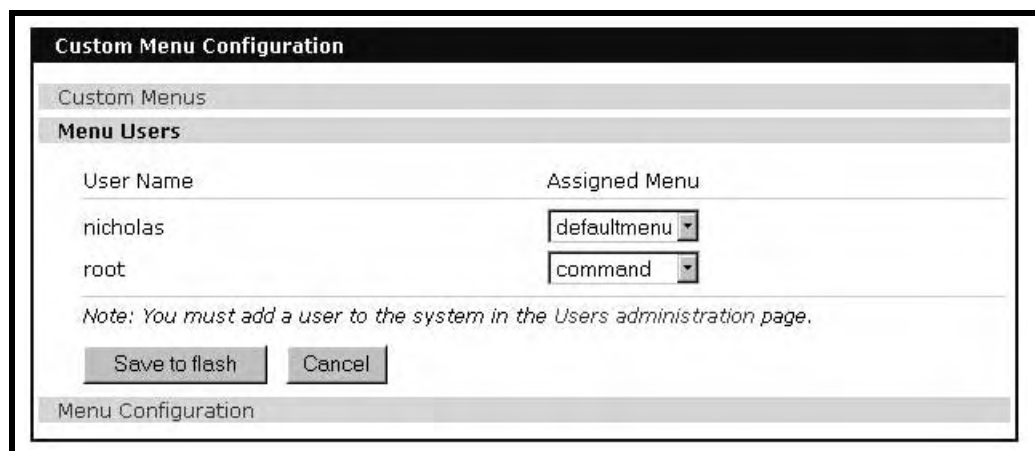
Note: To add or configure submenus, select the Submenus hyperlink on the Menu Configuration page.

Assigning 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.
2. **Configuration > Custom Menu > Menu Users.**

A list of available users is displayed.



The screenshot shows a web interface titled "Custom Menu Configuration". Under the "Menu Users" section, there is a table with two columns: "User Name" and "Assigned Menu". The "User Name" column lists "nicholas" and "root". The "Assigned Menu" column shows dropdown menus with "defaultmenu" and "command" selected respectively. Below the table, there is a note: "Note: You must add a user to the system in the Users administration page." At the bottom of the form, there are two buttons: "Save to flash" and "Cancel".

User Name	Assigned Menu
nicholas	defaultmenu
root	command

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 PortAccess menu:

- Assigned IP address (see "Configuring Host Mode" on page 62)
- 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 chapter "Administering Users" on page 69)
- By calling "portaccessmenu" from the command line

The PortAccess menu allows simple access to each port.

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

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

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

About the Digi Passport Unit's Support for Microsoft Windows Server 2003

The Digi Passport 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 International versions of SAC are now supported. When a server running Windows Server 2003 is connected to the Digi Passport 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.

Manage [MS SAC] on port 1	
System	
System Name:	WHQLED
Operating System:	Windows Server 2003 Enterprise Edition
OS Version:	5.2
Service Pack:	None
System date/time:	04/30/2003 20:31:04 (GMT)
Time since last restart:	2 seconds.
Control	
<input type="button" value="Connect"/>	Connect to Microsoft SAC console
<input type="button" value="Restart"/>	Restart system
<input type="button" value="Shutdown"/>	Shutdown system
Performance	
Processes	
Serial Port Log	
IP Settings	

Setup Overview

Setup for the Digi Passport 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. For further information please refer to Setting Up the Windows Server 2003 Port below.
2. Cable the console port on the Windows Server 2003 to the Digi Passport unit's port.
3. Set up the Digi Passport unit for SAC support. See "Setting Up the Digi Passport Unit for SAC Support" on page 108.

Setting 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

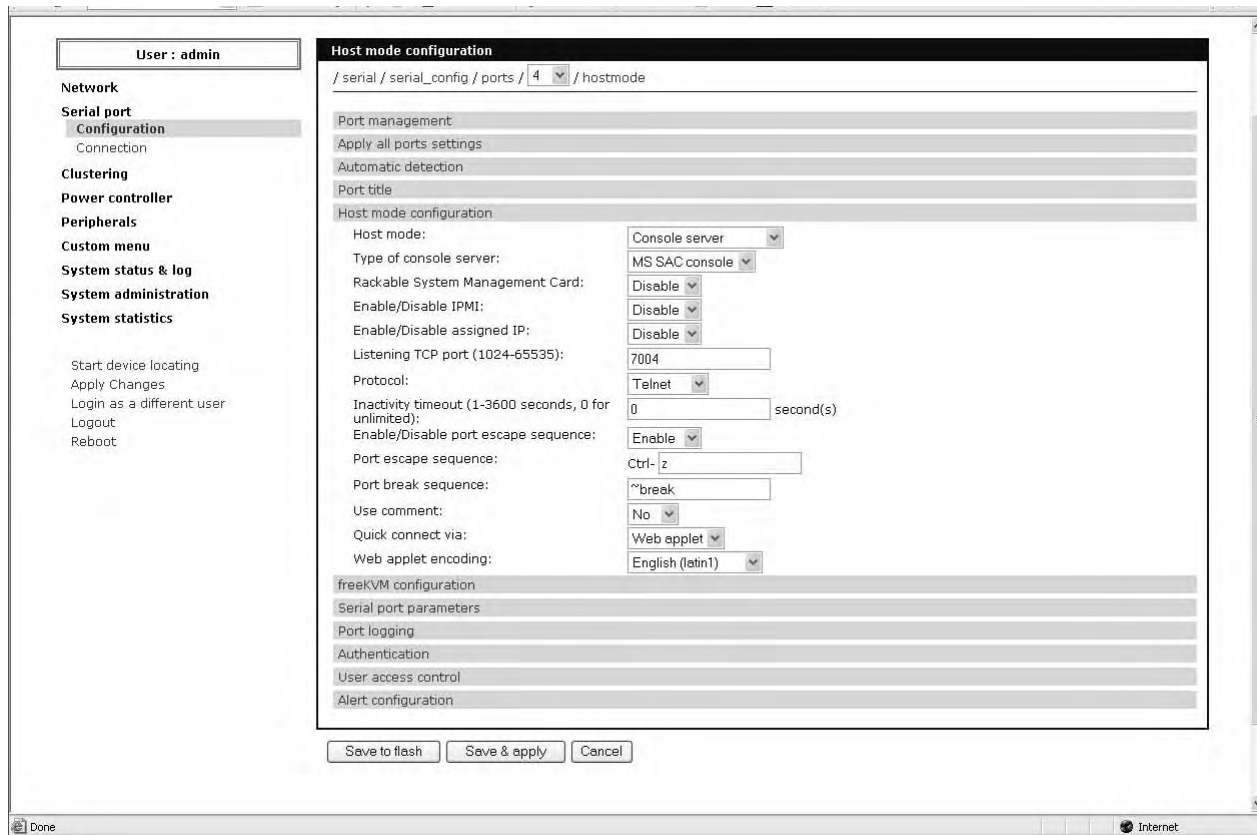
In this example, console output is redirected to COM 2, the boot entry is specified as 1, and the port speed set to 115200.

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

Setting Up the Digi Passport 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.
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 International) 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.

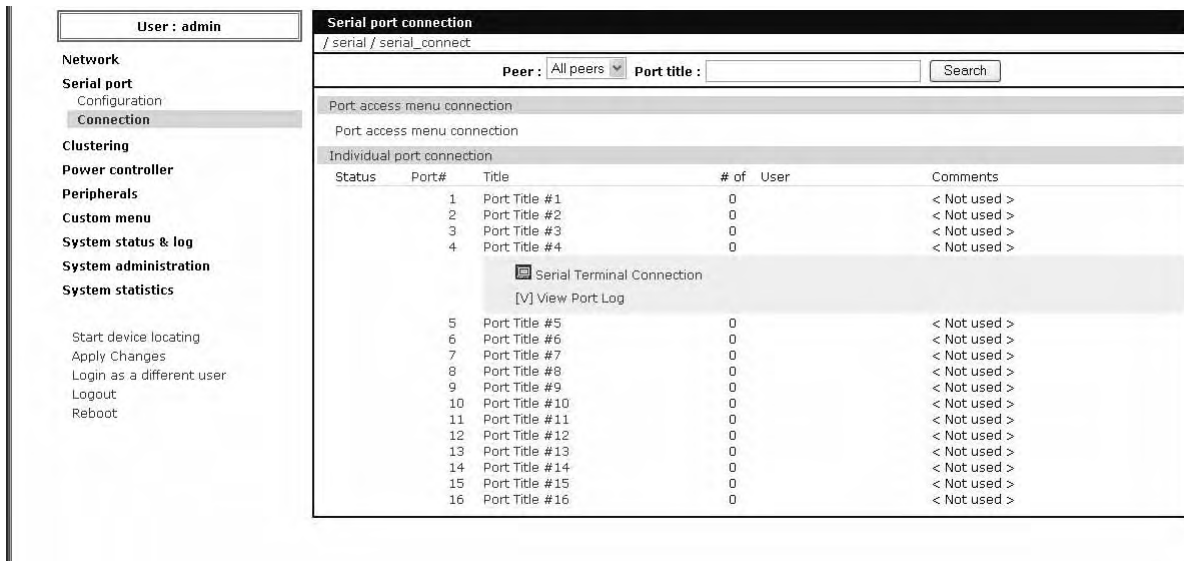
Accessing the Windows Server 2003 Console Port from the Digi Passport Unit's GUI

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

1. Access the web interface.
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.

Note: If support for "Windows Server 2003" and "Rackable Systems Management Card"

Accessing the Windows Server 2003 Console Port from the Digi Passport Unit's GUI



is selected a menu will appear and you must choose between the two functions.

- Use the Digi Passport 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.
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. However, the IP settings are only temporary, you cannot change the IP settings permanently through this method.

Introduction

The Digi Passport provides a method for gaining access to the graphical interface of a system using the network. Using this method, FreeKVM, 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
- Web redirection
- A user-defined option

An Example Configuration

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

The screenshot shows the Digi Passport 16 Configuration and Management interface. The top bar includes the Digi logo, the title 'Digi Passport™ 16 Configuration and Management', and the Digi Passport logo. On the left is a navigation menu with categories like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled 'Serial port connection' and shows a table of port configurations. The table has columns for Status, Port#, Title, # of, User, and Comments. A search bar is located at the top of the table area. Below the table, there are checkboxes for 'Serial Terminal Connection' and 'freeKVM', along with a '[V] View Port Log' link.

Status	Port#	Title	# of	User	Comments
	1	Port Title #1	0		< Not used >
	2	Port Title #2	0		< Not used >
	3	Port Title #3	0		< Not used >
	4	Port Title #4	0		< Not used >
	5	Port Title #5	0		< Not used >
	6	Port Title #6	0		< Not used >
	7	Port Title #7	0		< Not used >
	8	Port Title #8	0		< Not used >
	9	Port Title #9	0		< Not used >
	10	Port Title #10	0		< Not used >
	11	Port Title #11	0		< Not used >
	12	Port Title #12	0		< Not used >
	13	Port Title #13	0		< Not used >
	14	Port Title #14	0		< Not used >
	15	Port Title #15	0		< Not used >
	16	Port Title #16	0		< Not used >
	17	test	0		< Not used >

Free Protocols

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

Free Protocol	Tested Client Software
Remote Desktop	Windows 2000, XP, 2003 Remote Desktop Client Linux: rdesktop
VNC	Windows: tightVNC, realVNC, UltraVNC Linux: vncviewer
X Window System	Windows: Xmanager Linux/Unix: X Window System

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

Using FreeKVM with Remote Desktop Protocol

This section describes how to:

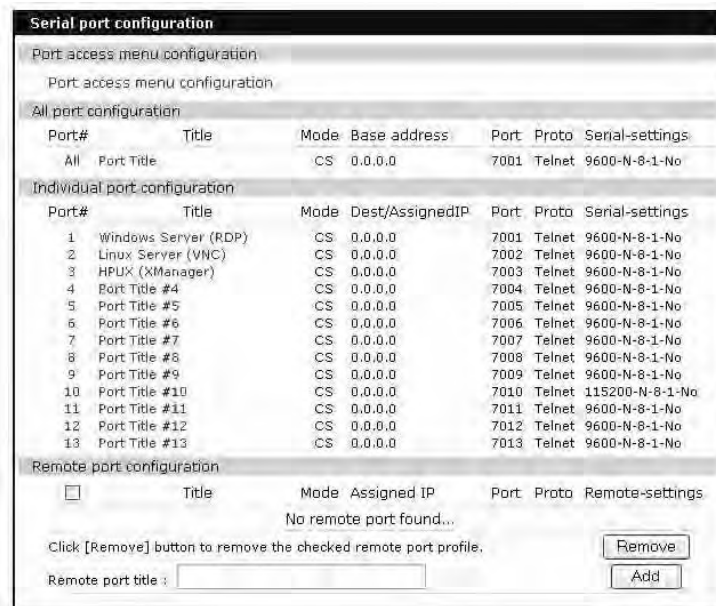
- Configure FreeKVM with Remote Desktop Protocol
- Connect to a system through FreeKVM using Remote Desktop Protocol

Configuring

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

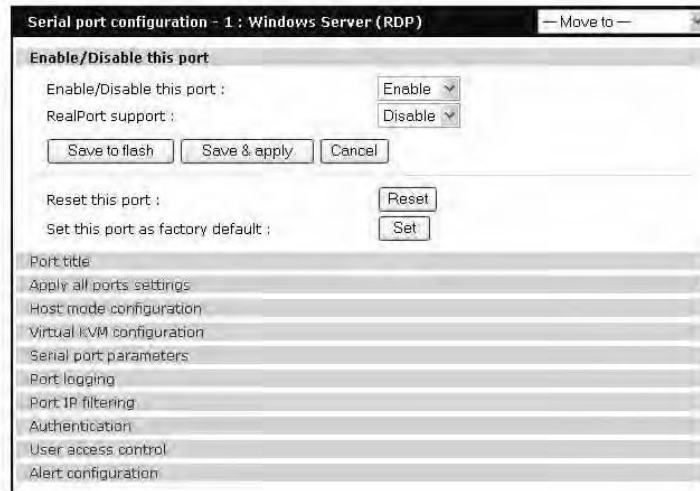
1. Access the Digi Passport Web interface and log in.
2. Choose Serial Port > Configuration.

This window opens:



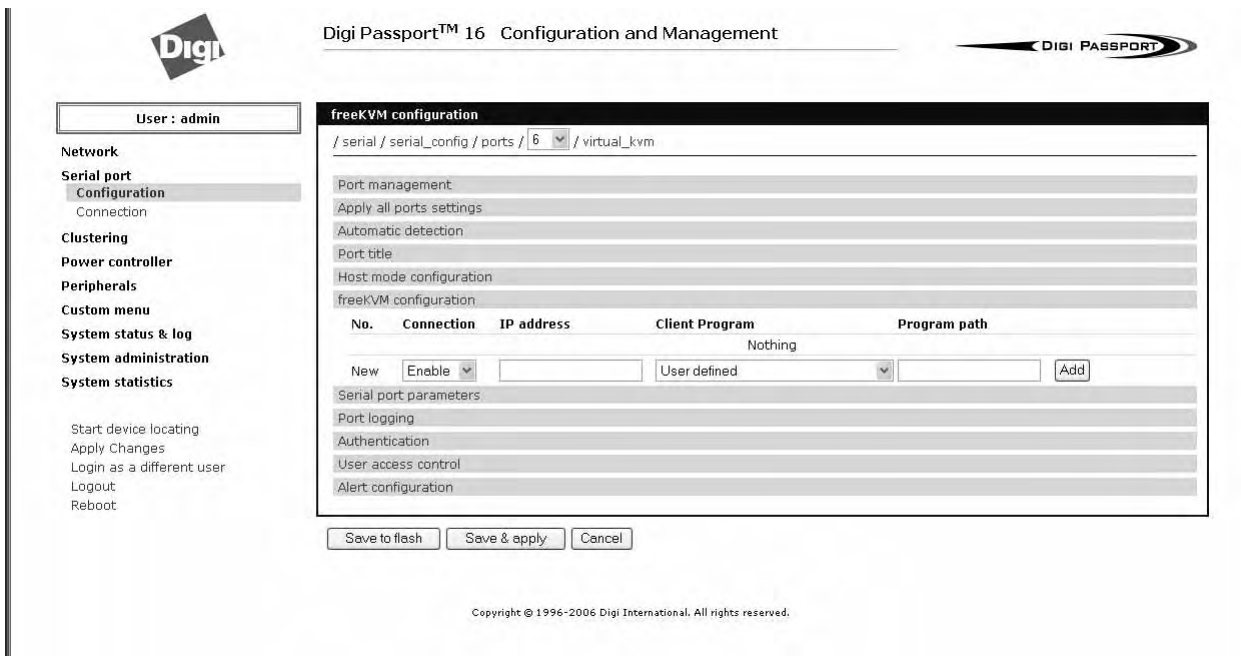
3. Choose the port you want to configure, and then select the FreeKVM tab. (In this example, port 1 is selected.)

A window similar to this one opens, showing the serial port number and title:



4. Click FreeKVM configuration.

This window opens:



5. From the drop-down list next to FreeKVM configuration, select Enable.

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

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

7. 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

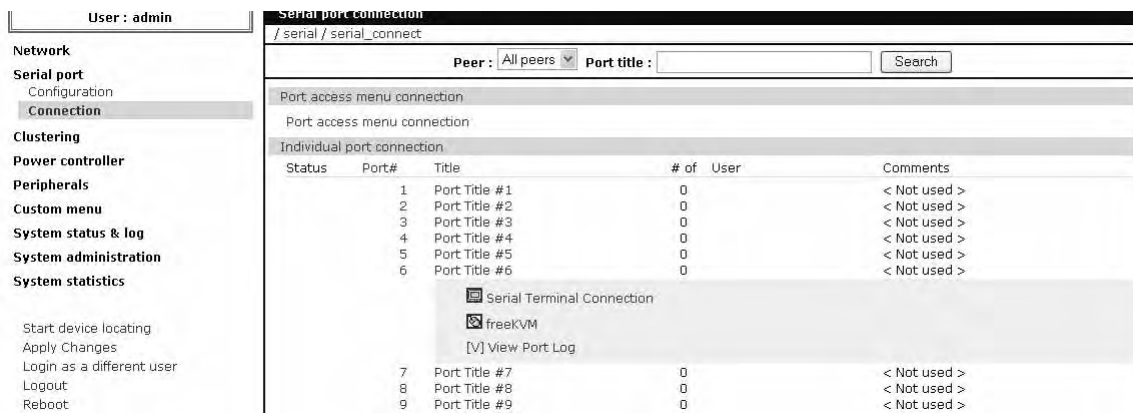
Using FreeKVM with VNC Protocol

SAC console before you configure the FreeKVM feature for the port. For more information, see "Setting Up the Digi Passport Unit for SAC Support" on page 108.

Connecting to a system through FreeKVM using Remote Desktop Protocol

When you connect through the Connection window, and a FreeKVM 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 FreeKVM graphical interface
- The manage button, which connects to the SAC GUI screen



To connect through FreeKVM using Remote Desktop, follow these steps:

1. Click on the mouse icon.
2. Click OK in each of the three Java confirmation request windows.
3. The application starts and you see a message that the connection succeeded:

This login screen opens:



4. 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 "Installing Programs for FreeKVM" on page 122.

Using FreeKVM with VNC Protocol

This section describes how to:

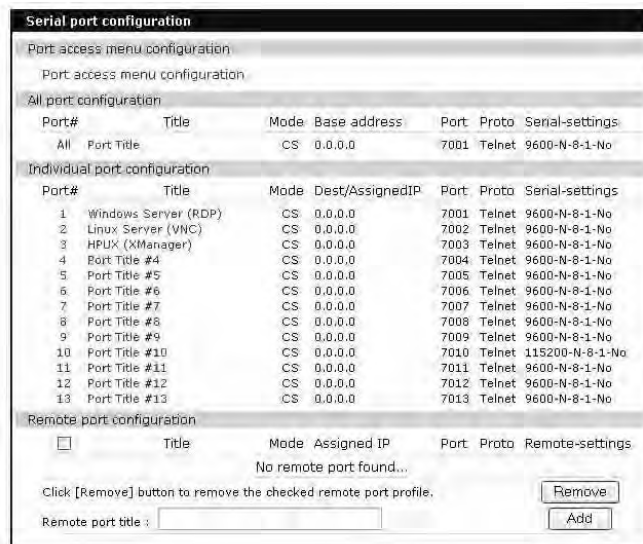
- Configure FreeKVM with VNC Protocol
- Connect to a system through FreeKVM using VNC Protocol

Configuring

To configure FreeKVM with VNC protocol, follow this procedure:

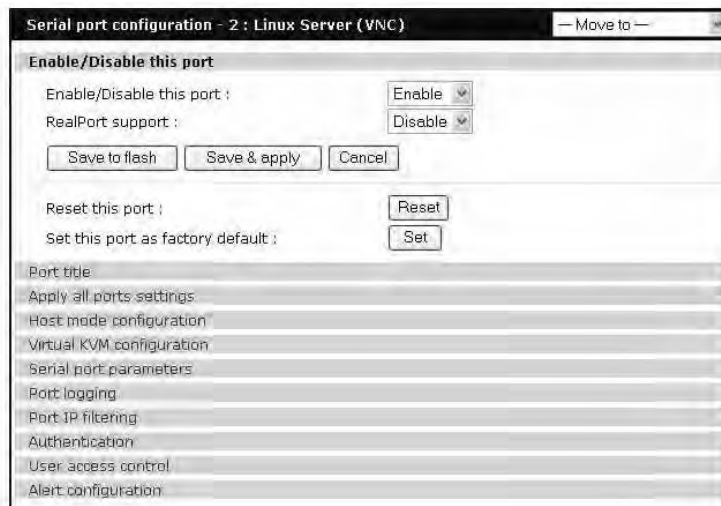
1. Access the Digi Passport Web interface and log in.
2. Choose Serial Port > Configuration.

This window opens:



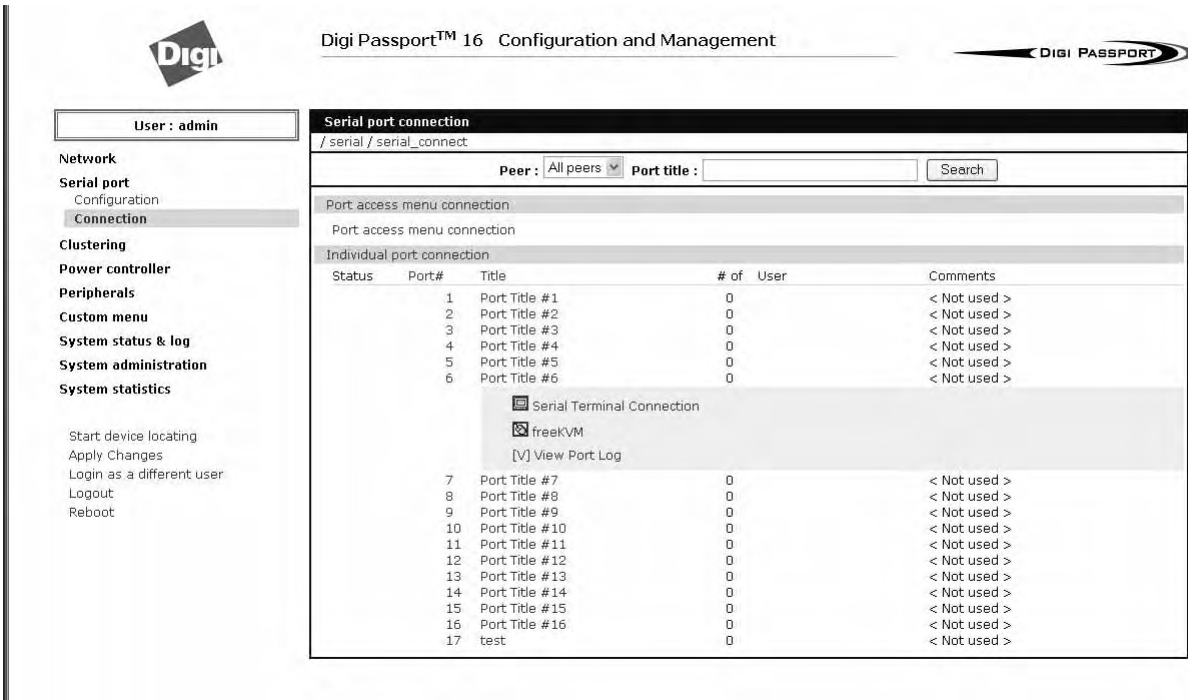
3. Double-click the port you want to configure.

A window similar to this one opens, showing the serial port number and title:



4. Select the FreeKVM tab.

This window opens:



5. From the FreeKVM connection drop-down list, select Enable.

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

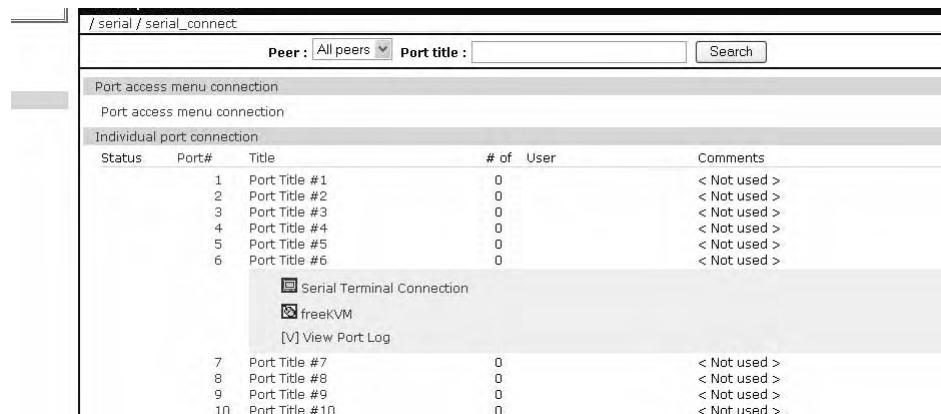
6. Adjust the VNC socket/screen number, if necessary (the default is 1).

7. Click on the Save & Apply button.

Connecting to a system through FreeKVM using VNC

When you connect through the Connection window, and a FreeKVM 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 FreeKVM graphical interface

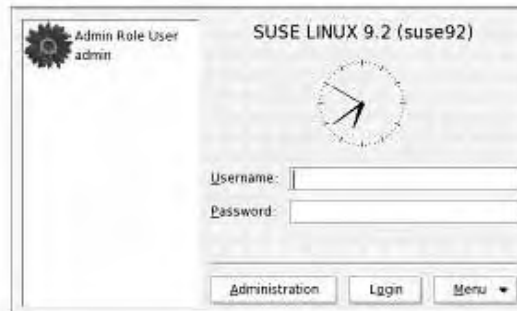


To connect through FreeKVM using VNC:

1. Click on the mouse button.
2. Click OK in each of the three Java confirmation request windows.

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

The FreeKVM VNC Connection opens:



3. 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 "Installing Programs for FreeKVM" on page 122.

Using FreeKVM with X Window System Protocol and XManager Software

This section describes how to:

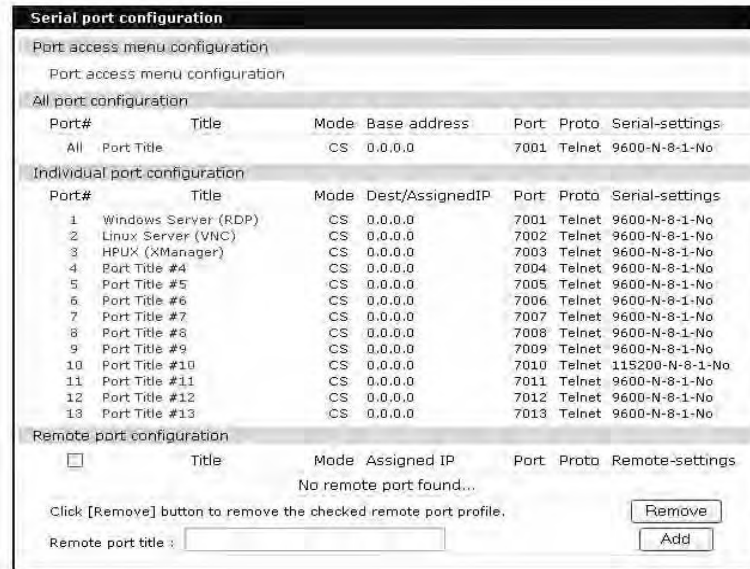
- Configure FreeKVM with X Window System Protocol and XManager Software
- Connect to a system through FreeKVM with X Window System Protocol and XManager Software

Configuring

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

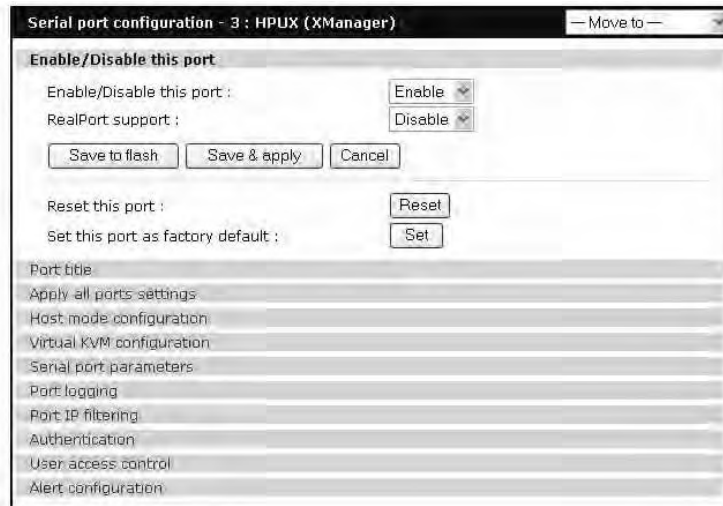
1. Access the Digi Passport Web interface and log in.
2. Choose Serial Port > Configuration.

You see this window:



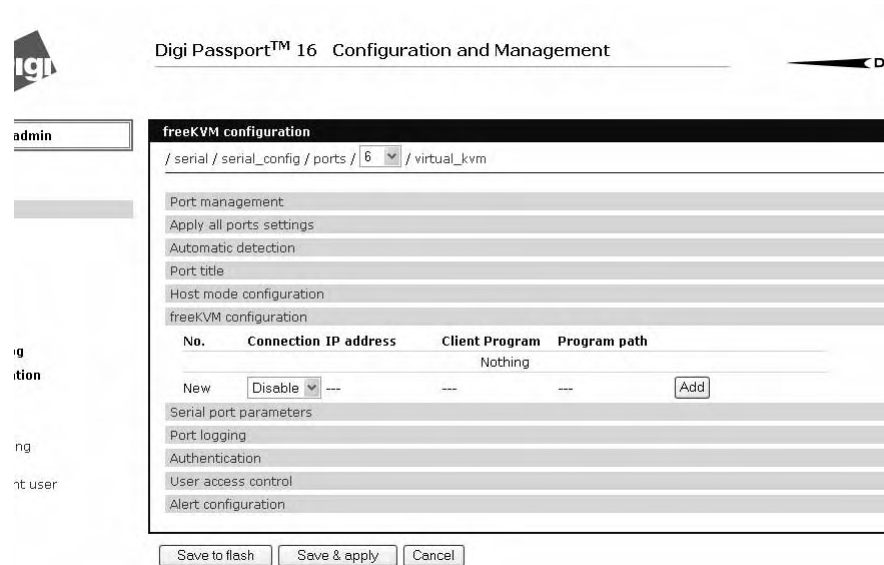
3. Choose the port you want to configure.

A window similar to this one opens, showing the serial port number and title:



4. Choose FreeKVM configuration.

This window opens:

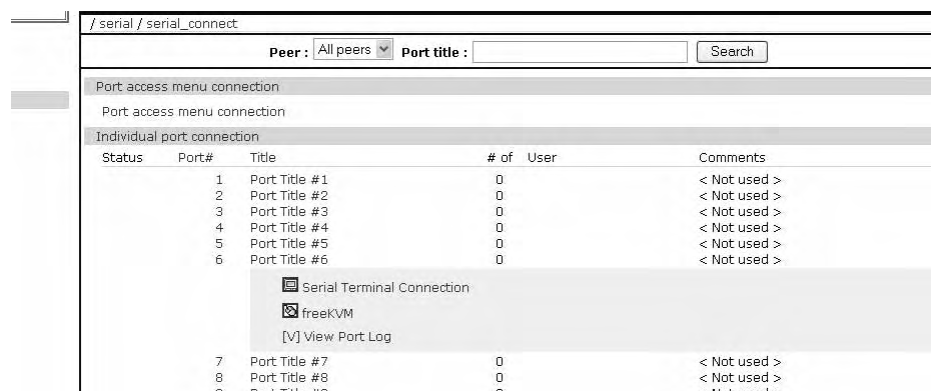


5. From the FreeKVM connection drop-down list, select Enable. Then, from the Client program drop-down list, choose the Xmanager program.
6. Click Save and Apply.

Connecting to a system through FreeKVM using Xmanager

When you connect through the Connection window, and a FreeKVM 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 FreeKVM graphical interface

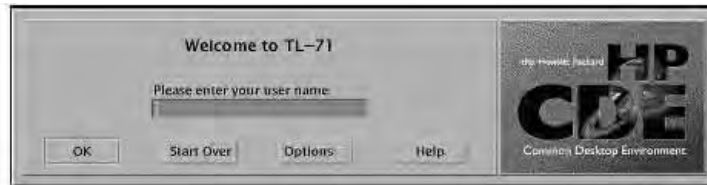


To connect through FreeKVM using X Window System Protocol and XManager Software:

1. Click on the mouse icon.

Web Redirection

2. Click OK for each of the three Java requests in pop-up windows.
The application starts, and you see a message that the connection succeeded:
The FreeKVM VNC Connection comes up:



3. Enter your user name and password, and click OK.

If the application does not start, check to make sure that the application is in the search path on your server. See "Installing Programs for FreeKVM" on page 122.

Web Redirection

It is also possible to use the Web redirection feature to link to a web configuration or management interface. Choosing Web redirection will create a link to `http://IP` in the connection window. If the remote system supports https, just change the reference to `https://IP`. If there is a specific page or nonstandard socket requirement, modify the connection accordingly, e.g.: `http://IP:8080/specific/filename.htm`

Installing Programs for FreeKVM

FreeKVM 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 FreeKVM.

- Because the FreeKVM 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 primary VGA data. Windows systems prior to Server 2003 provide the VGA facility on the standard data stream.

To access the primary VGA data stream, use Remote Desktop Client -- console.

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 <http://www.tightvnc.com/>
- RealVNC software from <http://www.realvnc.com/>
- UltraVNC from <http://www.ultravnc.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.

For secure VNC from Windows desktops, Digi provides an automatic VNC tunnelling toolkit. The toolkit is included on the Passport CD and is available from the Digi website <http://www.digi.com/support> under Digi Passport.

To use the tool (called ssh_vnc.exe) unzip the toolkit and place the files inside it into a directory in your path. A good default is %WINDIR% (usually this is C:\Windows).

To use the tool, use User defined protocol, set the program name to ssh_vnc \$IP\$:5901 (or whatever socket your VNC application is listening to). Full documentation for the tool is provided in the release notes included in the zip file.

Xmanager

Client Software Needed

The Xmanager software is available for a free 30 day evaluation download from <http://www.netsarang.com/download/main.html>

Installing Programs for FreeKVM

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.

Chapter 12 Rackable® Systems Management Card

Introduction

Rackable® Systems manufactures a management card that is built into some of their servers. It interfaces between the Digi Passport unit and the server's serial port. In normal mode, it allows transparent communication between the Digi Passport 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 Passport unit offers a graphical web based user interface to manage the Rackable Systems Management Card.

Set up

Setup of the Digi Passport 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 Passport 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 Passport 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.

Accessing the Rackable Systems Management Card from the Digi Passport Unit's User Interface

1. Access the Digi Passport unit's web interface.
2. Under the **Serial Port** heading choose **Connection**.

A screen similar to the following appears.

The screenshot shows the Digi Passport 16 Configuration and Management web interface. The user is logged in as 'admin'. The left sidebar contains a navigation menu with categories like Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled 'Serial port connection' and shows a table of port configurations. The table has columns for Status, Unit, Port#, Title, # of, User, and Comments. Port 1 is titled 'Port Title#1 Alpha' and is currently 'Not used'. Below the table, there are links for 'Serial Terminal Connection', 'View Port Log', and 'Rackable Systems Mgmt Card'.

Status	Unit	Port#	Title	# of	User	Comments
		1	Port Title#1 Alpha	0		< Not used >
		2	Port Title#2	0		< Not used >
		3	Port Title#3	0		< Not used >
		4	Port Title#4	0		< Not used >
		5	Port Title#5	0		< Not used >
		6	Port Title#6	0		< Not used >
		7	Port Title#7	0		< Not used >
		8	Port Title#8	0		< Not used >
		9	Port Title#9	0		< Not used >
		10	Port Title#10	0		< Not used >
		11	Port Title#11	0		< Not used >
		12	Port Title#12	0		< Not used >
		13	Port Title#13	0		< Not used >
		14	Port Title#14	0		< Not used >
		15	Port Title#15	0		< Not used >
		16	Port Title#16	0		< Not used >

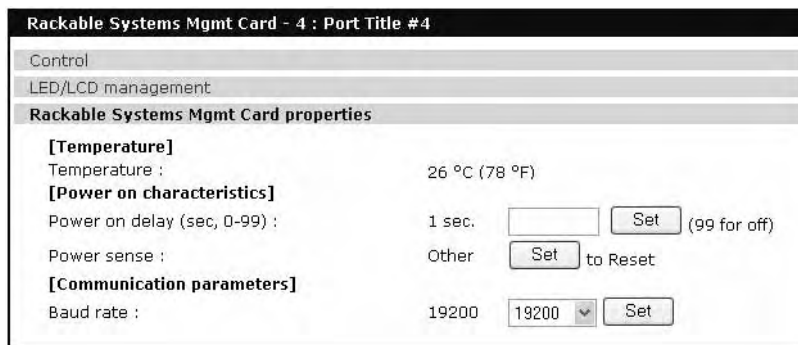
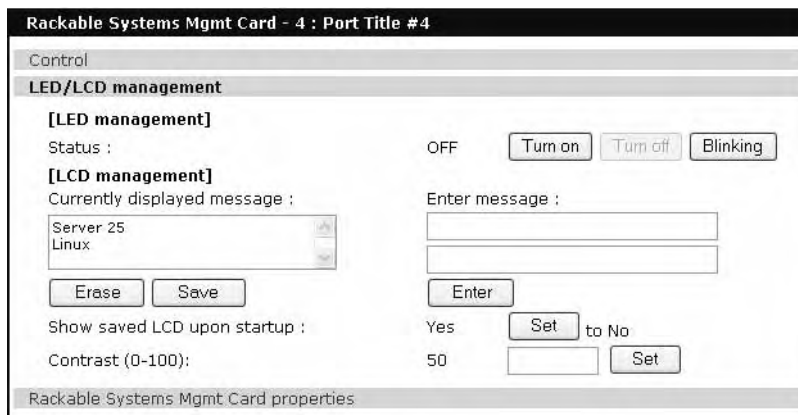
Copyright © 1996-2006 Digi International. All rights reserved.

3. Click on the Rackable Server link.

A screen similar to the following appears.

The screenshot shows the 'Rackable Systems Mgmt Card - 4 : Port Title #4' control panel. It has a 'Control' section with the following information: Manufacturer: Rackable Systems, Power status: ON. There are buttons for 'Power on', 'Power off', and 'Reboot'. Below this, there is a 'Connect to Rackable Systems Mgmt Card console' button. The panel also has sections for 'LED/LCD management' and 'Rackable Systems Mgmt Card properties'.

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



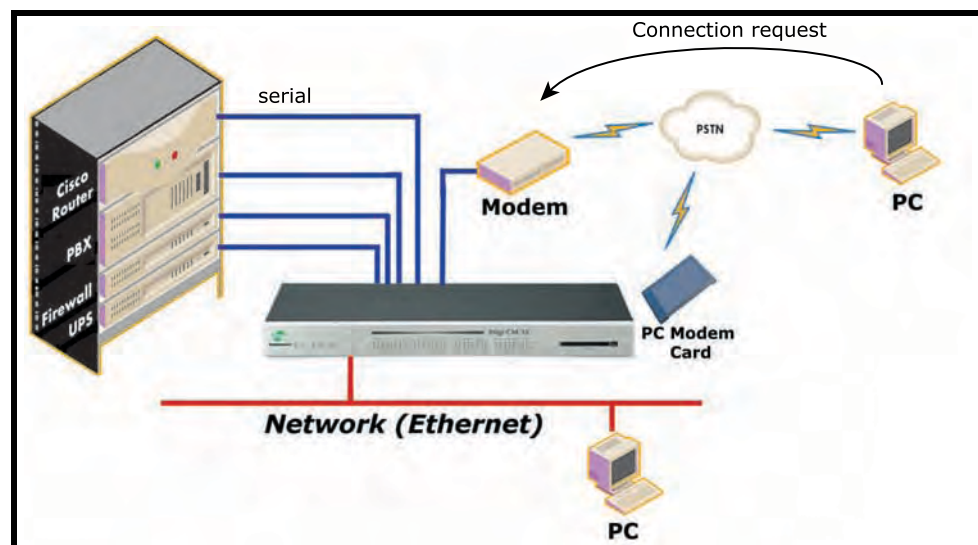
Field	Description
Control	
Power status	The first column shows the current state. Three buttons are available to initiate an action to either, power on, power off or restart the server. Dependant on the current status Power on or Power off is disabled.
Reboot	Reboot the Rackable Server by sending a 500ms 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.
Erase	This function clears the LCD display. The saved message stays saved to flash.
Save	Save currently displayed message to flash memory.

Field	Description
Show saved LCD message upon startup	The first column 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 Passport unit's port settings.

Introduction

The Digi Passport unit supports dial-in connections from remote sites for out-of-band access. In this configuration, the Digi Passport 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 Passport unit accepts the connection and displays a menu of available serials ports. In a dial-in terminal server mode, the Digi Passport 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" on page 59.

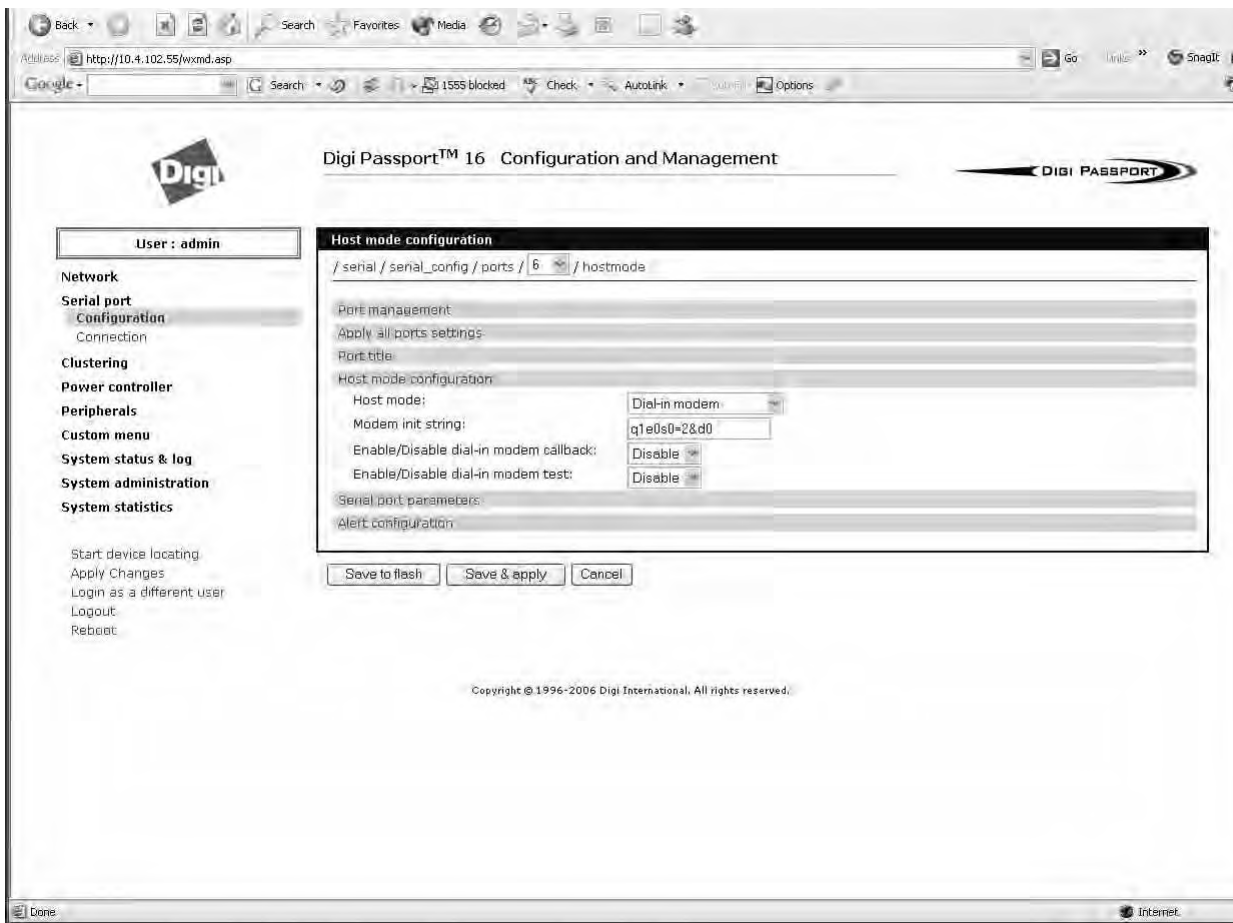


Configuring for Dial-In Modem Access

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.
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.

Configuring for Dial-In Modem Access



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 Passport unit's serial port. See your modem user manual for more information.

Callback - For security reasons, the callback feature can be activated.

Enable/Disable dial-in modem callback :	Enable
Dial-in modem callback phone number :	1234444567

If callback is enabled, the Digi Passport 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”.

Modem test - To ensure the proper functionality of the modem, the Digi Passport 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 Passport 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 Passport unit:

```
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
```

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.

- e-mail based notification

The **Alert configuration** dialog of the port configuration, contains multiple settings:

Serial port configuration - 1 : Port Title #1 [Move to]

Enable/Disable this port

Port title

Apply all ports settings

Host mode configuration

Serial port parameters

Alert configuration

[Email alert configuration]

Email alert for dial-in modem test : Enable

Title of email : Modem test port 1

Recipient's email address : modemtest@example.com

[SNMP trap configuration]

Dial-in modem test 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

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.

Adding a PC Modem

The Trap MIB can be downloaded from support.digi.com (select your product and go to Diagnostics, Utilities and MIBs).

6. Click Save & apply.

Adding a PC Modem

A PC card slot is provided on the front panel of the Digi Passport unit. To install and configure the PC modem on the Digi Passport unit, do the following.

1. Insert the card into the PC slot located on the front of the device.
2. Access the web interface.
3. From the menu, choose **Configuration** under the **PC card** heading.
4. Choose Discover a new card.

The Digi Passport unit searches for a PC card and displays a configuration menu.

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

Configuring 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.
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.

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.

6. Click Save & apply.

Configuring Remote Dial-In Access

The screenshot displays the Digi Passport 16 Configuration and Management web interface. At the top left is the Digi logo, and at the top right is the Digi Passport logo. The page title is "Digi Passport™ 16 Configuration and Management". A navigation menu on the left includes sections like Network, Serial port, Configuration, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration, and System statistics. The main content area is titled "Host mode configuration" and shows a breadcrumb path: "/ serial / serial_config / ports / 6 / hostmode". The configuration fields are as follows:

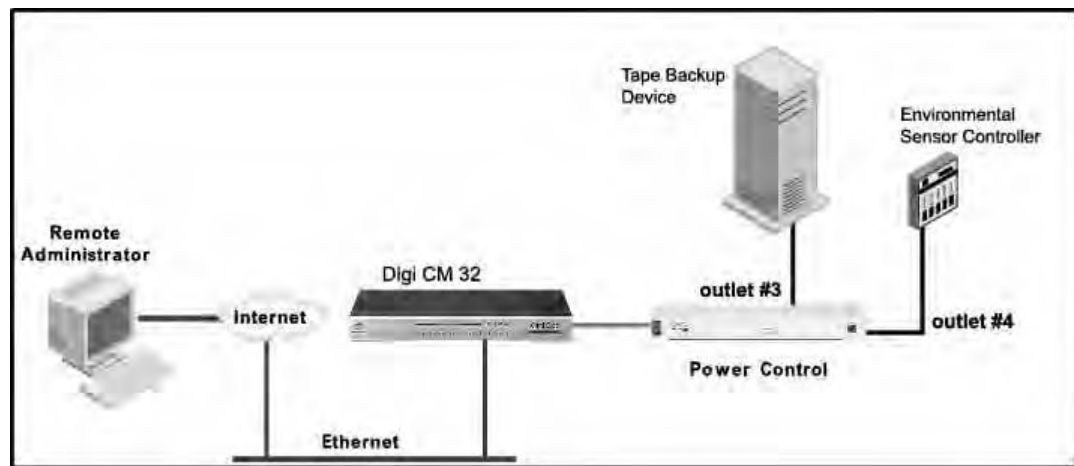
Host mode:	Dial-in terminal server
Terminal server option:	Remote connection
Destination IP:	
Destination port (0-65535):	
Protocol:	Telnet
Inactivity timeout (1-3600 seconds, 0 for unlimited):	0 second(s)
Modem init string:	q1e0s0=2&d0

Below the configuration fields are buttons for "Save to flash", "Save & apply", and "Cancel". At the bottom of the page, there is a copyright notice: "Copyright © 1996-2006 Digi International. All rights reserved." The browser status bar at the bottom shows "Done" and "Internet".

Introduction

The Power Controller feature allows the administrators of the Digi Passport 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 Passport unit.

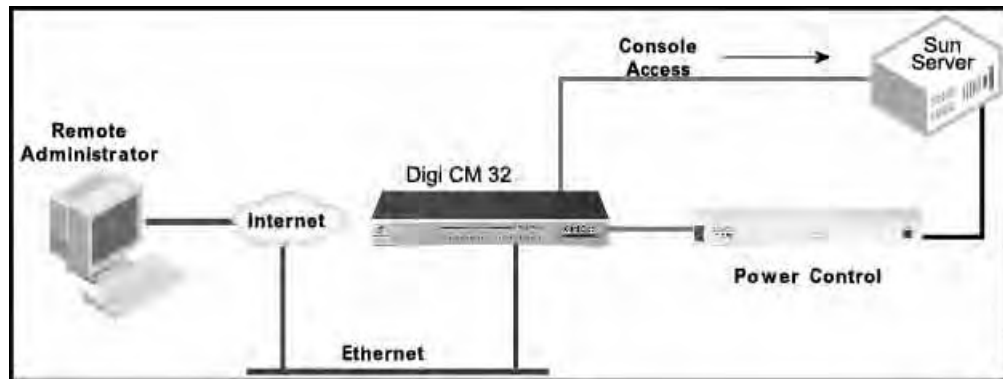
This illustration shows the a power controller configured through the Digi Passport unit for non-serial devices.



The second scenario is a serial device (such as a router or server) managed through a port on the Digi Passport 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 Passport 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 Passport unit does that for you.

Installing Power Controller

The following illustration shows a Sun server configured through a serial port connection on the Digi Passport 32.



Installing Power Controller

To connect the Digi RPM power controller to the Digi Passport 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 Passport 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 "Cascading Multiple Digi RPM Units" on page 144.

If you are using any other manufacturer of power controllers, please refer to "About Serial Port Cabling" on page 207 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 "Cascading Multiple Digi RPM Units" on page 144.

Configuring 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 Passport unit (username root, password dbps).
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.

- Continue by adding the power controller.

Add the Power Controller

- Log in to the Digi Passport unit (username root, password dbps).
- Click **Power Controller > Configuration**.

Power controller configuration				
Add power controller				
Port :		2		
Manufacturer :		DIGI RPM		
The number of cascaded units :		1		
Add controller				
Power controllers				
Port#	Manufacturer	Title	Outlets	Action
No power controller added...				

- 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.

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

Serial Port info

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.

-

Setting Alarms and Thresholds

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

The screenshot shows the 'Power controller configuration - Digi RPM 8' window. The 'Alarms & thresholds' section is active. It includes the following fields and options:

- Alarm threshold : amps (maximum value)
- Temperature threshold : °F °C
- Send email alert (On alarm threshold On temperature threshold)
- To :
- Send SNMP trap (On alarm threshold On temperature threshold)
- Use global SNMP configuration :
- Trap receiver settings :
- Table with 3 columns: IP Address, Community, Version.

IP Address	Community	Version
<input type="text" value="0.0.0.0"/>	<input type="text" value="public"/>	<input type="text" value="v1"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="public"/>	<input type="text" value="v1"/>

Outlets

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 (E-mail or 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 E-mail alert it is assumed that the mail server has already been set up. If not, go to "Configuring SMTP Alerts" on page 70. 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.

Digi Passport™ 16 Configuration and Management Digi PASSPORT

Power controller configuration - DIGI RPM on Port 2

/ power / power_config / power_controller

Power controller

Alarms & thresholds

Outlets

Outlet	Port	Title	Unit#	Outlet#
1	None	None		
2	None	None		
3	None	None		
4	None	None		
5	None	None		
6	None	None		
7	None	None		
8	None	None		
9	None	None		
10	None	None		

Serial port :

Outlet title :

User access control :

User or Access list	Power access	Action
<<Everyone>>	<input checked="" type="checkbox"/>	
<input type="text"/>	<input checked="" type="checkbox"/>	<input type="button" value="Add user"/>
<input type="text" value="Select an access list"/>	<input checked="" type="checkbox"/>	<input type="button" value="Add access"/>

Move to Access lists to edit access list.

3. Select the serial port number that controls the device connected to the Digi Passport 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" on page 140.
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 2

/ power / power_config / power_controller

Power controller

Alarms & thresholds

Outlets

Outlet	Port	Title	Unit#
1	None	Sun Server	
2	None	None	
3	None	None	
4	None	None	
5	None	None	
6	None	None	
7	None	None	
8	None	None	
9	None	None	
10	None	None	

Serial port : None

Outlet title : Sun Server

User access control :

User or Access list	Power access	Action
<<Everyone>>	<input type="checkbox"/>	
tomw	<input checked="" type="checkbox"/>	Remove
	<input type="checkbox"/>	Add user
	<input type="checkbox"/>	Add access

Move to Access lists to edit access list.

Save to flash Save & apply Cancel

Note: The screen above shows that serial port one on the Digi Passport unit is connected to a Sun Server that is supplied power from outlet 1 on the power controller. In the example above, tomw 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" on page 140.

User Access for Power Controller

The Digi Passport 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

Configuring to Allow Specific Users Access

To configure the Digi Passport 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 Passport unit (username root, password dbps)
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.

The screenshot shows the 'Power controller' configuration page with the 'Outlets' section. A modal window is open for configuring outlet #3. The modal includes fields for 'Serial port' (set to None), 'Outlet title' (Backup Tape Device), and a table for 'User access control'.

Outlet	Port	Title	Unit#	Outlet#
1	1	Sun Server	0	1
2	1	Sun Server	0	2
3	None	Backup Tape Device	0	3
4	None	Light display	0	4
5	None	None	0	5
6	None	Test	0	6
7	None	None	0	7
8	None	None	0	8

User	Power access	Action
<<Everyone>>	<input type="checkbox"/>	
jan1	<input checked="" type="checkbox"/>	Remove
<input type="text"/>	<input type="checkbox"/>	Add

Buttons: Save to flash, Save & apply, Cancel

Note: The screen above shows outlets 1 & 2 control power to the Sun Server configured on port 1 of the Digi Passport unit. Outlets 3 and 4 are not serial devices. jan1 has been designated the specific user to control outlet # 3.

Configuring 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 Passport unit (username root, password dbps).
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.

Power Controller Management

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.

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 Backup	0	2
3	None	Backup Tape Device	0	3
4	None	Environmental Sensor	0	4
5	None	None	0	5
6	None	None	0	6
7	None	None	0	7
8	None	None	0	8

Serial port :

Outlet title :

User access control :

User	Power access	Action
<<Everyone>>	<input checked="" type="checkbox"/>	
tomw	<input type="checkbox"/>	<input type="button" value="Remove"/>
<input type="text"/>	<input checked="" type="checkbox"/>	<input type="button" value="Add"/>

Note: tomw 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.

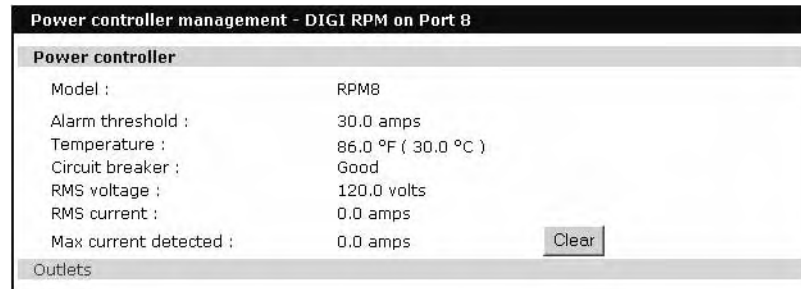
1. Under **Power Control** click **Management**.

Power controller management

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.

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

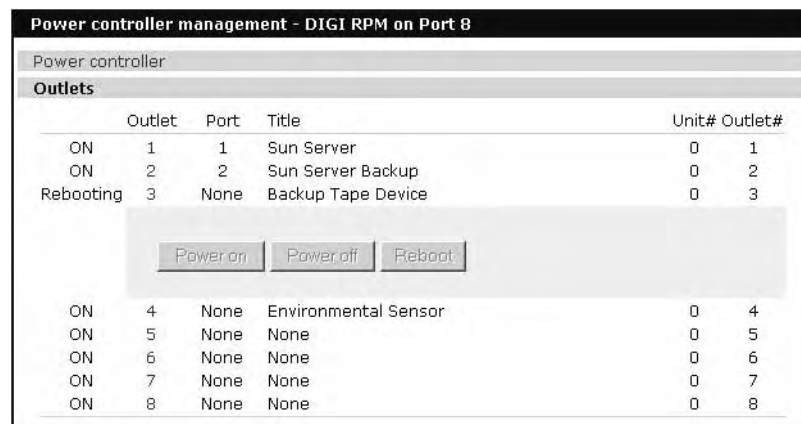


The Power controller statistics screen appears to show the Alarm threshold, Current temp, Circuit breaker condition, RMS voltage, RMS current, and Max current detected.

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

- 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.



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

Cascading Multiple Digi RPM Units

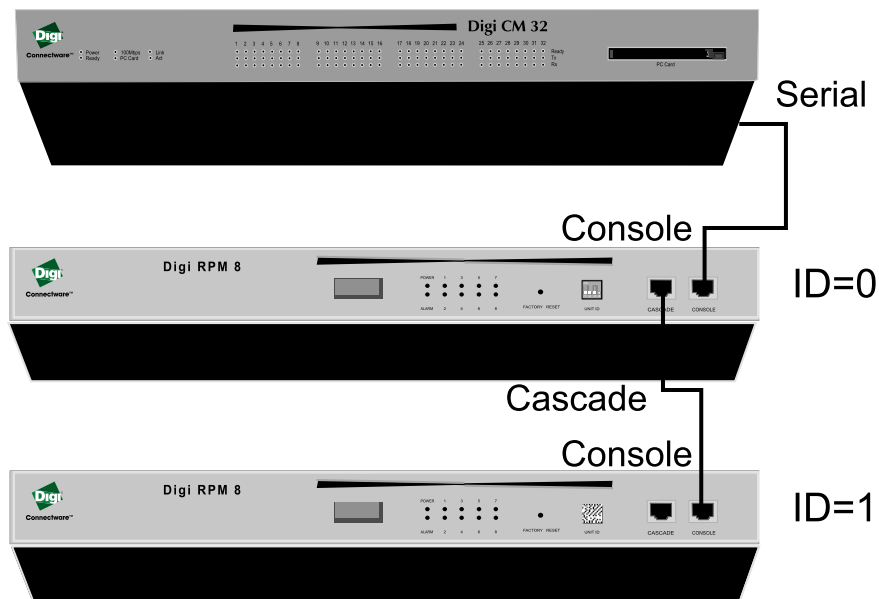
The Digi RPM power controllers can be cascaded when used with the Digi Passport unit.

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 Passport 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 Passport unit.

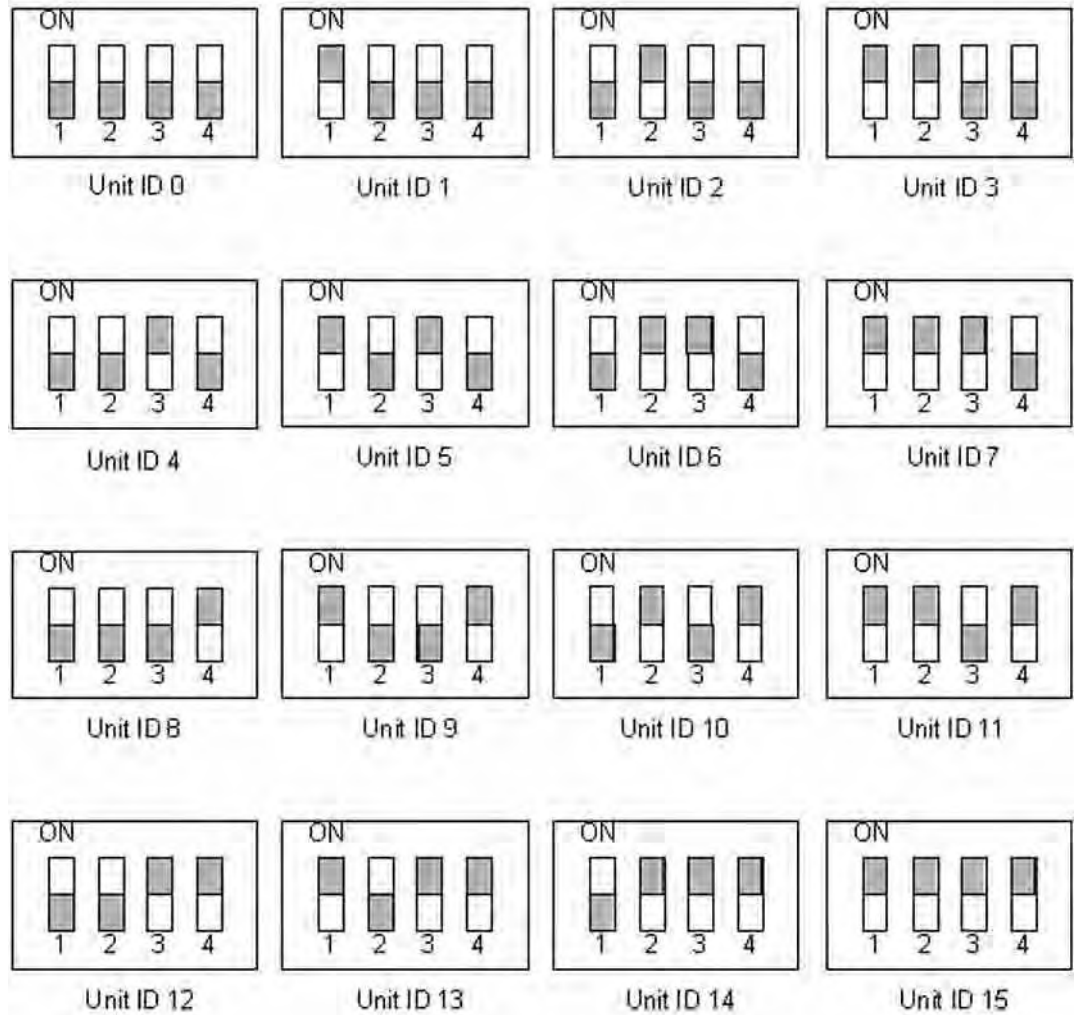
Please note that the ID for the first unit is set to 0 and for the second unit it is set to 1.



The next table shows all possible IDs that can be configured on the Digi RPM.

unit.

Unit ID Switch Configuration



Introduction

Port clustering is the ability to coherently manage serial ports across multiple devices. Digi Passport supports two methods of port clustering, both of which can be used concurrently.

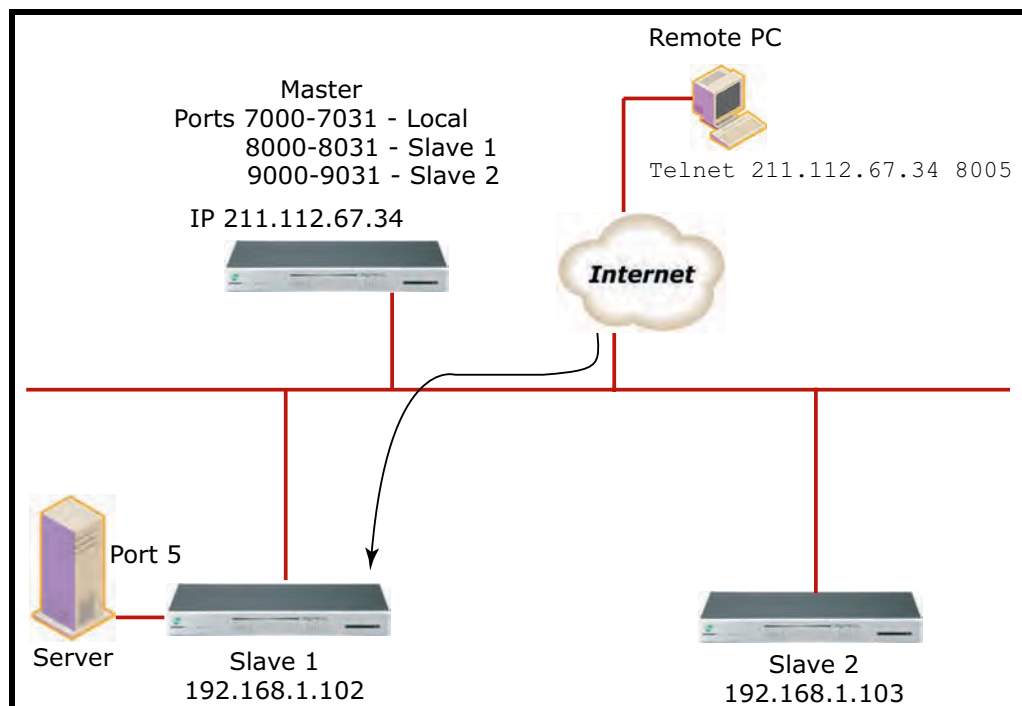
Master/Slave Clustering

This method allows serial ports on one or multiple slave devices to be managed from one master device using a single IP address. For instance, the Digi Passport 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 Passport unit for port clustering you will need to:

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

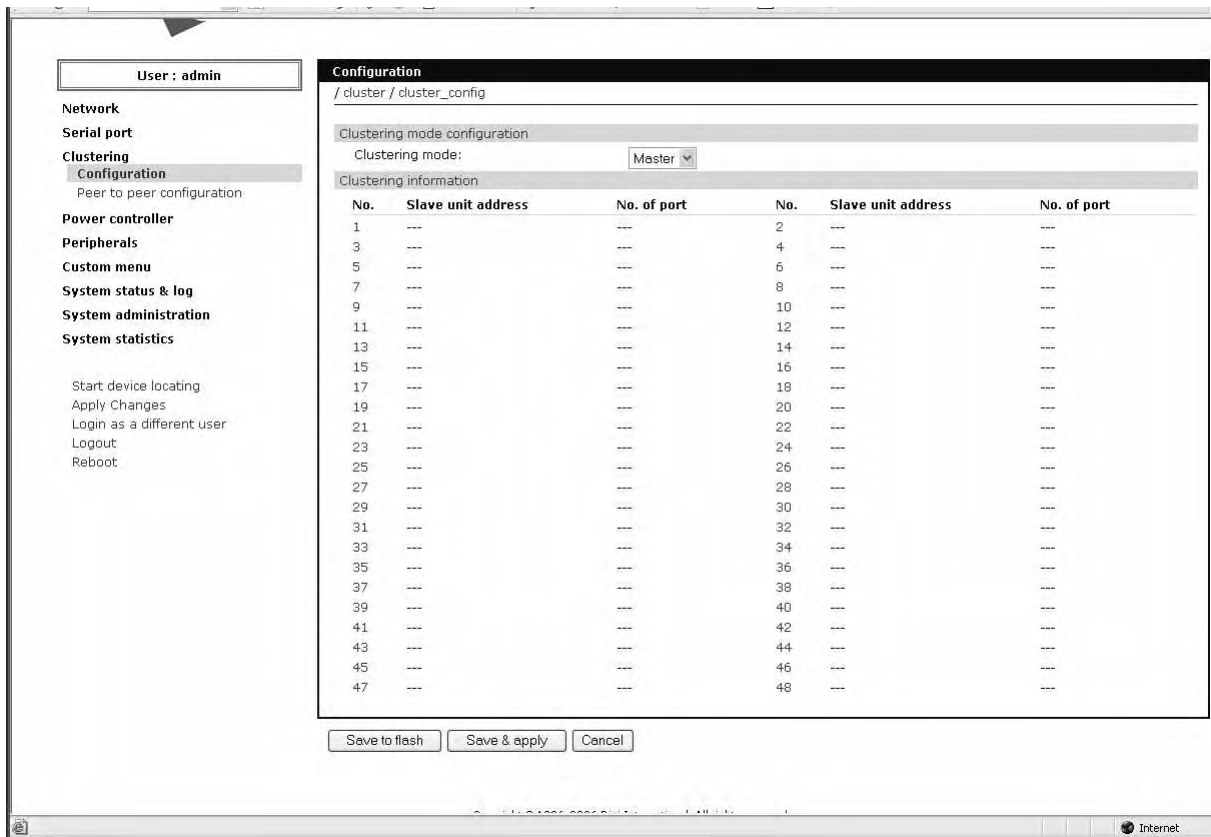


Configuring Port Clustering

Assigning Master Clustering Mode

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

1. Access the Digi Passport unit through the web interface. This Digi Passport 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 Slaves to Join a Cluster

Digi Passport units and 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 and apply**.

Clustering configuration

Clustering mode configuration

Clustering mode : Slave

Authentication mode : Local

Update master on changes : No

Save to flash Save & apply Cancel

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 procedure listed below.

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

Clustering configuration - Unit A

Basic configuration

Enable/Disable this unit : Disable

Save to flash Save & apply Cancel

3. Select Advanced from the Clustering > Master mode.

Clustering configuration - Unit A

Basic configuration **Advanced >>**

Enable/Disable this unit : Enable

Slave unit address : Auto Configure

No. of port : 48

Slave authentication mode : Local Set Authentication

Save to flash Save & apply Cancel

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 Passport 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.



User : root

- Network
- Serial port
- Clustering
 - Configuration**
 - Peer to peer configuration
- Power controller
- Peripherals
- Custom menu
- System status & log
- System administration
- System statistics

Start device locating
Apply Changes
Login as a different user
Logout
Reboot

Advanced

/ cluster / cluster_config / unit_info / 1 / advance

Enable/Disable this unit:

Slave unit address:

No. of port:

Slave authentication mode:

Update master on changes:

Advanced

Web port configuration

No.	Enable	Source port	Destination port	Protocol
1	<input checked="" type="checkbox"/>	<input type="text" value="50249"/>	<input type="text" value="80"/>	<input type="button" value="HTTP"/>

Port access menu configuration

No.	Enable	Source port	Destination port	Protocol
1	<input checked="" type="checkbox"/>	<input type="text" value="50200"/>	<input type="text" value="7000"/>	<input type="text" value="Telnet"/>

Individual port configuration

No.	Enable	Title at master unit	Source port	Dest port	Protocol
1	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #1"/>	<input type="text" value="50201"/>	<input type="text" value="7001"/>	<input type="text" value="Telnet"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #2"/>	<input type="text" value="50202"/>	<input type="text" value="7002"/>	<input type="text" value="Telnet"/>
3	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #3"/>	<input type="text" value="50203"/>	<input type="text" value="7003"/>	<input type="text" value="Telnet"/>
4	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #4"/>	<input type="text" value="50204"/>	<input type="text" value="7004"/>	<input type="text" value="Telnet"/>
5	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #5"/>	<input type="text" value="50205"/>	<input type="text" value="7005"/>	<input type="text" value="Telnet"/>
6	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #6"/>	<input type="text" value="50206"/>	<input type="text" value="7006"/>	<input type="text" value="Telnet"/>
7	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #7"/>	<input type="text" value="50207"/>	<input type="text" value="7007"/>	<input type="text" value="Telnet"/>
8	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #8"/>	<input type="text" value="50208"/>	<input type="text" value="7008"/>	<input type="text" value="Telnet"/>
9	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #9"/>	<input type="text" value="50209"/>	<input type="text" value="7009"/>	<input type="text" value="Telnet"/>
10	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #10"/>	<input type="text" value="50210"/>	<input type="text" value="7010"/>	<input type="text" value="Telnet"/>
11	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #11"/>	<input type="text" value="50211"/>	<input type="text" value="7011"/>	<input type="text" value="Telnet"/>
12	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #12"/>	<input type="text" value="50212"/>	<input type="text" value="7012"/>	<input type="text" value="Telnet"/>
13	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #13"/>	<input type="text" value="50213"/>	<input type="text" value="7013"/>	<input type="text" value="Telnet"/>
14	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #14"/>	<input type="text" value="50214"/>	<input type="text" value="7014"/>	<input type="text" value="Telnet"/>
15	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #15"/>	<input type="text" value="50215"/>	<input type="text" value="7015"/>	<input type="text" value="Telnet"/>
16	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #16"/>	<input type="text" value="50216"/>	<input type="text" value="7016"/>	<input type="text" value="Telnet"/>
17	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #17"/>	<input type="text" value="50217"/>	<input type="text" value="7017"/>	<input type="text" value="Telnet"/>
18	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #18"/>	<input type="text" value="50218"/>	<input type="text" value="7018"/>	<input type="text" value="Telnet"/>
19	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #19"/>	<input type="text" value="50219"/>	<input type="text" value="7019"/>	<input type="text" value="Telnet"/>
20	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #20"/>	<input type="text" value="50220"/>	<input type="text" value="7020"/>	<input type="text" value="Telnet"/>
21	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #21"/>	<input type="text" value="50221"/>	<input type="text" value="7021"/>	<input type="text" value="Telnet"/>
22	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #22"/>	<input type="text" value="50222"/>	<input type="text" value="7022"/>	<input type="text" value="Telnet"/>
23	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #23"/>	<input type="text" value="50223"/>	<input type="text" value="7023"/>	<input type="text" value="Telnet"/>
24	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #24"/>	<input type="text" value="50224"/>	<input type="text" value="7024"/>	<input type="text" value="Telnet"/>
25	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #25"/>	<input type="text" value="50225"/>	<input type="text" value="7025"/>	<input type="text" value="Telnet"/>
26	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #26"/>	<input type="text" value="50226"/>	<input type="text" value="7026"/>	<input type="text" value="Telnet"/>
27	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #27"/>	<input type="text" value="50227"/>	<input type="text" value="7027"/>	<input type="text" value="Telnet"/>
28	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #28"/>	<input type="text" value="50228"/>	<input type="text" value="7028"/>	<input type="text" value="Telnet"/>
29	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #29"/>	<input type="text" value="50229"/>	<input type="text" value="7029"/>	<input type="text" value="Telnet"/>
30	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #30"/>	<input type="text" value="50230"/>	<input type="text" value="7030"/>	<input type="text" value="Telnet"/>
31	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #31"/>	<input type="text" value="50231"/>	<input type="text" value="7031"/>	<input type="text" value="Telnet"/>
32	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #32"/>	<input type="text" value="50232"/>	<input type="text" value="7032"/>	<input type="text" value="Telnet"/>
33	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #33"/>	<input type="text" value="50233"/>	<input type="text" value="7033"/>	<input type="text" value="Telnet"/>
34	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #34"/>	<input type="text" value="50234"/>	<input type="text" value="7034"/>	<input type="text" value="Telnet"/>
35	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #35"/>	<input type="text" value="50235"/>	<input type="text" value="7035"/>	<input type="text" value="Telnet"/>
36	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #36"/>	<input type="text" value="50236"/>	<input type="text" value="7036"/>	<input type="text" value="Telnet"/>
37	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #37"/>	<input type="text" value="50237"/>	<input type="text" value="7037"/>	<input type="text" value="Telnet"/>
38	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #38"/>	<input type="text" value="50238"/>	<input type="text" value="7038"/>	<input type="text" value="Telnet"/>
39	<input checked="" type="checkbox"/>	<input type="text" value="Port Title #39"/>	<input type="text" value="50239"/>	<input type="text" value="7039"/>	<input type="text" value="Telnet"/>

Peer to Peer Clustering

Peer to Peer clustering allows multiple Digi Passport units to share information without requiring one of the units to be the master. This avoids the single point of failure associated with "centralized system" control -- with Peer to peer clustering, each unit is capable of initiating connections to ports on any other unit, avoiding the "what if that unit is unreachable?" problem.

Note: If a Digi Passport unit has Master/Slave clustering configured, it will report all of its slave ports to the other peer units, however, it is still necessary for that Digi Passport unit to be operational to reach the Slave ports it controls

Accessing 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. Clustered Ports appear in the WebUI, and can be sorted by Port Title or Port Number. If there are more ports than will display on the screen, use the "Move To" pager feature on the upper right of the Port list.
2. To adjust the number of ports that display on a page, See Web Server configuration ON PAGE XXXXX and adjust the "serial ports count on connection page."

— Command Line Access

1. From Ports Menu, choose R to see a list of peered units or S to see a list of Slave units.
- 2.

Clustering Peer-to-peer

Master / slave defines one unit as the master and the other units as slaves. While it is possible to define multiple units as masters for a common set of slaves, a unit cannot be both a master and a slave at the same time.

Peer to peer clustering allows units to have equal status within a cluster, so that any unit in the cluster (typically the closest unit to the user) can act as a master. Peer to peer clustered units can also control slave units as well, allowing for a more scalable and robust implementation, since if any one unit is offline, there is no single point of failure to reach the other units.

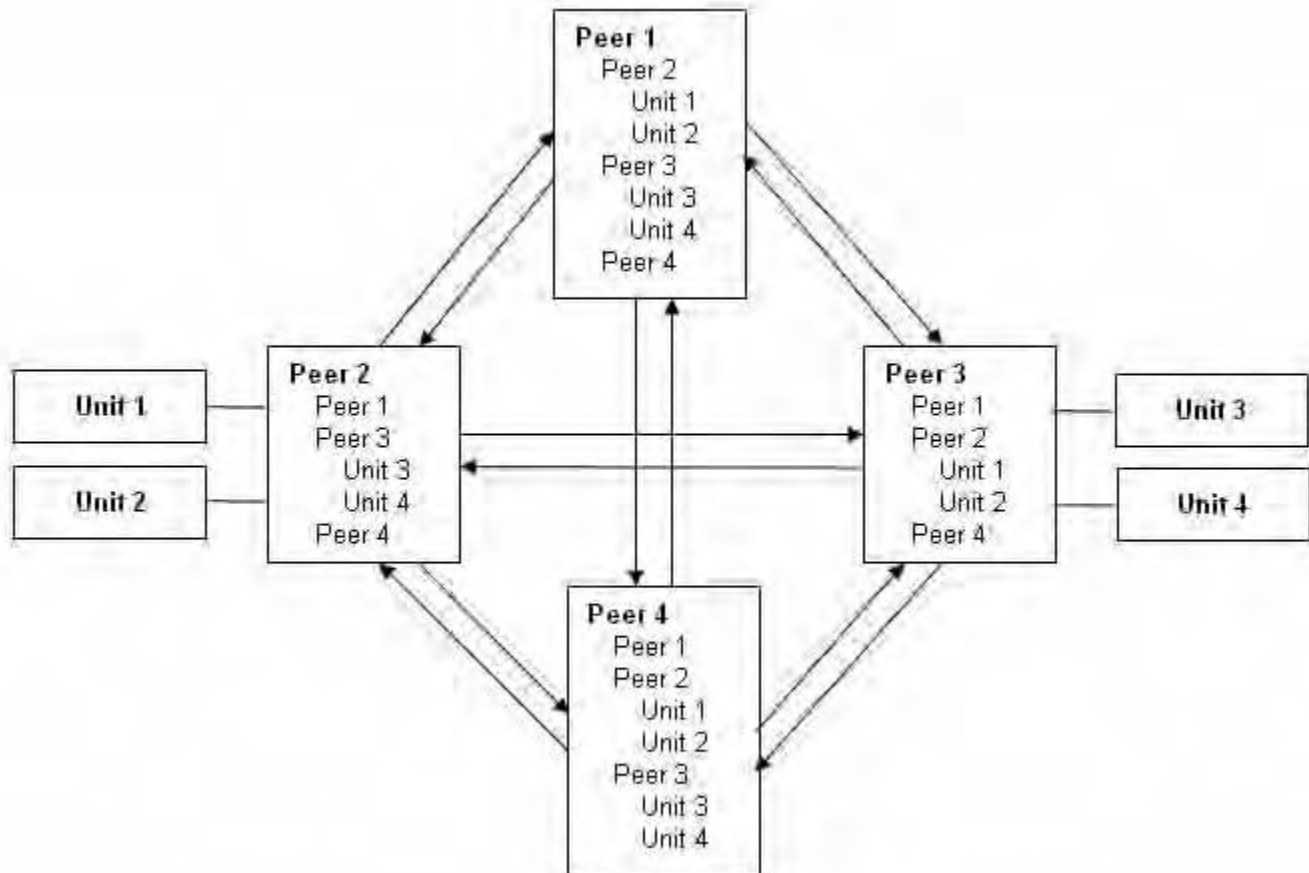


Figure 3. Clustering peer-to-peer

Users can access use any peer in peer-to-peer group to access any peer or its slave units. It extends the limitation of clustering slave units. A master unit can have up to 48 slave units. 48 peers can join to clustering peer-to-peer group. If each 48 peer with 48 slave units joins a peer-to-peer group, 2352 units ($49 * 48$) can be clustered together.

Changes between peered units are updated to the other peers automatically, even if the peer's IP address is changed.

Making up a peer_to_peer group

Making up a peer_to_peer group

Peer to peer mode configuration

The screenshot shows the 'Peer to peer mode configuration' page. At the top, the breadcrumb is '/ cluster / cluster_p2p_config / mode'. Below this, there are two main sections: 'Peer to peer mode configuration' and 'Peer to peer information'. In the first section, 'Peer to peer mode' is set to 'Enable', 'Peer to peer authentication method' is set to 'Local', and both password fields are filled with four dots. At the bottom, there are three buttons: 'Save to flash', 'Save & apply', and 'Cancel'.

Figure 4. Peer to peer mode configuration

1. Enable Peer to Peer mode
2. Define the authentication method to be used
3. If Local authentication is used, this peer will continue to authenticate users locally and independently of other peers.
4. If Peer authentication is used, the first peer contacted will perform the authentication.

Peered units have to share the same password.

Peer to peer information

The screenshot shows the 'Peer to peer information' page. The breadcrumb is '/ cluster / cluster_p2p_config / p2p_info'. Below this, there are two main sections: 'Peer to peer mode configuration' and 'Peer to peer information'. In the second section, 'Peer to peer status' is 'Not joined'. There are buttons for 'Join', 'Withdraw', 'Refresh', and 'Update'. Below this is a table with columns: Peer no., IP, Authen. method, Web port Protocol, Port access Protocol Source, Source port, Slave Unit, and Action. The table is currently empty with the text 'No peer found....' below it. At the bottom, there is a button labeled 'Invite peers'.

Figure 5. Peer to peer information

Peer to peer status:

Not ready: - Peer to peer mode is not active

Not joined: -Peer to peer mode is active but no peers have been defined.

Joining: - Joining peer_to_peer group.

Joined: -Joined peer_to_peer group.

Changing peers: -Changing the information of peers in peer_to_peer group

Withdrawing: - Withdrawing from peer_to_peer group.

Withdrawn: - Withdrawn from last peer_to_peer group.

[Refresh] update display of this page

[Join] button: Used to join peer_to_peer group of a designated peer (requires common password).

[Withdraw] button: Used to withdraw from the current peer_to_peer group.

[Update] button:Used to get the information of peers which have not responded.

Peers list: -The list of the peers that are members of the current peer_to_peer group.

Join

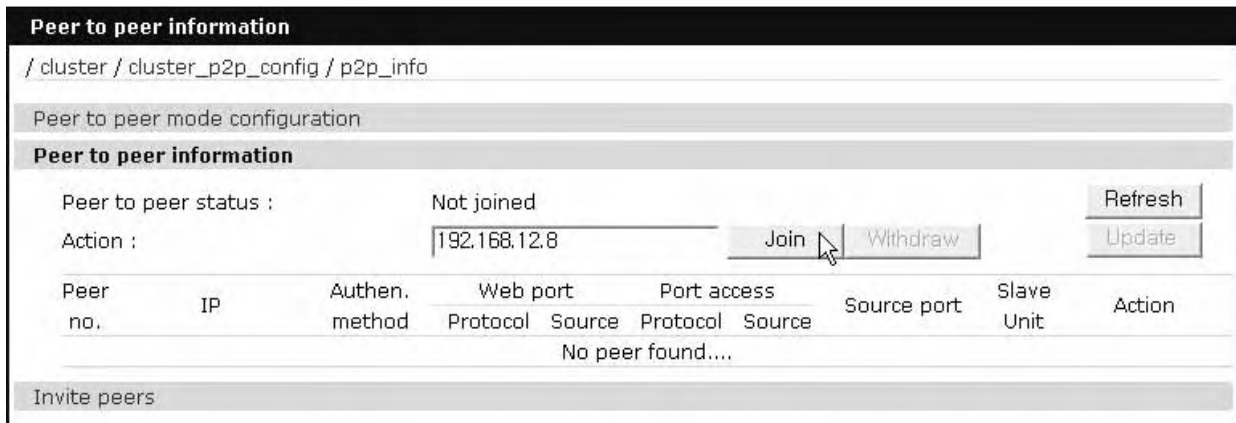


Figure 6. Join

To join an existing peer_to_peer group , enter the IP address of a member of that group and click the [Join] button. The joining process will fail if the peer is not enabled or the password is incorrect.

Figure 6 Peer to peer information of joining peer

Figure 6 shows peer to peer information of a joining peer after joining an existing group. The list of peers consists of peer number, IP address, peer to peer authentication method, the link to the web interface of each member of the group, the link to the port access menu and method, the source port number range and the count of slave units.

Figure 7. Peer to peer information of the designated peer

Making up a peer_to_peer group

Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Joined

Action :

Peer no.	IP	Authen. method	Web port		Port access		Source port	Slave Unit	Action
			Protocol	Source	Protocol	Source			
1	192.168.12.8	Local	HTTPS	15000	Telnet	15001	15002 ~ 15010	--	<input type="button" value="Remove"/>
2	192.168.19.6	Local	HTTPS	15011	Telnet	15012	15013 ~ 15061	1	This

Invite peers

Figure 7 shows peer to peer information of the designated peer.

Invite peers

Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Joined Refresh

Action : Join Withdraw Update

Peer no.	IP	Authen. method	Web port		Port access		Source port	Slave Unit	Action
			Protocol	Source	Protocol	Source			
1	192.168.12.8	Local	HTTPS	15000	Telnet	15001	15002 ~ 15010	--	Remove
2	192.168.19.6	Local	HTTPS	15011	Telnet	15012	15013 ~ 15061	1	This
3	<input style="width: 100%;" type="text" value="192.168.12.32"/>								
4	<input style="width: 100%;" type="text" value="192.168.12.48"/>								
5	<input style="width: 100%;" type="text"/>								
6	<input style="width: 100%;" type="text"/>								
7	<input style="width: 100%;" type="text"/>								
8	<input style="width: 100%;" type="text"/>								Invite
9	<input style="width: 100%;" type="text"/>								
10	<input style="width: 100%;" type="text"/>								
11	<input style="width: 100%;" type="text"/>								
12	<input style="width: 100%;" type="text"/>								

Figure 8. Invite peers

To invite peers, enter their IP addresses and click the [Invite] button. Each unit will be invited to join the peer_to_peer group of the current unit (or a group will be established if there is no current group). If the remote host is not already part of a group and its password matches that of the requesting peer, it will join the local peer to peer group. All existing units in the same peer to peer group will receive information about the invited hosts.

Making up a peer_to_peer group

Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Joined Refresh

Action : Join Withdraw Update

Peer no.	IP	Authen. method	Web port		Port access		Source port	Slave Unit	Action
			Protocol	Source	Protocol	Source			
1	192.168.12.8	Local	HTTPS	15000	Telnet	15001	15002 ~ 15010	--	Remove
2	192.168.19.6	Local	HTTPS	15011	Telnet	15012	15013 ~ 15061	1	This
3	<input type="text" value="192.168.12.32"/>								
4	<input type="text" value="192.168.12.48"/>								
5	<input type="text"/>								
6	<input type="text"/>								
7	<input type="text"/>								
8	<input type="text"/>								Invite
9	<input type="text"/>								
10	<input type="text"/>								
11	<input type="text"/>								
12	<input type="text"/>								

Peer to peer information									
/ cluster / cluster_p2p_config / p2p_info									
Peer to peer mode configuration									
Peer to peer information									
Peer to peer status :		Joined						Refresh	
Action :		<input type="text"/> <input type="button" value="Join"/> <input type="button" value="Withdraw"/>				Update			
Peer no.	IP	Authen. method	Web port		Port access		Source port	Slave Unit	Action
			Protocol	Source	Protocol	Source			
1	192.168.12.8	Local	HTTPS	15000	Telnet	15001	15002 ~ 15010	--	This
2	192.168.19.6	Local	HTTPS	15011	Telnet	15012	15013 ~ 15061	1	Remove
3	192.168.12.32	Local	HTTPS	15099	Telnet	15100	15101 ~ 15132	--	Remove
4	192.168.12.48	Local	HTTPS	15133	Telnet	15134	15135 ~ 15181	--	Remove
Invite peers									

Figure 9. Peer to peer information after inviting peers

Withdraw

Used to withdraw peer_to_peer group.

Remove

Used to remove the peer from the peers list.

Update

Used to get the information of the peers which have not responded

Connecting to peers**Link to web interface**

To link to the web interface of the peer, click the protocol or the source port of the web port. Please, refer to Figure 9.

Link to port access menu

To connect to the port access menu of the peer, click the protocol or the source port of the port access menu. Please, refer to Figure 9.

Using the Passport to connect to devices on clustered systems

Ports on clustered systems appear in the Web UI alongside ports from the local system. The only limitations are that the number of users attached to a port and the comments field are not available unless you are connected from the local system for that port. (But this information is still available when you actually connect to the port)

Serial port connection page

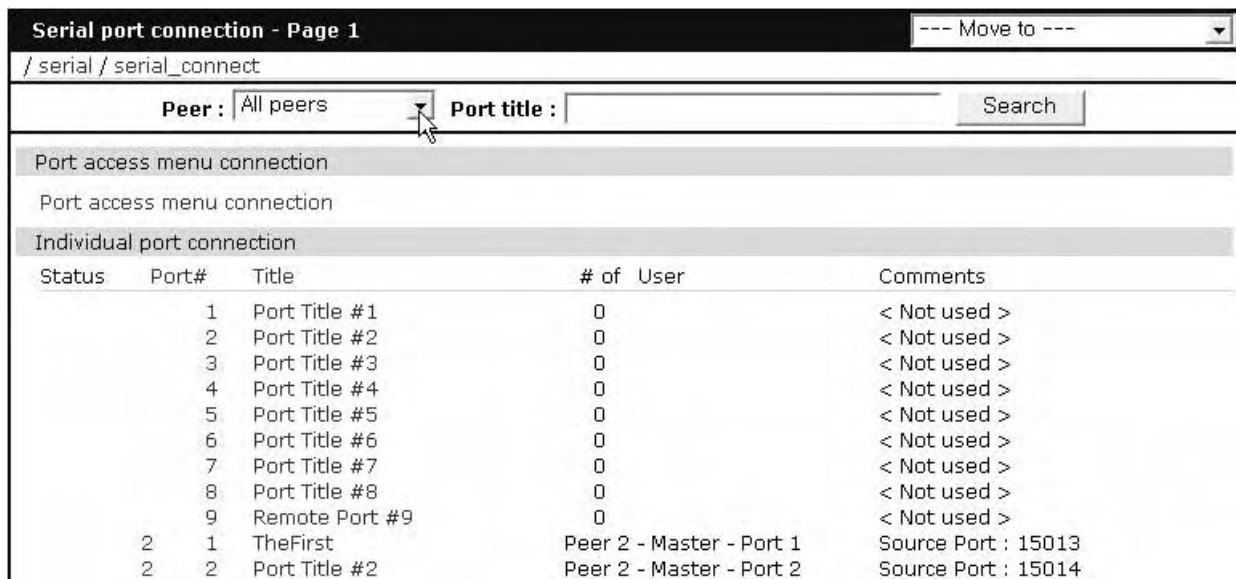


Figure 10. Serial port connection page

Figure 10 shows the serial port connection page. If more ports are configured than will fit on a page, the [--- Move to ---] list box can be used to change the display to show the rest of the ports that are not displayed on the first page.

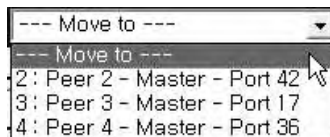


Figure 11. Move to list box

By selecting a peer in the Peer list box, users can limit those ports that belong to the selected peer. Figure 12 shows the Peer: searching option.

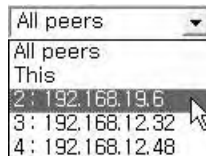


Figure 12. Peer list box

The port number consists of the peer number, unit number and port number. This example shows the first port of slave unit 4 of the second peer.

Connect to a port via connect.asp

Connecting by URL

Users can access to ports using the connect.asp tool on the Passport by using the following URL construction rules. Connect.asp supports connections by

Port Title (t=) and by Port Designator (p=). Connections made via the t= construction will be made to the first port with that title, in the case of duplicate titles. Connections made via the p= construction will allow explicit connection to any port.

The p= option can designate ports in the following format:

[R{peer_number}] [S{unit_number}] [P]port_number where peer_number is the peer number, unit_number is slave unit number and port_number is port number.

Ex)

<http://192.168.12.8/connect.asp?t=any-unique-port-title> (anywhere in the cluster)

<http://192.168.12.8/connect.asp?p=1> (This Peer – Port 1)

<http://192.168.12.8/connect.asp?p=R2P1> (Peer 2 – Port 1)

<http://192.168.12.8/connect.asp?p=R2S0P1> (Peer 2 – Port 1 -- Slave 0 means the master)

<http://192.168.12.8/connect.asp?p=R2S4P1> (Peer 2 – Slave unit 4 – Port 1)

Connect to a port via ssh

Users can also access ports using ssh console by including the t= or p= option.

Ex)

ssh root:t=any-unique-port-title@192.168.12.8 (where 192.168.12.8 is any peer)

ssh root:p=1@192.168.12.8 (192.168.12.8's local port 1)

ssh root:p=R2P1@192.168.12.8 (Peer 2 port 1)

ssh root:p=R2S0P1@192.168.12.8

ssh root:p=R2S4P1@192.168.12.8 (Peer 2 Slave 4 port 1)

ssh root:15064@192.168.12.8 (Socket, including socket on a slave via peer)

Custom menu

Users can add the ports of the peers or the slave units of the peers to the custom menu.

Introduction

This chapter 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. The Digi Passport unit runs the embedded Hard Hat Linux operating system.

Upgrading the Firmware

Web Interface

The web interface allows you to download the latest firmware version to the Digi Passport unit. The latest firmware can be found at: <http://www.digi.com> under Support, Firmware, Passport. Do the following to upgrade the firmware:

1. Access the web interface.
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 Passport unit will automatically reboot when the upgrade is complete.

Firmware upgrade

Select the new firmware binary file
This will take 8 minutes maximum

Location :

Local machine :

Automatic firmware and configuration upgrade at boot time :

Protocol :

Use DHCP option for remote server and hash file :

IP address of remote server :

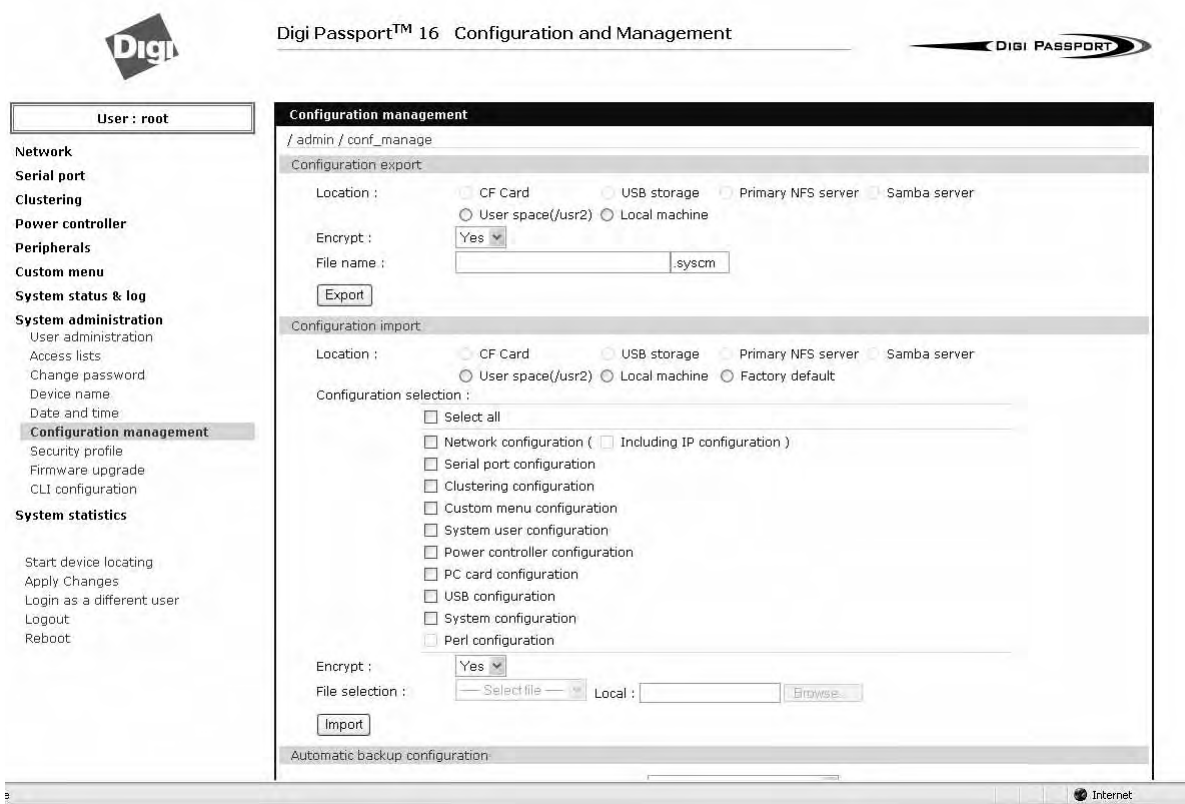
Hash file name :

Note: Do not remove power from the unit while it is updating the firmware. The unit will reboot automatically when it is done flashing the new firmware.

Configuration 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 Passport 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 Passport unit in /tmp/cnf directory by default. Manage these configurations by exporting the files to your location of choice.

1. Click **System 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.



Automatically Saving the Configuration

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.

The screenshot displays the configuration management interface of a Digi Passport Unit. The left sidebar contains navigation options: Change password, Device name, Date and time, Configuration management (highlighted), Security profile, Firmware upgrade, CLI configuration, System statistics, Start device locating, Apply Changes, Login as a different user, Logout, and Reboot. The main content area is titled 'Configuration selection' and includes a list of configuration categories with checkboxes: Select all, Network configuration (Including IP configuration), Serial port configuration, Clustering configuration, Custom menu configuration, System user configuration, Power controller configuration, PC card configuration, USB configuration, System configuration, and Perl configuration. Below this is an 'Encrypt' dropdown set to 'Yes' and a 'File selection' section with a 'Select file' dropdown, a 'Local' text field, and a 'Browse...' button. An 'Import' button is also present. The 'Automatic backup configuration' section is expanded, showing 'Automatic backup option' set to 'Disable'. The 'Location' section has radio buttons for CF Card, USB storage, Primary NFS server, Samba server, and User space(/usr2). The 'Encrypt' dropdown is set to 'No'. The 'File name' field contains '.tar.gz'. The 'Backup interval (hour, 1 - 720)' field contains '0'. The 'Recipient's email address' field is empty. At the bottom are 'Save to flash', 'Save & apply', and 'Cancel' buttons.

Automatically Upgrading the Digi Passport Unit's Firmware or Configuration using TFTP

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

During boot, the Digi Passport 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 Passport 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 Passport 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 Passport 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 Passport 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.

The Structure of the Hash File

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

There are 3 actions defined:

1. Upgrade firmware
2. Upgrade configuration
3. Upgrade any file
4. 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. DigiPassport4, DigiPassport8, DigiPassport16, DigiPassport32, DigiPassport48.

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

<version>. the version number of the firmware

The Digi Passport 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 Passport 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 Passport unit will download the configuration if the version in the hash file is different from the version saved in the file /tmp/cnf/.cnf-version. 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 Passport unit boots again.

A sample hash file can be downloaded from: <http://cm.digi.com>.

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 Passport unit to place the file

Resetting Factory Defaults

These files are downloaded every time the Digi Passport 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>`

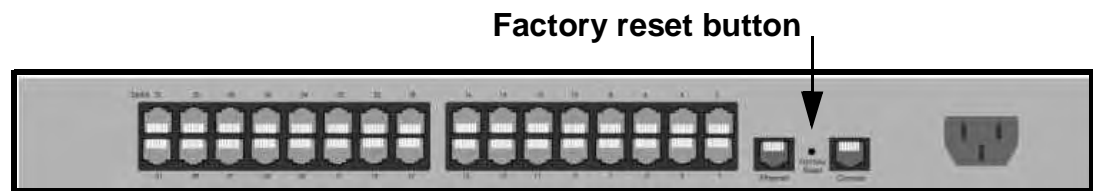
<command> . any application resign on the Digi Passport unit that is executed by root

<parameter> . all parameters this application requires

Example: `touch /tmp/test`

Resetting 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.



Digi Passport 32 shown

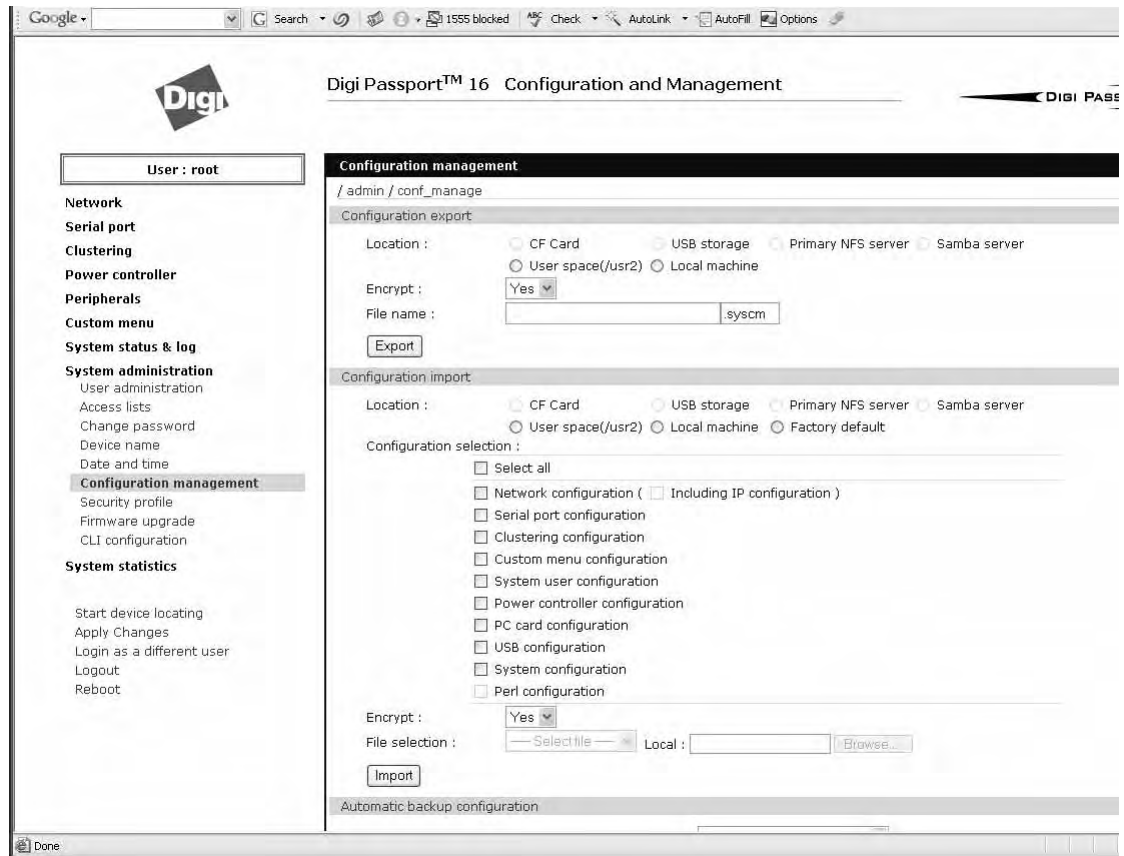
The alternative method to reset the unit is through the web interface or CLI. The web interface provides the option of retaining the IP settings. To use the web interface to reset the Digi Passport unit, do the following:

1. Access the web interface.
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 Passport unit will automatically reboot.

From the CLI you can type "factory_reset" this functions the same as the reset button

The following are the default values when the Digi Passport 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-

Setting Date and Time

The Digi Passport 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 Passport unit for date and time, do the following:

1. Access the web interface.
2. **System administration > Date and time.**
3. To use an NTP server, choose Enable, the NTP server's IP address, the Time offset, and the Date and Time fields.

or

To use the internal battery, fill in 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.

Configuring a Host Name

The screenshot shows the web interface for a Digi Passport 16 unit. The page title is "Digi Passport™ 16 Configuration and Management". The user is logged in as "root". The left sidebar contains a navigation menu with categories: Network, Serial port, Clustering, Power controller, Peripherals, Custom menu, System status & log, System administration (with sub-items: User administration, Access lists, Change password, Device name, Date and time, Configuration management, Security profile, Firmware upgrade, CLI configuration), and System statistics (with sub-items: Start device locating, Apply Changes, Login as a different user, Logout, Reboot). The "Date and time" page is active, showing the following configuration options:

- Use NTP:
- Date (mm/dd/yyyy):
- Time (hh:mm:ss):
- Timezone selection:
- Standard time:
 - Timezone:
 - Time offset from UTC (UTC + [x.x]hours):
- Daylight saving time:
 - Enable/Disable daylight saving time:

At the bottom of the configuration area are three buttons: "Save to flash", "Save & apply", and "Cancel".

Configuring a Host Name

The system administrator can assign a Host name to the Digi Passport unit. This is often helpful for administration purposes to locate a specific Digi Passport unit on the network. To assign the Digi Passport unit a device name, do the following:

1. Access the web interface.
2. **System administration > Device name.**
3. Enter the name you want to assign the Digi Passport unit.
4. Choose Save & apply.

Introduction

The Digi Passport 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 Passport unit through Telnet or SSH. To gain access to the command prompt, the root user uses the username **root** and the root password. The default root password is **dbps**.

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: The root user should be aware that deleting or corrupting files may prevent the Digi Passport 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 Passport 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 Passport unit and the serial ports are the `portaccessmenu` and `configmenu`.

- `portaccessmenu`: This menu allows the user to access the serial ports on the Digi Passport unit.
- `configmenu`: This menu enables the system administrator to configure the Digi Passport 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.
- `portset #`: This command allows the user to reset a specific port. It restarts all processes associated with the port.
- `factory_reset`: functions identical to the Factory reset button

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	gunzip	gzip	zcat	tar
dd	df	du	find	cat
vi	tail	mkdosfs	mke2fs	e2fsck
fsck	mount	umount	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 Passport 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 Passport 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 Passport 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
/.ssh	
ssh public keys	Key file format <<name>>_auth_key2
/bin -active_detect	Active port detection config
passive_detect	Passive port detection config
rportcon	Remote port config
cluster	
./cluster_p2p	Directory for Peer to Peer clustering
cluster.cnf	Basic cluster info
./cluster_p2p/cluster_p2p.cnf	Basic Peer to Peer cluster info
unit#.cnf	Basic slave info
/etc -client.pem	Web Certificate
dhcpd.opt	DHCP certificate file
group	User group info
hostname	Passport host name
hosts	Name resolution hosts file
interfaces	Basic loopback (lo) and ethernet interface (eth0, eth1) info (lp, gateway, etc).
ip6tables.save	IPv6 IP access
iptables.save	IPv4 access
krb5.conf	Kerberos config file
nsswitch	Search order for files and DNS
./pam.d	Authorization table directory
passwd	User password file
./ppp -	PPP info directory
resolv.conf	DNS info

Important File Locations

File Name	Description
server.pem	Stores the private keys when using SSH with key certification.
shadow	The secure passwd file
snmpd.conf	All snmp info
sshd_config	SSH config file
syslog-ng.conf	Syslog-ng config file
timezone	Timezone file
./xinetd.d	Network services for serial and remote ports
./xinetd.d/master - ./xinetd.d/port# - ./xinetd.d/telnet -	
menu	
./menu	Directory for custom menu xml files
ports	
./allports	All ports config dir
./master.cnf	Port access menu config file
./port#	Specific port and remote config dir
./port#/keywords.cnf	Port and remote port keyword alert file
./port#/portinfo.cnf	Port and remote port info file
./rport.default	Remote port config dir
./power	
./power/power.cnf	Power controller config
./sys	
autobk.cnf	Auto backup
autofwup.cnf	Auto firmware via TFTP
cliauth.cnf	Authentication method via CLI
datetime.cnf	Date/time
modem.cnf	Internal modem
./network	Directory with all network config files
ccard.cnf	PC Card
security.cnf	Security profile

File Name	Description
syslog-ng.cnf	Syslog-ng
system.cnf	System log

User Storage Space

The Digi Passport unit comes with 16 megabytes 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 Passport 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
```

Example Scripts

```
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 Passport products (for SSH only)

This prevents root access from any means except physically logging in on the Digi Passport 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 Passport 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 be 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: <http://ftp.digi.com/support/utilities/digicm/>

User Administration

Add, edit or delete users with the Digi Passport unit's command line interface.

```
root@Digi_CM_Device:~# useradd -d/tmp-g 502 -s/bin/editconf -p test1 test1
usage: useradd [-u uid [-o]] [-g group] [-G group,...]
              [-d home] [-s shell] [-c comment] [-m [-k template]]
              [-f inactive] [-e expire] [-p passwd] name
useradd -D [-g group] [-b base] [-s shell]
              [-f inactive] [-e expire] ]
root@Digi_CM_Device:~#
```

- 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 Passport 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 Passport 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 Passport 48 can be deactivated and reactivated with the following file and command.

Note: All other Digi Passport units have the locator feature without a Find Me LED. To identify another Digi Passport 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/blinkled stop
```

```
root@mankato:~# /bin/blinkled start
```

Introduction to the Configuration Menu

The configuration menu presents the same functionality in configuring the Digi Passport 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 Passport unit, log in (username `root`, password `dbps`) and enter `configmenu` to start any configuration. If you log in as `admin`, the configuration menu will automatically appear.

Accessing 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 Passport 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 Passport 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.

```

root@Digi_Passport ~]# configmenu
-----
Welcome to Digi Passport 16 configuration page
Current time : 04/18/2006 14:21:48      F/W REV.      : v0.8.0a1
Serial No.   : pp16proto-0610-0001     MAC addr.(eth0): 00-40-9D-22-DE-60
IP addr.(eth0) : 10.4.102.55
-----
1. Network
2. Serial port
3. Clustering
4. Power controller
5. Peripherals
6. System status & log
7. System administration
8. Stop device locating

[h]help, [s]lave, [a]pply, e[x]it
COMMAND <Display HELP : help>>

```

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.

Configuring 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.

The Save changes option saves changes to flash memory only.

```

No. Title Mode Dest/AssignedIP Port Protocol Serial-Settings
1. Port Title#1 Al CS 0.0.0.0 7001 Telnet 9600-N-8-1-NO
2. Port Title#2 CS 0.0.0.0 7002 Telnet 9600-N-8-1-NO
3. Port Title#3 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 9600-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
14. Port Title#14 CS 0.0.0.0 7014 Telnet 9600-N-8-1-NO
15. Port Title#15 CS 0.0.0.0 7015 Telnet 9600-N-8-1-NO
16. Port Title#16 CS 0.0.0.0 7016 Telnet 9600-N-8-1-NO
<ESC> Back, <ENTER> More
[h]help, [s]lave, [a]pply, e[x]lit, [+l]add, [-r]remove, [0]all
COMMAND <Display HELP : help>> 1

Ports configuration <1>
/serial/serial_config/ports/*1

1. Port management
2. Apply all ports settings
3. Automatic detection
4. Port title
5. Host mode configuration
6. Virtual RUM configuration
7. Serial port parameters
8. Port logging
9. Authentication
10. User access control
11. Alert configuration

[h]help, [s]lave, [a]pply, e[x]lit
COMMAND <Display HELP : help>> 5

Host mode configuration
/serial/serial_config/ports/*1/hostmode

1. Host mode : Console server
2. Type of console server : Other
3. Rackable System Management Card : Enable
4. Enable/Disable assigned IP : Disable
5. Listening TCP port : 7001
6. Protocol : Telnet
7. Inactivity timeout : 100
8. Enable/Disable port escape sequence : Enable
9. Port escape sequence : Z
10. Port break sequence : ~break
11. Use comment : No
12. Quick connect via : Web applet
13. Web applet encoding : English <latin1>

[h]help, [s]lave, [a]pply, e[x]lit
COMMAND <Display HELP : help>> 6

Protocol
/serial/serial_config/ports/*1/hostmode/protocol

1. Telnet[*]
2. SSH
3. RawTCP

[SELECT]> 2
    
```

3. Use the ESC key to return to the main configuration menu.
4. Choose Exit and apply changes.

Adding, Editing, and Removing Users

1. Choose System administration > User administration and then choose an operation to perform (Add, Remove, or Edit)
2. Configure the user as required.

Adding and Configuring a PC Card

To add a modem card, compact-flash card, wireless LAN card, or a network card to the Digi Passport unit using the configuration menu, do the following:

1. Access the configuration menu. (1 Network Configuration, 5 Peripherals)
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. 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.

Port Parameters

```
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.

Port Parameters

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.

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
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 configre < 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 Passport 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 Passport 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 "Adding a Compact-flash Card" on page 33. In Passport, all log messages are sent to syslog-ng daemon. And 'local 0' facility is only used for system log messages. And 'local 1' ~ 'local7' facilities can be used for port log.

Each system log logging or port log logging to Syslog server(syslog-ng) can be set at System logging or Port logging menu, respectively. There is no enable/disable option for System log to SYSLOG server because it is default function.

And you can also specify facility for each port log from local1 to local7 (local 0 facility is fixed for system log). With this configuration, the management of all messages sent to Syslog server(syslog-ng) can be configured at SYSLOG-NG configuration.

By default, syslog-ng configuration has internal RAMDISK(/var/log/messages) logging configuration for system log message(local 0). You can change filter options for this default configuration by clicking it. Syslog-NG filter configuration page has all filter options that syslog-ng daemon supports. So if you add Priority(debug) option to default system log configuration, All local syslog messages with debug priority will be logged to /var/log/messages additionally. (Linux kernel and xinetd send some of their message to syslog with debug priority.)

To send log messages to a remote syslog server, you should add new destination with "destination=TCP/UDP" and "Location=IP address of remote server" to syslog-ng configuration.

Procedure for an NFS or SYSLOG Server

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.

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.

So if you add new destination with UDP, local 0 facility and IP address of remote syslog server to syslog-ng configuration, then you can receive system log messages from Passport.

Using the flexibility of Syslog-NG configuration menu,

4. you can add 2nd or 3rd remote SYSLOG server or you can group port logs according to the facility..

Configuring 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.

Configuring 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
-----
->

```

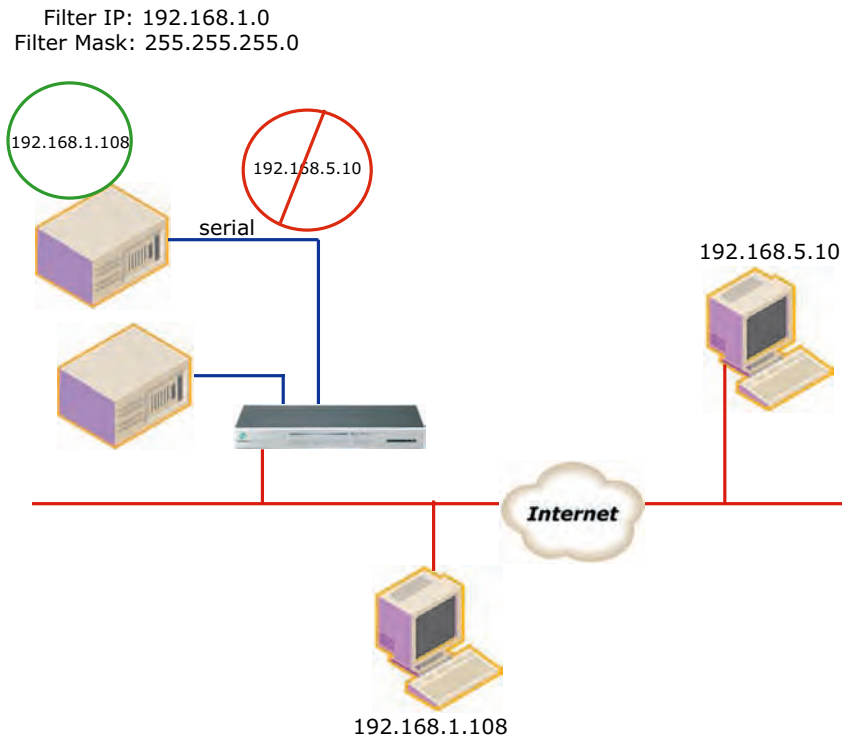
3. Enter the desired parameters for the menu items.

Configuring Network IP Filtering

The Digi Passport 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.

Configuring Network IP Filtering

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



It is also possible to enable or disable specific services of the Digi Passport unit by creating IP Filtering rules:

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

#	Interface	Option	IP address/Mask	Protocol	Port	Chain rule	Action
1	all	Normal	0.0.0.0/0.0.0.0	TCP	22	ACCEPT	Remove
2	all	Normal	0.0.0.0/0.0.0.0	TCP	443	ACCEPT	Remove
3	all	Normal	0.0.0.0/0.0.0.0	TCP	80	ACCEPT	Remove
4	all	Normal	0.0.0.0/0.0.0.0	TCP	23	DROP	Remove
	all	Normal		TCP		ACCEPT	Add

Save to flash Save & apply Cancel

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 Passport 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 Passport 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.

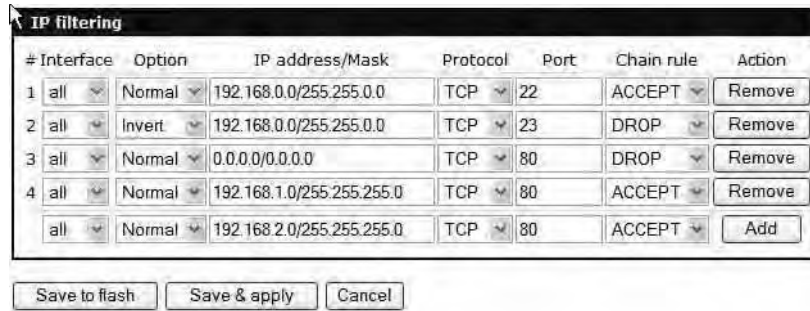
To remove a rule, click the Remove button.

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	<p>Defines SSH access to the Digi Passport unit (port 22).</p> <ul style="list-style-type: none"> 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	<p>Defines Telnet access to the Digi Passport unit (port23).</p> <ul style="list-style-type: none"> 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, 4, 5	<p>Define access to the Digi Passport unit using HTTP (port 80).</p> <ul style="list-style-type: none"> 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 Host 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

Network IP Filtering

To configure the Digi Passport 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 Passport 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.

```

c:\ Telnet 143.191.3.9
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
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 configure < 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, "Viewing A Sniff Session" on page 191.

Viewing 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 Passport 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.

```

c:\ Telnet 143.191.3.9
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).

```

c:\ Telnet 143.191.3.9
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

Escape Sequence Ctrl+	Description of Action	Occurrence
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 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.

Upload Server Certificate

```
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
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 configre < 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
--> ?

Serial configuration --> All ports --> Authentication
-----
1. Authenticaon 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.

But please note that this menu is displayed only when you run configmenu on the serial console of the Digi Passport 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.

Please don't forget to run saveconf command in CLI if you want to keep this change permanently.

You can use your own certificate for your Digi Passport 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
# ./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.cnf 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 password 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.

Upload Server Certificate

----- ; 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
```

Making 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 Passport*

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)

Signing 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)" on page 195

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 Passport'

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

Dial-in Modem Access

```
Subject: C=US, ST=Minnesota, L=Minneapolis, O=Digi International, CN=Digi Passport
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 Passport 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 Passport
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 Passport
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 Passport 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 configre < 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 Passport 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 Passport 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 : qle0s0=2
<ESC> Back, <ENTER> Refresh
----> 1
Select Host mode :
1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
4 = Dial-In Terminal 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

By 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 Passport 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      0 D UNKNOW  2      0      0      0 D UNKNOW
  3      0      0      0 D UNKNOW  4      0      0      0 D UNKNOW
  5      0      0      0 D UNKNOW  6      0      0      0 D UNKNOW
  7      0      0      0 D UNKNOW  8      0      0      0 D UNKNOW
  9      0      0      0 D UNKNOW 10      0      0      0 D UNKNOW
 11      0      0      0 D UNKNOW 12      0      0      0 D UNKNOW
 13      0      0      0 D UNKNOW 14      0      0      0 D UNKNOW
 15      0      0      0 D UNKNOW 16      0      0      0 D UNKNOW
 17      0      0      0 D UNKNOW 18      0      0      0 D UNKNOW
 19      0      0      0 D UNKNOW 20      0      0      0 D UNKNOW
 21      0      0      0 D UNKNOW 22      0      0      0 D UNKNOW
 23      0      0      0 D UNKNOW 24      0      0      0 D UNKNOW
 25      0      0      0 D UNKNOW 26      0      0      0 D UNKNOW
 27      0      0      0 D UNKNOW 28      0      0      0 D UNKNOW
 29      0      0      0 D UNKNOW 30      0      0      0 D UNKNOW
 31      0      0      0 D UNKNOW 32      0      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 Passport unit will reboot automatically. If a **Firmware upgrade failed!** Warning appears, do not reboot the unit but repeat the upgrade process.

Restoring 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
```

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 "Adding and Configuring a PC Card" on page 181 for more information.

Setting Date and Time

Date and time on the Digi Passport unit can either be kept internally or by an NTP server. To set the parameters for date and time on the Digi Passport 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.

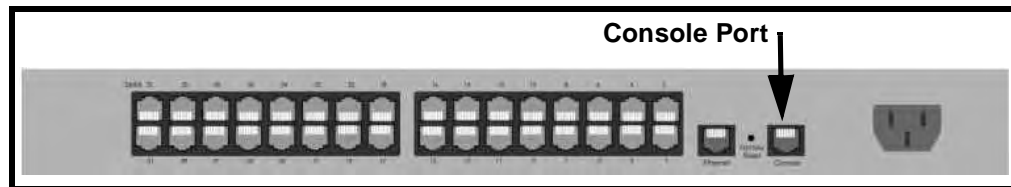
Accessing the Boot Loader Program

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 Passport 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 Passport unit to a serial port on a workstation. Use the Ethernet cable packaged with the Digi Passport unit and attach the DB-9 adapter. The arrow in the following graphic points to the Console Port.



back of Digi Passport 32 shown

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 Passport unit. From the Boot Loader menu, choose the number 3 to access the Hardware test. Options for several components appear.

Disaster Recovery

The Digi Passport unit provides a disaster recovery procedure in the event the configuration data is destroyed or corrupted. The Digi Passport unit automatically restores a corrupted configuration file system to the factory default settings. However, if the Digi Passport 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 Passport 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 Passport 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 Passport unit.
4. Press the ESC key within three seconds of applying power to the device.

The following screen appears.

Accessing the Boot Loader Program

Use the ESC key to return to an earlier menu screen.

```
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. RIC 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 Passport 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.

Introduction

This chapter provides information on Digi Passport 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

Digi Passport 48

Hardware Specifications		
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)
Dimensions: packaged	20.375" x 15.25" x 4.75 (517.5 mm 387.3 mm x 120.6 mm)	20.375" x 15.25" x 4.75 (517.5 mm 387.3 mm x 120.6 mm)
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 Passport 16 and Digi Passport 32

Attribute	AC Powered Value	DC Powered Value
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)
Dimensions: packaged	20.375" x 15.25" x 4.75 (517.5 cm x 387.3 cm x 120.6 cm)	20.375" x 15.25" x 4.75 (517.5 cm x 387.3 cm x 120.6 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 Passport 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
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 Passport 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	100Mbps	On when 100Base-TX connection is detected
	LINK	On when connected to an Ethernet network
	Act	Blinks when there is activity on the Ethernet port
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 Passport 48

About Serial Port Cabling

The Digi Passport 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 Passport serial cable as well.

Serial Port Pinouts

The Digi Passport unit uses an RJ-45 connector for serial ports. Pin assignments are listed in the following table.

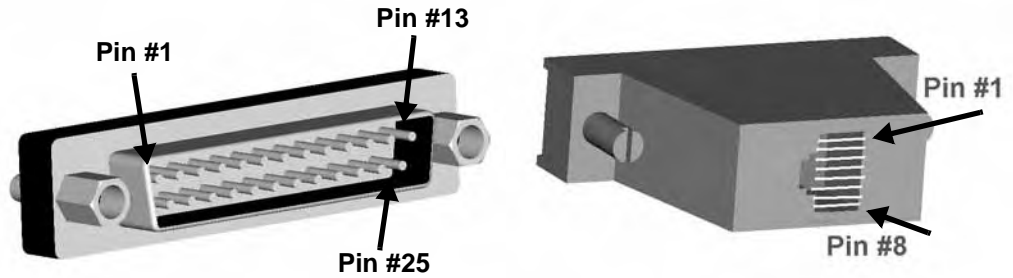
Pin	Description
1	CTS
2	DSR
3	RxD
4	GND
5	DCD Note: Inbound signal can also be used as a second ground.
6	TxD
7	DTR
8	RTS

Cable Adapters

The Digi Passport 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

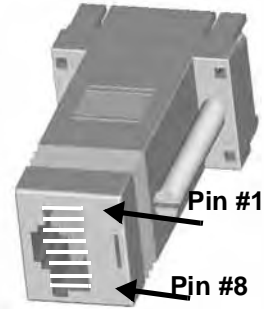
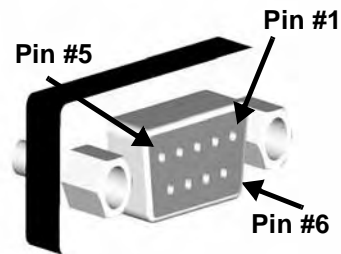
(Digi 8-pack reorder P/N 76000672)



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	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

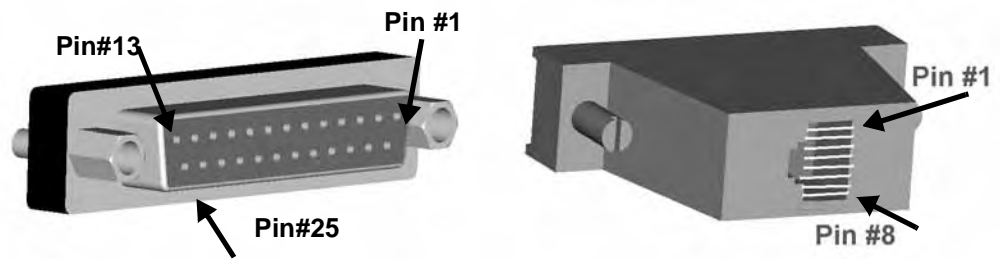
DB-9 Female Console Adapter
 (Digi 8-pack reorder P/N 76000671)



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	GND	Connected to	5	GND
6	TxD	Connected to	2	RxD
7	DTR	Connected to	1	DCD
			6	DSR
8	RTS	Connected to	8	CTS

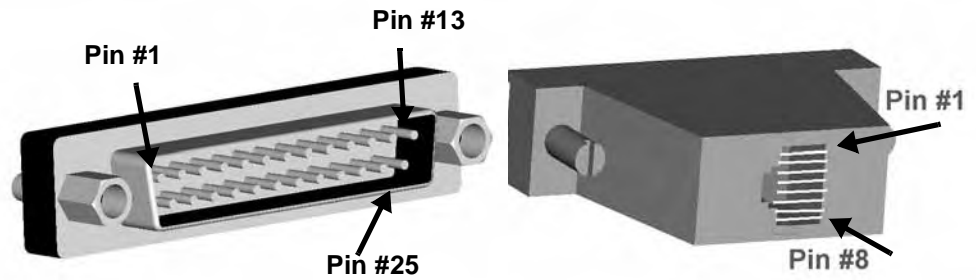
DB-25 Female Console Adapter
 (Digi 8-pack reorder P/N 76000673)



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)



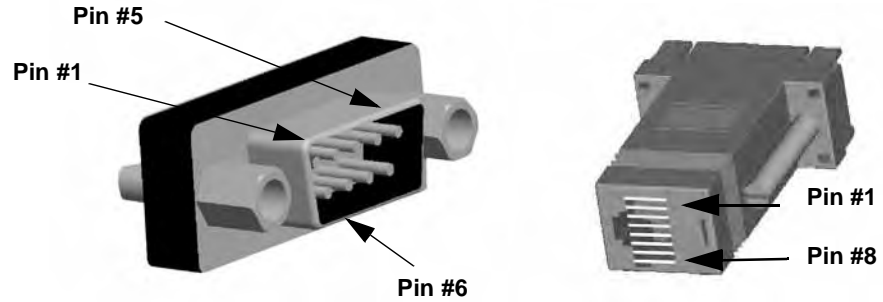
DB-25 Male Modem to RJ-45 Pin Assignment

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

Ethernet Pinouts

DB-9 Male Modem Adapter (Digi 8-pack reorder P/N 76000702)

(Available but not included)



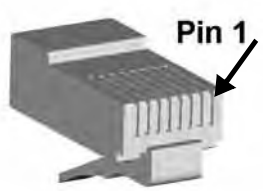
DB-9 Male Modem to RJ-45 Pin Assignment

RJ-45	Signal		DB-9M	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

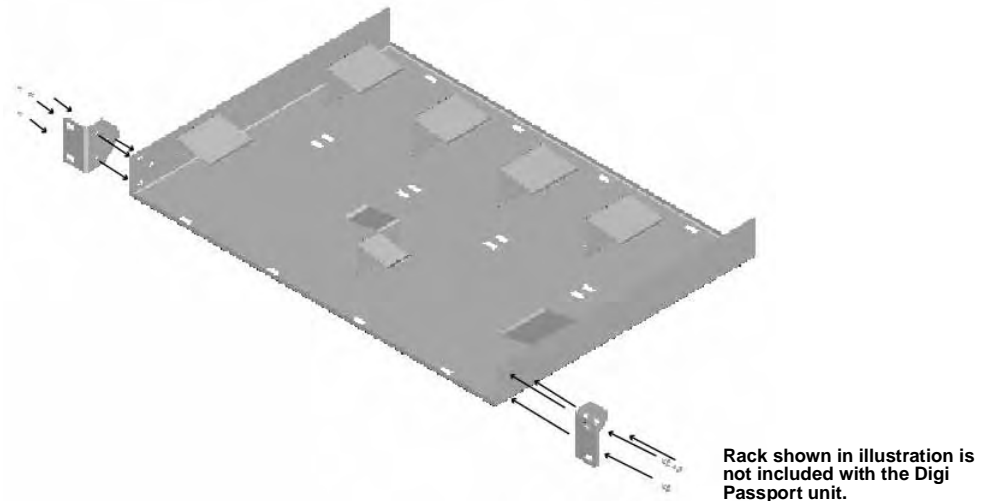
Ethernet Pinouts

The Digi Passport 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 Passport unit on the rack.

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.

Rack Mounting Installation

- 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.
-

This equipment is indoor use and all the communication wirings are limited to inside of the building."

Rack-mountable

1. Elevated Operating Ambient Temperature – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in a environment compatible with the manufacturer's maximum rated ambient temperature (T_{mra}).
2. Reduced Air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised,
3. Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
4. Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
5. Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit.

Lithium Battery

"CAUTION"

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer.

(Manufacturer: SONY FUKUSHIMA CORP., Model: CR2032.

Toshiba Battery Co.,Ltd , Model : CR2032)

DISPOSE OF USED BATTERIES ACCORDING TO THE NATIONAL CODE OR RECYCLING PROGRAM.

Safety

- US: UL1950
- Canada: CSA 22.2 No. 60950
- Europe: EN60950 (CB Scheme Report)

Working Inside the Digi Passport Unit

NOTICE: Do not attempt to service the Digi Passport unit yourself, except when following the instructions from Technical Support personnel. In such a case, first perform the following actions:

- Turn off the Digi Passport 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 Passport 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.

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 Passport 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 Passport unit:

- Do not position the Digi Passport 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 Passport 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 Amps maximum.

Note: The Digi Passport unit is intended to connect to networking devices. Do not attempt connecting to a telephone line.

Safety Instructions

CAUTION: Do not operate the Digi Passport unit with the cover removed.

- To avoid shorting out the Digi Passport 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 Passport 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 Passport 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 Passport 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 Passport unit. If it gets wet, contact Technical Support.
- Do not push objects into the openings of the Digi Passport unit. Doing so can cause fire or electric shock by shorting out interior components.
- Keep the Digi Passport unit away from heat sources and do not block cooling vents.

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 Passport 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.

3DES 27

A

accessing a port
 web interface 17
 ADDP (Advanced Device Discover Protocol) 16
 administration See system administration
 alerts and notifications
 for Power Controller 130
 port event handling 65
 SMTP alerts 62
 SNMP information 62
 traps 63
 apply all ports settings 51
 applyconf 153
 assigning IP settings 25
 authentication 84
 configuration menu 171
 configuring 84
 local 84
 automatic device recognition 23
 configuring 49

B

Blowfish 27
 Boot Loader program 179
 accessing 180
 boot sequence 154

C

cable adapters 186
 callback 122
 Cascading multiple Digi RPM units 136
 certifications
 Emissions 195
 Immunity 195
 Safety 193
 Solaris Ready 195
 command line interface 17
 example scripts 156
 important file locations 154
 Linux commands 153
 user administration 158
 compact-flash card
 adding 31
 configuring 32
 formatting the card 32
 configmenu 16, 153
 configuration management 146
 configuration menu 16
 description 16

 using 30
 configuring automatic device recognition 49
 configuring host mode 54
 configuring system logging 41
 console server mode 52
 custom menus 20, 89

D

date and time
 configuration menu 179
 setting 151
 default menu
 port access menu 92
 default password 15
 defaults See factory defaults
 device name
 configuring 151
 device recognition
 configuring 49
 dial-in modem
 configuring access 121, 128, 175
 mode 53
 dial-in terminal server 54
 configuring access 124
 configuring access (configuration menu) 176
 Digi Passport
 access methods 17
 adding and configuring PC cards 31
 certifications 193
 configuration menu interface 161
 configuration methods 15
 configuring ports 47
 feature overview 13
 hardware information 183
 port clustering 139
 power controller 127
 system administration 69
 web interface for 16
 Digi RPM
 cascading multiple units 136
 direct port access 20
 disaster recovery 180
 DTR settings 56

E

emissions certifications 195
 EMS support 95
 enabling system logging 37
 encryption
 SSH 27
 wireless LAN 34

F

- factory defaults
 - reset button 150
 - resetting 150
 - restoring (configuration menu) 179
 - values 150
- firmware
 - automatically upgrading 147
 - upgrade (configuration menu) 178
 - upgrading 145

H

- hardware specifications 183
- hardware test menu 180
- host mode
 - configuring (configuration menu) 163
- host name configuration 151
- HyperTerminal 25

I

- immunity certifications 195
- inter-character timeout 56
- IP filtering
 - configuring network 73
 - examples 76
 - network (configuration menu) 167
 - port (configuration menu) 168
- IP settings 25

L

- LDAP 84
- LED Indicators 185
- Linux
 - commands 153
 - default script 154
 - file and disk utilities 154
 - Hard Hat 153
 - network utilities 154
 - shell utilities 154
 - system utilities 154

M

- menus
 - adding menu items 91
 - assigning users 92
 - creating menu names 90
 - creating submenu 91
 - port access menu 164
 - using the configuration menu 161
- Microsoft Server 2003 SAC support 95
- modem
 - adding 124
- modem init string 121
- modem test 122

N

- network card
 - adding 32
- NTP server 151

P

- password 15
- PC card
 - adding and configuring (configuration menu) 163
- PC cards
 - compact-flash 31
 - compatible cards 31
 - installing and configuring 31
 - network 32
 - serial modem 34
 - wireless LAN 33
- port
 - apply all settings 51
 - reset 49
- port access menu 19, 164
- port clustering
 - assigning master unit 140
 - configuration menu 177
 - configuring slave ports 140, 141
- Port Escape Menu 21
- port logging 43
 - enabling 38
- port parameters 25
 - configuration menu 164
- port title 49
- portaccessmenu 153
- portreset # 153
- Power Controller
 - overview 127
- power controller
 - alarms and thresholds 130
 - configuring 128
 - installing 128
 - managing 134
- protocols 56
 - RawTCP 56
 - Telnet 56

R

- Rackable Systems MGMT Card 117
 - set up 117
- RADIUS 84
- RealPort 47
- resetting ports 49

S

- SAC support 95
- safety certifications 193
- saveconf 153
- saving and applying changes 22

- serial modem
 - adding 34
- serial port parameters 56
- serial port pinouts 185
- SMTP
 - alerts 62
 - configuring 166
- sniff session
 - configuration menu 168
 - viewing 169
- SNMP 62
 - configuring 63, 166
 - configuring (configuration menu) 166
 - managing the SNMP protocol 64
- Solaris Ready 195
- SSH 20
 - accessing a port 27
 - configuring (configuration menu) 162
 - encryption methods 27
- SYSLOG server
 - enabling 40
- system administration
 - configuration management 146
 - firmware upgrades 145
 - host name configuration 151
 - resetting factory defaults 150
 - user administration 69
- system logging 164
 - configuration menu 164
 - configuring device (configuration menu) 165
- system logs 43

T

- TACACS+ 84
- Telnet 20
- terminal server mode 53
- TFTP 147
- traps 63

U

- user access control
 - to Power Controller 132
 - to serial ports 77
- user groups 15
- user storage space 156
- username 15
- users
 - adding 89
 - adding, editing, and removing 29, 69
 - admin username and default password 15
 - administration 69
 - root username and default password 15, 153
 - system admin 15

W

- web interface menu 17
- WEP 33
- wireless LAN card 33



www.digi.com

Making
DEVICE NETWORKING
easy™



PN:(1P) 90000767-88 A