Digi Passport User's Guide

90000767_D

Contents

Chapter 1 Introduction

Chapter 2 Getting Started

Chapter 3 Install and Configure PC Cards

Chapter 4 System Status and Port Logging

Chapter 5 Configure Ports

Chapter 6 Alerts and Notifications

Chapter 7 Service Processors

Chapter 8 Users, Security, and Authentication

Chapter 9 Custom and Default Menus

Chapter 10 Microsoft SAC Support

Chapter 11 Configure and Use freeKVM

Chapter 12 Rackable® Systems Management Card

Chapter 13 Configure Remote Dial-In Access

Chapter 14 Power Controller

Chapter 15 Port Clustering

Chapter 17 Command Line Interface

Chapter 18 System Administration

Chapter 19 Specifications and Certifications

Chapter 1 **Introduction**

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

Feature Category	Feature
Network and Security	• IP v4/v6 dual stack • RealPort® and Encrypted RealPort support • 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 and Certifications	• User access per port • Access lists per port • Local user database • TACACS+ • RADIUS • RSA SecurID® support using RADIUS • LDAP and Active Directory • Kerberos support for customized PAM Modules • Solaris Ready
Console Access Methods	• Direct SSH and Telnet to individual ports • SSH sessions simultaneously on all ports • Web interface--HTTP/HTTPS • RemotePorts™ extends console management features to remote devices • Multi level menus • Multiple concurrent users per port • Independent IP addresses per port • Raw TCP • Port escape menu • Service Processors: IPMI 2.0, iLO, DRAC, ALOM
Console Monitoring Capabilities	• Automatic Device Recognition (ADR) • Port Triggers and Alerts • Local port logging

Feature Category	Feature
Digi Passport Self-Management Capabilities	• Advanced Digi Discovery Protocol (ADDP) for locating the the Digi Passport unit unit on the network • Find Me locator light • Telnet/SSH • Command line interface • Web interface--HTTP/HTTPS • SNMPv3 management interface • Secure Clustering: Single IP address for multiple Digi Passport devices • TFTP firmware with automated capability and configuration update upon boot • Custom applications • Perl programming and scripting • USB Export option • Flash upgradable
freeKVM™ access	• Windows Remote Desktop • VNC • Xmanager (X Window System) • Web Redirection • Radmin • User defined
Expandable Capabilities	• CompactFlash/PC Card: - Flash memory card - Wireless LAN adapter (802.11b) - Ethernet LAN adapter - PSTN/CDMA modem card • USB: Expandable storage to USB flash • Integrated power management and control in conjunction with Digi RPM and third-party power strips • External logging (syslog, NFS, PC card, USB Flash)
Service processors	Support for various service processors, such as: • Intelligent Platform Management Interface (IPMI), Integrated Lights Out (iLO), • Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), • Dell Remote Access Controller (DRAC). Service processors are configured through the remote port.

Discovering and Configuring the Digi Passport unit

See the Quick Start Guide that came with the the Digi Passport unit to connect the hardware and configure an IP address for the unit.

Alternatively, insert the Software and Documentation CD in your computer’s CD drive, and select the **Digi Device Discovery** program. This program uses the Digi-proprietary Advanced Digi Discovery Protocol (ADDP) to discover all devices on a network. Once discovered, devices can be viewed and configured. Start the program and click the correct device to configure.

The Digi Device Discovery program knows the default password for the the Digi Passport unit. If the password has been changed from the default, **dbps**, a prompt for entering the password is displayed.

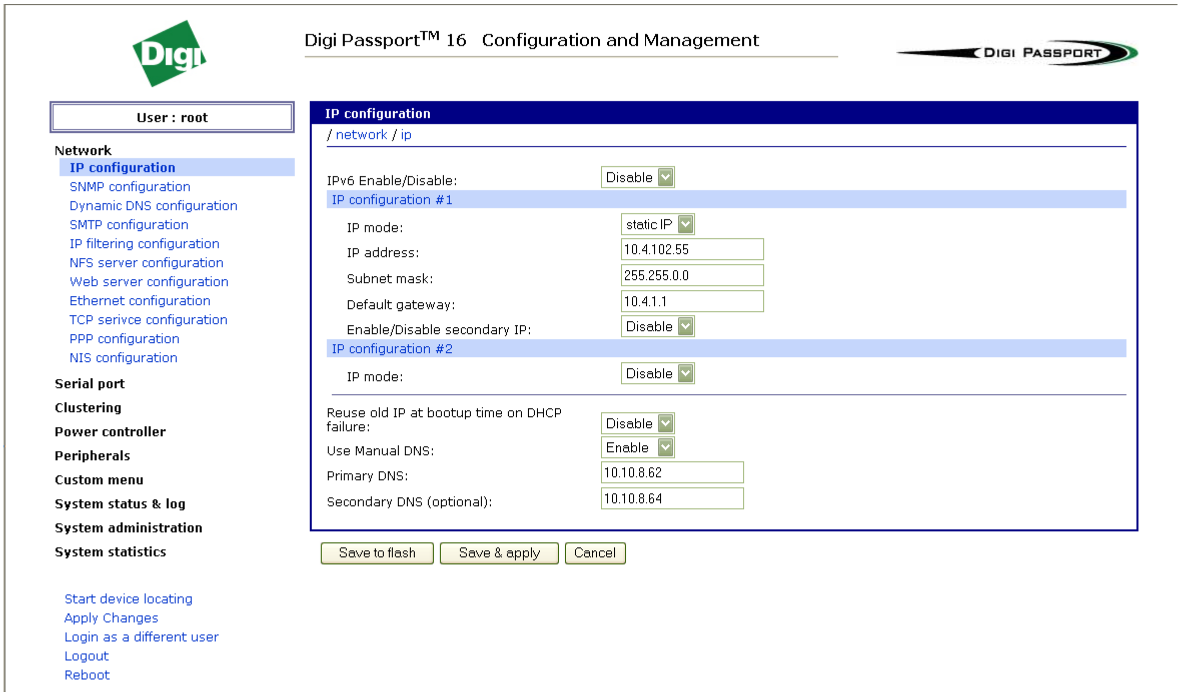
Configure the IP address. Once the Digi Passport is configured with a valid IP address, log in to the Web user interface with username **admin**, password **admin**.

Configuration User Interface Options for Digi Passport

There are several interface options for configuring the Digi Passport unit: using the web interface, configuration menu, command line interface, or Simple Network Management Protocol (SNMP).

Web Interface

The Digi Passport 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. The web interface can be accessed either by using Digi's device discovery tool, Advanced Digi Discovery Protocol (ADDP), or by entering the IP address of the Digi Passport unit or its hostname directly into the address bar of a browser. Here is an example page of the web interface.



Digi Passport™ 16 Configuration and Management

User : root

IP configuration

/ network / ip

IPv6 Enable/Disable: Disable

IP configuration #1

IP mode: static IP

IP address: 10.4.102.55

Subnet mask: 255.255.0.0

Default gateway: 10.4.1.1

Enable/Disable secondary IP: Disable

IP configuration #2

IP mode: Disable

Reuse old IP at bootup time on DHCP failure: Disable

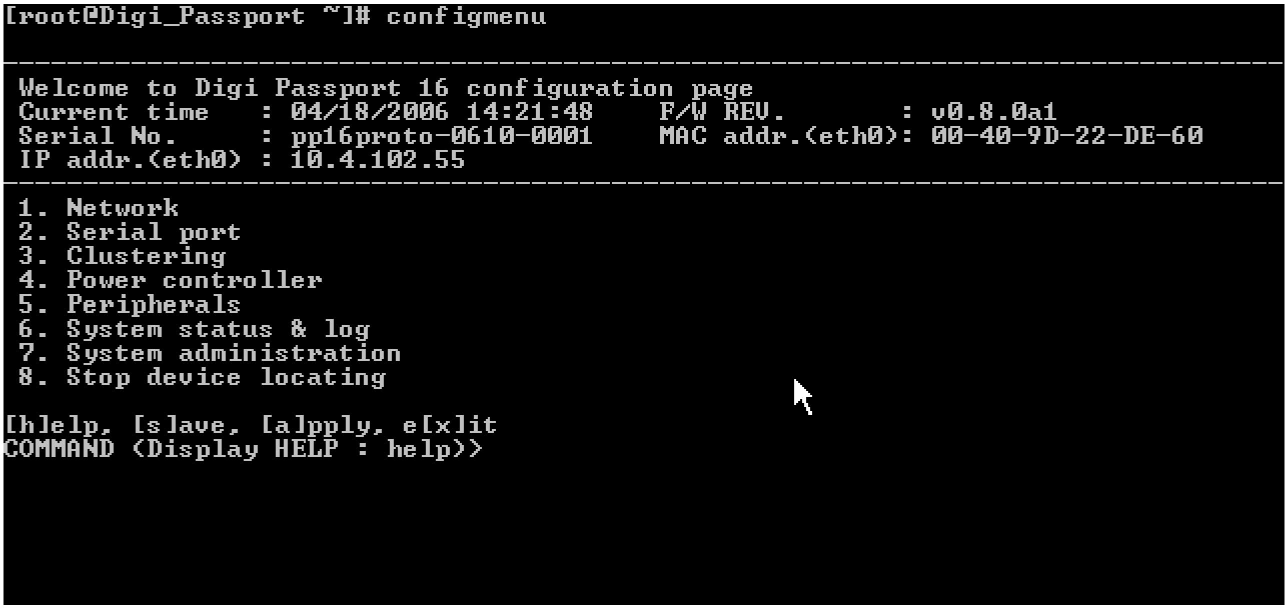
Use Manual DNS: Enable

Primary DNS: 10.10.8.62

Secondary DNS (optional): 10.10.8.64

Configuration Menu

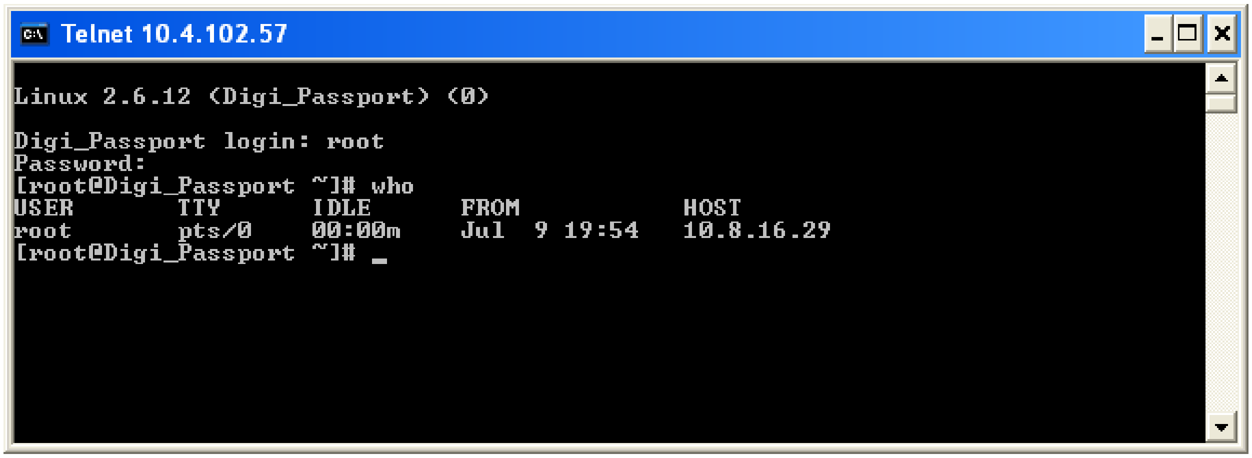
The root user and system administrator have full access to the configuration menu from a Telnet or SSH session or a serial connection through the console port. Functionality is similar to the web interface, with the exception of custom menus, which can be created only from the web interface. The configuration menu is presented by entering the command **configmenu**. For more information about the configuration menu, see "Configuration Menu Interface" on page 239.



```
[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]ave, [a]pply, e[x]it
COMMAND (Display HELP : help)>
```

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, and the admin user can be granted read-only permission.



```
Linux 2.6.12 (Digi_Passport) (0)

Digi_Passport login: root
Password:
[root@Digi_Passport ~]# who
USER        TTY       IDLE      FROM          HOST
root        pts/0     00:00m    Jul  9 19:54   10.8.16.29
[root@Digi_Passport ~]# _
```

SNMP

An SNMP MIB to configure the Digi Passport unit is available on the Passport CD and can be downloaded from support.digi.com. To allow use of this MIB, SNMP configuration must be enabled in the security profile. In the Web interface, this is accomplished through the **System Administration > Security Profile** section of the configuration screen. See "Security Profile" on page 148 for more information

Users and User Groups

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.

User Groups

The Digi Passport unitcomes 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 multiple people are responsible for the Sun Servers and identical access rights for them are desired, create an access list named **Sun-admin**, which grants access to all the ports connected to Sun servers. Then make all the Sun administrators members of the **Sun-admin** access list. See "Add an Access List and Add Users to It" on page 40 for more information.

Options for Accessing the Digi Passport Ports

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

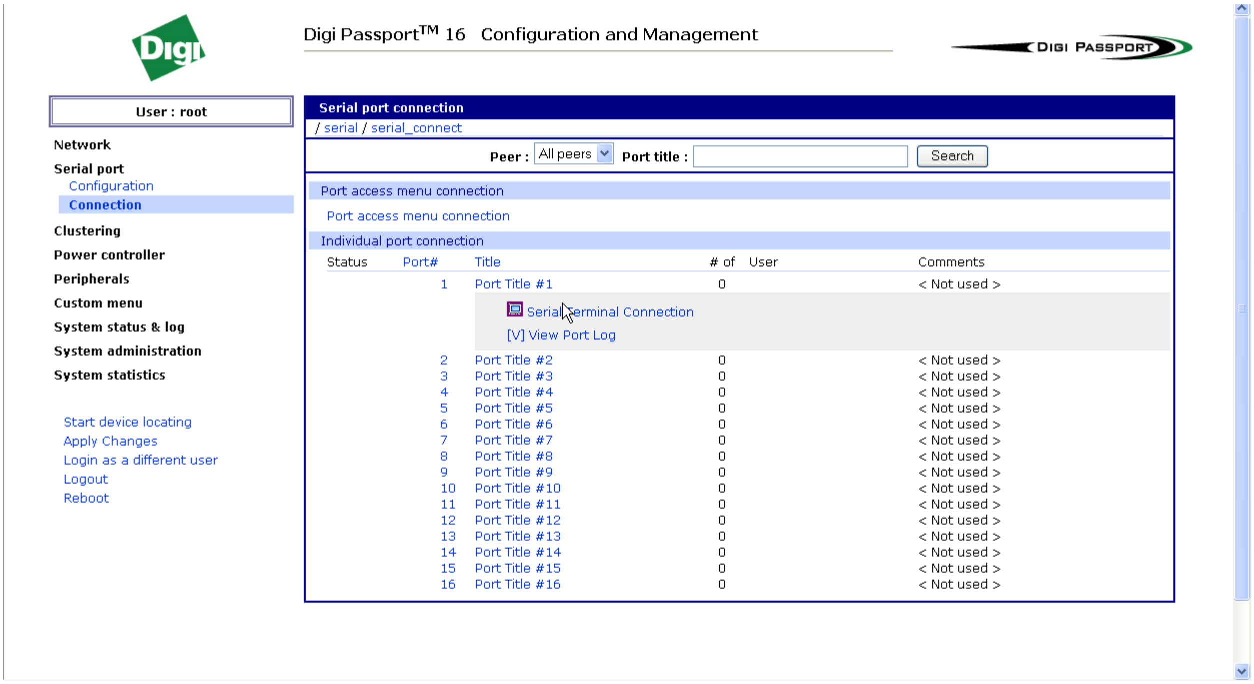
- Web Interface
- Port Access Menu
- Direct Port Access
- Custom Menus

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 address bar. Only ports with allowed access are displayed.

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

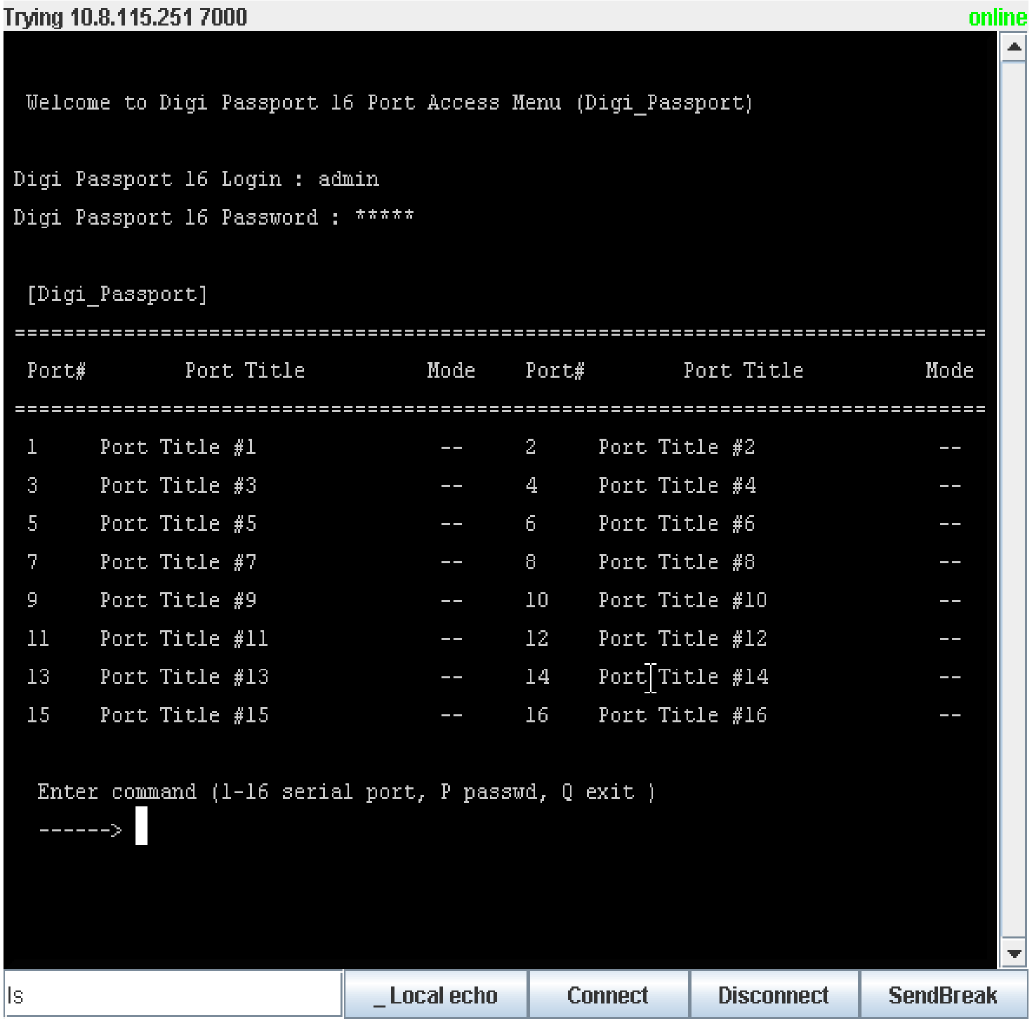
1. Enter the IP address of the Digi Passport unit into the address bar of the browser to access the web interface.
2. Click **Serial port** > **Connection**.



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.



```
 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 )
  ------>
```

The web interface can also be configured to call a local Telnet or SSH application, see "Host Mode Configuration" on page 71.

Port Access Menu

Access Type	Permissions	Procedure
Web interface	Any user can use this method.	1. Access the web interface 2. Select **Serial port > Connection > Port access menu connection** 3. Log in
Telnet/SSH	Any user can use this method.	1. Telnet to the Digi Passport unit specifying its IP address and port 7000. (7000 is the default socket port for access menu) 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. The example assumes that the Listening TCP port is 7003, the default for port 3.

Type	Command Syntax	Example: Connection to Port 3
Telnet	telnet *ip-address tcp-port* where *ip-address* is the Digi Passport unit’s IP address and *tcp-port* is the Listening TCP port for a port	telnet 192.168.15.7 7003 (7000 is the default socket port for both Telnet and SSH)
SSH	ssh *user-name@ ip-address tcp-port* where *user-name* is a user’s name, *ip-address* is the Digi Passport unit’s IP address and *tcp-port* is the Listening TCP port for a port ssh *user-name:”p=port-number”@ip-address* or ssh *user-name:”t=port-title”@ip-address*	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
WEB	http://ip-address/connect.asp?t=*port-title* http://ip-address/connect.asp?p=*port-number* where *ip-address* is the Digi Passport unit IP address or DNS name, *port-number* is the number of the serial port and *port title* is the name of the port as assigned in serial port, port title.	http://passportdemo.digi.com connect.asp?t=CISCO.Router.port3 (the port name is case sensitive)

Custom Menus

Custom menus are created by either root or the system administrator to limit access to specific ports. For more information, see "Recommended Process for Implementing Custom Menus" on page 157.

Port Escape Menu

Port escape is the ability to escape from a port without disconnecting. In port escape mode, a menu of options is displayed, for example, to power the connected device on or off, send messages to port users, or close the current connection to the port. Port escape is available in main sessions as well as sniff sessions. Every connection method accommodates port escape. Configure the escape sequence per port. To configure the port escape sequence, follow these steps.

1. **Serial Port** > **Configuration** > ***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.

   The port escape menu is automatically started if there is one active session to the port established.
4. Enter the port escape sequence that was configured in step 2.

Port Escape Sequences

The following table describes the fields and the operations for the port escape feature. The fields displayed are those allowed by permissions.

By entering a 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 port escape menu will not open.

Escape Sequence Ctrl+	Description of Action	Occurrence
a	Send message to port user(s).	Not available to sniff users.
b	Send break.	Not functional for sniff users.
d	Disconnect a sniff session.	Only functional to admin.
g	Create and use port group.	
l	Show last 100 lines of log buffer.	Must enable logging for this option.
p	Power device on/off.	Show only on or off only if power management is available on this port.
r	Reboot device using power-switch.	Only if power management is available on this port.
x	Close current connection to port.	Closes the current sniff session.

Automatic Device Recognition

The Automatic Device Recognition feature allows the Digi Passport unit to automatically detect and recognize attached devices. The Digi Passport unit sends a set of automatic detection criteria, including sets of serial parameters and a probe string (default is < Enter >), and analyzes the response. If **Use detected port title** is enabled, the Digi Passport unit displays the detected OS, device, and port number in the format:

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

Automatic Device Recognition also monitors each of the configured serial ports. If there is a change in the expected response from the device connected to the serial port, an email message or SNMP trap can be issued. This means that notifications are sent if the device goes down or is disconnected for any reason.

To configure the alarm feature, see "Configure Ports" on page 60. For a further discussion of the automatic detection feature and the settings involved, see "Configure Automatic Detection" on page 77. To enable Automatic Device Recognition:

1. **Serial Port** > **Configuration** > Select the port number or All.
2. Port title
   - **Automatic Detection:** Enable
   - **DSR status**
   - **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**.

Locator LEDs

The the Digi Passport unit has two locator LEDs labeled **Find**, one on each side of the unit, that can be used can be used to physically locate the unit.

Enable Locator LEDs

1. Log into the Web interface as **admin** or **root**.
2. In the Web interface menu, click **Activate Passport Locator LED**. A confirmation dialog is displayed.
3. Click **OK** and the locator LED will blink.

Turn Off Locator LEDs

In the Web interface, click **Stop Passport Locator LED**.

Chapter 2 Getting Started

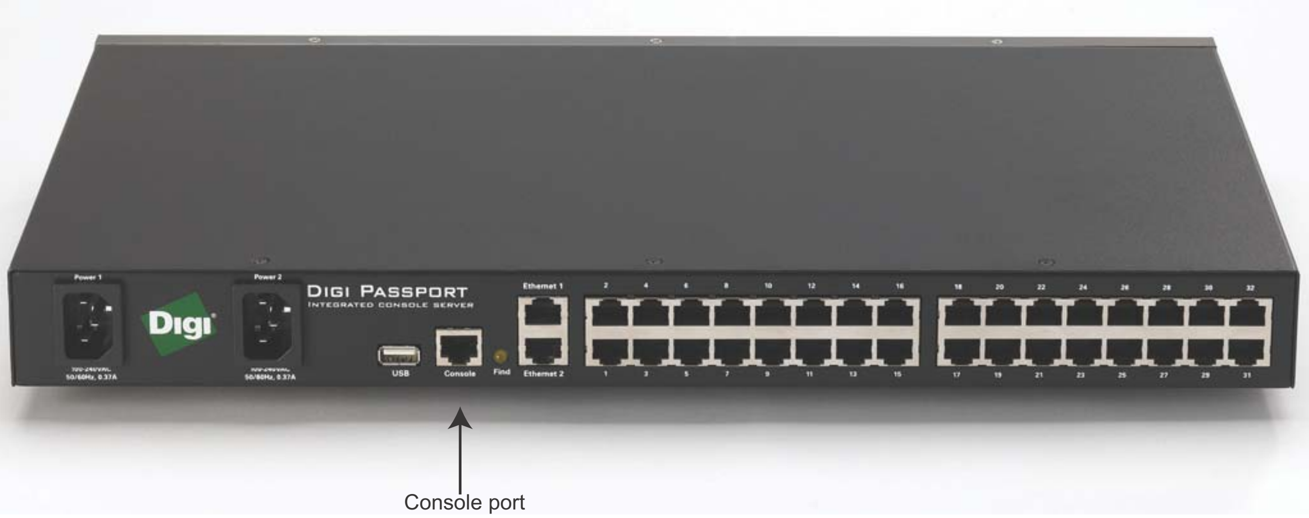
This chapter covers basic configuration topics, including assigning IP settings, accessing and navigating in the web interface, enabling secure access with the web interface, accessing the unit through SSH, and user administration: adding, editing, or removing users, managing user accounts, and creating access lists.

Initial setup is described in the *Quick Start Guide* included with the product packaging.

Assign IP Settings from the Console Port

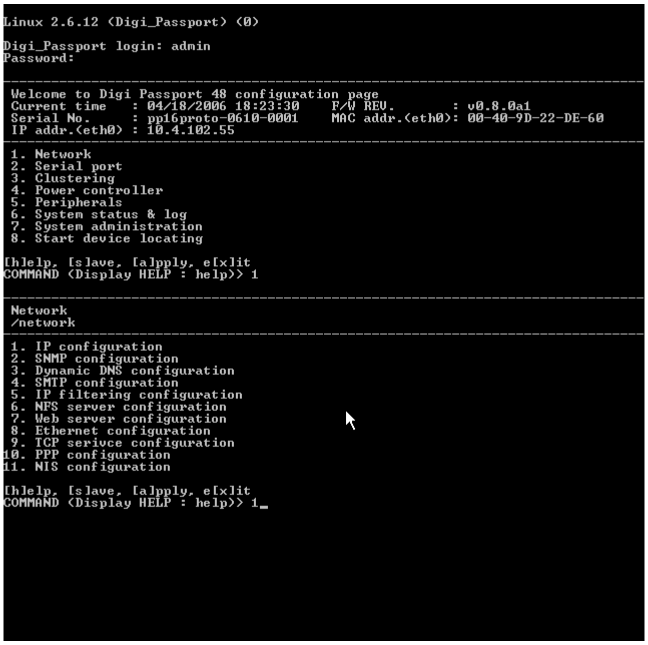
To assign IP settings to Ethernet port #1 via the console port, follow these steps. The default IP address is **192.168.161.5**.

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 these settings:
   - **bps**=9600
   - **data bits**=8
   - **parity**=none
   - **stop bits**=1
   - **flow control**=none.
3. Establish a connection to the console port of the Digi Passport unit and press **Enter** to get a command prompt.
4. At the login prompt, log in as **admin**. The default password for admin is **admin**. The Configuration menu is displayed.

5. Enter the number **1** for Network Configuration.
6. 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

[h]elp, [s]ave, [a]pply, e[x]it
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 serivce configuration
10. PPP configuration
11. NIS configuration

[h]elp, [s]ave, [a]pply, e[x]it
COMMAND (Display HELP : help)> 1_
```

7. Enter **1** for IPv4.
8. Enter the appropriate parameters for the IP settings.
9. From the menu, enter **a** to apply, and enter **x** to exit.

   Changes are saved and applied immediately. There is no need to reboot.

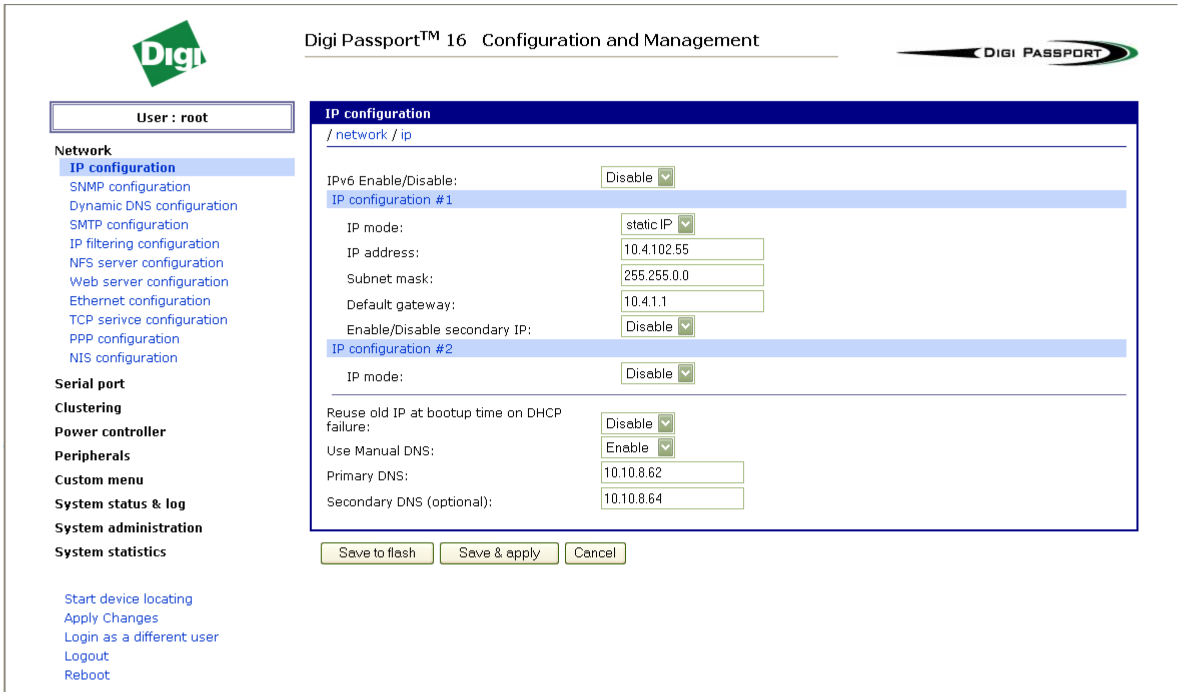
Access the Web interface

There are two ways to access the web interface.

- Using Digi's device discovery tool, ADDP (Advanced Digi Discovery Protocol). This device discovery tool is used to find and launch the 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 the device and double-click it to access the web interface, or select the device and click Configure network settings (on the left navigation bar).
- By entering the IP address of the Digi Passport unit or its hostname directly into the address bar of a browser. The IP address and DNS server must already be set up.

Home Page for Web Interface

Once the web interface is accessed, the home page of the web interface page is displayed after login:



IP configuration

/ network / ip

IPv6 Enable/Disable:	Disable
IP configuration #1	
IP mode:	static IP
IP address:	10.4.102.55
Subnet mask:	255.255.0.0
Default gateway:	10.4.1.1
Enable/Disable secondary IP:	Disable
IP configuration #2	
IP mode:	Disable
Reuse old IP at bootup time on DHCP failure:	Disable
Use Manual DNS:	Enable
Primary DNS:	10.10.8.62
Secondary DNS (optional):	10.10.8.64

User Interface Differences for End Users

For Passport end users, the only option available under **System administration** is to change the user password. Users can also log in as a different user or log out of the system.

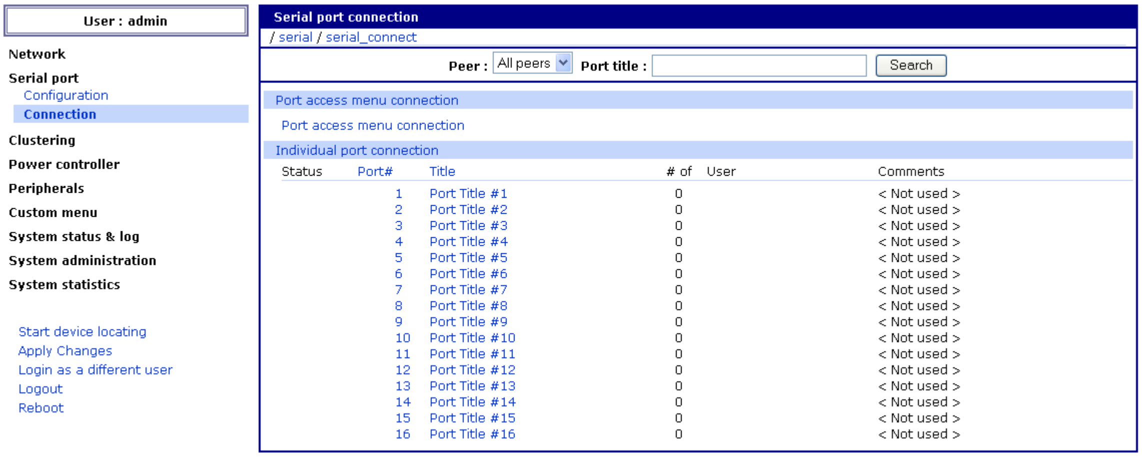
Saving and Applying Changes in the Web interface

In the web interface, there are two ways save and apply configuration changes.

- To save and apply changes immediately, click the **Save & apply** button.
- To save multiple changes, but apply changes once, click the **Save to flash** button. Changes are immediately saved, but they do not take effect until clicking **Apply changes**. The **Apply changes** link is located on the left navigation menu. Or use the **Save & apply** button at the bottom of the page.

Serial Port Connection Page: Manage and Control Connections

Upon login, a page showing the systems that can be managed and controlled is displayed.



User : admin

Network

Serial port
- Configuration
- Connection

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

Serial port connection

/ serial / serial_connect

Peer : All peers Port title : [ ] Search

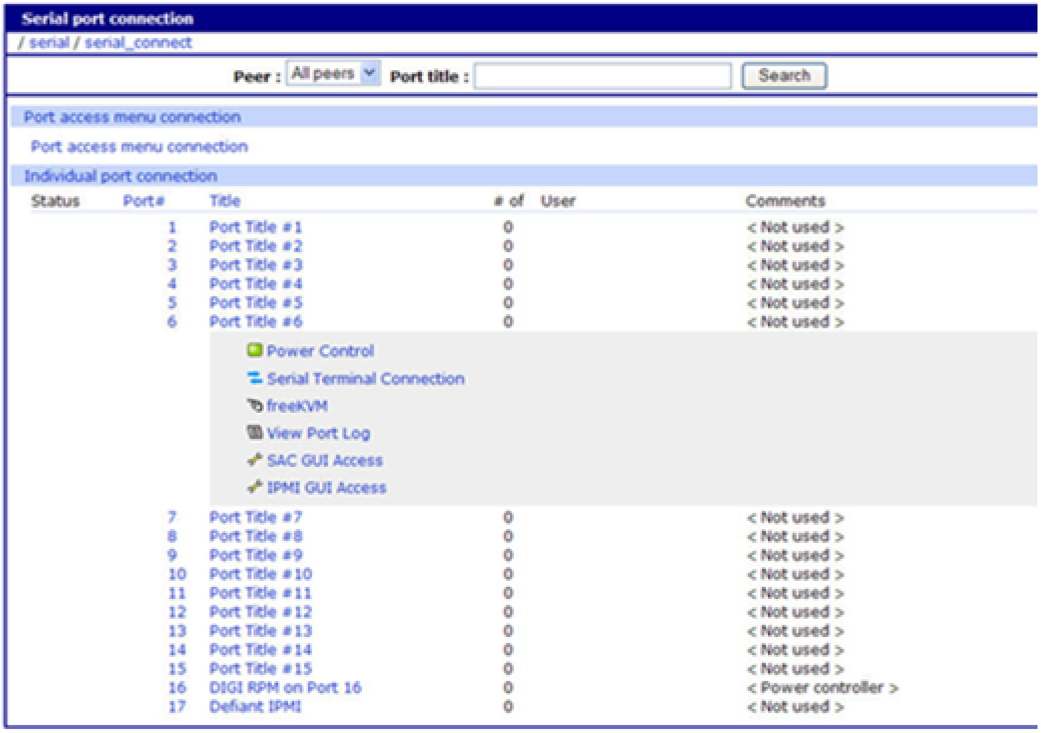
Port access menu connection

Port access menu connection

Individual port connection

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 >

The **Serial port connection** page displays status of all ports at a glance. Clicking on the port number or title of the port expands the view, showing all the available methods of connection or management for the port, such as power control, serial terminal connection, port log, or alternate user interfaces, as shown.



Serial port connection

/ serial / serial_connect

Peer : All peers Port title : [ ] Search

Port access menu connection

Port access menu connection

Individual port connection

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 >
		Power Control Serial Terminal Connection freeKVM View Port Log SAC GUI Access IPMI GUI Access			
	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	DIGI RPM on Port 16	0		< Power controller >
	17	Defiant IPMI	0		< Not used >

Warnings and Alerts on the Serial Port Connection Page

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

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

Capabilities from the Serial Port Connection Page

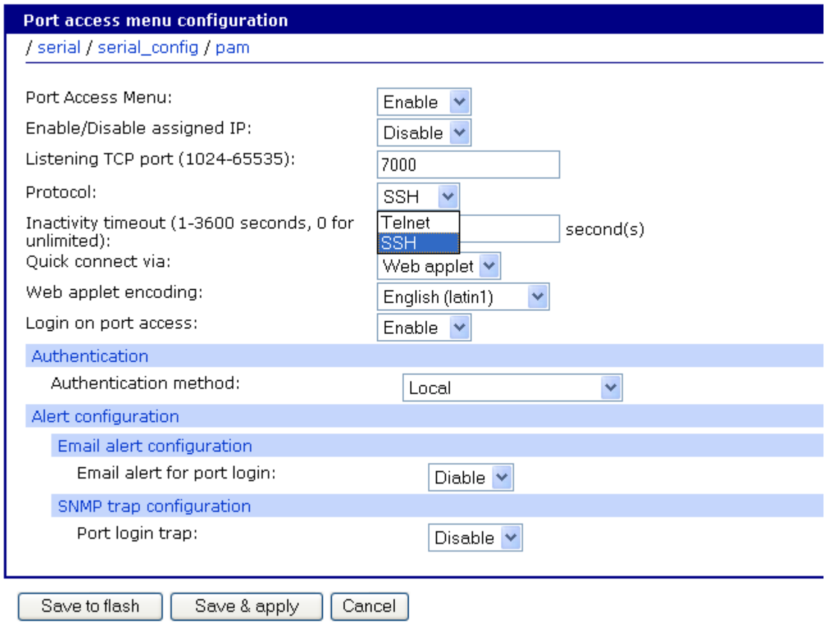
Systems can be powered on and off, a console to the serial console can be launched, and a freeKVM session can be initiated to the server. The port log can also be reviewed to see what event triggered the alarm.

Configure Access to Digi Passport via SSH

Access to the Digi Passport unit's command line via SSH is enabled by default (TCP port 22). The Port Access Menu and individual ports can be configured for SSH. The Digi Passport unit supports Blowfish and 3DES encryption methods for SSH.

Configure the Port Access Menu for SSH

1. Enter the IP address of the Digi Passport unit into the address bar of the browser to 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. Select **Serial port > Configuration > Port access menu configuration**. The Port access configuration menu is displayed.



Port access menu configuration

/ serial / serial_config / pam

Port Access Menu: Enable

Enable/Disable assigned IP: Disable

Listening TCP port (1024-65535): 7000

Protocol: SSH

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

Quick connect via: Web applet

Web applet encoding: English (latin1)

Login on port access: Enable

Authentication

Authentication method: Local

Alert configuration

Email alert configuration

Email alert for port login: Diable

SNMP trap configuration

Port login trap: Disable

4. For **Port access menu protocol**, select SSH.

   When enabled, the **Log in on port access** feature requires two logins, once for access to the port access menu and again for the specific port. If this feature is disabled the only login challenge is to the Port Access Menu, though only permitted users can successfully connect to any specific port.
5. Click **Save & apply**.

Configure a Port for SSH

1. Enter the IP address of the Digi Passport unit into the address bar of the browser to 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 ports or an individual port to configure for SSH.
5. Click **Host mode configuration**.
6. For **Protocol**, select **SSH**.
7. Click **Save & apply**.

Configure Access to Digi Passport via PPP

The Digi Passport unit can be configured to support access to it via dial-in Point-to-Point (PPP) connections. PPP can be configured from a variety of interfaces, including the Digi Passport unit's web interface, Windows XP, or a Linux client.

Configure PPP from the Passport Web Interface

1. Select **Network > PPP configuration >Basic PPP settings**. Enter settings:
   - **Dynamic IP address pool for incoming connections**: select **Enable**.
   - **First IP address**: Enter the starting address of IP pool, for example, 192.168.161.200*.*
   - **Number of address**: Enter the desired number for the address, for example, 10. Must be greater than 1.

   When all basic PPP settings are entered, click **Save to flash.**
2. Select **Network > PPP configuration > incoming PPP connection**.

   Add a user for PPP connection and set parameters for each user:

   For **Authentication configuration**, enter:
   - **Username:** admin
   - **Password (new):** admin

     Specify the Password after setting all other parameters and just before clicking **Save to flash**. If not, a Null Password can be specified while changing other parameters.
   - **Password (confirm): admin**
   - **Authentication: CHAP/PAP**

   For **Peer configuration**, enter:
   - (*****) Automatically assign remote IP address from IP address pool.
   - (**v**) Allow client access to local network via PPP connection.

   Click **Save to flash**.
3. Go to **Peripherals > Modem configuration**. Enable the PPP connection on the Modem.
4. Click **Save & apply**.

Configure PPP from the Windows XP Interface

1. Select **Start > Control Panel > Network Connections**. The Network Connections window is opened.
2. Select **File > New connection** to launch the New connection Wizard.
3. Select **Connect to the network at my workplace** and click **Next**.
4. Select **Dial-up connection** and click **Next**.
5. Enter Connection name and click **Next**.
6. Enter Phone number and click **Next**.
7. For **Connection Availability**, select **Anyone** or **My use only** and click **Next**.
8. Click **Finish**.
9. Right-click the on the connection just created to open the connection properties window.
10. On **Security** tab, check **Advanced** for Security options and click **Settings**.
11. On the **Advanced Security Settings** window, set the parameters as follows:
    - **Data encryption**: Optional encryption (connect even if no encryption)
    - **Allow these protocols**: Unencrypted password(PAP)/Challenge Handshake Authentication Protocol(CHAP).

    Click **OK**.
12. Check the **Run script** checkbox, select **Generic login**, and click **Edit**.
13. Check the **Show Terminal Window** checkbox.
14. Run the dialup connection and click the **Properties** button.
15. Click the **Security** tab. In the **Interactive logon and Scripting** section, check the **Show Terminal Window** checkbox.This option will display the terminal window so that you can type a user name and password manually.
16. In file **switch.inf,** edit following lines as instructed:

    ```
    line 72: OK=<match>"login:" => OK=<match>"login :"
    (insert a space character before ":")
    line 80: COMMAND=<user name><cr> => COMMAND=admin<cr>
    line 89: OK=<match>"password:" => OK=<match>"password :"
    (insert a space character before ":")
    line 97: COMMAND=<password><cr> => COMMAND=admin<cr>
    ```

    Then save the **switch.inf** file.
17. On the **Properties** window, click **OK**.
18. On **Dial-up connection,** double-click the **Connect** icon.
19. Enter the **User name** and **Password**, then click the **Dial** button.

Configure PPP from a Linux Client

1. From the command line of a Linux client on a Redhat 9 machine, run the kppp utility:

   ```
   # kppp
   ```

2. On the **KPPP** window, click **Setup**.
3. On the **Accounts** tab of the KPPP Configuration window, click **New.**
4. On the **Create New Account** window, select **Dialog Setup**.
5. On the **Dial** tab of the **New Account** window, enter the desired name in the **Connection name** field. Click **Add**.
6. Enter the phone number of internal modem and click **OK**.
7. For **Authentication**, select **PAP/CHAP**.
8. On the **IP** tab, select **Dynamic IP address**.
9. On the **Gateway** tab, select **Default gateway.**
10. On the **DNS** tab, select **Automatic configuration**.
11. On the **Login Script** tab, specify the following under **Login Scripts sequentially**:

    ```
    Expect Login :
    Send admin
    Expect Password :
    Send admin
    ```

    For **Expect Login** and **Expect Password**, note that there is a space character before the "**:**" character.

    Click **OK**.

12. On the **KPPP Configuration** window, click the **Device** tab and check the parameters. Default values can be used for all device types except **Modem**. Select the device to which the modem is connected. Click **OK.**
13. On the **KPPP** window, select the **Connection** name that was just configured. Enter the login ID and password and check the **Show log window** checkbox.
14. Click **Connect**. The login process is displayed in the **Login Script Debug** Window.

    If errors occur, error messages are displayed on the Redhat machine in the file **/var/log/messages**.

    After connection, check whether correct PPP interfaces exist on both the Digi Passport unit and Redhat machines.

Set PPP Host Mode for a Serial Port

To set PPP host mode for a serial port, go to **Serial port configuration >Host mode configuration >Host mode**. See "Host Mode Configuration" on page 71 and the description of PPP host mode in "PPP Mode" on page 75.

User Administration

Required Privileges for User Administration

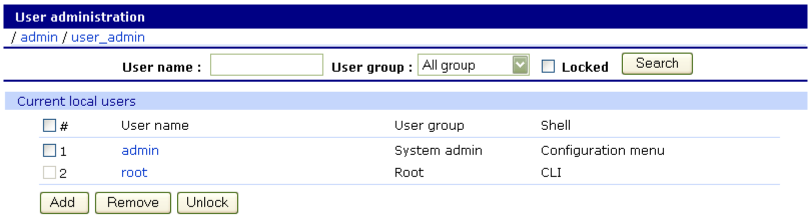
Only root and admin users can administer other users. The root user has unlimited administration privileges. The admin user can view and change all attributes except those that belong to the root user.

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.

Add a User

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Log in as **root** or **admin**. The default password for **root** is **dbps**; for admin, **admin**.
3. Under **System administration**, select **User administration**. The **User administration** page is displayed:



User administration

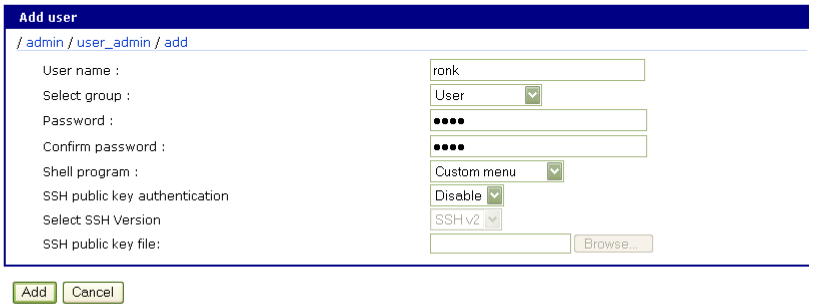
/ admin / user_admin

User name : User group : All group ☐ Locked

Current local users

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

4. Click **Add**. The **Add user** page is displayed:



Add user

/ admin / user_admin / add

User name :	ronk
Select group :	User
Password :	••••
Confirm password :	••••
Shell program :	Custom menu
SSH public key authentication	Disable
Select SSH Version	SSH v2
SSH public key file:	

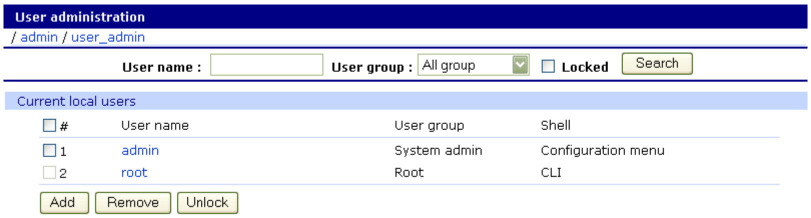
5. Fill in the user attribute fields, as described in the table below. When done, click **Add**.

User attributes

User attribute	Description
User name	Name for the user. Rules for user names include: • User names are case-sensitive. • Must be between 3 and 29 characters. • Cannot include colons (:), less than or greater than signs (< >), ampersand (&), spaces, or quotation marks. • The at sign @ and period. are acceptable.
Select group	The group to which the user is assigned. Groups include **Root**, **System Admin**, **Port Admin** and **User**. See "User Groups" on page 18 for more information
Password	Password to assign to the user.
Confirm password	Confirms the password.
Shell program	Determines the user interface displayed when establishing a Telnet or SSH session or connecting via the console port with the Digi Passport unit. Shell program options vary by user group: **root**: command line **system admin**: command line, configuration menu, port access menu, custom menus **port admin**: configuration menu, port access menu, custom menus **user**: port access menu, custom menus
SSH public key authentication	Alternative method of authenticating a user to a login server. More secure than a password only.
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.

Edit a User

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Log in as **root** or **admin**. The default password for **root** is **dbps**; for admin, **admin**.
3. Under **System administration**, select **User administration**. The **User administration** page is displayed:



User administration

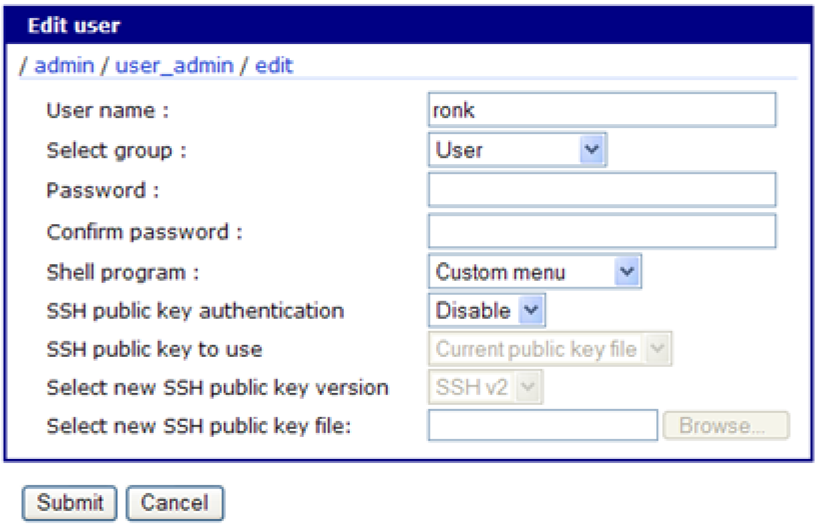
/ admin / user_admin

User name : User group : All group □ Locked

Current local users

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

4. Click on the username. The **Edit user** page is displayed, showing the user attributes:



Edit user

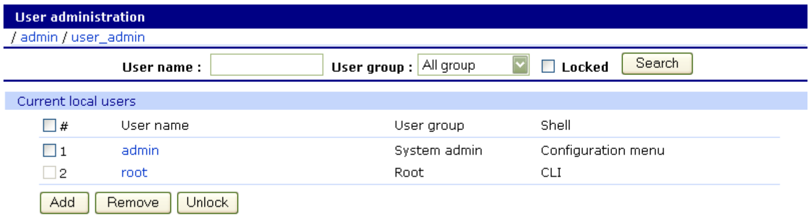
/ admin / user_admin / edit

User name :	ronk
Select group :	User
Password :	
Confirm password :	
Shell program :	Custom menu
SSH public key authentication	Disable
SSH public key to use	Current public key file
Select new SSH public key version	SSH v2
Select new SSH public key file:	

5. Change the user attribute fields as needed. For descriptions, see "User attributes" on page 37.
6. Click **Submit**.

Remove a User

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Log in as **root** or **admin**. The default password for **root** is **dbps**; for admin, **admin**.
3. Under **System administration**, select **User administration**. The **User administration** page is displayed:



User administration

/ admin / user_admin

User name : User group : All group □ Locked

Current local users

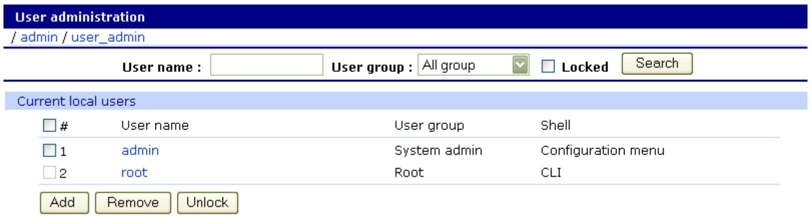
□ #	User name	User group	Shell
□ 1	admin	System admin	Configuration menu
□ 2	root	Root	CLI

4. Select the checkbox next to the user to be removed.
5. Click **Remove**.
6. Click **OK** at the prompt.

Unlock a User Account

For users with the Enforce max password attempts setting enabled (in **System administration > Security profile > Enforce max password** attempts), and the user account was locked because the maximum password attempts were entered, the user account can be unlocked.

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Log in as **root** or **admin**. The default password for **root** is **dbps**; for admin, **admin**.
3. Under **System administration**, select **User administration**. The following screen is displayed:



User administration

/ admin / user_admin

User name : User group : All group □ Locked

Current local users

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

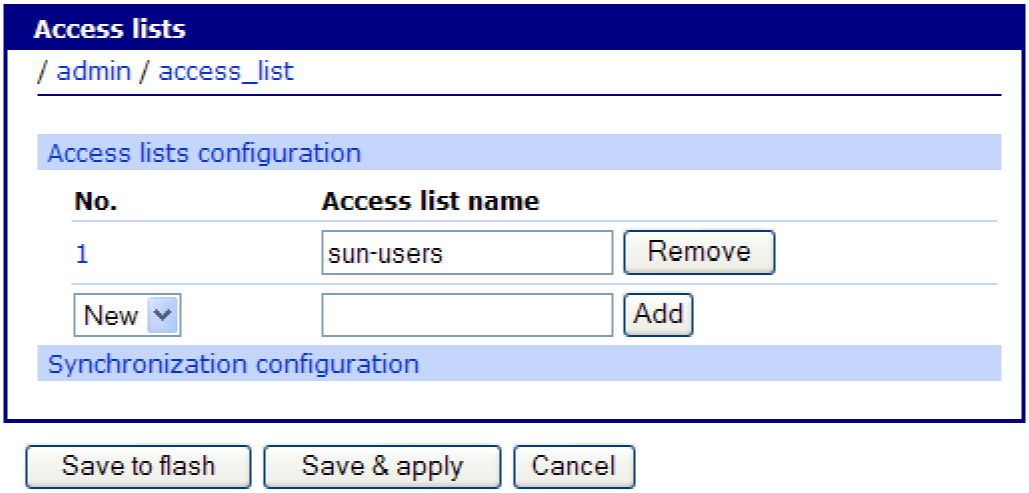
Add an Access List and Add Users to It

Access lists are used to add rights to a single user or to multiple users at the same time. In addition, multiple users can be grouped and assigned one, some, or all these rights:

- Port access rights
- Port monitor rights
- Power management rights to an access list

To add an access list:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Log in as **root** or **admin**. The default password for **root** is **dbps**; for admin, **admin**.
3. Under **System administration**, click **Access List**. The Access lists page is displayed:



Access lists

/ admin / access_list

Access lists configuration

No.	Access list name	
1	sun-users	Remove
New		Add

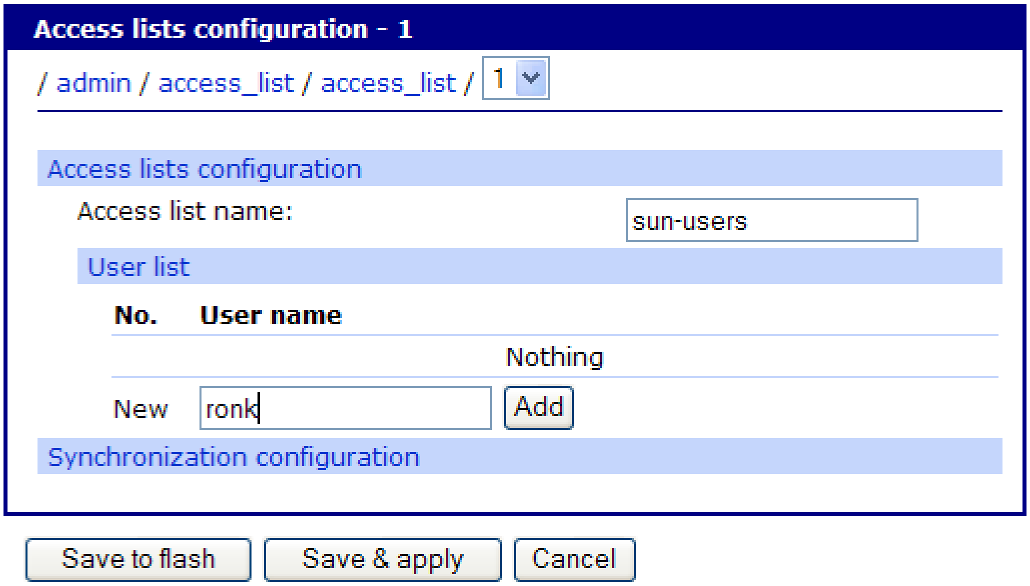
Synchronization configuration

4. Enter the name of the access list and click **Add**.
5. To add users to the access list, click on the access list's number in the **No.** column.

6. Add the users to the access list.

   Add one user at a time to the access list by entering the name into the **User name** edit-box and clicking **Add**. Add users that are not locally configured on the Digi Passport unit, but use a centralized authentication method such as RADIUS, LDAP etc.

   Important: Take care when entering user names in the access list, as the spelling of user names is not verified against the local user database. A misspelled user name could result in adding externally configured users that only exist in the RADIUS, LDAP or other central databases.



Access lists configuration - 1

/ admin / access_list / access_list / 1

Access lists configuration

Access list name: sun-users

User list

No.	User name
	Nothing
New	ronk

7. Click **Save & apply**.

   For more information about configuring access rights for specific users, see "Configure User Access Privileges" on page 144.

   To change the privileges of an Access list, see "Change the Privileges of an Access List" on page 145.

Chapter 3 Install and Configure PC Cards

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.

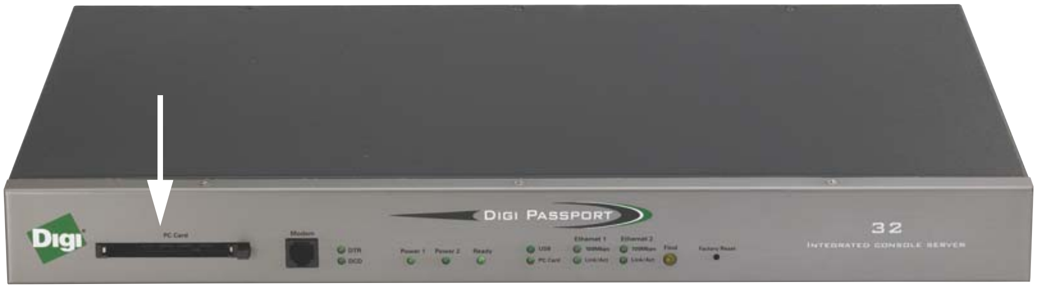
Compatible PC Cards

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/.

Add 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.

Important: Before removing a PC card, always click the **Stop card service** button, then **Save & apply**.

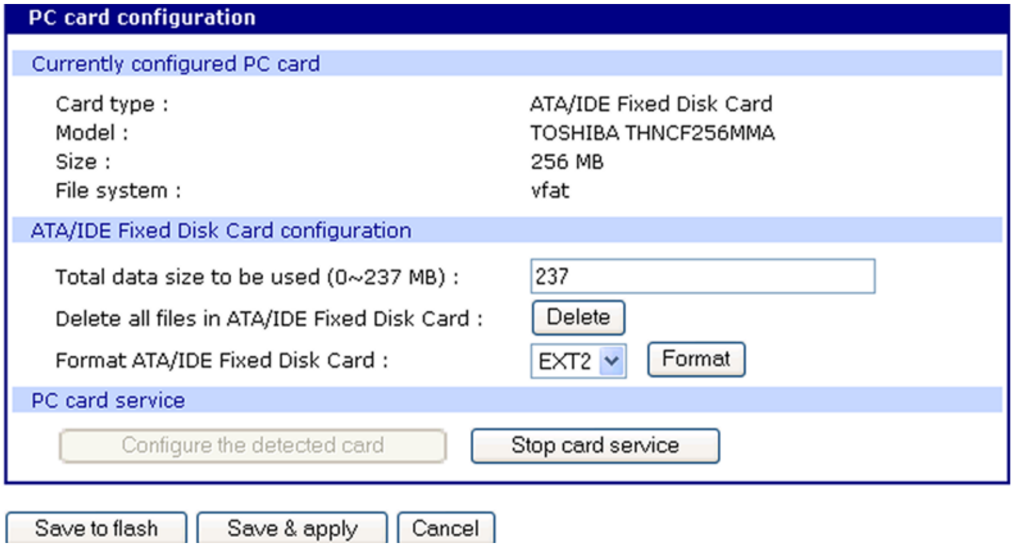


PC card slot

Digi Passport 32 showr

To install and configure the compact-flash card on the Digi Passport unit:

1. Insert the card into the PC card slot.
2. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
3. Under the **PC card** heading, click **Configuration**.
4. Click **Configure the detected card**. These settings are displayed.
    - ATA/IDE Fixed Disk Card configuration
    - **Total data size to be used**: Enter the amount of memory to assign to the compact-flash card for configuration files.
    - **Delete all files in ATA/IDE Fixed Disk Card**: Click **Delete** to clear the 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 this option and click the **Format** button.



PC card configuration

Currently configured PC card

Card type :	ATA/IDE Fixed Disk Card
Model :	TOSHIBA THNCF256MMA
Size :	256 MB
File system :	vfat

ATA/IDE Fixed Disk Card configuration

Total data size to be used (0~237 MB) :	237
Delete all files in ATA/IDE Fixed Disk Card :	Delete
Format ATA/IDE Fixed Disk Card :	EXT2 Format

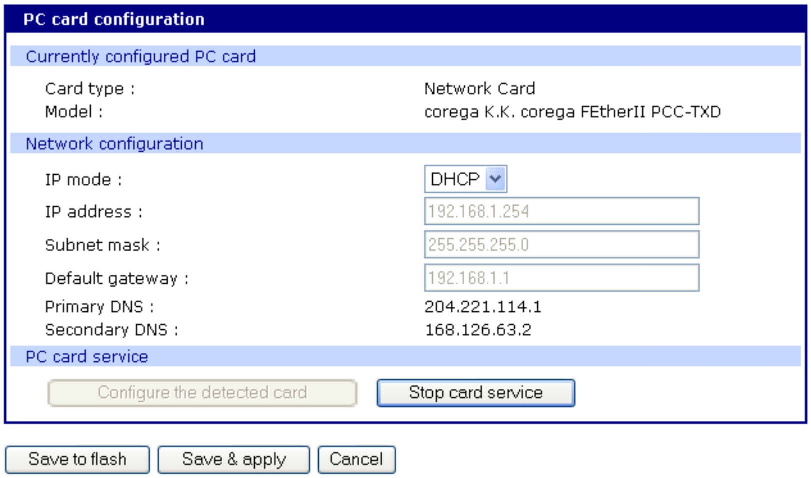
PC card service

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

Add 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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
3. Under the **PC card** heading, click **Configuration**. 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

5. Click **Save & apply**.

   If DHCP is active, the IP address will appear after **Save & apply** is clicked.

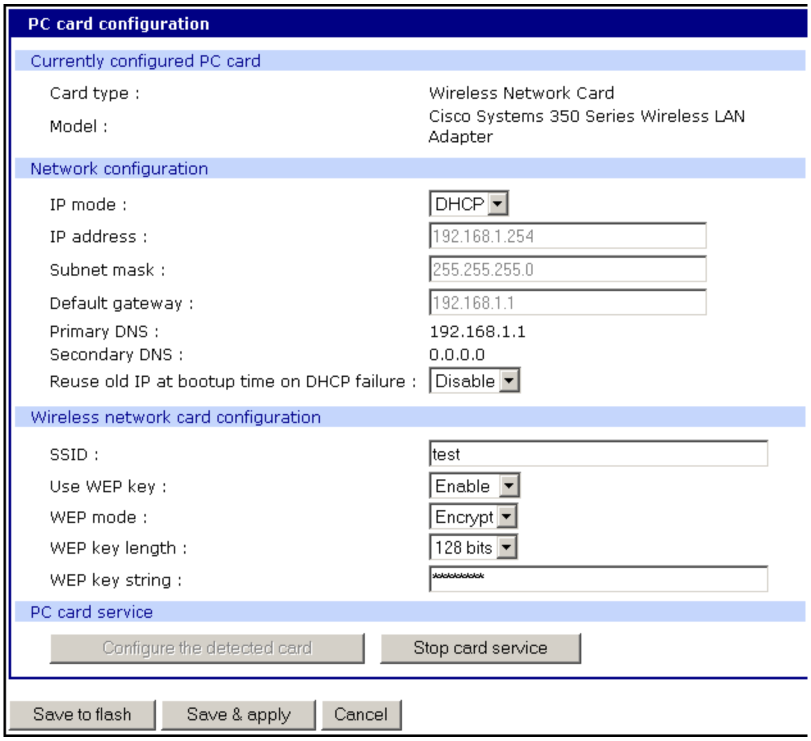
Add a Wireless LAN Card

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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
3. Under the **PC card** heading, click **Configuration**. 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 the settings for the wireless card are not known, contact the 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**: If the WEP key is enabled, the options are 40 or 128 bits.
   - **WEP key string**: Refer to the wireless network administrator for the wireless encryption key string.



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

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

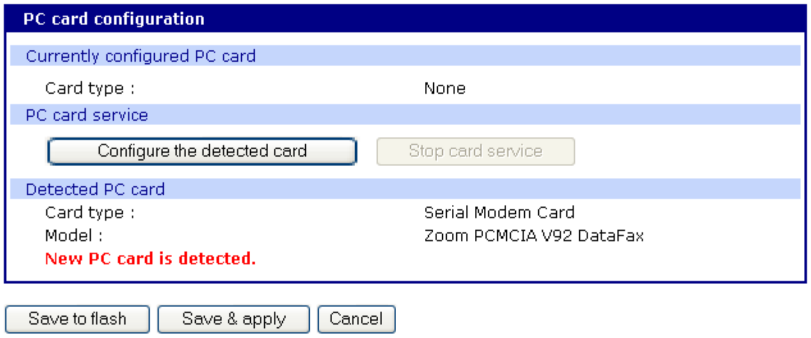
SSID : test
Use WEP key : Enable
WEP mode : Encrypt
WEP key length : 128 bits
WEP key string : ********

6. Click **Save to flash**.

Add a Serial Modem

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

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. From the menu, select **Configuration** under the **PC card** heading. The card is automatically discovered and a configuration menu is displayed.



PC card configuration

Currently configured PC card

Card type : None

PC card service

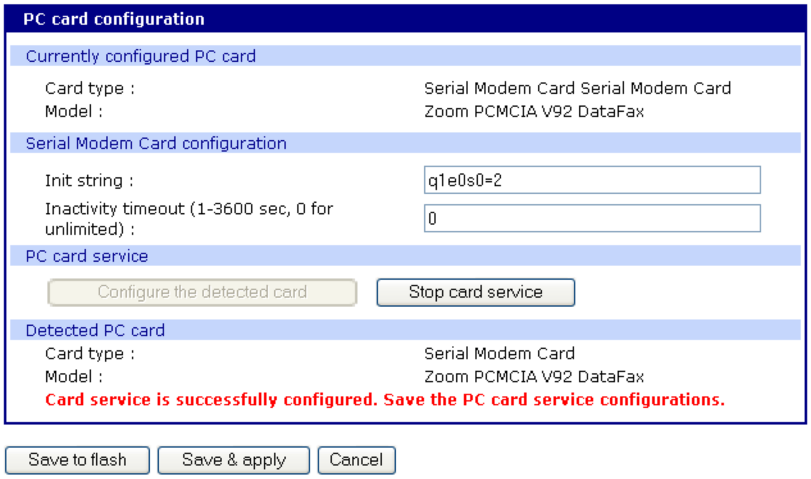
Detected PC card

Card type : Serial Modem Card

Model : Zoom PCMCIA V92 DataFax

New PC card is detected.

3. Click **Configure the detected card**.



PC card configuration

Currently configured PC card

Card type : Serial Modem Card Serial Modem Card

Model : Zoom PCMCIA V92 DataFax

Serial Modem Card configuration

Init string : q1e0s0=2

Inactivity timeout (1-3600 sec, 0 for unlimited) : 0

PC card service

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**.

Chapter 4 System Status and Port Logging

This chapter describes the system status and port logs available for the Digi Passport.

Available options for system status an port logs

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

- A syslog server
- An NFS server
- A removable flash storage device (PC card or USB)
- The Digi 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, enable the devices and/or enter the required information, then 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**. System status information includes:

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: Enabled or Disabled.
- **Send system log by email**: Condition for notification.
- **PC card type**: Description of PC card if configured
- **PC card model**: Model of PC card if configured
- **Power status**: Dual power (1 - Normal, 2 - Normal)

IP Information

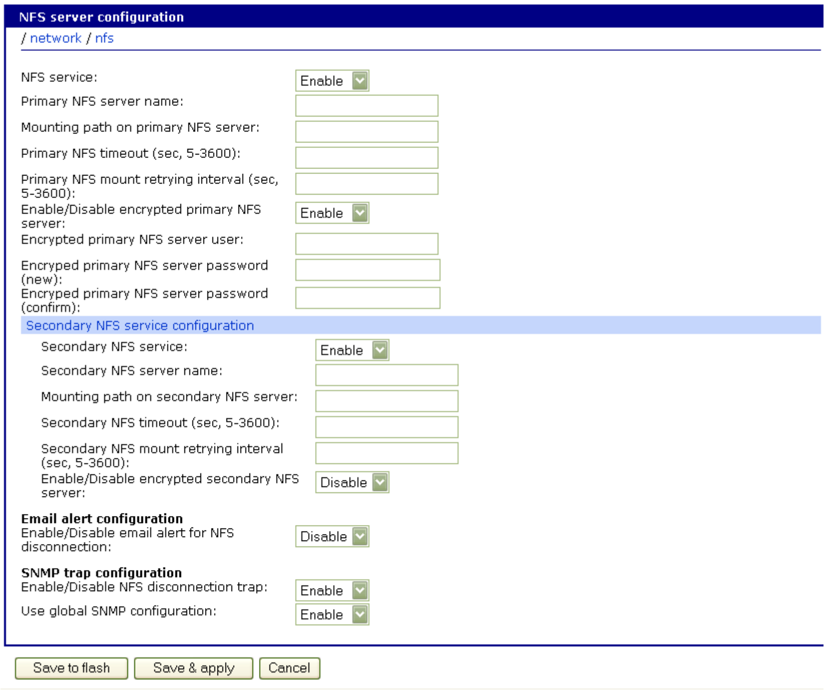
- **IP mode**: Method for setting IP address: Static, DHCP, PPPoE, or Disabled
- **IP expiration**: When the IP address will expire.
- **IP address**: Actual IP address.
- **Subnet mask**: Address of the Subnet mask.
- **Gateway**: Address of the Gateway.
- **Receive/Transmit errors**: Number of errors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

Enable Log Storage Location

Enable NFS Server

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

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the Network heading, click **NFS server configuration**. The NFS server configuration settings are displayed:



NFS server configuration

/ network / nfs

NFS service:	Enable
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:	Enable
Encrypted primary NFS server user:	
Encryped primary NFS server password (new):	
Encryped primary NFS server password (confirm):	

Secondary NFS service configuration

Secondary NFS service:	Enable
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:	Disable

Email alert configuration

Enable/Disable email alert for NFS disconnection:	Disable

SNMP trap configuration

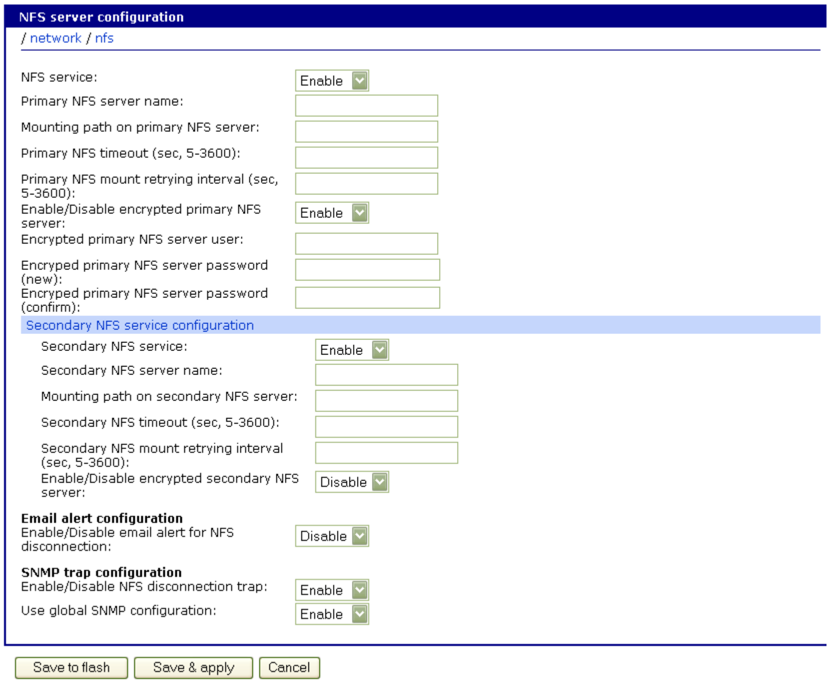
Enable/Disable NFS disconnection trap:	Enable
Use global SNMP configuration:	Enable

3. Set or change the NFS Configuration parameters as needed:
   - **NFS service**: Enabled or disabled.
   - **Primary NFS server name**: IP address of NFS server or DNS name.
   - **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**: Re-enter the password.
   - **Secondary NFS service**: Enabled or Disabled.
   - **Secondary NFS server name**: Name of server.
   - **Mounting path on secondary NFS server**: Directory path to the NFS 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**: Specifies whether the secondary server supports encrypted NFS server.
   - **Encrypted secondary NFS server user**: User name.
   - **Encrypted secondary NFS server password**: Password.
   - **Confirm secondary NFS server password**: Re-enter the password.
4. To activate NFS logging, select **Enable**.
5. Enter the IP address of the primary and secondary (if applicable) NFS server and the mounting path of each.
6. Click **Save & apply**.

Set Up Alert for NFS Server Disconnect

When the NFS server disconnects, an alert in the form of an email message and/or an SNMP trap can be sent. To configure an alert, follow these steps.

1. On 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**.



NFS service: Enable
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: Enable
Encrypted primary NFS server user:
Encryped primary NFS server password (new):
Encryped primary NFS server password (confirm):

Secondary NFS service configuration

Secondary NFS service: Enable
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: Disable

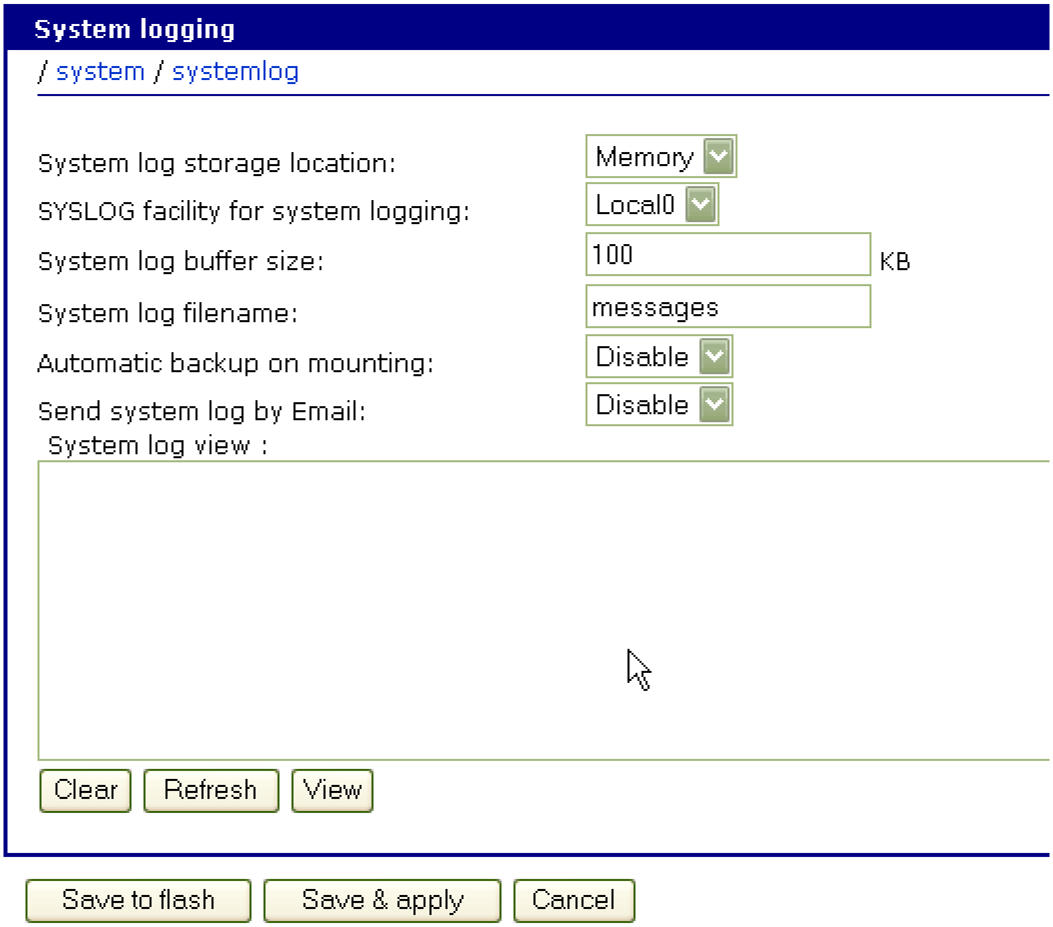
Email alert configuration
Enable/Disable email alert for NFS disconnection: Disable

SNMP trap configuration
Enable/Disable NFS disconnection trap: Enable
Use global SNMP configuration: Enable

Enable Syslog Server

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

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the **Systems status & log** heading, click **SYSLOG-NG Configuration**.
3. Enter the IP address of the primary and secondary (if applicable) syslog server, and select the syslog facility from the pulldown menu.
4. Click **Save & apply**.



System logging

/ system / systemlog

System log storage location: Memory

SYSLOG facility for system logging: Local0

System log buffer size: 100 KB

System log filename: messages

Automatic backup on mounting: Disable

Send system log by Email: Disable

System log view :

Enable a Compact-flash Card

The compact-flash card must be installed and configured on the Digi Passport unit before it can be used for system logging or storing the Digi 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 Digi Passport unit used. The maximum settings for log file sizes are listed in the following table. See also "Add a Compact-flash Card" on page 43.

Total Flash Card Size	Digi 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	

File Size and Memory Use for System and Port Logs

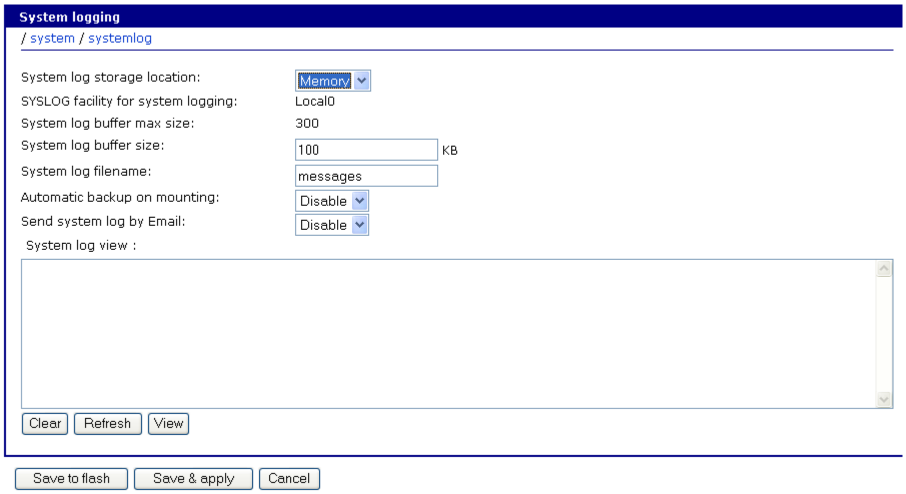
The Digi Passport unit’s memory is already enabled for port logging. It only needs to be configured to accommodate the system and port log files. When storing log files to the Digi Passport unit’s local memory, a total of 3.5M is available. The amount of memory per serial port is dependent on the port count of the Digi Passport unit used. The log file sizes shown in the following table are maximum settings. See also "Configure System Logging" on page 55.

Digi Passport	System Log	Port Log (per port)	Total Memory Used
4	300K	800K	3.5M
8		400K	
16		200K	
32		100K	
48		66K	

Configure System Logging

To configure the Digi Passport unit for system logging:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System status & log** > **System logging**. The system logging settings are displayed:



System logging

/ system / systemlog

System log storage location: Memory

SYSLOG facility for system logging: Local0

System log buffer max size: 300

System log buffer size: 100 KB

System log filename: messages

Automatic backup on mounting: Disable

Send system log by Email: Disable

System log view :

3. Enter system log settings:
   - **System log storage location**: Select the desired location for the system log. The choices depend on what is enabled and/or installed. The Digi 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 to SYSLOG server**: Enable to store system logs to a SYSLOG server.
   - **System log buffer size (KB, 300 max)**: Log buffer size, in KB.
   - **Automatic backup on mounting**: 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 an 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.
4. Select 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.
5. Click **Save & apply**.

View System Logs

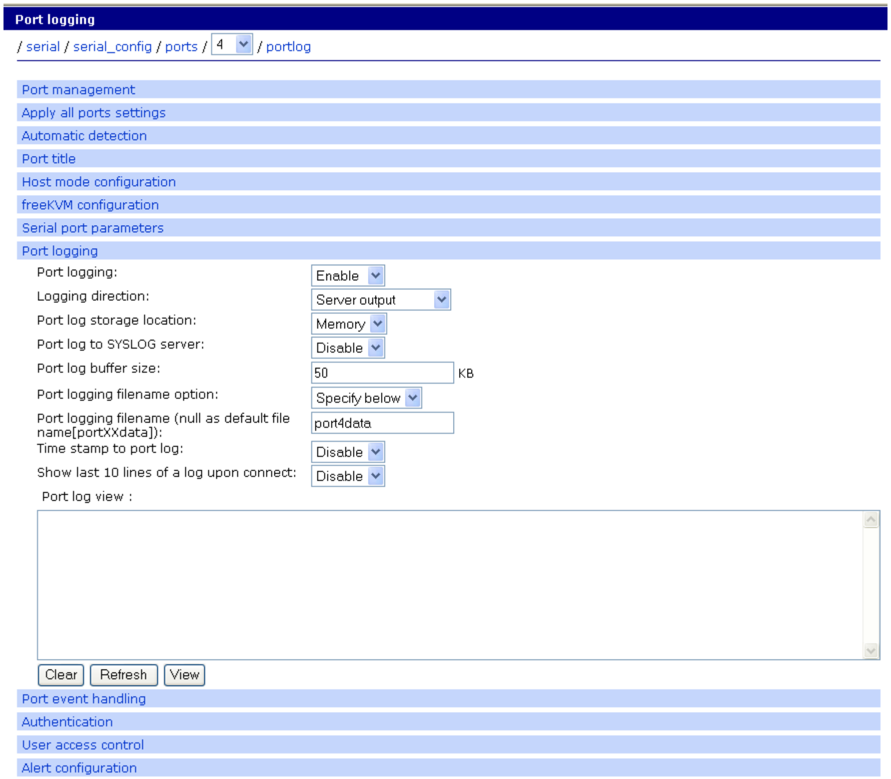
The system logs can be viewed from the web interface on the System logging page or from the location where they have been saved. The following table lists the file locations of the system logs.

System Logfile	
Log Storage	**File Location**
Digi memory	/tmp/logs
Compact-flash card	/mnt/flash/logs
Syslog server	must be viewed on the syslog server
NFS server	/mnt/nfs/logs
USB	/mnt/usb

Configure Port Logging

If a serial port is configured for console server mode, the port logging feature can be enabled. Port logging saves serial data to the memory of the Digi Passport unit, a compact-flash card, a syslog server, or an NFS server. If the memory is used for port logging, all data is cleared when the system's power is turned off. Alarm keywords can be defined for each serial port, for sending email alerts or SNMP traps to enable unattended serial data monitoring. To configure a serial port for port logging in console server mode, follow these steps.

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the **Serial port** heading, click **Configuration**.
3. Select **All** or the desired ***port number***.
4. Click **Advanced**.
5. For the **Port logging** setting, select **Enable**.
6. The port logging settings are displayed.



Port logging: Enable
Logging direction: Server output
Port log storage location: Memory
Port log to SYSLOG server: Disable
Port log buffer size: 50 KB
Port logging filename option: Specify below
Port logging filename (null as default file name[portXXdata]): port4data
Time stamp to port log: Disable
Show last 10 lines of a log upon connect: Disable
Port log view :

- **Logging direction**: Specifies what should be logged.

  Server: Server output only.

  User: User output only.

  Both Server and User with/without arrows: Server and user output with/without directional arrows.

  Default is **Server** output.

  Security note: During logging, user output passwords are saved into the log file.
- **Port log to SYSLOG server**: Enable to store port logs to a SYSLOG server.
- **Port logging filename**: The name of the port log file; specify a filename or use the port title as the filename.
- **Show last 10 lines of a log upon connect:** Show previous last 10 lines of log when connecting to this port.
- **Strip the ^M from SYSLOG**: For logging to a SYSLOG server, strip out all instances of the ^M character sequence.
- **Automatic backup on mounting**: Defines the action taken if a NFS partition of a CF card is mounted or re-mounted.

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

  Disable: Keep writing to the existing log file.
- **Monitoring interval**: The frequency to update the port log in seconds.

7. Click **Save & apply**.

   When port logging is enabled, a **Port Event Handling** page is available to create alarm keywords and send alerts. See "Alerts and Notifications" on page 107 for more information.

View Port Logs

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
USB	/mnt/usb

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

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

To view partial logfiles in the web interface, select **Serial port > Configuration >** ***port number*** **> Port logging**.

Chapter 5 Configure Ports

This chapter shows how to configure serial ports, both physical serial ports and remote ports, which are any type of ports that can be accessed using Telnet, SSH, or Raw TCP protocol, including support for the ALOM, ILOM, iLO, IPMI, DRAC, and SMASH protocols. It presents a quick-start method for configuring all serial ports quickly. It then reviews basic and advanced serial port settings, which can be modified from the factory default settings as needed. It also covers configuring remote ports.

Key serial port configuration settings include whether 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. The Digi Passport unit can also be configured to automatically recognize the type of devices connected to serial ports.

Next, the chapter reviews basic and advanced serial port settings, which can be modified or restored to the factory default settings, and resetting port connections. It also covers configuring and removing remote ports.

Configure Physical Serial Ports

There are several ways to configure physical serial ports:

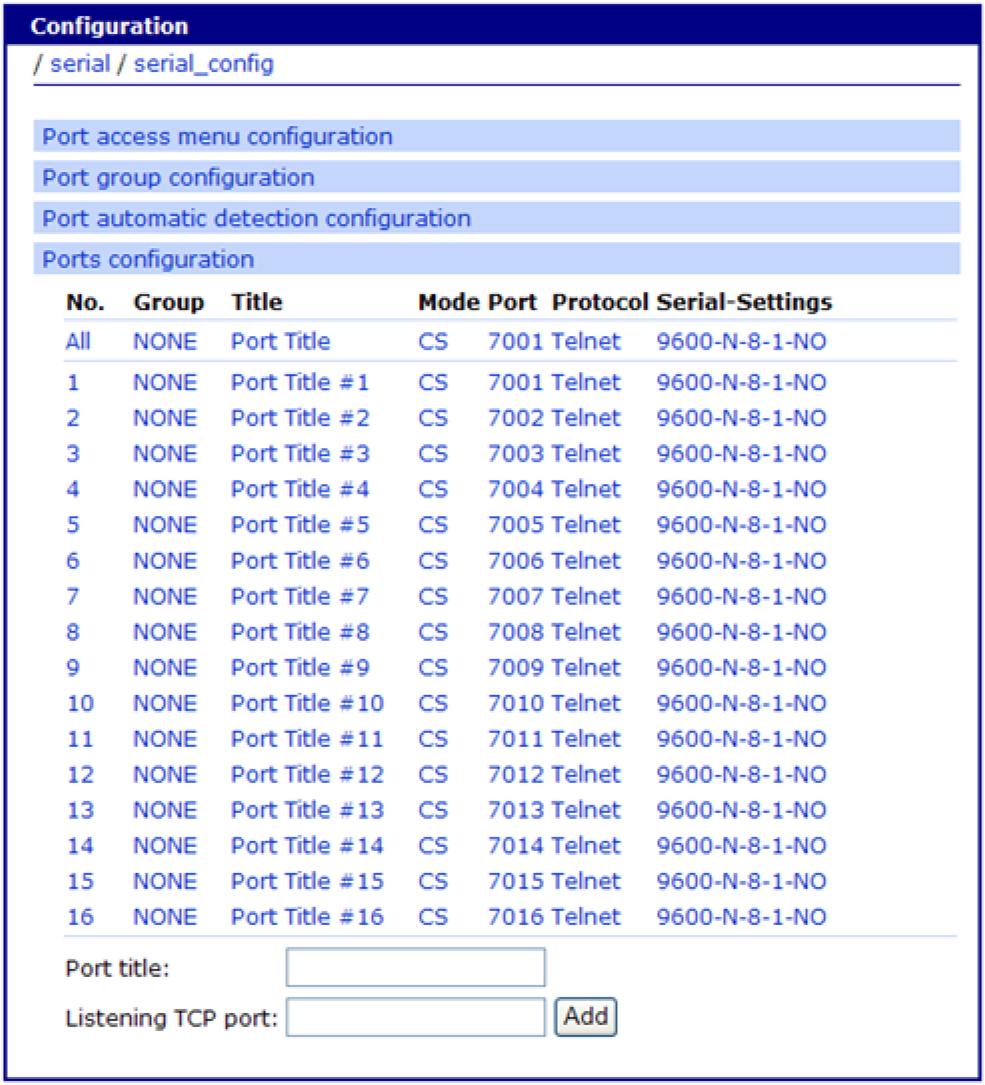
- Using a quick-start procedure that applies a set of configuration settings to all serial ports, and configures the Automatic Device Recognition (ADR) feature, shown on page 62.
- Setting basic configuration settings for individual serial ports. See "Basic Port Configuration Settings" on page 68.
- Setting advanced configuration settings for selected serial ports as needed. See "Advanced Port Configuration Settings" on page 92.

Quick-Start Procedure

Configure Ports with Automatic Device Recognition (Optional)

This procedure is the fastest way to configure Automatic Device Recognition (ADR) for physical serial ports. It results in ports being configured identically, starting from and retaining factory defaults for most settings, and adjusting the most common parameters to fit the requirements of typical installations. It also shows how to optionally establish an automatic detection probe sequence to be performed on the ports to detect the devices that are attached to the Digi Passport unit.

1. In the Web interface for the the Digi Passport unit, go to **Serial Port > Configuration**. The **Ports configuration** page is displayed.



Configuration

/ serial / serial_config

Port access menu configuration

Port group configuration

Port automatic detection configuration

Ports configuration

No.	Group	Title	Mode	Port	Protocol	Serial-Settings
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO
1	NONE	Port Title #1	CS	7001	Telnet	9600-N-8-1-NO
2	NONE	Port Title #2	CS	7002	Telnet	9600-N-8-1-NO
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO
4	NONE	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO
5	NONE	Port Title #5	CS	7005	Telnet	9600-N-8-1-NO
6	NONE	Port Title #6	CS	7006	Telnet	9600-N-8-1-NO
7	NONE	Port Title #7	CS	7007	Telnet	9600-N-8-1-NO
8	NONE	Port Title #8	CS	7008	Telnet	9600-N-8-1-NO
9	NONE	Port Title #9	CS	7009	Telnet	9600-N-8-1-NO
10	NONE	Port Title #10	CS	7010	Telnet	9600-N-8-1-NO
11	NONE	Port Title #11	CS	7011	Telnet	9600-N-8-1-NO
12	NONE	Port Title #12	CS	7012	Telnet	9600-N-8-1-NO
13	NONE	Port Title #13	CS	7013	Telnet	9600-N-8-1-NO
14	NONE	Port Title #14	CS	7014	Telnet	9600-N-8-1-NO
15	NONE	Port Title #15	CS	7015	Telnet	9600-N-8-1-NO
16	NONE	Port Title #16	CS	7016	Telnet	9600-N-8-1-NO

Port title:

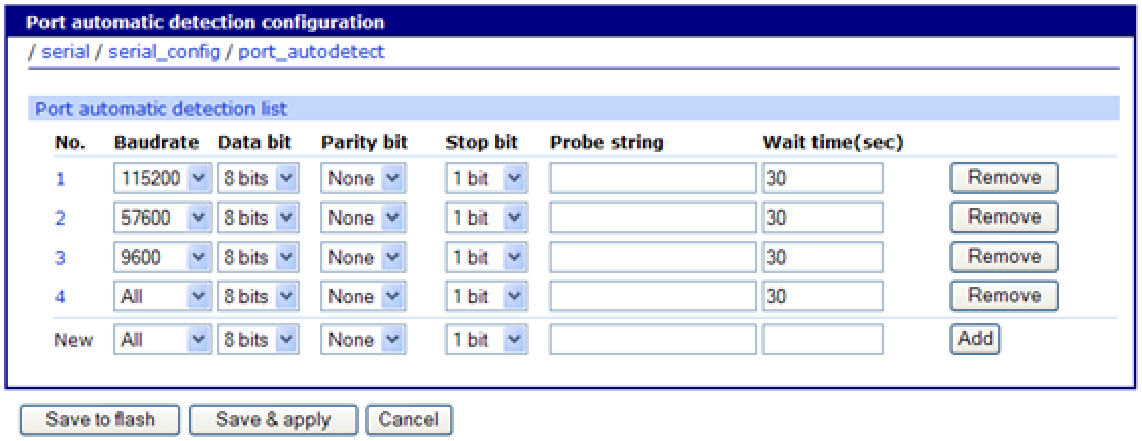
Listening TCP port:

2. **Before** connecting any serial devices to the Digi Passport unit, configure the *automatic detection* feature.

   Automatic detection allows the Digi Passport unit to automatically detect and recognize attached devices. The Digi Passport unit sends a set of automatic detection criteria, including sets of serial parameters and a probe string (default is < Enter >), and analyzes the response.

   On the **Configuration** page, click **Port automatic detection configuration**. Create a *port automatic detection list*, which is a set of entries of common serial port characteristics such as baud rate, data, parity, stop bits, and other values for the devices that are attached to the Digi Passport unit. The entries in the port automatic detection list are used as probe criteria when Automatic Device Recognition is activated and the serial ports are tested. For more information on Automatic Detection settings, see "Configure Automatic Detection" on page 77.

   Here is a sample port automatic detection list:



Port automatic detection configuration

/ serial / serial_config / port_autodetect

Port automatic detection list

No.	Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time(sec)	
1	115200	8 bits	None	1 bit		30	Remove
2	57600	8 bits	None	1 bit		30	Remove
3	9600	8 bits	None	1 bit		30	Remove
4	All	8 bits	None	1 bit		30	Remove
New	All	8 bits	None	1 bit			Add

3. Click **Save & apply**.
4. Enable Automatic Detection for all ports. In the serial ports view (**Serial Port > Configuration**), click **All** to select all ports. Change the **Automatic Detection** setting from **Off** to **Active**. See "Apply All Ports Settings" on page 64 for more information on this feature of applying configuration changes to all ports.
5. Click **Save & apply**.

Apply All Ports Settings

As another aid in configuring serial ports, the Digi Passport unit supports managing all ports simultaneously. This feature is referred to as **Apply all ports settings**. If configuration changes are made to a port and **Apply all ports settings** is enabled, the changes are automatically applied to all ports. Ports can also be excluded from this Apply all ports settings feature. When changing a parameter for all ports, all settings of the complete page are applied to all ports.

Enable/disable the Apply all port settings feature for all ports

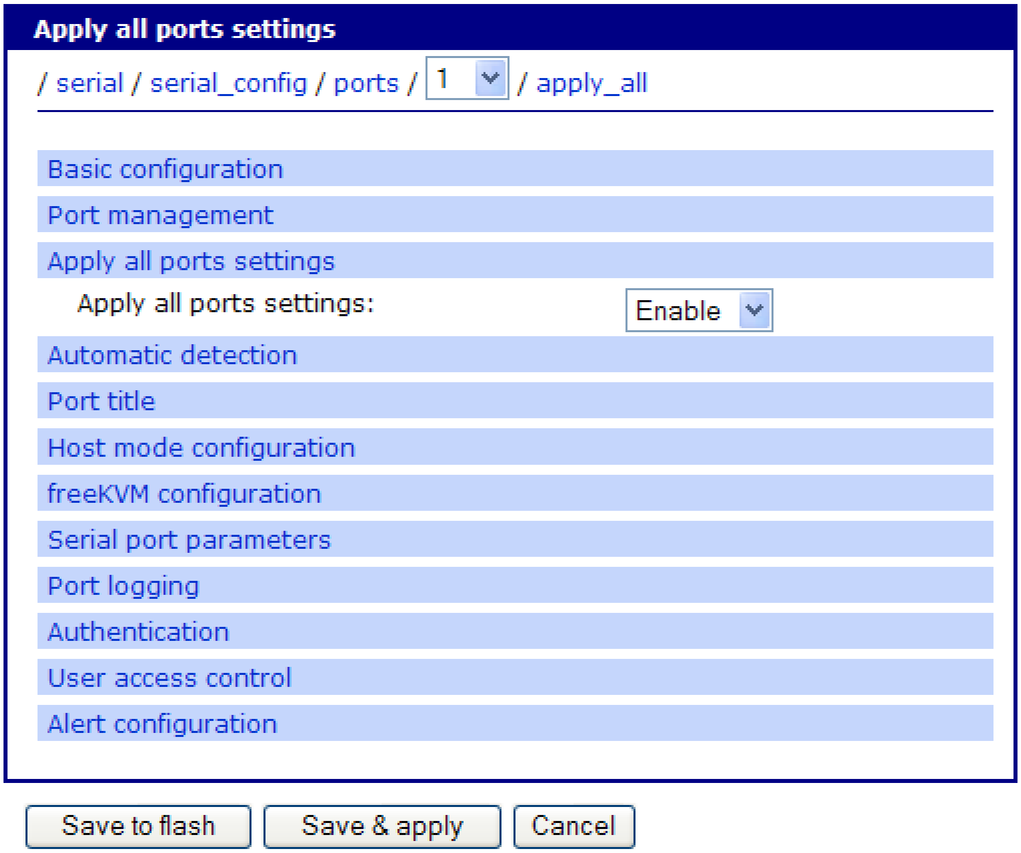
To enable or disable the Apply all ports settings feature for a port:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the **Serial Port** heading, click **Configuration**.
3. On the **Ports configuration** page, select **All**.
4. At the top of the **Basic configuration** page, for the **Apply all ports in a group** setting, select **Enable** to enable the Apply all ports settings feature for all ports, or **Disable** to disable it for all ports.
5. Click **Save to flash** and continue with other configurations, or click **Save & apply**.

Enable/disable the Apply all port settings feature for individual ports

To enable or disable the Apply all ports settings feature for an individual port:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the **Serial Port** heading, click **Configuration**.
3. On the **Ports configuration** page, select the port number.
4. On the **Basic configuration** page, click **Advanced configuration**.
5. On the **Port management** page, click **Apply all ports settings**.
6. On the **Apply all ports settings** page:
   - To enable the Apply all ports settings for the port, select **Enable**.
   - To disable the Apply all ports settings feature for the port, select **Disable** to disable it for all ports.



Apply all ports settings

/ serial / serial_config / ports / 1 / apply_all

Basic configuration

Port management

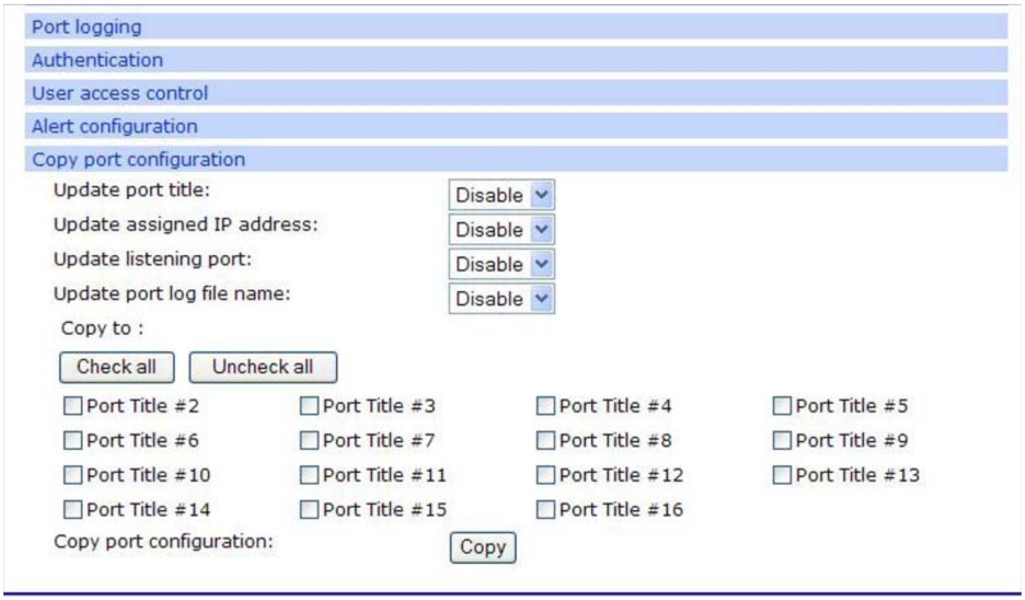
Apply all ports settings

Apply all ports settings: Enable

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

Clone ports

To clone ports, go to **Serial port->Config->"Port"->Copy config**



Copy port configuration

Update port title: Disable

Update assigned IP address: Disable

Update listening port: Disable

Update port log file name: Disable

Copy to :

□ Port Title #2	□ Port Title #3	□ Port Title #4	□ Port Title #5
□ Port Title #6	□ Port Title #7	□ Port Title #8	□ Port Title #9
□ Port Title #10	□ Port Title #11	□ Port Title #12	□ Port Title #13
□ Port Title #14	□ Port Title #15	□ Port Title #16	

Copy port configuration:

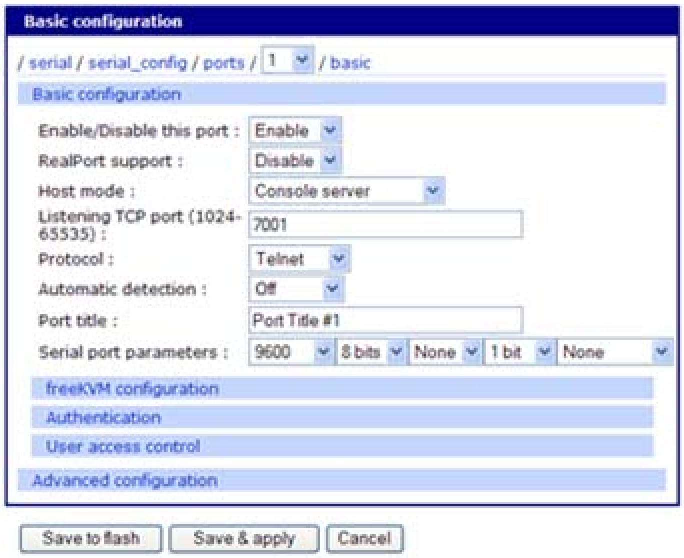
About Basic and Advanced Serial Port Settings

Besides using the quick-start procedure that applies to all serial ports, serial port settings can be modified from their factory defaults. The Digi Passport unit has two levels of serial port configuration settings:

- **Basic configuration**: Basic serial port settings needed for all ports.
- **Advanced configuration**: The complete set of serial port settings.

To Illustrate, here are examples of the basic and advanced configuration settings for the same port:

Basic configuration settings:



Basic configuration

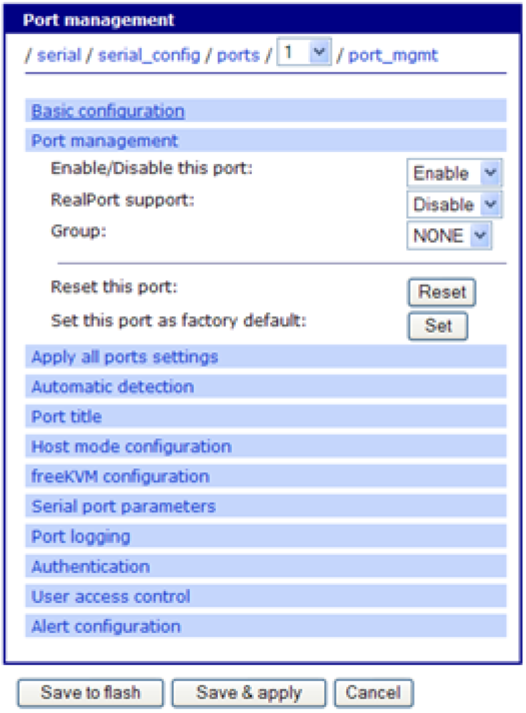
/ serial / serial_config / ports / 1 / basic

Basic configuration

Enable/Disable this port : Enable
RealPort support : Disable
Host mode : Console server
Listening TCP port (1024-65535) : 7001
Protocol : Telnet
Automatic detection : Off
Port title : Port Title #1
Serial port parameters : 9600 | 8 bits | None | 1 bit | None

freeKVM configuration
Authentication
User access control
Advanced configuration

Advanced configuration settings:



Port management

/ serial / serial_config / ports / 1 / port_mgmt

Basic configuration
Port management
Enable/Disable this port: Enable
RealPort support: Disable
Group: NONE
Reset this port: Reset
Set this port as factory default: Set
Apply all ports settings
Automatic detection
Port title
Host mode configuration
freeKVM configuration
Serial port parameters
Port logging
Authentication
User access control
Alert configuration

Links to other port configuration settings

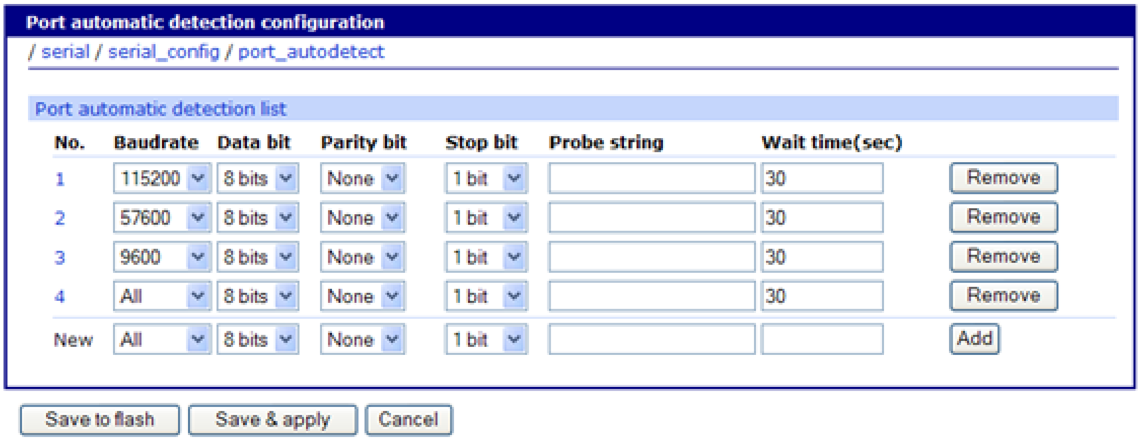
This topic focuses on the Basic and Advanced port configuration settings and on configuring automatic detection for serial ports. There are several other links to port settings on the Configuration screen which are covered d later in this chapter:

- **Port access menu configuration**: Configures the basic access options for the command-line based Port Access Menu.See "Port Access Menu Configuration" on page 86.
- **Port group configuration**: Configures groups of ports, which allows for commands to be sent to multiple ports. See "Port Group Configuration: Applying Commands to Multiple Ports" on page 87.

Recommended sequence for configuring port settings

If using the Basic and Advanced configuration settings to configure serial ports, the sequence is:

1. In the Web interface for the the Digi Passport unit, go to **Serial Port > Configuration**.
2. **Before** connecting any serial devices to the Digi Passport unit, configure the Automatic Detection feature. On the **Configuration** page, click **Port automatic detection configuration**. Create a *port automatic detection list*, which is a set of common serial port characteristics used to determine which kind of device is attached to the Digi Passport unit, such as baud rate, data, parity, stop bits, and a string sent to the device to detect its operating system and host name. The port automatic detection list is used as probe criteria when Automatic Device Recognition is activated and the serial ports are tested. For more information on Automatic Detection settings, see "Configure Automatic Detection" on page 77. Here is a typical example of probe criteria.



Port automatic detection configuration

/ serial / serial_config / port_autodetect

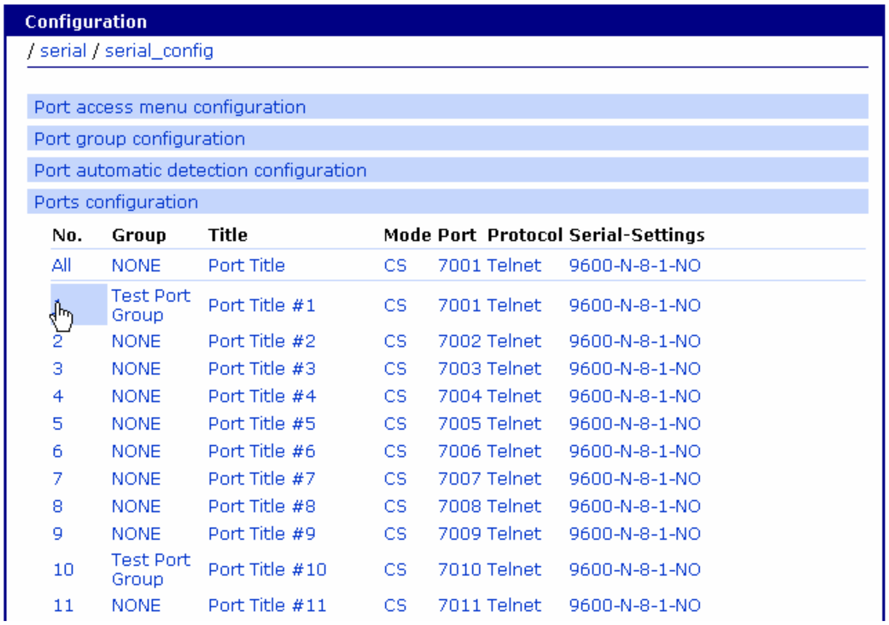
Port automatic detection list

No.	Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time(sec)	
1	115200	8 bits	None	1 bit		30	Remove
2	57600	8 bits	None	1 bit		30	Remove
3	9600	8 bits	None	1 bit		30	Remove
4	All	8 bits	None	1 bit		30	Remove
New	All	8 bits	None	1 bit			Add

3. Click **Save & apply**.
4. Enable Automatic Detection for all ports: In the serial ports view (**Serial Port > Configuration**), click **All** to select all ports. Change the **Automatic Detection** setting from **Off** to **Active**.
5. Click **Save & apply**.
6. As needed, change configuration settings for individual ports, using either **Basic configuration** or **Advanced configuration** settings. Basic configuration settings are described on page 68. Advanced configuration settings are described on page 92.

Basic Port Configuration Settings

On the **Ports configuration** page (selected by ***serial port >* Configuration**), selecting any port number in the **No.** column displays the **Basic configuration** page. For example:



Configuration

/ serial / serial_config

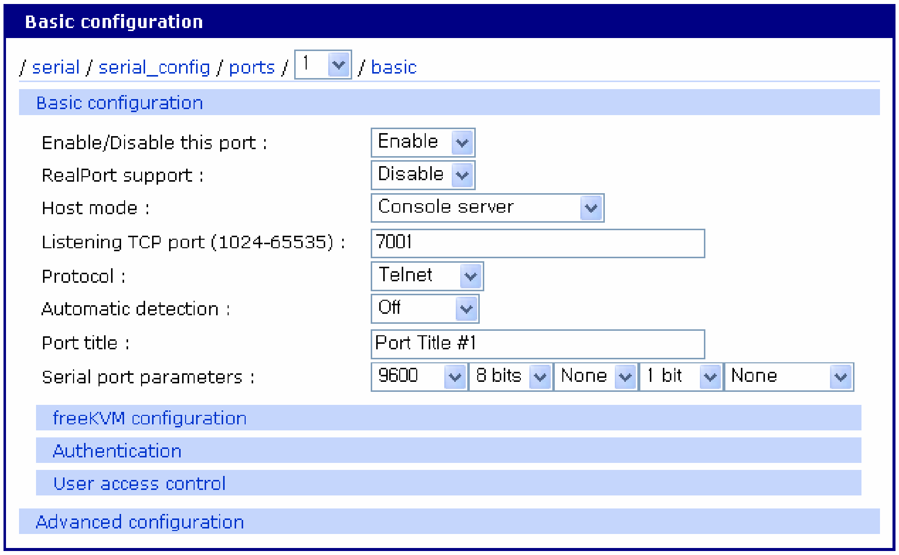
Port access menu configuration

Port group configuration

Port automatic detection configuration

Ports configuration

No.	Group	Title	Mode	Port	Protocol	Serial-Settings
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO
1	Test Port Group	Port Title #1	CS	7001	Telnet	9600-N-8-1-NO
2	NONE	Port Title #2	CS	7002	Telnet	9600-N-8-1-NO
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO
4	NONE	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO
5	NONE	Port Title #5	CS	7005	Telnet	9600-N-8-1-NO
6	NONE	Port Title #6	CS	7006	Telnet	9600-N-8-1-NO
7	NONE	Port Title #7	CS	7007	Telnet	9600-N-8-1-NO
8	NONE	Port Title #8	CS	7008	Telnet	9600-N-8-1-NO
9	NONE	Port Title #9	CS	7009	Telnet	9600-N-8-1-NO
10	Test Port Group	Port Title #10	CS	7010	Telnet	9600-N-8-1-NO
11	NONE	Port Title #11	CS	7011	Telnet	9600-N-8-1-NO



Basic configuration

/ serial / serial_config / ports / 1 / basic

Basic configuration

Enable/Disable this port :	Enable
RealPort support :	Disable
Host mode :	Console server
Listening TCP port (1024-65535) :	7001
Protocol :	Telnet
Automatic detection :	Off
Port title :	Port Title #1
Serial port parameters :	9600 / 8 bits / None / 1 bit / None

freeKVM configuration

Authentication

User access control

Advanced configuration

The **Basic configuration** page sets the essential parameters required to access the device attached to the corresponding serial port, including:

- Enabling or disabling the serial port
- Enabling or disabling use of RealPort for the serial port
- Host mode, or the mode of communication between serial devices and remote hosts
- The listening TCP port, or network port
- Protocol
- Enabling or disabling Automatic Detection of devices for the specific port
- Port title
- Serial port parameters

There are also links to additional pages of configuration settings:

- **freeKVM configuration**: to define the available methods for connecting to the freeKVM graphical interface of the attached system. See "Configure and Use freeKVM" on page 168.
- **Authentication**: to define the method used for approving access to the attached system (TACACS+, LDAP, RADIUS, Active Directory, Local User database, etc.) See "Authentication" on page 150.
- **User Access control**: to define user-specific access permissions and restrictions. See "Configure User Access Control" on page 142.

Clicking the **Advanced configuration** link displays a more detailed set of port configuration settings. These settings are described on "Advanced Port Configuration Settings" on page 92.

Enable and Disable Ports

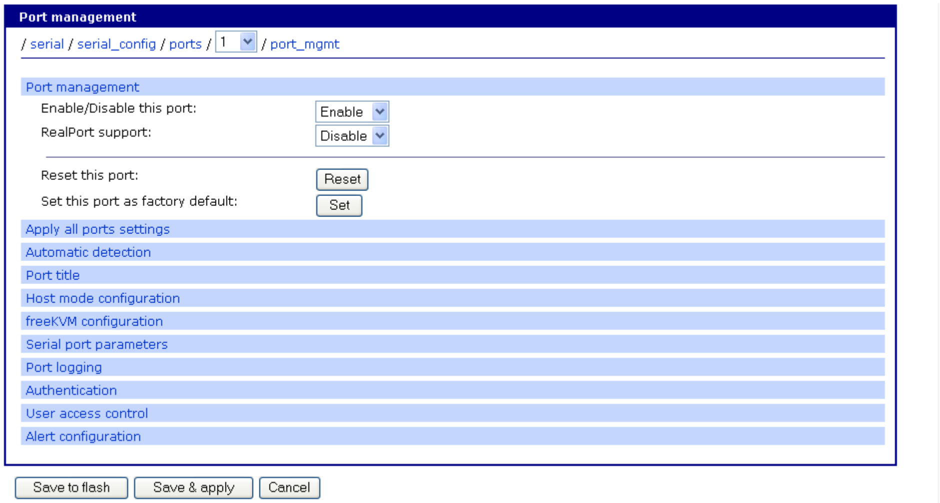
All serial ports may be enabled or disabled individually or as a group from the web interface. Click **Serial port** > **Configuration** > ***port number*** or all. Select **Port Management > Enable or Disable** from the pulldown menu. Then click **Save to flash** and continue with other configurations or click **Save & apply**.

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, while actually 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 are also included.

When RealPort is used to communicate with a serial port on the Digi Passport, the other capabilities of the Digi Passport are not available for that port. This means 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, click **Serial port** > **Configuration** > ***port number***. Select **Port Management > Enable this port** from the pulldown menu. Select **Enable RealPort support** from the pulldown menu. Click **Save to flash** and continue with other configurations or click **Save & apply**.



Port management

/ serial / serial_config / ports / 1 / port_mgmt

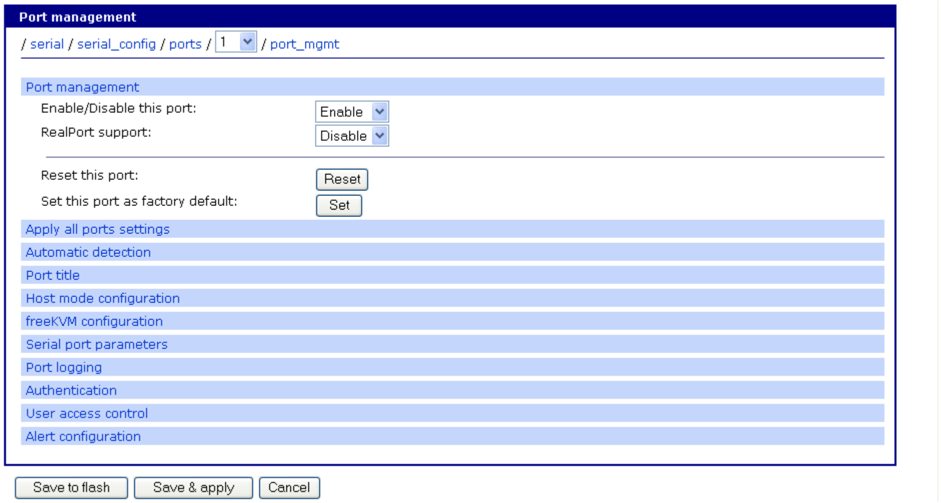
Port management

Enable/Disable this port: Enable

RealPort support: Disable

Reset this port: Reset

Set this port as factory default: Set



Port management

/ serial / serial_config / ports / 1 / port_mgmt

Port management

Enable/Disable this port: Enable

RealPort support: Disable

Reset this port: Reset

Set this port as factory default: Set

Host Mode Configuration

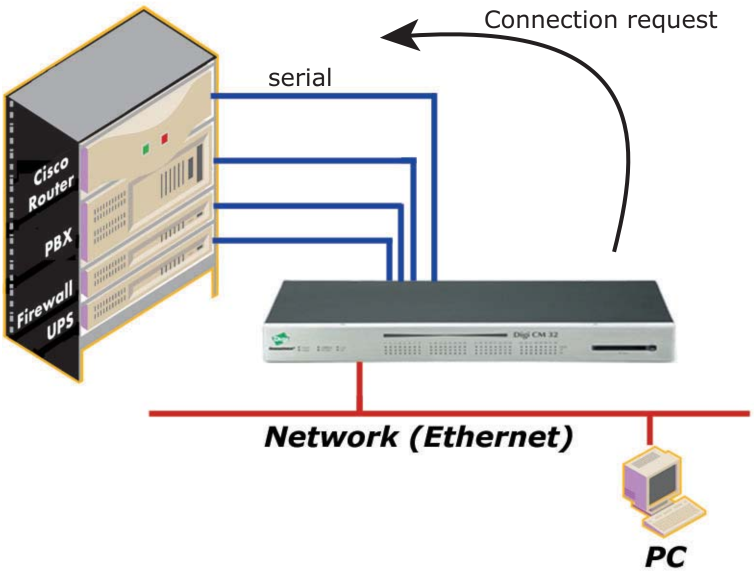
The Digi Passport unit provides several modes of communication between serial devices and remote hosts: Console server, terminal server, dial-in modem, dial-in terminal server, and Point-to-Point Protocol (PPP) mode.

On the **Basic configuration** page, for the **Host mode** setting, select from a set of predefined modes of communication between serial devices and remote hosts. Selecting the host mode automatically configures several settings, such as the type of console server, protocol, and escape sequences used. To review or modify any host-mode settings, go to the **Advanced configuration** settings and click the **Host mode configuration** link. See "Advanced Host Mode Settings" on page 97 for descriptions.

Here are descriptions of the supported host modes.

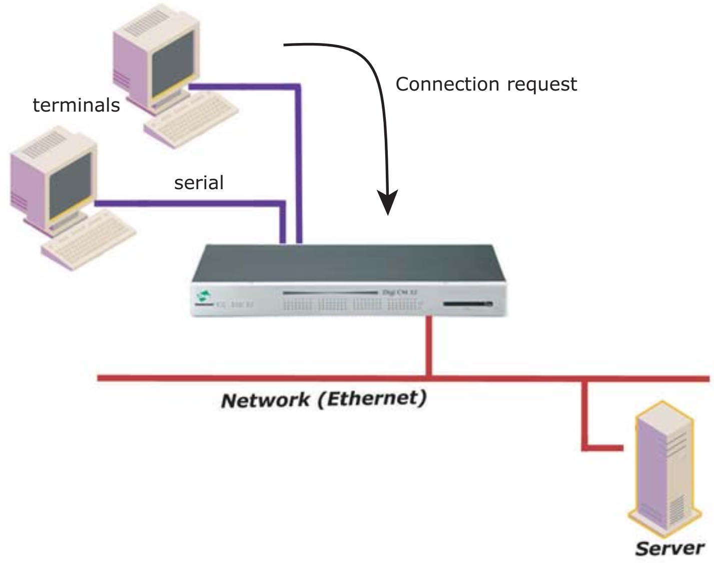
Console Server Mode (default host mode)

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. Connecting to the TCP socket provides access to the device attached to the serial port, as if the device were connected directly to the network. RawTCP is also supported with the Console Server Mode.



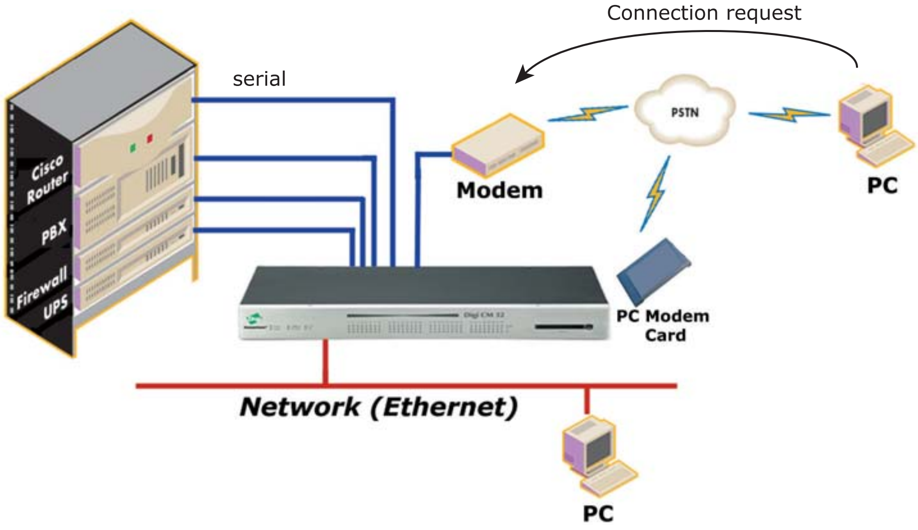
Terminal Server Mode

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 before the port can be configured for a Telnet or SSH client. This mode is used to access servers on the network from a serial terminal. RawTCP is also supported with the Terminal Server Mode.



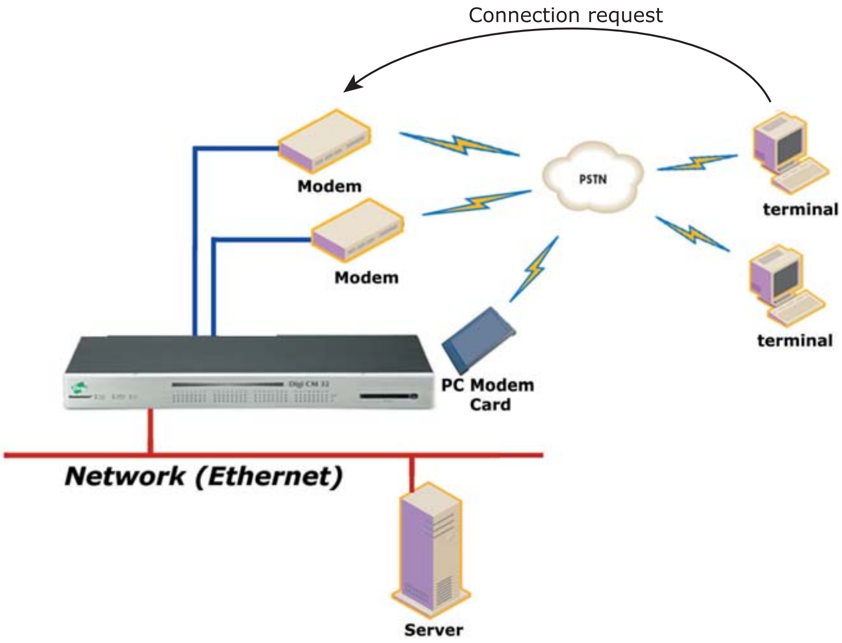
Dial-In Modem Mode

In dial-in modem 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 example, user **root** would see the command line interface (CLI), while user **admin** would see the configuration menu or CLI depending on the shell for that user.



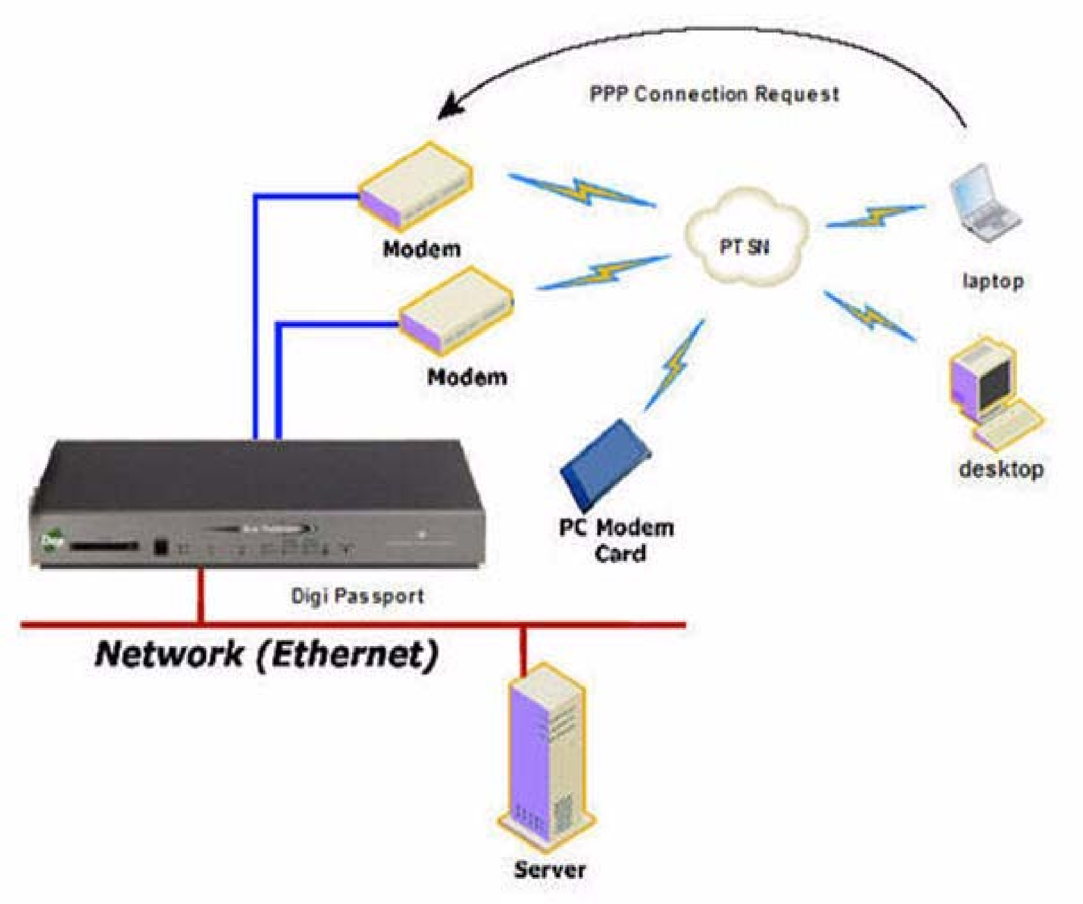
Dial-In Terminal Server Mode

Dial-in terminal server mode is a combination of terminal server mode and dial-in modem mode. In this 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 dialing 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 to use modems to access servers on a network.



PPP Mode

PPP (Point to Point Protocol) host mode configures the Digi Passport unit to support dial-in PPP connections to it.



Listening TCP Port

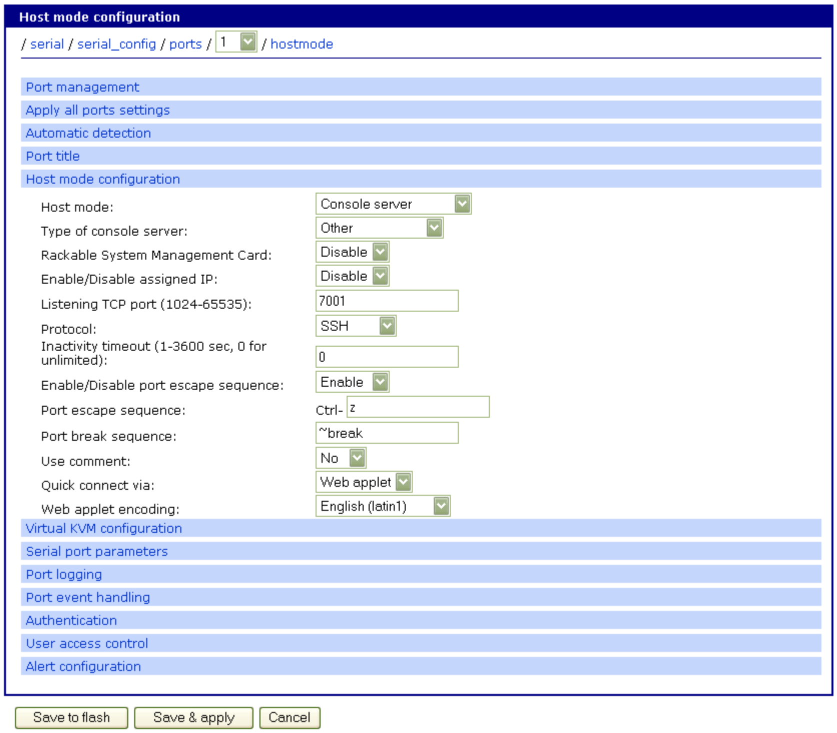
The listening TCP port is the TCP network port specified when connecting directly to the port using Telnet or SSH.

Protocol setting

The Protocol setting configures the communication protocol used over the serial port. There are three protocol options: RawTCP, SSH, and Telnet.

- Select **SSH** when logging in from an SSH client program to access a port.
- Select **RawTCP** when connecting directly to a TCP socket.
- Select **Telnet** when logging in from a Telnet client program and accessing the ports.

To select the correct protocol, use the Host mode configuration page in the web interface.



Host mode:	Console server
Type of console server:	Other
Rackable System Management Card:	Disable
Enable/Disable assigned IP:	Disable
Listening TCP port (1024-65535):	7001
Protocol:	SSH
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:	Web applet
Web applet encoding:	English (latin1)

Configure Automatic Detection

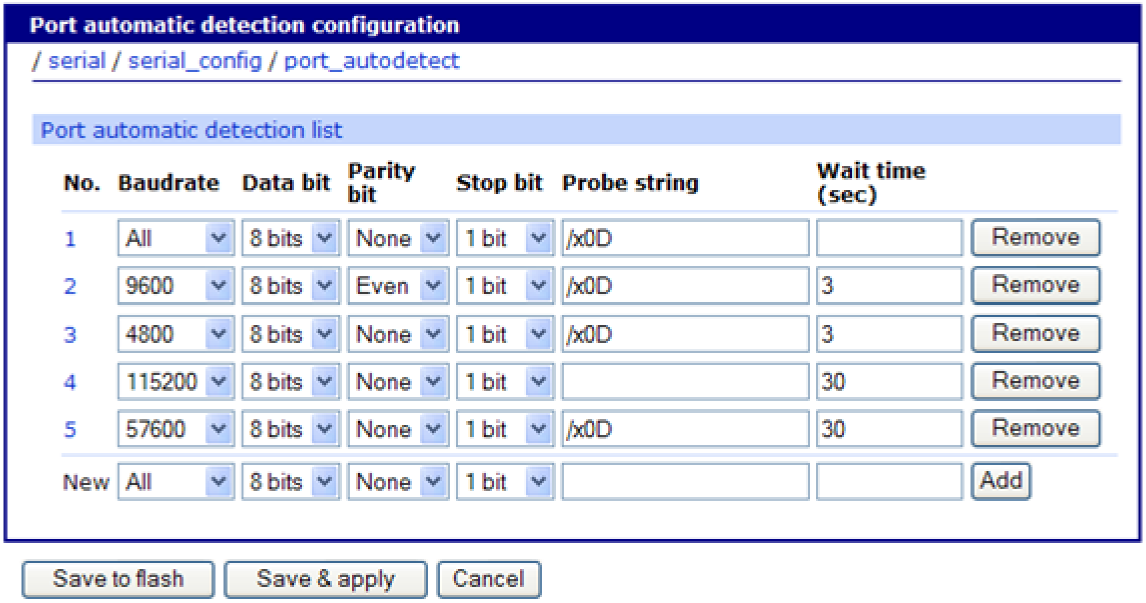
Automatic detection and its role in Automatic Device Recognition

The *Automatic Device Recognition* feature allows the Digi Passport unit to automatically detect and recognize attached devices and the serial parameters for the devices. The port configuration settings for *automatic detection* are used to determine the baud rate and other serial characteristics for the serial port, based on a user-defined list. Automatic Device Recognition takes this device recognition a step further, to determine the operating system and host name of the attached equipment.

There are several elements to automatic detection settings: the port automatic detection list, the automatic detection state, and the rules for performing automatic detection. Each of these elements has factory default settings that can be modified through the Basic or Advanced serial port configuration settings.

Port automatic detection list

The **Port automatic detection list**: a set of serial characteristics used to probe serial ports once automatic detection is active. Probe criteria include baud rate; data, parity and stop bits, a string to be sent during the probe, and how long to wait for a response. The port automatic detection list is defined by selecting Port automatic detection configuration on the main Configuration screen for ports. 16 entries can be made in the list, and they will each be tested in order listed when Automatic Device Recognition tests the port. Here is an example port automatic detection list:



Port automatic detection configuration

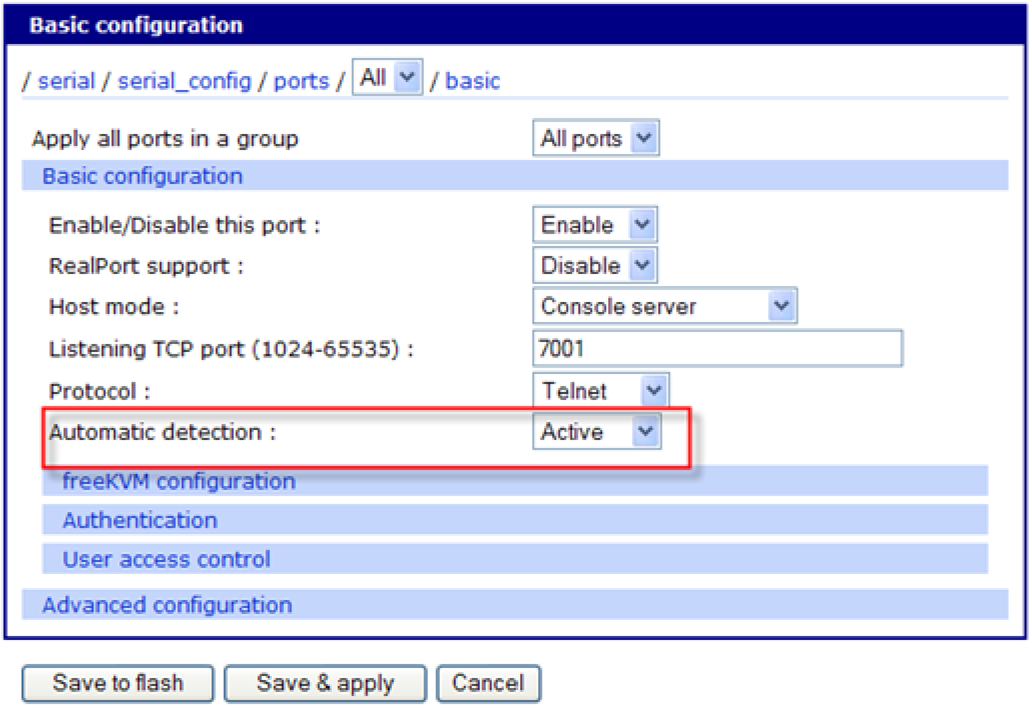
/ serial / serial_config / port_autodetect

Port automatic detection list

No.	Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time (sec)	
1	All	8 bits	None	1 bit	/x0D		Remove
2	9600	8 bits	Even	1 bit	/x0D	3	Remove
3	4800	8 bits	None	1 bit	/x0D	3	Remove
4	115200	8 bits	None	1 bit		30	Remove
5	57600	8 bits	None	1 bit	/x0D	30	Remove
New	All	8 bits	None	1 bit			Add

Automatic detection state: Off, Active, Passive

The *automatic detection state* for all or individual ports can be set to one of three states: **Off**, **Active**, or **Passive**. The automatic detection state is set by the Basic serial port configuration setting **Automatic detection**:



Basic configuration

/ serial / serial_config / ports / All / basic

Apply all ports in a group: All ports

Enable/Disable this port : Enable

RealPort support : Disable

Host mode : Console server

Listening TCP port (1024-65535) : 7001

Protocol : Telnet

Automatic detection : Active

The three automatic detection states have these effects:

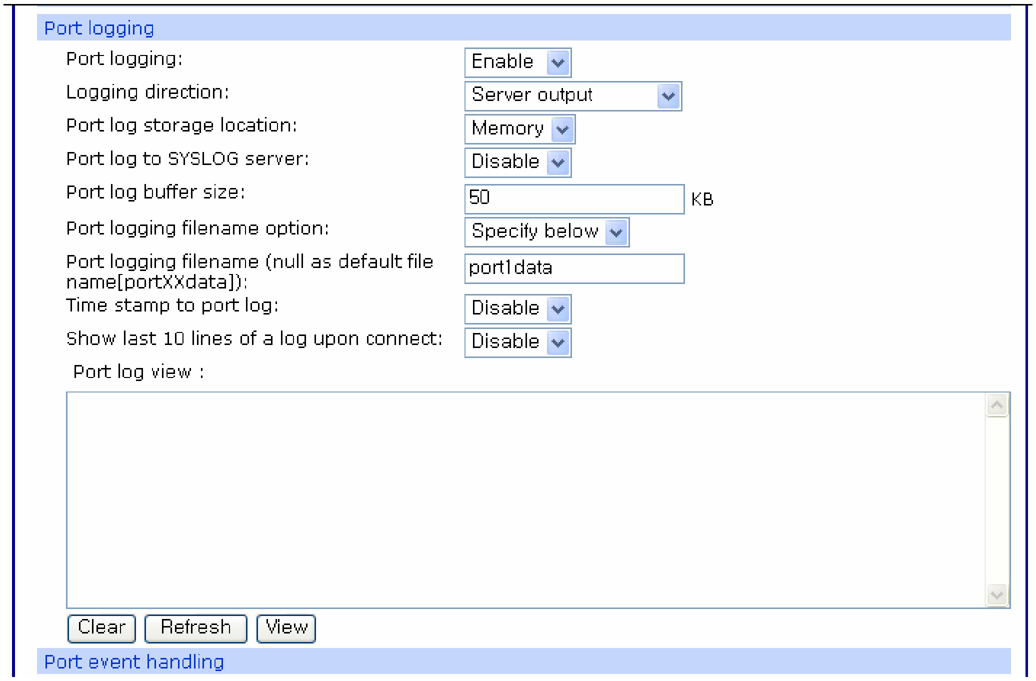
- **Off**: Automatic detection is not on. The Digi Passport will not attempt to determine what is attached to the serial port.
- **Active**: The Digi Passport unit sends probe sequences to the serial port according to the defined port automatic detection list.
- **Passive**: The Digi Passport unit does not send out probe sequences to the port. Instead, it passively monitors the port at the defined settings and attempts to discover the baud rate, operating system and hostname from traffic sent from the port and while it is used.

Important: For Active and Passive automatic detection to work, make sure that the **DNS configuration** and the **Port automatic detection** configuration are both properly configured.

Port logging and passive automatic detection

In **Passive automatic detection**, the **Port logging** option setting for the port or ports is enabled automatically, because passive automatic detection is done through the port log file.

For the port logging feature to create and log to the proper port log file, ensure that the serial port parameters are set correctly.



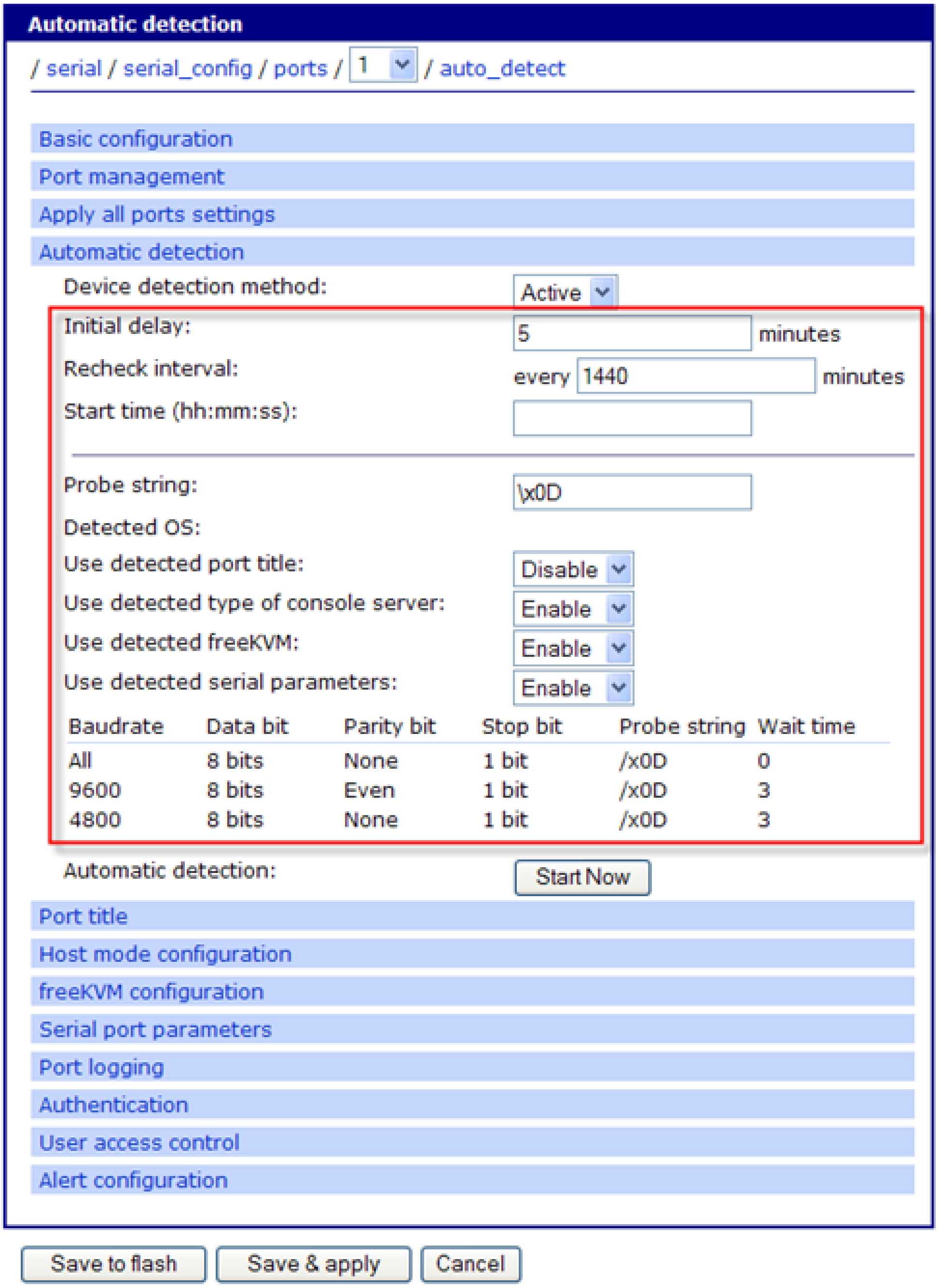
Port logging

Port logging:	Enable
Logging direction:	Server output
Port log storage location:	Memory
Port log to SYSLOG server:	Disable
Port log buffer size:	50 KB
Port logging filename option:	Specify below
Port logging filename (null as default file name[portXXdata]):	port1data
Time stamp to port log:	Disable
Show last 10 lines of a log upon connect:	Disable

Port log view :

Automatic detection rules

Automatic detection rules control how automatic detection is performed on serial ports, such as how long to wait before performing the original probe, how long to wait until the next probe, whether to start the probe at a particular time, and whether to use any detected values such as port title and serial port parameters. Automatic detection rules can be applied to all or selected serial ports, and there are default rules. All options on the **Automatic detection** page are enabled automatically. Automatic detection rules are set and changed in the **Advanced configuration** settings for serial ports (**Serial port > Configuration > All** or ***port No.*** **> Advanced Configuration > Automatic detection**). Here is an example of automatic detection rules:



Device detection method: Active

Initial delay: 5 minutes

Recheck interval: every 1440 minutes

Start time (hh:mm:ss):

Probe string: \x0D

Detected OS:

Use detected port title: Disable

Use detected type of console server: Enable

Use detected freeKVM: Enable

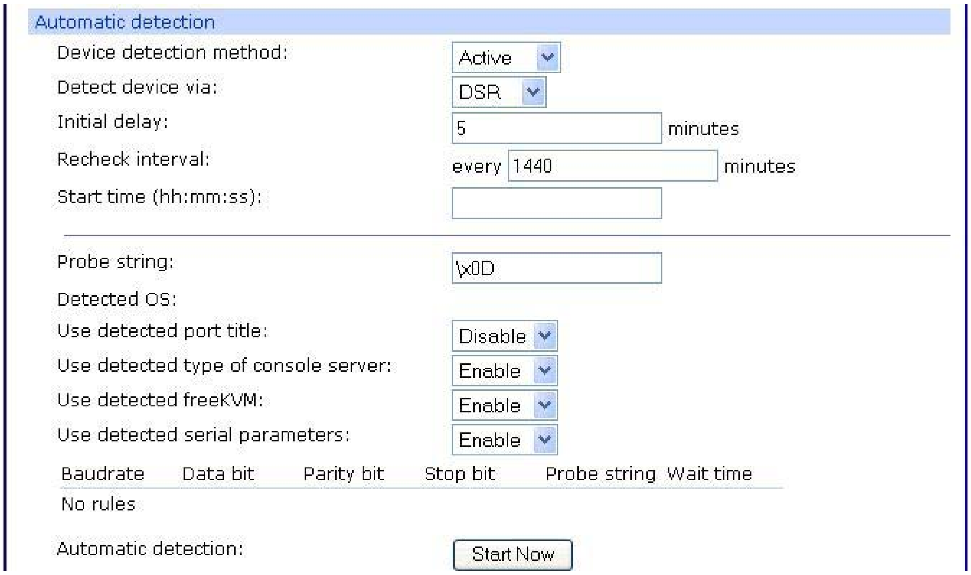
Use detected serial parameters: Enable

Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time
All	8 bits	None	1 bit	/x0D	0
9600	8 bits	Even	1 bit	/x0D	3
4800	8 bits	None	1 bit	/x0D	3

Automatic detection: Start Now

When automatic detection for connected devices begins

In factory default mode, if automatic detection is set to **Active**, the Digi Passport unit waits 5 minutes (the **Initial delay** setting), then probes the ports for which automatic detection is enabled using the specified port automatic detection list. After that, it waits an interval before performing the next probe. This interval is either 1440 minutes (the default value of the **Recheck interval** setting; this value can be changed) or until a specified start time occurs (the **Start time** setting).



Automatic detection

Device detection method: Active

Detect device via: DSR

Initial delay: 5 minutes

Recheck interval: every 1440 minutes

Start time (hh:mm:ss):

Probe string: \x0D

Detected OS:

Use detected port title: Disable

Use detected type of console server: Enable

Use detected freeKVM: Enable

Use detected serial parameters: Enable

Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time
No rules					

Automatic detection:

Note that the value for the **Initial delay** *must* be less than that for the **Recheck interval**.

Option to ignore the status of DSR signal. If you selected **None** for **Detect device via** option, Passport will start ADR regardless of the status of the DSR signal.

Automatic detection can also be started manually by clicking the **Start Now** button at the bottom of **Automatic detection** page. Automatic detection is then performed according to the selected Device detection method.

There are timing considerations when configuring automatic detection and connecting devices to the Digi Passport unit. Specifically, if automatic detection is set to **Active** and turned on *after* a device is physically plugged in to a serial port on the Digi Passport unit, automatic detection will not attempt to probe the port until after the time specified by the **Recheck Interval** elapses. Therefore, either:

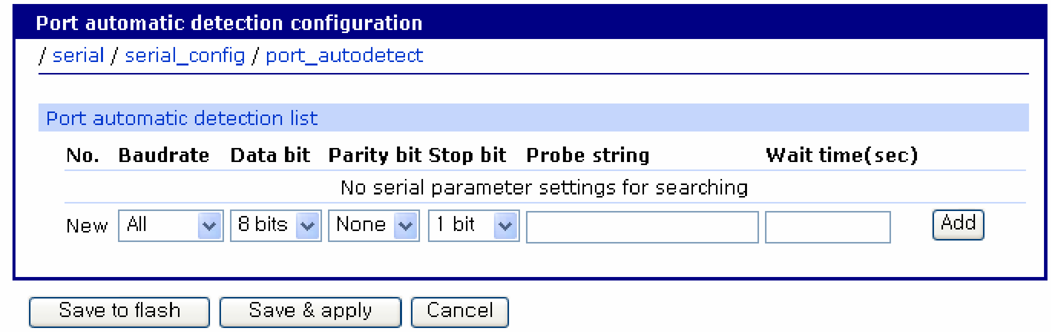
- Configure automatic detection before plugging devices into the Digi Passport unit

or

- Unplug devices, configure automatic detection, and plug in the devices again.

Configure automatic detection

1. Add the appropriate Port automatic detection list by navigating to **Serial port > Port automatic detection configuration > Port automatic detection list**. By factory default, there are no Port automatic detection lists defined as shown below:



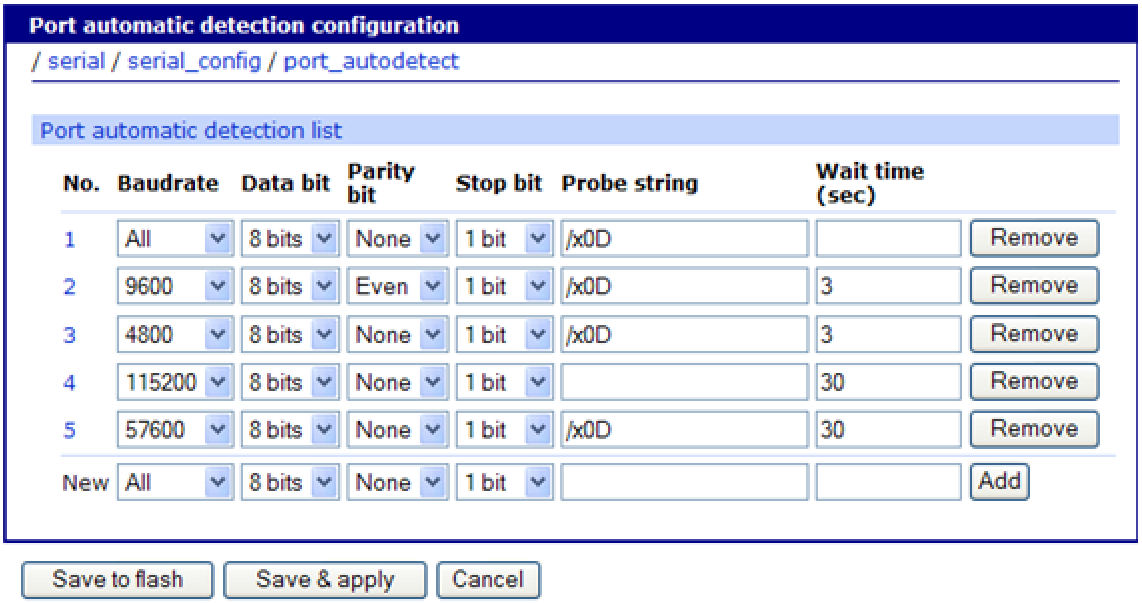
Port automatic detection configuration

/ serial / serial_config / port_autodetect

Port automatic detection list

No.	Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time(sec)	
No serial parameter settings for searching							
New	All	8 bits	None	1 bit			Add

2. Add as many sets of serial parameters to the port automatic detection list as needed, including baud rate, data bit, parity bit, stop bit, probe string, and wait time. These settings are described in more detail in "Advanced Serial Port Parameters" on page 98. For example:



Port automatic detection configuration

/ serial / serial_config / port_autodetect

Port automatic detection list

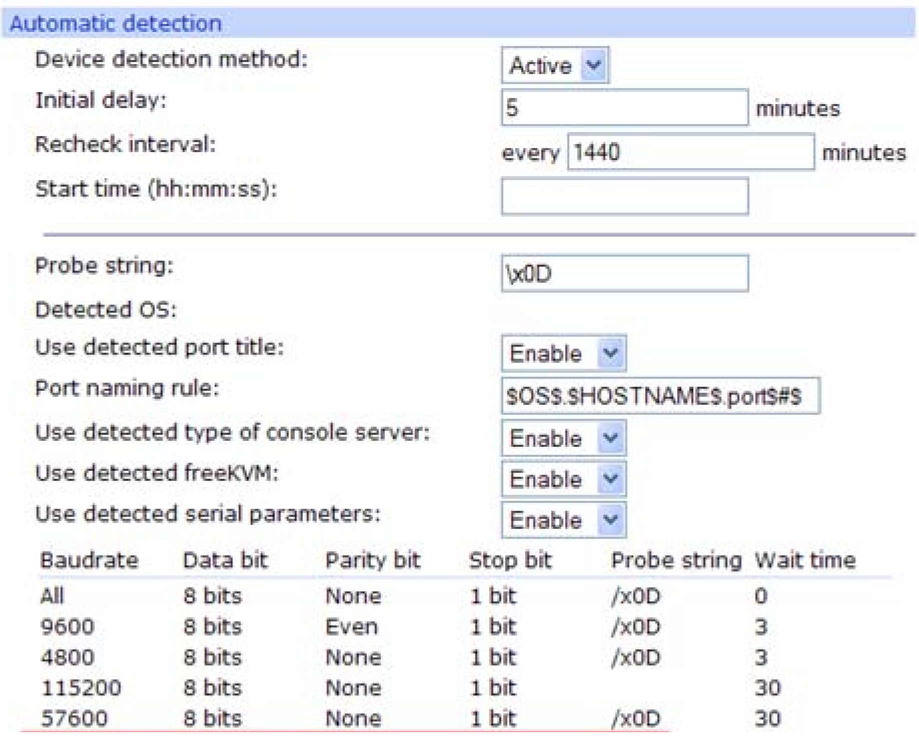
No.	Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time (sec)	
1	All	8 bits	None	1 bit	/x0D		Remove
2	9600	8 bits	Even	1 bit	/x0D	3	Remove
3	4800	8 bits	None	1 bit	/x0D	3	Remove
4	115200	8 bits	None	1 bit		30	Remove
5	57600	8 bits	None	1 bit	/x0D	30	Remove
New	All	8 bits	None	1 bit			Add

3. Set the Automatic Detection state (Off, Active, or Passive) for all or selected ports.

   In the serial ports view (**Serial Port > Configuration**), click **All** or ***port number***. Change the **Automatic Detection** setting from **Off** to **Active**.

   There are several other automatic detection parameters on the page. After selecting **Active** or **Passive** for **Automatic detection** on the **Basic configuration** page, these parameters are set to their defaults, as shown below; the one exception from the defaults in this example is the parameters below **Use detected serial parameters**. The default is an empty list, but the example shows the port automatic detection list created in step 2.

   For descriptions of the automatic detection options from **Initial delay** through **Use detected serial parameters**, see "Advanced Automatic Detection Settings" on page 93.



Automatic detection

Device detection method: Active

Initial delay: 5 minutes

Recheck interval: every 1440 minutes

Start time (hh:mm:ss):

Probe string: \x0D

Detected OS:

Use detected port title: Enable

Port naming rule: OS.$HOSTNAME$.port$#$

Use detected type of console server: Enable

Use detected freeKVM: Enable

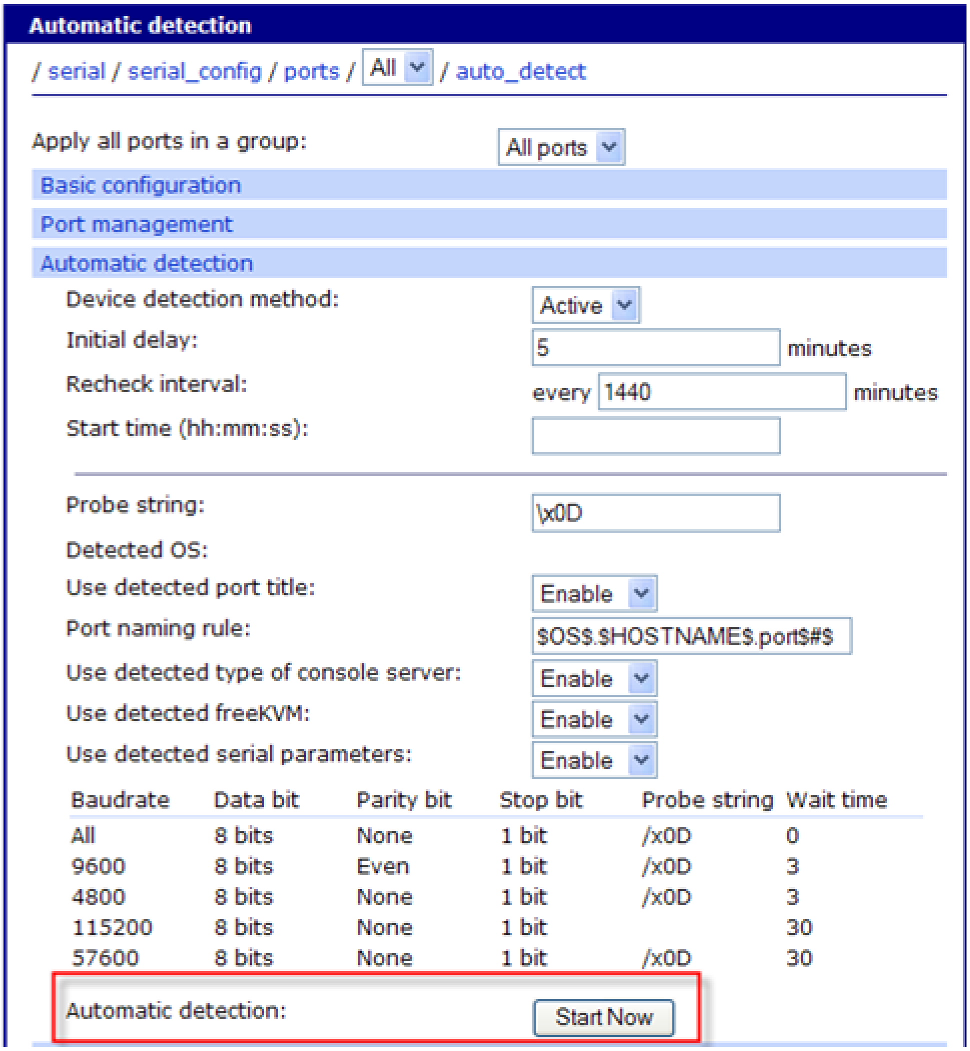
Use detected serial parameters: Enable

Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time
All	8 bits	None	1 bit	/x0D	0
9600	8 bits	Even	1 bit	/x0D	3
4800	8 bits	None	1 bit	/x0D	3
115200	8 bits	None	1 bit		30
57600	8 bits	None	1 bit	/x0D	30

4. Click **Save & apply**.

5. Start automatic detection on one or all ports.
   - If the **Device detection method** was set to **Active**, automatic detection is performed with the output messages of device. The Digi Passport unit performs serial parameter detection using the settings in the port automatic detection list.
   - If the **Device detection method** was set to **Passive**, automatic detection is performed using the port log.

     Important: Passive detection first detects parameters using the port log. Before setting the Device detection method to Passive, make sure the serial port parameters are correctly set and to enable Port logging (see "Configure Port Logging" on page 57.
   - To start automatic detection **manually**, go to the Advanced Automatic detection settings: select **Serial port > Configuration > All** or ***port number* > Advanced Configuration > Automatic detection.** Click the **Start Now** button at the bottom of **Automatic detection** page. In this case, automatic detection is performed according to the selected **Device detection method**.



Automatic detection

/ serial / serial_config / ports / All / auto_detect

Apply all ports in a group: All ports

Basic configuration

Port management

Automatic detection

Device detection method: Active

Initial delay: 5 minutes

Recheck interval: every 1440 minutes

Start time (hh:mm:ss):

Probe string: \x0D

Detected OS:

Use detected port title: Enable

Port naming rule: OS.$HOSTNAME$.port$#$

Use detected type of console server: Enable

Use detected freeKVM: Enable

Use detected serial parameters: Enable

Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time
All	8 bits	None	1 bit	/x0D	0
9600	8 bits	Even	1 bit	/x0D	3
4800	8 bits	None	1 bit	/x0D	3
115200	8 bits	None	1 bit		30
57600	8 bits	None	1 bit	/x0D	30

Automatic detection:

*free*KVM Configuration

freeKVM configuration is a link to the settings for configuring the freeKVM feature. See "Configure and Use freeKVM" on page 168 for more information.

Authentication

Authentication is a link to the settings for configuring any user authentication desired or required for users accessing ports. See "Configure Authentication Methods for Port Access" on page 151 for more information.

User Access Control

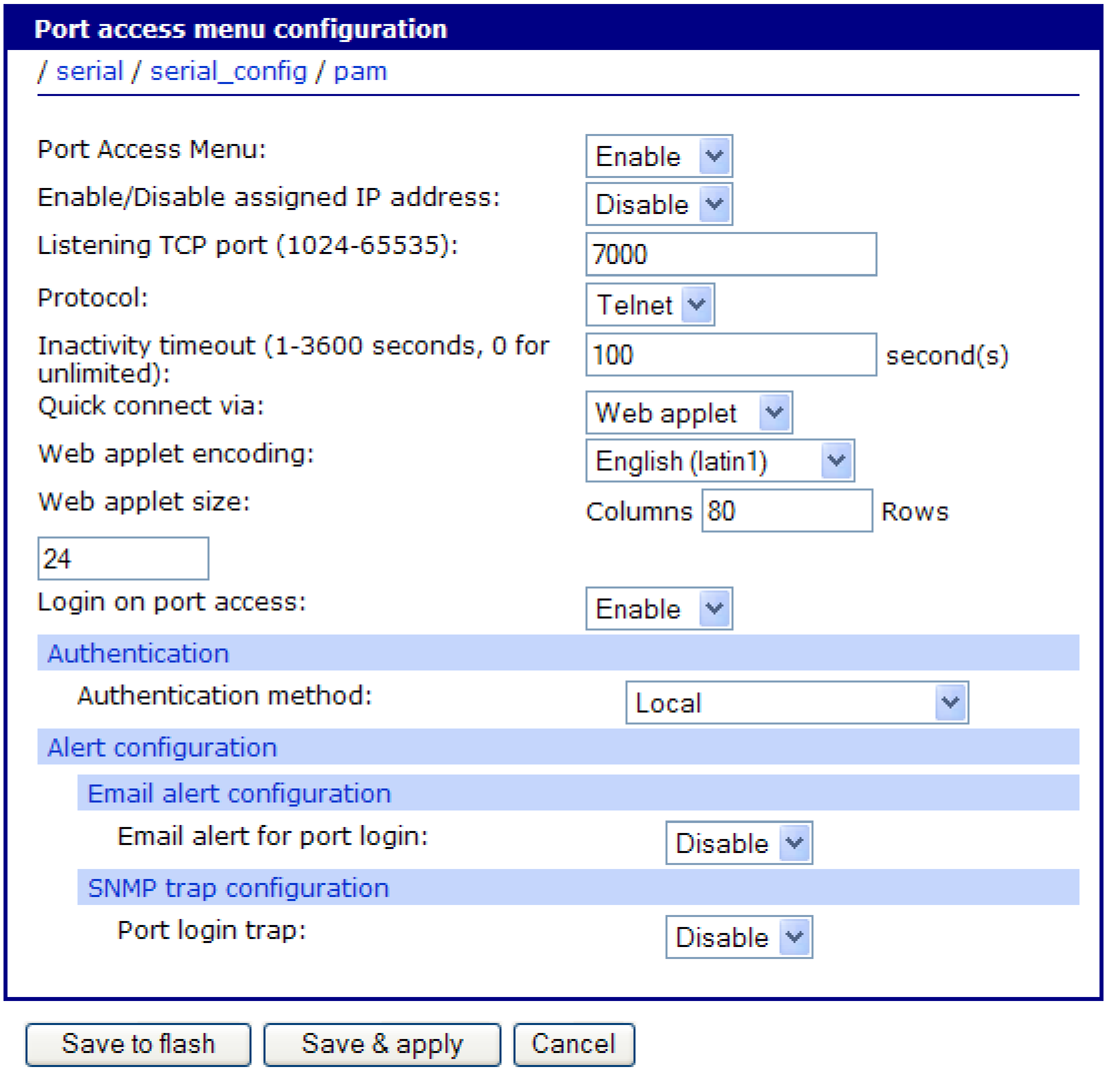
User access control is a link to the settings for configuring user access rights to ports. See "Configure User Access Control" on page 142 for more information.

Port Access Menu Configuration

The Port Access Menu provides a menu-driven command-line interface for Digi Passport users to access equipment through a standardized interface without using the Web interface. It is one of several alternative mechanisms available. Other alternatives include custom menus and direct access to the port via IP address or socket number. For more details about custom menus, see "Custom and Default Menus" on page 157.

In the web interface, the **Port Access menu configuration** page configures the basic options for the Port Access Menu, including the socket, protocol, and authentication for using this feature. To access this page, go to **Serial port > Configuration > Port access menu configuration**.

The **Login on port access** setting controls whether a login is forced whenever a user accesses the port. **Enable** means a login is forced. **Disable** means that the access rights from the user logged to the port access menu are inherited.



Port access menu configuration

/ serial / serial_config / pam

Port Access Menu: Enable

Enable/Disable assigned IP address: Disable

Listening TCP port (1024-65535): 7000

Protocol: Telnet

Inactivity timeout (1-3600 seconds, 0 for unlimited): 100 second(s)

Quick connect via: Web applet

Web applet encoding: English (latin1)

Web applet size: Columns 80 Rows 24

Login on port access: Enable

Authentication

Authentication method: Local

Alert configuration

Email alert configuration

Email alert for port login: Disable

SNMP trap configuration

Port login trap: Disable

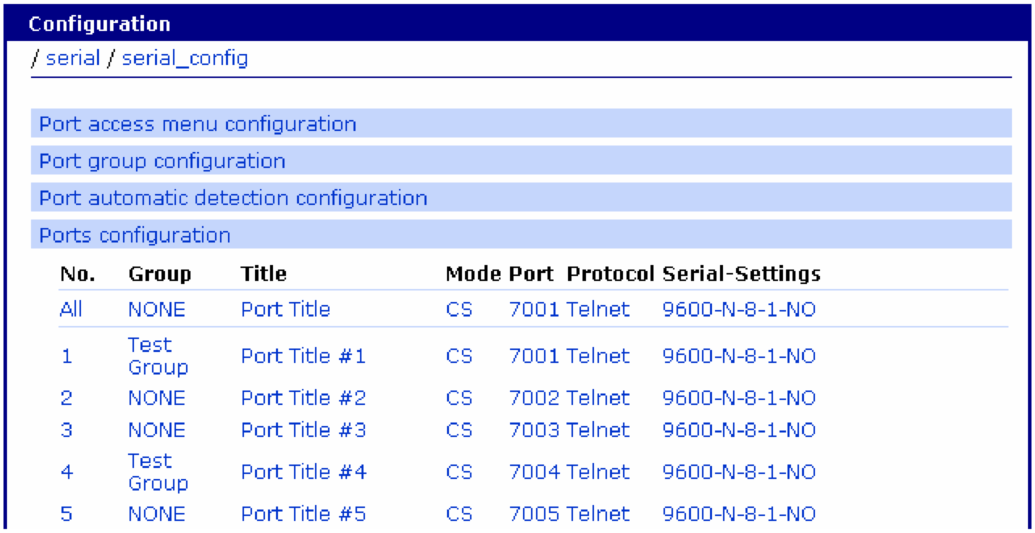
Port Group Configuration: Applying Commands to Multiple Ports

As a convenience feature, port groups can be created to apply commands to multiple ports. Instead of issuing commands to individual serial ports, the commands can be sent to all ports in a group simultaneously through the port escape menu. This can be useful for example when performing a mass upgrade or emergency mass shutdown to multiple systems.

Port groups are configured by clicking on the **Port group configuration** link.

There is no limit on the number of port groups that can be defined.

Here is a view of a list of ports for which some ports are assigned to a group and some ports are not.

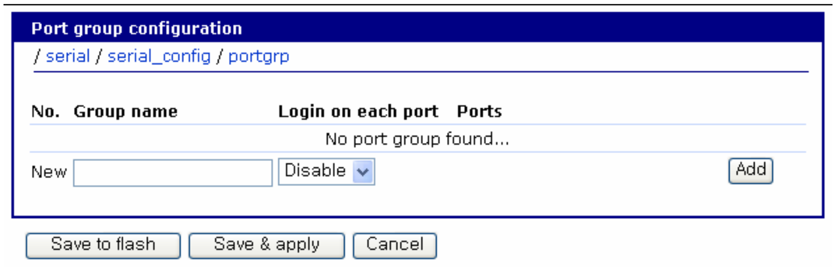


No.	Group	Title	Mode	Port	Protocol	Serial-Settings
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO
1	Test Group	Port Title #1	CS	7001	Telnet	9600-N-8-1-NO
2	NONE	Port Title #2	CS	7002	Telnet	9600-N-8-1-NO
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO
4	Test Group	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO
5	NONE	Port Title #5	CS	7005	Telnet	9600-N-8-1-NO

Create a port group

To create a port group:

1. On the serial port Configuration page, click the **Port group configuration** link. The Port group configuration settings are displayed.



Port group configuration

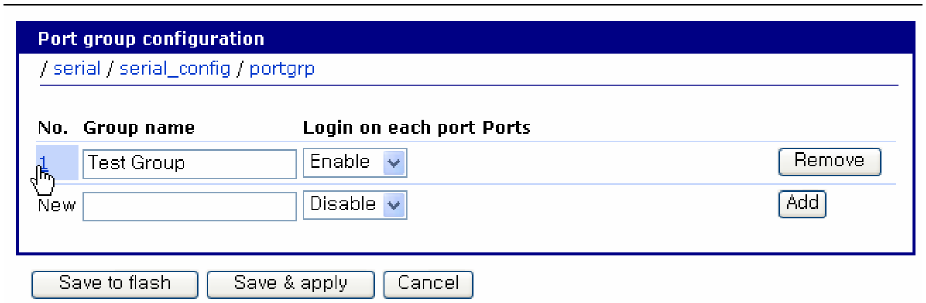
/ serial / serial_config / portgrp

No.	Group name	Login on each port	Ports	
No port group found...				
New		Disable		Add

2. In the **Group name** field, enter a name for the port group.
3. For the **Login on each port setting**, select whether a login should be performed on each port in the group.

   If **Login on each port** is **Enabled**, when a connection is made to the group, a separate login to each port is forced as well as a login to the group. This means that a login prompt for each individual port is displayed, as opposed to only displaying a login prompt when connecting to the group. The advantage of forcing a login to each port in the group is more specific logging of who is connected to each port and when (as when multiple users are attached to the group at the same time).

   Turning off **Login on each port** (**Disabled**) is useful when sending mass commands to multiple units, for example, when doing batch reconfiguration of identical systems. Disabling the port logins saves time because the login steps do not have to be performed on each port.
4. Click **Add**.
5. Once the group is added, further configure the group by clicking its port group number, as shown:

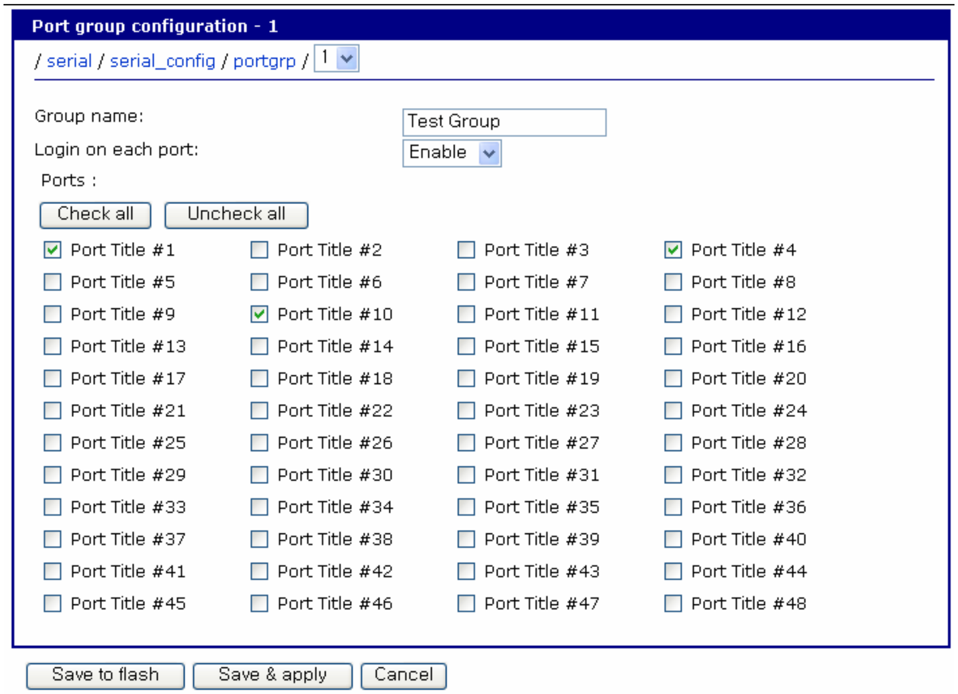


Port group configuration

/ serial / serial_config / portgrp

No.	Group name	Login on each port Ports	
1	Test Group	Enable	Remove
New		Disable	Add

6. A list of serial ports is displayed. Select the serial ports to add to the port group. If **Login on each port** is enabled, then a login will be performed for all selected ports.



Port group configuration - 1

/ serial / serial_config / portgrp / 1

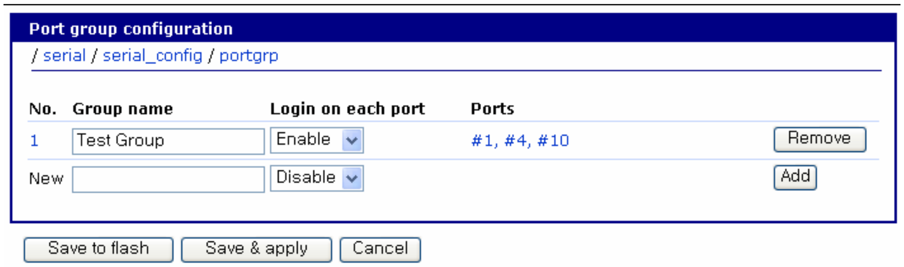
Group name: Test Group

Login on each port: Enable

Ports :

☑ Port Title #1	□ Port Title #2	□ Port Title #3	☑ Port Title #4
□ Port Title #5	□ Port Title #6	□ Port Title #7	□ Port Title #8
□ Port Title #9	☑ Port Title #10	□ Port Title #11	□ Port Title #12
□ Port Title #13	□ Port Title #14	□ Port Title #15	□ Port Title #16
□ Port Title #17	□ Port Title #18	□ Port Title #19	□ Port Title #20
□ Port Title #21	□ Port Title #22	□ Port Title #23	□ Port Title #24
□ Port Title #25	□ Port Title #26	□ Port Title #27	□ Port Title #28
□ Port Title #29	□ Port Title #30	□ Port Title #31	□ Port Title #32
□ Port Title #33	□ Port Title #34	□ Port Title #35	□ Port Title #36
□ Port Title #37	□ Port Title #38	□ Port Title #39	□ Port Title #40
□ Port Title #41	□ Port Title #42	□ Port Title #43	□ Port Title #44
□ Port Title #45	□ Port Title #46	□ Port Title #47	□ Port Title #48

After adding the serial ports to the group, they are listed on the **Port group configuration** page in the **Ports** column:

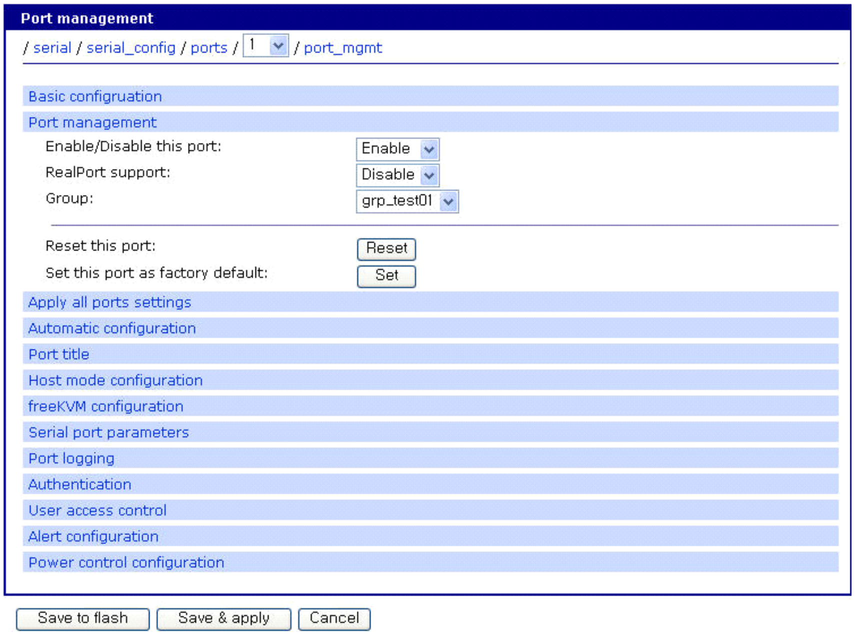


Port group configuration

/ serial / serial_config / portgrp

No.	Group name	Login on each port	Ports
1	Test Group	Enable	#1, #4, #10
New		Disable	

7. After port groups are defined, ports can be assigned to groups on the **Port management** page. Click the **Port management** link. In the **Group** setting, select the appropriate group from the pull-down menu.



Port management

/ serial / serial_config / ports / 1 / port_mgmt

Port management

Enable/Disable this port: Enable

RealPort support: Disable

Group: grp_test01

Manage port groups from the Port Menu

Once a port group is created and ports added to it, the Port Escape Menu displays an additional command, **g**. (See "Port Escape Menu" on page 23 for more details on accessing and using the Port Escape Menu.)

```
Port Menu:

 b      send break
 l      show last 100 lines of log buffer
 a      send message to port user
 g      port group 'Test Group'


 x      close current connection to port
```

To display the Port Group menu, enter **g**:

```
<Port Group 'Test Group'>
 c      send command to all ports
 s      switch to a port
 l      show last 100 lines of log buffer
```

To send commands to all ports in the same group, enter **c**.

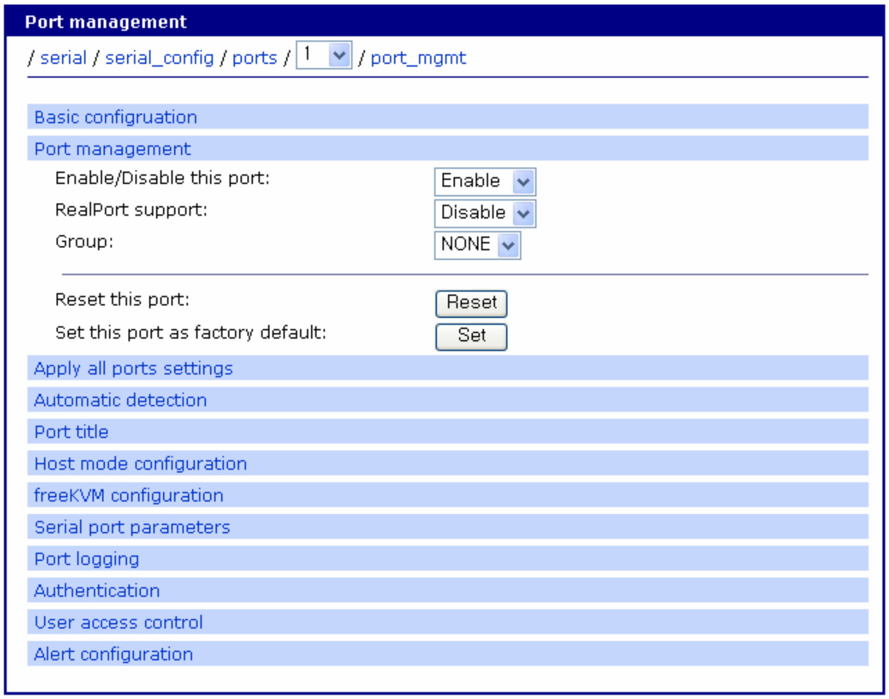
To access any port in a group, enter **s**.

To check the last 100 lines of the log buffer, enter **l**. Make sure that port logging is enabled to check last 100 lines of log buffer (see "Configure Port Logging" on page 57). For example:

```
<Port Group 'Test Group'>
 c      send command to all ports
 s      switch to a port
 l      show last 100 lines of log buffer
 Select a port to connect
 ( [*]1 4 10  )
 -----> 1

>>> Log buffer is empty !

 continue...
```

Advanced Port Configuration Settings

To display and configure more detailed serial port settings, click the Advanced configuration link. The advanced port configuration settings are displayed:



Port management

/ serial / serial_config / ports / 1 / port_mgmt

Basic configruation

Port management

Enable/Disable this port: Enable

RealPort support: Disable

Group: NONE

Reset this port: Reset

Set this port as factory default: Set

Apply all ports settings

Automatic detection

Port title

Host mode configuration

freeKVM configuration

Serial port parameters

Port logging

Authentication

User access control

Alert configuration

This topic covers groups of settings that are not otherwise accessible from the Basic configuration settings; that is:

- Advanced automatic detection settings
- Advanced host mode settings
- Advanced serial port parameters
- Port logging
- Authentication
- User Access control
- Alert configuration

Advanced Automatic Detection Settings

The advanced automatic detection settings allow configuring the rules and execution of the automatic detection feature in more detail than on the Basic settings.

Note: If any settings on this page are changed from their default values for Active or Passive automatic detection, the next time you navigate to the **Basic configuration** page, the **Automatic detection** setting will have changed to **Custom**.

Advanced **Automatic detection** settings include:

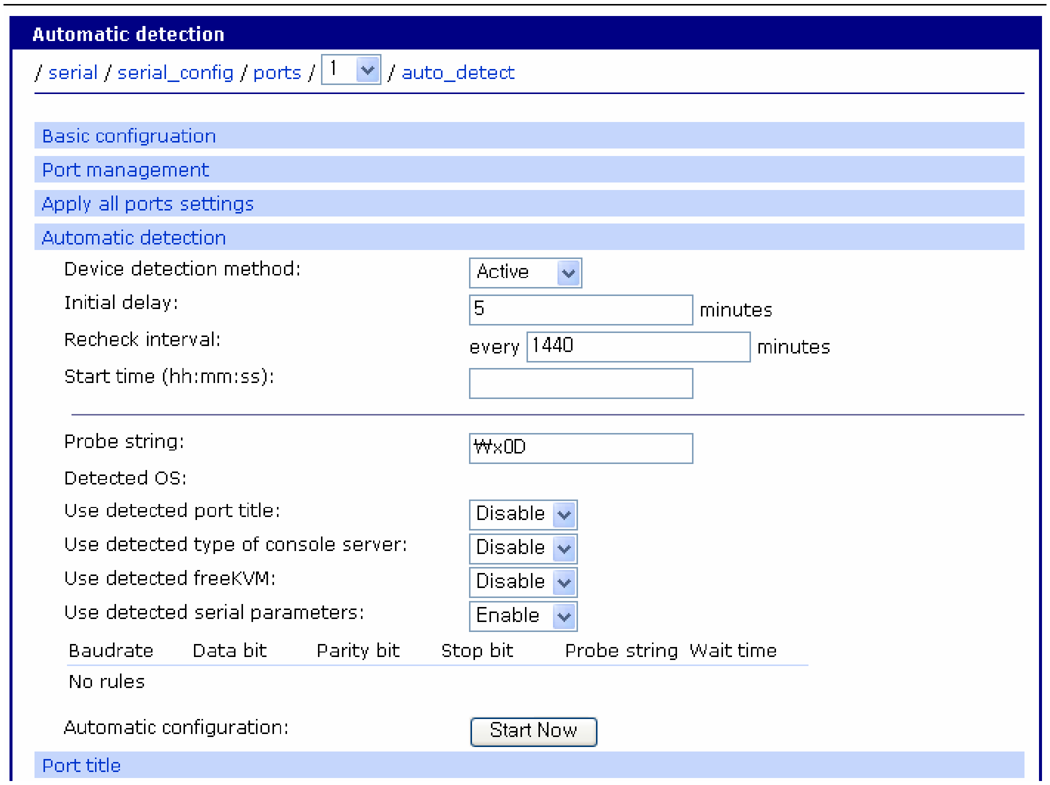
- **Device detection method**: Sets the automatic detection method to **Active** or **Passive**, or turns automatic detection **Off**.
- **Initial delay**: The time which the initial attempt at automatic detection is delayed before starting. For Active automatic detection, the serial parameter detection starts immediately regardless of this value. The default is 5 minutes.
- **Recheck interval**: The time interval between automatic detection attempts. This value must be greater than the value of the Initial delay. The default is every 1440 minutes.
- **Start time**: Sets the start time of the first automatic-detection recheck. This value is not a specific time of day, but rather the time elapsed after the device is detected.
- **Probe string**: An ASCII string sent to the device to detect the operating system and host name in use for the device, when automatic detection is enabled set to the **Active** state. To include special characters in the probe string, see page 96. If the automatic detection state is **Passive**, scripts are run instead of sending a probe string; see page 96.
- **Detected OS**: When the operating system for the device connected to the serial port is detected, it is displayed in this field.
- **Use detected port title**: If this option is enabled, the **Port title** will be set automatically by the rules defined in the scripts **/tmp/cnf/bin/active_detect** or **/tmp/cnf/bin/passive_detect** script. See page 96 for information about these scripts.
- **Port naming rule**: The naming convention for the port when the device is detected. The default naming convention is **OS.HOSTNAME$.port$#$**. This convention can be modified as needed.
- **Use detected type of console server**: If this option is enabled, the Passport will detect the type of console and set the **Type of console server** parameter to **MS SAC console** or **Other** automatically. The default is **Enable**.

- **Use detected freeKVM**: If enabled, the Digi Passport unit detects the IP address of the server connected to the serial port automatically and sets parameters related with freeKVM configuration, such as the IP address and client program. If the connected console is MS SAC, the IP address is detected through the MS SAC console directly. If the connected console is not MS SAC, the IP address is detected through the DNS server using the detected hostname. The default is **Enable**.

  To get the correct automatic freeKVM configuration, before starting automatic detection, go to **Network > IP configuration** and configure the DNS server settings. The DNS settings have the IP address and hostname information for the servers connected to the serial port of the the Digi Passport unit. Also, if the connected console is MS SAC, the settings **Windows RDP standard connection**, **Windows RDP console connection** and **Radmin** will be set to client programs for freeKVM. If the connected console is not MS SAC, the settings **VNC** and **XManager** will be set as the client programs for freeKVM. See "Configure and Use freeKVM" on page 168 for more information.

- **Use detected serial parameters** and the port automatic detection list, if defined: This setting and parameters are displayed only if the **Device detection method** is set to **Active**. Once this option is enabled, the **Port automatic detection** list is displayed just below the option. The Digi Passport unit will detect the serial parameters of the server connected to the serial port automatically. If no port automatic detection list has been created, the text **No rules** is displayed below the parameter labels, as shown on the following screen. The factory default is **Enable** and empty port automatic detection list.

  To create or change port automatic detection list of serial parameters, go to **Serial port > Port automatic detection configuration > Port automatic detection list**.



Automatic detection

/ serial / serial_config / ports / 1 / auto_detect

Basic configruation

Port management

Apply all ports settings

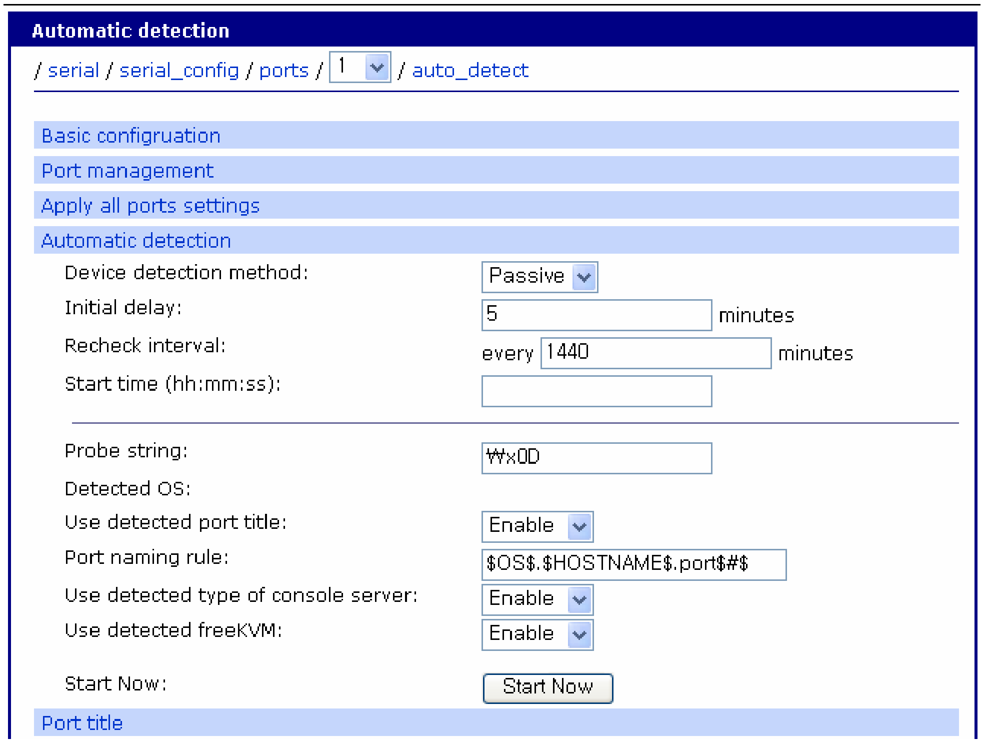
Automatic detection

Device detection method:	Active
Initial delay:	5 minutes
Recheck interval:	every 1440 minutes
Start time (hh:mm:ss):	
Probe string:	₩x0D
Detected OS:	
Use detected port title:	Disable
Use detected type of console server:	Disable
Use detected freeKVM:	Disable
Use detected serial parameters:	Enable

Baudrate	Data bit	Parity bit	Stop bit	Probe string	Wait time
No rules					

Automatic configuration: Start Now

Port title



Automatic detection

/ serial / serial_config / ports / 1 / auto_detect

Basic configruation

Port management

Apply all ports settings

Automatic detection

Device detection method:	Passive
Initial delay:	5 minutes
Recheck interval:	every 1440 minutes
Start time (hh:mm:ss):	
Probe string:	₩x0D
Detected OS:	
Use detected port title:	Enable
Port naming rule:	OS.$HOSTNAME$.port$#$
Use detected type of console server:	Enable
Use detected freeKVM:	Enable

Start Now: Start Now

Port title

Including special characters in probe strings

To include special characters in the probe string, such as carriage returns, line feeds, and escape characters, specify them as hexadecimal values. For example, here are hexadecimal equivalents for several common special characters:

- Carriage return (CR): \x0d
- Line feed (LF): \x0a
- Escape (ESC): \x1B

Here are examples of the output generated by several probe strings:

Probe 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>

For Passive automatic detection, scripts used instead of probe strings

If the automatic detection state is set to **Passive**, no probe string is sent to the attached device but the port buffer is analyzed.

Instead, the script **/tmp/cnf/bin/passive_detect** is executed and the results are saved to these files: **/var/run/HostnamePortxx** and **/var/run/OSPortxx**.

The commands to parse the system response are user-customizable. Therefore, 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.

After executing the **saveconf** command, execute the **applyconf** command for the change to take effect immediately.

Advanced Host Mode Settings

Advanced **Host mode configuration** settings allow for viewing and modifying the configuration settings that define the communication between serial devices and remote hosts in use with the Digi Passport unit in more detail than the Basic configuration settings. Advanced host mode configuration settings include:

- **Host mode**: Console server mode, terminal server mode, dial-in modem mode, and dial-in terminal server mode.
- **Type of console server**: Select **MS SAC** to provide a graphic user interface to the Windows Server 2003 Special Administration Console (see "Microsoft SAC Support" on page 163). In all other cases, select **Other**.
- **Rackable Systems Mgmt Card**: Enable to use Rackable Management card.
- **Service processor:** If the attached device uses one of the following supported protocols, select that here. For a full description of service processor configuration, see "Service Processors" on page 120.
- **Enable/Disable assigned IP address**: 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, allowing a Telnet connection directly to the serial port using an IP address, without specifying a TCP port.
- **Listening TCP port**: The TCP network port used when connecting directly to the port using Telnet or SSH.
- **Protocol**: The communications protocol used for communications between serial devices and host: **SSH**, **RawTCP**, or **Telnet**. When **RawTCP** is selected, several more options are displayed in the Serial port parameters to enable and specify the and set the inter-character timeout.
- **Inactivity timeout**: The time set for inactivity to trigger an action, in seconds. 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.
- **Web applet size**: Defines the default size of the Terminal Console Web Applet in rows and columns.

freeKVM Configuration

freeKVM configuration is a link to the settings for configuring the freeKVM feature. See "Configure and Use freeKVM" on page 168 for more information.

Advanced Serial Port Parameters

Serial port parameters is a link to the serial parameters for a port. When attaching a serial device to the Digi Passport unit’s serial port, the serial port parameters must match. The serial ports by default are enabled, allowing full access to the port.

Advanced serial port parameters include:

- **UART type:** The type of UART (Universal Asynchronous Receiver/ Transmitter) in use to control the the Digi Passport unit’s interface to its attached serial devices. On this page, UART type is read-only.
- **Baudrate**: The baud rate for the serial port in bits per second. The default is **9600**.
- **Data bit:** The bits that make up the transmitted data over the serial port. Usually, seven or eight data bits are grouped together. Each group of data bits in a transmission is preceded by a start bit and followed by an optional parity bit as well as one or more stop bits. The default is 8 bits.
- **Parity bit**: The parity used with transmitted data over the serial port:
  - **None**: No parity.
  - **Even**: Even parity.
  - **Odd**: Odd parity.

  The default is **none**.
- **Stop bit**: The number of stop bits per character to use on the serial port. The value used here must match the setting on the device connected to this port. Use 1 or 2 stop bits. The default is **1 bit**.
- **Flow control**: The kind of flow control is used on the serial port.
  - **None**: No flow control.
  - **XON/XOFF:** Software flow control (Xon/Xoff)
  - **Hardware**: Hardware flow control (RTS/CTS).

  The default is **None**.
- **DTR option**: DTR (Data Terminal Ready) 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 default is **High when open**. When the host mode is configured for dial-in modem or dial-in terminal server mode, the DTR setting cannot be set by a user.
- **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.

Special Use of Serial Port when Data is Processed in Chunks

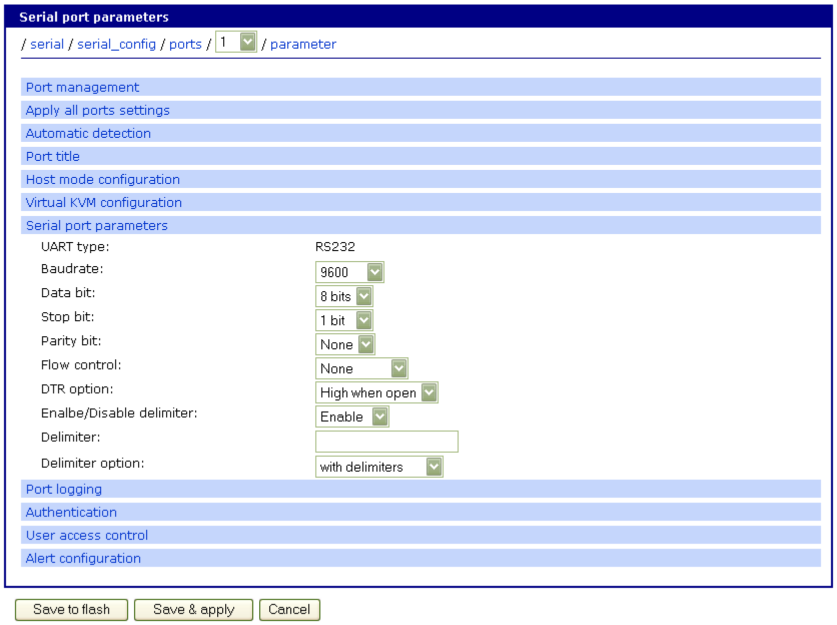
Some applications are written to process only chunks of data rather than continuous streams of data. The Digi Passport unit supports *chunking*, or holding back data from the serial device to the application on the network until it detects a delimiter - at which point it sends the data to the application.

To configure a port for this mode:

1. Open a web connection to the Digi Passport unit.
2. Select **Serial Port > Configuration**.
3. Select **All ports** to configure.
4. Select **Host Mode configuration**.
5. Under **Protocol**, select **RawTCP**.
6. Click **Save & apply**.
7. Select **Serial port parameters**.
8. Configure the delimiter and supporting settings.
   - **Enable/Disable delimiter**: Allows delimiter to function.
   - **Delimiter**: The sequence that should be received before forwarding the data to the application
   - **Delimiter option**: Specifies handling of the delimiter in data sent to the application:

     with delimiters: Sends the delimiter as part of the data to the application.

     without delimiters: Removes the delimiter before sending the data to the application.
   - **Inter character time-out timeout**: Timeout, in milliseconds.If no delimiter is detected the data is delivered after this timeout has elapsed. The range is 1-10000.



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

Remote port parameters

If remote ports are defined and a remote port is selected,
Remote port parameters is a link to the settings for configuring remote ports. See "Configure Remote Ports" on page 102 for descriptions of these settings.

Port Logging

Port logging is a link to the settings for configuring writing of port event data to a log file. See "Configure Port Logging" on page 57.

Authentication

Authentication is a link to the settings for configuring any user authentication desired or required for users accessing ports. See "Configure Authentication Methods for Port Access" on page 151 for more information.

User Access Control

User access control is a link to the settings for configuring user access rights to ports. See "Configure User Access Control" on page 142 for more information.

Alert Configuration

Alert configuration is a link to the settings for configuring system alerts and notifications. See "Alerts and Notifications" on page 107.

Reset Ports

The Digi Passport unit allows restarting all processes associated with a port and to disconnect all sessions.

To reset an individual port:

1. Click **Serial port** > **Configuration** > ***port number***.
2. For **Reset this port**, click **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**.

Configure Remote Ports

The Digi Passport unit supports RemotePorts™. RemotePorts are any type of port that can be accessed using Telnet, SSH, or Raw TCP protocols, or through service processors (for detailed information on configuring service processors, see "Service Processors" on page 120). This type of remote-port access includes connections to Digi PortServer Terminal Servers, Sun ALOM ports, and iLo, DRAC, and IPMI management ports. The RemotePorts 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

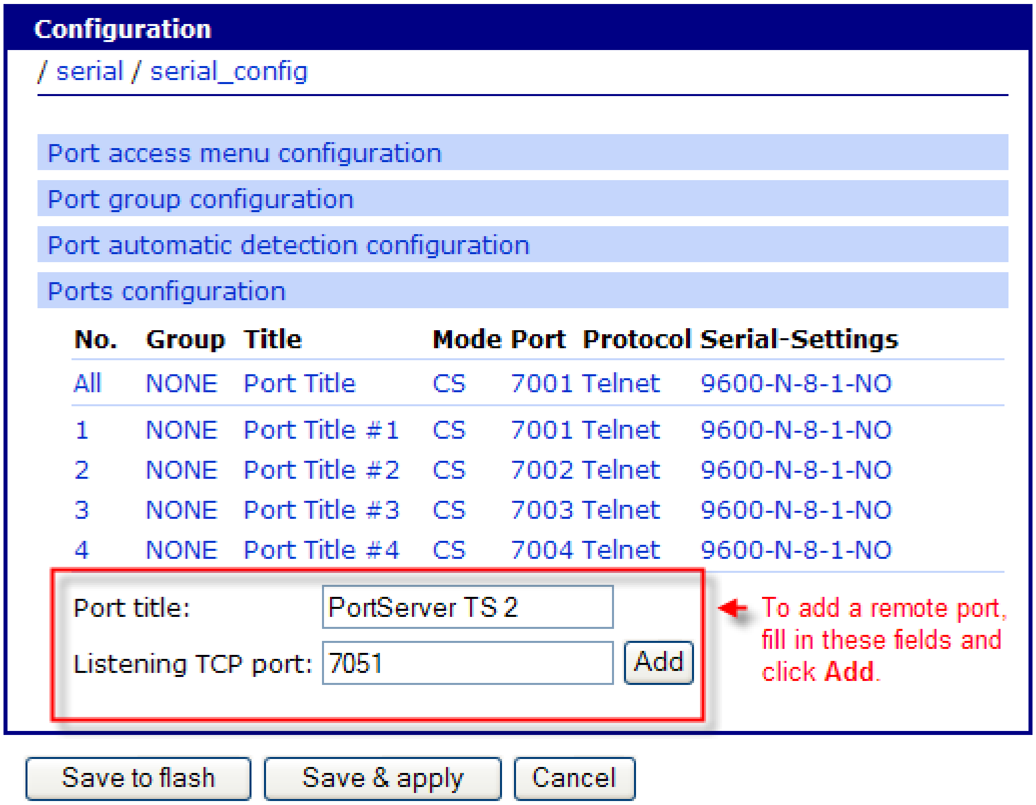
Remote ports also provide the additional capabilities described in the sections on Port Logging, Alerts and Notifications, and freeKVM.

There are two modes of using remote ports: basic and advanced. Basic use is for ports accessed through Telnet, SSH, and Raw TCP protocols, and is covered in this chapter. Advanced use is for ports accessed through service processors. Configuration of remote ports for service processors is covered in "Service Processors" on page 120.

Add and Configure a Remote Port

To configure a remote port:

1. Access the Digi Passport unit's web interface
2. Under the **Serial Port** heading, click **Configuration**.
3. On the **Ports configuration** page, go to the **Port title** and **Listening TCP** port settings at the bottom of the page, as shown below. Enter the **Port title** and the **Listening TCP port** to use, and click **Add**.



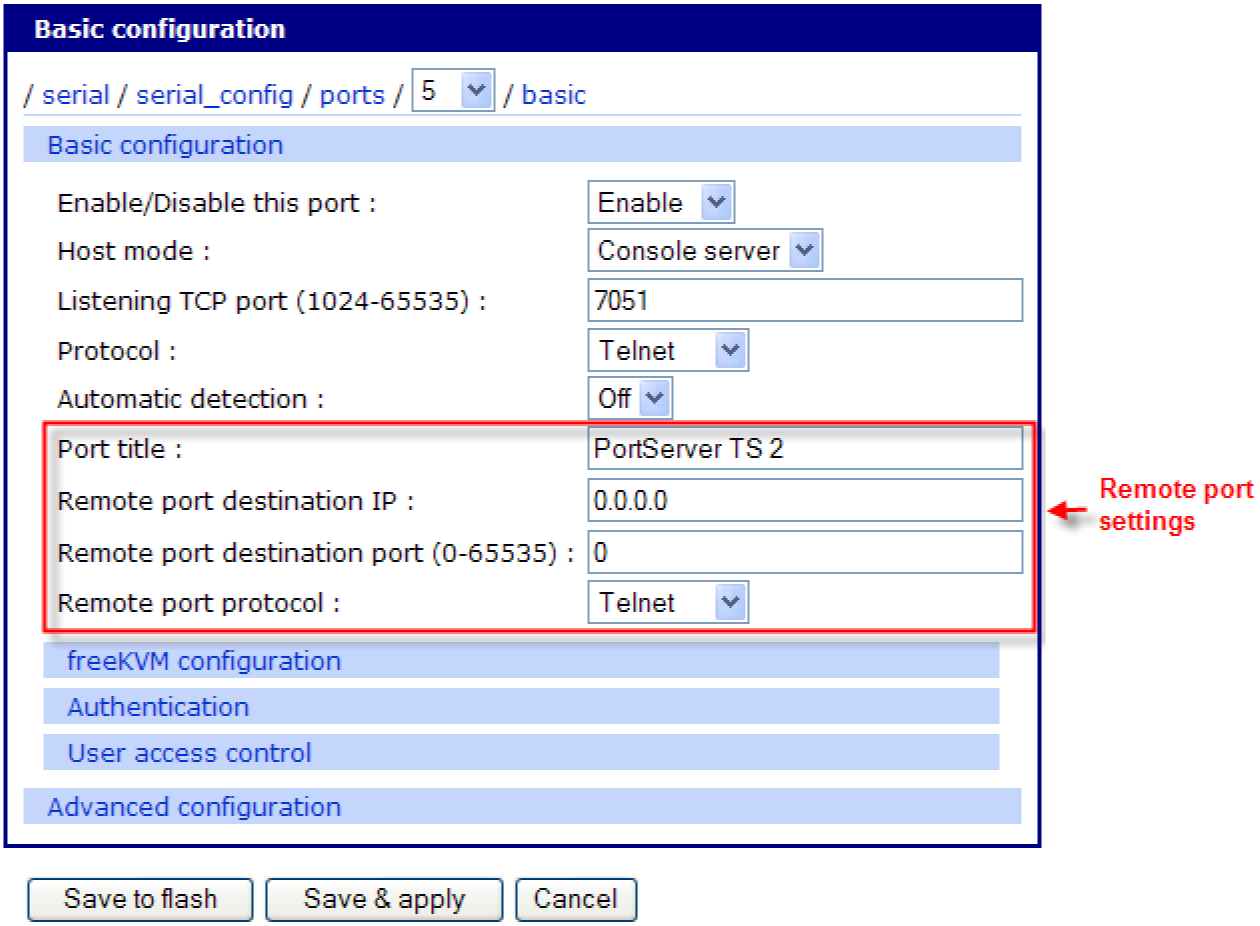
No.	Group	Title	Mode	Port	Protocol	Serial-Settings
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO
1	NONE	Port Title #1	CS	7001	Telnet	9600-N-8-1-NO
2	NONE	Port Title #2	CS	7002	Telnet	9600-N-8-1-NO
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO
4	NONE	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO

Port title: PortServer TS 2

Listening TCP port: 7051

To add a remote port, fill in these fields and click **Add**.

4. The serial port **Basic configuration** page is displayed, with several additional parameters for configuring remote ports.



Basic configuration

/ serial / serial_config / ports / 5 / basic

Basic configuration

Enable/Disable this port : Enable

Host mode : Console server

Listening TCP port (1024-65535) : 7051

Protocol : Telnet

Automatic detection : Off

Port title : PortServer TS 2

Remote port destination IP : 0.0.0.0

Remote port destination port (0-65535) : 0

Remote port protocol : Telnet

Remote port settings

Enter the remote port settings:

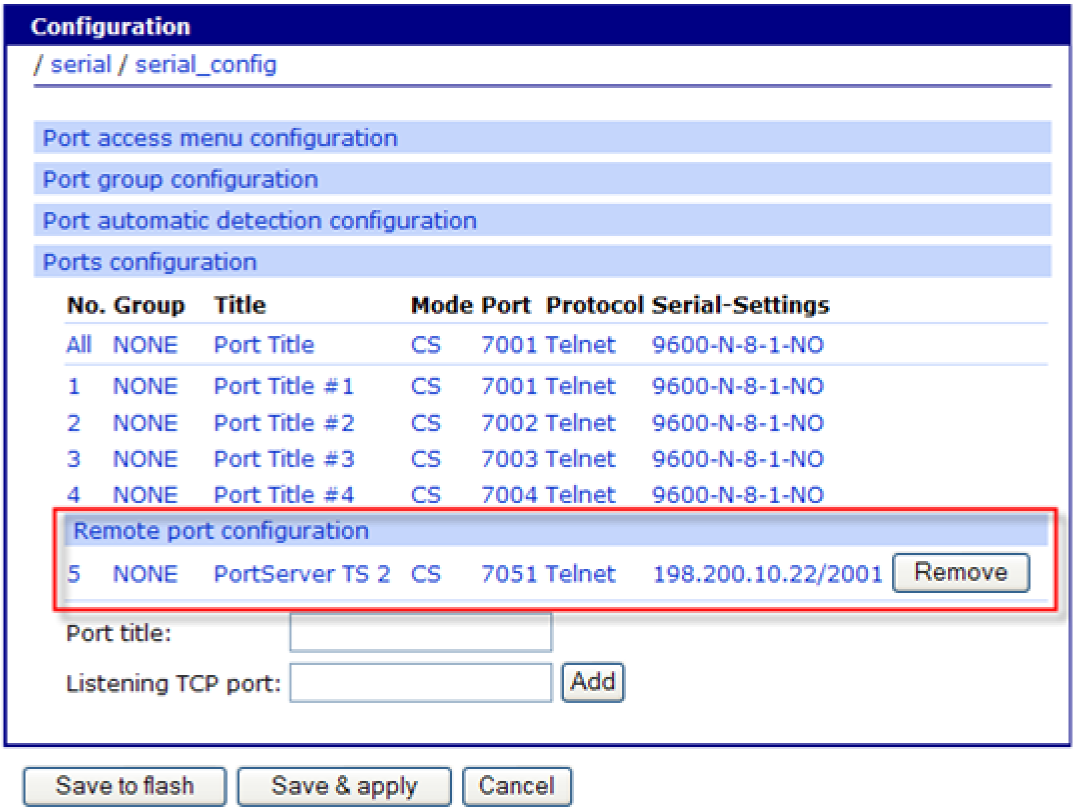
- **Remote port destination IP**: The IP address of the remote device.
- **Remote port destination port (0-65535)**: The port number on the remote device.
- **Remote port protocol**: The communications protocol used to communicate with the remote device: **Telnet**, **SSH**, or **RawTCP**.

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

To use a Digi PortServer TS 2 as a remote device, configure as follows: IP address as assigned, IP port 2001 for port 1 or 2002 for port 2, and Telnet or port 2501/ 2502 when using SSH as protocol.

5. Click **Save & apply** to confirm selections. A confirmation message is displayed.

The remote port will now be displayed in the list of ports on the **Ports configuration** page, under the heading **Remote port configuration**. For example:



No.	Group	Title	Mode	Port	Protocol	Serial-Settings
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO
1	NONE	Port Title #1	CS	7001	Telnet	9600-N-8-1-NO
2	NONE	Port Title #2	CS	7002	Telnet	9600-N-8-1-NO
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO
4	NONE	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO
Remote port configuration						
5	NONE	PortServer TS 2	CS	7051	Telnet	198.200.10.22/2001

Port title:

Listening TCP port:

Remote port added to port list

Advanced Remote Port Parameters

When remote ports are defined and selected, the Advanced port configuration settings has a link, Remote port parameters. Parameters include:

- **Destination IP address**: The IP address of the remote device.
- **Destination port (0-65535)**: The port number on the remote device.
- **Protocol**: The communications protocol used to communicate with the remote device: **Telnet**, **SSH**, or **RawTCP**.
- **Allow unattended continuous connection**: **Allow unattended continuous connection**: If enabled, when the connection is lost, it is reestablished automatically. Enabling this setting also enables the **Automatic login** setting and additional login settings. Default is **Disable**.
- **Automatic login**: Specifies whether a login to the remote device is automatically performed. Enabling this setting displays the user login settings. Default is **Disable** (no automatic login).
- **User name**. The user name to be used for the automatic login.
- **Password**: The password to be used for the automatic login. Supply and confirm the password for the specified user.

Access a Remote Port

To connect to a remote port using the web, Telnet or SSH client, 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 to the IP and the port number**. The specific port number is defined on the ’Host mode configuration’ page. For example:

  ```
  telnet 143.191.3.9 7051
  ```

- **SSH to the IP address and port number**. The specific port number is defined on the **Host mode configuration** page.

- **SSH to the IP address and port name**. The specific port number is defined on the **Host mode configuration** page. For example:

  ```
  Ssh user-name:’t=port-title’@ip-Address
  Ssh sunadmin:’t=Switch3level’:@MainDigi
  ```

A remote port can be accessed just like any local port: directly using the port number.

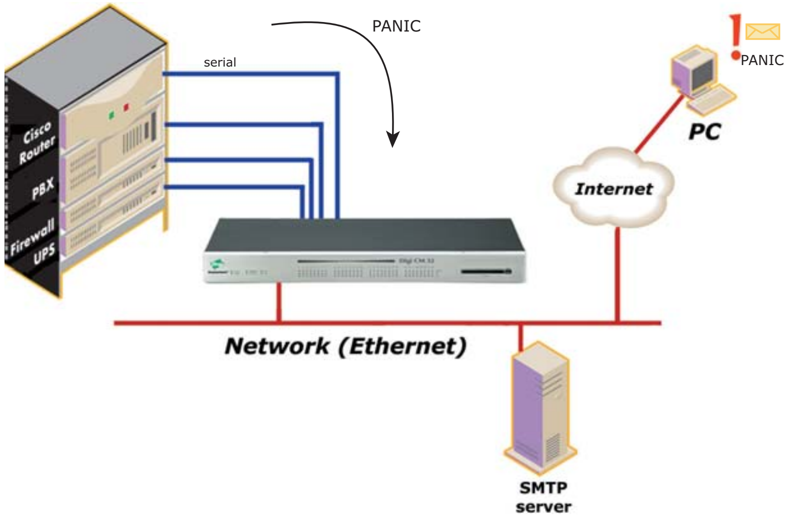
The parameters of the remote port are equivalent to regular serial ports. Enter any additional parameters for the remote and click **Save & apply** or **Apply all changes**.

Chapter 6 Alerts and Notifications

About Alerts and Notifications

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 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.

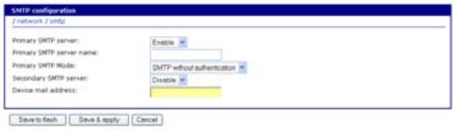


Configure SMTP Alerts

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 SMTP alerts on the Digi Passport unit, do the following:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Network > SMTP configuration**.



SMTP configuration

/ network / smtp

Primary SMTP server: Enable

Primary SMTP server name:

Primary SMTP Mode: SMTP without authentication

Secondary SMTP server: Disable

Device mail address:

3. Specify the SMTP settings as needed.
   - **SMTP server**: Use either the hostname or the IP address.
   - **Device mail address**: The sender’s email address for the log and alarm delivery.
   - **SMTP mode**: The type of SMTP server to use.
   - **Username and password**: Required if using POP before SMTP and SMTP with authentication servers.
4. Click **Save & apply**.

Supported SNMP Traps

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. Supported traps include Authentication, power on, link up, login, NFS, Samba, Power Management, Power Fail and IPMI traps.

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

Setting Additional Traps at the Port Level

Additional traps can be set at the port level. The table shows where the trap is located in the serial port configuration settings in the web interface (in **Serial port** > **Configuration**), the trap name, 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 "Discovering and Configuring the Digi Passport unit" on page 14, 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 are on the Passport CD and at http://www.digi.com/support/ under Digi Passport utilities.

Configure SNMP v1 or v2

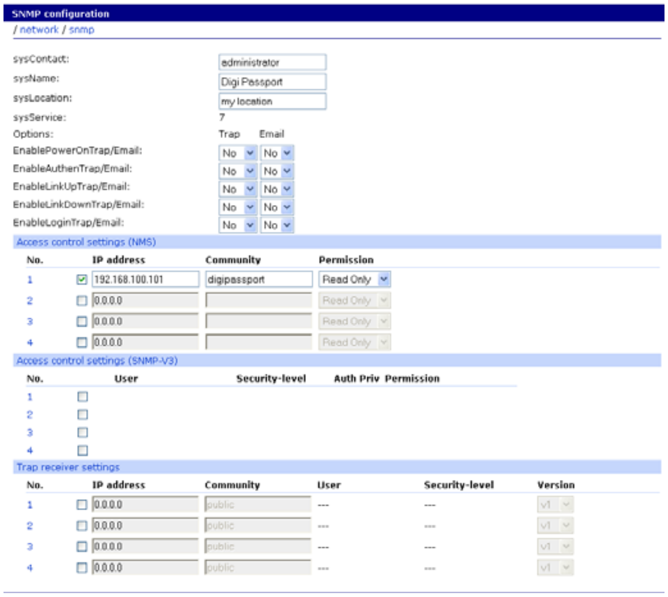
To configure the Digi Passport unit for SNMP do the following:

1. Access the Digi Passport unit’s web interface.
2. Select **Network > SNMP configuration**.
3. In the MIB-II system objects section, enter MIB-II information as needed and enable authentication traps by selecting **Yes** under **EnableAuthenTrap**. Enable other SNMP traps as needed.

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

   - **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; for example, DigiPassport@companyname.com.
   - **sysLocation**: The physical location of the unit, for example, 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**: Whether the SNMP agent generates a trap each time the Digi Passport unit is started.
   - **EnableAuthenTrap**: Whether the SNMP agent process is permitted to generate authentication failure traps.
   - **EnableLinkUpTrap**: Whether the SNMP agent generates a trap each time the network connection comes up.
   - **EnableLinkDownTrap**: Whether the SNMP agent generates a trap each time the network connection goes down.
   - **EnableLoginTrap**: Whether the SNMP agent generates a trap for each login.
4. Enter Access control settings.
   - **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; this value must match the string used in the SNMP software.
   - **Permissions**: The options are Read only or Read/Write.

5. Enter Trap receiver settings.
   - **IP Address**: The IP address of the device receiving the trap alerts.
   - **Community**: The options are public or private; this value must match the string used in the SNMP software.
   - **Version**: The SNMP version, either version 1 or version 2c.



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	☑	192.168.100.101	digipassport	Read Only
2	□	0.0.0.0		Read Only
3	□	0.0.0.0		Read Only
4	□	0.0.0.0		Read Only

Access control settings (SNMP-V3)

No.		User	Security-level	Auth Priv	Permission
1	□				
2	□				
3	□				
4	□				

Trap receiver settings

No.		IP address	Community	User	Security-level	Version
1	□	0.0.0.0	public	---	---	v1
2	□	0.0.0.0	public	---	---	v1
3	□	0.0.0.0	public	---	---	v1
4	□	0.0.0.0	public	---	---	v1

6. Click **Save & apply**.

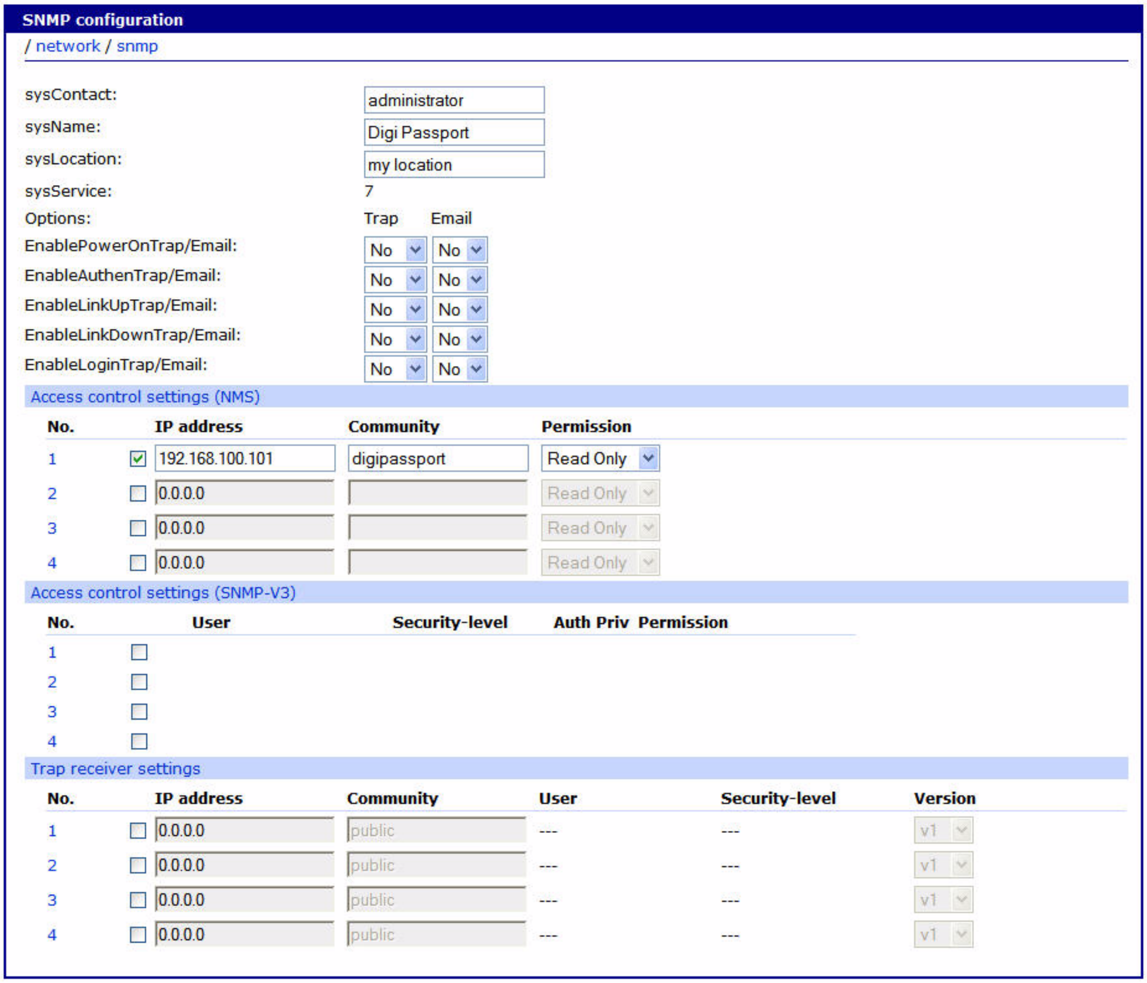
Manage SNMP configuration

The Digi Passport unit's SNMP configuration 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. To configure SNMPv3 access control and SNMPv3 traps, follow these steps.

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	☑	192.168.100.101	digipassport	Read Only
2	□	0.0.0.0		Read Only
3	□	0.0.0.0		Read Only
4	□	0.0.0.0		Read Only

Access control settings (SNMP-V3)

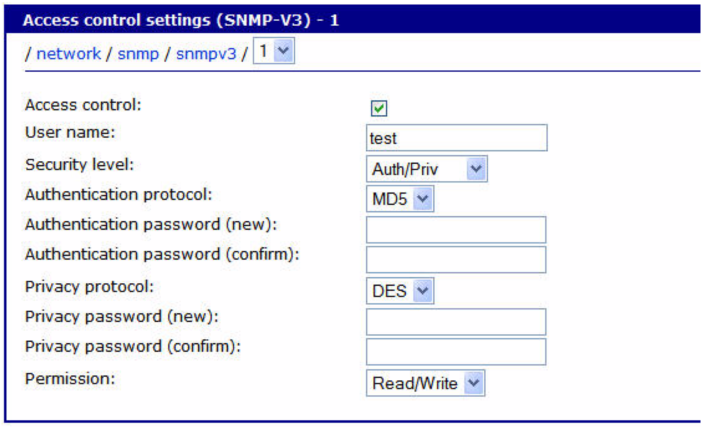
No.		User	Security-level	Auth Priv	Permission
1	□				
2	□				
3	□				
4	□				

Trap receiver settings

No.		IP address	Community	User	Security-level	Version
1	□	0.0.0.0	public	---	---	v1
2	□	0.0.0.0	public	---	---	v1
3	□	0.0.0.0	public	---	---	v1
4	□	0.0.0.0	public	---	---	v1

2. In the **Access control settings (SNMPv3)**, add a user.

3. Select **1**. The **Access control settings (SNMP V3) - 1** page is displayed:



Access control settings (SNMP-V3) - 1

/ network / snmp / snmpv3 / 1

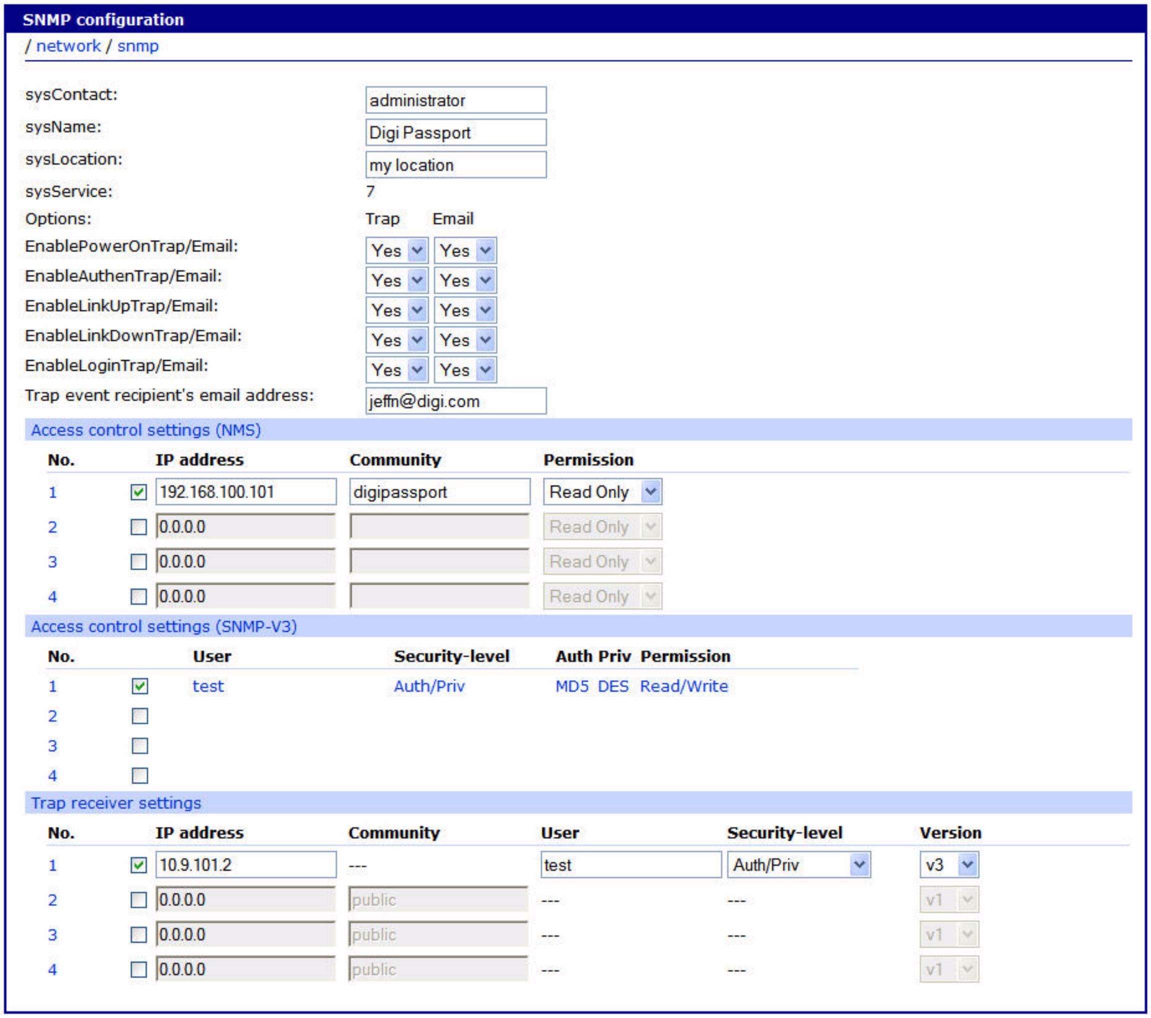
Access control:	☑
User name:	test
Security level:	Auth/Priv
Authentication protocol:	MD5
Authentication password (new):	
Authentication password (confirm):	
Privacy protocol:	DES
Privacy password (new):	
Privacy password (confirm):	
Permission:	Read/Write

Enter settings:

- **User name**: enter the user name that has been set up for SNMPv3 access in the SNMP browser software.
- **Security level**: This setting should match the security level that is configured in the SNMPv3 software.
- **Authentication protocol**: This setting should match the security level that is configured in the SNMPv3 software.
- **Authentication password (new)/(confirm)**: Supply and confirm the **password** for the user. This setting should match the security level that is configured in the SNMPv3 software.
- **Privacy protocol**: This setting should match the security level that is configured in the SNMPv3 software.
- **Privacy password (new)/(confirm)**: Supply and confirm the **privacy password** for the user. This setting should match the security level that is configured in the SNMPv3 software.
- **Permission**: Select the appropriate permission level.

When done, click **Save to flash**.

4. 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@digi.com

Access control settings (NMS)

No.		IP address	Community	Permission
1	☑	192.168.100.101	digipassport	Read Only
2	□	0.0.0.0		Read Only
3	□	0.0.0.0		Read Only
4	□	0.0.0.0		Read Only

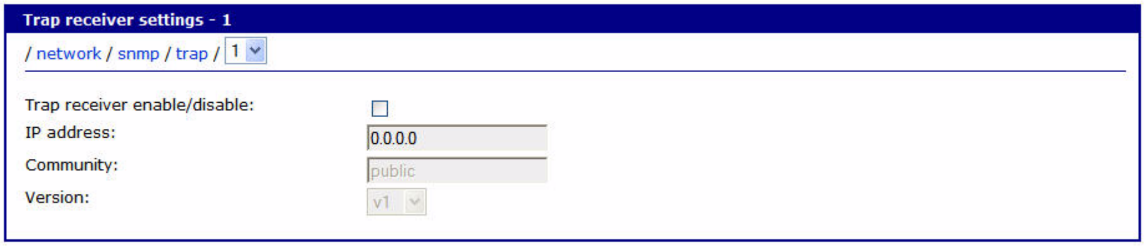
Access control settings (SNMP-V3)

No.		User	Security-level	Auth	Priv	Permission
1	☑	test	Auth/Priv	MD5	DES	Read/Write
2	□					
3	□					
4	□					

Trap receiver settings

No.		IP address	Community	User	Security-level	Version
1	☑	10.9.101.2	---	test	Auth/Priv	v3
2	□	0.0.0.0	public	---	---	v1
3	□	0.0.0.0	public	---	---	v1
4	□	0.0.0.0	public	---	---	v1

5. Configure the **Trap receiver settings**. From the list, select number **1**. The trap receiver settings are displayed.

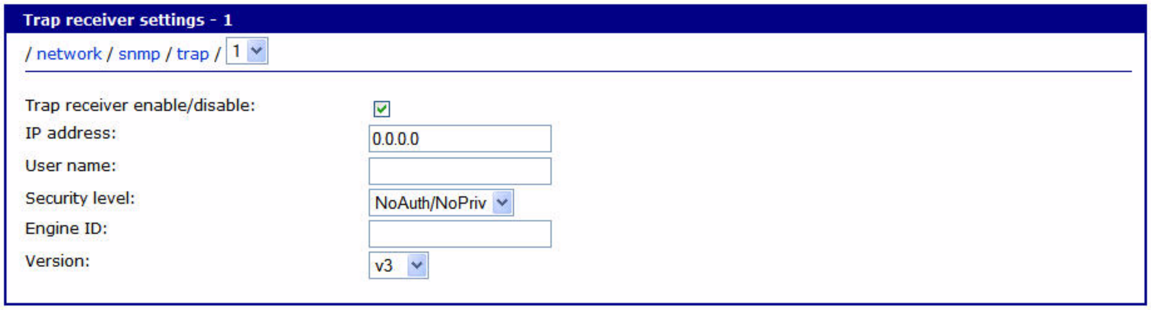


Trap receiver settings - 1

/ network / snmp / trap / 1

Trap receiver enable/disable:	□
IP address:	0.0.0.0
Community:	public
Version:	v1

6. Select the **Trap receiver enable/disable** checkbox, then select **v3** from the **Version** menu. The Trap receiver settings -1 page is displayed:



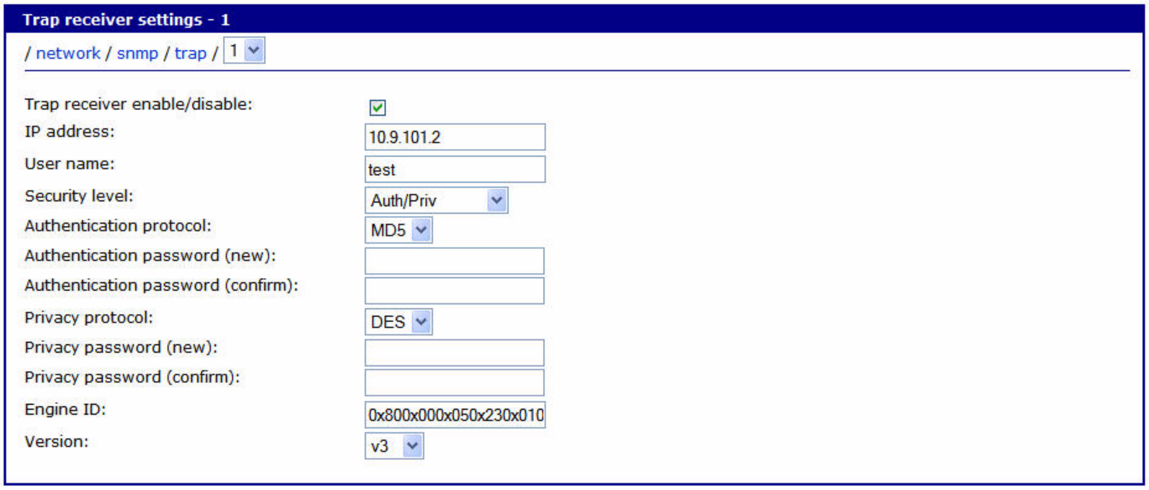
Trap receiver settings - 1

/ network / snmp / trap / 1

Trap receiver enable/disable:	☑
IP address:	0.0.0.0
User name:	
Security level:	NoAuth/NoPriv
Engine ID:	
Version:	v3

Enter settings:

- **IP address**: Enter the IP address of the Trap receiver.
- **User name**: Fill in the **User name**; this value is the same user from the SNMPv3 software.
- Select the **Security level.** Additional security level settings are displayed, shown below. Use the same steps as in the **Access control settings** section for the Authentication and Privacy Protocols and their passwords.
- **Engine ID**: This value is supplied by the SNMPv3 software. Delete the spaces from the original engine ID.



Trap receiver settings - 1

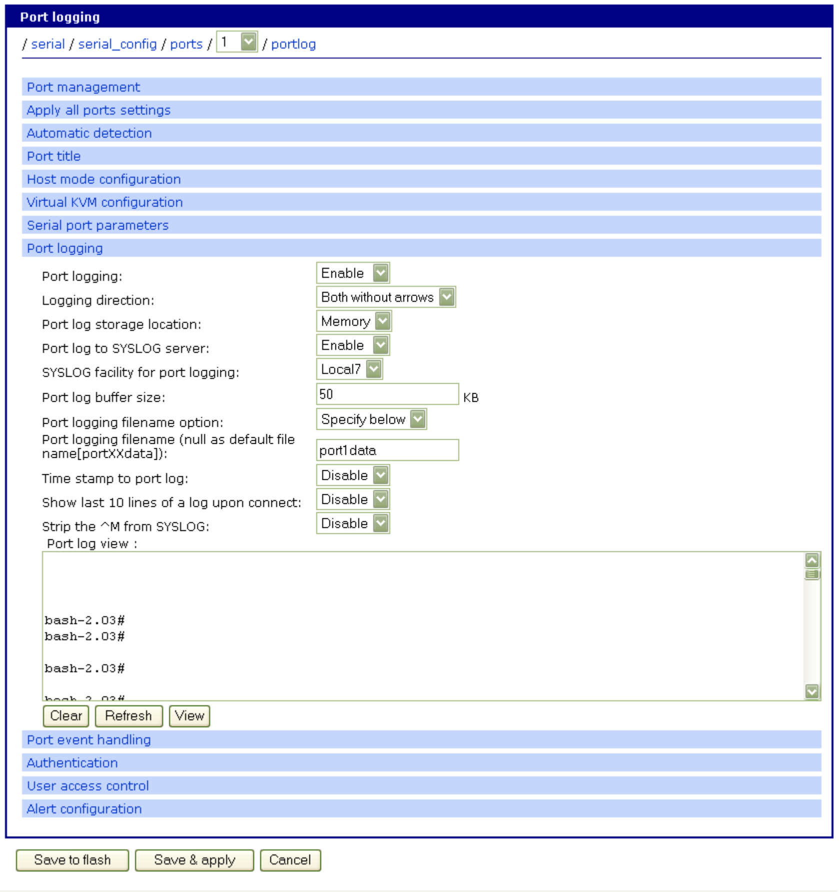
/ network / snmp / trap / 1

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

Configure Port Event Handling

Once an SMTP or SNMP server has been configured, it can be used to send port-related alerts and notifications. To configure a port for port event handling, follow these steps. This procedure assumes that SMTP is configured first. If not, see "Configure SMTP Alerts" on page 108.

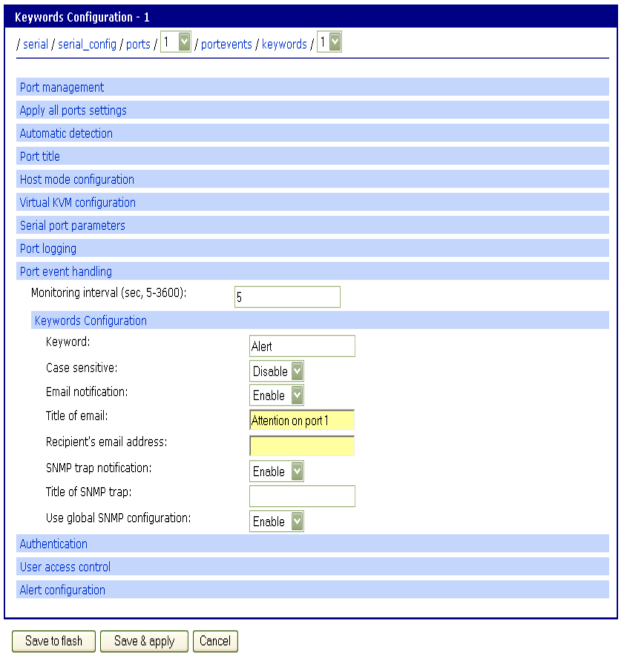
1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port** > **Configuration**.
3. Select a port to configure, then **Advanced configuration > Port logging**. The port logging settings are displayed.
4. For **Port logging**, select **Enable**.
5. For **Logging direction**, select which port events should be included in the log and how they are displayed:
   - **Server output**: Output from the server only.
   - **User input**: User input only.
   - **Both with arrows**: Both server output and user input, with arrows to indicate direction.
   - **Both without arrows**: Both server output and user input, without direction indicator arrows.
6. Click **Save & apply**.



Port logging: Enable
Logging direction: Both without arrows
Port log storage location: Memory
Port log to SYSLOG server: Enable
SYSLOG facility for port logging: Local7
Port log buffer size: 50 KB
Port logging filename option: Specify below
Port logging filename (null as default file name[portXXdata]): port1data
Time stamp to port log: Disable
Show last 10 lines of a log upon connect: Disable
Strip the ^M from SYSLOG: Disable
Port log view :

```
bash-2.03#
bash-2.03#

bash-2.03#

bash-2.03#
```

7. Select **Port event handling**. The port event handling settings are displayed.



Monitoring interval (sec, 5-3600): 5

Keyword: Alert

Case sensitive: Disable

Email notification: Enable

Title of email: Attention on port 1

Recipient's email address:

SNMP trap notification: Enable

Title of SNMP trap:

Use global SNMP configuration: Enable

- Select an action and enter the keyword for the port event handling. The keyword is any text string that will trigger an alert when it traverses the serial port.
- Enable **Email notification**.
- Enter the title of the Email (subject line).
- Enable or Disable **Case sensitive**.
- Enter the Email recipient’s address.
- Enable SNMP trap notification.
- Enter the title of the trap.
- Select either to use the global SNMP settings by enabling **Use global SNMP configuration** or specify special settings for this port.
- Enter the IP address of the trap receiver.
- Enter the SNMP community.
- Select the version.

8. Complete configuration and click **Save & apply**.

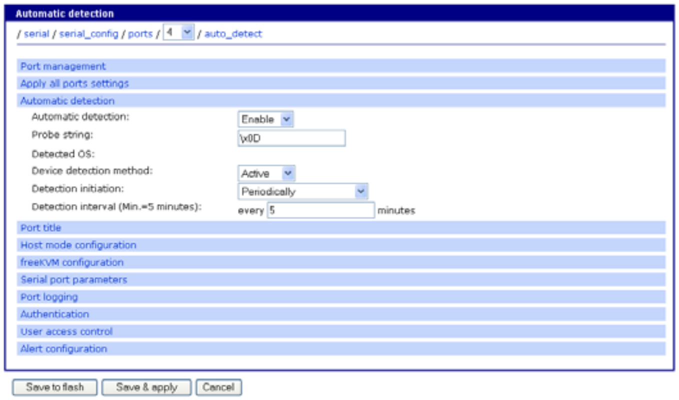
Configure Alerts for Automatic Device Recognition (ADR)

Before configuring the alerts for Automatic Device Recognition (ADR), make sure the sure the port for ADR has been configured, as described in "Configure Automatic Detection" on page 77.

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Under the **Serial Port** heading, Click **Configuration**.
3. Select **All > Alert Configuration** or ***port number* > Alert Configuration**.
4. Follow the Email Alert steps to configure the email alert or follow the SMTP Notification to configure SMTP.

Email Alert	SMTP Notification
1. Enable **Email Alert for active detection.** 2. Enter the **Title** of email. 3. Enter **Name** and **email address** where the email should be sent.	1. **Enable Active detection trap**. 2. Configure the trap receiver by one of the following ways: - Select **Use global SNMP configuration**. **OR** - Enter the IP address of the trap receiver, the SNMP trap community and select the version.

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



Automatic detection

/ serial / serial_config / ports / 4 / auto_detect

Automatic detection: Enable

Probe string: \x0D

Detected OS:

Device detection method: Active

Detection initiation: Periodically

Detection interval (Min.=5 minutes): every 5 minutes

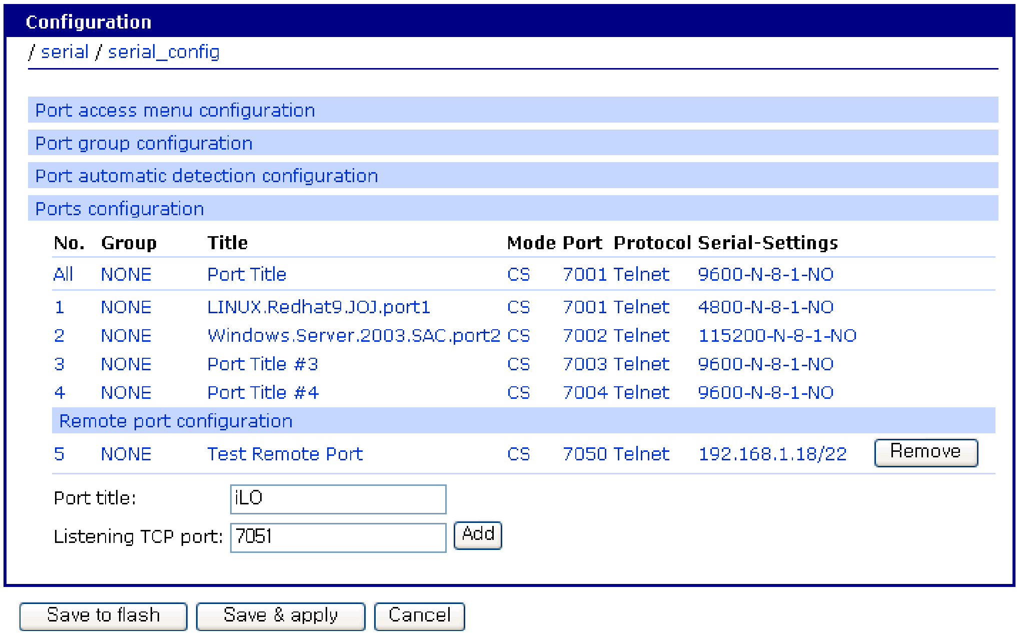
Chapter 7 Service Processors

Digi Passport provides support for various service processors, such as Intelligent Platform Management Interface (IPMI), Integrated Lights Out (iLO), Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP), and Dell Remote Access Controller (DRAC). Service processors are configured through the remote port. This chapter describes configuring and using service processors.

Configuring a Service Processor

To configure a service processor:

1. Add a remote port, as instructed in "Add and Configure a Remote Port" on page 103.



Configuration

/ serial / serial_config

Port access menu configuration

Port group configuration

Port automatic detection configuration

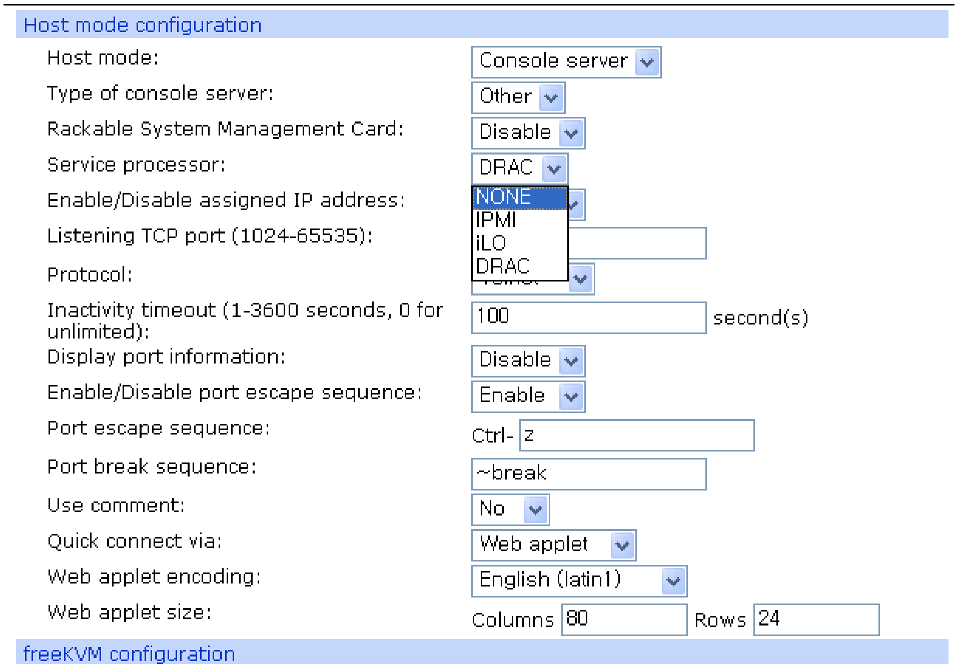
Ports configuration

No.	Group	Title	Mode	Port	Protocol	Serial-Settings	
All	NONE	Port Title	CS	7001	Telnet	9600-N-8-1-NO	
1	NONE	LINUX.Redhat9.JOJ.port1	CS	7001	Telnet	4800-N-8-1-NO	
2	NONE	Windows.Server.2003.SAC.port2	CS	7002	Telnet	115200-N-8-1-NO	
3	NONE	Port Title #3	CS	7003	Telnet	9600-N-8-1-NO	
4	NONE	Port Title #4	CS	7004	Telnet	9600-N-8-1-NO	
Remote port configuration							
5	NONE	Test Remote Port	CS	7050	Telnet	192.168.1.18/22	Remove

Port title: iLO

Listening TCP port: 7051

2. On the **Host mode configuration** page, use the **Service processor** setting to select the service processor. Available options are **NONE**, **IPMI**, **iLO**, and **DRAC**.



Host mode configuration

Host mode:	Console server
Type of console server:	Other
Rackable System Management Card:	Disable
Service processor:	DRAC
Enable/Disable assigned IP address:	
Listening TCP port (1024-65535):	
Protocol:	
Inactivity timeout (1-3600 seconds, 0 for unlimited):	100 second(s)
Display port information:	Disable
Enable/Disable port escape sequence:	Enable
Port escape sequence:	Ctrl- z
Port break sequence:	~break
Use comment:	No
Quick connect via:	Web applet
Web applet encoding:	English (latin1)
Web applet size:	Columns 80 Rows 24

freeKVM configuration

Intelligent Platform Management Interface (IPMI)

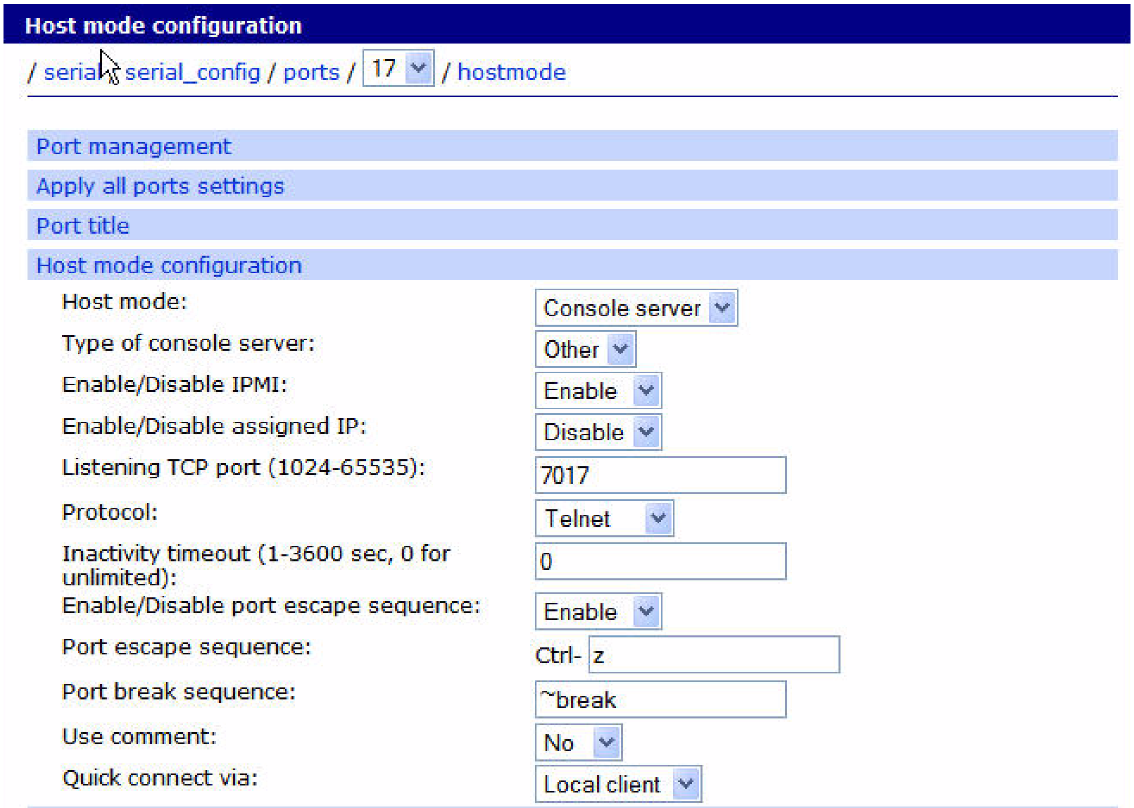
Intelligent Platform Management Interface (IPMI) is a specification for the equipment that monitors the physical environment and condition of a computer hardware server. The specification is intended to cover the regulation of temperature, voltage and power, and to ensure the proper operation of the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

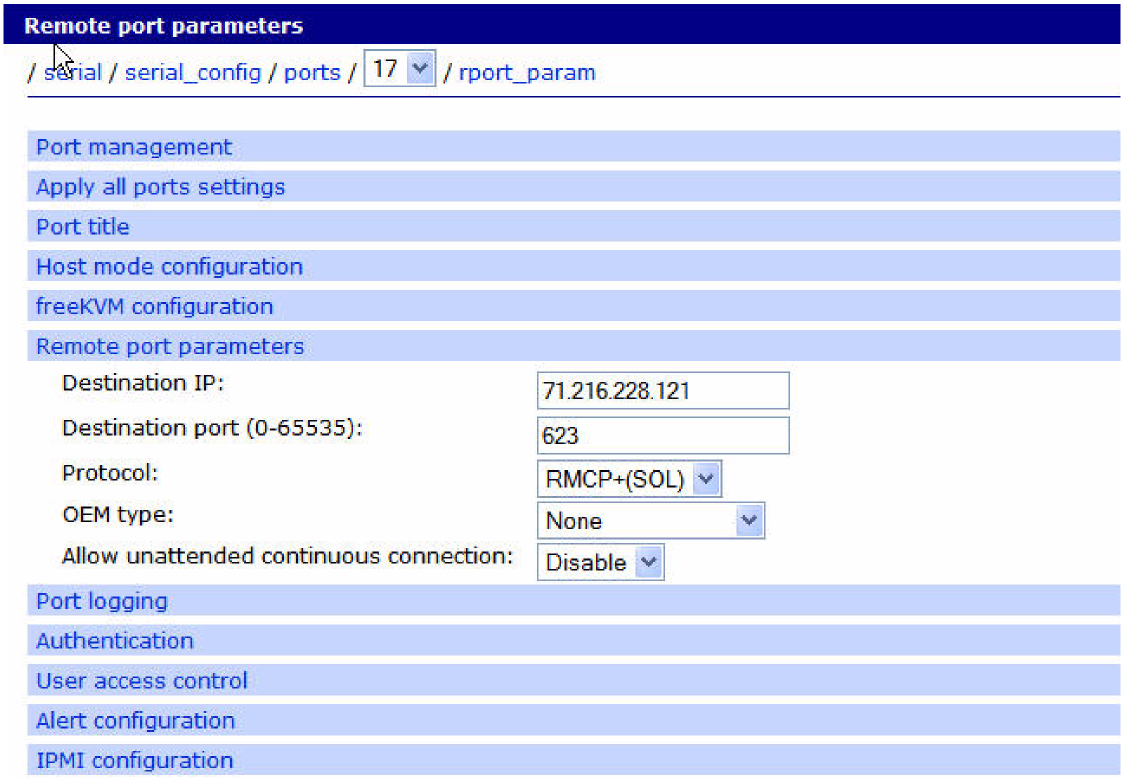
Configure IPMI

1. In the Web interface, select **Serial port configuration**, then select the port to configure for IPMI.
2. From the menu, select **Host mode configuration**. In the host mode configuration settings, for the Enable/Disable IPMI setting, select **Enable**. Save to flash.



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. Select **Remote port parameters** from the main configuration page. The remote port settings are displayed.



Remote port parameters

/ serial / serial_config / ports / 17 / rport_param

Destination IP: 71.216.228.121

Destination port (0-65535): 623

Protocol: RMCP+(SOL)

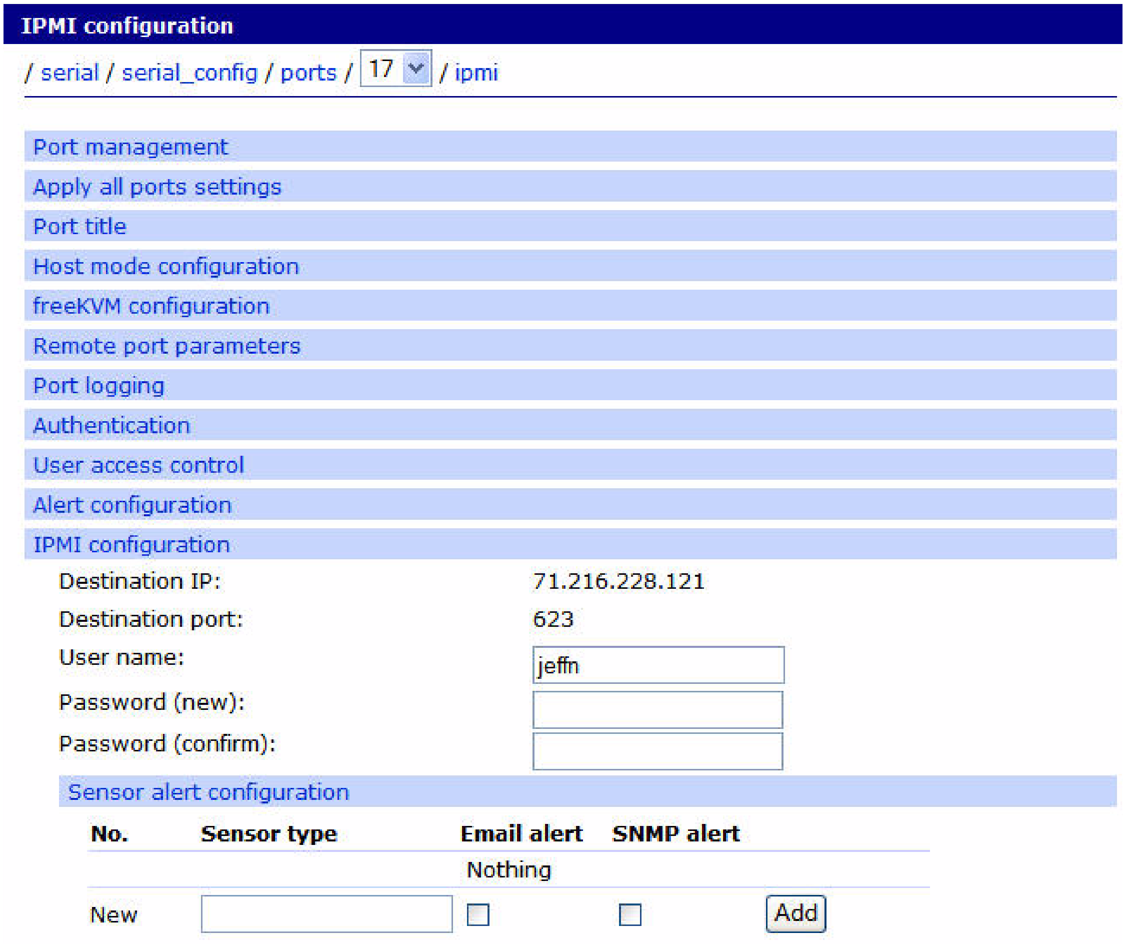
OEM type: None

Allow unattended continuous connection: Disable

- **Destination IP**: The address of the server to monitor. Generally, this is the address assigned to the BMC (Baseboard Management Controller).
- **Destination port**. Normally, 623 is the port used for IPMI, but this may vary on individual servers.
- **Protocol**: Select the protocol. RMCP+ is the protocol used for SOL.
- **OEM type**: Set to **None** in most cases. Use **Intel IPMI 2.0 BMC** only if the server has an actual Intel 2.0 BMC.

When done, click **Save to Flash**.

4. From the main configuration page, select **IPMI Configuration**. The IPMI configuration settings are displayed.



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):	

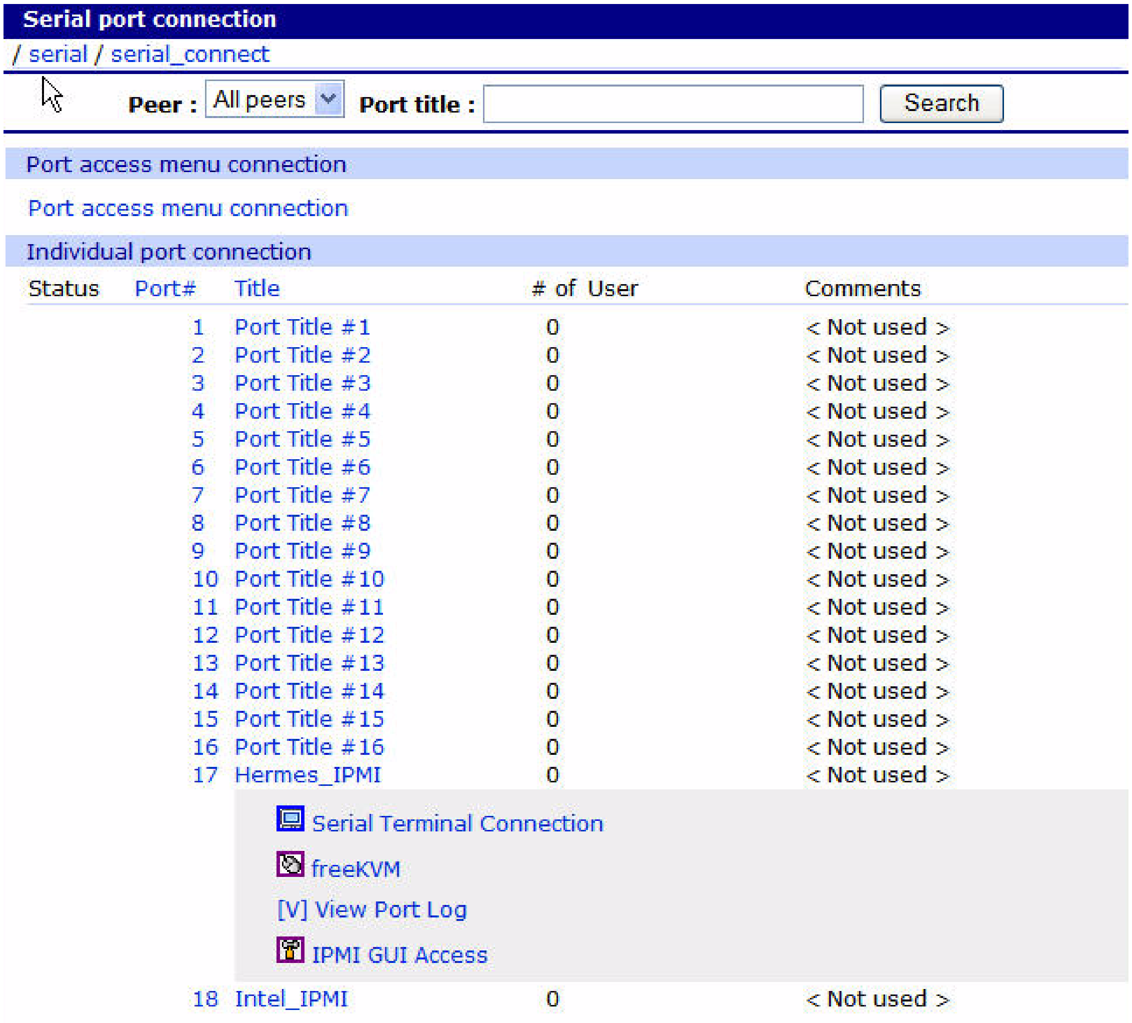
Sensor alert configuration

No.	Sensor type	Email alert	SNMP alert	
		Nothing		
New		□	□	Add

- **Destination IP**: The address of the server to monitor. Generally, this is the address assigned to the BMC (Baseboard Management Controller). For a remote port, this value is supplied from the "Remote port parameters".
- **Destination port**: normally, 623 is the port used for IPMI, but this value may vary on individual servers. For a remote port, this value is supplied from the "Remote port parameters".
- **User name**: The user name for a user configured on the server that can access the BMC.
- **Password**: Supply and confirm the password for the user.
- **Sensor alert configuration** creates create a list of sensors on the server from which notifications are sent.

Connect to a Server via IPMI

1. To connect to a server via the IPMI GUI, select the serial port connection page.
2. Select the serial port configured for IPMI. This menu is displayed:



Serial port connection

/ serial / serial_connect

Peer : All peers Port title :

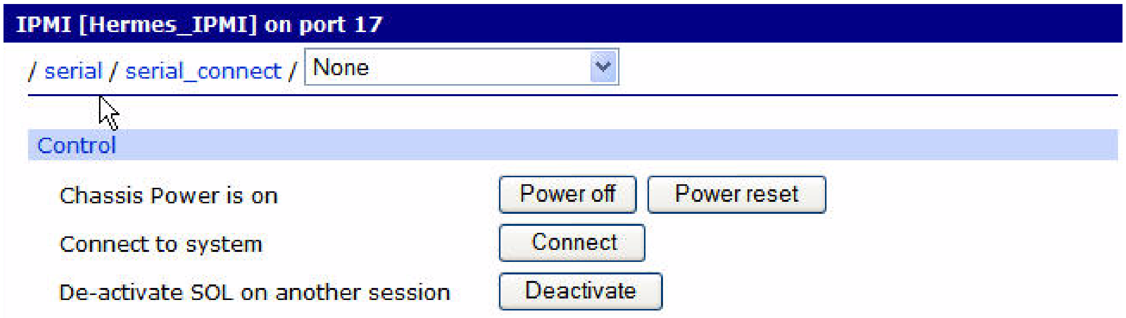
Port access menu connection

Port access menu connection

Individual port connection

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	Hermes_IPMI	0	< Not used >
		Serial Terminal Connection freeKVM [V] View Port Log IPMI GUI Access		
	18	Intel_IPMI	0	< Not used >

3. Select **IPMI GUI Access**. This connect to the server via IPMI. This page is displayed:



IPMI [Hermes_IPMI] on port 17

/ serial / serial_connect / None

Control

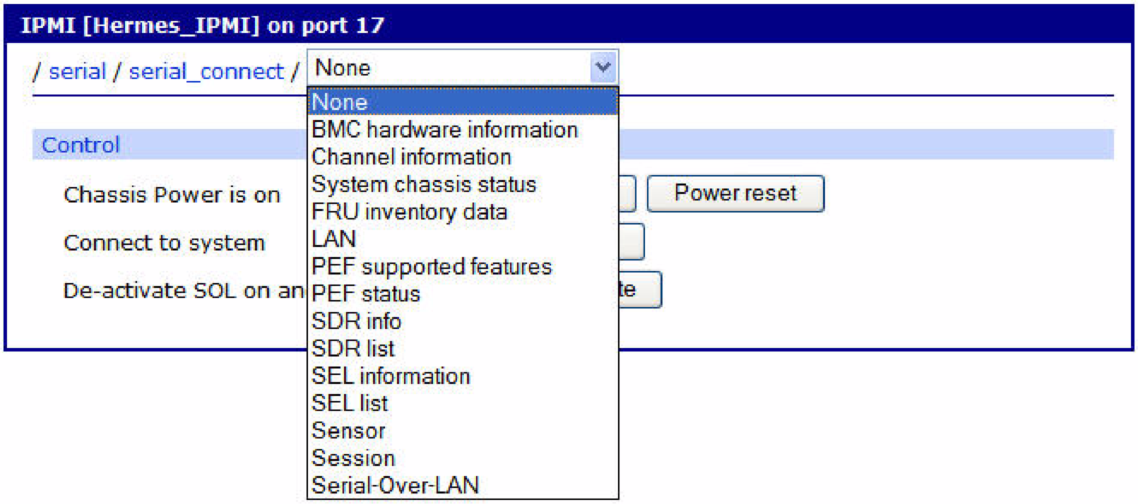
Chassis Power is on

Connect to system

De-activate SOL on another session

4. From this page, select the BMC statistics to monitor, power-cycle the server, or make an SOL connection to the server's console port.

5. Select the information to monitor from the pulldown menu.


IPMI [Hermes_IPMI] on port 17

/ serial / serial_connect / None

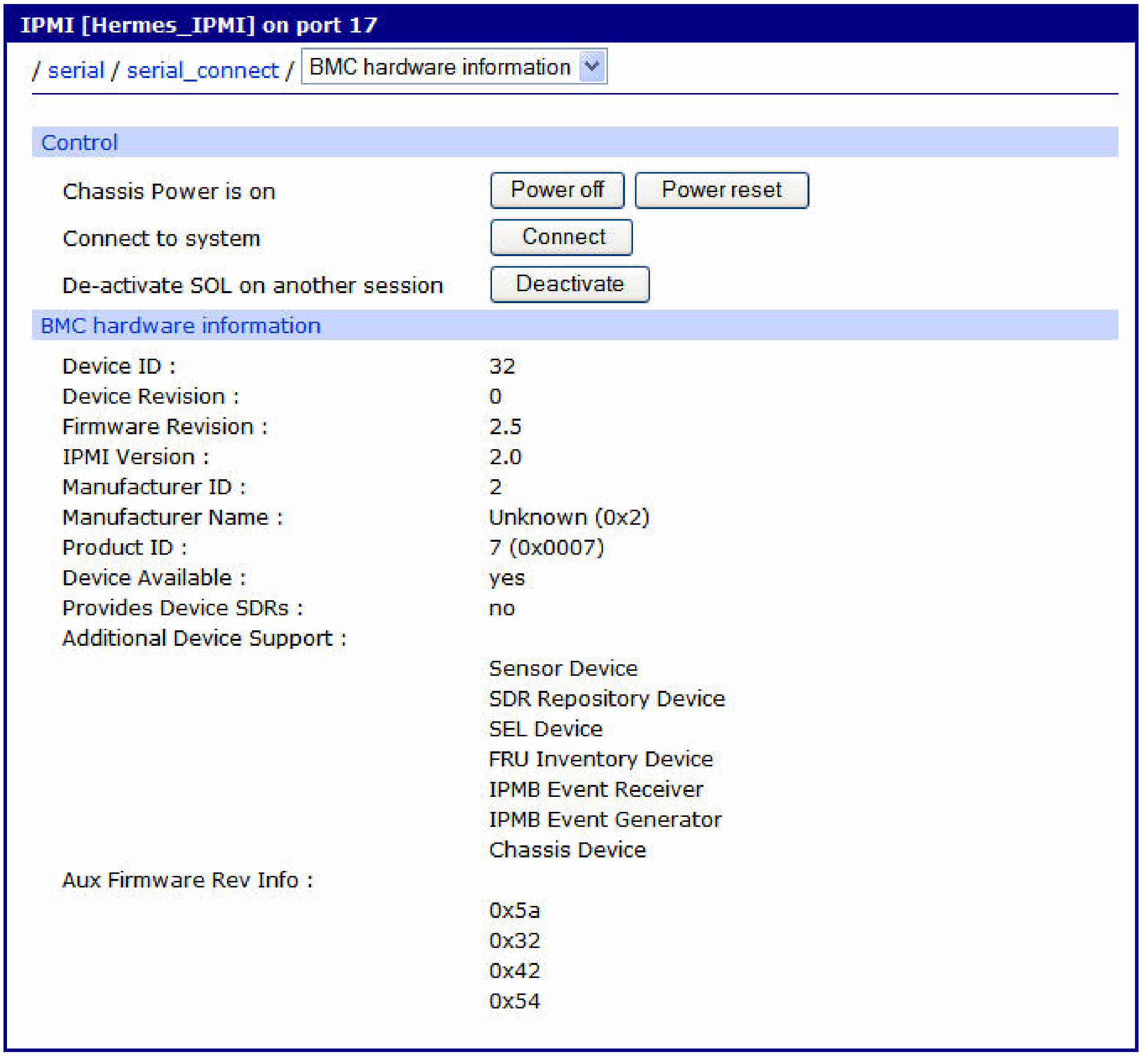
Control

Chassis Power is on

Connect to system

De-activate SOL on an

For example, if BMC hardware information is selected, this page is displayed. The information displayed varies between server manufacturers.


IPMI [Hermes_IPMI] on port 17

/ serial / serial_connect / BMC hardware information

Control

Chassis Power is on

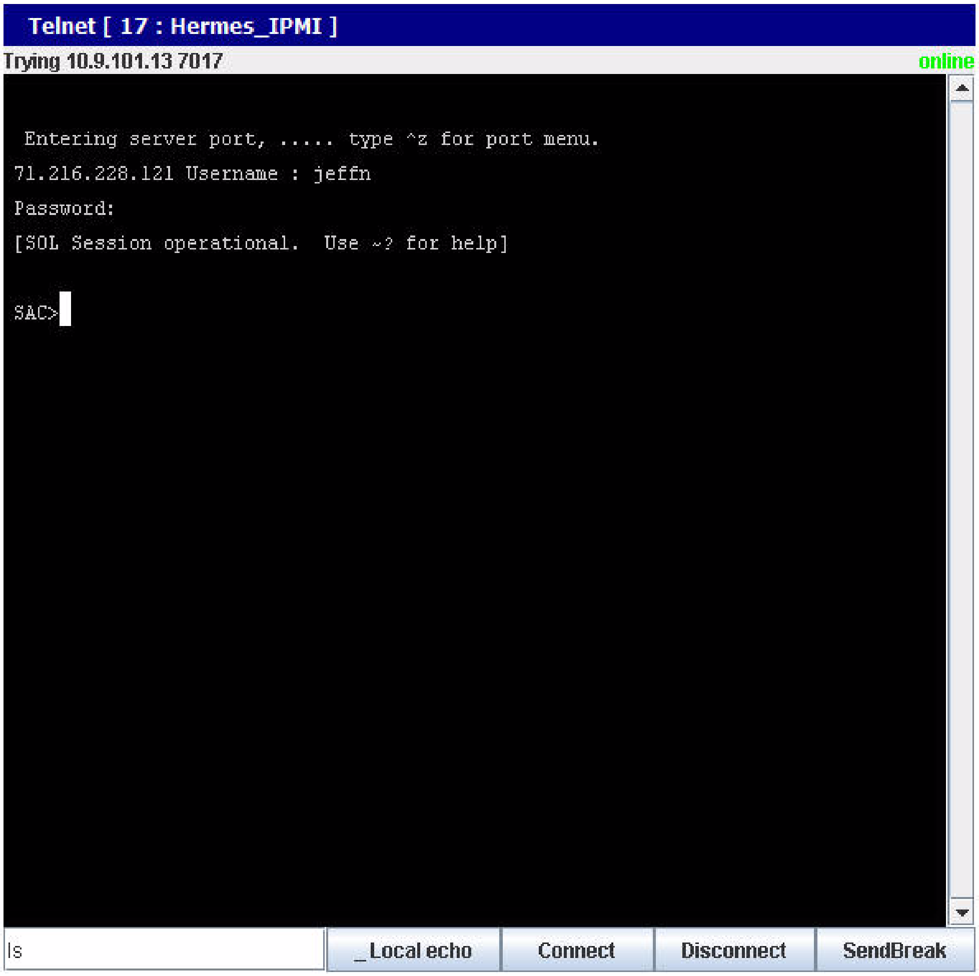
Connect to system

De-activate SOL on another session

BMC hardware information

Device ID :	32
Device Revision :	0
Firmware Revision :	2.5
IPMI Version :	2.0
Manufacturer ID :	2
Manufacturer Name :	Unknown (0x2)
Product ID :	7 (0x0007)
Device Available :	yes
Provides Device SDRs :	no
Additional Device Support :	
	Sensor Device SDR Repository Device SEL Device FRU Inventory Device IPMB Event Receiver IPMB Event Generator Chassis Device
Aux Firmware Rev Info :	
	0x5a 0x32 0x42 0x54

6. To make an SOL connection to the servers console port, click the **Connect** button. The resulting window is displayed. The example shown below is a console connection to a Windows 2003 servers SAC port.



```
 Entering server port, ..... type ^z for port menu.
71.216.228.121 Username : jeffn
Password:
[SOL Session operational.  Use ~? for help]

SAC>
```

SMASH CLP

Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) is a command/response specification transmitted and received over a text message-based transport protocol. It was developed and released by DMTF (Distributed Management Task Force). SMASH CLP addresses the end user requirement for a common command line syntax, allowing systems offered by different vendors to be managed in similar ways. Digi Passport supports SMASH CLP for iLO2 and DRAC5. Instructions for configuring SMASH CLP are integrated into the sections for iLO and DRAC.

Integrated Lights Out (iLO, iLO2)

Integrated Lights Out (iLO and iLO2) is an HP 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.

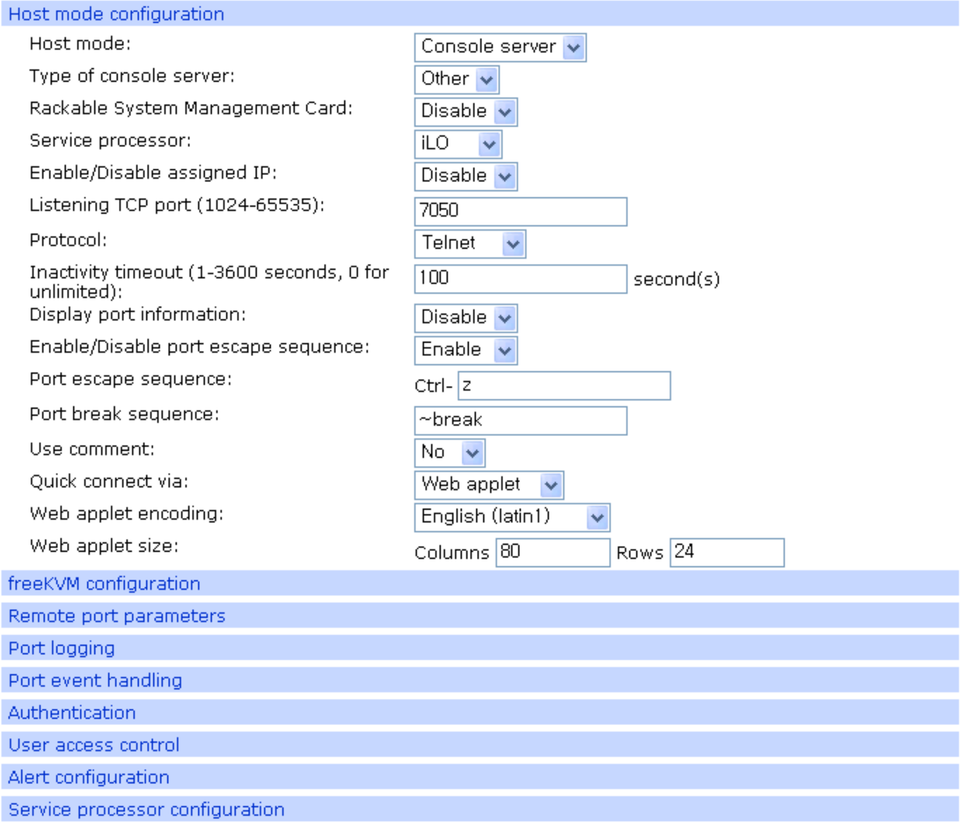
iLO works with hardware servers regardless of the operating platform or other software they may run. iLO allows an administrator to manage multiple servers from a single location by means of a user-friendly interface. Critical system events for each server can be logged. Settings for each basic input/output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

iLO2 adds advanced digital video redirection to the specification.

Configure iLO and SMASH CLP on a Remote Port

To configure iLO including SOL (Serial Over LAN) and SMASH CLP on a remote port, follow these steps.

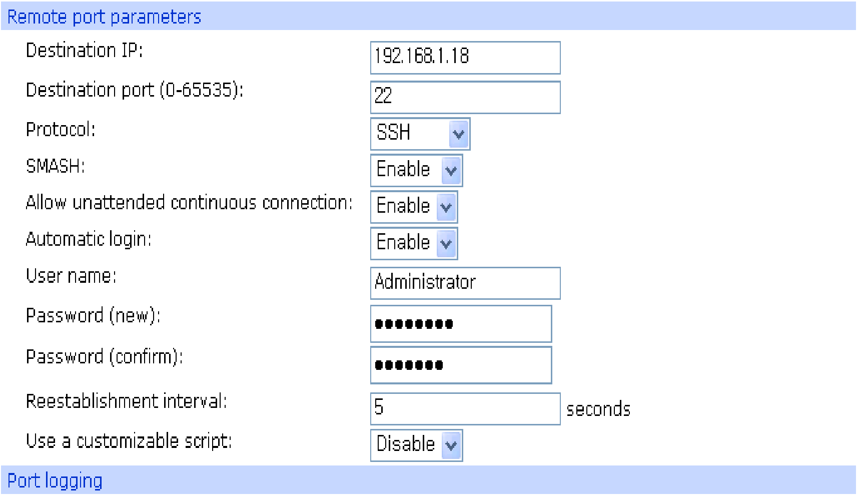
1. In the Web interface, select **Serial port configuration** and select the port to configure for iLO.
2. From the menu, select **Advanced configuration.**
3. In the next screen displayed, select **Host mode configuration**.
4. From the pulldown menu for **Service processor**, select **iLO.** Click **Save to flash**.



Host mode configuration

Host mode:	Console server
Type of console server:	Other
Rackable System Management Card:	Disable
Service processor:	iLO
Enable/Disable assigned IP:	Disable
Listening TCP port (1024-65535):	7050
Protocol:	Telnet
Inactivity timeout (1-3600 seconds, 0 for unlimited):	100 second(s)
Display port information:	Disable
Enable/Disable port escape sequence:	Enable
Port escape sequence:	Ctrl- z
Port break sequence:	~break
Use comment:	No
Quick connect via:	Web applet
Web applet encoding:	English (latin1)
Web applet size:	Columns 80 Rows 24

5. Click **Remote port parameters.** Remote port parameters are displayed:



Remote port parameters

Destination IP:	192.168.1.18
Destination port (0-65535):	22
Protocol:	SSH
SMASH:	Enable
Allow unattended continuous connection:	Enable
Automatic login:	Enable
User name:	Administrator
Password (new):	●●●●●●●●
Password (confirm):	●●●●●●●
Reestablishment interval:	5 seconds
Use a customizable script:	Disable

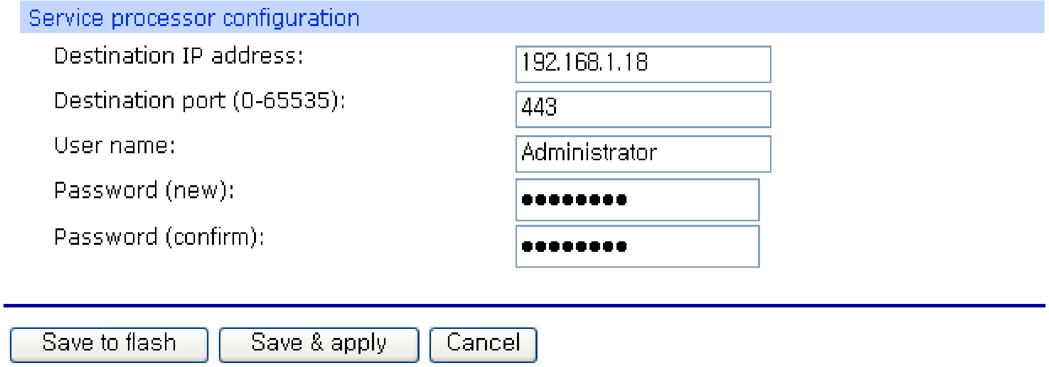
Port logging

Enter the remote port parameters as follows:

- **Destination IP**: The IP address of the server to monitor. Generally, this is the IP address assigned to the iLO management channel.
- **Destination port**: Normally 22 for SSH or 23 for Telnet; the actual port may vary on individual servers.
- **Protocol**: The Protocol to be used on the port normally this would be SSH, but Telnet or RawTCP can be used if it is enabled on the server.
- **SMASH**: Select to Enable or Disable.
- **Allow unattended continuous connection**: If enabled, when the connection is lost, it is reestablished automatically. Enabling this setting also enables the **Automatic login** setting and additional login settings.
- **Automatic login**: whether the specified user should be automatically logged in.
- **User name**. This is a user configured on the server with access to iLO.
- **Password**: Supply and confirm the password for the specified user.
- **Reestablishment interval value**: The time, in seconds, after which a lost connection will be reestablished. The default is 5 seconds.

Click **Save to flash**.

6. The **Service processor configuration** settings are displayed at the bottom of the **Serial port configuration** page. Select **Service processor configuration**. The Service processor configuration settings are displayed.



Service processor configuration

Destination IP address:	192.168.1.18
Destination port (0-65535):	443
User name:	Administrator
Password (new):	●●●●●●●●●
Password (confirm):	●●●●●●●●●

Enter the Service processor configuration settings:

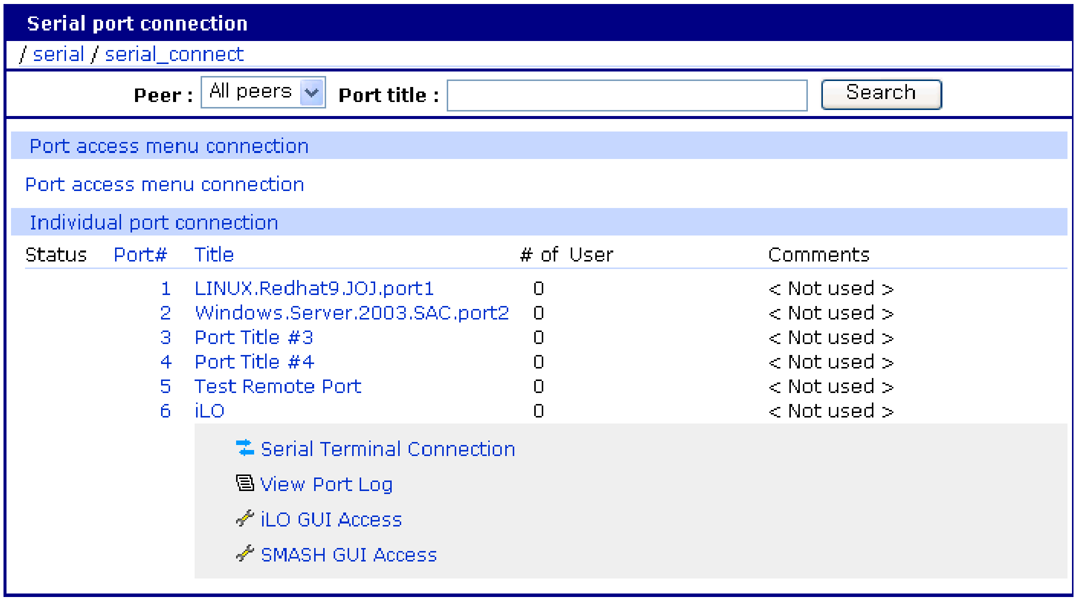
- **Destination IP address**: This is the IP of the iLO server.
- **Destination port**: The port used for HTTPS on the iLO server, normally 443.
- **User name**: This is a user configured on the server with access to iLO.
- **Password**: Supply and confirm the password for the above user.

Click **Save and apply**.

Access iLO Port or SMASH-CLP Support

After finishing configurations for iLO and SMASH-CLP, access iLO port or SMASH-CLP support from the **Serial port > Connection** page.

When iLO and SMASH are configured, four connection icons are displayed on the Serial port connection page, as shown:



Serial port connection

/ serial / serial_connect

Peer : All peers Port title :

Port access menu connection

Port access menu connection

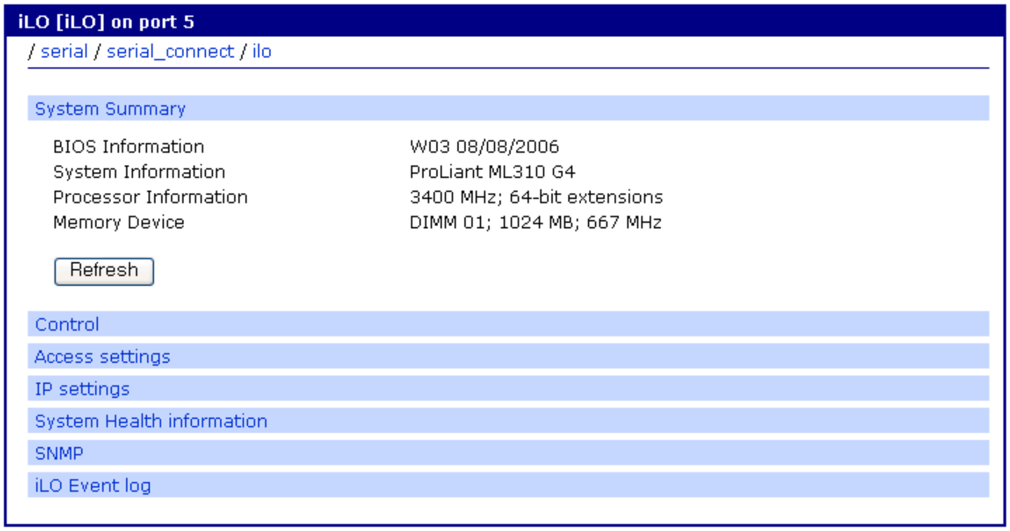
Individual port connection

Status	Port#	Title	# of User	Comments
	1	LINUX.Redhat9.JOJ.port1	0	< Not used >
	2	Windows.Server.2003.SAC.port2	0	< Not used >
	3	Port Title #3	0	< Not used >
	4	Port Title #4	0	< Not used >
	5	Test Remote Port	0	< Not used >
	6	iLO	0	< Not used >

Serial Terminal Connection is for direct access to the iLO service process.

View Port log is for checking logs for the connection made from the Passport.

iLO GUI Access is for connecting to a SAC-like iLO user interface page, as shown below.

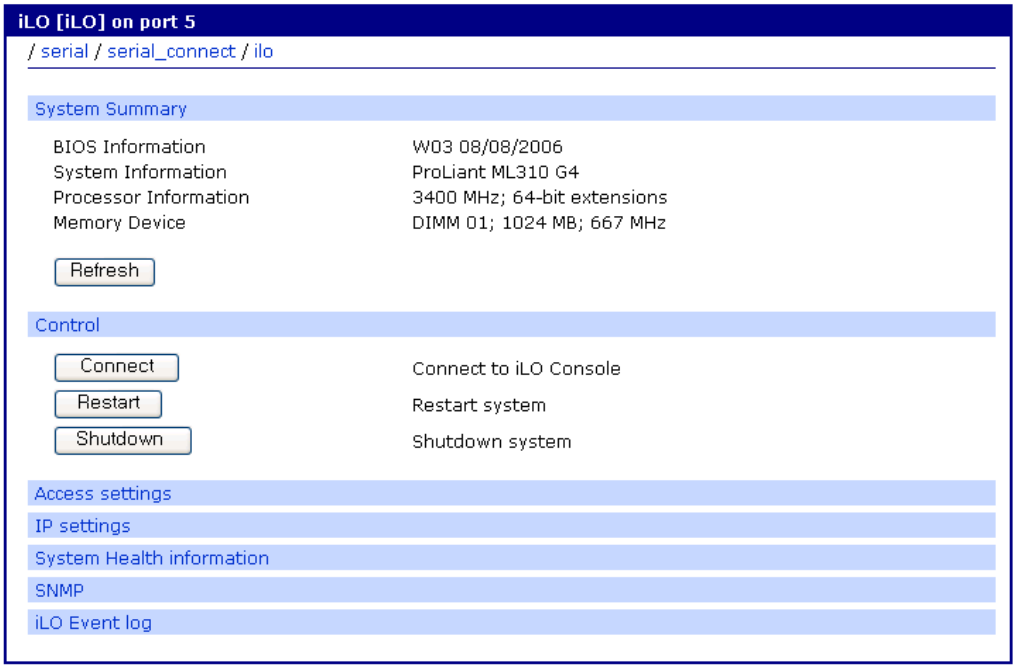


iLO [iLO] on port 5

/ serial / serial_connect / ilo

System Summary

BIOS Information	W03 08/08/2006
System Information	ProLiant ML310 G4
Processor Information	3400 MHz; 64-bit extensions
Memory Device	DIMM 01; 1024 MB; 667 MHz



iLO [iLO] on port 5

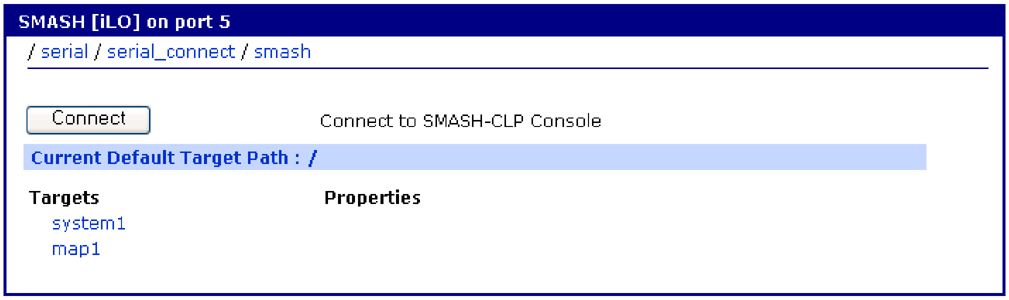
/ serial / serial_connect / ilo

System Summary

BIOS Information	W03 08/08/2006
System Information	ProLiant ML310 G4
Processor Information	3400 MHz; 64-bit extensions
Memory Device	DIMM 01; 1024 MB; 667 MHz

Connect	Connect to iLO Console
Restart	Restart system
Shutdown	Shutdown system

SMASH GUI Access accesses the SMASH-CLP user interface, as shown below.



SMASH [iLO] on port 5

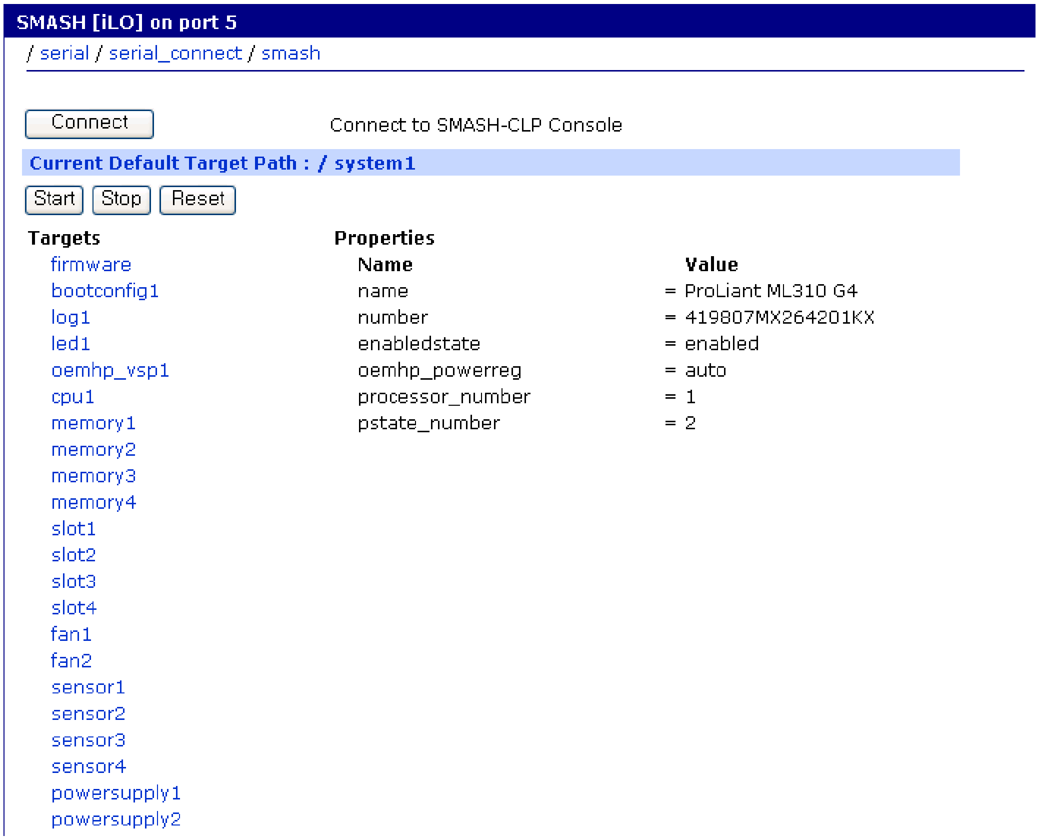
/ serial / serial_connect / smash

Connect	Connect to SMASH-CLP Console

Current Default Target Path : /

Targets	Properties
system1 map1	

Under **Targets**, click the links to move to the corresponding target path. SMASH-CLP shows sub targets and properties. Any commands that can be executed on the corresponding target path, such as **Start**, **Stop** and **Reset**, are displayed.



Connect to SMASH-CLP Console

Current Default Target Path : / system1

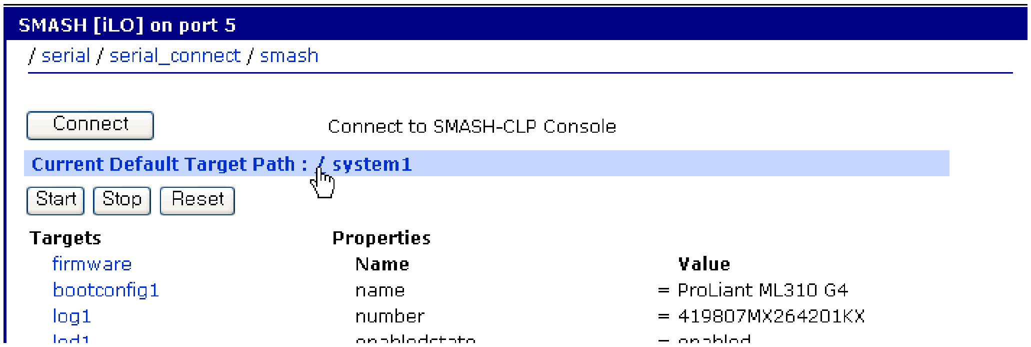
Targets

- firmware
- bootconfig1
- log1
- led1
- oemhp_vsp1
- cpu1
- memory1
- memory2
- memory3
- memory4
- slot1
- slot2
- slot3
- slot4
- fan1
- fan2
- sensor1
- sensor2
- sensor3
- sensor4
- powersupply1
- powersupply2

Properties

Name	Value
name	= ProLiant ML310 G4
number	= 419807MX264201KX
enabledstate	= enabled
oemhp_powerreg	= auto
processor_number	= 1
pstate_number	= 2

To move to the root path, click the leftmost **/** on **Current Default Target Path**, as shown.



Connect to SMASH-CLP Console

Current Default Target Path : / system1

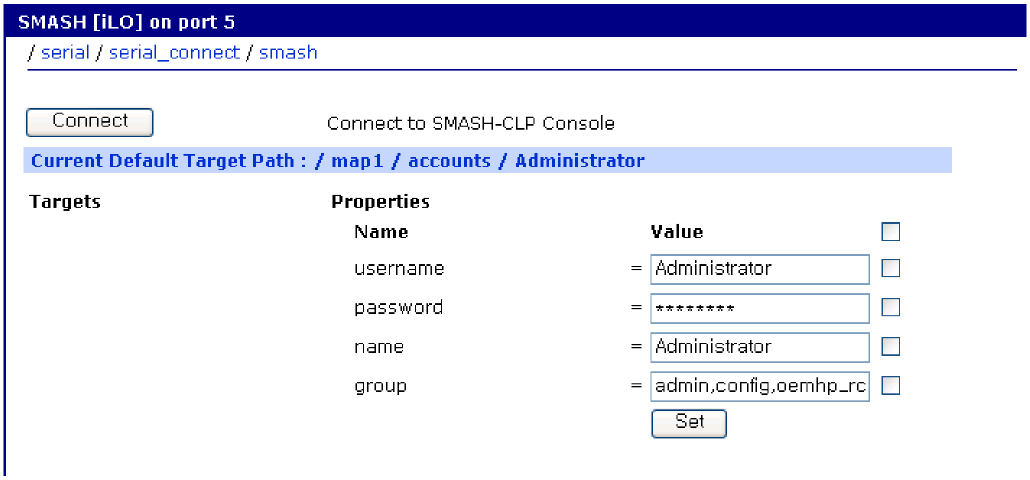
Targets

- firmware
- bootconfig1
- log1
- led1

Properties

Name	Value
name	= ProLiant ML310 G4
number	= 419807MX264201KX
enabledstate	= enabled

If the target path has properties that can be set, the SMASH-CLP user interface displays an edit box for changing properties; for example:



SMASH [iLO] on port 5

/ serial / serial_connect / smash

Connect to SMASH-CLP Console

Current Default Target Path : / map1 / accounts / Administrator

Targets

Properties

Name		Value	□
username	=	Administrator	□
password	=	********	□
name	=	Administrator	□
group	=	admin,config,oemhp_rc	□

Dell Remote Access Controller (DRAC)

Dell Remote Access Controller (DRAC) is a specification for the equipment that monitors the physical environment and condition of Dell servers. The specification is intended to cover the regulation of temperature, voltage and power, and to ensure the proper operation of the firmware.

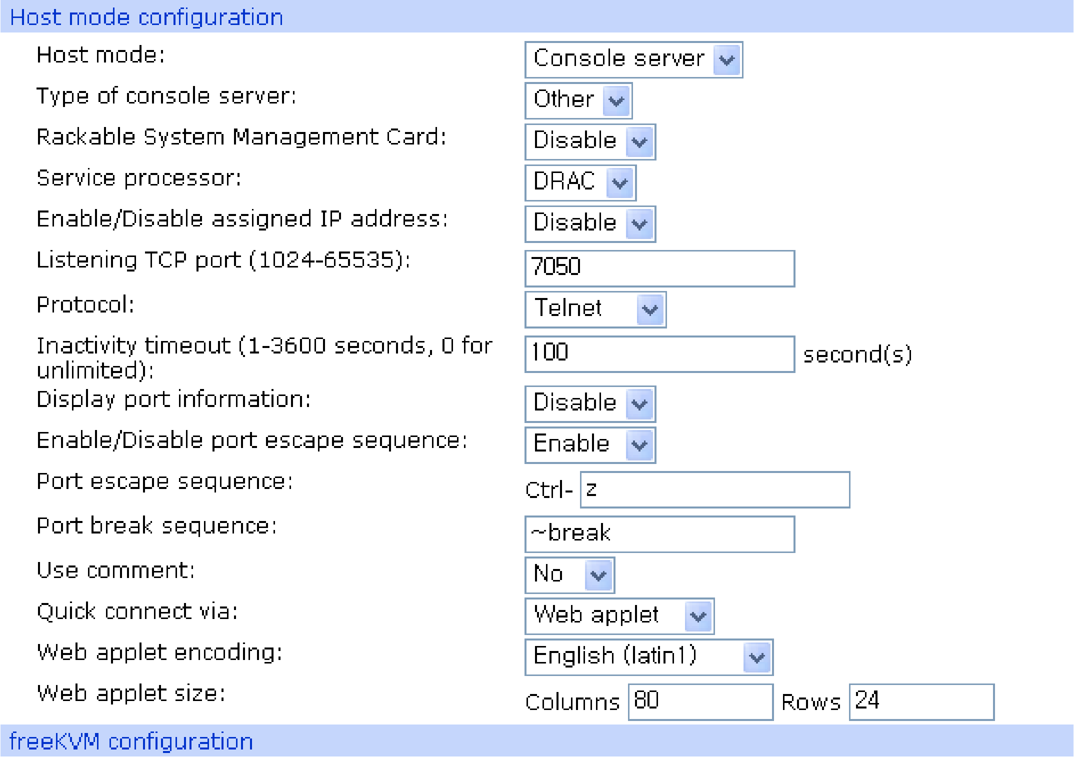
DRAC works with hardware servers regardless of the operating platform or other software they may run. DRAC allows an administrator to manage multiple servers from a single location by means of a user-friendly interface. Critical system events for each server can be logged. Settings for each basic input/output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

powered on or off, rebooted, or reset as necessary. Digi Passport supports DRAC 4 and DRAC 5.

Configure DRAC

To configure DRAC including SOL (Serial Over Lan) and SMASH CLP on a remote port, follow these steps.

1. In the Web interface, select Serial port configuration. Select the port to configure for DRAC.
2. From the menu, select **Advanced configuration**.
3. From the next menu displayed, select **Host mode configuration**.
4. For **Service processor**, select **DRAC**.
5. Click **Save to flash**. The Host Mode Configuration settings are displayed.

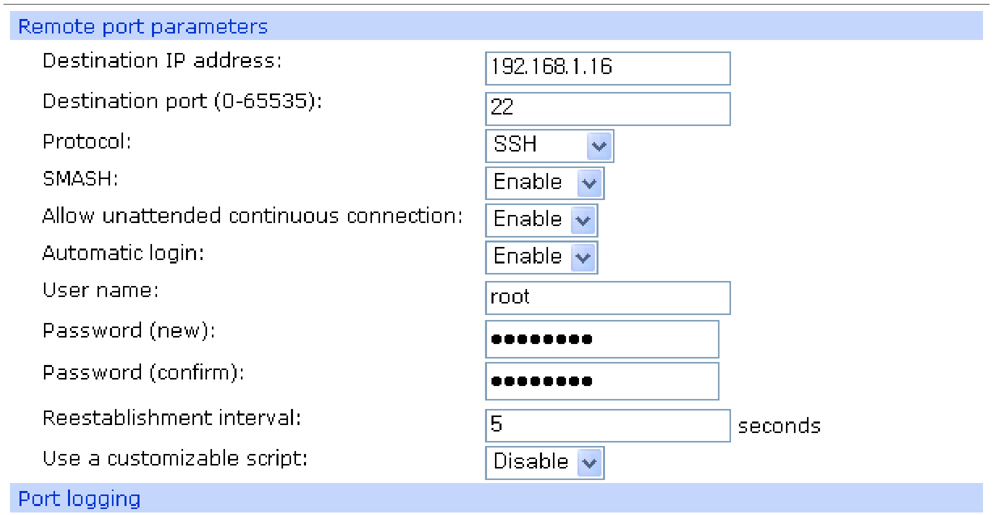


Host mode configuration

Host mode:	Console server
Type of console server:	Other
Rackable System Management Card:	Disable
Service processor:	DRAC
Enable/Disable assigned IP address:	Disable
Listening TCP port (1024-65535):	7050
Protocol:	Telnet
Inactivity timeout (1-3600 seconds, 0 for unlimited):	100 second(s)
Display port information:	Disable
Enable/Disable port escape sequence:	Enable
Port escape sequence:	Ctrl- z
Port break sequence:	~break
Use comment:	No
Quick connect via:	Web applet
Web applet encoding:	English (latin1)
Web applet size:	Columns 80 Rows 24

freeKVM configuration

6. Select **Remote port parameters**.



Remote port parameters

Destination IP address:	192.168.1.16
Destination port (0-65535):	22
Protocol:	SSH
SMASH:	Enable
Allow unattended continuous connection:	Enable
Automatic login:	Enable
User name:	root
Password (new):	●●●●●●●●●
Password (confirm):	●●●●●●●●●
Reestablishment interval:	5 seconds
Use a customizable script:	Disable

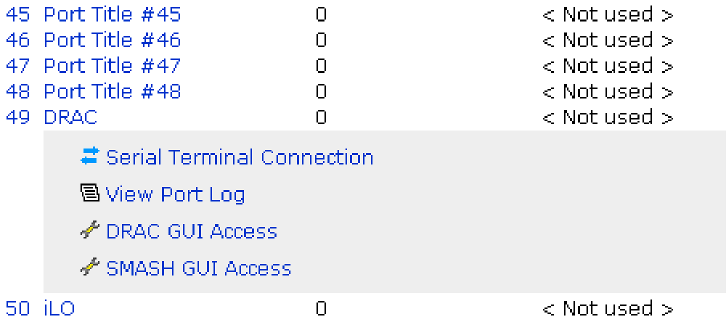
Port logging

Enter the remote port parameters:

- **Destination IP address**: The address of the server to monitor. Generally this will be the address assigned to the DRAC management channel.
- **Destination port**: normally 22 for SSH or 23 for Telnet, but these may vary on individual servers.
- **Protocol**: The protocol to be used on the port. Normally, the protocol is SSH, but Telnet or RawTCP can be used if enabled on the server.
- **SMASH**: Enables or disables use of the SMASH (Systems Management Architecture for Server Hardware).
- **Allow unattended continuous connection**: If Enabled, when the connection is lost, it is reestablished automatically. Enabling this setting also enables the **Automatic login** setting and additional login settings.
- **Automatic login**: whether the specified user should be automatically logged in.
- **User name**: A user configured on the server with access to DRAC.
- **Password**: Supply and confirm the password for the above user.
- **Reestablishment interval value**: The time, in seconds, after which a lost connection will be reestablished. The default is 5 seconds.

Click **Save and apply**.

After DRAC is configured, to access the DRAC port, select **Serial port > Connection**. If DRAC and SMASH are configured, four connection icons are shown, as in the example below.

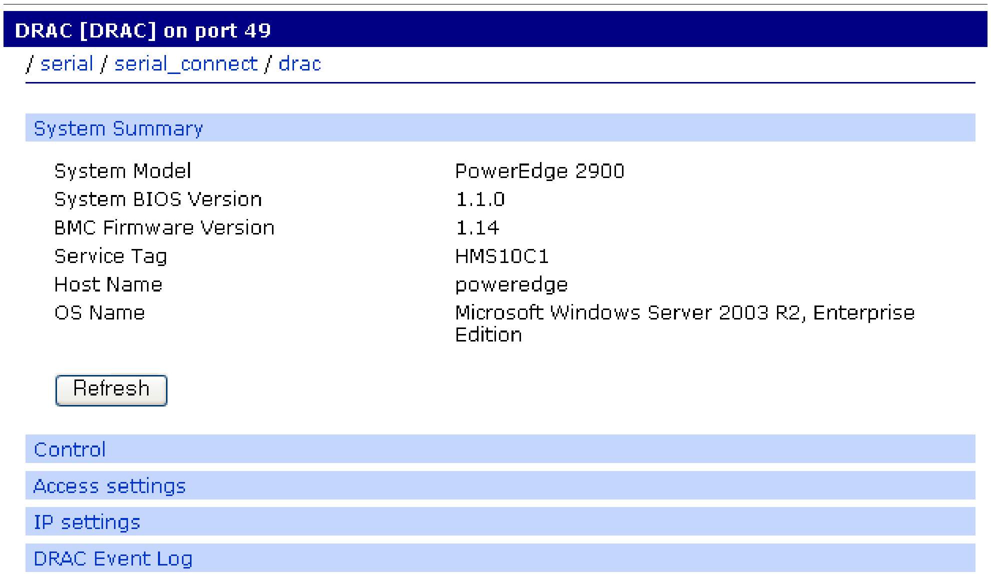


45	Port Title #45	0	< Not used >
46	Port Title #46	0	< Not used >
47	Port Title #47	0	< Not used >
48	Port Title #48	0	< Not used >
49	DRAC	0	< Not used >
	Serial Terminal Connection View Port Log DRAC GUI Access SMASH GUI Access		
50	iLO	0	< Not used >

Serial Terminal Connection is for direct access to the DRAC service process.

View Port Log displays logs for the connection made from the Digi Passport unit.

DRAC GUI Access is for connecting to a SAC-like DRAC user interface page as shown in the example screens.



DRAC [DRAC] on port 49

/ serial / serial_connect / drac

System Summary

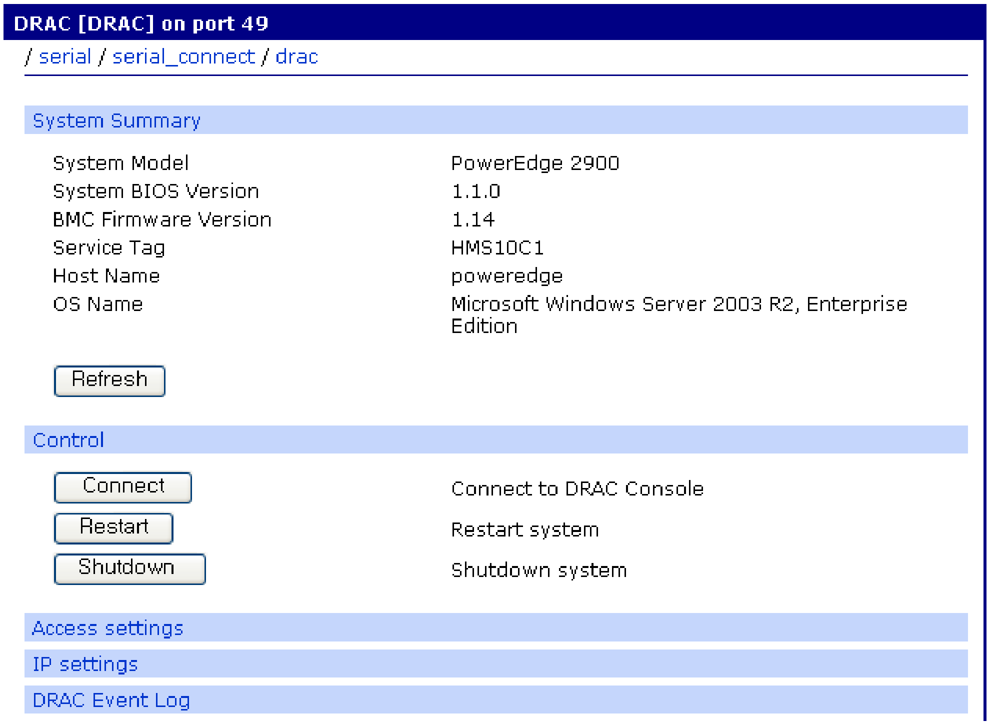
System Model	PowerEdge 2900
System BIOS Version	1.1.0
BMC Firmware Version	1.14
Service Tag	HMS10C1
Host Name	poweredge
OS Name	Microsoft Windows Server 2003 R2, Enterprise Edition

Control

Access settings

IP settings

DRAC Event Log



DRAC [DRAC] on port 49

/ serial / serial_connect / drac

System Summary

System Model	PowerEdge 2900
System BIOS Version	1.1.0
BMC Firmware Version	1.14
Service Tag	HMS10C1
Host Name	poweredge
OS Name	Microsoft Windows Server 2003 R2, Enterprise Edition

Control

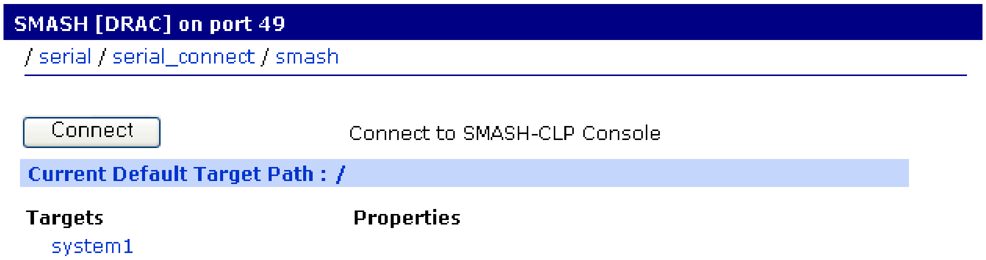
Connect	Connect to DRAC Console
Restart	Restart system
Shutdown	Shutdown system

Access settings

IP settings

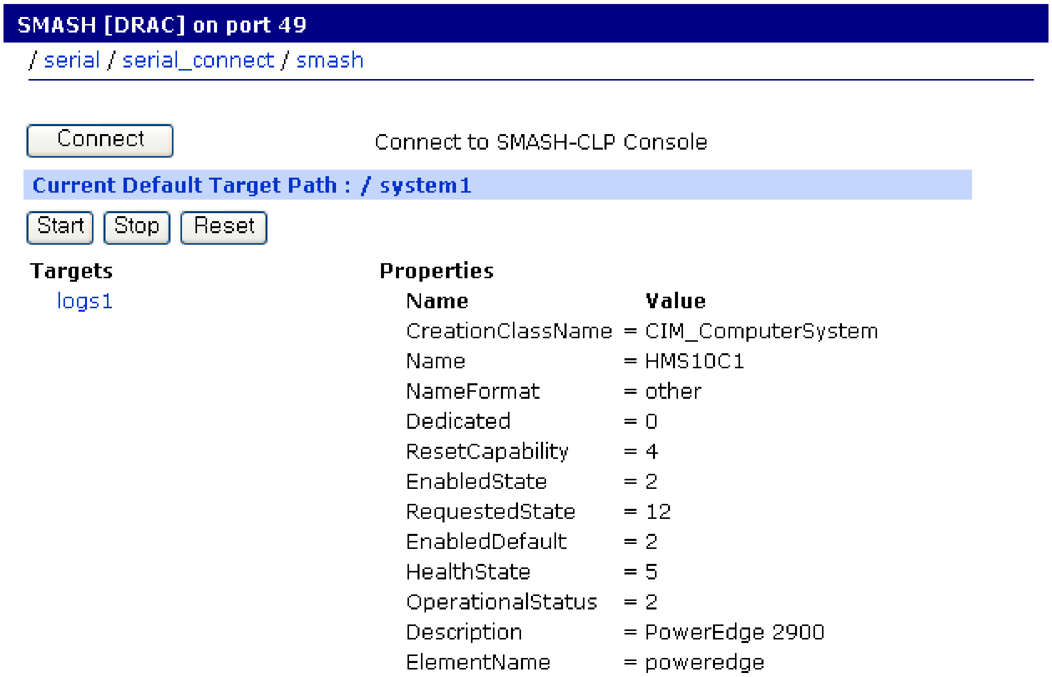
DRAC Event Log

SMASH GUI Access opens the SMASH-CLP user interface, as shown in the example.


SMASH [DRAC] on port 49
/ serial / serial_connect / smash
Connect
Connect to SMASH-CLP Console
Targets
system1
Properties

Current Default Target Path : /

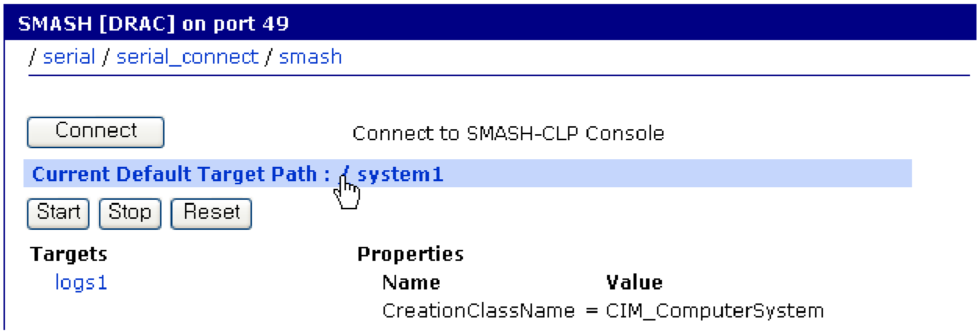
Under **Targets**, click the links to move to the corresponding target path, and SMASH-CLP shows sub targets and properties. Any commands that can be executed on the corresponding target path, such as Start, Stop and Reset, are displayed.



Current Default Target Path : / system1

```
Name                    Value
CreationClassName  = CIM_ComputerSystem
Name               = HMS10C1
NameFormat         = other
Dedicated          = 0
ResetCapability    = 4
EnabledState       = 2
RequestedState     = 12
EnabledDefault     = 2
HealthState        = 5
OperationalStatus  = 2
Description        = PowerEdge 2900
ElementName        = poweredge
```

To move to the root path, click the leftmost **/** on **Current Default Target Path** as shown.



Current Default Target Path : / system1

```
Name                    Value
CreationClassName  = CIM_ComputerSystem
```

Chapter 8 Users, Security, and Authentication

Methods for Controlling User Access

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

  Users can easily be added and removed from lists of restricted and permitted users.

- Enabling sniff session access

  This method allows multiple users to access a single port.

- Using a central point (**System administration > Security profile**) for establishing security parameters per network, port, or password.

Supported Authentication Methods

The Digi Passport unit supports several authentication methods, including:

- Local
- RADIUS
- TACACS+
- LDAP
- Kerberos
- Custom PAM. Authentication can be configured so that a secondary method is attempted if the primary method fails.

Configure User Access Control

Another method for controlling access to the serial ports on the Digi Passport unit is the User Access Control configuration. User access control can be set up 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, select **System administration > Users administration**. For details about adding users, see "Add a Compact-flash Card" on page 43.

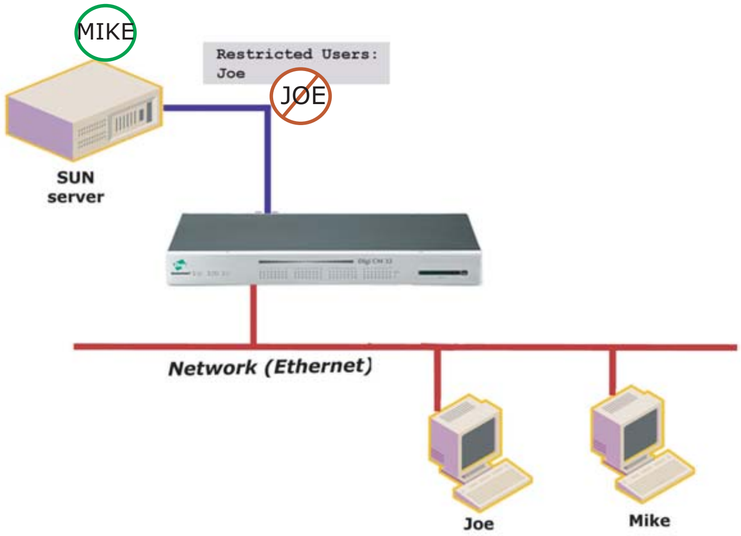
Users do not need to be configured locally; they can be defined on a remote authentication server.

Access lists are used to add rights to a single user or to multiple users at the same time. In addition, multiple users can be grouped and assigned one, some, or all these rights:

- Port access rights
- Port monitor rights
- Power management rights to an access list
- Break access rights
- Hot key rights to access port logs

See "Add an Access List and Add Users to It" on page 40 for the procedure for adding access lists.

This scenario shows a configuration with a restricted user: Joe does not have access to the Sun server, while Mike does.



A 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.

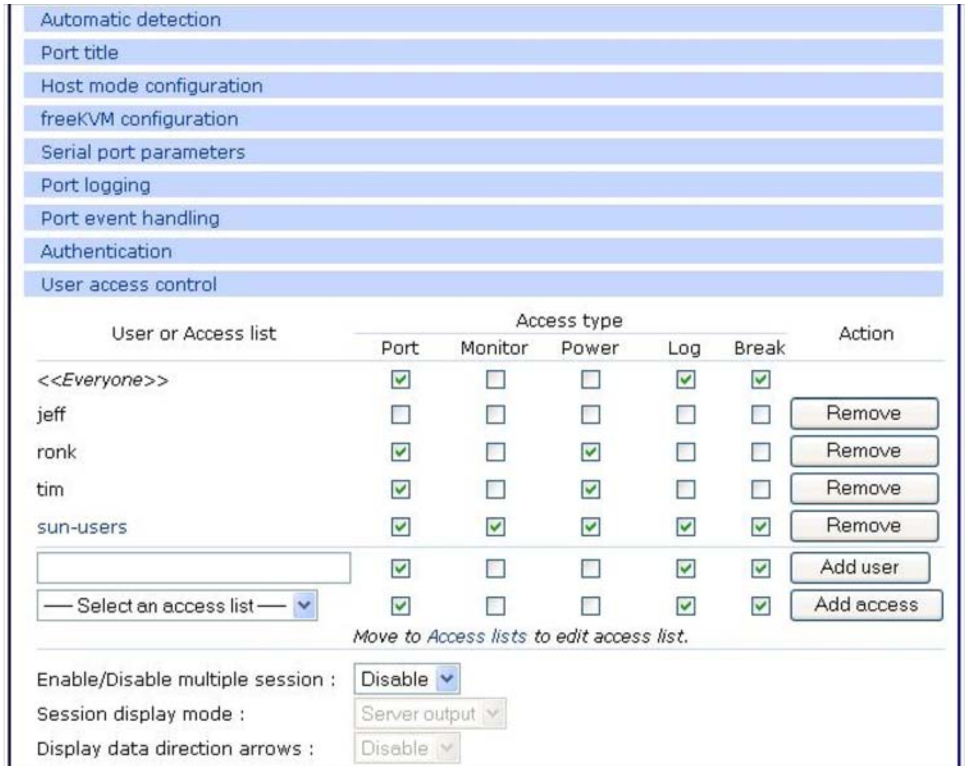
Selecting **<<Everyone>>**, means that all users, whether they are configured locally or are using a remote authentication (such as LDAP or Kerberos), have access to this port.

If **<<Everyone>>** is not selected, no users are allowed to access this port unless they are individually listed.

Usernames for access permissions or restrictions must be entered exactly as listed locally or on the remote authentication server, and are case-sensitive.

In the next example, three users are configured on the Digi Passport unit: **jeff**, **ronk**, and **tim**. To give users **tim** and **ronk** read/write access and power access to this port, either:

- Grant rights to **ronk** and **tim**.
- Restrict rights for user **jeff**.
- Add users to an access list, in this example, **sun-users**. To create access lists, go to **System administration > Access list**. For more information, see "Add an Access List and Add Users to It" on page 40.



User or Access list	Access type					Action
	Port	Monitor	Power	Log	Break	
<<Everyone>>	☑	□	□	☑	☑	
jeff	□	□	□	□	□	Remove
ronk	☑	□	☑	□	□	Remove
tim	☑	□	☑	□	□	Remove
sun-users	☑	☑	☑	☑	☑	Remove
	☑	□	□	☑	☑	Add user
— Select an access list —	☑	□	□	☑	☑	Add access

Move to Access lists to edit access list.

Enable/Disable multiple session : Disable

Session display mode : Server output

Display data direction arrows : Disable

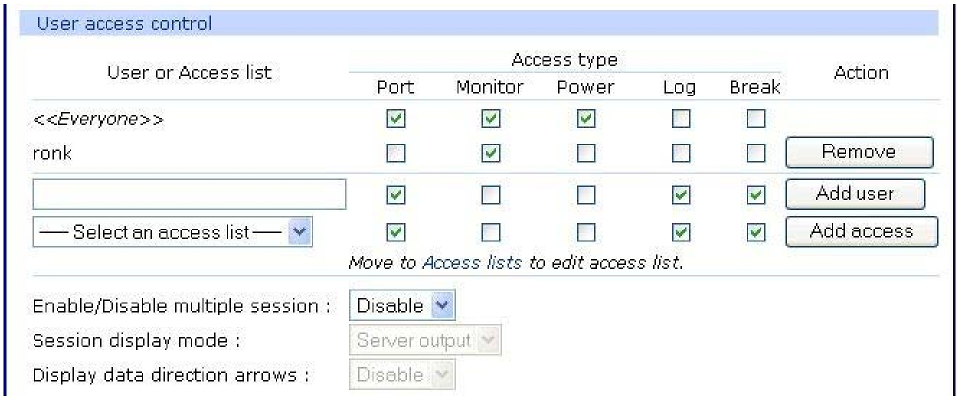
Configure User Access Privileges

1. Select **Serial Port Configuration > All Ports** or **Serial Port Configuration >** ***port number.***
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. Select **Port configuration > User access control.**
2. Enter privileges for **<<Everyone>>**.
3. Enter restricted user's name. In this example, it is **ronk**.
4. Enter the privileges for the user. Notice that **<<Everyone>>** has more access than **ronk** does.



User access control

User or Access list	Access type					Action
	Port	Monitor	Power	Log	Break	
<<Everyone>>	☑	☑	☑	□	□	
ronk	□	☑	□	□	□	Remove
	☑	□	□	☑	☑	Add user
— Select an access list —	☑	□	□	☑	☑	Add access

Move to Access lists to edit access list.

Enable/Disable multiple session : Disable

Session display mode : Server output

Display data direction arrows : Disable

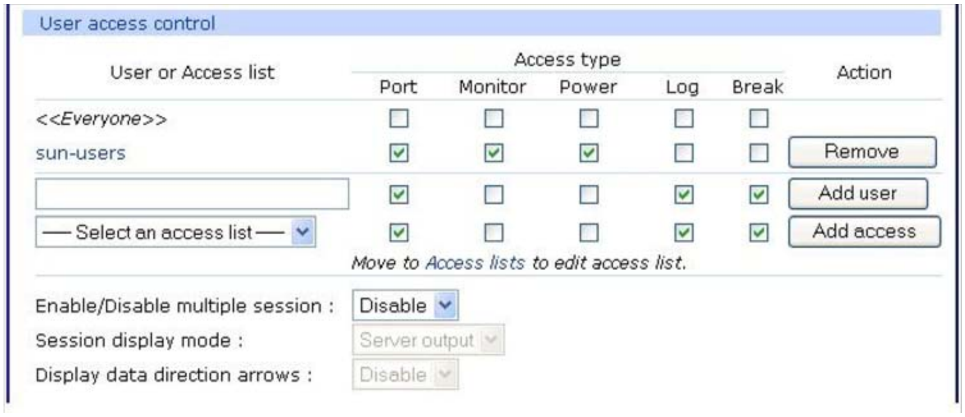
The usernames and passwords on the Digi Passport unit are case-sensitive. Notice **<<Everyone>>** has access to Port, Monitor, and Power, while user **ronk** has access to only Monitor, with no Port or Power access.

Change the Privileges of an Access List

1. On the same screen shown in the previous procedure, select an access list from the pulldown box.
2. Click **Add access**, then click **Save & apply**.

When the access list is added, it will include users **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 access control

User or Access list	Access type					Action
	Port	Monitor	Power	Log	Break	
<<Everyone>>	□	□	□	□	□	
sun-users	☑	☑	☑	□	□	Remove
	☑	□	□	☑	☑	Add user
— Select an access list —	☑	□	□	☑	☑	Add access

Move to Access lists to edit access list.

Enable/Disable multiple session : Disable

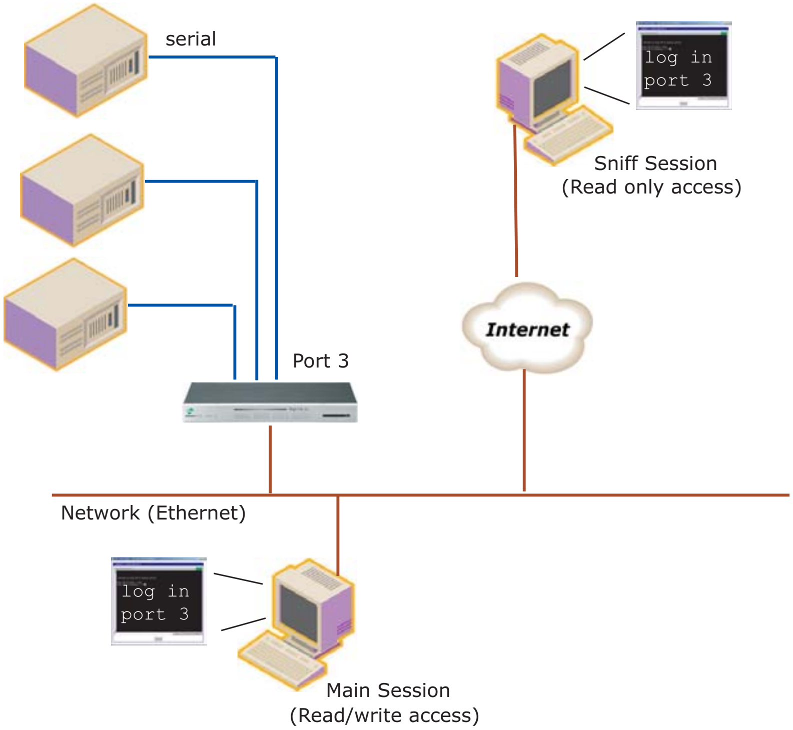
Session display mode : Server output

Display data direction arrows : Disable

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 selecting 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 deselecting the access types which the users 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**. Configure the sniff session modes per port on the serial port configuration page.

Sniff session settings include:

- **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 23.
- **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 Settings

System security settings include:

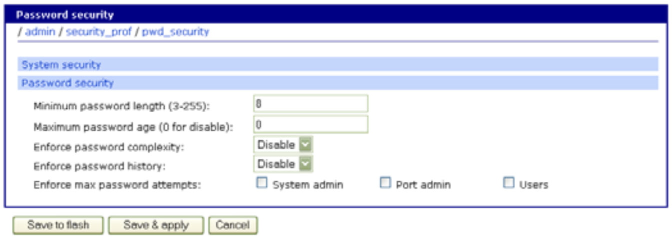
- **SNMP**: The Digi Passport unit allows using Get and Set commands for easy remote configuration and monitoring. Get and Set commands are configured individually using the **Network** > **SNMP Configuration** interface.

  This option provides 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 Advanced Digi Discovery Protocol (ADDP). 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 Settings

To enhance password security, 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**: Prevents including 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**: Prevents reusing the last nine passwords.
- **Enforce max password attempts**: Enforces maximum invalid login attempts before the user is locked out. It is selectable by the type of user.



Password security

/ admin / security_prof / pwd_security

System security

Password security

Minimum password length (3-255): 8

Maximum password age (0 for disable): 0

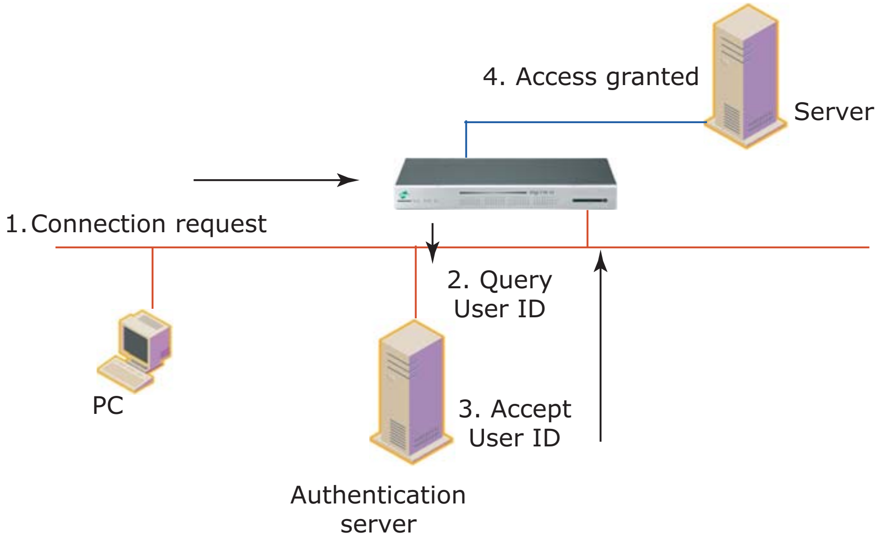
Enforce password complexity: Disable

Enforce password history: Disable

Enforce max password attempts: □ System admin □ Port admin □ Users

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 depends on the environment.

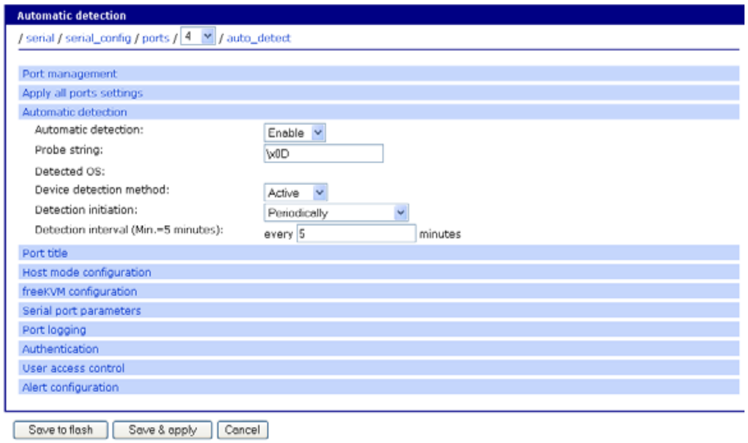


Configure Authentication Methods for Port Access

Authentication can be performed either through 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 configuring the Digi Passport unit for authentication.

To configure the Digi Passport unit for authentication:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port > Configuration**.
3. Select **All > Authentication** or ***port number*** **> Authentication**.
4. From the pulldown menu, select an authentication method. A configuration screen for the selected authentication method 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.



Automatic detection

/ serial / serial_config / ports / 4 / auto_detect

Automatic detection: Enable
Probe string: \x0D
Detected OS:
Device detection method: Active
Detection initiation: Periodically
Detection interval (Min.=5 minutes): every 5 minutes

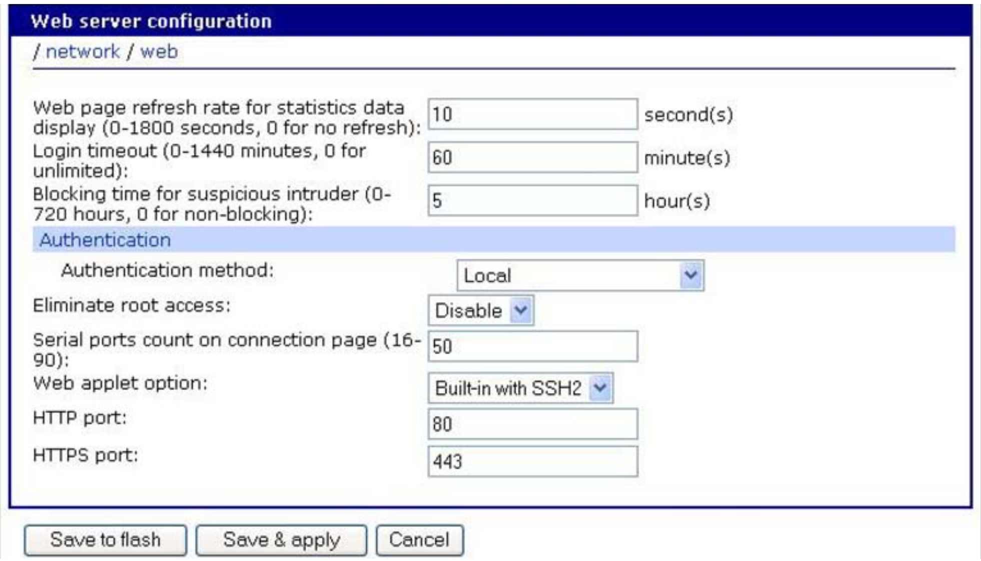
Note: To access the remote authentication to Port access menu, select **Serial port > Configuration > Port access Menu**.

5. Fill in the applicable fields.
6. Click **Save & apply**.

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.

Configure Authentication for the Web Server

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Network** > **Web server configuration**. The Web server configuration settings are displayed:



Web server configuration

/ network / web

Web page refresh rate for statistics data display (0-1800 seconds, 0 for no refresh): 10 second(s)
Login timeout (0-1440 minutes, 0 for unlimited): 60 minute(s)
Blocking time for suspicious intruder (0-720 hours, 0 for non-blocking): 5 hour(s)

Authentication

Authentication method: Local
Eliminate root access: Disable
Serial ports count on connection page (16-90): 50
Web applet option: Built-in with SSH2
HTTP port: 80
HTTPS port: 443

3. **Ability to see suspicious intruders' IP address in system logs:** Any suspicious intruder who requests a non-exist web page more than 10 times within the blocking time will be blocked during the blocking time for a suspicious intruder [**Network -> Web server configuration**]. Whenever any suspicious intruder is blocked or released, this event will be logged to the system log.
4. In the **Authentication method** setting, select an authentication method, then click **Save & apply**.

When using remote authentication for the web server, such as RADIUS, RADIUS Down-local, TACACS+, LDAP, Kerberos, or Custom PAM, user definitions must also be added to the local database **if you want access as someone other than a user**. The **user password** must be different from the one used for local authentication; otherwise, the Passport will authenticate against the local database instead of the remote one. For details, see "Install and Configure PC Cards" on page 42.

When the user password is approved by the authentication server, the Digi Passport unit uses the local permission rights to provide access privileges to ports and the configuration, except as in the note below.

Note: For remote authentication (Radius, TACACS, etc) via the web:

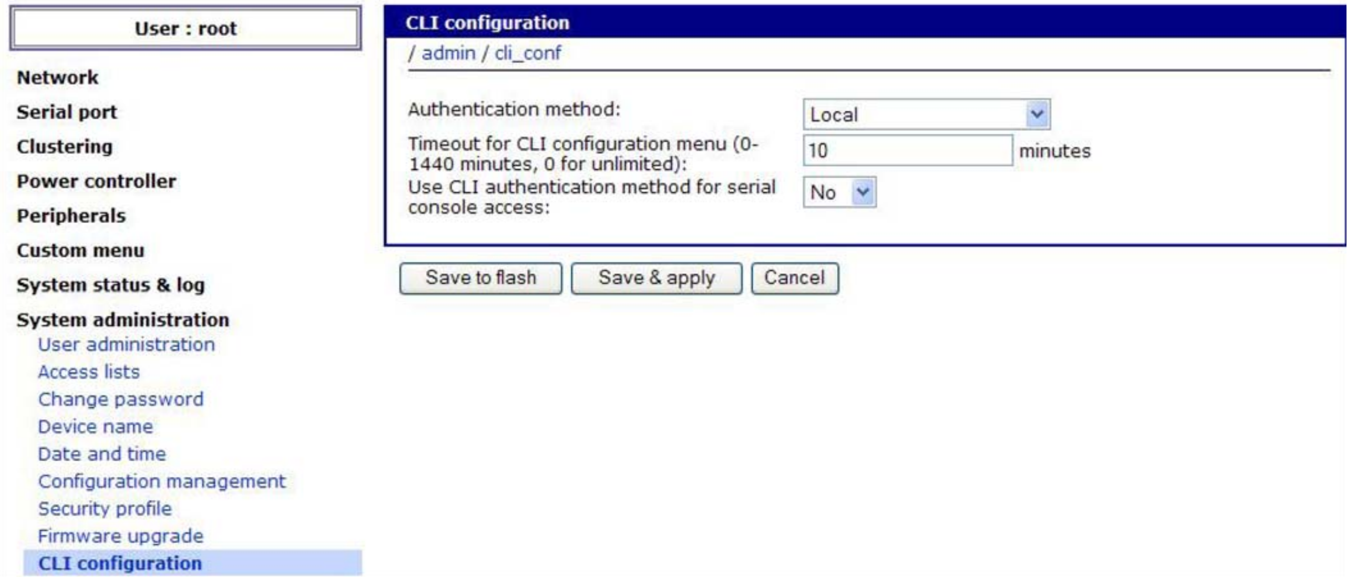
- For web access as a port or system adminstrator, specific named access lists must be created.
- For port admins. Create the access list title **web_padmin** and add all port admins under that.
- For system admins. Create the access list title **web_admin** and add all system admins under that.

Configure Authentication for the CLI

The CLI configuration is for specifying the authentication method and shell when accessing the Passport directly. Available options:

- **Authentication method:** Local, Radius, TACACS, LDAP, Kerberos
- **Timeout for CLI menu:** Specify the idletimeout in minutes.
- **Use CLI auth for serial console access:** Authentication method to be the same, or different, than the Passport console port.

When specifying a remote auth method you can specify the shell for them to use: Shell program: Port access or Custom menu.



CLI configuration

/ admin / cli_conf

Authentication method: Local

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

Use CLI authentication method for serial console access: No

LDAP Authentication

The Digi Passport unit supports authenticating against an LDAP-based database, including LDAP systems running on Linux servers, and Microsoft systems running the Microsoft Active Directory 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 a single container. The Digi Passport unit will extend the username using the LDAP search base and authenticate the user.

For example, consider a domain named **dilbert.com**. The LDAP server is at **10.1.1.1**. All users with access to the Digi Passport unit are located in the container **USA Users.**

The LDAP authentication for users of the domain is configured as follows:

```
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 the LDAP database resides on a Microsoft system, the Domain name for the active directory (in the above example, **dilbert.com**) must be configured.

If using a non-Microsoft system, do not use this setting, 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 creating a custom authentication schema or using 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@digi.com**

1. Place the custom PAM modules onto: /usr/2 on the Digi Passport unit.
2. Use an SCP client (such as WinSCP) to copy data to the /usr2 directory, or use an 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.

Configuration for a Samba Server

On the Samba server

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

On the Digi Passport

1. In the Web interface, go to **Network > Samba configuration**.
2. Set Samba configuration values as follows:
   - **Samba service**: Enable
   - **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, if the Samba server is a Windows server. The user name must be prefixed with the domain, for example, "digi\username"
   - **Samba server password**: Password of the user

The Samba directory will be mounted in the Digi Passport unit's file system in the **/mnt/smb** directory.

Chapter 9 Custom and Default Menus

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.

Recommended Process for Implementing Custom Menus

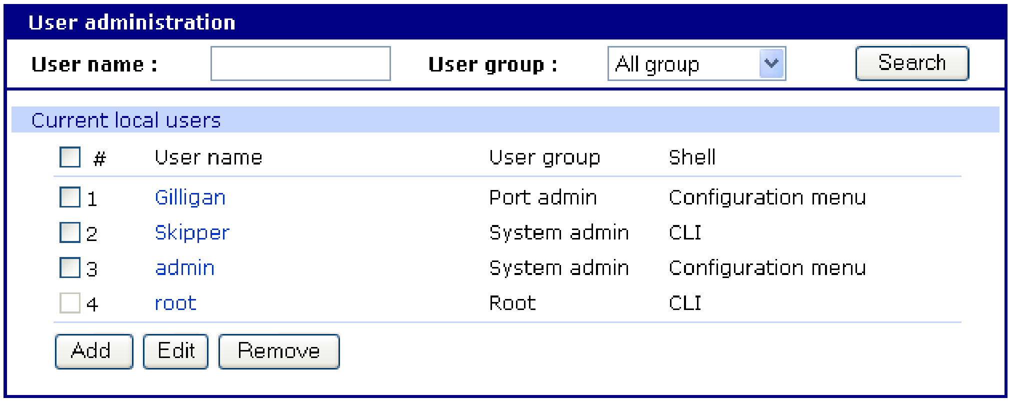
Before making custom menus, plan the kind of menus and menu items to make available for users. A good plan would include the following:

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

Add Users to the System

Before users can be assigned menus, the users must be added to the system.

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System administration > Users administration**. Click the **Add** button.



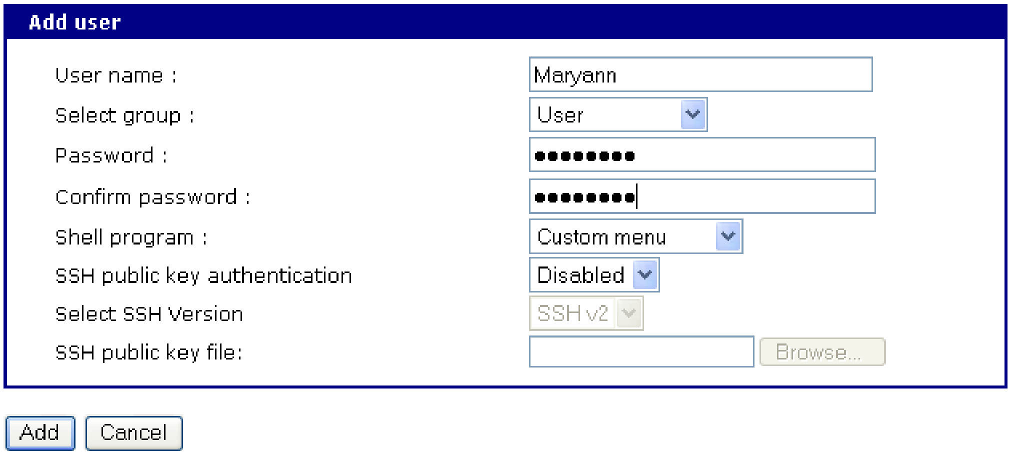
User administration

User name : ______ User group : All group

Current local users

□ #	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

3. Enter the User name and select the User group. For Shell program, select **Custom menu**.



Add user

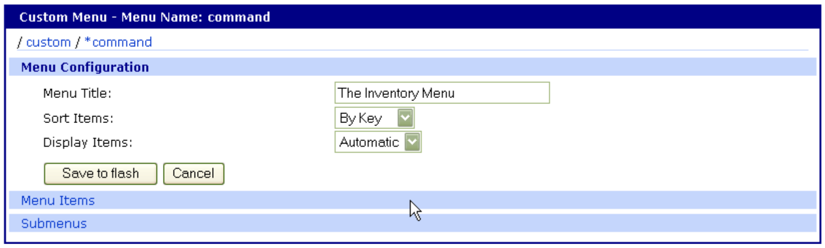
User name :	Maryann
Select group :	User
Password :	••••••••
Confirm password :	••••••••
Shell program :	Custom menu
SSH public key authentication	Disabled
Select SSH Version	SSH v2
SSH public key file:	

4. Click **Add** to add the user.
5. Continue to add users as needed. Clicking **Save to flash** or **Apply changes** is not required for users to be added.

Create Menu Names

To name a custom menu, do the following:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Custom Menu** > **Configuration**.



Custom Menu - Menu Name: command

/ custom / *command

Menu Configuration

Menu Title: The Inventory Menu

Sort Items: By Key

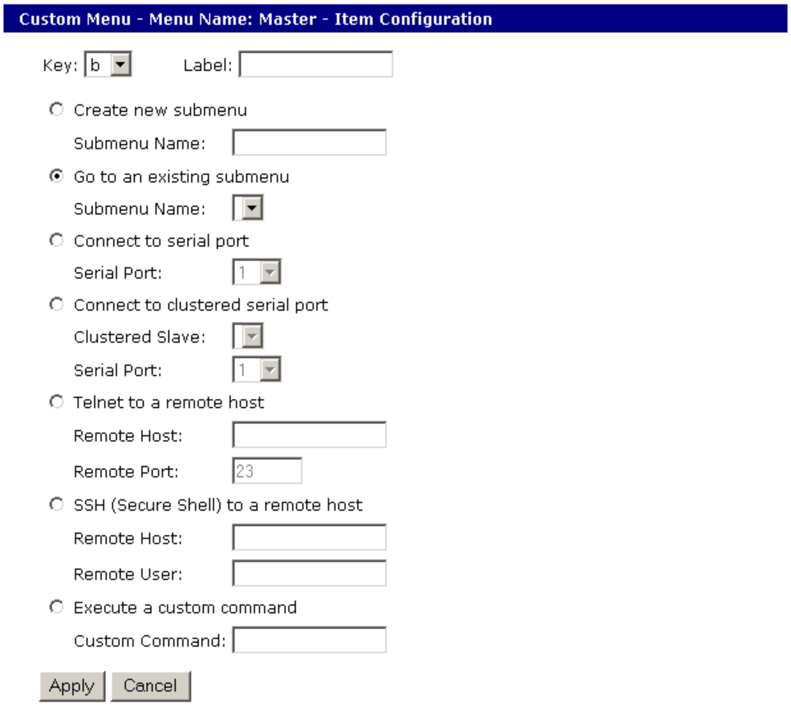
Display Items: Automatic

3. Enter the Menu Name to assign and click the **Add Menu** button.

   The menu is added.
4. Click the hyperlink to the menu just created.
5. From the pulldown menu, select the method to Sort and Display items.
6. Click **Save & apply**.
7. Repeat as required to create additional menus.

Add Menu Items

1. Select **Custom Menu** > **Configuration** >***menu name*** link for the menu to configure.
2. Select **Menu Items > Add Item**. The Custom Menu Item Configuration settings are displayed.



Custom Menu - Menu Name: Master - Item Configuration

Key: b   Label:

○ Create new submenu

Submenu Name:

● Go to an existing submenu

Submenu Name:

○ Connect to serial port

Serial Port: 1

○ Connect to clustered serial port

Clustered Slave:

Serial Port: 1

○ Telnet to a remote host

Remote Host:

Remote Port: 23

○ SSH (Secure Shell) to a remote host

Remote Host:

Remote User:

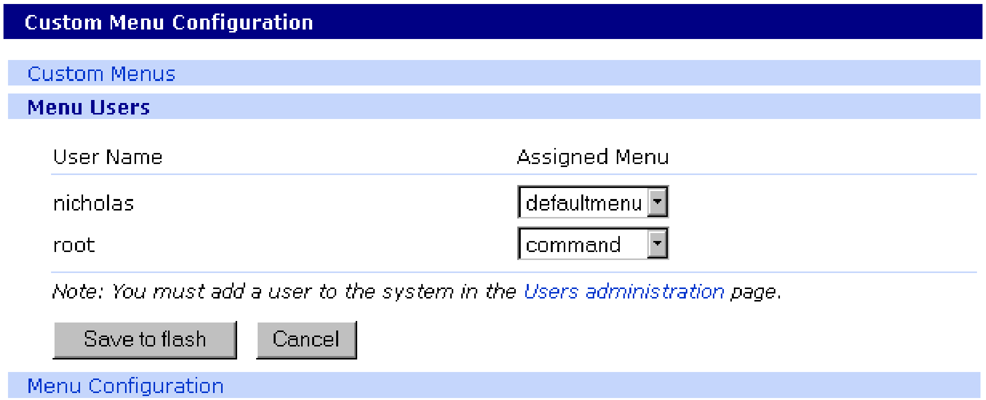
○ Execute a custom command

Custom Command:

3. Fill in the desired parameters:
   - **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**: Select an existing submenu from the pulldown menu that this menu item will be assigned or linked to.
   - **Connect to serial port**: Connects to a specified port.
   - Connect to clustered serial port: Connects to a clustered port.
   - **Telnet to a remote host**: A remote host's IP address or host name.
   - **SSH (Secure Shell) to a remote host**: Enter the host name or IP address of a remote host and the remote username.
   - **Execute a custom command**: A customized command, any valid command on the command line with acceptable user privileges.
4. Click **Apply.**
5. To add more menu items, repeat this procedure. To add or configure submenus, select **Submenus** on the **Menu Configuration** page.

Assign Users to a Menu

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Configuration > Custom Menu > Menu Users**. A list of available users is displayed.



User Name	Assigned Menu
nicholas	defaultmenu
root	command

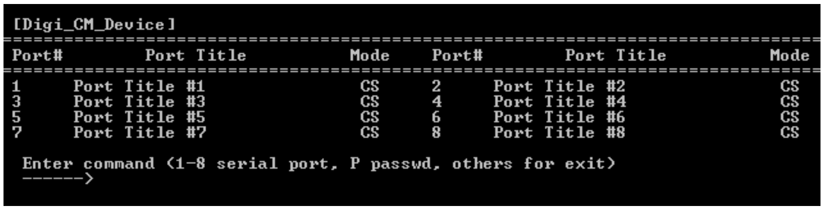
Note: You must add a user to the system in the Users administration page.

3. Select a menu for a user by selecting a menu from the pulldown **Assigned Menu** list.
4. Click **Save & apply**.

Default Menu: The Port Access Menu

The port access menu is a flat (one level) menu showing all ports, port titles and the mode of each port. It provides an overview of all ports and initiating a connection to any of them.

When connecting to a specific port, a prompt for the username and password us displayed.



```
[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)
 ------>
```

Access the port access menu

There are multiple ways to access the port access menu:

- Using an assigned IP address (see "Host Mode Configuration" on page 71)
- Using TCP/IP port 7000
- Using TCP/IP port 22 or 23 if the **Shell program** is set to **port access menu** for this specific user. See "Add a Compact-flash Card" on page 43.
- Entering **portaccessmenu** from the command line

Connect to ports

The port access 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, either Telnet or SSH.

Change password

To change your own password, press the **P** Key.

Display and connect to slave units

If the Digi Passport unit is configured to be the master in a master-slave scenario. Pressing the **S** key displays a list of all slave units. Selecting a slave displays the port access menu of the slave.

To search via port title

Press the F key and then enter your search string.

Port display for Digi Passport 48 only

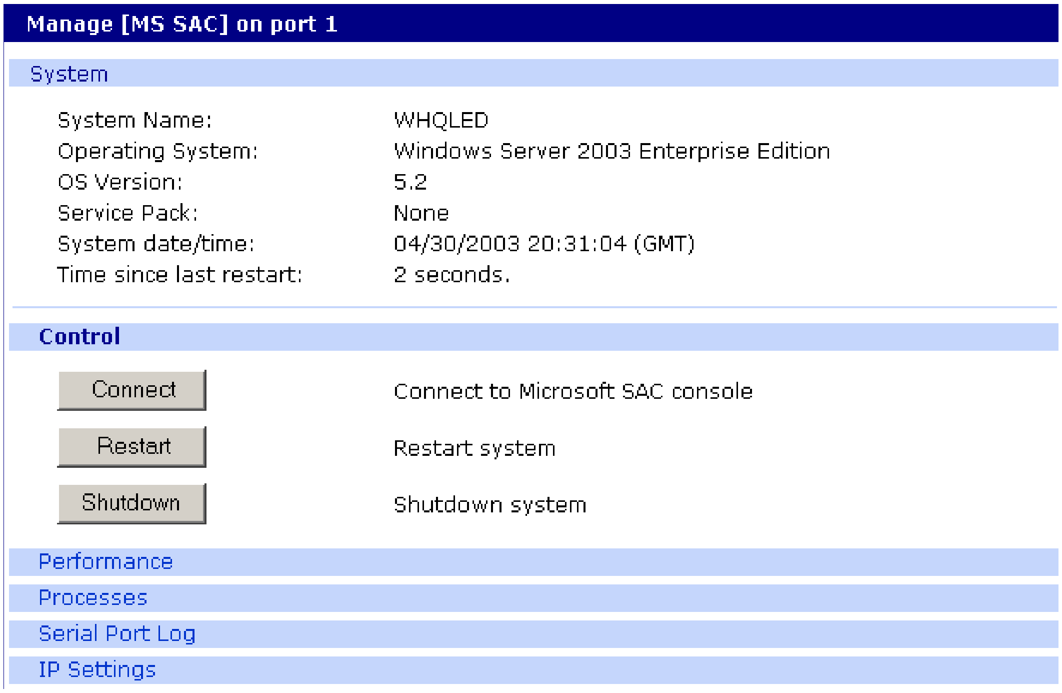
When using a Digi Passport 48, not all ports can be displayed on one screen. Press **Enter** to display ports 33-48.

Support for Microsoft Windows Server 2003 in Digi Passport

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.

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

Connect	Connect to Microsoft SAC console
Restart	Restart system
Shutdown	Shutdown system

Performance

Processes

Serial Port Log

IP Settings

Process for Setting Up Microsoft SAC Support

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 Set 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 Set Up the Digi Passport Unit for SAC Support"Set Up the Digi Passport Unit for SAC Support" on page 166.

Set Up the Windows Server 2003 Port

1. Sign on to the Windows Server 2003 as the administrator.
2. Access the command line.
3. Use the **bootcfg** command to redirect console traffic to the correct COM port. The following is the command syntax and an example. See the Microsoft documentation for additional information on the SAC feature.

Command Syntax

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

where*:*

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

Command Example

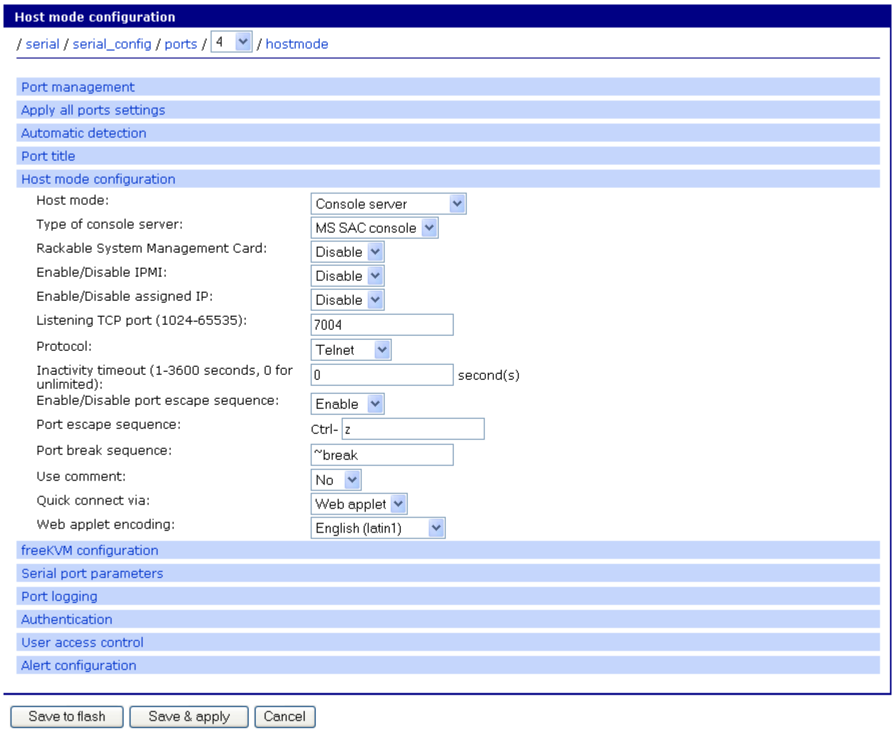
In this example, console output is redirected to COM 2, the boot entry is specified as 1, and the port speed set to 115200.

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

Set Up the Digi 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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port** > **Configuration**.
3. Select a port.
4. Select **Host mode configuration**. The Host mode configuration page is displayed.
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.



Host mode: Console server
Type of console server: MS SAC console
Rackable System Management Card: Disable
Enable/Disable IPMI: Disable
Enable/Disable assigned IP: Disable
Listening TCP port (1024-65535): 7004
Protocol: Telnet
Inactivity timeout (1-3600 seconds, 0 for unlimited): 0 second(s)
Enable/Disable port escape sequence: Enable
Port escape sequence: Ctrl- z
Port break sequence: ~break
Use comment: No
Quick connect via: Web applet
Web applet encoding: English (latin1)

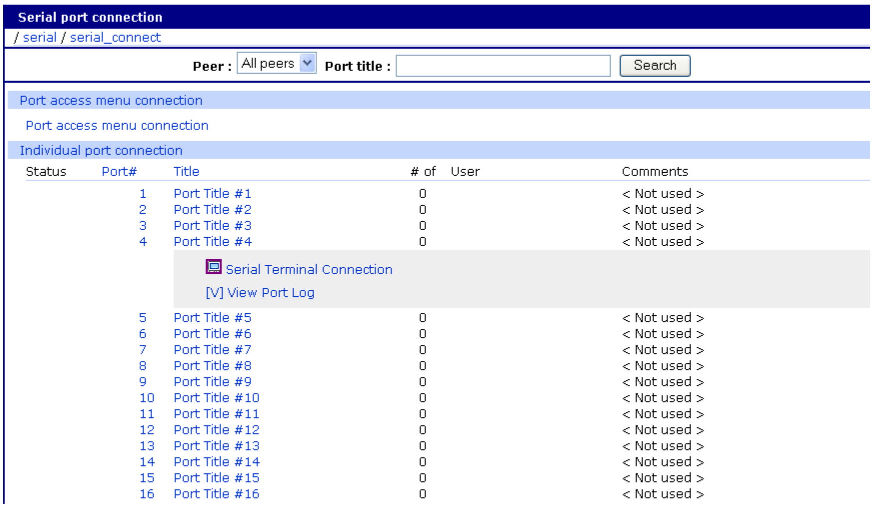
6. Set other fields as appropriate.
7. Click **Save & apply**.
8. Configure serial port communication settings:
   - Select Serial port parameters from the menu.
   - Adjust settings as required. This includes ensuring that the Baud rate matches the setting on the Windows Server 2003 serial port and Flow control is set to None. Ignore the DTR behavior field.

   When done, click **Save & apply**.

Access Windows Server 2003 Console Port from Digi Passport Unit’s GUI

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

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port** > **Connection**. A screen similar to the following is displayed.



Serial port connection

/ serial / serial_connect

Peer : All peers Port title : Search

Port access menu connection

Port access menu connection

Individual port connection

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 >
		Serial Terminal Connection [V] View Port Log			
	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. Click on the **title** of the port to which the Windows Server 2003 console port is connected.

   If support for "Windows Server 2003" and "Rackable Systems Management Card" is selected, a menu for selecting one of the two functions is displayed.
4. 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**: Selecting **Shutdown** switches off the server, meaning it can no longer be accessed remotely.
Performance	Displays to Microsoft Server 2003 status information.
Process	Displays the process list, for viewing and killing active processes.
Serial Port Log	Displays to port logging information.
IP Settings	Displays IP settings, to verify and change settings as needed. However, the IP settings are only temporary; they cannot be changed permanently through this method

Chapter 11 Configure and Use freeKVM

About freeKVM

The Digi Passport provides a method, called freeKVM, for gaining access to the graphical interface of a system using the network. Using freeKVM involves specifying a connection method and IP address to use to reach the system. Supported connection methods include:

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

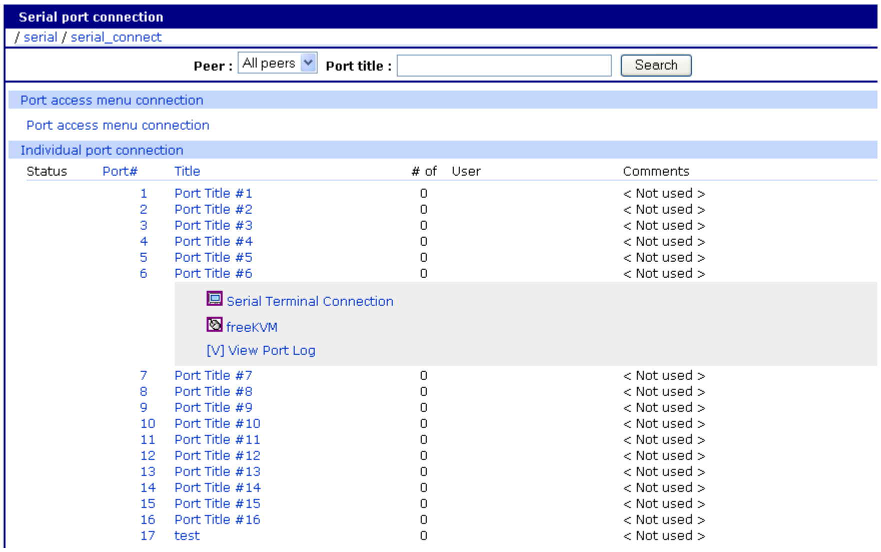
Supported Free Protocols and Tested Client Software

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

Example Configuration

Here is an example of a Digi Passport managing a Linux SuSE 9.2 system, a Windows 2003 system, and an HPUX system.



Serial port connection

/ serial / serial_connect

Port access menu connection

Port access menu connection

Individual port connection

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

freeKVM

[V] View Port Log

Status	Port#	Title	# of	User	Comments
	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 >

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

Use freeKVM with Remote Desktop Protocol

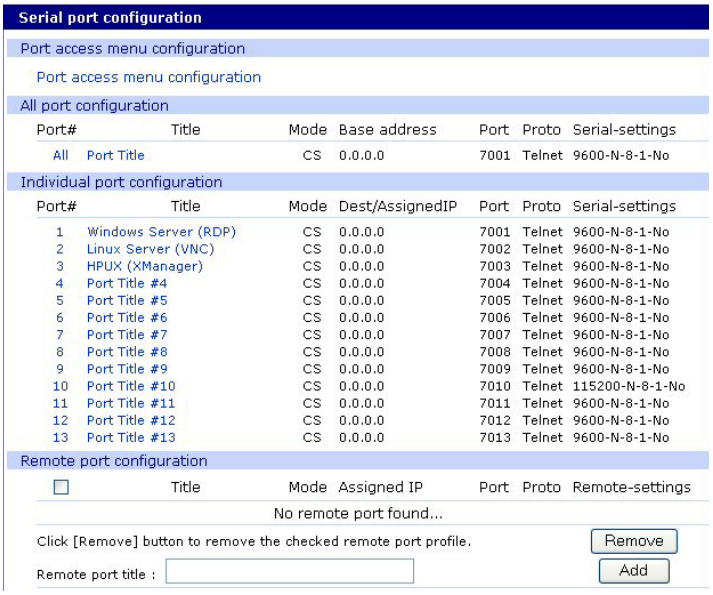
This section describes how to configure freeKVM with Remote Desktop Protocol, and connect to a system through freeKVM using Remote Desktop Protocol.

Configure freeKVM with Remote Desktop Protocol

To set up freeKVM with Remote Desktop protocol, follow this procedure.

Note: When using Remote Desktop configuration and automatic IP address detection is desired, configure the host mode for the port to MS SAC console before configuring the freeKVM feature for the port. For more information, see "Set Up the Digi Passport Unit for SAC Support" on page 166.

1. Access the Digi Passport Web interface and log in.
2. Select **Serial Port > Configuration**. This window opens:



Serial port configuration

Port access menu configuration

Port access menu configuration

All port configuration

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

Individual port configuration

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

Remote port configuration

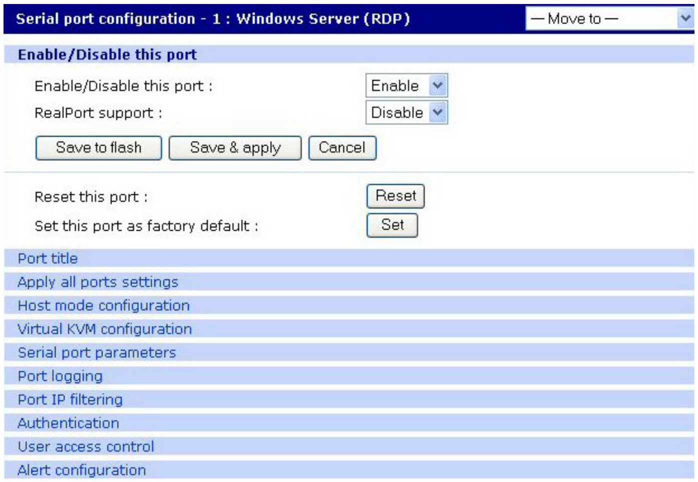
□	Title	Mode	Assigned IP	Port	Proto	Remote-settings

No remote port found...

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

Remote port title : Add

3. Select the port to configure, then click the **freeKVM** link. (In this example, port 1 is selected.) A window similar to this one opens, showing the serial port number and title:



Serial port configuration - 1 : Windows Server (RDP)

Enable/Disable this port

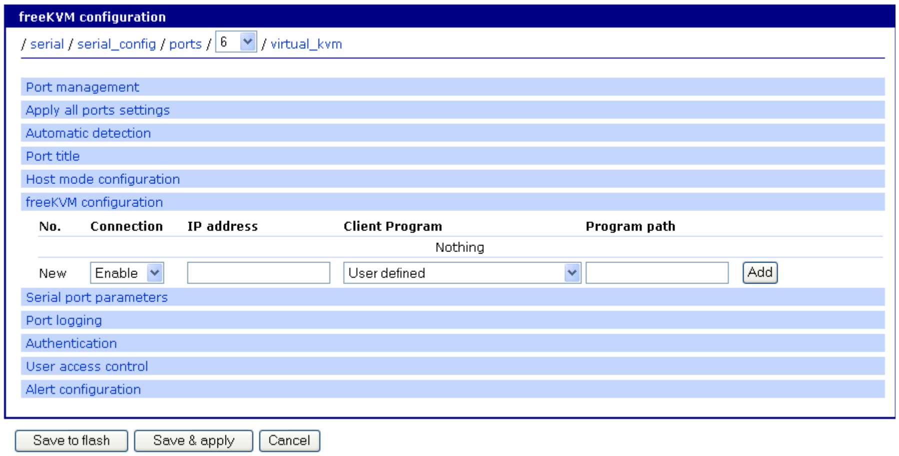
Enable/Disable this port : Enable

RealPort support : Disable

Reset this port : Reset

Set this port as factory default : Set

4. Click **freeKVM configuration**. This window is displayed:



No.	Connection	IP address	Client Program	Program path
		Nothing		
New	Enable		User defined	

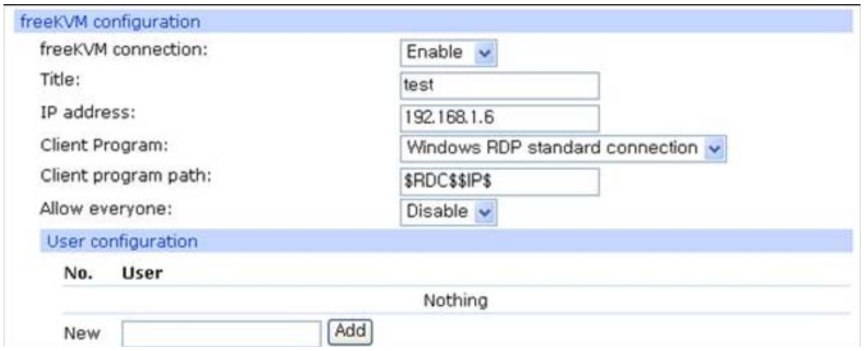
5. For the **freeKVM configuration** setting, select **Enable**.

   From the **Client program** pulldown, select
   Windows remote desktop connection.

6. If not using IP automatic detection, enter the IP address.
7. Enter title for KVM connection.
8. Click **Save & Apply**.

User permission for each freeKVM session can be specified separately

Click **No.** on each freeKVM session configuration, then enter extended configuration page for assigning user access list of each freeKVM session.



freeKVM connection:	Enable
Title:	test
IP address:	192.168.1.6
Client Program:	Windows RDP standard connection
Client program path:	$RDC$$IP$
Allow everyone:	Disable

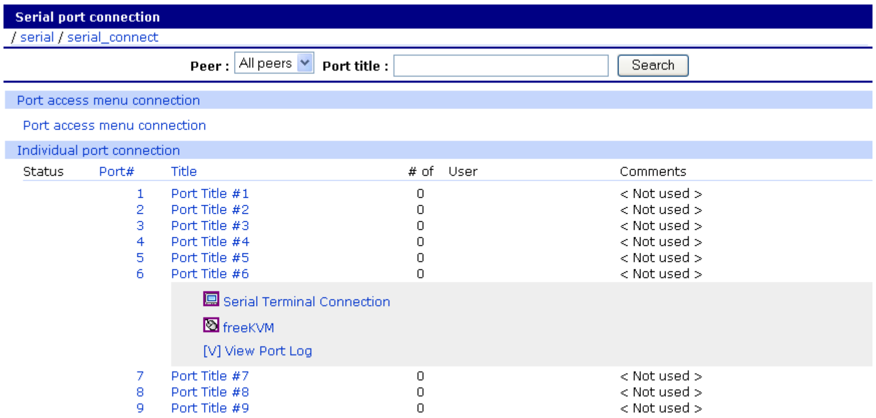
No.	User
	Nothing
New	

Any user who is added to this list can only access freeKVM on the connection page.

Connect to a System through freeKVM using Remote Desktop Protocol

When connecting through the Connection window, and a freeKVM connection is configured, these things are now displayed:

- 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.



Serial port connection

/ serial / serial_connect

Peer : All peers Port title :

Port access menu connection

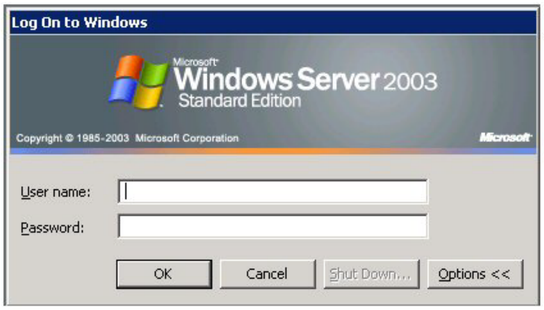
Port access menu connection

Individual port connection

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 freeKVM [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 >

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 a message that the connection succeeded is displayed. This login screen is displayed:



Log On to Windows

Copyright © 1985-2003 Microsoft Corporation

User name:

Password:

4. Enter user name and password, and click **OK**.

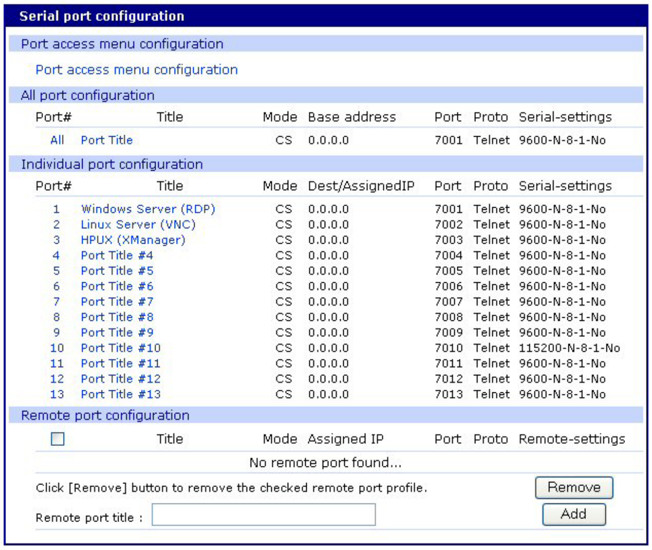
If the application does not start, check to make sure that the application is in the search path on the server. See "Installing Programs for freeKVM" on page 179.

Use freeKVM with VNC Protocol

This section describes how to configure freeKVM with the VNC Protocol, and connect to a system through freeKVM using VNC.

Configure freeKVM with VNC Protocol

1. Access the Digi Passport Web interface and log in.
2. Select **Serial Port > Configuration**. This window is displayed:



Serial port configuration

Port access menu configuration

Port access menu configuration

All port configuration

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

Individual port configuration

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

Remote port configuration

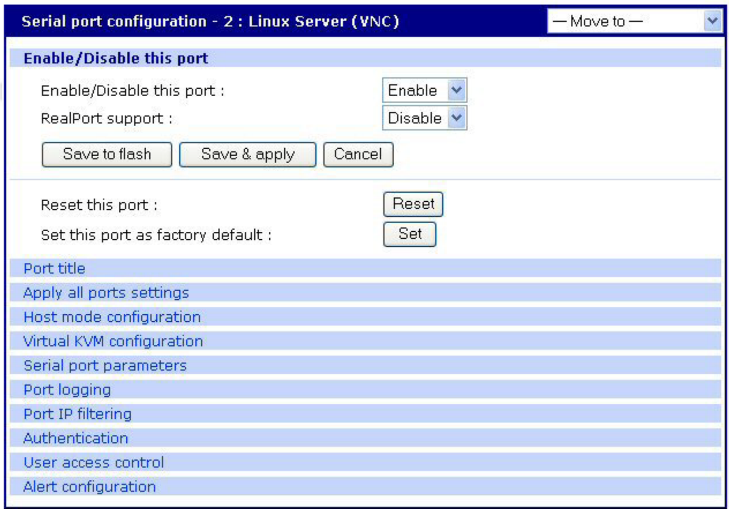
□	Title	Mode	Assigned IP	Port	Proto	Remote-settings

No remote port found...

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

Remote port title :

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



Serial port configuration - 2 : Linux Server (VNC)

Enable/Disable this port

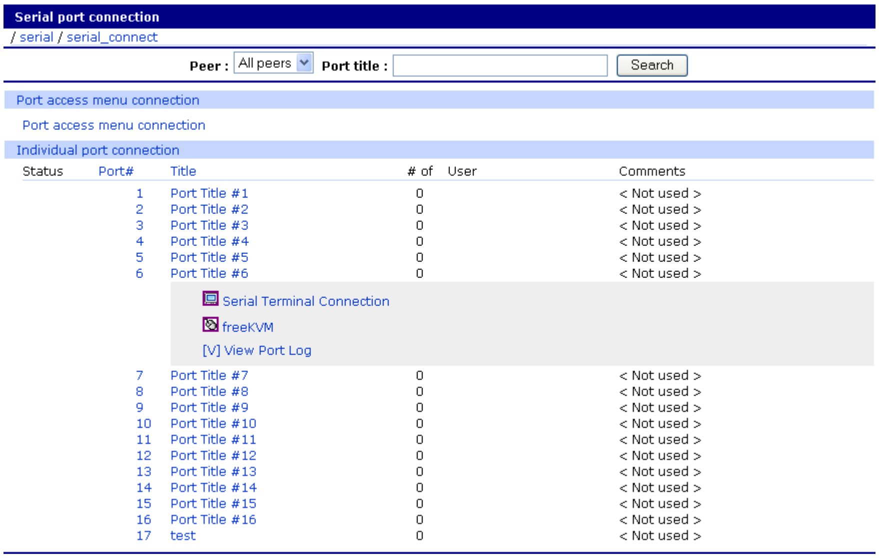
Enable/Disable this port : Enable

RealPort support : Disable

Reset this port :

Set this port as factory default :

4. Select the **freeKVM** tab. This window is displayed:



Serial port connection

/ serial / serial_connect

Peer : All peers Port title : Search

Port access menu connection

Port access menu connection

Individual port connection

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 freeKVM [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 >
	17	test	0		< Not used >

5. From the freeKVM connection pulldown list, select **Enable**.

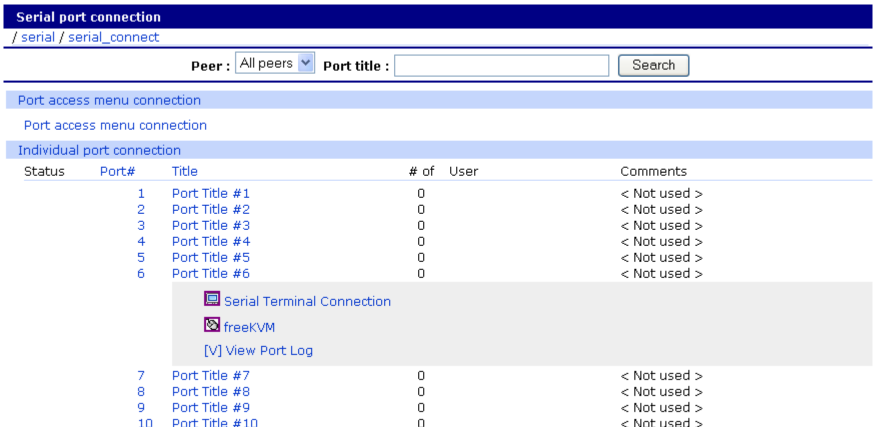
   Then, from the Client program pulldown list, select the VNC Client program.

6. Adjust the VNC socket/screen number, if necessary. The default is 1.
7. Click **Save & apply**.

Connect to a System through freeKVM using VNC

When connecting through the Connection window, and a freeKVM connection is configured, these things are displayed:

- 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.



Serial port connection

/ serial / serial_connect

Port access menu connection

Port access menu connection

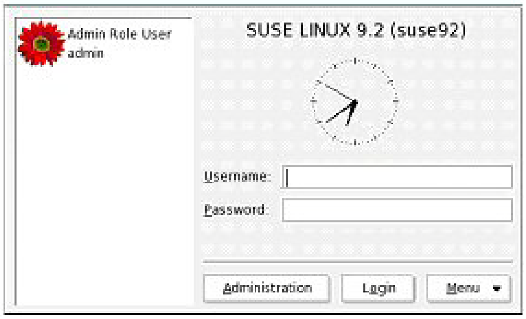
Individual port connection

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 freeKVM [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 >

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 a message that the connection succeeded is displayed. The freeKVM VNC Connection opens:



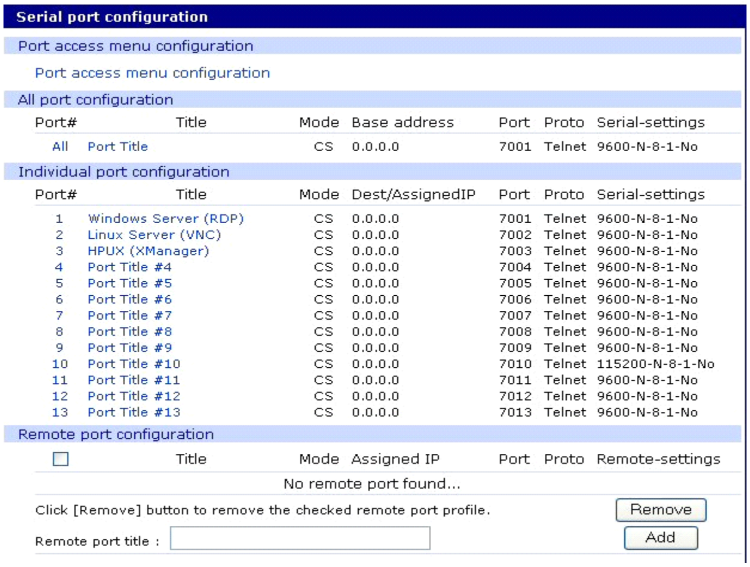
3. Enter user name and password, and click **Login**. If the application does not start, check to make sure that the application is in the search path on the server. See "Installing Programs for freeKVM" on page 179.

Use freeKVM with X Window System Protocol and XManager Software

This section describes how to configure freeKVM with X Window System Protocol and XManager software and connect to a system with it.

Configure freeKVM with X Window System Protocol

1. Access the Digi Passport Web interface and log in.
2. Select **Serial Port > Configuration**. This window is displayed.



Serial port configuration

Port access menu configuration

Port access menu configuration

All port configuration

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

Individual port configuration

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

Remote port configuration

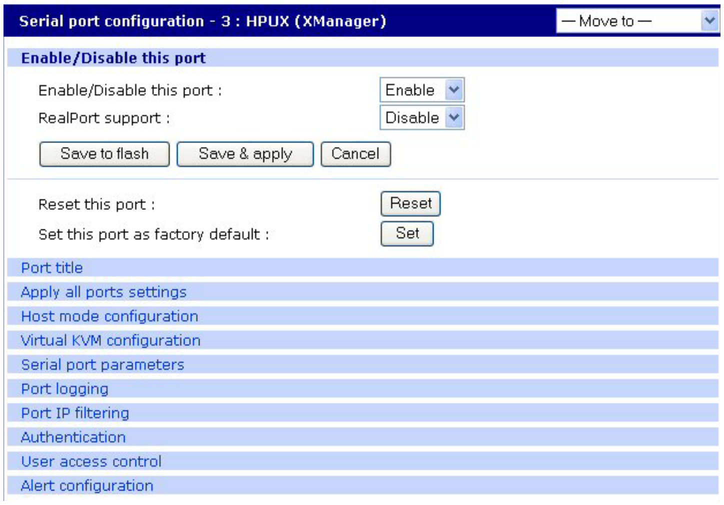
□	Title	Mode	Assigned IP	Port	Proto	Remote-settings

No remote port found...

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

Remote port title :

3. Select the port to configure. A window similar to this one is displayed, showing the serial port number and title:



Serial port configuration - 3 : HPUX (XManager)

Enable/Disable this port

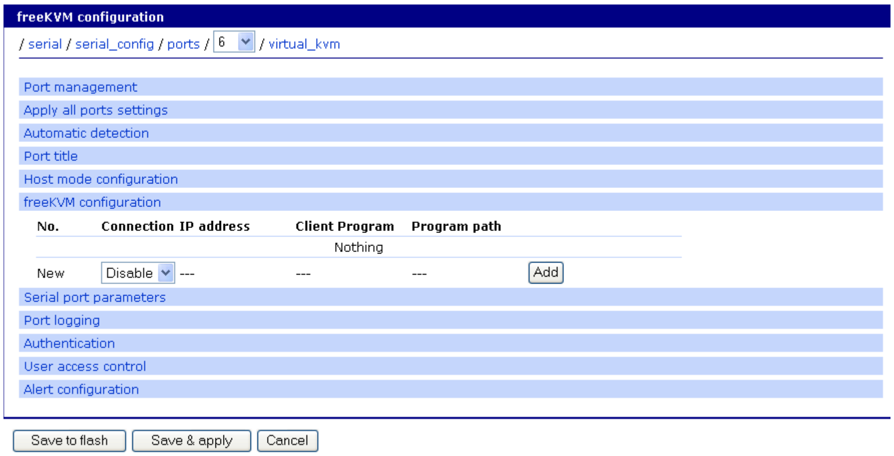
Enable/Disable this port : Enable

RealPort support : Disable

Reset this port :

Set this port as factory default :

4. Select **freeKVM configuration**. This window is displayed:



freeKVM configuration

/ serial / serial_config / ports / 6 / virtual_kvm

- Port management
- Apply all ports settings
- Automatic detection
- Port title
- Host mode configuration
- freeKVM configuration

No.	Connection	IP address	Client Program	Program path	
			Nothing		
New	Disable	---	---	---	Add

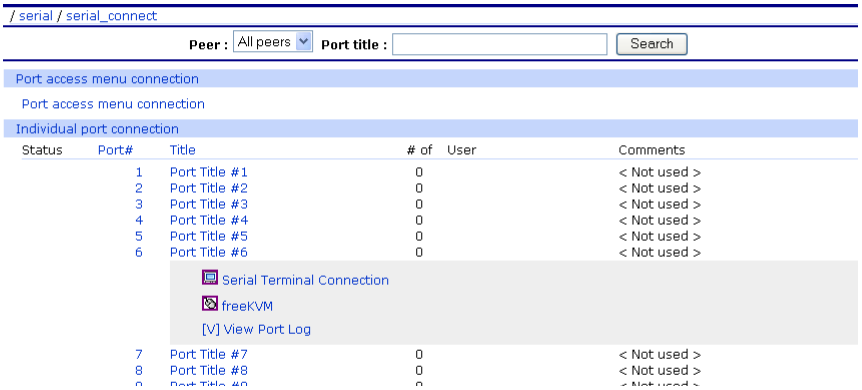
- Serial port parameters
- Port logging
- Authentication
- User access control
- Alert configuration

5. From the **freeKVM connection** pulldown list, select **Enable**.
6. From the **Client** program pulldown list, select the **Xmanager** program.
7. Click **Save and Apply**.

Connect to a system through freeKVM using Xmanager

When connecting through the Connection window, and a freeKVM connection is configured, these things are displayed:

- 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.



/ serial / serial_connect

Peer : All peers Port title : Search

Port access menu connection

Port access menu connection

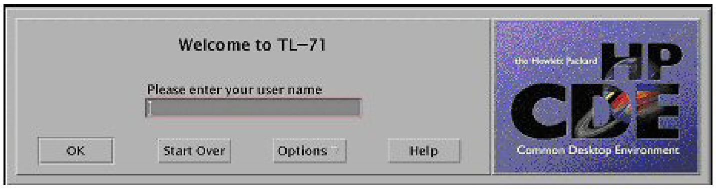
Individual port connection

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 freeKVM [V] View Port Log			
	7	Port Title #7	0		< Not used >
	8	Port Title #8	0		< Not used >

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

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

   The application starts, and a message that the connection succeeded is displayed. The freeKVM VNC Connection is displayed:



Welcome to TL–71

Please enter your user name

3. Enter 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 the server. See "Installing Programs for freeKVM" on page 179.

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, for example:

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 when using freeKVM.

Check software levels and install software as needed

Some general software considerations:

- Because the freeKVM is launched by a Java applet, Java must be installed on the Workstation and in a browser.
- Regardless of the software package, make sure that the server has support for that package enabled.

Remote Desktop Protocol

Required Software

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 the software 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 the user path on the Linux/Unix server.

Usage Notes

Applications management and most diagnostics can be performed 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 a Windows Server 2003 System, right-click on **My Computer** and select **Properties** > **Remote** > **Enable Remote Desktop on this Computer**.

VNC Viewer

Required Client Software

Windows:

- TightVNC from **http://www.tightvnc.com/**
- RealVNC software from **http://www.realvnc.com/**
- UltraVNC from **http://www.ultravcn.com/**

Linux: vncviewer from the VNC client software package for the distribution.

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

Usage Notes

Follow the distribution-specific instructions for enabling VNC support on the 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 put the files in the toolkit into a directory in your path. A good default is **%WINDIR%**; usually, this maps to C:\Windows).

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

Xmanager

Required Client Software

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

Usage Notes

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

Make sure the X Window System is configured to allow for remote connections from the Client workstation’s IP address.

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

Chapter 12 Rackable® Systems Management Card

About the Rackable Systems Management Card

Rackable® Systems manufactures a management card that is built into some of their servers. This card 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, the card allows control functions from the server independently of the main processor, including

- 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.

Rackable Systems Management Card Configuration

To configure the serial port to provide access to the Rackable Systems Management console:

1. Access the Digi Passport unit’s web interface.
2. Select **Serial Port > Configuration**.
3. Select a port.
4. Select **Host mode configuration**. The Host mode configuration page is displayed.
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. From the menu, select **Serial port parameters** .
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

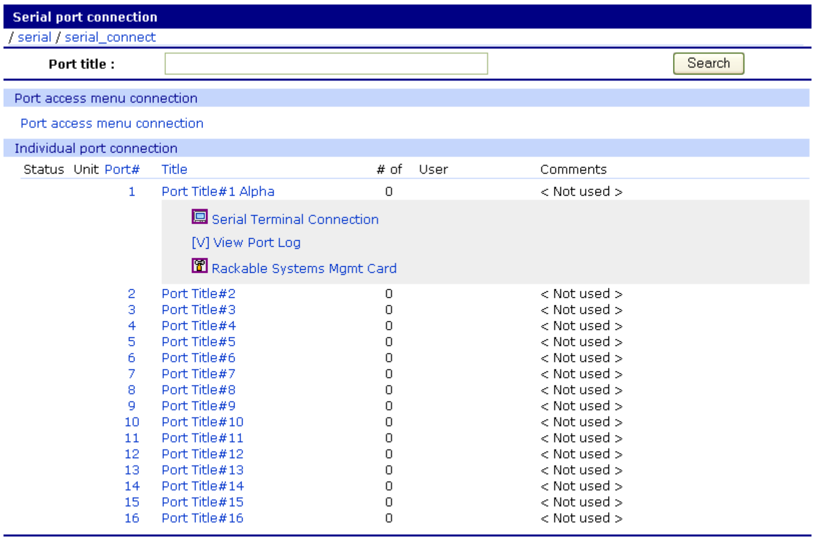
3. Click **Save & apply**.

Assign a Port Name

1. From the menu, select **Port title**.
2. Enter a port title.
3. Click **Save & apply**.

Access Rackable Systems Management Card from Digi Passport GUI

1. Access the Digi Passport unit’s web interface.
2. Select **Serial Port > Connection**. A screen similar to the following is displayed.



Serial port connection

/ serial / serial_connect

Port title :

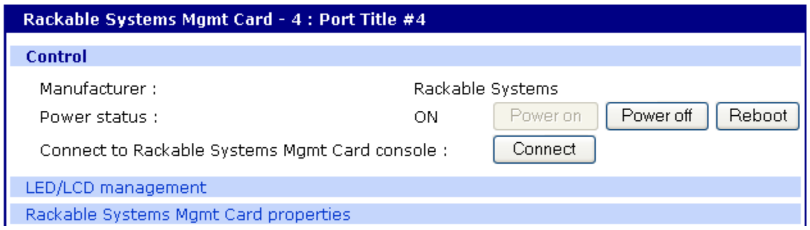
Port access menu connection

Port access menu connection

Individual port connection

Status	Unit	Port#	Title	# of	User	Comments
		1	Port Title#1 Alpha	0		< Not used >
			Serial Terminal Connection [V] View Port Log Rackable Systems Mgmt Card			
		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. Click on the **Rackable Server** link. A screen similar to the following is displayed.



Rackable Systems Mgmt Card - 4 : Port Title #4

Control

Manufacturer : Rackable Systems

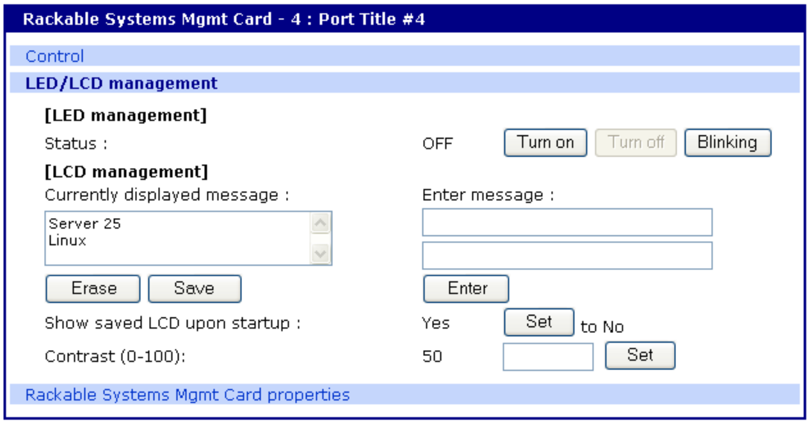
Power status : ON

Connect to Rackable Systems Mgmt Card console :

LED/LCD management

Rackable Systems Mgmt Card properties

4. Use the Digi Passport unit's user interface to perform Rackable Systems Management Card functions. Attributes of the user interface controls are shown below and described in the following table.



Rackable Systems Mgmt Card - 4 : Port Title #4

Control

LED/LCD management

[LED management]

Status : OFF

[LCD management]

Currently displayed message :

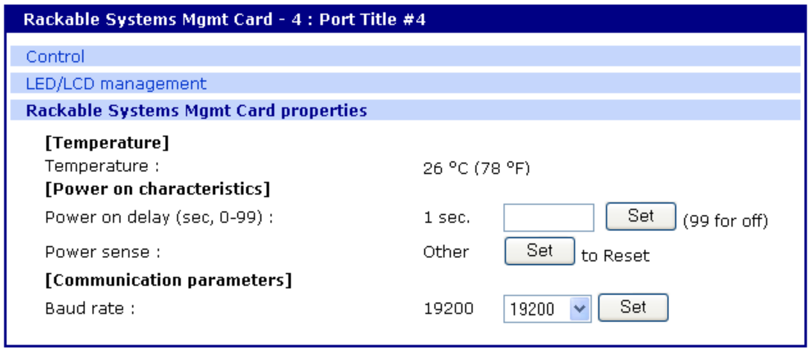
Server 25
Linux

Enter message :

Show saved LCD upon startup : Yes — Set to No

Contrast (0-100): 50

Rackable Systems Mgmt Card properties



Rackable Systems Mgmt Card - 4 : Port Title #4

Control

LED/LCD management

Rackable Systems Mgmt Card properties

[Temperature]

Temperature : 26 °C (78 °F)

[Power on characteristics]

Power on delay (sec, 0-99) : 1 sec. — Set (99 for off)

Power sense : Other — Set to Reset

[Communication parameters]

Baud rate : 19200 — 19200 — Set

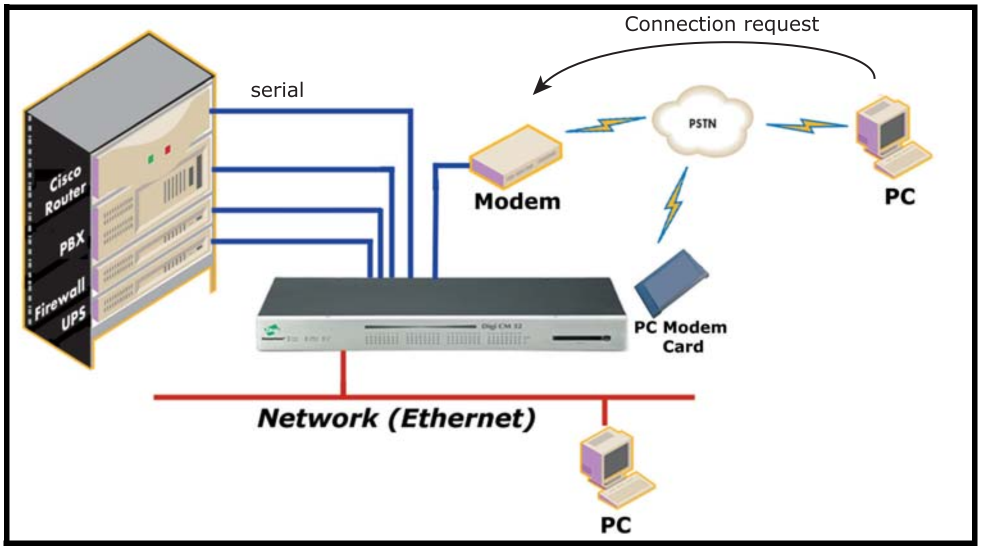
Rackable Systems Management Card Properties and Controls

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. Depending 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/LCD Mgmt:	
LED Management	Controls 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 Management:	
Currently displayed message	Shows the message currently displayed on the LCD display.
Erase	Clears the LCD display. The saved message stays saved to flash.
Save	Save currently displayed message to flash memory.
Show saved LCD message upon startup	The first columns shows the current status: Yes or No. This parameter defines which message is displayed upon startup of the server, either the saved message or the standard: “**Rackable Systems Phantom Vx.xx**”.
Contrast	Sets a contrast for the LCD panel. The default is 50, the range is 0 – 100.
Rackable Systems Mgmt Card properties	
Temperature	Indicates current temperature inside the Rackable Systems Server.
Power on characteristics:	
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 parameters:	
Baud Rate	Configures 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.

Configure Remote Dial-In Access

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. When dialing 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.

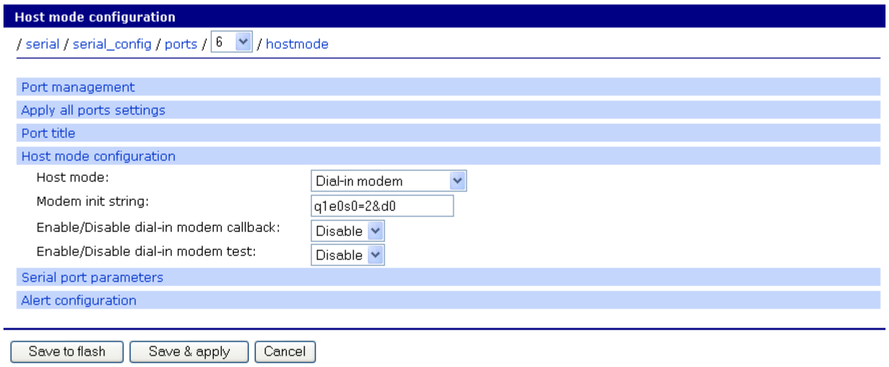
For more information on the different types of Host mode configuration, see "Host Mode Configuration" on page 71.



Configure for Dial-In Modem Access

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

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port > Configuration**.
3. Under Individual port configuration, select a specific port and then select **Host mode configuration**.
4. For the Host mode, select **Dial-in modem**.
5. Fill in the appropriate fields as needed.



Host mode configuration

/ serial / serial_config / ports / 6 / hostmode

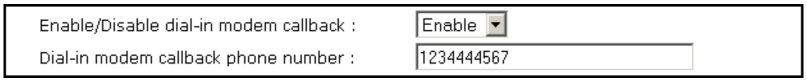
Host mode: Dial-in modem

Modem init string: q1e0s0=2&d0

Enable/Disable dial-in modem callback: Disable

Enable/Disable dial-in modem test: Disable

- **Modem init string**: The modem init string is used for initializing an external modem attached to the Digi Passport unit's serial port. The default modem init string is **q1e0s0=2**. This default init string sets the modem to quiet mode, echo off, and Auto Answer on two rings. See the modem's user manual for more information.
- **Callback**: For security reasons, the callback feature can be activated.

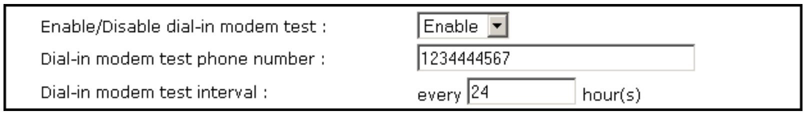


Enable/Disable dial-in modem callback : Enable

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 a phone number and an interval to be specified. 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 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. If the other modem is in use, the tests will fail.

There are multiple ways to review the information about the mode test:

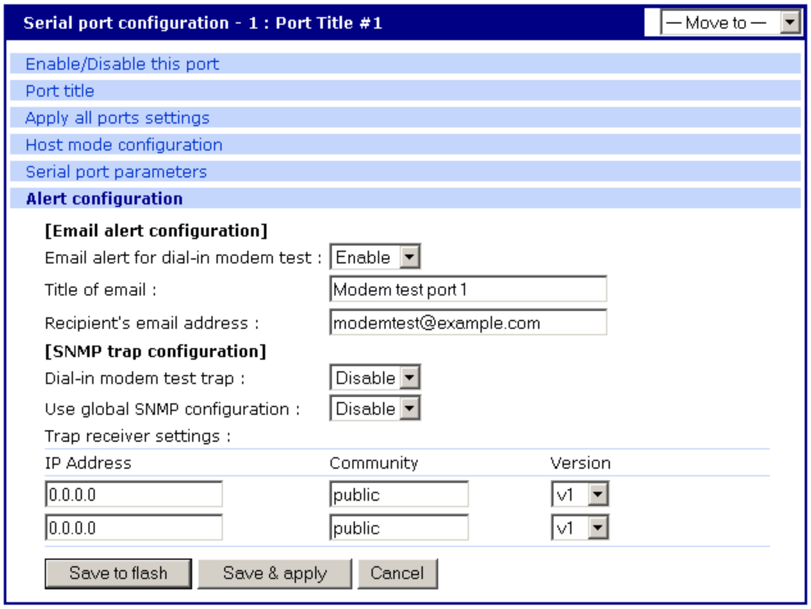
Through the syslog in the Digi Passport unit:

In this example, a modem connected to port 16 calls another modem connected to port 15. Here is how this activity is logged in the syslog. Any errors occurring are captured in the syslog file as well.

```
07-16-2004 12:45:01 > Port #16 - Modem Test started. Calling to
1234444567.

07-16-2004 12:45:22 > Modem connected through Port #15

07-16-2004 12:45:22 > Port #16 - Modem Test succeeded
```

By e-mail based notification.

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



[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

The title of the e-mail and the address can be configured.

To configure e-mail notifications, a primary SMTP server must be configured under **Network** > **SMTP configuration**.

By SNMP configuration

It is also possible to receive notifications using SNMP traps. When using SNMP traps the global settings for IP address, Community and Version can be used, or specified separately. The Trap MIB can be downloaded from support.digi.com (select the product and go to **Diagnostics, Utilities and MIBs**).

6. Click **Save & apply**.

Add 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.

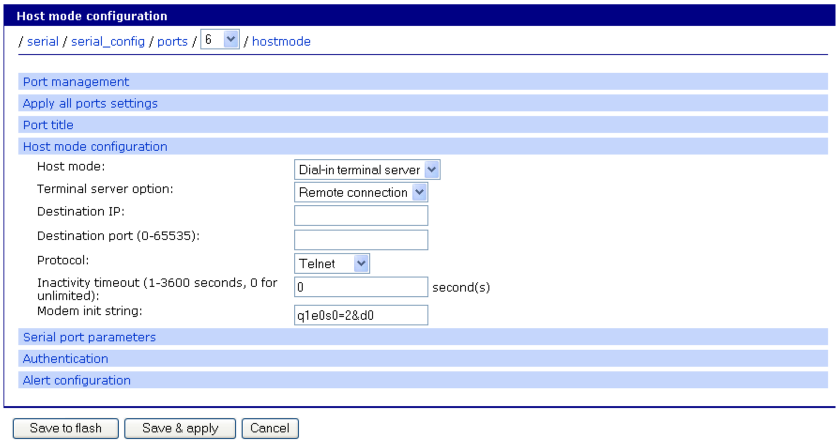
1. Insert the card into the PC slot located on the front of the device.
2. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
3. From the menu, select **PC card > Configuration**.
4. Click **Discover a new card**. The Digi Passport unit searches for a PC card and displays a configuration menu.
5. Enter the appropriate parameters in the configuration menu.
6. Click **Save & apply**.

Configure for Dial-In Terminal Server Access

The host mode Dial-In Terminal Server is similar to the host mode Terminal Server, but also allows configuring 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 and configure dial-in terminal server access:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **Serial port > Configuration**.
3. Under Individual port configuration, select a specific port and then select **Host mode configuration**.
4. Select Dial-in terminal server for the Host mode from the pulldown menu.

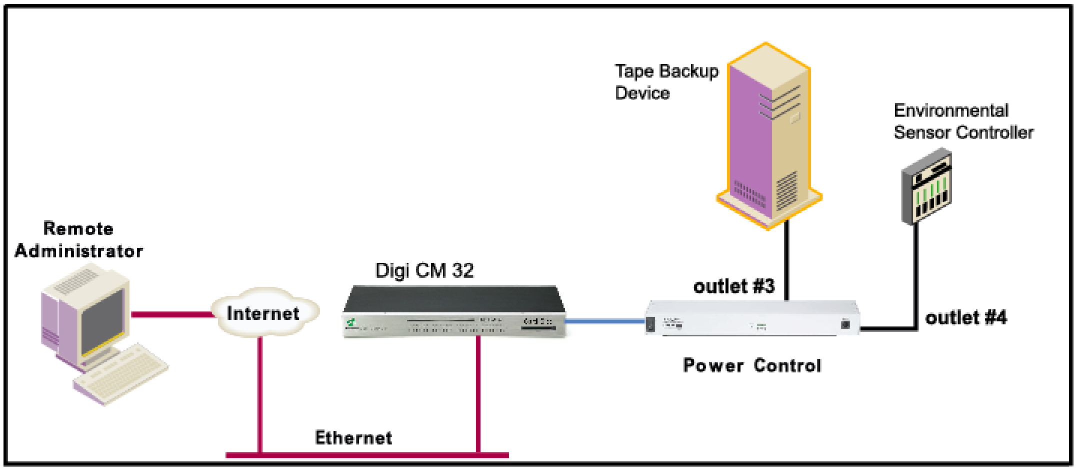


Host mode:	Dial-in terminal server
Terminal server option:	Remote connection
Destination IP:	
Destination port (0-65535):	
Protocol:	Telnet
Inactivity timeout (1-3600 seconds, 0 for unlimited):	0 second(s)
Modem init string:	q1e0s0=2&d0

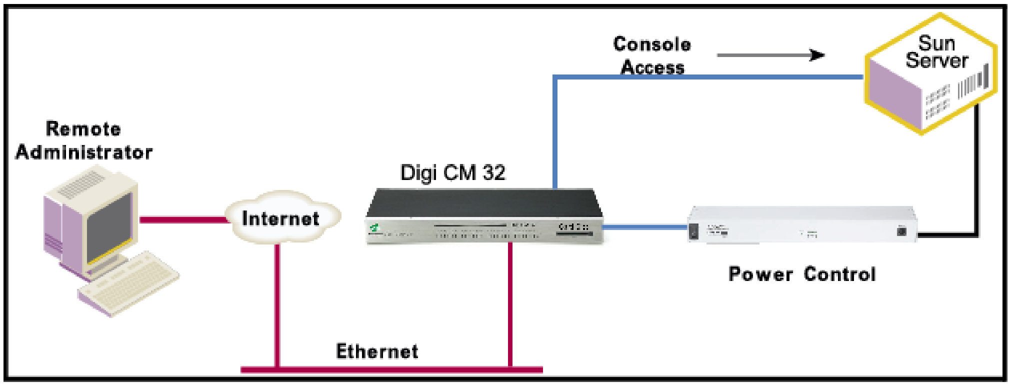
5. Configure settings as needed.
   - **Destination IP**: The IP address of the system that will be automatically connected to when the port is accessed.
   - **Destination port**: The TCP port that used when the port is automatically connected to a system on the network.
   - **Protocol**: The protocol 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 the desired init string.
6. Click **Save & apply**.

About the Power Controller Feature

The Power Controller feature allows 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, power is managed by connecting to the console management port on the Digi Passport unit. The Power Controller feature handles the relationship of a specific outlet to a serial device as if the power supply were also connected to the same port as the serial device. In other words, it is not necessary to view the physical connection or remember which outlet controls a specific serial device after configuration, because the Digi Passport unit performs those actions. The illustration shows a Sun server configured through a serial port connection on the Digi Passport 32.



Install 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 connecting multiple power controllers, set up all of them as described before proceeding. For details configuring the Digi RPM unit for cascading, see "Cascading Multiple Digi RPM Units" on page 202.

If using any other manufacturer of power controllers, see "Serial Port Cabling" on page 302 for more information.

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

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, see "Cascading Multiple Digi RPM Units" on page 202.

Configure Power Controller

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

Configure the Serial Port Parameters to Match the Power Controller

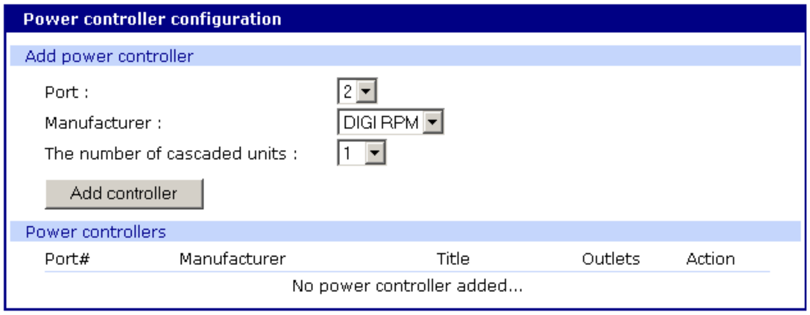
1. Log in to the Digi Passport unit (username **root**, password **dbps**).
2. Click **Serial port** > **Configuration**.
3. Select the port number of the serial port to connect to the power controller.
4. Select the **Serial port parameters**. Default serial port parameters are:

Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None
DTR behavior	High when open

5. Click **Save & apply**.
6. Continue by adding the power controller.

Add the Power Controller

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



Power controller configuration

Add power controller

Port : 2

Manufacturer : DIGI RPM

The number of cascaded units : 1

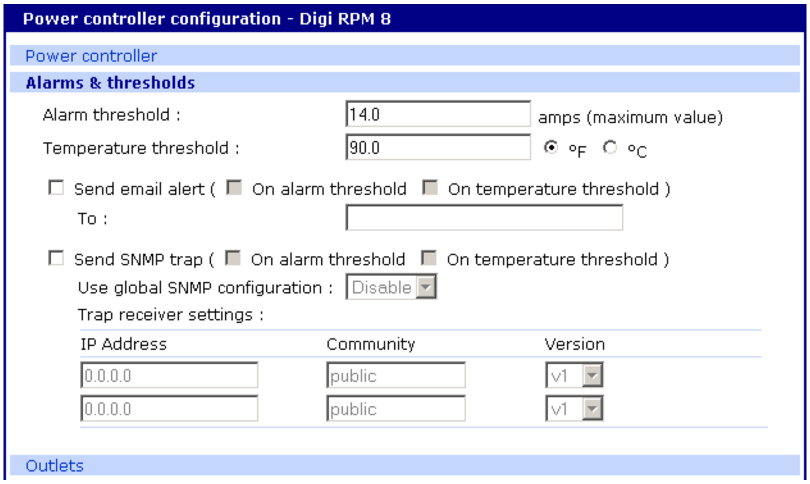
Power controllers

Port#	Manufacturer	Title	Outlets	Action
No power controller added...				

3. Select the port number of the serial port to connect to the power controller(s), manufacturer of the power controller, and the number of units to be cascaded. **1** means that one unit will be connected; that is, no cascading. The number of cascaded units cannot be changed later. Make sure all power controllers are connected before proceeding. The default title is the manufacturer brand and the port number to which it is connected. This title can be changed in step 5 if needed.
4. Click **Add controller**.
5. After the controller is detected automatically, correct the number of ports, or edit the port title as needed.
6. Click **Save & apply**.
7. Continue by setting the alarms and thresholds.

Set Alarms and Thresholds

The Power Controller can be set to issue an alert via E-mail notification or an SNMP trap when environmental conditions exceed specifications.



Power controller configuration - Digi RPM 8

Power controller

Alarms & thresholds

Alarm threshold : 14.0 amps (maximum value)

Temperature threshold : 90.0 ● °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 : Disable

Trap receiver settings :

IP Address	Community	Version
0.0.0.0	public	v1
0.0.0.0	public	v1

Outlets

1. On the **Power Controller Configuration** page, 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).

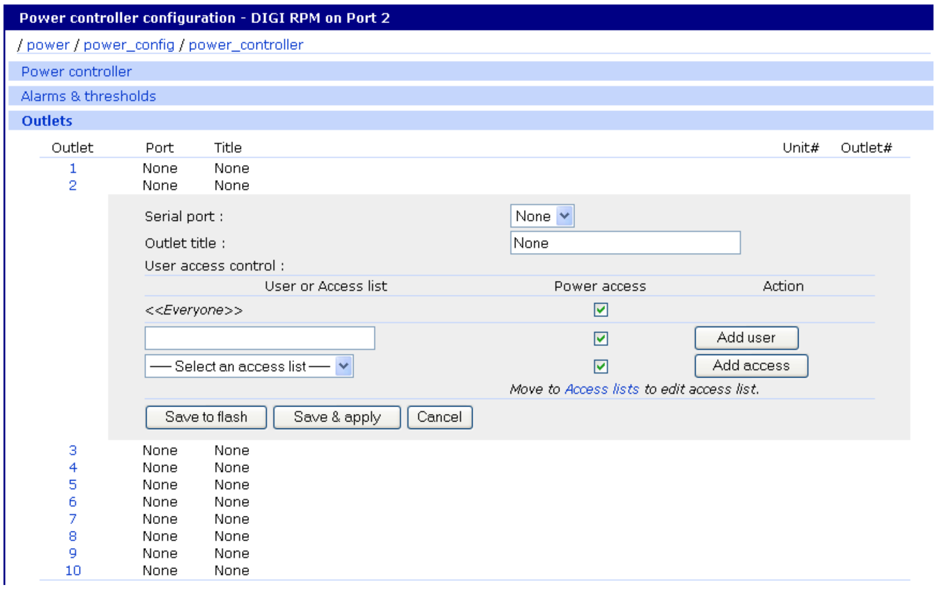
   If multiple power management units are cascaded, the alarm threshold is set for the sum of all outlets.

   To set up an E-mail alert, a mail server is required. If the mail server has not already been configured, see "Configure SMTP Alerts" on page 108. If the SMTP server is not set up, the E-mail option is not available.
3. Click **Save & apply**.
4. Continue by configuring the outlets.

Configure Outlets

To configure the power supplied to the device from the power controller, follow these steps.

1. Under **Power controller**, click **Outlets**.
2. Click the outlet number to configure.



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		

Serial port : None

Outlet title : None

User access control :

User or Access list	Power access	Action
<<Everyone>>	☑	
	☑	Add user
—— Select an access list ——	☑	Add access

Move to Access lists to edit access list.

Save to flash | Save & apply | Cancel

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

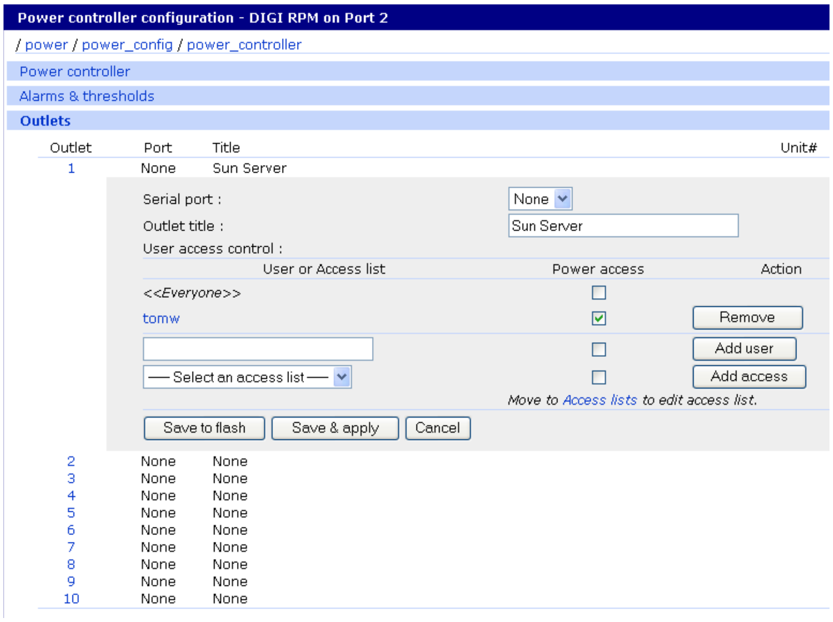
3. Select the serial port number that controls the device connected to the Digi Passport unit (if any). If the port number has a title, it will appear.

   To add a title or change the existing title, go to **Serial port > Configuration** and select the port number to be changed. Enter the title and click **Save & apply**. To continue, go to **Power Controller > Configuration > Title > Outlets** and select the appropriate outlet.

4. If not selecting a serial port number, user access parameters can be changed on this page. Enter the User Access Control parameters - see "User Access for Power Controller" on page 198.
5. Click **Save to flash** and repeat steps 2- 4 for each outlet to configure.

6. Click **Save & apply**.

   This screen 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 this example, user **tomw** has access to the power outlets.



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	

Serial port : None

Outlet title : Sun Server

User access control :

User or Access list	Power access	Action
<<*Everyone*>>	□	
tomw	☑	Remove
	□	Add user
—— Select an access list ——	□	Add access

Move to Access lists to edit access list.

Save to flash | Save & apply | Cancel

Outlet	Port	Title	Unit#
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	

7. To select the parameters for the User Access Control, click the **User Access** link. Users can be granted 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 198.

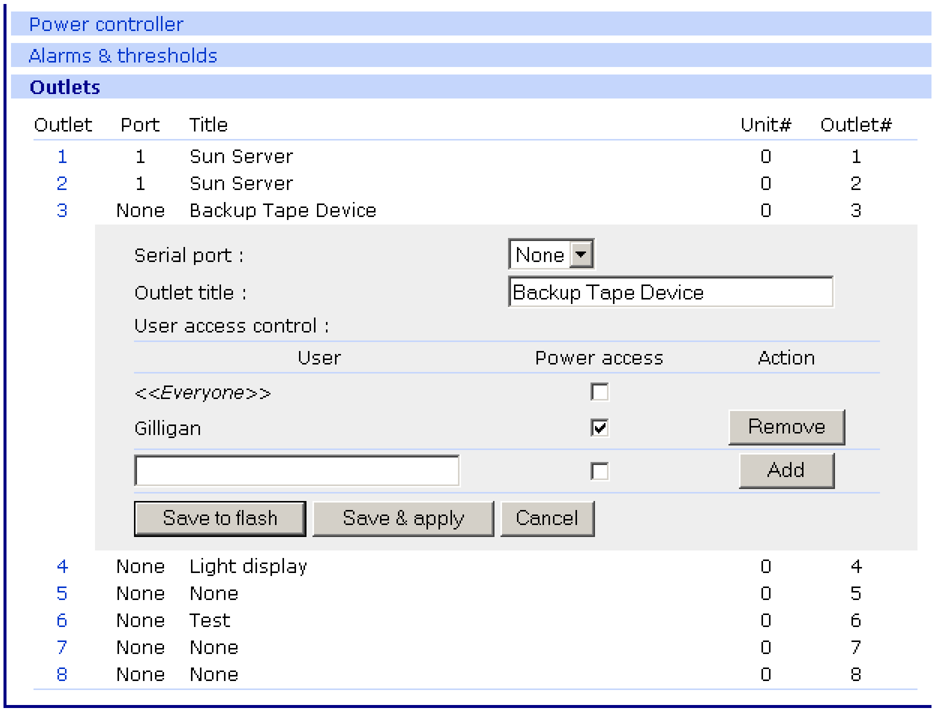
User Access for Power Controller

The Digi Passport unit can be configured to allow all 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 per-outlet basis. User Access to a serial device that is connected to the power controller in configured under **Serial Port > Configuration > Port # > User Access**.

Configure to Allow Specific Users Access

To configure the Digi Passport unit for specific users, deselect access for **<<Everyone>>** and add 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** > ***outlet number 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**, deselect the type of power access and click **Save to flash**.
7. Enter the user that will have access and check the Access type: **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.



Outlet	Port	Title	Unit#	Outlet#
1	1	Sun Server	0	1
2	1	Sun Server	0	2
3	None	Backup Tape Device	0	3

Serial port : None

Outlet title : Backup Tape Device

User access control :

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

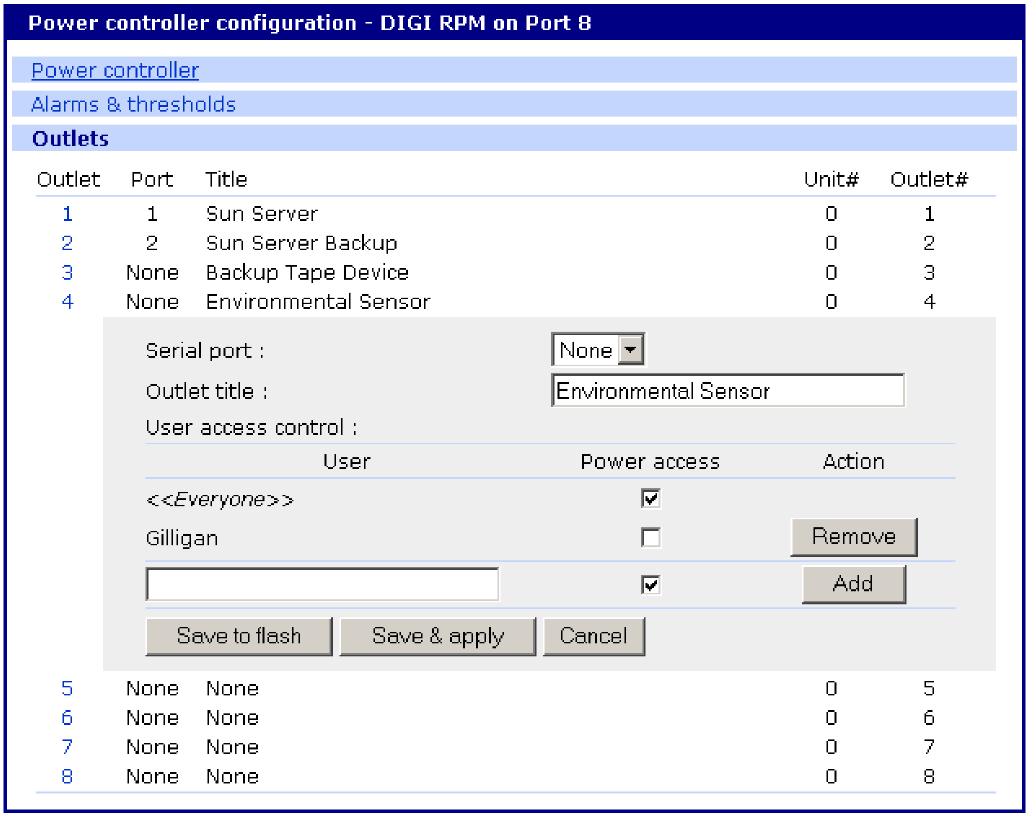
Outlet	Port	Title	Unit#	Outlet#
4	None	Light display	0	4
5	None	None	0	5
6	None	Test	0	6
7	None	None	0	7
8	None	None	0	8

Configure to Restrict Specific Users

To restrict specific users, 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. Select **Power Controller > Configuration > Outlets > *outlet number to configure***.
3. Select the port to configure to the outlet. If it is a non-serial device select None.
4. Edit the outlet title. If there is a serial port, the port title will appear and cannot be edited from this screen.
5. Click **Save & apply**.
6. Check Everyone and click **Save to flash**.
7. Enter the username that will NOT have access, deselect the Access types that are restricted, and click **Add**.
    - **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**.

The screen shows that outlets 1 and 2 control power to the Sun Server configured on port 1 of the Digi Passport unit. Outlets 3 and 4 are not serial devices. User **janl** has been designated the specific user to control outlet # 3. User **tomw** does not have access to Outlet # 4.



Power controller configuration - DIGI RPM on Port 8

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

Serial port : None

Outlet title : Environmental Sensor

User access control :

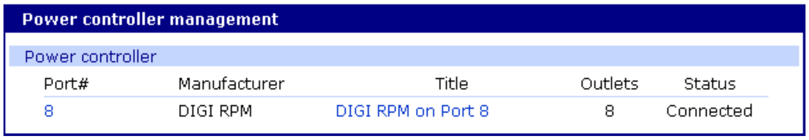
User	Power access	Action
<<*Everyone*>>	☑	
Gilligan	□	Remove
	☑	Add

Outlet	Port	Title	Unit#	Outlet#
5	None	None	0	5
6	None	None	0	6
7	None	None	0	7
8	None	None	0	8

Power Controller Management

The Power Controller Management option changes outlet settings and provides a quick update of the power controller status.

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



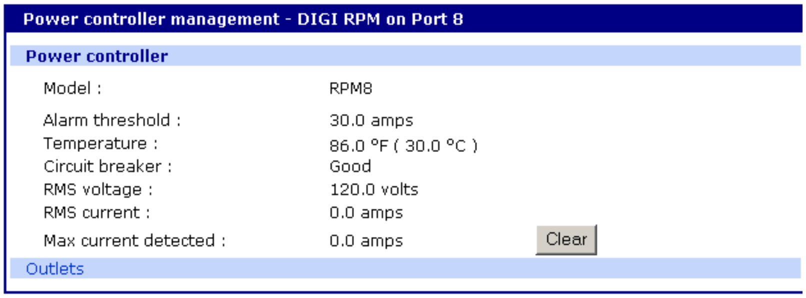
Power controller management

Power controller

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

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

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



Power controller management - DIGI RPM on Port 8

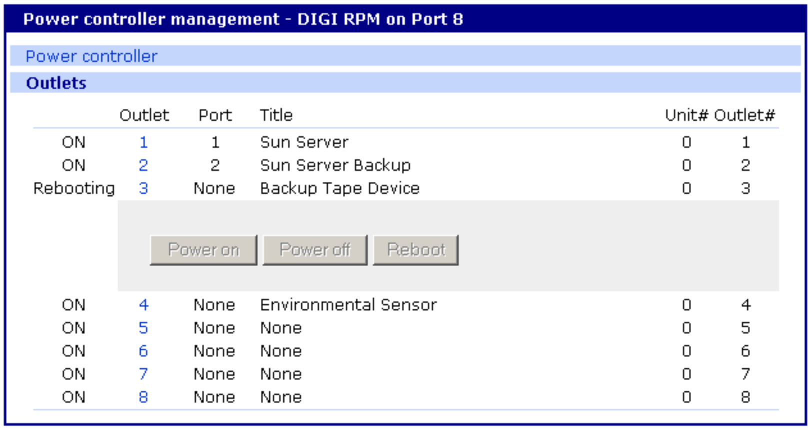
Power controller

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

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

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

3. Select the outlet number to manage. This screen shows that all the outlets are powered on and outlet 3 is rebooting. Therefore, the Backup Tape Device is power-cycling.



Power controller management - DIGI RPM on Port 8

Power controller

Outlets

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

4. Select the desired action for the outlet: **Power on**, **Power off**, or **Reboot**.

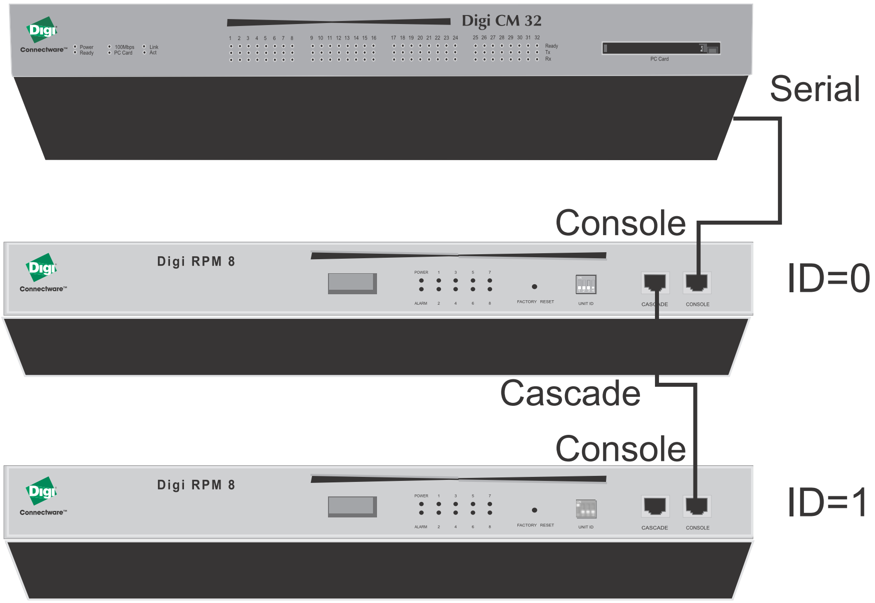
Cascading Multiple Digi RPM Units

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.

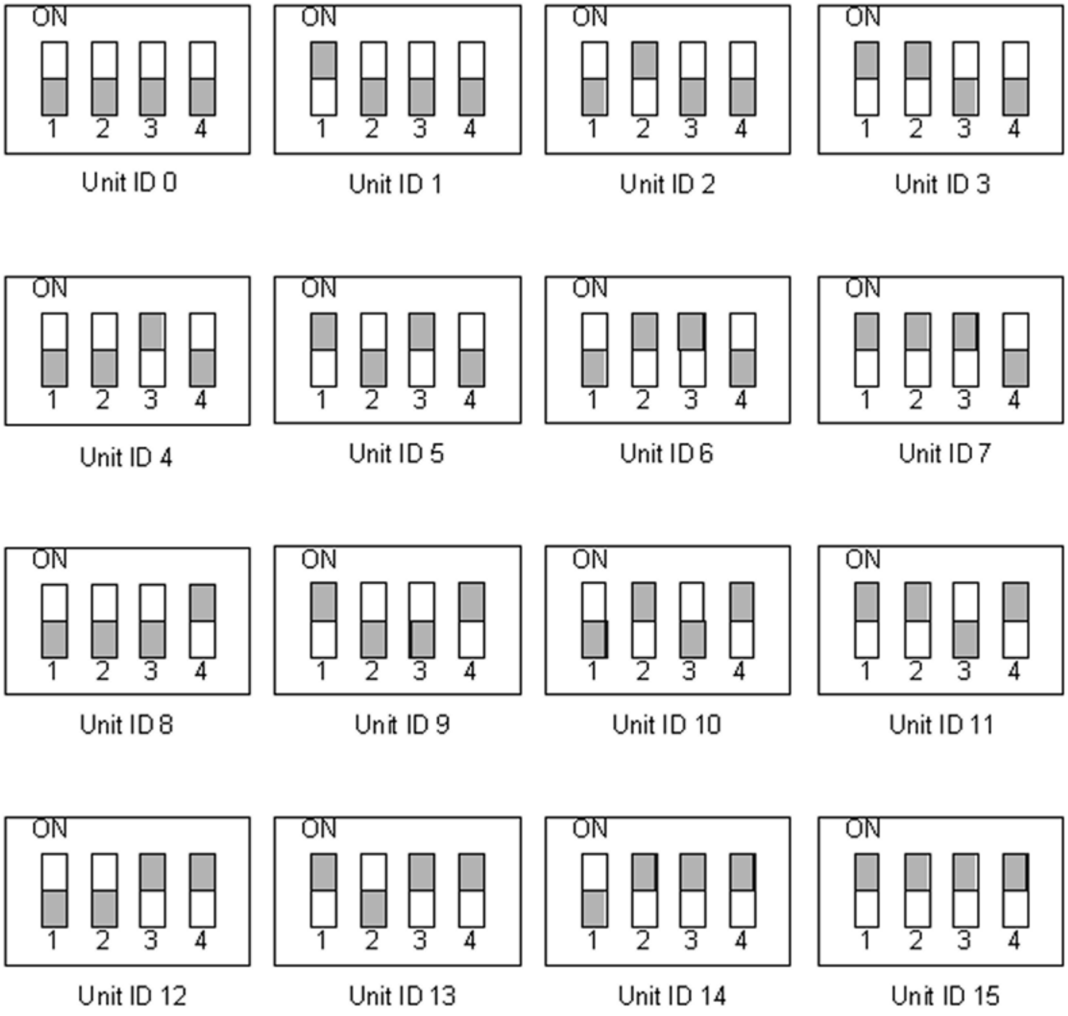
Here is an example of two cascaded Digi RPM units connected to a Digi Passport unit. Note that the ID for the first unit is set to 0 and for the second unit it is set to 1.



Allowed IDs for Digi RPM Unit

The figure shows all possible IDs that can be configured on the Digi RPM unit, and the switch settings to configure each ID.

Unit ID Switch Configuration



Managing Digi RPM from the Command Line

The Digi RPM can be managed using ASCII commands. For information about these commands, see the Digi Knowledge Base article

Quick reference to the RPM command line, at:

http://www.digi.com/support/kbase/kbaseresultdetl.jsp?id=866

Third-Party Power Controllers

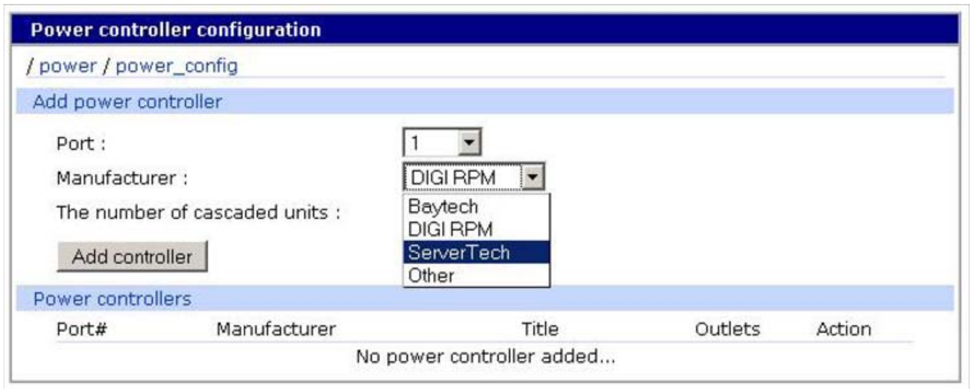
In addition to the Digi RPM power controller, Digi supports several third-party power controllers, including controllers manufactured by ServerTech and BayTech. The serial-based controllers are configured in the same manner as the Digi RPM, described previously. Additionally, Digi Passport supports ServerTech network-enabled power strips. The additional steps for configuring network-enabled power strips are described below.

Additional Configuration: Network-Enabled ServerTech Power Controller

Remote ServeTech Power Controller

To install a remote ServerTech power controller, follow the steps below.

1. In the Web go to **Power controller > Configuration** the page below will open.



Power controller configuration

/ power / power_config

Add power controller

Port : 1

Manufacturer : DIGI RPM

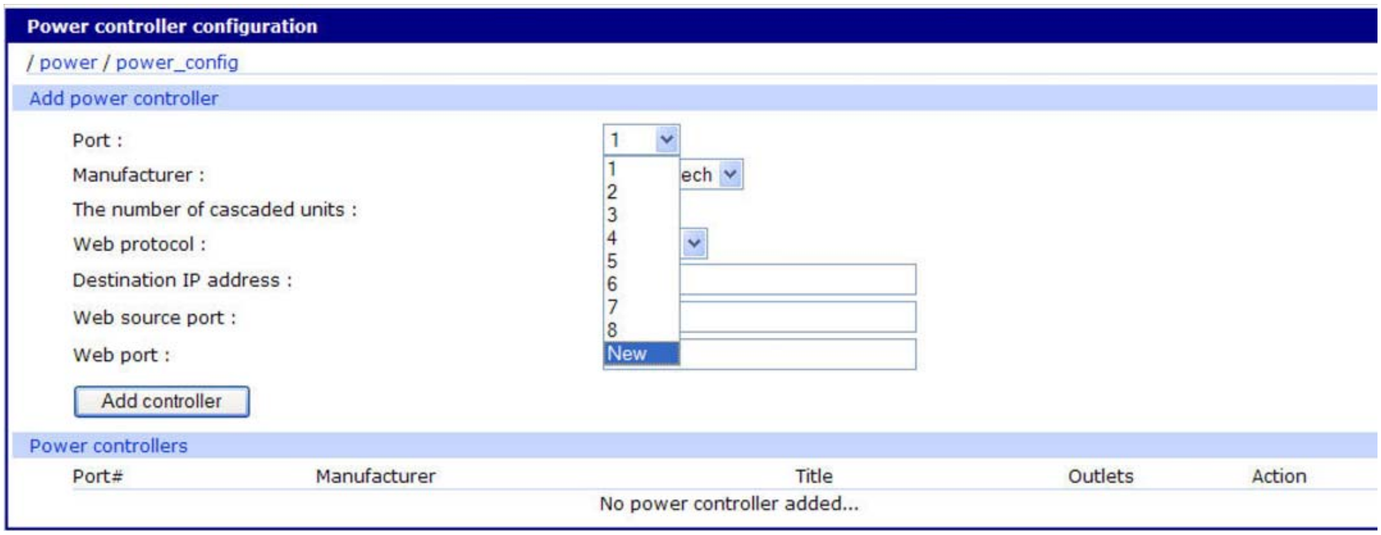
The number of cascaded units :

Power controllers

Port#	Manufacturer	Title	Outlets	Action
		No power controller added...		

2. Select **ServerTech** from the Manufacturer drop down.

3. Select **New** in Port menu list on the Add power controller page as shown below.



Power controller configuration

/ power / power_config

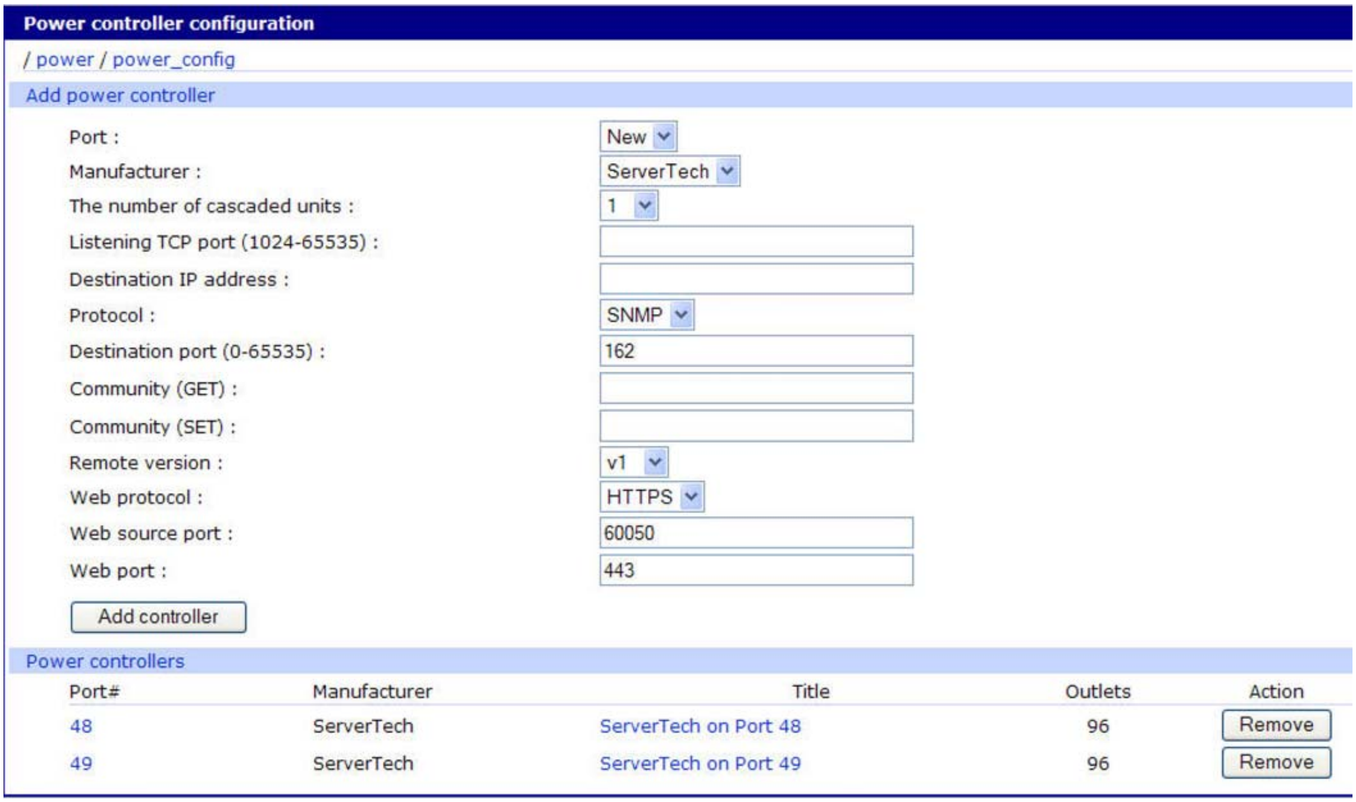
Add power controller

Port :	1
Manufacturer :	ech
The number of cascaded units :	
Web protocol :	
Destination IP address :	
Web source port :	
Web port :	

Power controllers

Port#	Manufacturer	Title	Outlets	Action
		No power controller added...		

This page below will open:



Power controller configuration

/ power / power_config

Add power controller

Port :	New
Manufacturer :	ServerTech
The number of cascaded units :	1
Listening TCP port (1024-65535) :	
Destination IP address :	
Protocol :	SNMP
Destination port (0-65535) :	162
Community (GET) :	
Community (SET) :	
Remote version :	v1
Web protocol :	HTTPS
Web source port :	60050
Web port :	443

Power controllers

Port#	Manufacturer	Title	Outlets	Action
48	ServerTech	ServerTech on Port 48	96	Remove
49	ServerTech	ServerTech on Port 49	96	Remove

4. Set the number of cascaded units.
5. Fill in the listening port (for example 7049). This will be added as a remote port.
6. Fill in the destination IP address with the IP assigned to the ServerTech device.

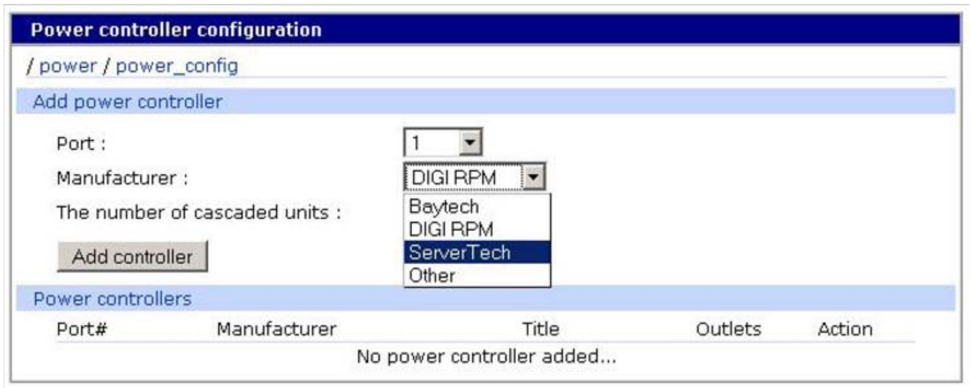
7. Set the Protocol to **SNMP**.
8. Specify the destination port number. Normally, this number is 162.
9. Specify the Get and Set community strings (by default these are public and private).
10. Set the Remote version to v1 from the drop down list.
11. Select the Web protocol.
12. Click **Add controller**.

Locally connected ServerTech power controller

To install a locally connected ServerTech power controller, follow the steps listed.

1. Connect the serial port of the ServerTech device to one of the serial ports on the Passport using a standard Ethernet cable.
2. In the Web go to **Power controller > Configuration**. The page below will open.

   After adding the Power controller a page similar to the one below will be displayed.



Power controller configuration

/ power / power_config

Add power controller

Port : 1

Manufacturer : DIGI RPM

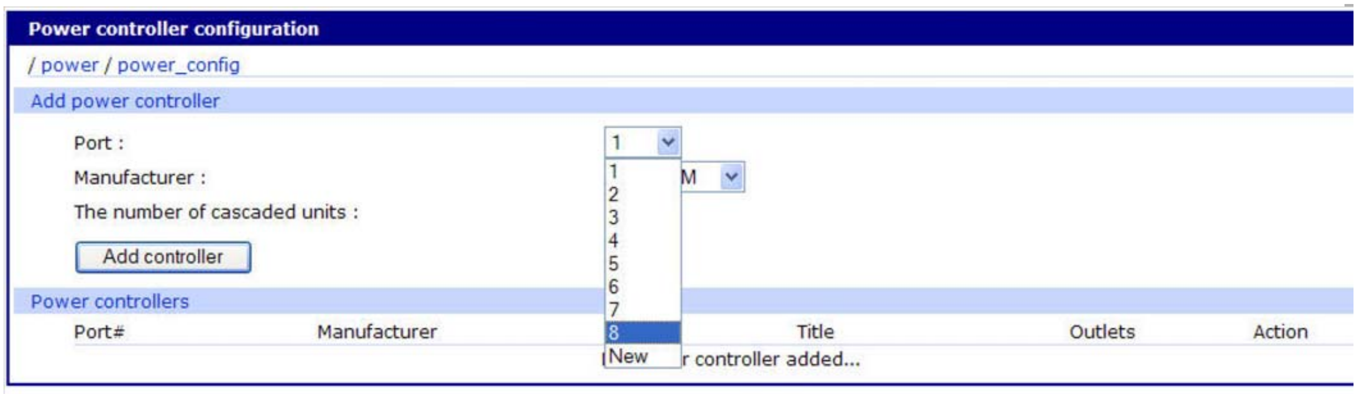
The number of cascaded units :

Power controllers

Port#	Manufacturer	Title	Outlets	Action

No power controller added...

3. Select **ServerTech** from the Manufacturer pull down.
4. Select the serial port that the device is connected to, from the Port menu list on the Add power controller page as shown below.



Power controller configuration

/ power / power_config

Add power controller

Port : 1

Manufacturer : M

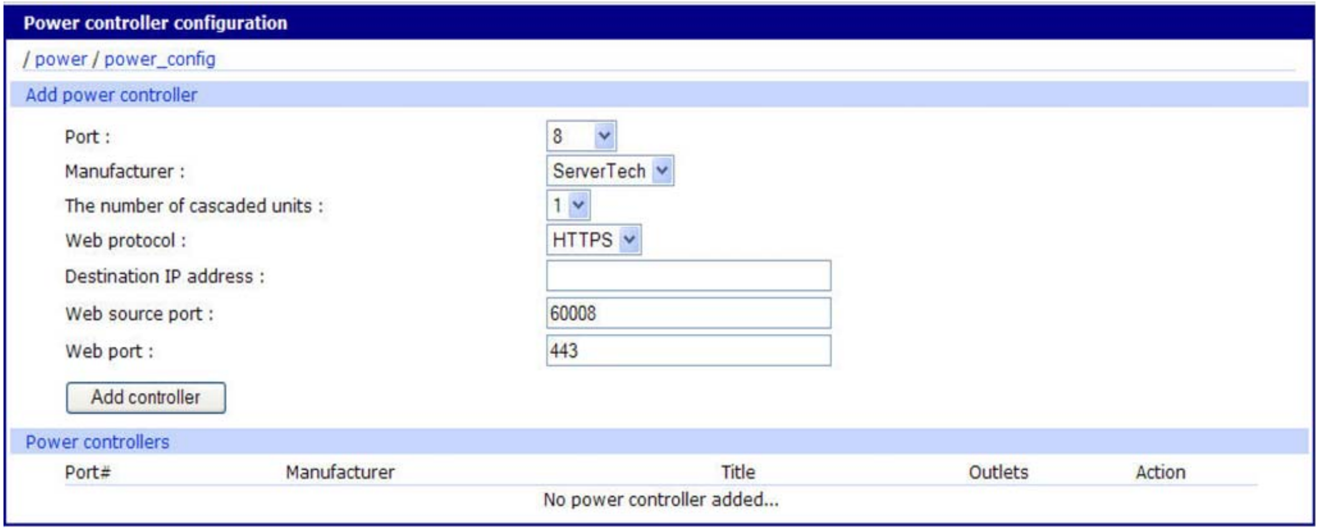
The number of cascaded units :

Power controllers

Port#	Manufacturer	Title	Outlets	Action

r controller added...

The resulting page will open.



Power controller configuration

/ power / power_config

Add power controller

Port : 8

Manufacturer : ServerTech

The number of cascaded units : 1

Web protocol : HTTPS

Destination IP address :

Web source port : 60008

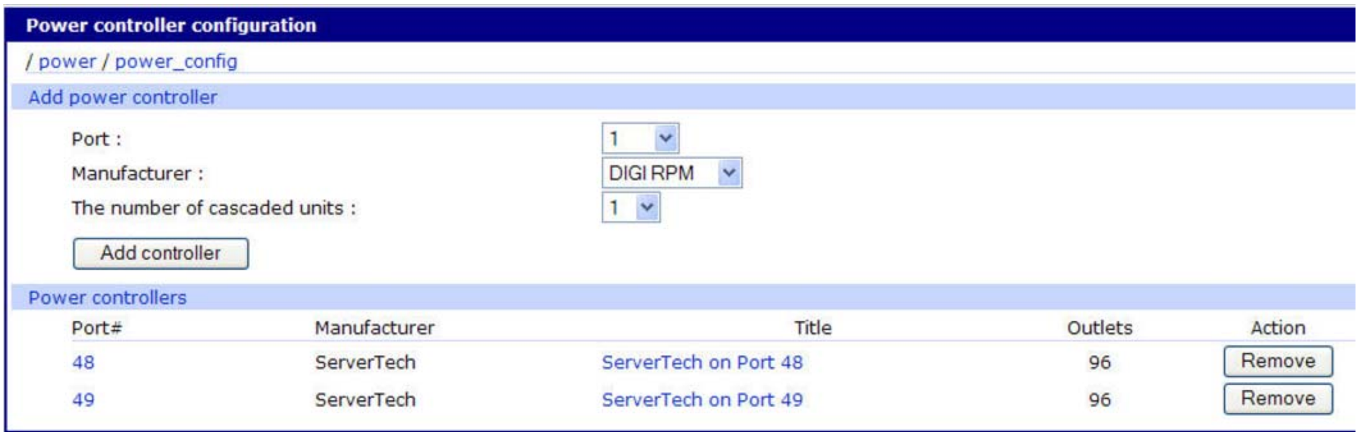
Web port : 443

Power controllers

Port#	Manufacturer	Title	Outlets	Action
		No power controller added...		

5. Set the number of cascaded units.
6. Set the web protocol.
7. Fill in the destination IP address. This is assigned to the ServerTech device.
8. Press **Add controller.**

After adding the Power controller a page similar to the one below will be displayed.



Power controller configuration

/ power / power_config

Add power controller

Port : 1

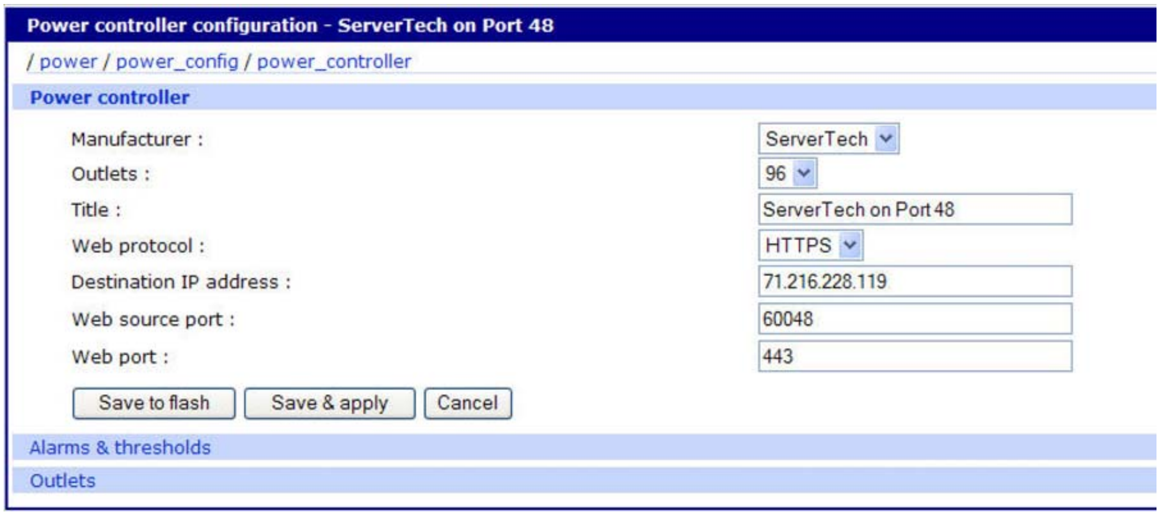
Manufacturer : DIGI RPM

The number of cascaded units : 1

Power controllers

Port#	Manufacturer	Title	Outlets	Action
48	ServerTech	ServerTech on Port 48	96	Remove
49	ServerTech	ServerTech on Port 49	96	Remove

9. To configure the outlets on the controller, select a power controller from the installed Power controllers and a new page will be displayed, similar to the one shown below.



Power controller configuration - ServerTech on Port 48

/ power / power_config / power_controller

Power controller

Manufacturer : ServerTech

Outlets : 96

Title : ServerTech on Port 48

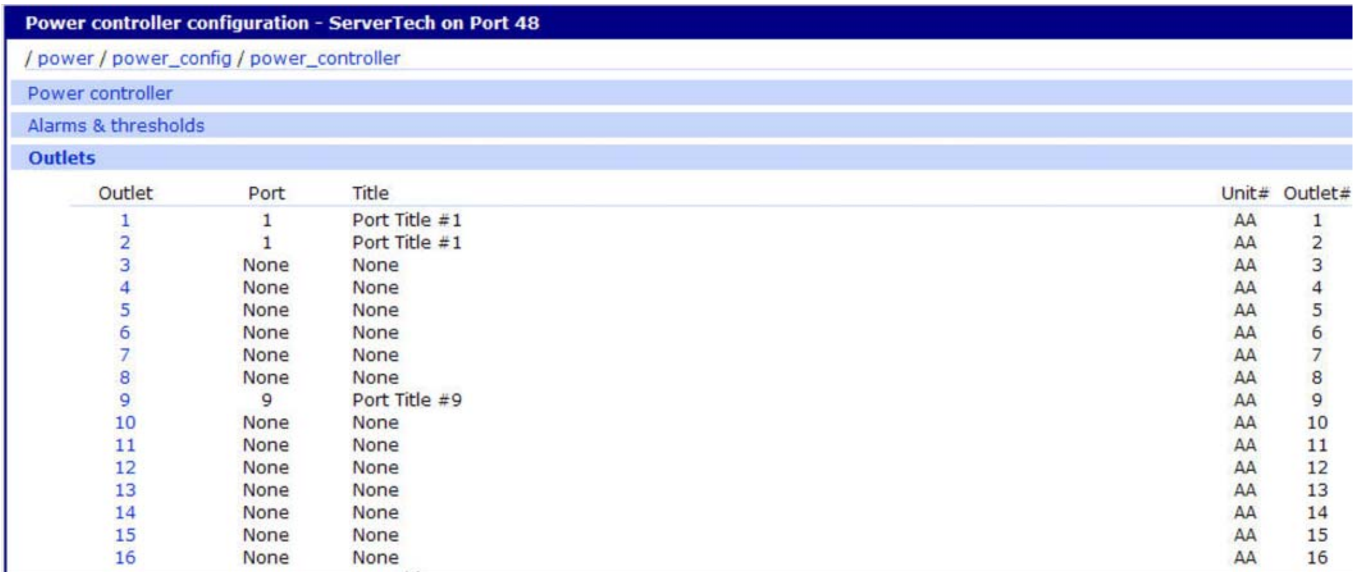
Web protocol : HTTPS

Destination IP address : 71.216.228.119

Web source port : 60048

Web port : 443

10. From this page select the **Outlets** link and a new page will be displayed, where you can configure the outlets. Select an outlet to configure.



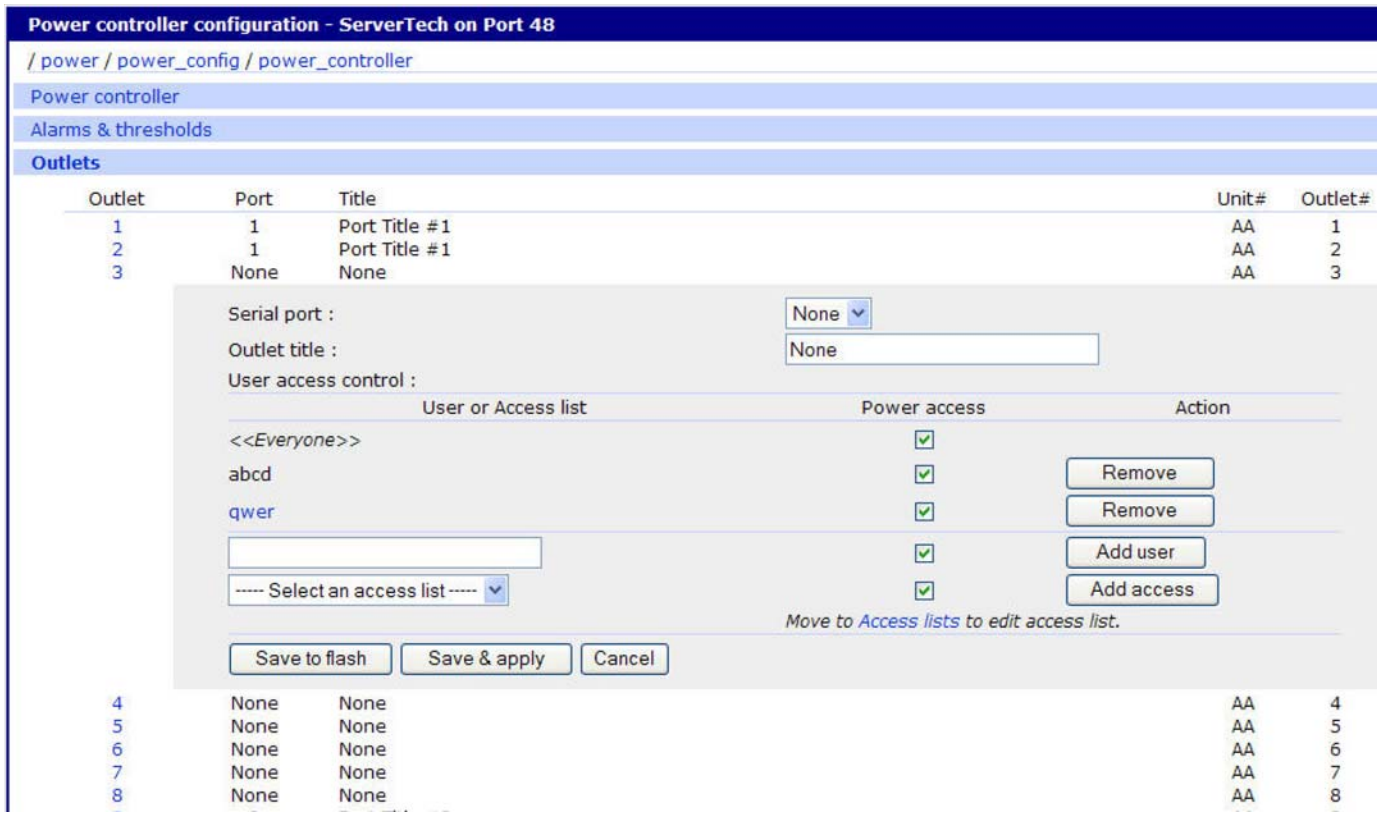
Power controller configuration - ServerTech on Port 48

/ power / power_config / power_controller

Outlets

Outlet	Port	Title	Unit#	Outlet#
1	1	Port Title #1	AA	1
2	1	Port Title #1	AA	2
3	None	None	AA	3
4	None	None	AA	4
5	None	None	AA	5
6	None	None	AA	6
7	None	None	AA	7
8	None	None	AA	8
9	9	Port Title #9	AA	9
10	None	None	AA	10
11	None	None	AA	11
12	None	None	AA	12
13	None	None	AA	13
14	None	None	AA	14
15	None	None	AA	15
16	None	None	AA	16

11. A page and similar to the following is displayed.



Power controller configuration - ServerTech on Port 48

/ power / power_config / power_controller

Power controller

Alarms & thresholds

Outlets

Outlet	Port	Title	Unit#	Outlet#
1	1	Port Title #1	AA	1
2	1	Port Title #1	AA	2
3	None	None	AA	3

Serial port : None

Outlet title : None

User access control :

User or Access list	Power access	Action
<<Everyone>>	☑	
abcd	☑	Remove
qwer	☑	Remove
	☑	Add user
----- Select an access list -----	☑	Add access

Move to Access lists to edit access list.

Save to flash | Save & apply | Cancel

Outlet	Port	Title	Unit#	Outlet#
4	None	None	AA	4
5	None	None	AA	5
6	None	None	AA	6
7	None	None	AA	7
8	None	None	AA	8

From this page you can link the outlet to a serial port, give the outlet a name and assign user access rights.

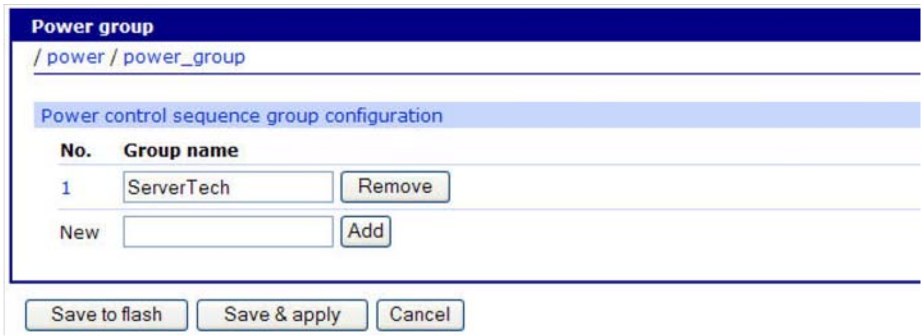
12. When you are finished configuring the outlet. select **Save & apply**.

Power groups

Power groups are groups of outlets that can be controlled at the same time.

To configure a power group:

1. In the Web UI, go to **Power controller > Power group** and the page below will be displayed.



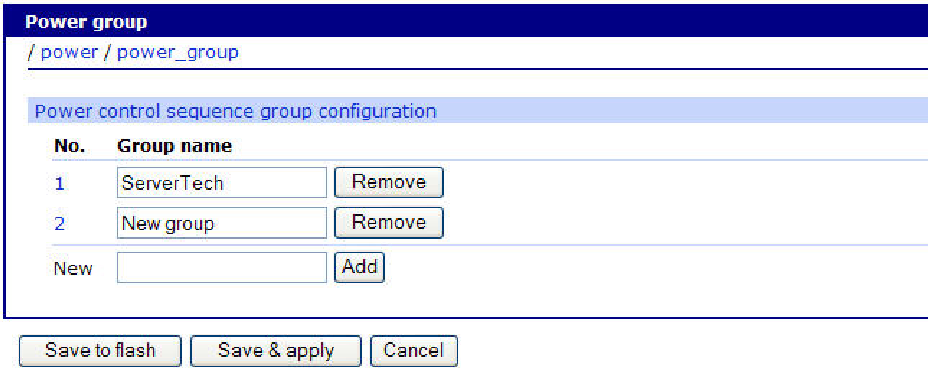
Power group

/ power / power_group

Power control sequence group configuration

No.	Group name	
1	ServerTech	Remove
New		Add

2. Enter a name for the new group and click **Add**. This page is displayed.



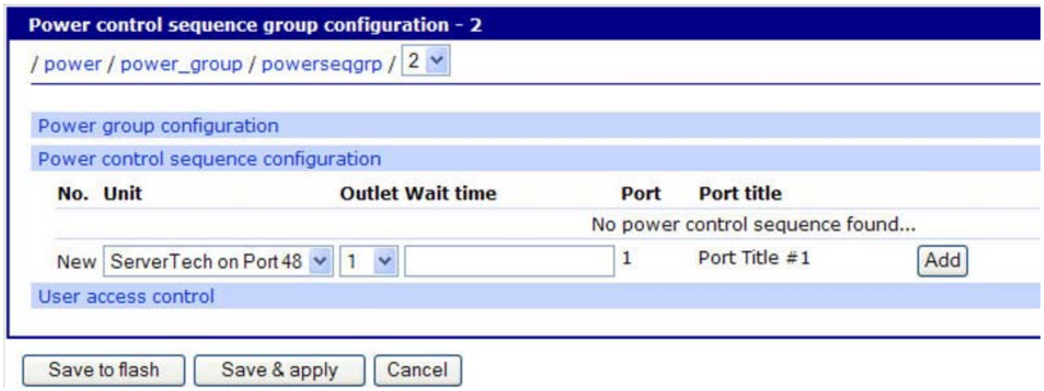
Power group

/ power / power_group

Power control sequence group configuration

No.	Group name	
1	ServerTech	Remove
2	New group	Remove
New		Add

3. To add outlets to the newly created group, select the number next to the group name. This page is displayed.



Power control sequence group configuration - 2

/ power / power_group / powerseqgrp / 2

Power group configuration

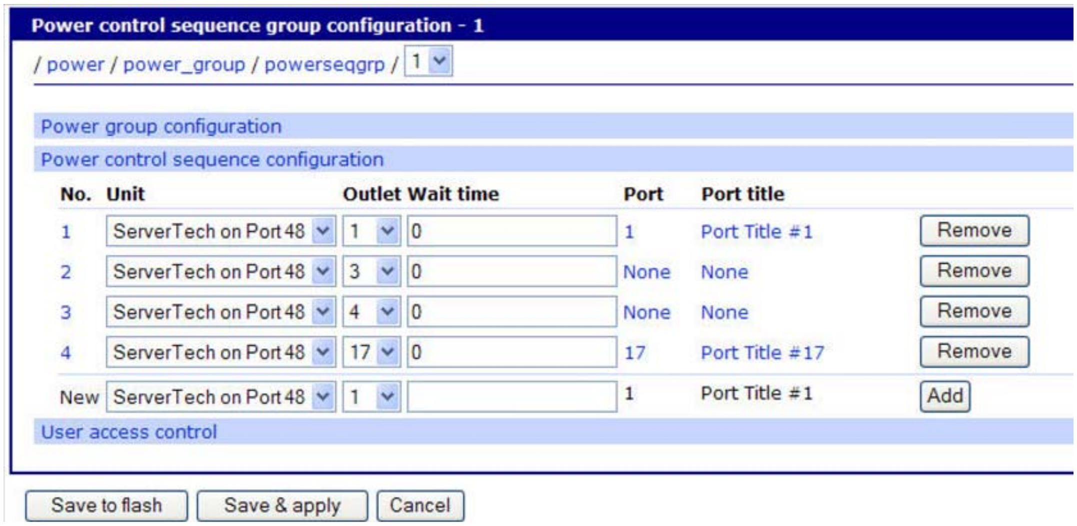
Power control sequence configuration

No.	Unit	Outlet	Wait time	Port	Port title	
				No power control sequence found...		
New	ServerTech on Port 48	1		1	Port Title #1	Add

User access control

4. Select the power controller from the drop down list.
5. Select the outlet to add to the group from the drop down list.
6. If desired, enter an outlet wait time.
7. Click **Add**.

8. Repeat steps until all outlets for this group are added.
9. Click **Save & apply**. A page similar to the one below is displayed.



Power control sequence group configuration - 1

/ power / power_group / powerseqgrp / 1

Power group configuration

Power control sequence configuration

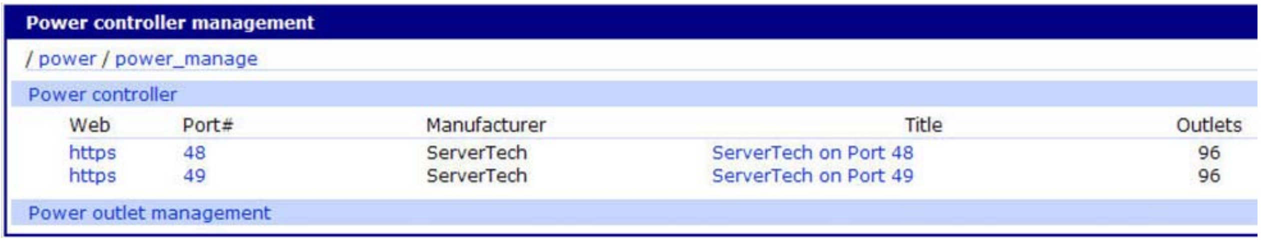
No.	Unit	Outlet	Wait time	Port	Port title	
1	ServerTech on Port48	1	0	1	Port Title #1	Remove
2	ServerTech on Port48	3	0	None	None	Remove
3	ServerTech on Port48	4	0	None	None	Remove
4	ServerTech on Port48	17	0	17	Port Title #17	Remove
New	ServerTech on Port48	1		1	Port Title #1	Add

User access control

Outlet management

To manage the outlets on the power controller:

1. In the Web UI, go to **Power controller > Manage** and the page below will be displayed.



Power controller management

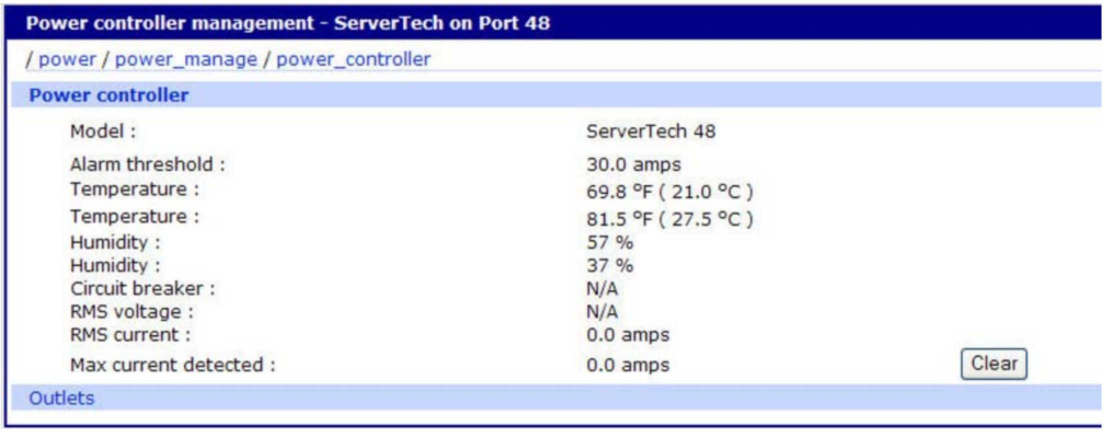
/ power / power_manage

Power controller

Web	Port#	Manufacturer	Title	Outlets
https	48	ServerTech	ServerTech on Port 48	96
https	49	ServerTech	ServerTech on Port 49	96

Power outlet management

2. From this page, you can select power controller from the list or select the Power outlet management link.
   - Selecting the Power controller https/http link from the list will result in opening the Web UI for the ServerTech device. This allows direct access to all the features on the ServerTech.
   - Selecting the Power controller title from the list will result in opening a new web page similar to the one below.



Power controller management - ServerTech on Port 48

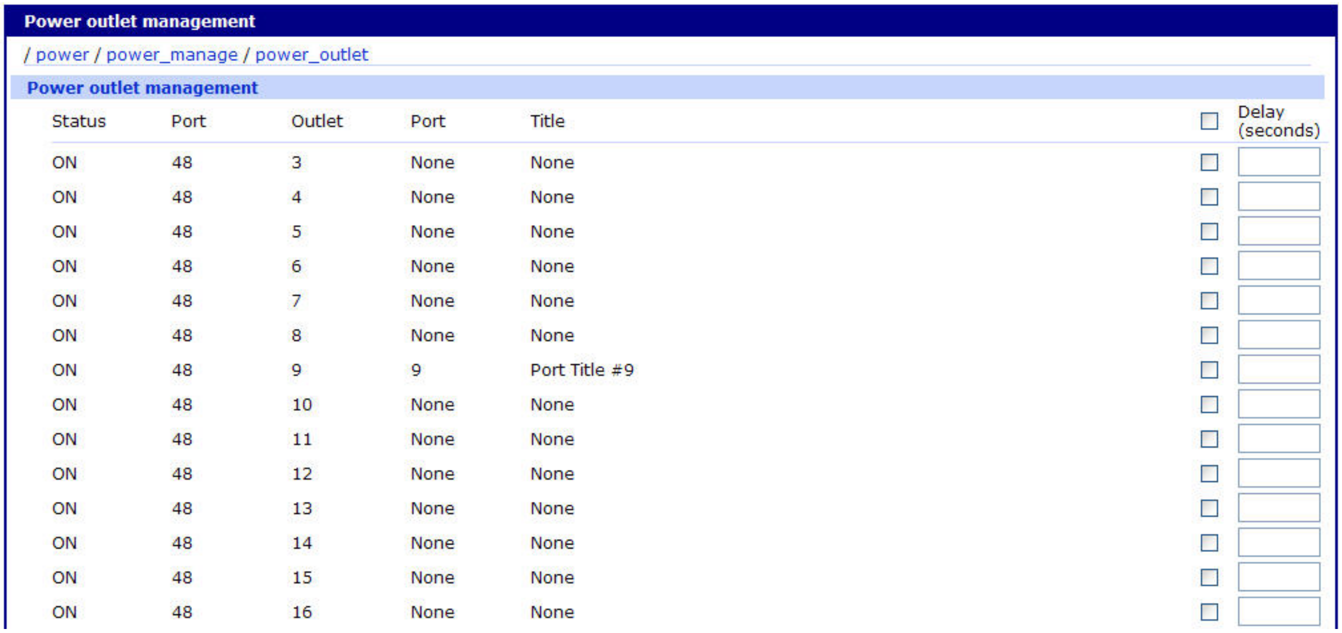
/ power / power_manage / power_controller

Power controller

Model :	ServerTech 48
Alarm threshold :	30.0 amps
Temperature :	69.8 °F (21.0 °C)
Temperature :	81.5 °F (27.5 °C)
Humidity :	57 %
Humidity :	37 %
Circuit breaker :	N/A
RMS voltage :	N/A
RMS current :	0.0 amps
Max current detected :	0.0 amps

Outlets

3.Selecting the Power outlet management link will result in a new page similar to the one shown below.



Power outlet management

/ power / power_manage / power_outlet

Power outlet management

Status	Port	Outlet	Port	Title	□	Delay (seconds)
ON	48	3	None	None	□	
ON	48	4	None	None	□	
ON	48	5	None	None	□	
ON	48	6	None	None	□	
ON	48	7	None	None	□	
ON	48	8	None	None	□	
ON	48	9	9	Port Title #9	□	
ON	48	10	None	None	□	
ON	48	11	None	None	□	
ON	48	12	None	None	□	
ON	48	13	None	None	□	
ON	48	14	None	None	□	
ON	48	15	None	None	□	
ON	48	16	None	None	□	

From this page you can manage individual outlets or manage a group of outlets.

Manage individual outlets

1. Select the outlets from the list.
2. Select **Power on**, **Power off** or **Reboot**.

Manage a group of outlets

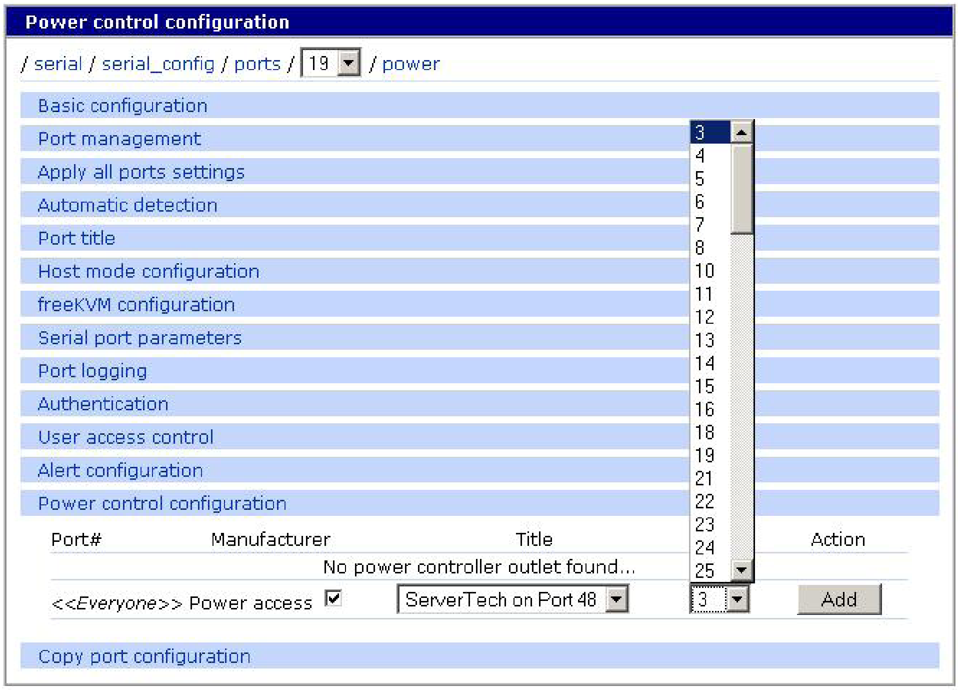
1. Select the power group from the drop down list.
2. Select **Power on**, **Power off** or **Reboot**.

Associate Power outlets with specific serial ports

Go to **Serial Port > Configuration**.

1. Choose **Advanced Power Control Configuration**.
2. Choose the serial port that you want associated with a power outlet.
3. Choose the power outlet to associate.
4. Click **Add.**
5. If there are multiple outlets, add the next outlet.

6. Click **Save & Apply.**



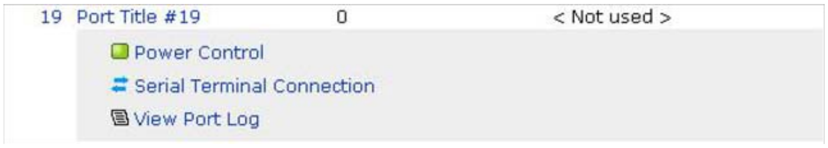
Power control configuration

/ serial / serial_config / ports / 19 / power

Port#	Manufacturer	Title		Action
No power controller outlet found...				
<<*Everyone*>> Power access ☑		ServerTech on Port 48	3	Add

Connect to the port

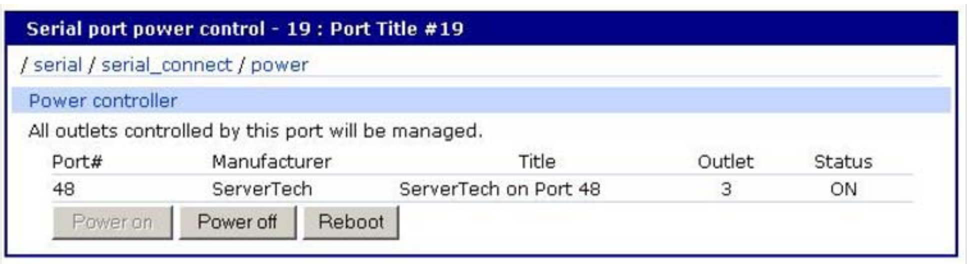
To connect to the port, choose **Serial Port > Connection** and choose the port number.



19 Port Title #19 0 < Not used >

You can either control the power through the web interface by clicking on the Power control button or through the serial console connection by clicking on the serial terminal connection and then using the port menu key.

Power Control Screen:



Serial port power control - 19 : Port Title #19

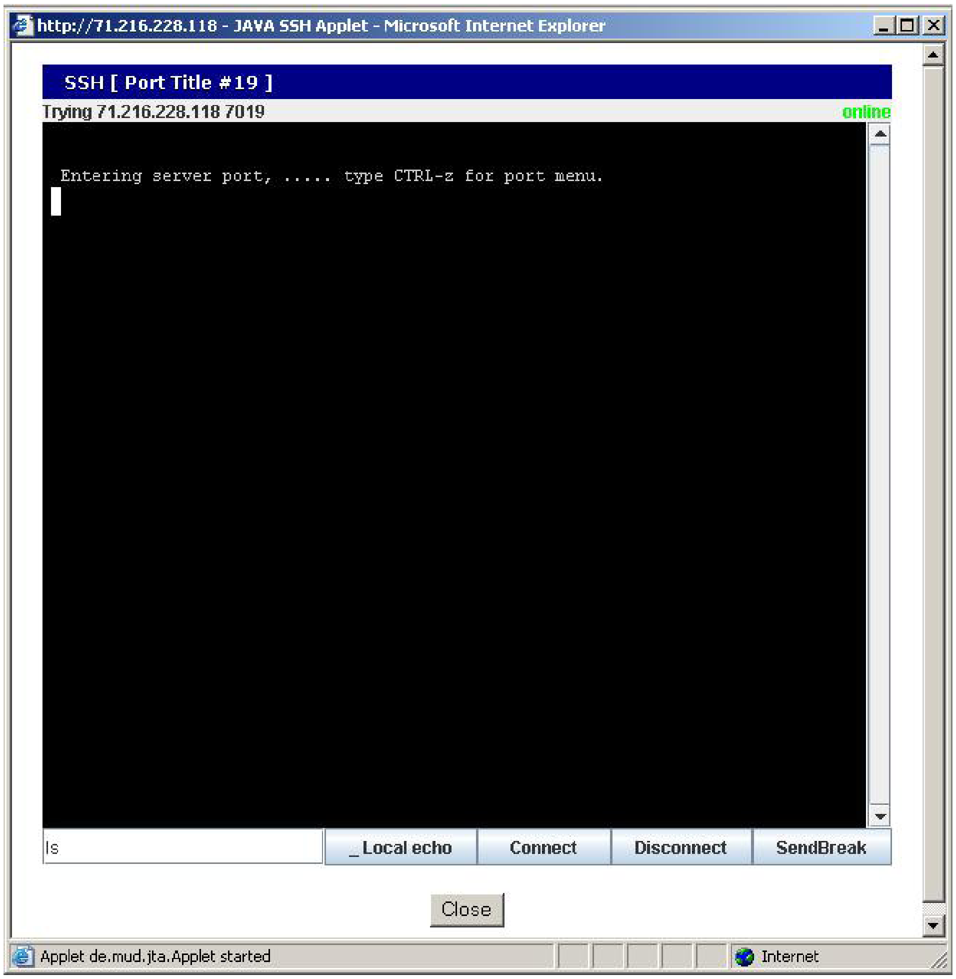
/ serial / serial_connect / power

Power controller

All outlets controlled by this port will be managed.

Port#	Manufacturer	Title	Outlet	Status
48	ServerTech	ServerTech on Port 48	3	ON

Serial Console Screen:



http://71.216.228.118 - JAVA SSH Applet - Microsoft Internet Explorer

SSH [Port Title #19]

Trying 71.216.228.118 7019

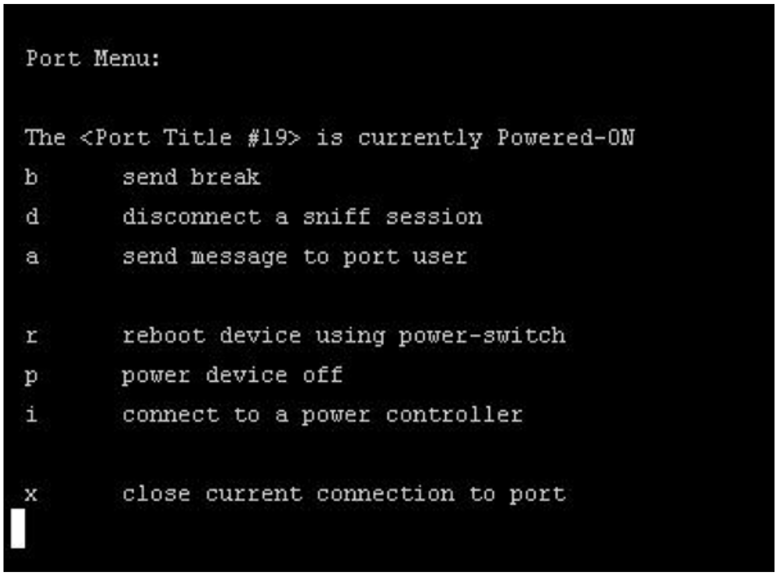
online

```
Entering server port, ..... type CTRL-z for port menu.
```

ls

Applet de.mud.jta.Applet started

After typing the port menu key:



```
Port Menu:

The <Port Title #19> is currently Powered-ON
b      send break
d      disconnect a sniff session
a      send message to port user

r      reboot device using power-switch
p      power device off
i      connect to a power controller

x      close current connection to port
```

Type **p** to power device off or **r** to reboot device.

The Hot Key by default is **Ctrl-Z.**

This can be changed by going to **Configuration > Serial Ports > {Port # or All} > Host mode configuration > {set the Port Escape Sequence} > Save & Apply.**

Note: This is also what is displayed when connecting directly to the port using ssh or telnet without going through the web interface.

Pinouts for Third-Party Power Controllers and Digi Passport

Pinouts for supported power controllers and the Digi Passport follow.

An Ethernet cable can be used to connect the ServerTech Sentry Power Controller to the the Digi Passport unit.

Pinouts for RS-232 Port of ServerTech Sentry Power Controller

Pin Number	EIA-232 Signal
1	RTS
2	DTR
3	Tx
4	GND
5	GND
6	Rx
7	DSR
8	CTS

Pinouts for RS232 Port of BayTech RPC series

Pin Number	EIA-232 Signal
1	DTR
2	GND
3	RTS
4	Tx
5	Rx
6	N/C
7	GND
8	DCD

Pinouts for console port of Digi Passport

Pin Number	EIA-232 Signal
1	CTS
2	DSR
3	RxD
4	GND
5	DCD
6	TxD
7	DTR
8	RTS

About Port Clustering

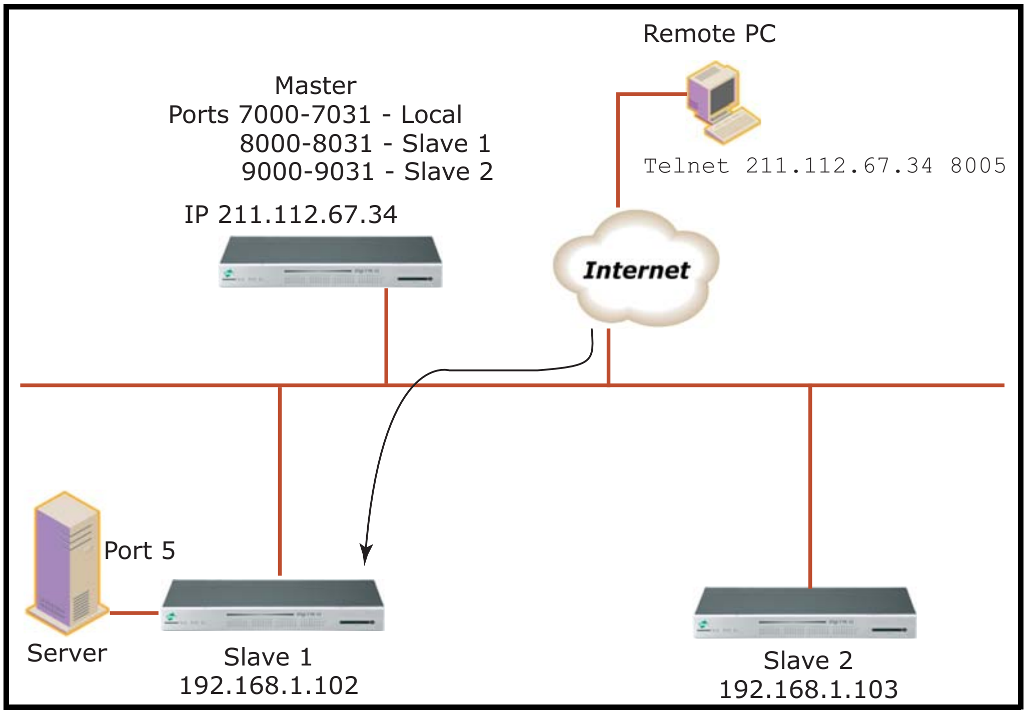
Port clustering is the ability to coherently manage serial ports across multiple devices. Digi Passport supports two methods of port clustering, both of which can be used concurrently:

- Master/Slave Clustering
- Peer-to-Peer Clustering

Master/Slave Clustering

Master/slave clustering allows serial ports on one or multiple slave devices to be managed from one master device using a single IP address. One unit is defined as the master and the other units as slaves.

For example, the Digi Passport unit can manage up to 48 slaves or a maximum of 2352 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**.



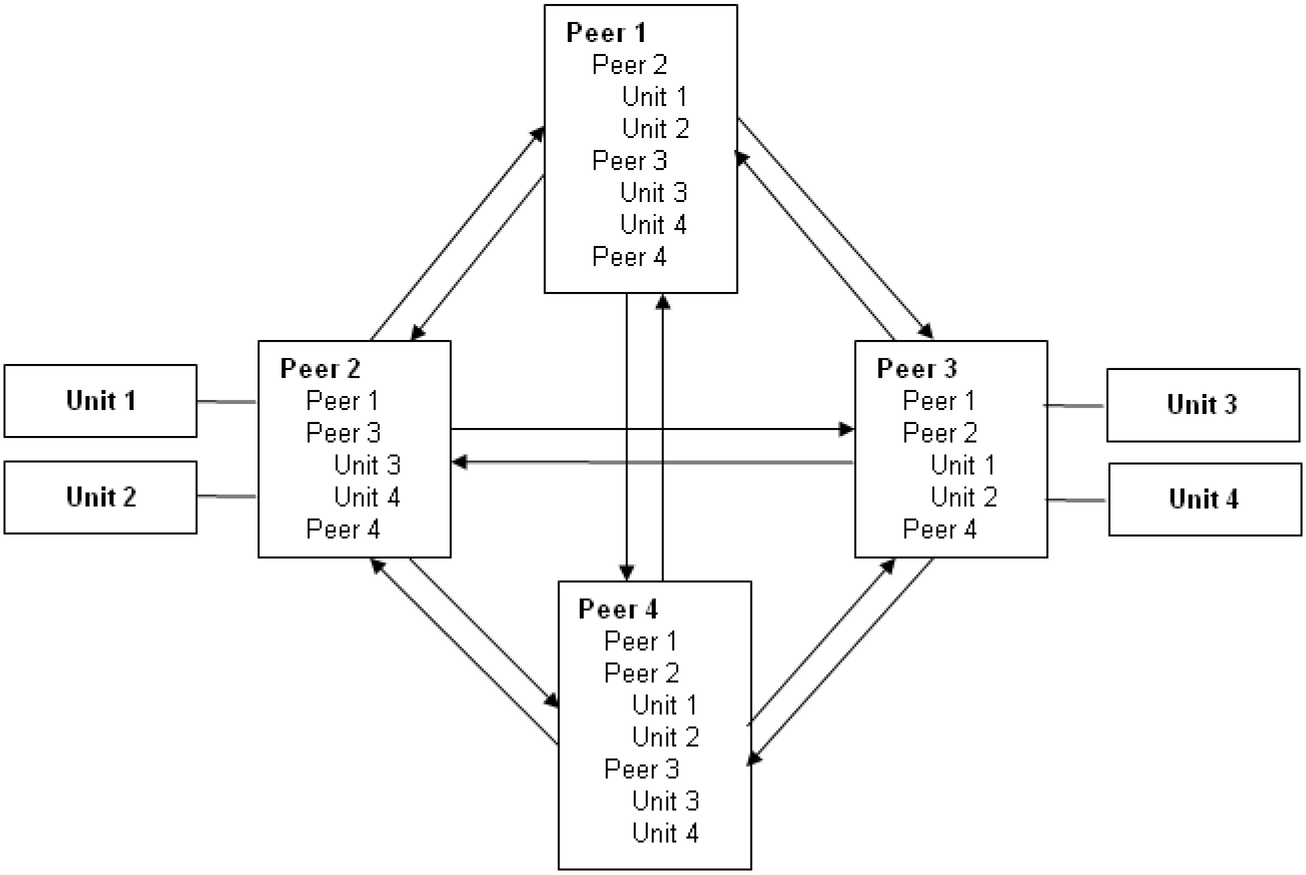
While it is possible to define multiple units as masters for a common set of slaves, a unit cannot be both a master and a slave at the same time. If a Digi Passport unit has Master/Slave clustering configured, it reports all of its slave ports to the other peer units. However, it is still necessary for that Digi Passport unit to be operational to reach the Slave ports it controls.

Peer-to-Peer Clustering

Peer-to-peer clustering allows multiple Digi Passport units to share information and have equal status within a cluster, without requiring one of the units to be the master. Any unit in the cluster, typically, the closest unit to the user, can act as a 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. 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.

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.



Configure Master-Slave Port Clustering

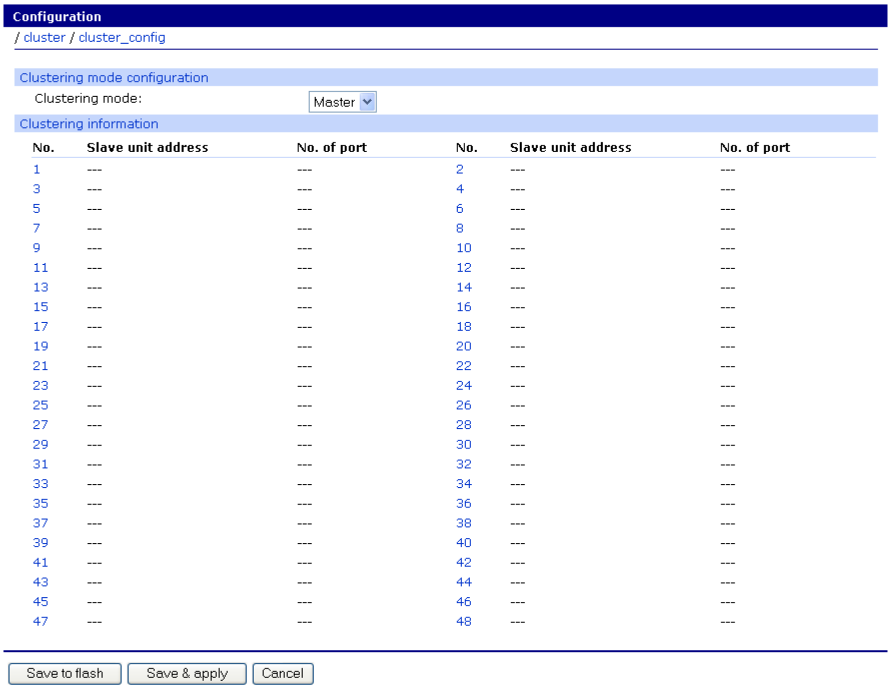
Configuring the Digi Passport unit for port clustering requires these tasks:

- 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 the slave configuration to the Digi Passport unit's master device.

Assign 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 will be the Master.
2. Select **Clustering > Configuration**.
3. For the Clustering mode setting, select **Master**. (By default, subsequent Digi Passport units are configured in Slave mode.)
4. Click **Save & apply**.



Configuration

/ cluster / cluster_config

Clustering mode configuration

Clustering mode: Master

Clustering information

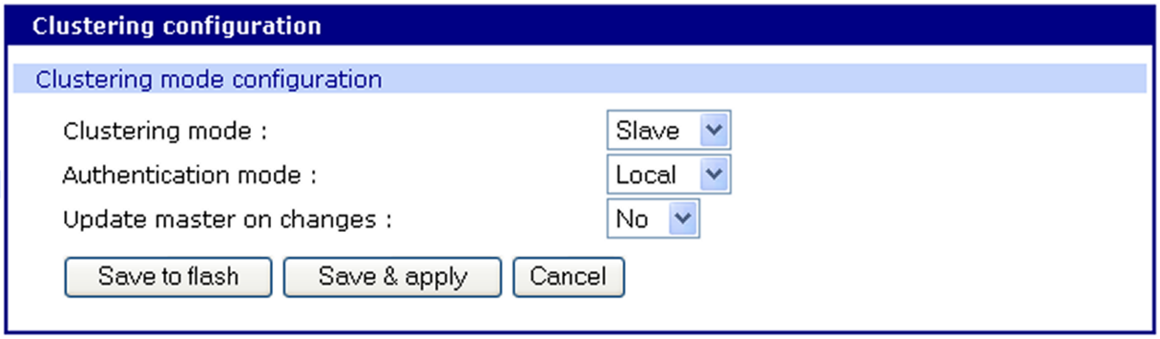
No.	Slave unit address	No. of port	No.	Slave unit address	No. of port
1	---	---	2	---	---
3	---	---	4	---	---
5	---	---	6	---	---
7	---	---	8	---	---
9	---	---	10	---	---
11	---	---	12	---	---
13	---	---	14	---	---
15	---	---	16	---	---
17	---	---	18	---	---
19	---	---	20	---	---
21	---	---	22	---	---
23	---	---	24	---	---
25	---	---	26	---	---
27	---	---	28	---	---
29	---	---	30	---	---
31	---	---	32	---	---
33	---	---	34	---	---
35	---	---	36	---	---
37	---	---	38	---	---
39	---	---	40	---	---
41	---	---	42	---	---
43	---	---	44	---	---
45	---	---	46	---	---
47	---	---	48	---	---

Configure Slaves to Join a Cluster

Digi Passport 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 set to **Yes**.

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



Clustering configuration

Clustering mode configuration

Clustering mode : Slave

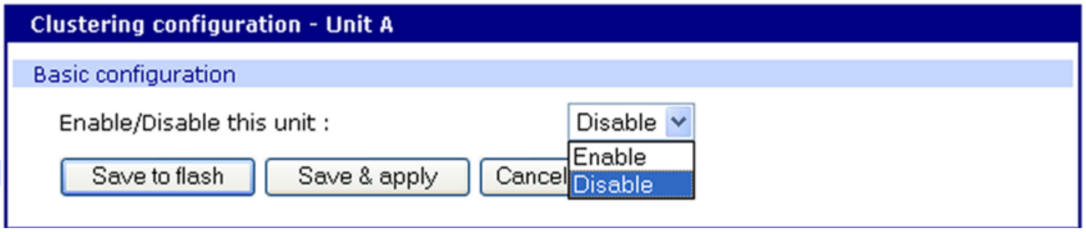
Authentication mode : Local

Update master on changes : No

Configure Advanced Clustering Settings

To refine a cluster environment, use the advanced clustering configuration settings.

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

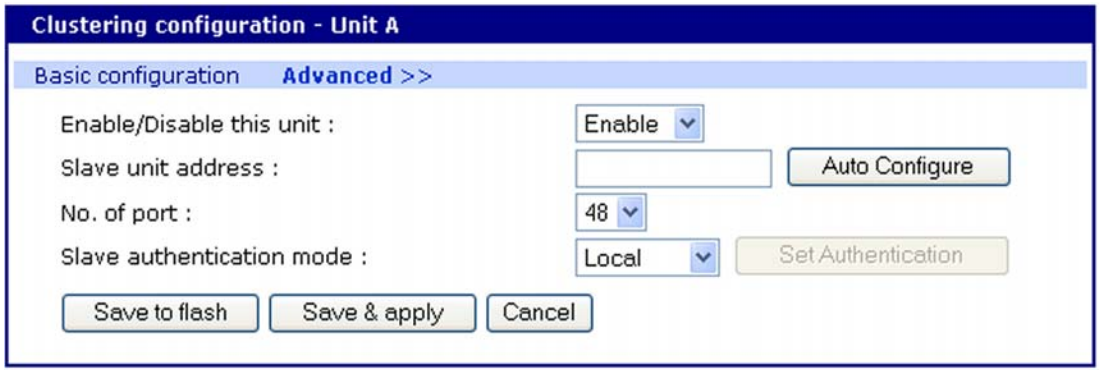


Clustering configuration - Unit A

Basic configuration

Enable/Disable this unit : Disable

3. From the **Clustering >Master mode**, select **Advanced**.



Clustering configuration - Unit A

Basic configuration   Advanced >>

Enable/Disable this unit : Enable

Slave unit address :

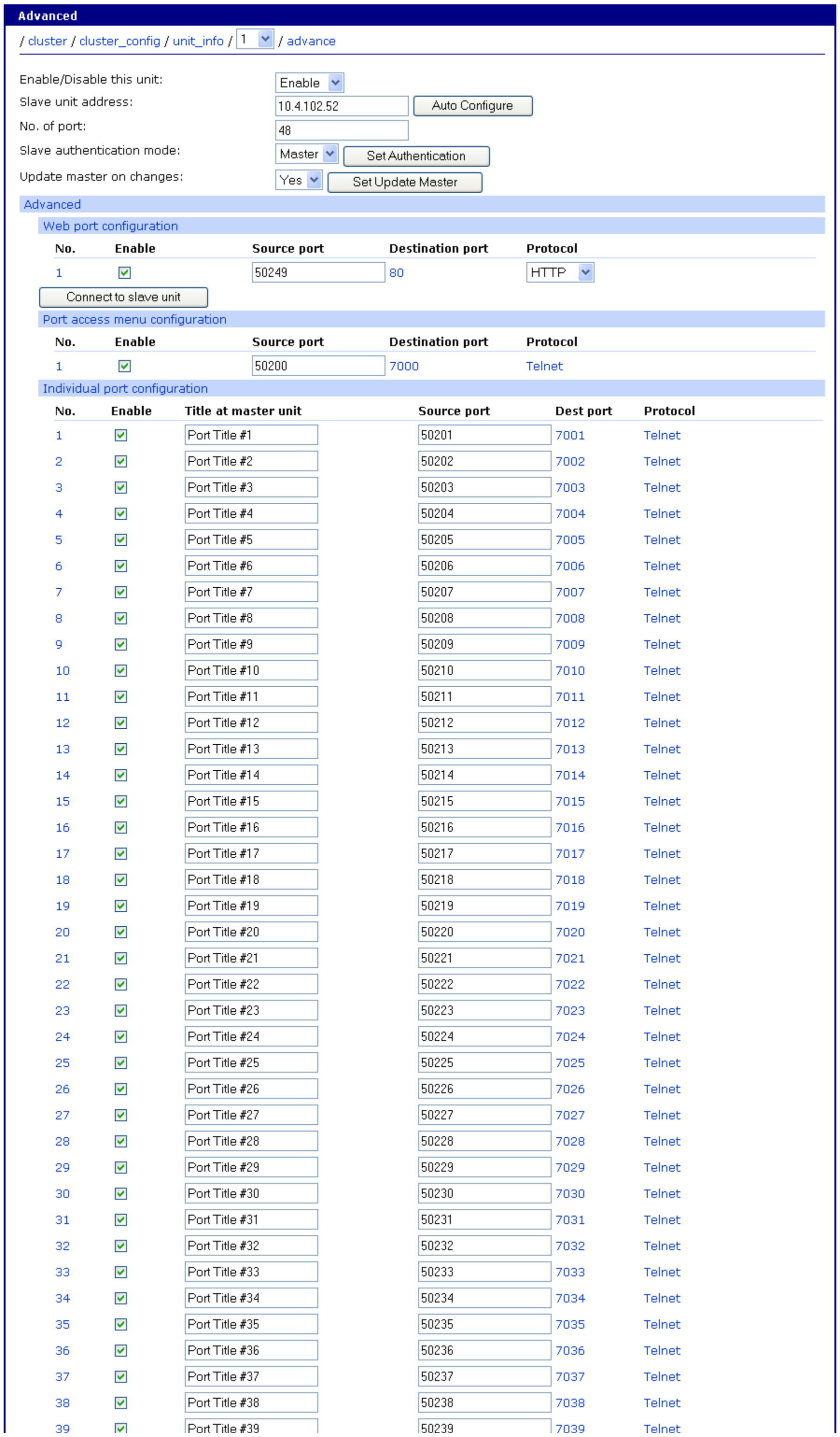
No. of port : 48

Slave authentication mode : Local

Advanced master-slave clustering settings include:

- **Enable**: Shows whether the port is enabled or disabled. All ports are enabled by default.
- **Slave unit address**: The IP address of slave.
- **No. of ports**: The number of ports on the slave.
- **Slave authentication mode**: Whether the 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 set to **yes**.
- **Connect to slave unit to change configuration**: A quick access method to connect to the slave.
- **Source port**: The port number accessed 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 corresponding port number on the slave unit. On a 32-port slave unit, the destination port numbers range from 7001 to 7032.
- **Protocol**: Options are N/A (not available), SSH, Telnet, and RawTCP.

  Base source port: If not using AutoConfig, these ports can be set manually. The 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 7032. Port number 7100 is the port access menu of the slave. If configuring the device manually, the port access menu must also be configured separately. However, if the base source port number is changed to another number and the rest of the ports on the unit will be sequentially numbered from the base source port.
- **Base destination port**: The physical port numbers of the slave device.



Advanced

/ cluster / cluster_config / unit_info / 1 / advance

Enable/Disable this unit:	Enable
Slave unit address:	10.4.102.52 [Auto Configure]
No. of port:	48
Slave authentication mode:	Master [Set Authentication]
Update master on changes:	Yes [Set Update Master]

Advanced

Web port configuration

No.	Enable	Source port	Destination port	Protocol
1	☑	50249	80	HTTP

[Connect to slave unit]

Port access menu configuration

No.	Enable	Source port	Destination port	Protocol
1	☑	50200	7000	Telnet

Individual port configuration

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

Access the Cluster Ports

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

From the Web Interface

1. Clustered Ports appear in the Web user interface, 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, go to **Network > Webserver Configuration** and adjust the **Serial ports count on connection page** setting. See "Configure Authentication for the Web Server" on page 152.

From the Command Line Interface

From the Ports Menu, select R to see a list of peered units or S to see a list of Slave units.

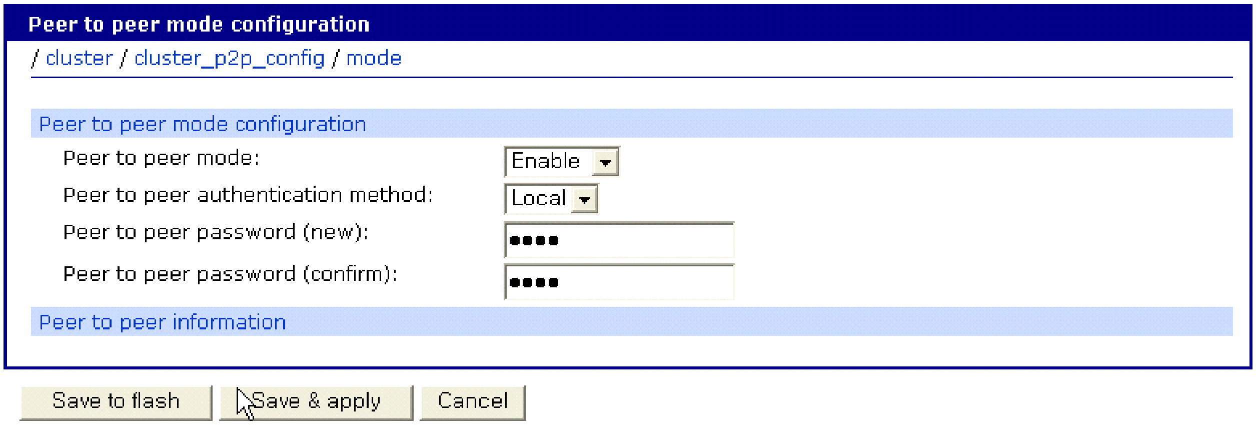
Configure peer-to-peer Clustering

Configure Peer-to-peer Mode

1. Access the Digi Passport unit through the web interface.
2. Select **Configuration > Peer-to-Peer configuration**.
3. Configure peer-to-peer mode settings:
   - **Peer-to-peer mode**: select **Enable**.
   - **Peer-to-peer authentication method**: Select authentication method to be used.

     Local authentication: this peer will continue to authenticate users locally and independently of other peers.

     Peer authentication: the first peer contacted will perform the authentication.
   - **Peer-to-peer password (new)/(confirm)**: Peered units must share the same password.



Peer to peer mode configuration

/ cluster / cluster_p2p_config / mode

Peer to peer mode configuration

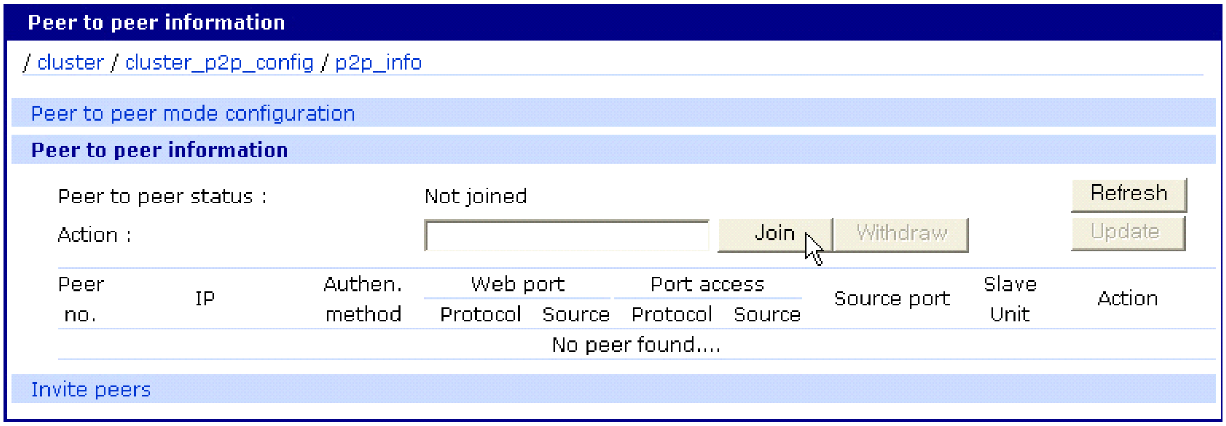
Peer to peer mode:	Enable
Peer to peer authentication method:	Local
Peer to peer password (new):	••••
Peer to peer password (confirm):	••••

Peer to peer information

4. Click **Save & apply**.

Peer-to-peer Information Page

The **Peer to peer information** page allows for joining and withdrawing peer-to-peer connections, and displays status of peer-to-peer connections.



Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Not joined

Action :

Peer no.	IP	Authen. method	Web port		Port access		Source port	Slave Unit	Action
			Protocol	Source	Protocol	Source			
No peer found....									

Invite peers

Status fields and buttons on this page include:

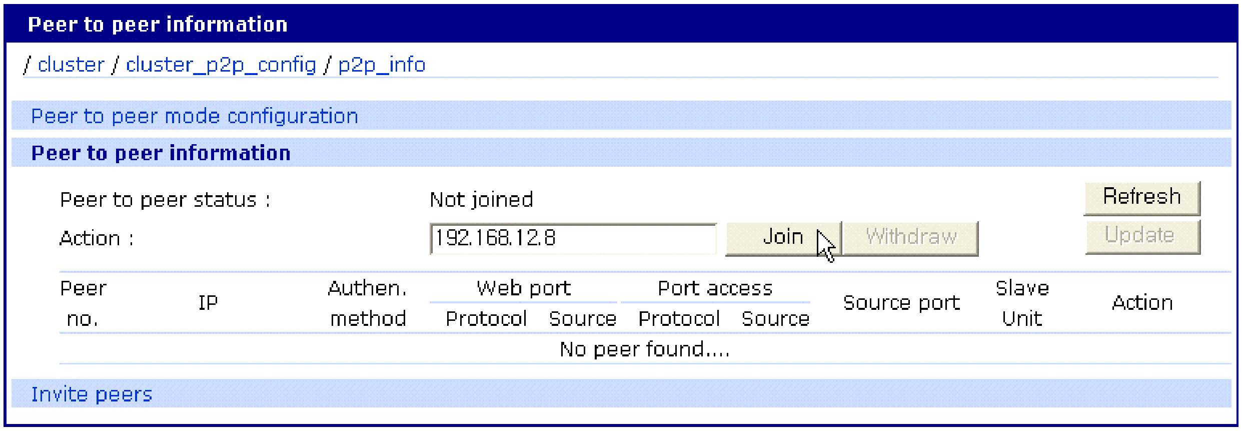
- **Not ready**: Peer-to-peer mode is not active
- **Not joined**: Peer-to-peer mode is active but no peers have been defined.
- **Joining**: Joining peer-to-peer group.
- **Joined**: Joined peer-to-peer group.
- **Changing peers**: Changing the information of peers in peer-to-peer group.
- **Withdrawing**: Withdrawing from peer-to-peer group.
- **Withdrawn**: Withdrawn from last peer-to-peer group.
- **Refresh** button: Update display of this page.
- **Join** button: Used to join peer-to-peer group of a designated peer (requires common password).
- **Withdraw** button: Withdraws from the current peer-to-peer group.
- **Update** button: Gets the information of peers that have not responded.
- **Peers** list: The list of the peers that are members of the current peer-to-peer group.

Join a Peer-to-peer Group

To join an existing peer-to-peer group, enter the IP address of a member of that group and click the **Join** button. If the peer is not enabled or the password is incorrect, the joining process will fail.

Peer information for a joining peer

This screen 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.



Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Not joined

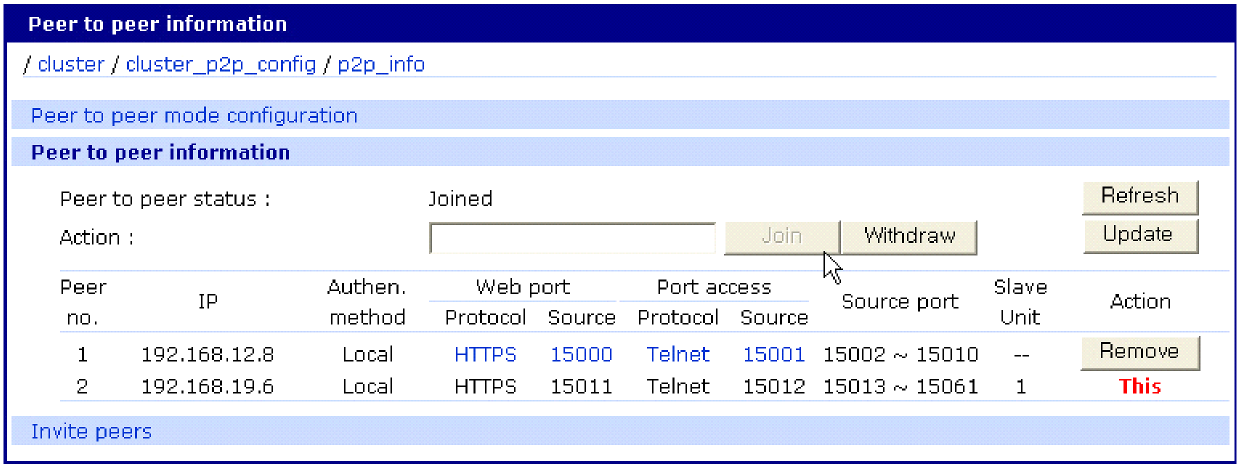
Action : 192.168.12.8

Peer no.	IP	Authen. method	Web port Protocol	Web port Source	Port access Protocol	Port access Source	Source port	Slave Unit	Action
				No peer found....					

Invite peers

Peer-to-peer information for the designated peer

This screen shows peer-to-peer information of the designated peer.



Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Joined

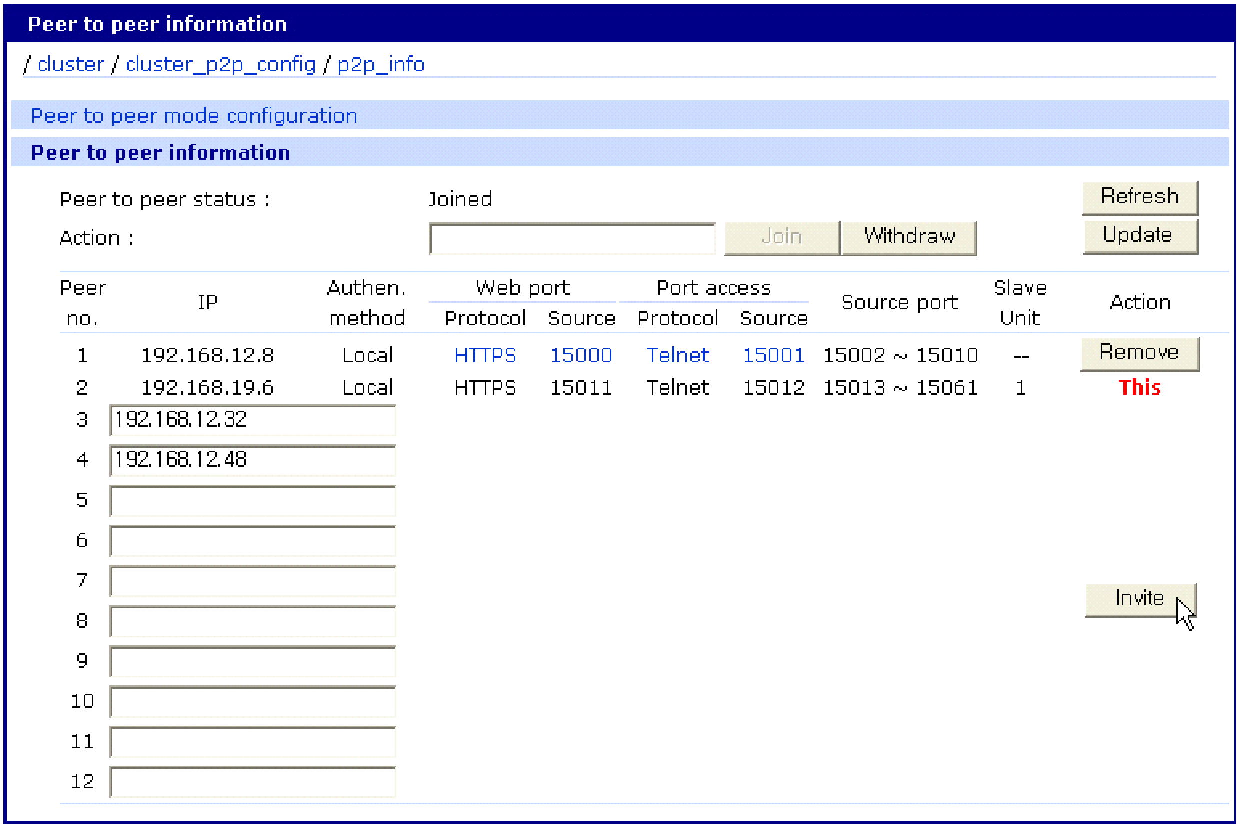
Action :

Peer no.	IP	Authen. method	Web port Protocol	Web port Source	Port access Protocol	Port access Source	Source port	Slave Unit	Action
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

Invite peers

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.



Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

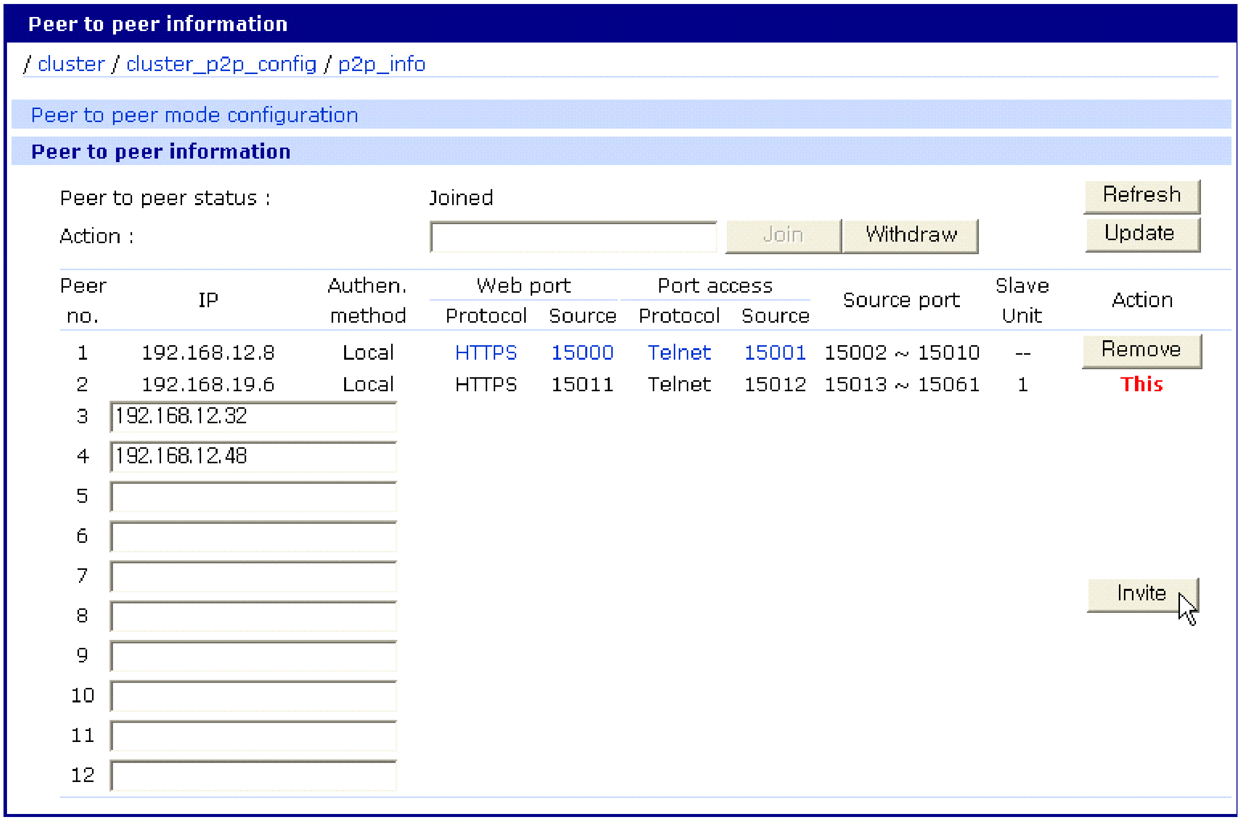
Peer to peer status : Joined

Action : [ ] Join Withdraw

Refresh

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	192.168.12.32								
4	192.168.12.48								
5									
6									
7									Invite
8									
9									
10									
11									
12									



Peer to peer information

/ cluster / cluster_p2p_config / p2p_info

Peer to peer mode configuration

Peer to peer information

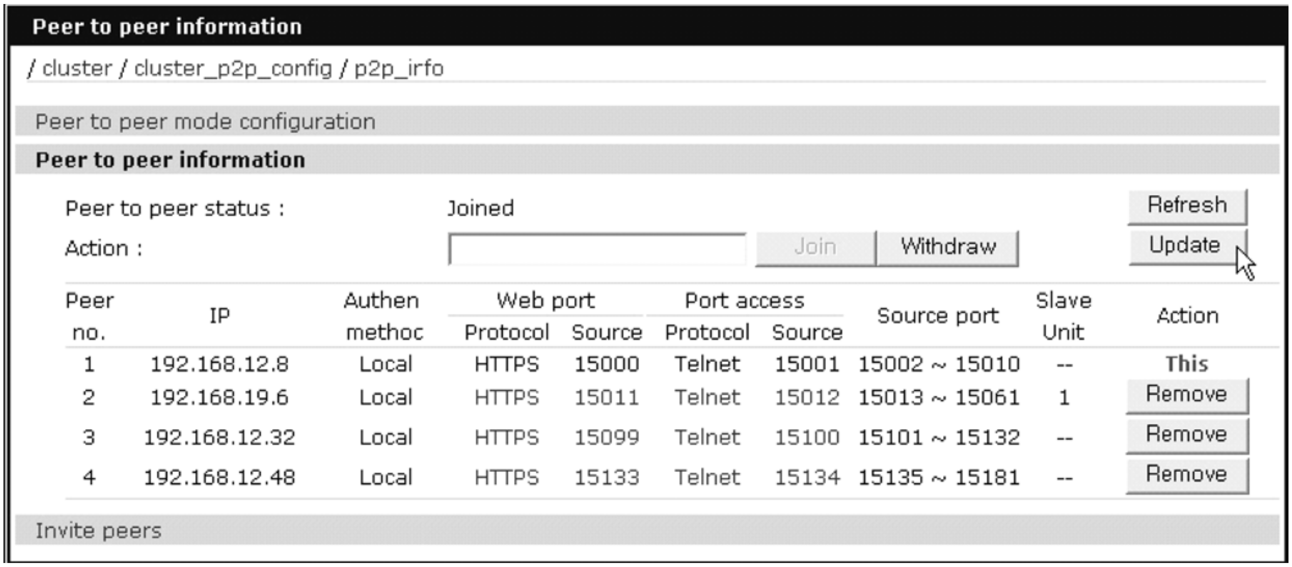
Peer to peer status : Joined

Action :

Peer no.	IP	Authen. method	Web port Protocol	Web port Source	Port access Protocol	Port access Source	Source port	Slave Unit	Action
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	192.168.12.32								
4	192.168.12.48								
5									
6									
7									Invite
8									
9									
10									
11									
12									

Peer-to-peer information after inviting peers

- **Withdraw**: Withdraws the peer-to-peer group.
- **Remove**: Removes the peer from the peers list.
- **Update**: Gets the information of the peers that have not responded.



Peer to peer information

/ cluster / cluster_p2p_config / p2p_irfo

Peer to peer mode configuration

Peer to peer information

Peer to peer status : Joined

Action :

Peer no.	IP	Authen. methoc	Web port Protocol	Web port Source	Port access Protocol	Port access Source	Source port	Slave Unit	Action
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

Connect 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.

Link to Port Access Menu

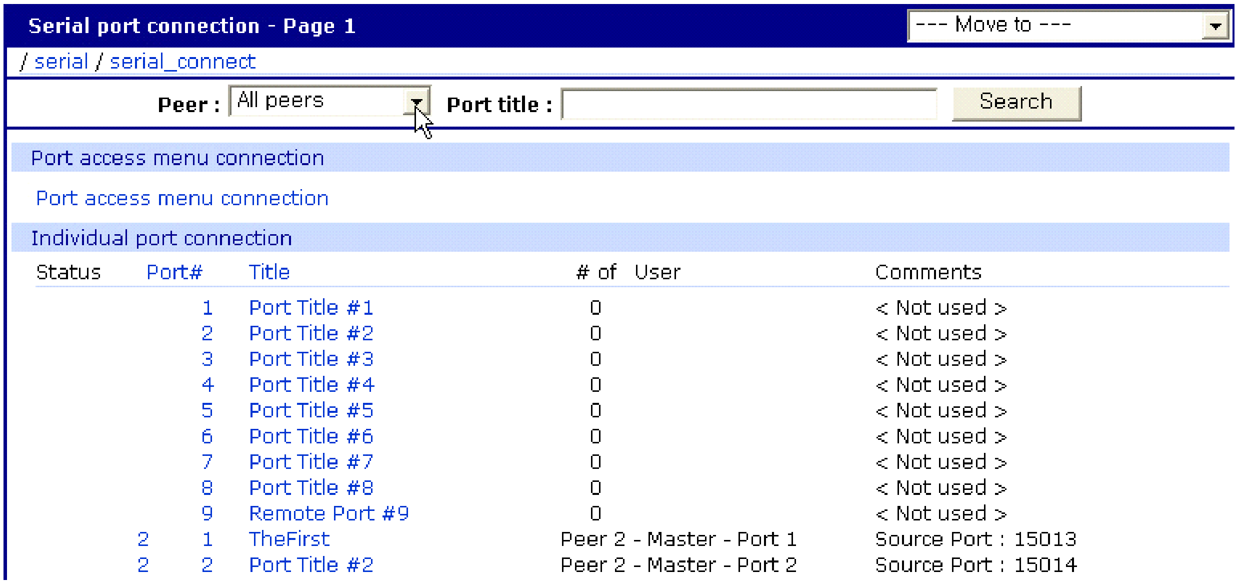
To connect to the port access menu of the peer, click the protocol or the source port of the port access menu.

Use the Digi Passport unit 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 connected from the local system for that port. However, this information is still available when connecting to the port.

Serial Port connection Page

This figure 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.



Serial port connection - Page 1

/ serial / serial_connect

Peer : All peers   Port title :

Port access menu connection

Port access menu connection

Individual port connection

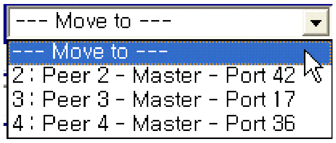
Status	Port#	Title	# of User	Comments
	1	Port Title #1	0	< Not used >
	2	Port Title #2	0	< Not used >
	3	Port Title #3	0	< Not used >
	4	Port Title #4	0	< Not used >
	5	Port Title #5	0	< Not used >
	6	Port Title #6	0	< Not used >
	7	Port Title #7	0	< Not used >
	8	Port Title #8	0	< Not used >
	9	Remote Port #9	0	< Not used >
	2 1	TheFirst	Peer 2 - Master - Port 1	Source Port : 15013
	2 2	Port Title #2	Peer 2 - Master - Port 2	Source Port : 15014

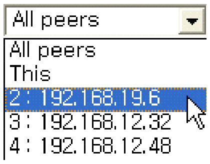
Move to and Peer list

To limit those ports that belong to the selected peer, select a peer in the 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.


--- Move to ---
--- Move to ---
2 : Peer 2 - Master - Port 42
3 : Peer 3 - Master - Port 17
4 : Peer 4 - Master - Port 36



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 the slave unit number, and *port_number* is port number.

For example:

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.

For example:

`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)

Add Ports of Peers or Slaves to the Custom Menu

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

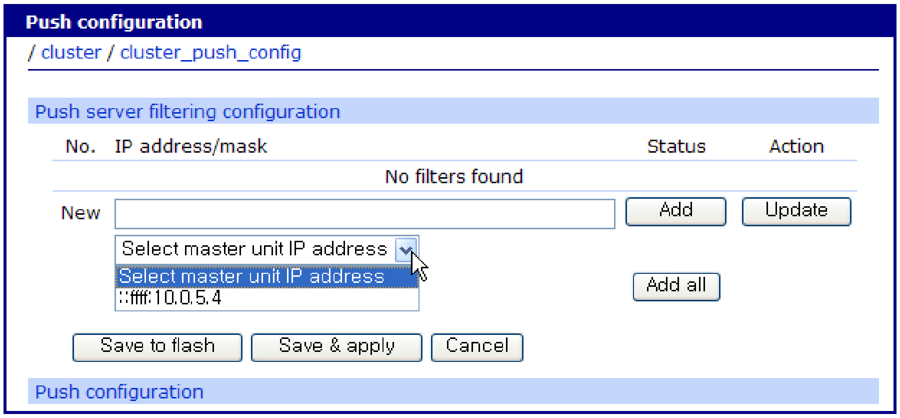
Clustering push configuration

Clustering push configuration is used to push the configuration of one Passport (Push server) to the other Passport unit in the cluster. This can facilitate initial configuration of multiple Passport units. Because of security concerns, pushing configuration is only possible to the units which have default root password (dbps). Also only the ADR and User configuration can be pushed.

Clustering push configuration has two main configuration menus.

- Push server filtering configuration
- Push configuration

The Push server filtering configuration menu is used to set push server(s) which can push its configuration (ADR and User configuration) to the unit. If there is no server configured, any Passport unit in the cluster can push its configuration to the unit. If the unit is set as clustering slave unit and is already configured as a slave by a master clustering unit. The **Push server filtering configuration** page will also show the IP address of master unit.



Push configuration

/ cluster / cluster_push_config

Push server filtering configuration

No.	IP address/mask	Status	Action
No filters found			

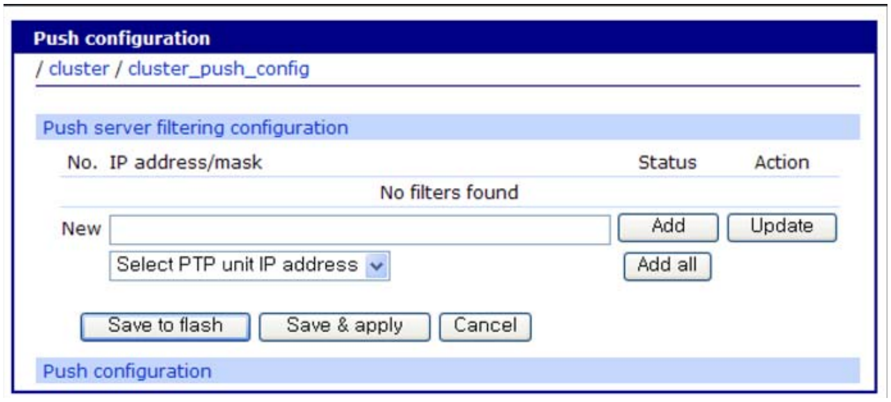
New

Select master unit IP address

Select master unit IP address
::ffff:10.0.5.4

Push configuration

If the unit is set as clustering master unit, the **Push server filtering configuration** page will *not* show the IP address of master unit menu.



Push configuration

/ cluster / cluster_push_config

Push server filtering configuration

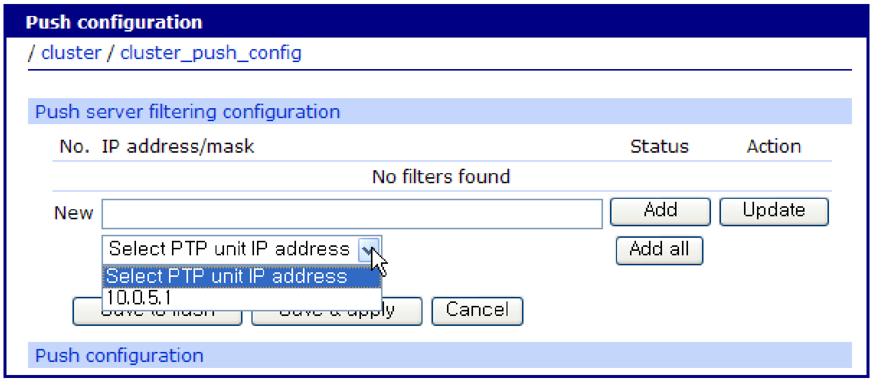
No.	IP address/mask	Status	Action
No filters found			

New

Select PTP unit IP address

Push configuration

If the unit is joined peer to peer clustering, you can see the peer list on the **Push server filtering configuration** page.



Push configuration

/ cluster / cluster_push_config

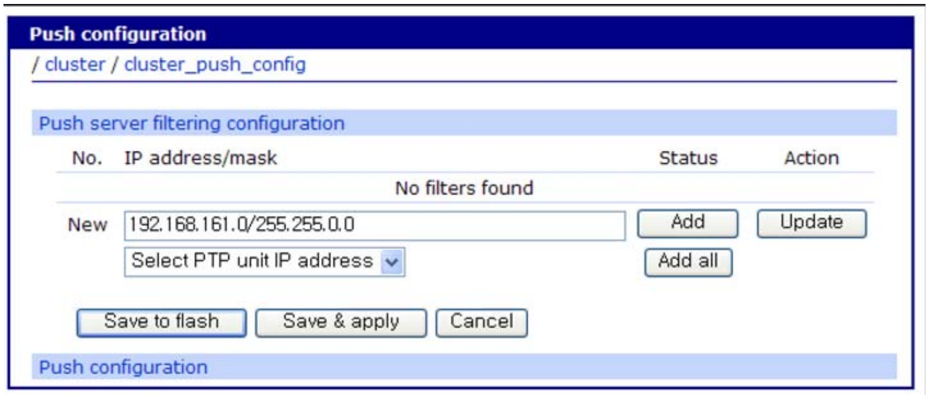
Push server filtering configuration

No.	IP address/mask	Status	Action
No filters found			

New

Select PTP unit IP address

You can also add the push server manually by entering the IP address and net work mask to the new option box and then pressing **Add**.



Push configuration

/ cluster / cluster_push_config

Push server filtering configuration

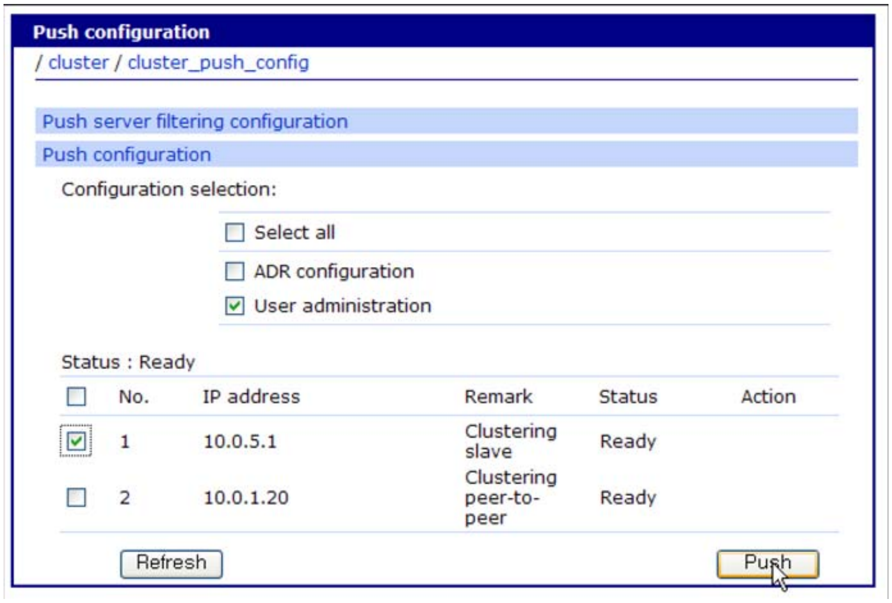
No.	IP address/mask	Status	Action
No filters found			

New 192.168.161.0/255.255.0.0

Select PTP unit IP address

Once the push servers are configured, only the Passport unit listed on the **Push server filtering configuration** page can push the configuration to the unit.

Pushing the configuration can be done through **Push configuration** menu page. If the unit has salve unit or joins peer to peer clustering, you will see the list of clustered units on this page. After selecting the configuration and unit to be pushed the configuration, press the push button. And then wait until the Status has changed from Busy to Ready. Once the status has changed to Ready again, you will find selected configuration was pushed the target unit.



Push configuration

/ cluster / cluster_push_config

Push server filtering configuration

Push configuration

Configuration selection:

□ Select all

□ ADR configuration

☑ User administration

Status : Ready

□	No.	IP address	Remark	Status	Action
☑	1	10.0.5.1	Clustering slave	Ready	
□	2	10.0.1.20	Clustering peer-to-peer	Ready	

Chapter 16 **Configuration Menu Interface**

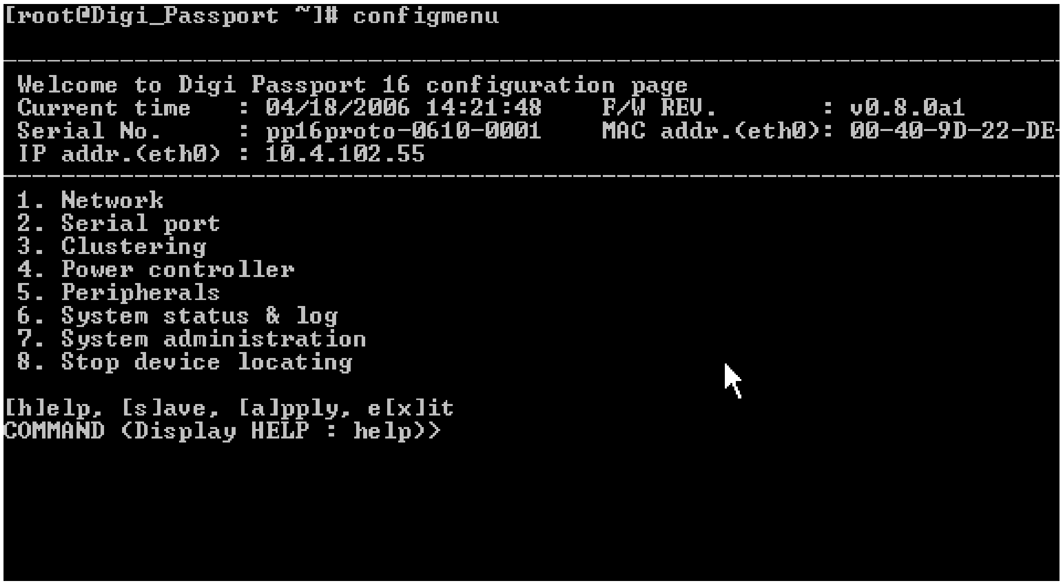
About the Configuration Menu

The configuration menu enables authorized users to configure the Digi Passport unit with the same functionality as is available with the web interface, except for creating custom menus.

Access the Configuration Menu

The configuration menu is available through a Telnet or SSH session to the root user, system administrator, or port administrator. (Port administrator can only change serial port parameters.)

1. Telnet into the Digi Passport unit.
   - If logging in as root, username **root**, password **dbps**. By default, the root user is connected from a Telnet session to the Linux command line.
   - If logging in as **admin**, the configuration menu is automatically displayed.
2. At the command prompt, enter **configmenu**. 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-
 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]ave, [a]pply, e[x]it
COMMAND (Display HELP : help)>
```

Navigating in the Configuration Menu

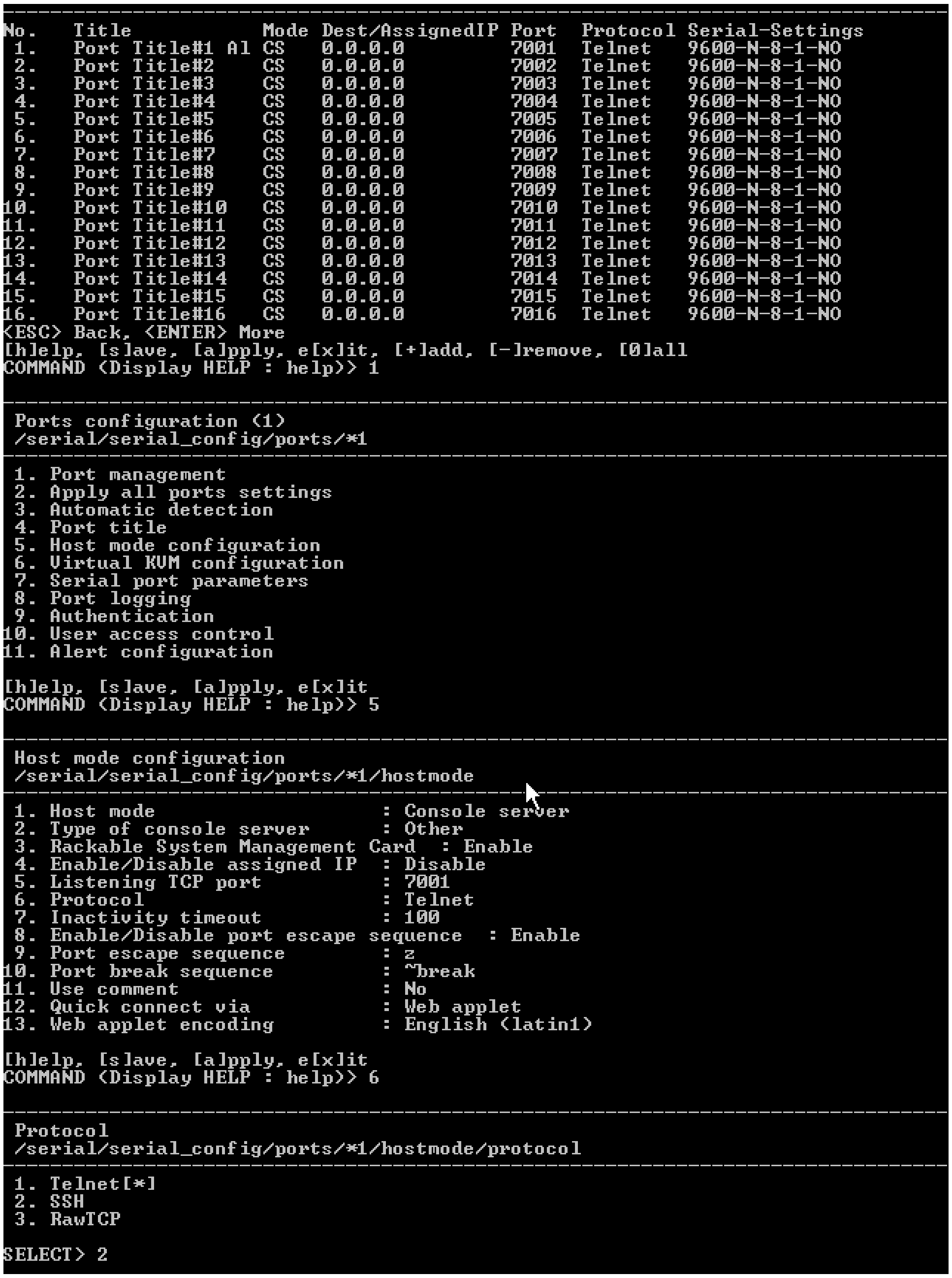
To choose items from the configuration menu, enter the number of the menu item. To move back a menu, press the **ESC** key. Sometimes only one menu item is presented; however, that single menu item has two or more options that have to be configured.

Saving Changes

The save command, **[s]ave**, saves changes to flash memory only.

Configure SSH

1. Select **Serial Port Configuration >** ***port number*** or **0** (zero) for all ports.
2. Select **Host mode configuration > Protocol > SSH**.



```
------------------------------------------------------------------------------
No.   Title           Mode Dest/AssignedIP Port  Protocol Serial-Settings
 1.   Port Title#1 A1 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]elp, [s]ave, [a]pply, e[x]it, [+]add, [-]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 KVM configuration
 7. Serial port parameters
 8. Port logging
 9. Authentication
10. User access control
11. Alert configuration

[h]elp, [s]ave, [a]pply, e[x]it
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]elp, [s]ave, [a]pply, e[x]it
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. Select **Exit** and apply changes.

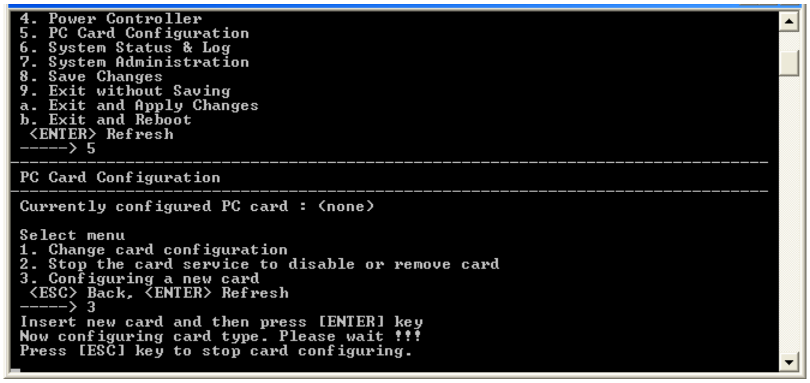
Add, Edit, and Remove Users

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

Add and Configure a PC Card

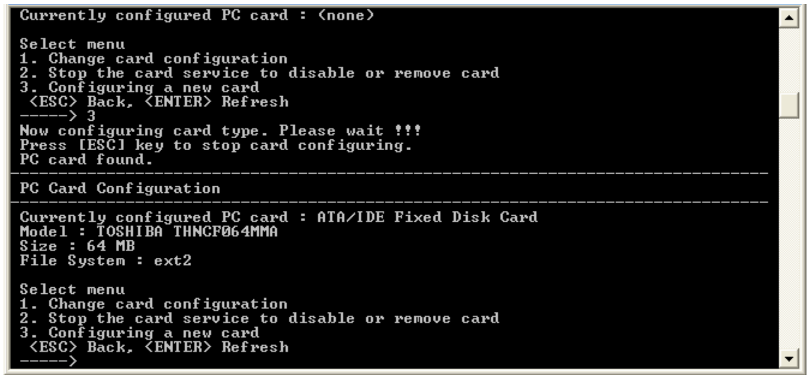
To add a modem card, compact-flash card, wireless LAN card, or network card to the Digi Passport unit using the configuration menu, do the following:

1. Access the configuration menu. (**1 Network Configuration**, **5 Peripherals**).
2. Select **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**. The system searches for the card and displays information on the product model number and type of card.

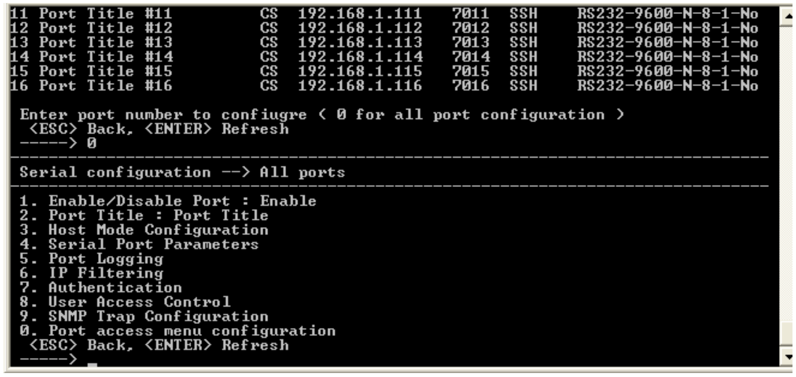


```
Currently configured PC card : (none)

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. Select **Save Changes**.

Host Mode Configuration

1. Access the configuration menu.
2. Select **Serial Port Configuration** > ***port number*** or **0** (zero) for all ports **> Host Mode Configuration**.

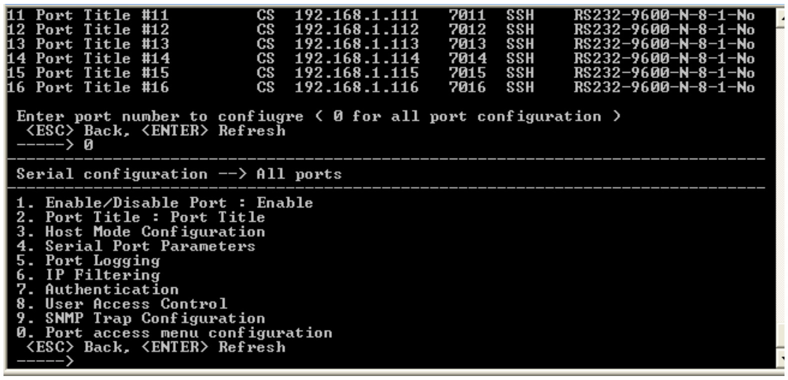


```
11 Port Title #11         CS  192.168.1.111   7011  SSH    RS232-9600-N-8-1-No
12 Port Title #12         CS  192.168.1.112   7012  SSH    RS232-9600-N-8-1-No
13 Port Title #13         CS  192.168.1.113   7013  SSH    RS232-9600-N-8-1-No
14 Port Title #14         CS  192.168.1.114   7014  SSH    RS232-9600-N-8-1-No
15 Port Title #15         CS  192.168.1.115   7015  SSH    RS232-9600-N-8-1-No
16 Port Title #16         CS  192.168.1.116   7016  SSH    RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 0
-------------------------------------------------------------------------------
 Serial configuration --> All ports
-------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. SNMP Trap Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
 -----> _
```

3. Enter the desired parameters for each menu item.

Port Parameters

1. Access the configuration menu.
2. Select **Serial Port Configuration** > ***port number*** or **0** or 0 (zero) for all ports.



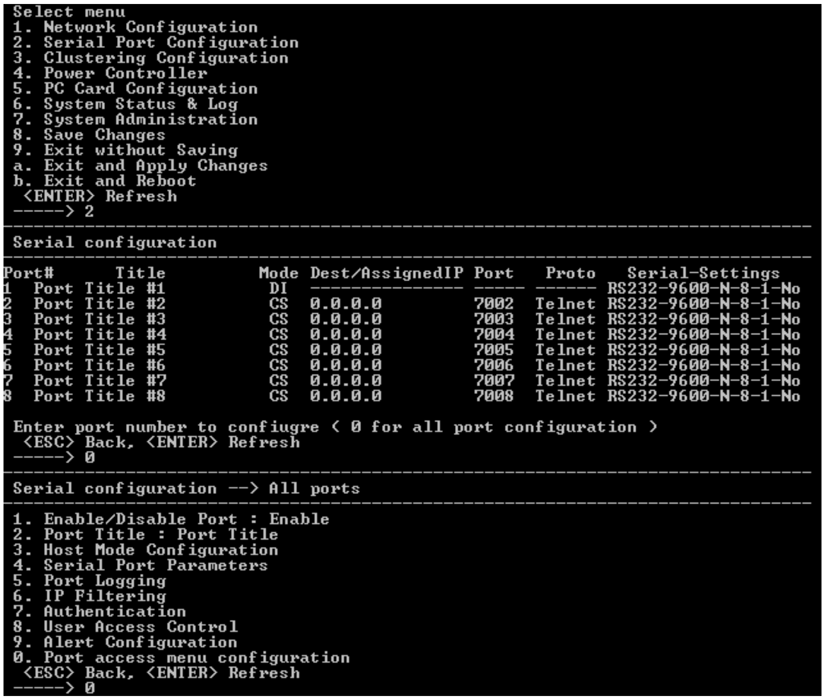
```
11 Port Title #11         CS  192.168.1.111   7011  SSH    RS232-9600-N-8-1-No
12 Port Title #12         CS  192.168.1.112   7012  SSH    RS232-9600-N-8-1-No
13 Port Title #13         CS  192.168.1.113   7013  SSH    RS232-9600-N-8-1-No
14 Port Title #14         CS  192.168.1.114   7014  SSH    RS232-9600-N-8-1-No
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 the configuration menu.
2. Select **Serial Port Configuration**.
3. Select 0 for all ports.
4. Select **Port access menu configuration**.



```
 Select menu
 1. Network Configuration
 2. Serial Port Configuration
 3. Clustering Configuration
 4. Power Controller
 5. PC Card Configuration
 6. System Status & Log
 7. System Administration
 8. Save Changes
 9. Exit without Saving
 a. Exit and Apply Changes
 b. Exit and Reboot
  <ENTER> Refresh
 -----> 2
--------------------------------------------------------------------------------
 Serial configuration
--------------------------------------------------------------------------------
Port#      Title         Mode Dest/AssignedIP Port   Proto   Serial-Settings
1  Port Title #1          DI  --------------- -----  ------ RS232-9600-N-8-1-No
2  Port Title #2          CS  0.0.0.0         7002  Telnet RS232-9600-N-8-1-No
3  Port Title #3          CS  0.0.0.0         7003  Telnet RS232-9600-N-8-1-No
4  Port Title #4          CS  0.0.0.0         7004  Telnet RS232-9600-N-8-1-No
5  Port Title #5          CS  0.0.0.0         7005  Telnet RS232-9600-N-8-1-No
6  Port Title #6          CS  0.0.0.0         7006  Telnet RS232-9600-N-8-1-No
7  Port Title #7          CS  0.0.0.0         7007  Telnet RS232-9600-N-8-1-No
8  Port Title #8          CS  0.0.0.0         7008  Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 0
--------------------------------------------------------------------------------
 Serial configuration --> All ports
--------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. Alert Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
 -----> 0
```

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, the root user 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. Second, 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 "Add a Compact-flash Card" on page 43. In the Digi Passport unit, all log messages are sent to the **syslog-ng** daemon. The **local 0** facility is only used for system log messages. The **local 1 ~ local7** facilities can be used for port log.

To configure system or port logging to the Syslog server (**syslog-ng**), go to the **System logging** or **Port logging** menu. There is no enable/disable option for System log to SYSLOG server because it is default function.

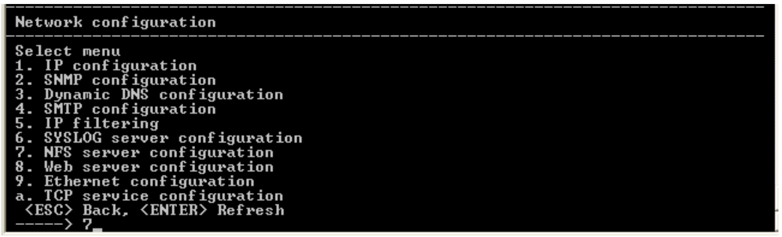
The facility for each port log from local1 to local7 can be specified. The local 0 facility is fixed for system log. With this configuration, the management of all messages sent to Syslog server (**syslog-ng**) can be configured during configuration of SYSLOG-NG.

By default, the syslog-ng configuration has an internal RAMDISK, **/var/log/messages**, that logs the configuration for system log message (local 0). To change filter options for this default configuration, click it. The Syslog-NG filter configuration page has all filter options supported by the syslog-ng daemon. For example, if the **Priority(debug)** option is added to the default system log configuration, all local syslog messages with debug priority are also logged to **/var/log/messages**. The Linux kernel and xinetd send some of their messages to syslog with debug priority.

To send log messages to a remote syslog server, add a new destination to the syslog-ng configuration, specifying **destination=TCP/UDP** and **location=*IP address of remote server***.

Configure an NFS or SYSLOG Server

1. Access the configuration menu.
2. Select **Network configuration > NFS or SYSLOG server configuration**.

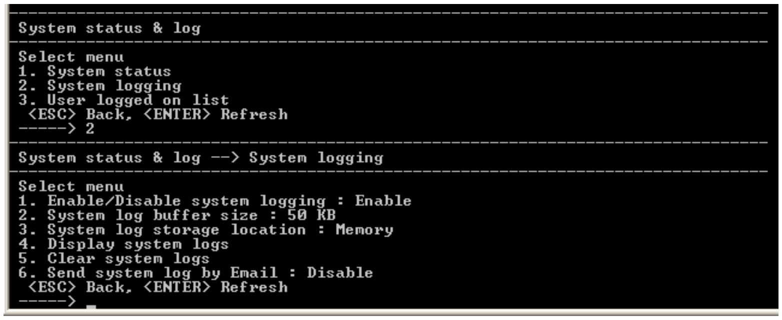


```
--------------------------------------------------------------------------------
Network configuration
--------------------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
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. Select **System Status & log > System logging**.



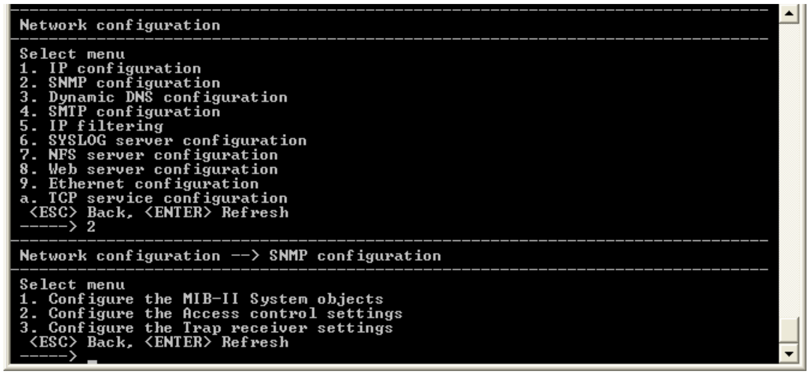
```
--------------------------------------------------------------------------------
System status & log
--------------------------------------------------------------------------------
Select menu
1. System status
2. System logging
3. User logged on list
 <ESC> Back, <ENTER> Refresh
-----> 2
--------------------------------------------------------------------------------
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. For example, to receive system log messages from Passport, add a new destination with UDP, local 0 facility and the IP address of remote syslog server to syslog-ng configuration. The flexibility of Syslog-NG configuration menu allows for adding a second or third remote Syslog server or grouping port logs according to the facility.

Configure SNMP

To configure SNMP from the configuration menu, do the following:

1. Access the configuration menu.
2. Select **Network Configuration > SNMP configuration**.



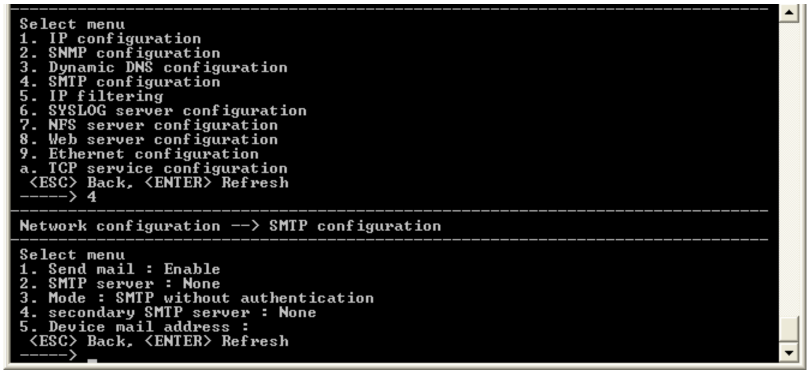
```
--------------------------------------------------------------------------------
Network configuration
--------------------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
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.

Configure SMTP

To configure SMTP from the configuration menu, do the following:

1. Access the configuration menu.
2. Select **Network configuration > SMTP configuration**.



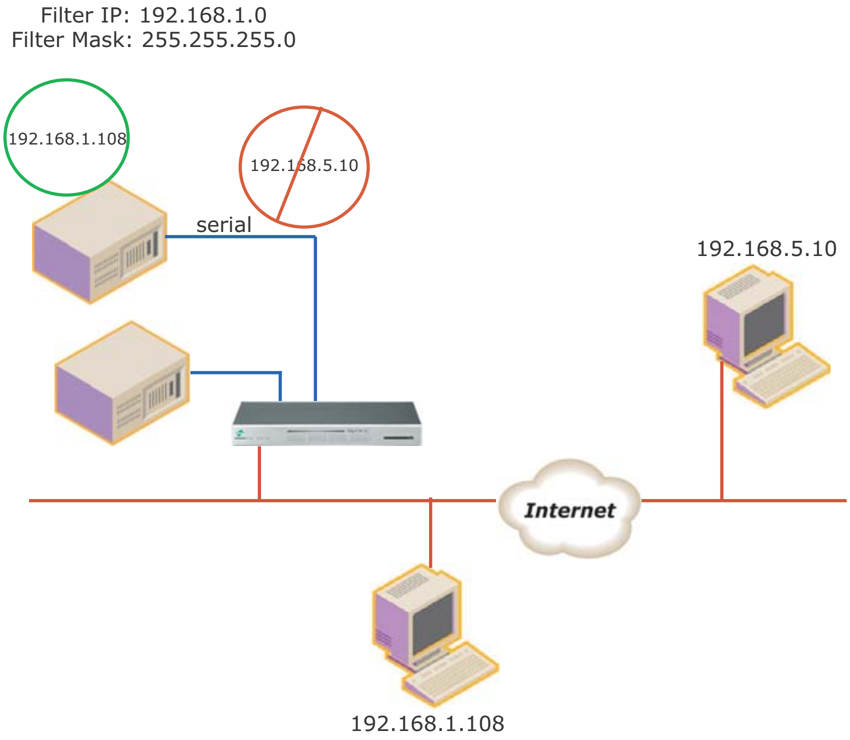
```
--------------------------------------------------------------------------------
Select menu
1. IP configuration
2. SNMP configuration
3. Dynamic DNS configuration
4. SMTP configuration
5. IP filtering
6. SYSLOG server configuration
7. NFS server configuration
8. Web server configuration
9. Ethernet 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.

Configure 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.

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.

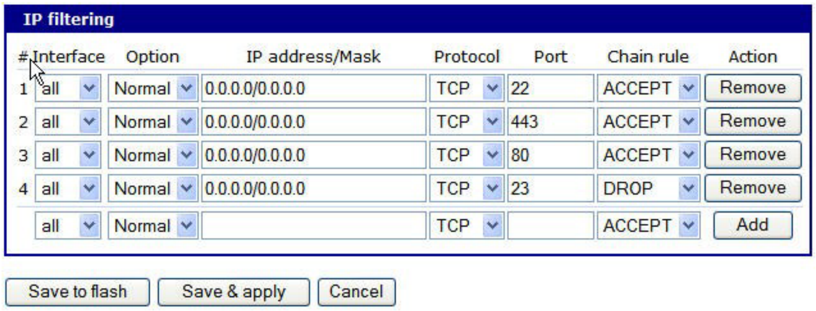


It is also possible to enable or disable specific services of the Digi Passport unit by creating IP Filtering rules for the following network services:

Network Service	Network port number
Telnet console	TCP/IP port 23
SSH console	TCP/IP port 22
Web configuration interface	TCP/IP port 80

IP Filtering Settings

The IP filtering settings page looks like this.



#	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

Settings include:

- **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
  - **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 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. Specify either one port, using a single value, or a range of ports using 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

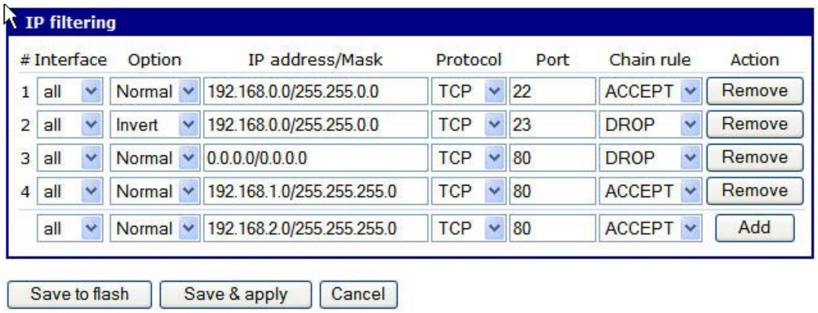
To add a new IP filtering rule, enter the values for the parameters and click the **Add** button on the right side of the table.

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

When finished editing the table, save the settings to flash. Changes must be applied to make them active.

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

This screen shows five established IP rules.



#	Interface	Option	IP address/Mask	Protocol	Port	Chain rule	Action
1	all	Normal	192.168.0.0/255.255.0.0	TCP	22	ACCEPT	Remove
2	all	Invert	192.168.0.0/255.255.0.0	TCP	23	DROP	Remove
3	all	Normal	0.0.0.0/0.0.0.0	TCP	80	DROP	Remove
4	all	Normal	192.168.1.0/255.255.255.0	TCP	80	ACCEPT	Remove
	all	Normal	192.168.2.0/255.255.255.0	TCP	80	ACCEPT	Add

IP Filtering Rules

This table describes the IP filtering rules.

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

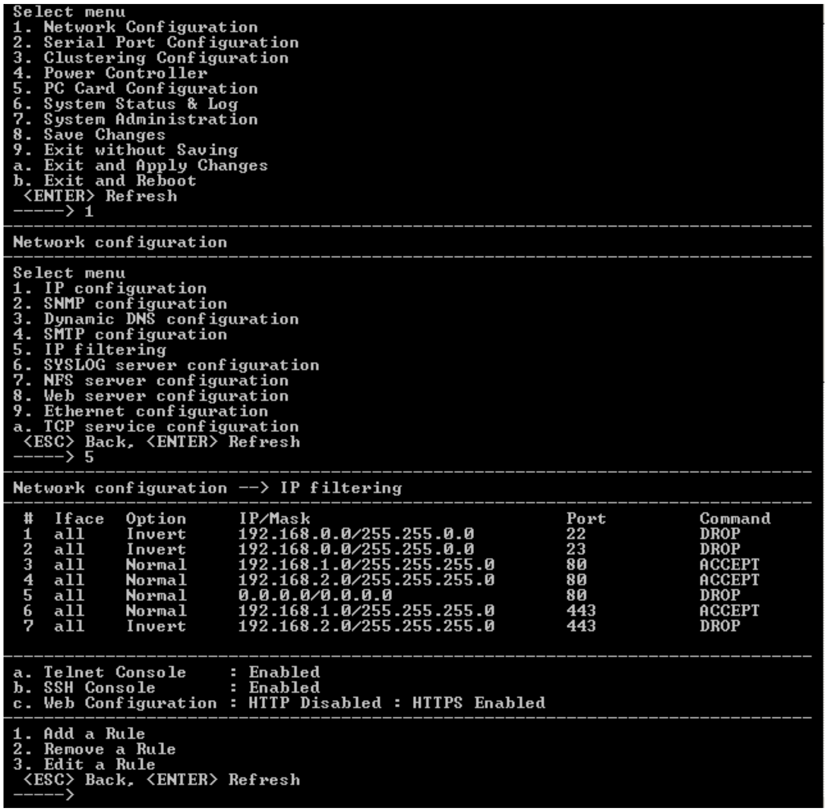
Allowable Hosts	Input format	
	Base Host IP Address	Subnet mask
Any host	0.0.0.0	0.0.0.0
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 - 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 - 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 - 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 - 192.168.1.254	192.168.1.128	255.255.255.128

Configure Network IP Filtering from the Configuration Menu

To configure the Digi Passport unit for Network IP filtering, do the following:

1. Access the configuration menu.
2. Select **Network configuration > IP filtering**.

s



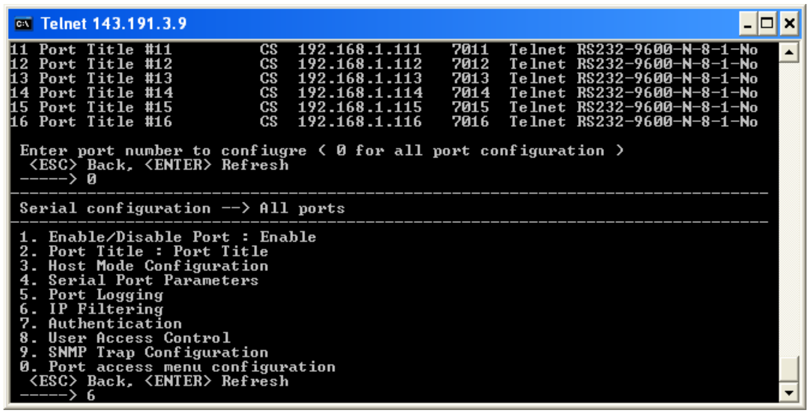
```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 1
--------------------------------------------------------------------------------
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. Select a menu item and enter the desired parameters for the menu items.
4. Use the **ESC** key to return to the main menu.
5. Select **Save changes**.

Configure Port IP Filtering

To configure the Digi Passport unit for Port IP filtering, do the following:

1. Access the configuration menu.
2. Select **Serial port configuration**.
3. Select ***port number*** or **0** (zero) for all ports **> IP filtering**.



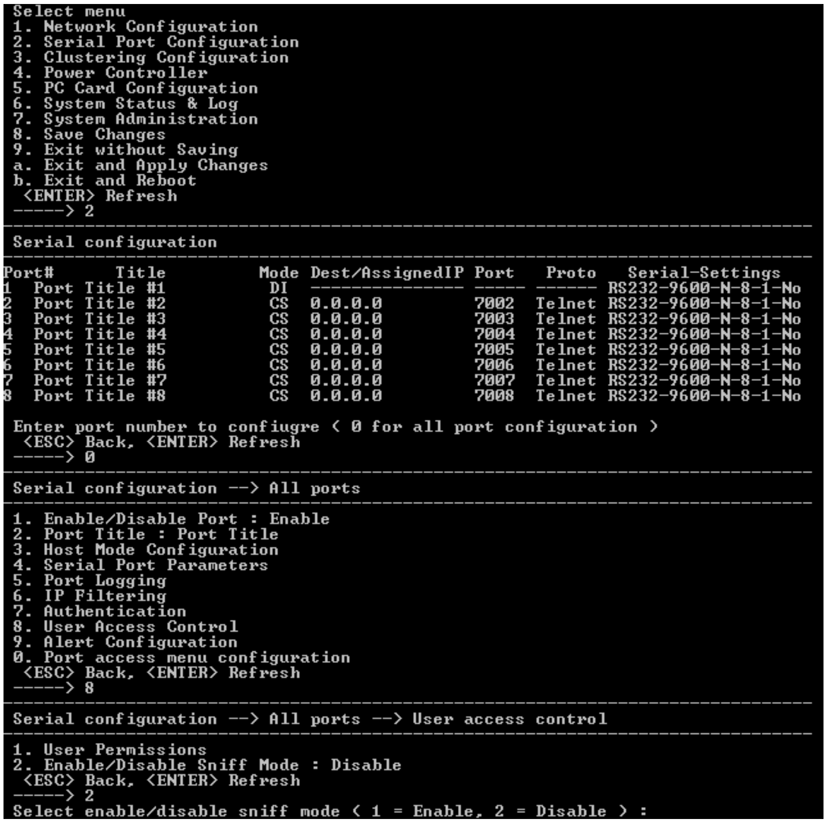
```
11 Port Title #11          CS  192.168.1.111   7011  Telnet RS232-9600-N-8-1-No
12 Port Title #12          CS  192.168.1.112   7012  Telnet RS232-9600-N-8-1-No
13 Port Title #13          CS  192.168.1.113   7013  Telnet RS232-9600-N-8-1-No
14 Port Title #14          CS  192.168.1.114   7014  Telnet RS232-9600-N-8-1-No
15 Port Title #15          CS  192.168.1.115   7015  Telnet RS232-9600-N-8-1-No
16 Port Title #16          CS  192.168.1.116   7016  Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 0
------------------------------------------------------------------------------
 Serial configuration --> All ports
------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. SNMP Trap Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
 -----> 6
```

4. Select a menu item and enter the desired parameters for the menu items.
5. When all parameters are entered, use the **ESC** key to return to the main menu.
6. Select **Save changes**.

Configure and View Sniff Sessions

To configure a port or all ports for sniff users, do the following:

1. Access the configuration menu.
2. Select **Serial port configuration**.
3. Select ***port number*** or **0** (zero) for all ports **> User access control**.
4. Select **User Access Control**.
5. Select **Enable/Disable Sniff Mode**.



```
Select menu
1. Network Configuration
2. Serial Port Configuration
3. Clustering Configuration
4. Power Controller
5. PC Card Configuration
6. System Status & Log
7. System Administration
8. Save Changes
9. Exit without Saving
a. Exit and Apply Changes
b. Exit and Reboot
 <ENTER> Refresh
-----> 2
---------------------------------------------------------------------------------
Serial configuration
---------------------------------------------------------------------------------
Port#      Title          Mode Dest/AssignedIP Port   Proto   Serial-Settings
1  Port Title #1           DI  --------------- -----  ------ RS232-9600-N-8-1-No
2  Port Title #2           CS  0.0.0.0         7002   Telnet RS232-9600-N-8-1-No
3  Port Title #3           CS  0.0.0.0         7003   Telnet RS232-9600-N-8-1-No
4  Port Title #4           CS  0.0.0.0         7004   Telnet RS232-9600-N-8-1-No
5  Port Title #5           CS  0.0.0.0         7005   Telnet RS232-9600-N-8-1-No
6  Port Title #6           CS  0.0.0.0         7006   Telnet RS232-9600-N-8-1-No
7  Port Title #7           CS  0.0.0.0         7007   Telnet RS232-9600-N-8-1-No
8  Port Title #8           CS  0.0.0.0         7008   Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 0
---------------------------------------------------------------------------------
 Serial configuration --> All ports
---------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. Alert Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
 -----> 8
---------------------------------------------------------------------------------
 Serial configuration --> All ports --> User access control
---------------------------------------------------------------------------------
 1. User Permissions
 2. Enable/Disable Sniff Mode : Disable
  <ESC> Back, <ENTER> Refresh
 -----> 2
 Select enable/disable sniff mode ( 1 = Enable, 2 = Disable ) :
```

6. Select a menu item and enter the desired parameters.
7. When all parameters are entered, use the **ESC** key to return to the main menu.
8. Select **Save changes**.

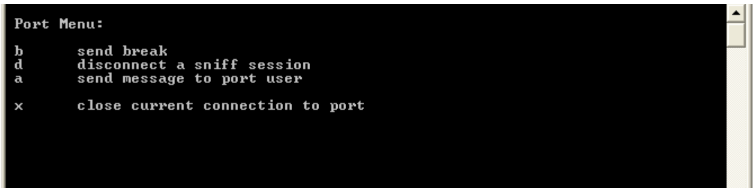
For information on entering a sniff session, see "View a Sniff Session" on page 254.

View a Sniff Session

A sniff user enters a sniff session by starting a Telnet session on a specified port. In the following example, a sniff user uses Telnet to connect to port 7 of the Digi Passport unit. From the command prompt enter the following command:

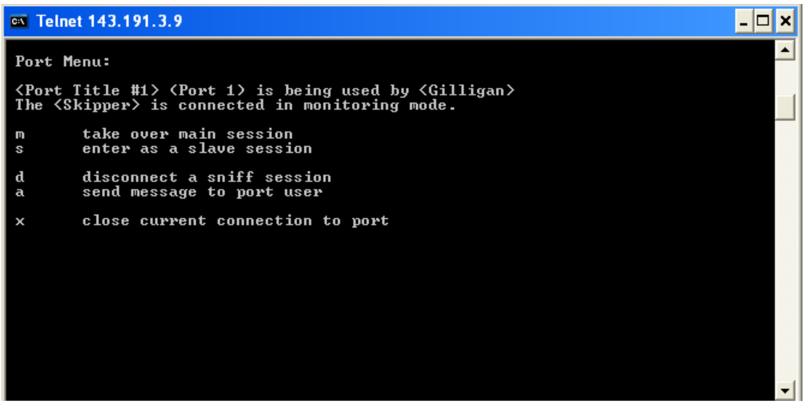
```
telnet 192.168.100.42 7007
```

1. Log in and enter your password.
2. Enter the port escape sequence.



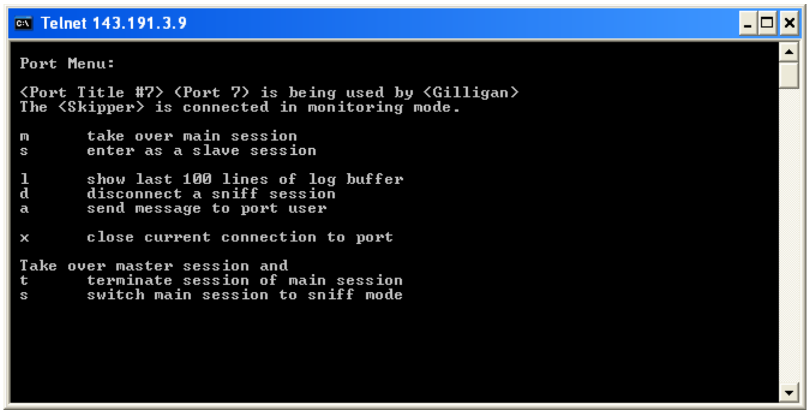
```
Port Menu:

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 allowed options. The first user (with port access rights) to login to the port is in the main session.



```
Port Menu:

<Port Title #1> <Port 1> is being used by <Gilligan>
The <Skipper> is connected in monitoring mode.

m      take over main session
s      enter as a slave session

d      disconnect a sniff session
a      send message to port user

x      close current connection to port
```

The next user (with port access rights) to enter the port will be given the option to take over the main session. This user is given the option to take over the main session by either terminating the first user or switching the first user to sniff (read only).



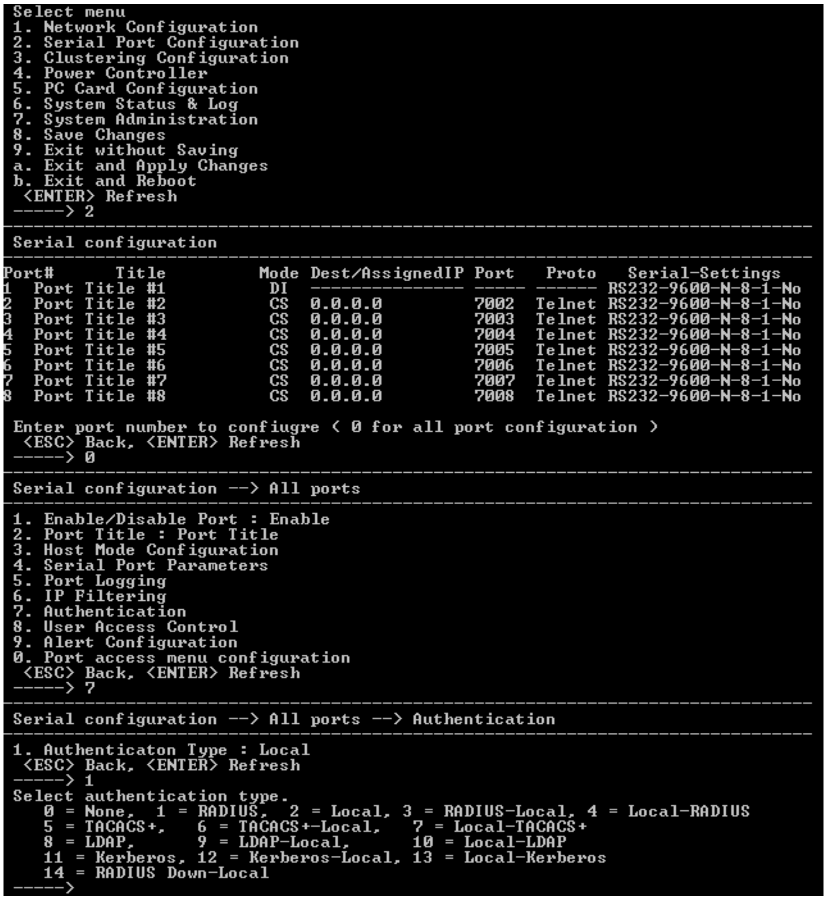
```
Port Menu:

<Port Title #7> <Port 7> is being used by <Gilligan>
The <Skipper> is connected in monitoring mode.

m      take over main session
s      enter as a slave session

l      show last 100 lines of log buffer
d      disconnect a sniff session
a      send message to port user

x      close current connection to port

Take over master session and
t      terminate session of main session
s      switch main session to sniff mode
```

Escape Sequences for Sniff Sessions

Escape Sequence Ctrl+	Action	Occurrence
m	Take over main session (read/write).	Presented only to users with read/write access upon entering a session.
s	Enter as a slave session (read only).	Presented only 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. Select **Serial port configuration**.
3. Select an individual port number or 0 (zero) for all ports > **Authentication**.
4. Select **Authentication type**.



```
 Select menu
 1. Network Configuration
 2. Serial Port Configuration
 3. Clustering Configuration
 4. Power Controller
 5. PC Card Configuration
 6. System Status & Log
 7. System Administration
 8. Save Changes
 9. Exit without Saving
 a. Exit and Apply Changes
 b. Exit and Reboot
  <ENTER> Refresh
 -----> 2
-------------------------------------------------------------------------------
 Serial configuration
-------------------------------------------------------------------------------
Port#      Title         Mode Dest/AssignedIP Port   Proto   Serial-Settings
1  Port Title #1          DI  --------------- ----- ------ RS232-9600-N-8-1-No
2  Port Title #2          CS  0.0.0.0         7002  Telnet RS232-9600-N-8-1-No
3  Port Title #3          CS  0.0.0.0         7003  Telnet RS232-9600-N-8-1-No
4  Port Title #4          CS  0.0.0.0         7004  Telnet RS232-9600-N-8-1-No
5  Port Title #5          CS  0.0.0.0         7005  Telnet RS232-9600-N-8-1-No
6  Port Title #6          CS  0.0.0.0         7006  Telnet RS232-9600-N-8-1-No
7  Port Title #7          CS  0.0.0.0         7007  Telnet RS232-9600-N-8-1-No
8  Port Title #8          CS  0.0.0.0         7008  Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 0
-------------------------------------------------------------------------------
 Serial configuration --> All ports
-------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Port Logging
 6. IP Filtering
 7. Authentication
 8. User Access Control
 9. Alert Configuration
 0. Port access menu configuration
  <ESC> Back, <ENTER> Refresh
 -----> 7
-------------------------------------------------------------------------------
 Serial configuration --> All ports --> Authentication
-------------------------------------------------------------------------------
 1. Authenticaton Type : Local
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select authentication type.
    0 = None,  1 = RADIUS,  2 = Local, 3 = RADIUS-Local, 4 = Local-RADIUS
    5 = TACACS+,   6 = TACACS+-Local,   7 = Local-TACACS+
    8 = LDAP,      9 = LDAP-Local,      10 = Local-LDAP
    11 = Kerberos, 12 = Kerberos-Local, 13 = Local-Kerberos
    14 = RADIUS Down-Local
 ----->
```

5. To the main menu, use the **ESC** key.
6. Select **Save changes**.

Certificate Management

Upload a Server Certificate

To upload a server certificate, use either of these methods,

- Use the **Upload Server Certificate** menu. This menu is displayed only when running **configmenu** on the serial console of the Digi Passport unit. (Running **configmenu** on CLI via Telnet or SHI does not display this menu.)
- Use the **scp** command to copy your **server.pem** file to **/tmp/cnf/etc**. To make this change permanent, run the **saveconf** command from the command line interface.

Create/Use a Server Certificate

To use your server certificate for the Digi Passport unit, after replacing the original server.pem file on **/tmp/cnf/etc** with your own file, import an SSL certificate for the HTTPS interface.

1. Download the latest openssl package.
2. Install the openssl package:

```
# cd /work/
# tar -xvzf openssl-0.9.7c.tar.gz
# cd openssl-0.9.7c
# ./config
# make
# make test
# make install
```

3. Edit the **openssl** configuration file:

```
# vi /usr/share/ssl/openssl.cnf
```

4. In the **openssl.cnf** file, modify the **[req_distinguished_name]** section Refer to sample openssl.conf file (**openssl.conf.digi**).
5. Modify the **[req_attributes]** section as follows:

```
challengePassword_min =0
challengePassword_max =0
```

6. 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
```

7. Use the configuration from this location:

```
/usr/local/ssl/lib/ssleay.cnf
```

8. Generate a 1024-bit RSA private key.

```
........++++++
.....................++++++
```

9. Write new private key to this location:

```
./demoCA/private/./cakey.pem'
```

10. Enter the PEM pass phrase:

```
; CA Password (Enter password and remember this)
Verify password - Enter PEM pass phrase: ; CA Password
-----
```

The information entered next will be incorporated into the certificate.

11. Enter text for a field call Distinguished Name or a DN. Although there are many fields, some can be left blank, use a default, or enter **.** and the field will be left blank.

```
----- ; CA's Information
Country Name (2 letter code) [AU]:  US
State or Province Name (full name) [Your-State]: Minnesota
Locality Name (e.g., city) []: Minneapolis
Organization Name (e.g., company): Digi International
Organizational Unit Name (e.g., section) [](Enter)
Common Name (e.g., YOUR name) []: Bob Alou
Email Address []:(Enter)
#
```

12. Verify that the CA key file (**demoCA/private/cakey.pem**) and CA certificate (**demoCA/cacert.pem**) are generated.

```
# ls demoCA/
cacert.pem certs crl index.txt newcerts
private serial

# ls demoCA/private
cakey.pem
```

Make a Certificate Request

To make new certificates, first, make a certificate request.

1. Enter:

   ```
   # cd /work/openssl-0.9.7c/CA
   ```

2. Run the following commands. It is assumed that the sample configuration file, **openssl.conf.digi**, is being used.

   ```
   # openssl genrsa -out key.pem 1024
   # openssl req -new -key key.pem -out req.pem
   ```

3. Use the configuration from **/usr/share/ssl/openssl.cnf.**

   A prompt is displayed to enter information that will be incorporated into the certificate request.

   There are many fields, but some can be left blank and some fields have default values. Entering **.** leaves the field blank.

4. Enter text for a field call Distinguished Name or a DN.

   ```
   ----- ; CA's Information
   Country Name (2 letter code) [AU]:  US
   State or Province Name (full name) [Your-State]: Minnesota
   Locality Name (e.g., city) []: Minneapolis
   Organization Name (e.g., company): Digi International
   Organizational Unit Name (e.g., section) [](Enter)
   Common Name (e.g., YOUR name or your server’s hostname) []: Digi
   Passport
   Email Address []:(Enter)
   ```

5. Enter the following 'extra' attributes to be sent with the certificate request:

   ```
   A challenge password []:(Press Enter - Do not enter any other
   characters)
   An optional company name []:(Press Enter - Do not enter any other
   characters)
   ```

Sign a Certificate Request

1. To sign a certificate request, enter the following:

   ```
   # cd /work/openssl-0.9.7c/CA
   # cp req.pem newreq.pem
   # sh /usr/local/ssl/misc/CA.sh -sign
   ```

2. Use the configuration from sample file **/usr/share/ssl/openssl.cnf**.
3. Enter PEM pass phrase. Enter the CA Password created in "Create/Use a Server Certificate" on page 257, in the step that begins **Enter the PEM pass phrase**.

   ```
   CA Password
   ```

4. 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
   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
   ```

5. Verify that the signed certificate, **newcert.pem**, is generated.

```
# ls
demoCA key.pem newcert.pem newreq.pem req.pem
```

Make Certificate for the Digi Passport Unit

1. Remove 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. Concatenate file **key.pem** to **server.pem**:

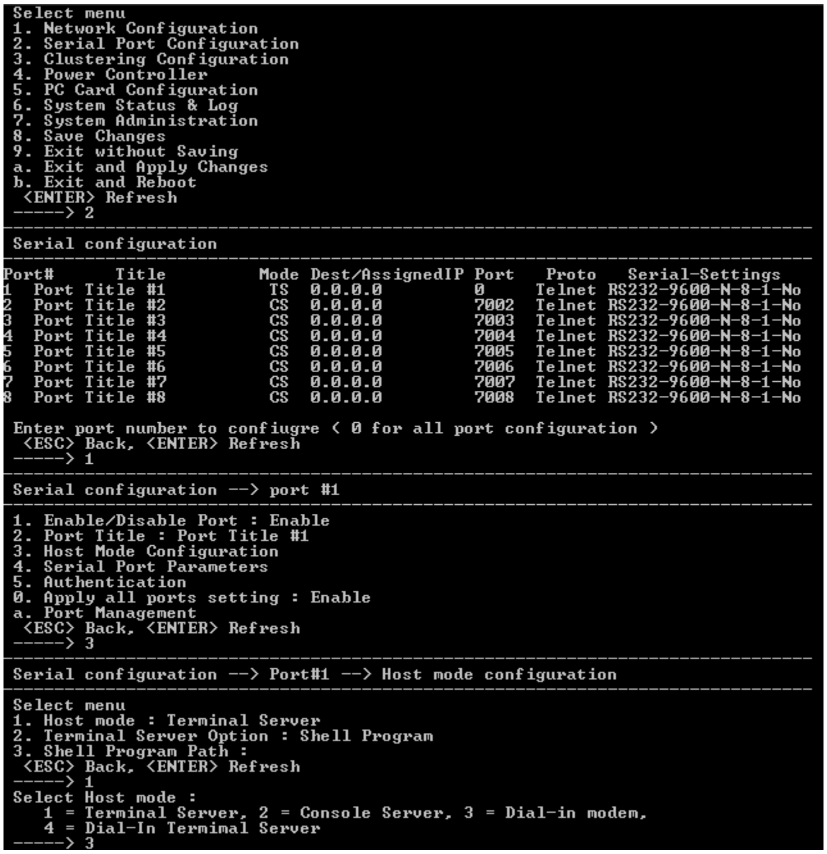
```
# cat key.pem >> server.pem
```

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. Select **Serial Port Configuration**.
3. Select an individual port number and then **Host Mode Configuration**.
4. Select **Host mode** and then **Dial-in modem**.



```
 Select menu
 1. Network Configuration
 2. Serial Port Configuration
 3. Clustering Configuration
 4. Power Controller
 5. PC Card Configuration
 6. System Status & Log
 7. System Administration
 8. Save Changes
 9. Exit without Saving
 a. Exit and Apply Changes
 b. Exit and Reboot
  <ENTER> Refresh
 -----> 2
--------------------------------------------------------------------------------
 Serial configuration
--------------------------------------------------------------------------------
Port#      Title         Mode Dest/AssignedIP Port    Proto   Serial-Settings
1  Port Title #1          TS  0.0.0.0         0      Telnet RS232-9600-N-8-1-No
2  Port Title #2          CS  0.0.0.0         7002   Telnet RS232-9600-N-8-1-No
3  Port Title #3          CS  0.0.0.0         7003   Telnet RS232-9600-N-8-1-No
4  Port Title #4          CS  0.0.0.0         7004   Telnet RS232-9600-N-8-1-No
5  Port Title #5          CS  0.0.0.0         7005   Telnet RS232-9600-N-8-1-No
6  Port Title #6          CS  0.0.0.0         7006   Telnet RS232-9600-N-8-1-No
7  Port Title #7          CS  0.0.0.0         7007   Telnet RS232-9600-N-8-1-No
8  Port Title #8          CS  0.0.0.0         7008   Telnet RS232-9600-N-8-1-No

 Enter port number to confiugre ( 0 for all port configuration )
  <ESC> Back, <ENTER> Refresh
 -----> 1
--------------------------------------------------------------------------------
 Serial configuration --> port #1
--------------------------------------------------------------------------------
 1. Enable/Disable Port : Enable
 2. Port Title : Port Title #1
 3. Host Mode Configuration
 4. Serial Port Parameters
 5. Authentication
 0. Apply all ports setting : Enable
 a. Port Management
  <ESC> Back, <ENTER> Refresh
 -----> 3
--------------------------------------------------------------------------------
 Serial configuration --> Port#1 --> Host mode configuration
--------------------------------------------------------------------------------
 Select menu
 1. Host mode : Terminal Server
 2. Terminal Server Option : Shell Program
 3. Shell Program Path :
  <ESC> Back, <ENTER> Refresh
 -----> 1
 Select Host mode :
    1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
    4 = Dial-In Terminal Server
 -----> 3
```

5. To return to the main menu, use the **ESC** key.
6. Select **Save changes**.

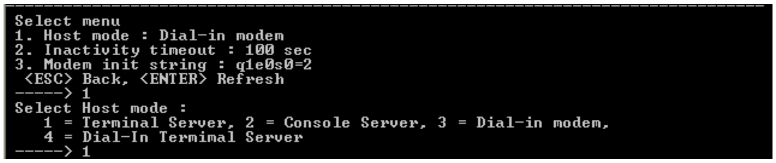
Dial-in Terminal Server Access

Individual serial ports on the Digi Passport unit can be configured for dial-in terminal server access. To use dial-in terminal server access, an external modem is attached to a serial port on the Digi Passport unit, 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.

Terminal server mode makes a direct connection to a server.

To configure a serial port for a dial-in terminal server:

1. Access the configuration menu.
2. Select **Serial port configuration**.
3. Select an individual port number and then **Host Mode Configuration**.



```
Select menu
1. Host mode : Dial-in modem
2. Inactivity timeout : 100 sec
3. Modem init string : q1e0s0=2
 <ESC> Back, <ENTER> Refresh
-----> 1
Select Host mode :
   1 = Terminal Server, 2 = Console Server, 3 = Dial-in modem,
   4 = Dial-In Termimal Server
-----> 1
```

4. Select **Dial-in Terminal Server** and configure the other configuration parameters.
5. To return to the main menu, use the **ESC** key.
6. Select **Save changes**.

Clustering

By default, clustered slave devices are configured using the Telnet protocol and the following port parameters:

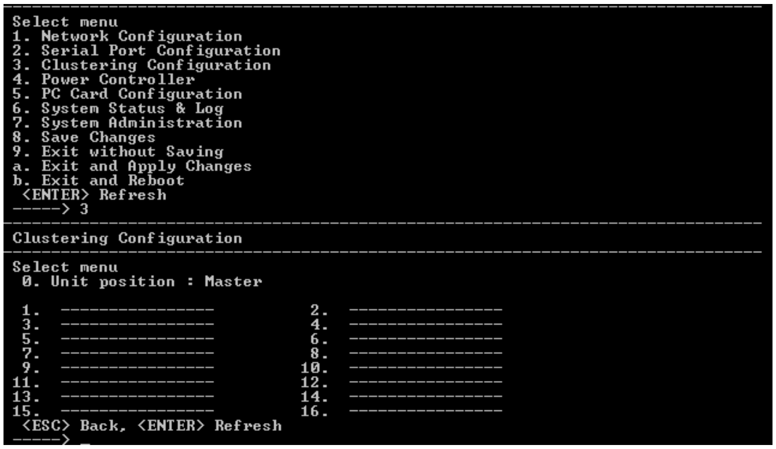
- **bps**=9600
- **data bits**=8
- **parity**=none
- **stop bits**=1
- **flow control**=none

When the master device autoconfigures a slave device, it simply imports the information from the slave unit. To use other protocols or port parameters, configure the slave unit with those parameters before autoconfiguring.

Set Up Digi Passport for Clustering

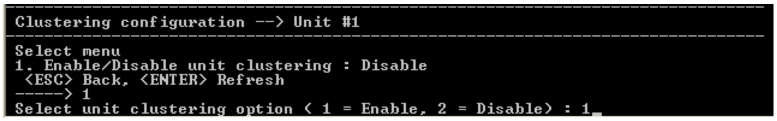
To set up the Digi Passport unit for clustering:

1. Access the configuration menu.
2. Select **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
-----> _
```

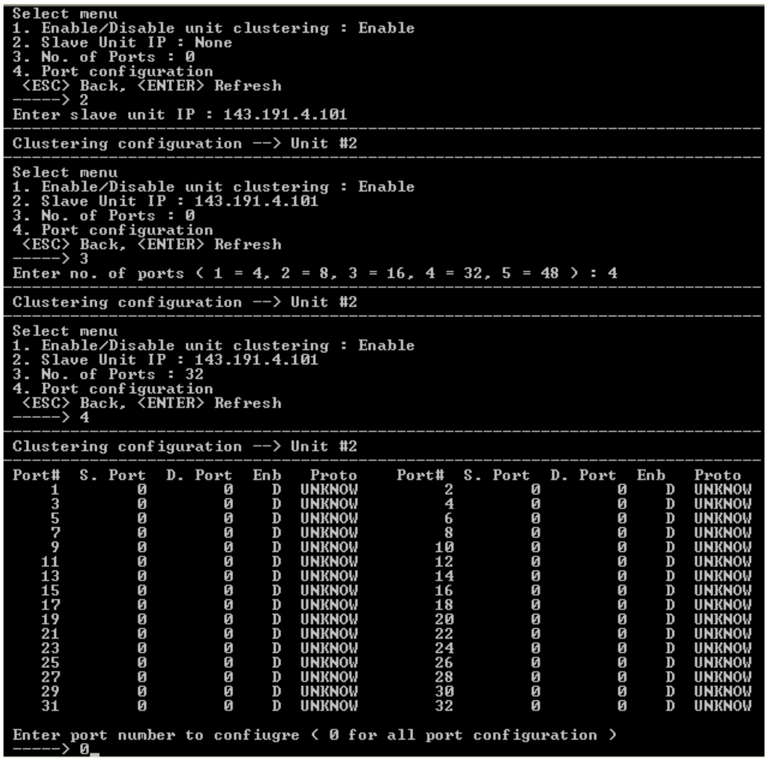
4. Enter the number 1 for the first slave unit.
5. Select **Enable/Disable unit clustering > Enable**.



```
Clustering configuration --> Unit #1
---------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Disable
 <ESC> Back, <ENTER> Refresh
-----> 1
Select unit clustering option ( 1 = Enable, 2 = Disable) : 1_
```

6. Enter the values for **Slave Unit IP**, **No. of ports**, and **Port configuration**.

7. Select the ***port number*** to configure or **0** for all ports.



```
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : None
3. No. of Ports : 0
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 2
Enter slave unit IP : 143.191.4.101
-------------------------------------------------------------------------------
Clustering configuration --> Unit #2
-------------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : 143.191.4.101
3. No. of Ports : 0
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 3
Enter no. of ports ( 1 = 4, 2 = 8, 3 = 16, 4 = 32, 5 = 48 ) : 4
-------------------------------------------------------------------------------
Clustering configuration --> Unit #2
-------------------------------------------------------------------------------
Select menu
1. Enable/Disable unit clustering : Enable
2. Slave Unit IP : 143.191.4.101
3. No. of Ports : 32
4. Port configuration
 <ESC> Back, <ENTER> Refresh
-----> 4
-------------------------------------------------------------------------------
Clustering configuration --> Unit #2
-------------------------------------------------------------------------------
Port#  S. Port  D. Port  Enb   Proto    Port#  S. Port  D. Port  Enb   Proto
    1        0        0    D  UNKNOW        2        0        0    D  UNKNOW
    3        0        0    D  UNKNOW        4        0        0    D  UNKNOW
    5        0        0    D  UNKNOW        6        0        0    D  UNKNOW
    7        0        0    D  UNKNOW        8        0        0    D  UNKNOW
    9        0        0    D  UNKNOW       10        0        0    D  UNKNOW
   11        0        0    D  UNKNOW       12        0        0    D  UNKNOW
   13        0        0    D  UNKNOW       14        0        0    D  UNKNOW
   15        0        0    D  UNKNOW       16        0        0    D  UNKNOW
   17        0        0    D  UNKNOW       18        0        0    D  UNKNOW
   19        0        0    D  UNKNOW       20        0        0    D  UNKNOW
   21        0        0    D  UNKNOW       22        0        0    D  UNKNOW
   23        0        0    D  UNKNOW       24        0        0    D  UNKNOW
   25        0        0    D  UNKNOW       26        0        0    D  UNKNOW
   27        0        0    D  UNKNOW       28        0        0    D  UNKNOW
   29        0        0    D  UNKNOW       30        0        0    D  UNKNOW
   31        0        0    D  UNKNOW       32        0        0    D  UNKNOW

Enter port number to confiugre ( 0 for all port configuration )
-----> 0_
```

8. Select **Enable configuration**.
9. Select **Auto Configuration**.
10. Select **Exit** and apply changes.

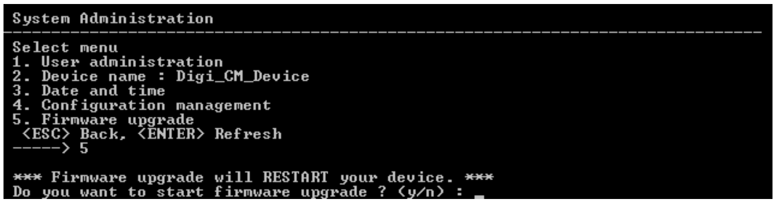
Upgrade Firmware

Before upgrading firmware from the configuration menu:

- Download the firmware to a system on the same subnet.
- Set up a terminal emulation program that supports the Zmodem transfer protocol.

To upgrade the firmware with the configuration menu:

1. Access the configuration menu.
2. Select **System administration**.



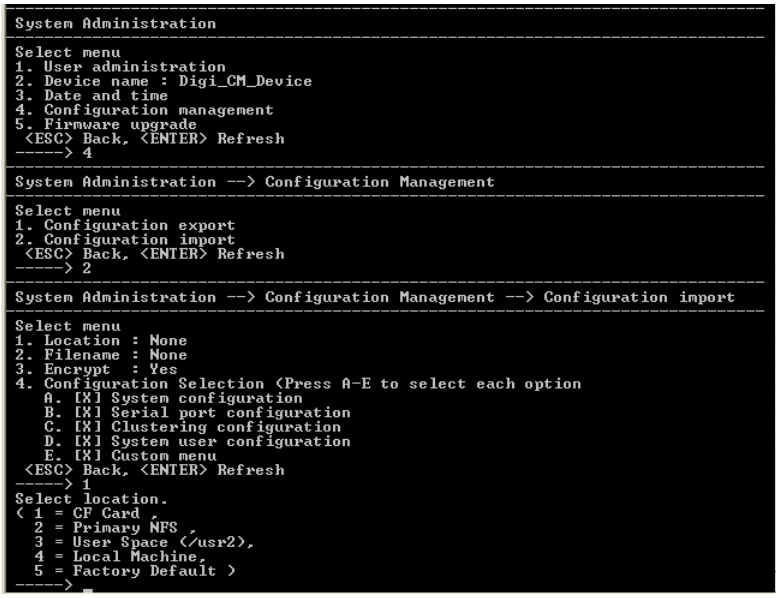
```
System Administration
--------------------------------------------------------------------------------
Select menu
1. User administration
2. Device name : Digi_CM_Device
3. Date and time
4. Configuration management
5. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
-----> 5

*** Firmware upgrade will RESTART your device. ***
Do you want to start firmware upgrade ? (y/n) : _
```

3. Select **Firmware upgrade**. Enter **y** for Yes when prompted whether to upgrade the firmware.
4. If the firmware upgrade is successful, the Digi Passport unit reboots automatically. If a **Firmware upgrade failed!** warning is displayed, do not reboot the unit but repeat the upgrade process.

Restore Factory Defaults

There are two choices to restore the unit to its factory defaults: restoring all factory defaults, or restoring all factory defaults except IP settings. To restore the Digi Passport unit unit to the factory defaults:

1. Access the configuration menu.
2. Select **System administration**.
3. Select **Configuration import**.
4. Select **Location**.



```
-------------------------------------------------------------------------------
System Administration
-------------------------------------------------------------------------------
Select menu
1. User administration
2. Device name : Digi_CM_Device
3. Date and time
4. Configuration management
5. Firmware upgrade
 <ESC> Back, <ENTER> Refresh
-----> 4
-------------------------------------------------------------------------------
System Administration --> Configuration Management
-------------------------------------------------------------------------------
Select menu
1. Configuration export
2. Configuration import
 <ESC> Back, <ENTER> Refresh
-----> 2
-------------------------------------------------------------------------------
System Administration --> Configuration Management --> Configuration import
-------------------------------------------------------------------------------
Select menu
1. Location : None
2. Filename : None
3. Encrypt  : Yes
4. Configuration Selection (Press A-E to select each option
   A. [X] System configuration
   B. [X] Serial port configuration
   C. [X] Clustering configuration
   D. [X] System user configuration
   E. [X] Custom menu
 <ESC> Back, <ENTER> Refresh
-----> 1
Select location.
( 1 = CF Card ,
  2 = Primary NFS ,
  3 = User Space (/usr2),
  4 = Local Machine,
  5 = Factory Default )
----->
```

5. Select **Factory Default**. The system will restore factory defaults, and the unit will automatically reboot.
6. Use System Administration to save the configuration in case it needs to be reloaded later or onto another system. See "Add and Configure a PC Card" on page 241 for more information.

Set Date and Time

Date and time on the Digi Passport unit can either be kept internally or by an NTP server. It is easier to set the date and time from the Digi Passport unit’s Web interface "Set Date and Time" on page 298. To set the date and time from the configuration menu:

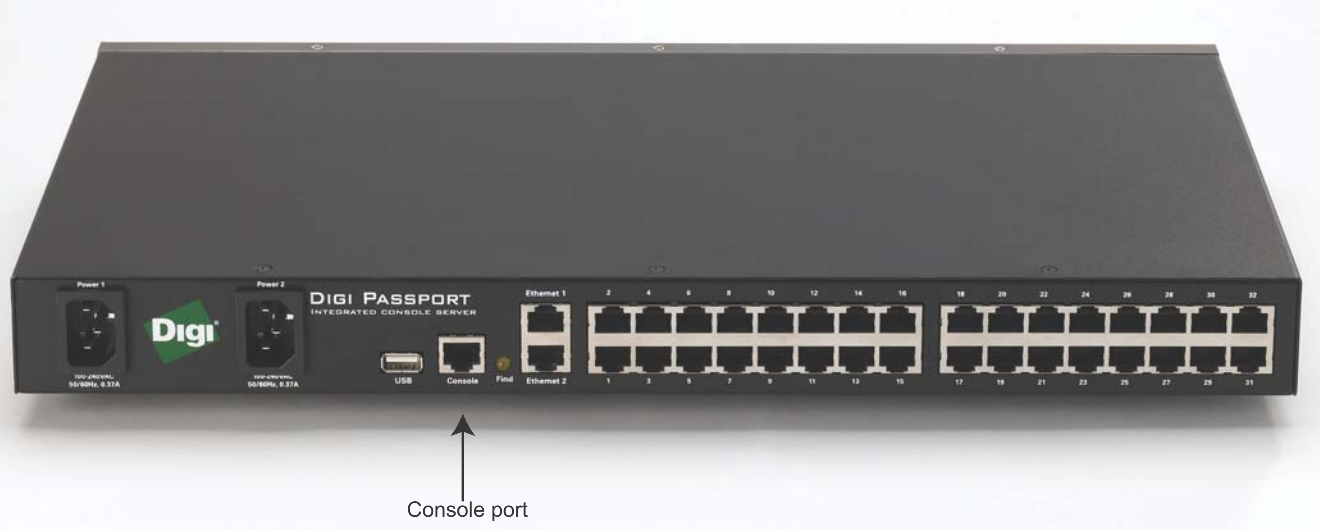
1. Access the configuration menu.
2. Select **System administration**.
3. Select **Date and Time**.
4. Enter the desired parameters.
5. Select **Save changes**.

Access the Boot Loader Program

The Boot Loader program can be accessed during the boot process. The main function of the program is to provide a backup means for restoring the firmware if the Digi 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:

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. In the photo of the back panel of the Digi Passport unit below, the arrow points to the console port. (The photo shows the back panel of a Digi Passport 32.)



Console port

2. Set up a terminal emulation program, such as HyperTerminal, using the following port parameters:
   - **bps**=9600
   - **data bits**=8
   - **parity**=none
   - **stop bits**=1
   - **flow control**=none
3. Turn on the power to the Digi Passport 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, select the number **3** to access the Hardware test. Options for several components appear.

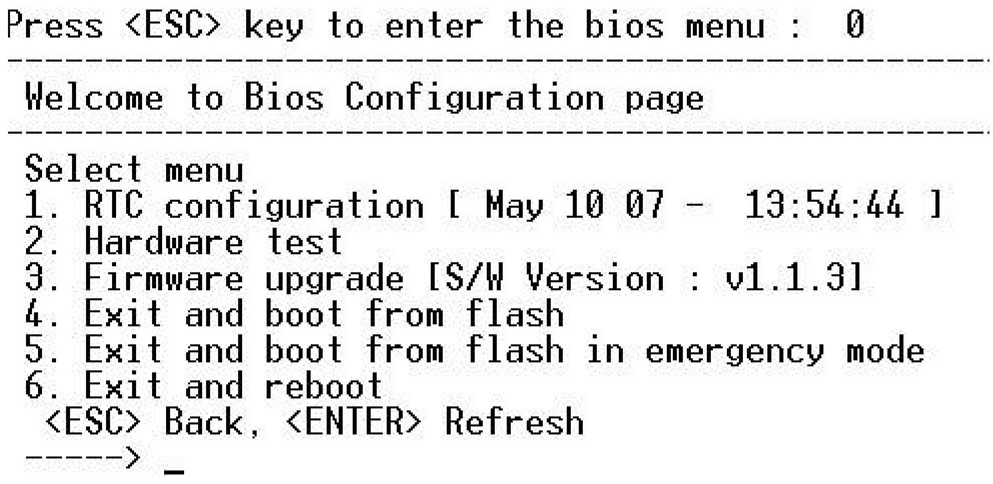
Disaster Recovery

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 using the Boot Loader program.

Restore Digi Passport to Factory Default Settings

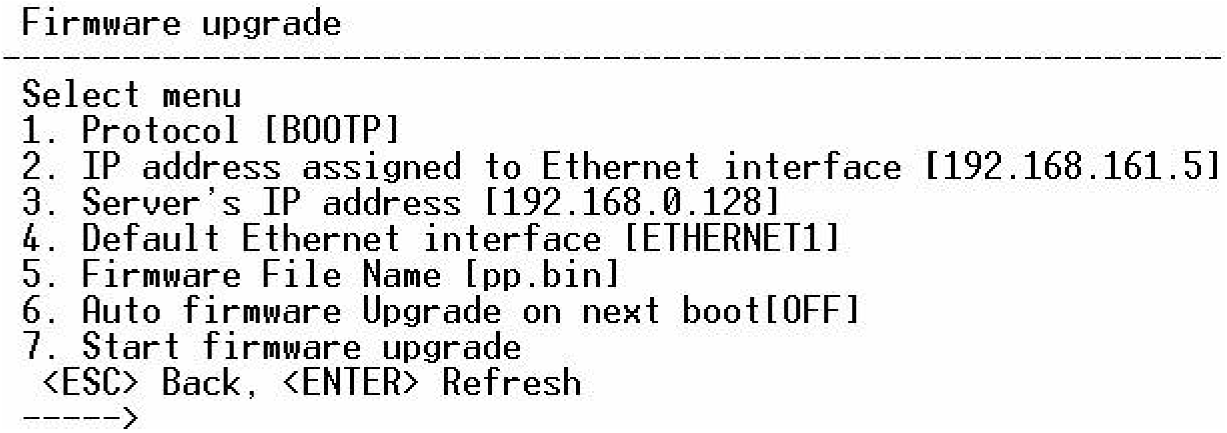
To restore the Digi Passport unit to the factory default configuration settings, use a TFTP or BOOTP server. To use the Boot Loader program to flash new firmware, do the following:

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 is displayed. Use the ESC key to return to an earlier menu screen, and the Enter key to refresh the menu screen.



```
Press <ESC> key to enter the bios menu :  0
------------------------------------------------------
 Welcome to Bios Configuration page
------------------------------------------------------
 Select menu
 1. RTC configuration [ May 10 07 -  13:54:44 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.1.3]
 4. Exit and boot from flash
 5. Exit and boot from flash in emergency mode
 6. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 -----> _
```

5. Choose **Firmware upgrade** by entering **3**. The following screen is displayed.



```
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. Default Ethernet interface [ETHERNET1]
5. Firmware File Name [pp.bin]
6. Auto firmware Upgrade on next boot[OFF]
7. 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.
   - **Ethernet interface**: 1 or 2.

   Use the ESC key to return to earlier menu screens.
7. Select **Start firmware upgrade**.

   The firmware upgrade will take several minutes to process.

   The factory default settings will be restored.
8. When the upgrade process is complete, press the **ESC** key to return to the main menu.
9. Select **Exit** and boot from flash.

Configmenu scripting

There are scripting capabilities built into Configmenu as a convenience for command-line users who need to configure multiple devices via scripts.

Note: Not all sections of Configmenu support the scripting feature (Clustering and Power Controller do not support scripting).

Syntax and examples

The following command line options are supported for scripting to UI (configmenu) in the CLI.

```
[root@Digi_Passport4 ~]# configmenu -help
Usage : configmenu [OPTION]
Option :
         -help : display this help and exit
         -f [Script file name] : read command from script file
         get [XML_PATH1 XML_PATH2 ...] : get value of XML_PATH
        set [XML_PATH1=VALUE1 XML_PATH2=VALUE2 ...] : set value to
  XML_PATH
         del rport [remote port number]
         add rport [listening port number]
         save : save change configuration
         apply : apply change configuration
```

Rules for these options include:

- “get” and “set” options can have multiple values.
- “save” and “apply” commands should be appended to set values.
- Add the remote port first using “add rport” before setting other parameters.
- Listening TCP port number should be provided if adding a new remote port but remote port number is required if deleting a remote port.
- All commands should be in one line.
- The configmenu supports configuration setting/getting with parameter's XML path & value as argument.
- Each XML path is defined in each configuration file under the **/tmp/cnf/** directory.

For example, you can find the XML paths related with IP configuration in file **tmp/cnf/sys/network/ip.cnf** as follows

```
[root@Digi_Passport ~]# more /tmp/cnf/sys/network/ip.cnf
/network/ip/dns1=206.13.28.12
/network/ip/dns2=0.0.0.0
/network/ip/ipconf1/ipconf1/gateway=10.0.0.1
/network/ip/ipconf1/ipconf1/ip_addr=10.0.5.1
/network/ip/ipconf1/ipconf1/ip_mode=1
/network/ip/ipconf1/ipconf1/s_ip_enb=0
/network/ip/ipconf1/ipconf1/subnet=255.255.0.0
/network/ip/ipconf1/ipconf1_ipv6/ip_mode=0
/network/ip/ipconf1/ipconf1_ipv6/ipv6to4_enb=0
/network/ip/ipconf2/ipconf2/ip_addr=192.169.161.5
/network/ip/ipconf2/ipconf2/ip_mode=0
/network/ip/ipconf2/ipconf2/s_ip_enb=0
/network/ip/ipconf2/ipconf2/subnet=255.255.0.0
/network/ip/ipconf2/ipconf2_ipv6/ip_mode=0
/network/ip/ipconf2/ipconf2_ipv6/ipv6to4_enb=0
/network/ip/manual_dns_enb=1
/network/ip/reuse_old_ip=0
/network/ip/src_based_route=0
```

To get the IP address of Ethernet 2 port(eth1), run the following command:

```
[root@Digi_Passport ~]# configmenu get /network/ip/ipconf2/
  ipconf2/ip_addr
Get : /network/ip/ipconf2/ipconf2/ip_addr=10.0.5.2
```

To set the IP address of Ethernet 2 port(eth1), run the following command:

```
[root@Digi_Passport ~]# configmenu set /network/ip/ipconf2/
  ipconf2/ip_addr=10.0.5.2
Set : /network/ip/ipconf1/ipconf1/ip_addr=10.0.5.2
```

To save the changes, run the "set" and "save" commands as shown below:

```
[root@Digi_Passport ~]# configmenu set /network/ip/ipconf2/
  ipconf2/ip_addr=10.0.5.2 save
Set : /network/ip/ipconf2/ipconf2/ip_addr=10.0.5.2
```

To apply the changes, issue the “apply” command:

```
[root@Digi_Passport ~]# configmenu set /network/ip/ipconf2/
  ipconf2/ip_addr=10.0.5.2 save apply
Set : /network/ip/ipconf2/ipconf2/ip_addr=10.0.5.2
.............
Apply Done.
```

The “apply” command can be also run separately after saving all changes

```
[root@Digi_Passport ~]# configmenu set /network/ip/ipconf2/
  ipconf2/ip_mode=1 save
Set : /network/ip/ipconf2/ipconf2/ip_mode=static IP (1)
[root@Digi_Passport ~]# configmenu set /network/ip/ipconf2/
  ipconf2/ip_addr=10.0.5.2 save
Set : /network/ip/ipconf2/ipconf2/ip_addr=10.0.5.2
[root@Digi_Passport ~]# configmenu apply
.............
Apply Done.
```

Here is an example of adding a new remote port with a TCP port of 7005:

```
[root@Digi_Passport4 ~]# configmenu add rport 7005 save apply
Add : /serial/serial_config/ports/*5
Set : /serial/serial_config/ports/*5/hostmode/listening_port=7005
...
Save Done.
..
Apply Done.
[root@Digi_Passport4 ~]#
```

All other settings, such as remote port parameters, must be set to make the remote port work correctly.

```
[root@Digi_Passport4 ~]# configmenu set \
/serial/serial_config/ports/*5/rport_param/dest_ip=192.168.1.2 \
/serial/serial_config/ports/*5/rport_param/dest_port=22 \
/serial/serial_config/ports/*5/rport_param/protocol=2 save apply

Set : /serial/serial_config/ports/*5/rport_param/
  dest_ip=192.168.1.2
Set : /serial/serial_config/ports/*5/rport_param/dest_port=22
Set : /serial/serial_config/ports/*5/rport_param/protocol=SSH (2)
..
Save Done.
.
Apply Done.
[root@Digi_Passport4 ~]#
```

Configuration commands can be entered and executed in a script file, as shown below. Each command should be on a separate line and the "save" and "apply" commands should be added at the end of file if you want to apply your changes.

```
[root@Digi_Passport4 ~]# more /usr2/rpot2
add rport 7006
set /serial/serial_config/ports/*6/rport_param/dest_ip=192.168.1.2
set /serial/serial_config/ports/*6/rport_param/dest_port=22
set /serial/serial_config/ports/*6/rport_param/protocol=2
save
apply
[root@Digi_Passport4 ~]# configmenu -f /usr2/rpot2
Add : /serial/serial_config/ports/*6
Set : /serial/serial_config/ports/*6/hostmode/listening_port=7006
Set : /serial/serial_config/ports/*6/rport_param/
  dest_ip=192.168.1.2
Set : /serial/serial_config/ports/*6/rport_param/dest_port=22
Set : /serial/serial_config/ports/*6/rport_param/protocol=SSH (2)
..
Save Done.
.....
Apply Done.
[root@Digi_Passport4 ~]#
```

To check XML paths and values, see these configuration files ,

/tmp/cnf/ports/port#/portinfo.cnf: Serial port # configuration

/tmp/cnf/sys/: System configuration

/tmp/cnf/sys/network: Network configuration

Current limitations

The following menus are not supported in scripting:

- Change password
- System status & log -> System status
- System status & log -> System log view
- Access lists add/remove
- User administration add/remove/edit => use 'passwd' command in the CLI
- Port automatic detection configuration
- Power controller management
- Peripherals configuration
- Firmware upgrade
- Configuration management

Chapter 17 Command Line Interface

Digi Passport runs the embedded Embedded 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 command line interface (CLI) 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.

Back Up All Configuration Files Before Using Commands

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 configuration files.

Linux Commands

This section lists 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. For more detailed command information, see the man pages on a Linux system.

Commands for Saving and Applying Changes

Two commands that are very important for saving and applying changes to the configuration files are:

- **saveconf**: Saves the configuration files to flash memory.
- **applyconf**: Immediately applies the configuration changes.

The configuration files are located in directory **/tmp/cnf**.

Commands for accessing and configuring Passport unit and serial ports

Several commands are used for accessing and configuring the Digi Passport unit and the serial ports.

- **configmenu**: A menu for system administrators 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.
- **connect:** Connects to ports, ether local or slave ports. The syntax is: `connect [-s slave ip address] [serial port]`
- **factory_reset:**

  Restore all configurations.

  Restore all configurations except user script (/usr2/rc.user).

  Restore all configurations except Perl packages.

  Restore all configurations except user script & Perl packages.
- **portaccessmenu**: A menu that allows access to the serial ports on the Digi Passport unit.
- **portset #**: Resets a specific port and restarts all processes associated with the port.

Dual Network Options

Source Based Routing

When more than one router is needed, with each network interface using a different router, set up source-based routing on the Passport.

The following commands are needed to be run for source based routing on the Passport

```
# /sbin/ip rule add from $IP table $TBL
# /sbin/ip route add default dev $ETH via $GW table $TBL
# /sbin/ip route add $NET dev $ETH table $TBL
```

where:

$IP is an IP address which should use a non-default gateway.

$NET is an IP network which should be routed straight, that is, not through the gateway.

$ETH is the network interface to route to

$GW is a gateway for this IP address.

$TBL is any free table name which is defined in /etc/iproute2/rt_tables file.

Note that every new non-standard gateway will require another table number.

If the **Source based routing** option is enabled under Network -> IP configuration in the Passport, then /etc/iproute2/setsbr.sh script will be started to run commands above for the interface eth1 automatically.

That is, $IP will be the IP address of eth1 interface, $NET will be the subnet mask of eth1 interface, $ETH will be eth0, $GW will be the gateway of eth1 interface and $TBL will be auxtbl by default.

This script can be modified to make eth1 as the main default gateway or add some more conditions.

For more information about source based routing from 'ip rule' and 'ip route' section of the Linux ip man page or Appendix D of "Guide to IP Layer Network Administration with Linux" (http://linux-ip.net/html/linux-ip.html#tools-ip-routing)

Ethernet Bridging

Ethernet bridging is commonly used to connect different networks of Ethernets together, so that these Ethernets will appear as one Ethernet to the participants. Ethernet bridging essentially involves combining an Ethernet interface with one or more physical Ethernet interfaces and bridging them together under the umbrella of a single bridge interface. Ethernet bridges represent the software analog to a physical Ethernet switch. The Ethernet bridge can be thought of as a kind of software switch which can be used to connect multiple Ethernet interfaces (either physical or virtual) on a single machine while sharing a single IP subnet.

In the Passport, a script file, **brmode** (/etc/init.d/**brmode**), can be used to enable/disable the Ethernet bridging. (Ethernet Bridging is supported only through CLI command. There is no option in UI.)

To enable the Ethernet Bridging, run following command in the CLI.

```
# service brmode start
```

Then, the IP address of the eth0 interface will be the common IP address for the bridging mode interface(br0).

After enabling Ethernet Bridging, eth0 and eth1 address will disappear.

Note that there will be a delay of a few minutes for changing the physical interface from Ethernet 1 port to Ethernet 2 port automatically by the bridging function. And also please note that eth1 (IP address #2) interface should be enabled first before start bridging.

To disable the Ethernet Bridging, run following command in the CLI.

```
# service brmode stop
```

To customize the bridging configuration, modify **/etc/init.d/brmode** and refer to Linux manual page regarding brctl for detailed configuration options.

Run the following command to remove following message on the serial console:

```
# brctl setageing br0 0
```

Shell and Shell Utilities

- ash
- bash
- echo
- env
- false
- grep
- more
- pwd
- sed
- sh
- which

File and Disk Utilities

- cat
- chmod
- cp
- dd
- df
- du
- e2fsck
- find
- fsck
- gunzip
- gzip
- ln
- ls
- mkdir
- mkdosfs
- mke2fs
- mknod
- mount
- mv
- rm
- rmdir
- scp
- sync
- tail
- tar
- touch
- vi
- umount
- zcat

System Utilities

- date
- free
- half
- hostname
- id
- init
- insmod
- kill
- killall
- lsmod
- modprobe
- poweroff
- ps
- reboot
- reset
- rmmod
- shutdown
- sleep
- stty
- su
- telnet
- uname
- useradd
- userdel
- usermod
- who
- whoami

Network Utilities

- ftp
- ifconfig
- iptables
- netstat
- ping
- route
- telnet
- ssh

Important File Locations

The Digi Passport unit has several files that are important for administrative use. This section lists and briefly describes some of the files that the root user or system administrator may wish to view, monitor, and 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

Configuration (Config) files for the most part reside in subdirectories of **tmp/cnf**. Config files include:

File Name	Description
/.ssh	SSH public key files. The format of key files is *name*_auth_key2.
active_detect	Active port detection configuration.
passive_detect	Passive port detection configuration.
rportcon	Remote port configuration.
./cluster_p2p	Directory for peer-to-peer clustering
cluster.cnf	Basic cluster information.
./cluster_p2p/cluster_p2p.cnf	Basic peer-to-peer cluster information.
unit#.cnf	Basic slave information.
/etc client.pem	Web Certificate
dhcpd.opt	DHCP certificate file.
group	User group information.
hostname	Passport host name.
hosts	Name resolution hosts file.
interfaces	Basic loopback (lo) and Ethernet interface (eth0, eth1) info (Ip, gateway, etc).
ip6tables.save	IPv6 IP access
iptables.save	IPv4 access

File Name	Description
krb5.conf	Kerberos configuration 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
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 ./xinetd.d/master ./xinetd.d/port# ./xinetd.d/telnet	Network services for serial and remote ports
./menu	Directory for custom menu XML files
./allports	All ports configuration directory.
./master.cnf	Port access menu configuration file.
./port#	Specific port and remote configuration directory.
./port#/keywords.cnf	Port and remote port keyword alert file.
./port#/portinfo.cnf	Port and remote port information file.
./rport.default	Remote port configuration directory.
./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

File Name	Description
ccard.cnf	PC Card
security.cnf	Security profile
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

Save 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 desired commands.

   ```
   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
   ```

If the Digi Passport unit is reset to factory defaults, the file **/usr2/rc.user** script file is moved to file **/usr2/rc.user.old#** and the default file **rc.user** is restored.

Change RADIUS socket ports

The radius client obtains the radius socket ports to use via the file **/etc/services**. The client only looks up the lines starting with **radius** and **radacct**.

1. In file **/etc/services,** change lines starting with **radius** and **radacct** to the desired socket numbers. For example:

   ```
   radius 1645/tcp
   radius 1645/ucp
   radacct 1646/tcp
   radacct 1646/ucp
   ```

2. After editing **/etc/services**, copy it to **/usr2:**

   ```
   cp /etc/services /usr2
   ```

3. Edit **/usr2/rc.user** and add this line just above **exit 0**:

   ```
   cp -a /usr2/services /etc/services
   ```

4. Reboot:

   ```
   reboot
   ```

If the Digi Passport unit is reset to factory defaults, the script file **/usr2/rc.user** is moved to **/usr2/rc.user.old#** and the default file **rc.user** is restored.

Limit root access to the console on Digi Passport products (for SSH only)

Limiting root access to the console prevents root access from any means except physically logging in on the Digi Passport console. To limit root access:

1. Modify file **/etc/inetd.conf** and append **-f /usr2/sshd_config** to the **sshd** line.

   ```
   cp /etc/inetd.conf /usr2/inetd.conf
   ```

2. Edit file **/etc/ssh/sshd_config**. Change **PermitRootLogin** to **no**.

   ```
   cp /etc/ssh/sshd_config /usr2
   ```

3. In the in the **/usr2/rc.user** script, add the following 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
   ```

If the Digi Passport unit is reset to factory defaults the script file **/usr2/rc.user** is moved to **/usr2/rc.user.old#** and the default file **rc.user** is restored.

Send break from existing session with the Digi Passport unit

From a Telnet session

If the Telnet session was initiated from a UNIX command line Telnet client, issuing the Telnet escape sequence **^]** (control-right_square_bracket) displays the **telnet>** prompt.

```
telnet>send brk
```

Other Telnet clients often have a "send break" option.

From an ssh session

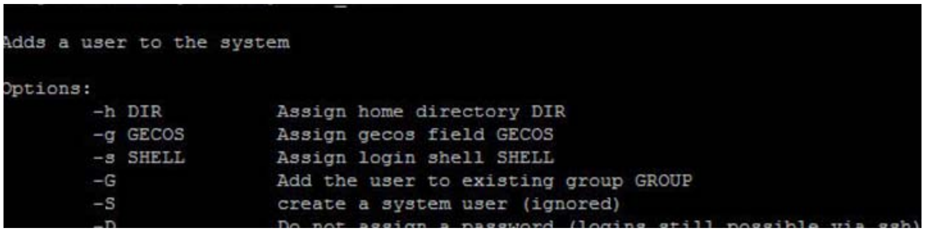
If the session was initiated from an SSH session, enter the SSH break character sequence. The default is **~break** [tilde-break]:

```
~break
```

To change the SSH break character sequence, go to **Serial ports > Configuration > Host mode configuration > SSH break sequence**

User Administration

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



```
Adds a user to the system

Options:
        -h DIR          Assign home directory DIR
        -g GECOS        Assign gecos field GECOS
        -s SHELL        Assign login shell SHELL
        -G              Add the user to existing group GROUP
        -S              create a system user (ignored)
        -D              Do not assign a password (logins still possible via ssh)
```

Add a user

The syntax for adding a user is:

```
adduser [username] -h /tmp [-g groupid] [-s shellprogram]
```

Where:

groupid

Is an identifier for the three types of groups supported by the Digi Passport.

500 or vadmin
Sys admin group ID.

501 or padmin
Port admin group ID.

502 or users
Standard User group ID.

shellprogram
Specifies the type of shell for the Digi Passport device. command line interface (CLI): Config menu, Port access menu, or Custom menu.

/bin/bash
Command Line Interface (CLI)

/bin/editconf
Configuration menu.

/bin/csm.master
Port access menu.

/bin/menu
Custom menu.

passwd [username]

copy passwd and shadow file to /tmp/cnf/etc/ directory

saveconf

applyconf

Delete a user

The syntax for deleting a user definition is:

```
deluser[username]
```

saveconf

applyconf

Locator LED Script

The Locator LED on the Digi Passport 48 can be deactivated and reactivated with the following file and command.

```
/bin/blinkled [{start|stop}]
```

For example, use these commands to stop and start Locator LEDS:

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

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

All other Digi Passport units have the locator feature without a Locator LED. To identify another Digi Passport unit, all the LEDs blink when the feature is activated.

Chapter 18 System Administration

This chapter describes how to perform system administration tasks for the Digi Passport unit, when logged in as either the root user or the system administrator. System administration tasks include firmware upgrades, saving configurations, resetting the Digi Passport unit to defaults, and disaster recovery procedures.

Upgrade Firmware

Web Interface

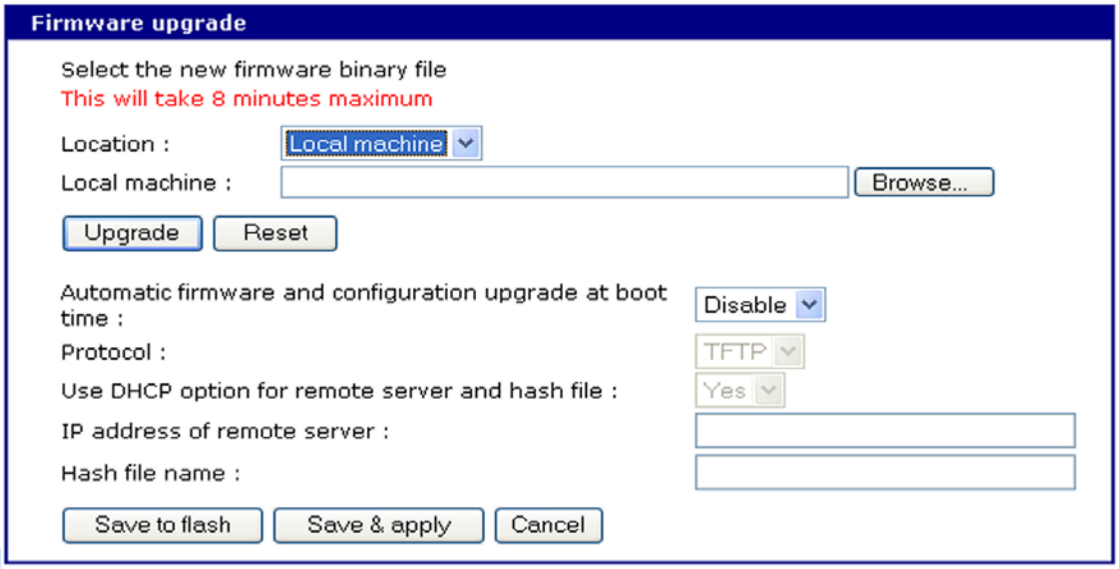
The latest firmware for the Digi Passport unit is in this location: **http://www.digi.com** under **Support, Firmware, Passport**.

To download the latest firmware version to the Digi Passport unit from the web interface:

1. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System administration** > **Firmware upgrade**.
3. Select Local machine or CF card, if configured.
4. Click **Browse** and locate the firmware download.
5. Click **Upgrade**.

   Important: Do not remove power from the unit while firmware is being updating.

   The unit will reboot automatically when it is done flashing the new firmware.



Firmware upgrade

Select the new firmware binary file

This will take 8 minutes maximum

Location : Local machine

Local machine :

Automatic firmware and configuration upgrade at boot time : Disable

Protocol : TFTP

Use DHCP option for remote server and hash file : Yes

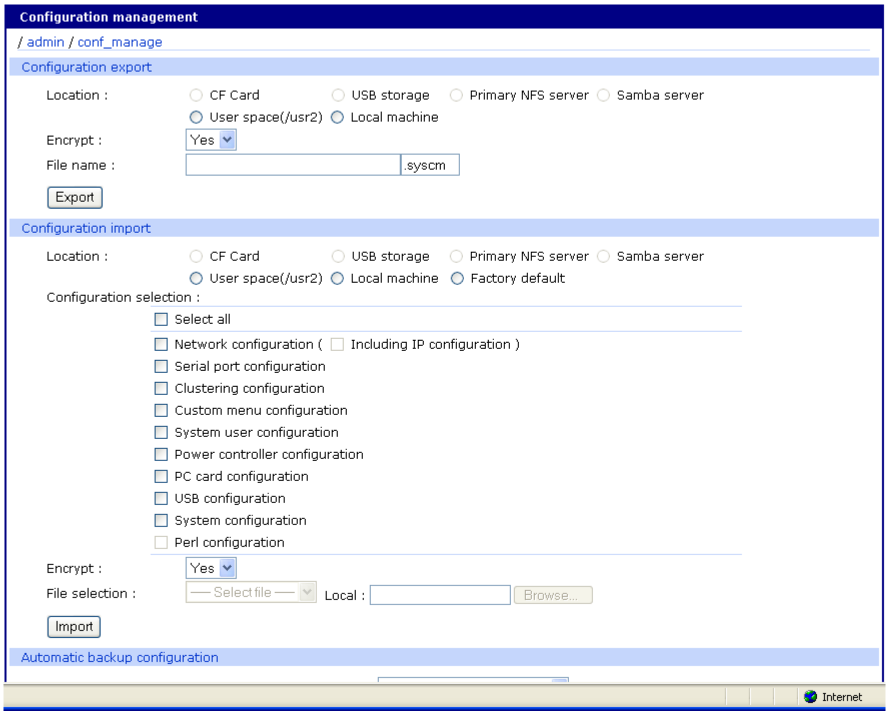
IP address of remote server :

Hash file name :

Configuration Management

Configuration management allows saving all or parts of a configuration at a specified interval: either periodically or ten minutes after the latest changes. The Digi Passport unit saves all configurations when clicking **Save & apply** or **Apply changes**. These configurations are saved to the local Digi Passport unit in the default directory, **/tmp/cnf**. Then, manage these configurations by exporting the files to the desired location.

1. Select **System administration** > **Configuration management**. The Configuration management screen is displayed.
2. Under **Configuration Export**, specify the location and file name in which to save the configuration, and click **Export**.



Configuration management

/ admin / conf_manage

Configuration export

Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server ○ User space(/usr2) ○ Local machine

Encrypt : Yes

File name : .syscm

Export

Configuration import

Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server ○ User space(/usr2) ○ Local machine ○ Factory default

Configuration selection :

□ 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

□ Perl configuration

Encrypt : Yes

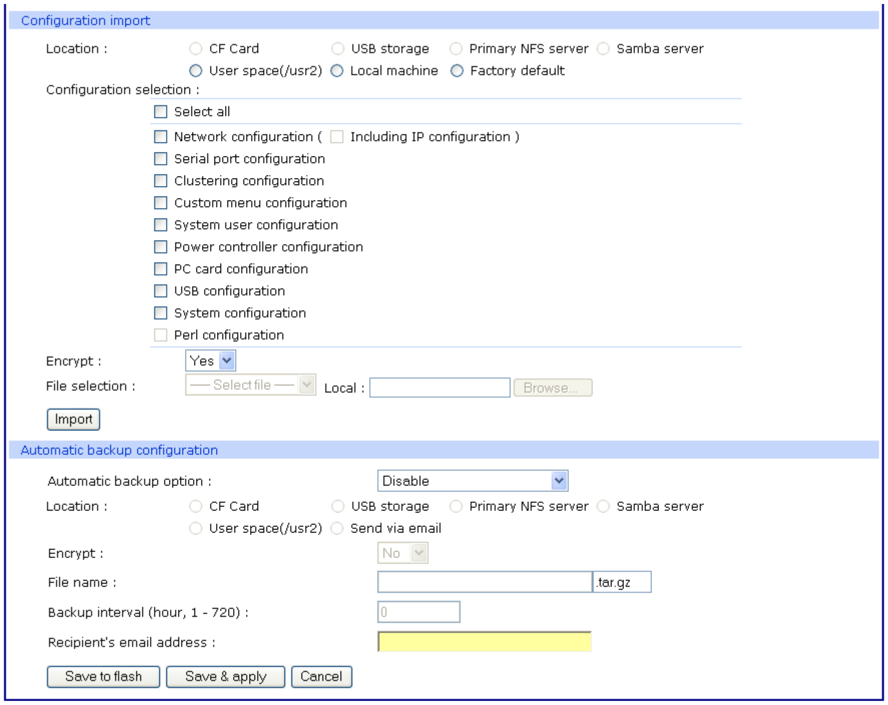
File selection : —— Select file —— Local : Browse...

Import

Automatic backup configuration

Automatically Save the Configuration

Further down the screen are the options for automatically saving the configuration either periodically or 10 minutes after the latest changes.



Configuration import

Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server
○ User space(/usr2) ○ Local machine ○ Factory default

Configuration selection :
□ 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
□ Perl configuration

Encrypt : Yes
File selection : —— Select file —— Local : Browse...

Import

Automatic backup configuration

Automatic backup option : Disable
Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server
○ User space(/usr2) ○ Send via email
Encrypt : No
File name : .tar.gz
Backup interval (hour, 1 - 720) : 0
Recipient's email address :

Save to flash | Save & apply | Cancel

Settings for automatic saving include:.

- **Automatic backup option:**

  Disable: Select if not using an automatic save option.

  Periodic: Save after the specified interval.

  10 minutes after last change: Save ten minutes after the last configuration change.

- **Location**: Where to save the configuration: CF card, Primary NFS server, User space, Send via email.
- **Encrypt**: Enables or disables use of encryption on the configuration file.

  Yes: File is encrypted (.syscm).

  No: File is not encrypted (.tar.gz) in a tar and a gzip 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.

Option for auto backup configuration to use an auto file naming scheme

The following file naming schemes are supported for the auto backup configuration

- $HOSTNAME$: Add host name
- $TIME$<time format>$: Add current time.

For example, config-$TIME$%m%d%y$.tar.gz makes config-052507.tar.gz file. For more detailed information about <time format>, please refer to the Linux man pager of ‘strftime’.

Configure the automatic backup option

To configure the automatic backup option:

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

Automatically Upgrade 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. When booting, the Digi Passport unit can verify a “hash” file and determine if it needs to download upgrades from the TFTP server. The TFTP upgrade function can be configured using DHCP or by directly configuring the TFTP server and the name of the hash file.

Using 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 (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 any problems occur during the TFTP upgrade process, verify that the hash file and the other files are accessible using TFTP.

Structure of the Hash File

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

The hash file defines several actions:

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.

Upgrade firmware action

The syntax for action 1: firmware upgrade is:

```
action #,image name,model name,version
```

Where:

action #

The action number to be performed. For upgrading firmware, the action number is 1.

image name

The path and the filename of the firmware on the TFTP server.

model name

The product name, including the port count, for example, DigiPassport4, DigiPassport8, DigiPassport16, DigiPassport32, DigiPassport48. This allows for a different hash file for different models.

version

The version number of the firmware

The Digi Passport unit downloads 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**).

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

For example:

```
1,Passport48.img,DigiPassport48,v1.1.0
```

After the firmware is upgraded the Digi Passport unit boots again.

Upgrade configuration action

The syntax for action 2, configuration upgrade, is:

```
action #,image name,model name,version
```

Where:

action #
The action number to be performed, which is 2.

image name
The path and the filename of the configuration file on the TFTP server.

model name
The product name, including the port count, for example, DigiPassport4, DigiPassport8, DigiPassport16, DigiPassport32, DigiPassport48. This allows for a different hash file for different models.

version
The version number of the firmware.

The Digi Passport unit downloads the configuration if the version in the hash file is different from the version saved in the file **/tmp/cnf/.cnfversion**. This file does not exist until the first automatic configuration upgrade. It is also deleted if the unit is reset to factory defaults. If the file **/tmp/cnf/.cnfversion** does not exist, no download occurs. The file **/tmp/cnf/.cnfversion** is a hidden file.

For example:

```
2,config.tar.gz,DigiPassport48,v1.1.0
```

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

Upgrade any file action

The syntax for action 3, file upgrade, is:

```
action #,file name,options,destination
```

Where:

action #
The action number to be performed, which is 3.

file name
The path and the filename of the file on the TFTP server.

options
Actions performed on the file:

F
Forced copy: override existing file.

X
Decompress file.

Z
Unzip file.

U
Upload file; this is the default option.

destination
The directory on the Digi Passport unit in which to put the file.

The specified files are downloaded every time the Digi Passport unit boots and there is no reboot after downloading.

For example:

```
3,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.

Execute command action

The syntax for action 4, execute a command, is:

```
action #,command parameters
```

Where:

action #
The action number to be performed, which is 4.

command
Any application on the Digi Passport unit that can be executed by the root user.

parameter
All parameters required by the application.

For example:

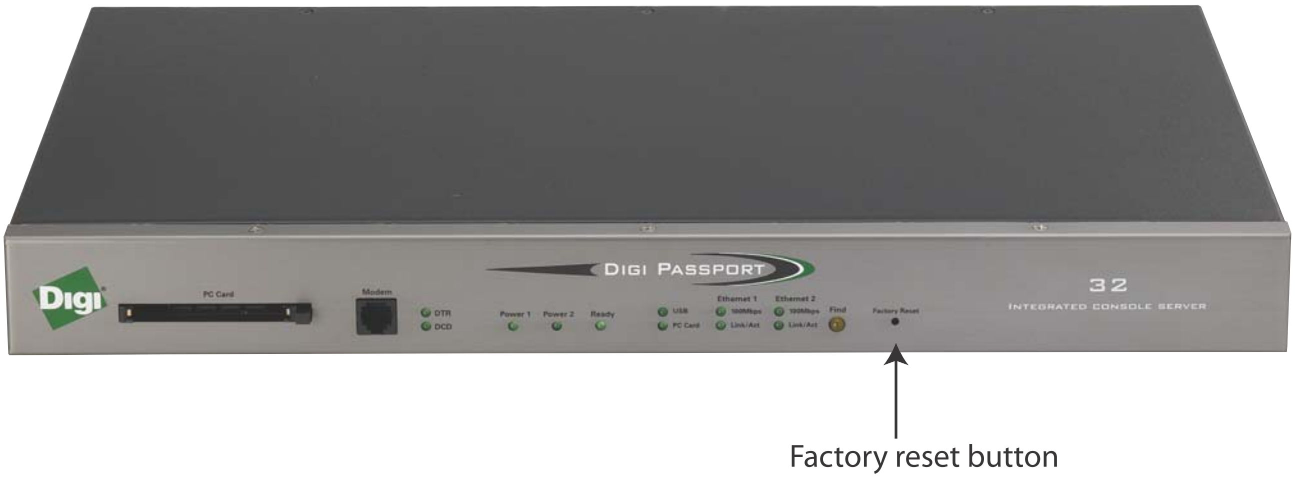
```
4,touch /tmp/test
```

Reset the Digi Passport unit to Factory Defaults

There are several ways to reset the Digi Passport unit to the factory defaults: using the Factory reset button on the unit, using the web interface, or entering a command through the command-line interface.

Using the Factory Reset Button

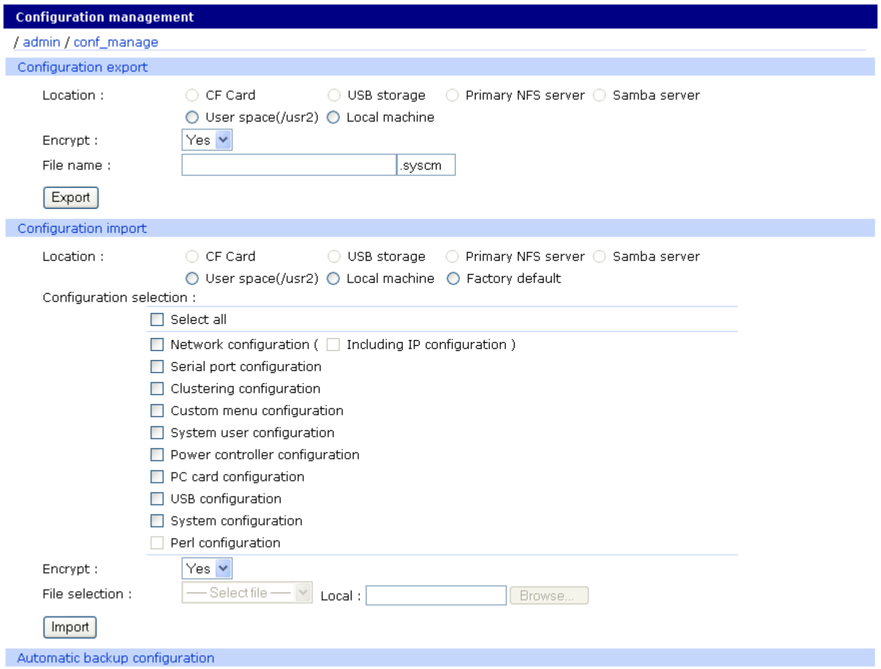
The quickest and simplest method is to push and hold the hardware factory default reset button until the Ready light on the front panel goes out. The reset button is located on the back panel of the unit next to the Ethernet port. The arrow points to the reset button's location. (Digi Passport 32 shown.)



Using the Web Interface

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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System administration** > **Configuration management**
3. Under **Configuration import**, select **Factory default**.



Configuration management

/ admin / conf_manage

Configuration export

Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server ○ User space(/usr2) ○ Local machine

Encrypt : Yes

File name : .syscm

Export

Configuration import

Location : ○ CF Card ○ USB storage ○ Primary NFS server ○ Samba server ○ User space(/usr2) ○ Local machine ○ Factory default

Configuration selection :

□ 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

□ Perl configuration

Encrypt : Yes

File selection : —— Select file —— Local : Browse...

Import

Automatic backup configuration

4. From the list, select the Configuration factory default options to restore.
5. Click **Import**. The Digi Passport unit automatically reboots.

From the Command Line Interface

From the CLI, entering **factory_reset** performs the same action as using the factory reset button.

Values Established through Factory Reset

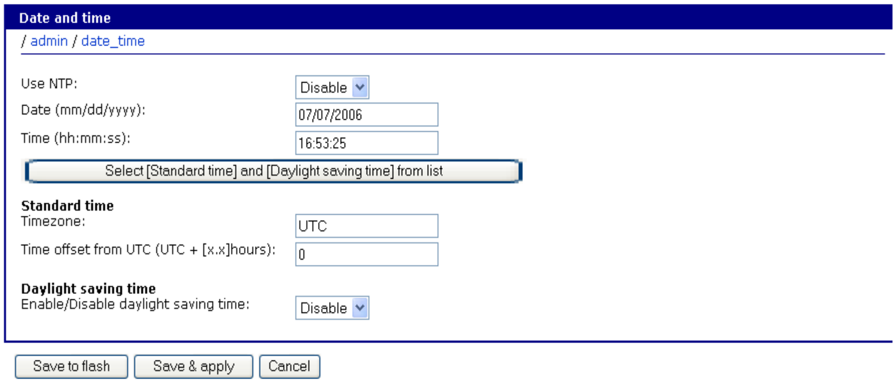
When the Digi Passport unit is reset to the factory defaults, these values are established:.

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

Set 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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System administration** > **Date and time**.



Use NTP: Disable

Date (mm/dd/yyyy): 07/07/2006

Time (hh:mm:ss): 16:53:25

Standard time

Timezone: UTC

Time offset from UTC (UTC + [x.x]hours): 0

Daylight saving time

Enable/Disable daylight saving time: Disable

3. **To use an NTP server**:

   Select **Enable**, the NTP server’s IP address, the Time offset, and the Date and Time fields.

   To use the internal battery:

   Fill in the **Date** and **Time** fields only.

   If the time zone is changed, for the change to be effective, the time for the time zone must also be reconfigured.
4. Click **Save & apply**.

Configure 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. Enter the IP address of the Digi Passport unit in the address bar of a web browser to access the web interface.
2. Select **System administration** > **Device name**.
3. Enter the name of the Digi Passport unit.
4. Click **Save & apply**.

Chapter 19 Specifications and Certifications

This chapter provides information on Digi Passport hardware, including hardware specifications, LED descriptions, pinouts for Ethernet cable and cable adapter, and rack mounting specifications. It also includes certification statements for the Digi Passport unit.

Hardware Specifications

Digi Passport 4 Models

Attribute	Value
Operating temperature	41°F to 122°F (0°C to 50°C)
Storage temperature	-20°F to 140°F (-30°C to 60°C)
Humidity	10% to 90% non-condensing
Power supply	External 5V, 4A adaptor
Power consumption	Typical: 7W Single Power max: 20W Dual Power max: N/A 48VDC max: 40W
Operating system	Linux Hard Hat embedded
SDRAM	128 megabytes
Flash memory	64 megabytes
Dimensions	Length: 8.00 in (20.30 cm) Depth: 1.10 in (2.90 cm) Width: 6.20 in (15.50 cm)
Weight	
Digi Passport 4	2.06 lb (0.94 kg)
Digi Passport 4 w/ Modem	2.39 lb (1.09 kg)

Digi Passport 8/16/32/48 Models

Attribute	Value AC Powered
Operating temperature	0°C to 50°C (41°F to 122°F)
Storage temperature	-30°C to 60°C (-20°F to 140°F)
Humidity	10% to 90% non-condensing
Power supply	
All models except Digi Passport 32 DC	Internal, 100 -240VAC, 50/60 Hz, 0.37A (max), 15W (power output side)
Digi Passport 32 DC	Internal, 36-72VDC, 50/60 Hz, 1.2A (max)
Power consumption	
Digi Passport 8	Typical: 11W Single Power max: 15W Dual Power max: 30W 48VDC max: 40W
Digi Passport 16	Typical: 12W Single Power max: 15W Dual Power max: 30W 48VDC max: 40W
Digi Passport 32	Typical: 13W Single Power max: 15W Dual Power max: 30W 48VDC max: 40W
Digi Passport 48	Typical: 14W Single Power max: 15W Dual Power max: 30W 48VDC max: 40W
Fuse (internal)	FUSE (Type L) AC250V, 2A
Operating system	Linux Hard Hat embedded
SDRAM	
Digi Passport 8/16	128 megabytes
Digi Passport 32/48	256 megabytes
Flash memory	64 megabytes

Attribute	Value AC Powered
Dimensions	
Digi Passport 8	Length: 17.50 in (44.30 cm) Depth: 1.80 in (4.40 cm) Width: 8.0 in (20.30 cm)
Digi Passport 16/32/48	Length: 17.50 in (44.30 cm) Depth: 1.80 in (4.40 cm) Width: 10.0 in (25.30 cm)
Weight	
Digi Passport 8	5.19 lb (2.28 kg)
Digi Passport 16	6.09 lb (2.78 kg)
Digi Passport 32	6.23 lb (2.85 kg)
Digi Passport 48	6.48 lb (2.96 kg)
Dual power models	Add 0.20 lb (0.09 kg)
Internal modem models	Add 0.33 lb (0.15 kg)

LED Indicators

Use the LED indicators to confirm network connectivity and that the Digi Passport unit is able to send and receive data.

LED Label		Function
Power		On when power is supplied.
Ready		On when system is ready to run.
PC Card		On when a PC device is running.
USB		On when a USB device is running.
Find		Blinks when the Activate Passport Locator LED option is selected in the the Digi Passport unit's Web interface. On when firmware is being updated.
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 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.

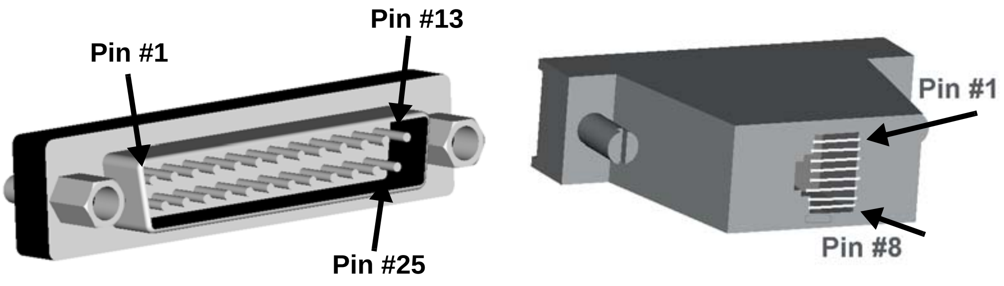
Pin	Description
1	CTS
2	DSR
3	RxD
4	GND
5	DCD Note: Inbound signal can also be used as a second ground.
6	TxD
7	DTR
8	RTS

Cable Adapters and Pinouts

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)

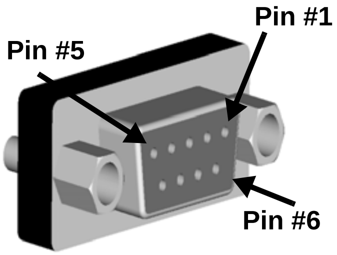


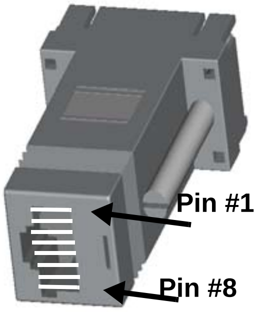
DB-25 Male to RJ-45 Connector Pin Assignments

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)



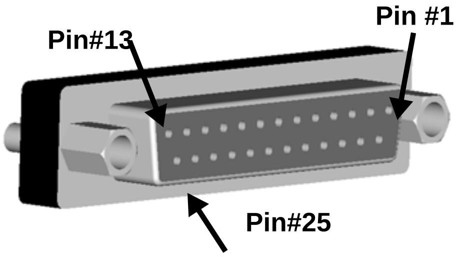


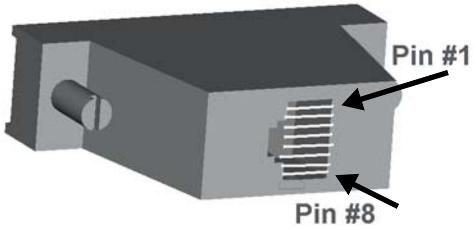
DB-9 Female to RJ-45 Pin Assignments

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)

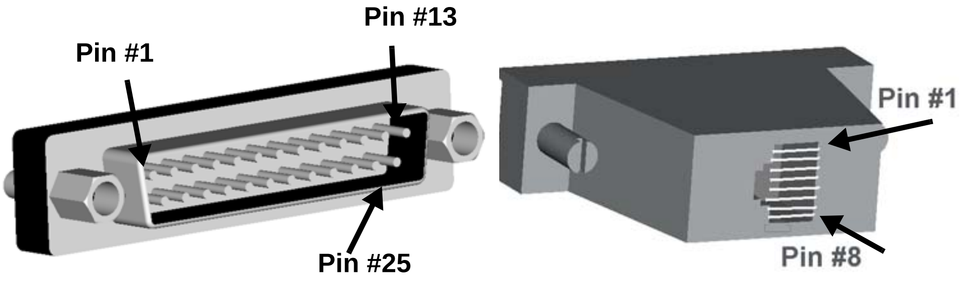




DB-25 Female to RJ-45 Pin Assignments

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)

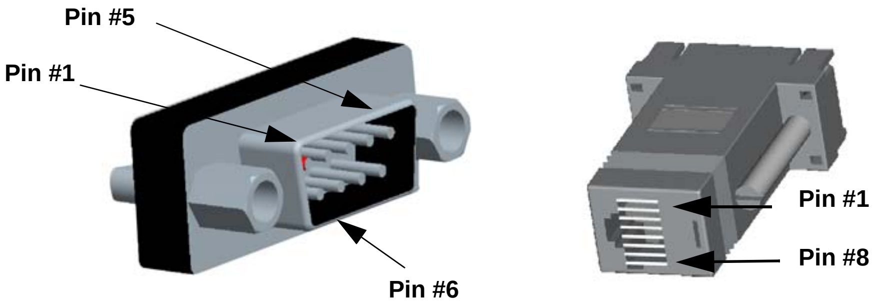


DB-25 Male Modem to RJ-45 Pin Assignment

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

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

(Available but not included

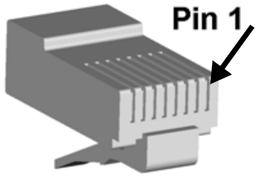


DB-9 Male Modem to RJ-45 Pin Assignment

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

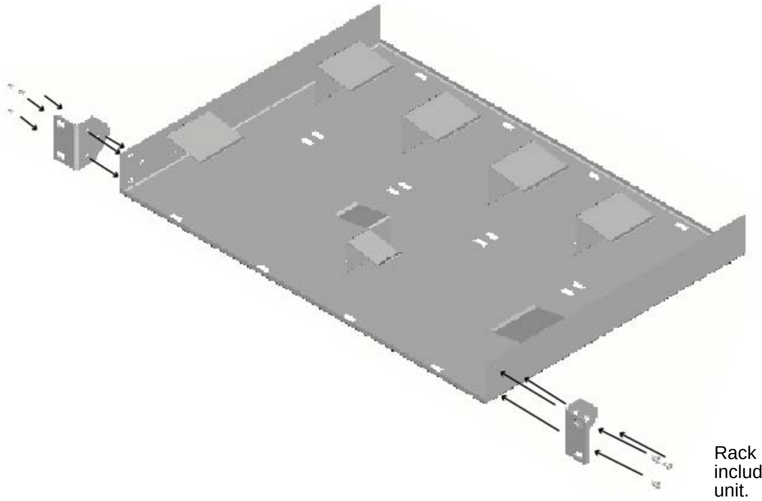
The Digi Passport unit uses a standard Ethernet connector, that is a shielded and compliant with AT&T 258 specifications.

Pin	Description	
1	Tx+	
2	Tx-	
3	Rx+	
4	NC	
5	NC	
6	Rx-	
7	NC	
8	NC	

Rack Mounting

Rack Mounting Installation

1. Attach enclosed bracket ears to rack as shown in illustration.



Rack shown in illustration is not included with the Digi Passport unit.

2. Follow safety and installation considerations when placing the Digi Passport unit on the rack.

Rack Mounting Safety and Installation Considerations

- **Physical location and spacing**
  - 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.
  - To ensure proper ventilation and air flow for units, provide at least 12 inches (30 centimeters) of clearance on all sides for each unit.
  - Distribute weight evenly in the rack to avoid overloading.
- **Temperature**
  - 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 temperature. Install rack-mounted equipment in an environment compatible with the manufacturer’s maximum rated ambient temperature (Tmra).
  - 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 the air in-between devices does not get warmer than 55°C by providing space between the devices, controlling the ambient temperature on the rack, distributing weight evenly in the rack to avoid overloading, checking equipment nameplate ratings before connecting to the supply circuit, and maintaining reliable earthing of the rack-mounted equipment.

- **Power and wiring**:
    - This equipment is for indoor use and all the communication wirings are limited to inside of the building.
    - Locate the DC supply source within the same premises as the equipment.
    - 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 of rack-mounted equipment. Pay particular attention to supply connections other than direct connections to the branch circuit.
    - 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.
    - 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.

Lithium Battery Replacement

A 3 Volt CR2032 battery maintains date and time information in the Digi Passport unit. If resetting the time and date information after turning on the Digi Passport unit is necessary, replace the battery.

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

Manufacturer: SONY FUKUSHIMA CORP., Model: CR2032.
Toshiba Battery Co.,Ltd, Model: CR2032)

Caution: A new battery can explode if incorrectly installed. Replace the 3 Volt CR2032 battery only with the same or equivalent type recommended by the battery manufacturer.

Dispose of used batteries according to the battery manufacturer's instructions and national code or recycling program.

Certifications

Safety Certifications

- 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.

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 using 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 Digi 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.

Environmental Considerations and Cautions

To ensure safe and efficient operation of the Digi Passport unit, follow these guidelines:

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

Emissions Certifications

- US: FCC part 15, Class A
- Canada: ICES 003 Class A
- Europe: EN55022
- Japan: VCCI
- Australia: AS3548

Immunity Certifications

Europe: EN55024:1998
EN61000-3-2: 2000
EN61000-3-3: 1998

Solaris Ready Certification

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.