Digi Connect® Family and ConnectPort® TS Family

Digi Connect Products:

Digi Connect SP
Digi Connect Wi-SP
Digi Connect ME
Digi Connect ME 4 MB
Digi Connect Wi-ME
Digi Connect EM
Digi Connect Wi-EM
Digi Connect ES 4/8 SB
Digi Connect ES 4/8 SB with Switch

ConnectPort TS Products:

ConnectPort TS 8 and 16
ConnectPort TS 8 MEI and TS 16 MEI
ConnectPort TS 8 48VDC and TS 16 48VDC
ConnectPort TS 4x4

User Guide

Revision history—90000565

Revision	Date	Description
N	November 2012	Updated copyright and trademark information. Changed all instances of developer.idigi.com to my.idigi.com.
P	September 2013	Applied branding changes to all text strings, screen captures, command options, and command output.
P1	April 2014	Updated Digi Connect ES 4/8 and Digi Connect 4/8 with Switch paragraph.
R	June 2015	Added information on ConnectPort TS 16 MEI. Resolved documentation issues.
S	April 2016	Added support for Connect Port TS 8 48VDC and TS 16 48VDC. Deleted references to the Digi Device Setup Wizard. Removed references to Connect TS W. Resolved documentation issues.

Product documentation

To find up-to-date documentation for all Digi products, visit www.digi.com/documentation.

To provide feedback on this documentation, send your comments to techcomm@digi.com.

Trademarks and copyright

Disclaimers

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

Warranty

To view product warranties online, visit www.digi.com/howtobuy/terms.

Customer support

Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, please contact us at 952.912.3456 or visit www.digi.com/support.

If you have a customer account, sign in to the Customer Support Web Portal at www.digi.com/support/eservice.

Contents

Monitoring and management

Device administration

Latency Tuning

Specifications and certifications

Troubleshooting

About this guide

Purpose

This guide describes how to install, provision, configure, monitor, and administer Digi™ devices.

Audience

This guide is intended for those responsible for setting up Digi devices. It assumes some familiarity with networking concepts and protocols.

Scope

This guide focuses on configuration, monitoring, and administration of Digi devices. It does not cover hardware details beyond a certain level, application development, or customization of Digi devices.

Where to find more information

In addition to this guide, you can find additional product and feature information in these specific documents:

- *Digi Connect ES Device Server Hardware Setup Guide*
- *RealPort® Installation Guide*
- *Digi Device Customization and Integration Guide*

The product page for your product on the Digi website provides one or more of the following product-specific documents:

- Release Notes
- Quick Start Guides
- Cabling Guides
- Digi Connect® Hardware Reference Guides
- Digi Device Cloud tutorials and user guides

For more additional information, see the following resources:

- Online help and tutorials in the web interface for the Digi device
- Digi Wiki for Developers
- Product information available on the Digi website, www.digi.com, and the Digi support site at www.digi.com/support, including support forums, Knowledge Base, datasheets/product briefs, application/solution guides, and carrier-specific documents
- Integration documentation: For customers who purchase the Digi Connect Integration Kit for product customization, the Integration Kit includes such resources as development board schematics for module products, firmware release notes, hardware reference manuals, specifications, and documentation for the sample applications. For more information, see the document *Getting Started with Digi Connect* included with the Integration Kit and accessed from the Start menu (**Start > Digi Connect > Getting Started with Digi Connect**).

Introduction

This chapter covers the following information:

- Digi devices and their product families
- Types of connections and data paths that Digi devices can use
- The interface options available for configuring, monitoring, and administering Digi devices

Important Safety Information

To avoid contact with electrical current:

- Never install electrical wiring during an electrical storm.
- Never install an Ethernet connection in wet locations unless that connector is specifically designed for wet locations.
- Use caution when installing or modifying lines.
- Use a screwdriver and other tools with insulated handles.
- Wear safety glasses or goggles.
- Do not place Ethernet wiring or connections in any conduit, outlet or junction box containing electrical wiring.
- Installation of inside wire may bring you close to electrical wire, conduit, terminals and other electrical facilities. Extreme caution must be used to avoid electrical shock from such facilities. Avoid contact with all such facilities.
- Ethernet wiring must be at least 6 feet from bare power wiring or lightning rods and associated wires, and at least 6 inches from other wire (antenna wires, doorbell wires, wires from transformers to neon signs), steam or hot water pipes, and heating ducts.
- Do not place an Ethernet connection where it would allow a person to use an Ethernet device while in a bathtub, shower, swimming pool, or similar hazardous location.
- Protectors and grounding wire placed by the service provider must not be connected to, removed, or modified by the customer.
- Do not touch uninsulated Ethernet wiring if lightning is likely.
- External Wiring: Any *external* communications wiring installed needs to be constructed to all relevant electrical codes. In the United States this is the National Electrical Code Article 800. Contact a licensed electrician for details.

The Digi Connect Family

This section describes Digi Connect Family products.

Digi Connect SP

The Digi Connect SP (Single Port) device server is the ideal platform for custom web- and network-enabled embedded applications. Combining Digi and NetSilicon technology, it eliminates the hardware design effort and delivers a true device networking solution that is powerful enough to meet future performance requirements.

Built on NetSilicon 32-bit NET+ARM technology, the Digi Connect SP device server provides a powerful off-the-shelf hardware platform for embedded web- and network applications with a seamless migration path to embedded modules and a fully integrated NetSilicon system-on-chip solution using the family of Ethernet-enabled NET+ARM microprocessors.

Digi Connect Wi-SP

The Digi Connect Wi-SP (Wireless Single Port) device server is a secure 802.11b wireless network solution. Combining Digi and NetSilicon technology, configuration is simple without complex integration tools. The compact hardware design delivers a powerful networking solution to meet performance requirements.

Built on NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-SP device server provides a powerful off-the-shelf hardware platform for embedded web- and network applications with a seamless migration path to embedded modules and a fully integrated NetSilicon system-on-chip solution using the family of Ethernet-enabled NET+ARM microprocessors.

Digi Connect ME

The Digi Connect ME (Micro Embedded) device server enables manufacturers to keep pace with evolving networking technology by easily adding web-enabled network connectivity to existing products. This network connectivity is provided without the added complexities of extensive hardware and software integration, and at a fraction of the time and cost that would be required to develop a custom solution.

Built on leading 32-bit ARM technology using the network-attached NetSilicon NS7520 microprocessor, the Digi Connect ME combines plug-and-play functionality with the freedom and flexibility of complete product customization options. These options are based on the NetSilicon NET+Works® development platform. This platform offers a migration path to a fully integrated NetSilicon system-on-chip solution.

You can use the Digi Connect ME Integration Kit customize the look-and-feel of the device interface.

Digi Connect Wi-ME

The Digi Connect Wi-ME (Wireless Micro Embedded) is a fully customizable and secure 802.11b wireless device server. It is pin-compatible with the Digi Connect ME, and makes fully transparent 802.11b integration possible without the traditional complexities of hardware and software integration work.It is based on the common platform design approach of the Digi Connect family of embedded products, which minimizes design risk and reduces time to market by allowing customers to easily accommodate both wired and wireless network functionality in a single future-proof product design. Built on NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-ME embedded module offers a migration path to a fully integrated NetSilicon system-on-chip solution. It combines plug-and-play functionality with the freedom and flexibility of complete software customization using the NetSilicon NET+Works development platform. You can use the Digi Connect Wi-ME Integration Kit to customize the look-and-feel of the device interface.

Digi Connect EM

The Digi Connect EM (Embedded Module) device server delivers web-enabled device networking that is easy and cost-effective to implement, while being powerful enough to meet future performance needs. Built on 32-bit ARM technology using the network-attached NetSilicon NS7520 microprocessor and featuring a wide variety of connectivity options, the Digi Connect EM provides the freedom and flexibility of complete custom product development. You can use the Digi Connect EM Integration Kit to customize the look-and-feel of the device interface.

Digi Connect Wi-EM

The Digi Connect Wi-EM (Wireless Embedded Module) device server is a fully customizable and secure 802.11b wireless embedded module that provides integration flexibility in a variety of connection options. It is pin-compatible with the Digi Connect EM, and makes fully transparent 802.11b integration possible without the traditional complexities of hardware and software integration work.Based on the common platform design approach of the Digi Connect family of embedded products, the Digi Connect Wi-EM minimizes design risk and reduces time to market by allowing you to easily accommodate both wired and wireless network functionality in a single future-proof product

design. Built on NetSilicon 32-bit NET+ARM technology, the Digi Connect Wi-EM combines plug-and-play functionality with the freedom and flexibility of complete software customization using the NetSilicon NET+Works development platform, and offers a seamless migration path to a fully integrated NetSilicon system-on-chip solution. You can use the Digi Connect Wi-EM Integration Kit to customize the look-and-feel of the device interface.

Digi Connect ES 4/8 SB and Digi Connect 4/8 SB with Switch

The Digi Connect ES is a high performance high-reliability serial-to-Ethernet concentrator designed with extended safety characteristics. The Digi Connect ES allows connection of sensitive RS-232 enabled devices to the network, sending data to a Data Management System. Models include DC-ES-4 series (4 port serial-to-Ethernet) and DC-ES-8 series (8 port serial to Ethernet). The product is compliant with IEC 60601-1 3rd edition and provides Galvanically isolated RS-232 serial and Ethernet ports.

Galvanic isolation provides extended electrical safety. There is no electrical path for current to earth ground, ensuring no electrical shock when making physical contact with the Digi Connect ES. There is no electrical path from port to port, ensuring a ground fault will not affect the operation of the Digi Connect ES or the operation of any device connected to it.

Digi's patented RealPort technology makes it possible to establish a connection between the host and a networked serial device by creating a local COM or TTY port on the host computer. Incoming/outgoing and telnet sessions on each port give system administrators a high level of control over networked serial devices.

ConnectPort® TS products

Digi ConnectPort TS (Terminal Server) products provide serial over Ethernet connectivity for applications today and into the future. They support IPv4 and IPv6 Ethernet protocols. The Digi ConnectPort TS 8 MEI product is the same size as the Digi ConnectPort TS 8 (RS-232 only) and is the smallest 8-port device with a Multiple Electrical Interface (MEI) in the industry. The ConnectPort TS 16 and ConnectPort TS 16 MEI are 1U Rack-mountable products.

ConnectPort TS 4x4 products

ConnectPort TS 4x4 products are device server products that not only provide serial over Ethernet connectivity, but additional Ethernet ports allow this product to act as an Ethernet switch in conjunction with a serial port server. The 4x4 has 4 Ethernet ports. Both products have 4 RS-232 serial ports. Applications include utilities, precision equipment, industrial automation, banking, retail, traffic as well as many more. The Python development environment allows you to create custom applications to run on the device. Simple configuration management is available through the web browser, command-line interface; in addition, the Device Cloud platform allows for setup, configuration, reporting and monitors of large installations.

Features

This is an overview of key features in Digi devices. The next three chapters cover firmware features in more detail. See Specifications and certifications on page 99 for hardware specifications.

User interfaces

There are several user interfaces for configuring and monitoring Digi devices, including:

- Device Cloud
- A web-based interface for configuring, monitoring, and administering Digi devices.
- A command-line interface available via local serial port, telnet or SSH.
- Configuration through Remote Command Interface (RCI) over the serial port.

- Simple Network Management Protocol (SNMP).

Configurable network services

You can enable or disable access to network services. This means that you can restrict a device's use of network services to those strictly needed by the device. To improve device security, you can disable non-secure services. You can enable or disable the following network services:

- Advanced Digi Discovery Protocol (ADDP): you can enable or disable ADDP, but you cannot change its network port number.
- RealPort
- Encrypted RealPort
- HTTP/HTTPS
- Line Printer Daemon (LPD)
- Remote login (rlogin)
- Remote shell (rsh)
- Simple Network Management Protocol (SNMP)
- Telnet
- Socket connectivity to the serial ports (for example, reverse telnet, reverse SSH, raw socket, and UDP)

In the web interface, you can enable or disable access to network services on the Network Services page of Network Configuration. For more information, see Network services settings on page 38. You can also enable or disable network services from the command-line interface by using the **set service** command. See the *Digi Connect Family Command Reference* for the **set service** command description.

IP protocol support

All Digi devices include an on-board TCP/IP stack with a built-in web server. Supported protocols vary by specific product and include, unless otherwise noted:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Telnet Com Port Control Option (telnet) including support of RFC 2217 (ability to control serial port through telnet). See Serial data communication over TCP and UDP on page 11 for additional information.
- Remote login (rlogin)
- Line Printer Daemon (LPD)
- HyperText Transfer Protocol (HTTP)/HyperText Transfer Protocol over Secure Socket Layer (HTTPS)
- Simple Mail Transfer Protocol (SMTP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Address Resolution Protocol (ARP)
- Advanced Digi Discovery Protocol (ADDP)

- Network Address Translation (NAT)/Port Forwarding (only some products have NAT)

The following sections provide an overview of some of the services provided by these protocols.

Serial data communication over TCP and UDP

Digi devices support serial data communication over TCP and UDP. The key features include:

- Serial data communication over TCP, also known as autoconnect and tcpserial can automatically perform the following functions:
  - Establish bidirectional TCP connections, known as autoconnections, between the serial device and a server or other network device. Autoconnections are based on data and or serial hardware signals.
  - Control forwarding characteristics based on size, time, and pattern.
  - Allow incoming raw, telnet, and SSL/TLS (secure-socket) connections.
  - Support RFC 2217, an extension of the telnet protocol.
- Serial data communication over UDP, also known as udpserial, can automatically perform the following functions:
  - Digi Connect products can automatically send serial data to one or more devices or systems on the network using UDP sockets. Options for sending data include whether specific data is on the serial line, a specific time period has elapsed, or after the specified number of bytes has been received on the serial port.
  - Control forwarding characteristics based on size, time, and patterns.
  - Support incoming datagrams from multiple destinations.
  - Support outgoing datagrams sent to multiple destinations.
- TCP/UDP forwarding characteristics.
- Extended communication control on TCP/UDP data paths.
  - Timeout
  - Hangup
  - User-configurable Socket ID string (text string identifier on autoconnect only)

Dynamic Host Configuration Protocol (DHCP)

You can use Dynamic Host Configuration Protocol (DHCP) to automatically assign IP addresses, deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and provide other configuration information. For more details, see Configure an IP address using DHCP on page 25.

Auto-IP

The Auto-IP protocol automatically assigns an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. Digi devices automatically obtain their IP addresses from a DHCP server. If the DHCP server is unavailable or nonexistent, Auto-IP assigns the device an IP address. For more details, see Configure an IP address using Auto-IP on page 26.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) manages and monitors network devices. The SNMP architecture enables a network administrator to manage:

- Nodes—servers, workstations, routers, switches, hubs, etc.—on an IP network

- Network performance, find and solve network problems, and plan for network growth.

Digi devices support SNMP Versions 1 and 2.

For more information on SNMP as a device-management interface, see Simple Network Management Protocol (SNMP) on page 20. For a list of SNMP-related of supported Request for Comments (RFCs) and Management Information Bases (MIBs), see Supported standard RFCs and MIBs on page 57.

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) provides authentication and encryption for Digi devices. For more information, see Security features in Digi devices on page 14.

Telnet

Digi devices support the following types of telnet connections:

- Telnet client
- Telnet server
- Reverse telnet, often used for console management or device management
- Telnet autoconnect
- RFC 2217, Telnet Com Port Control Option, an extension of the telnet protocol

For more information on these connections, see Supported connections and data paths in Digi devices on page 15. You can enable or disable access to telnet network services.

Remote login (rlogin)

Users can perform logins to remote systems (rlogin). You can enable or disable access to rlogin service.

Line Printer Daemon (LPD)

The Line Printer Daemon (LPD) allows network printing over a serial port. Each serial port has a dedicated LPD server that is independently configurable. You can enable or disable access to LPD service.

HyperText Transfer Protocol (HTTP)
HyperText Transfer Protocol over Secure Socket Layer (HTTPS)

Digi devices provide web pages for configuration that you can secure by requiring a user login.

Internet Control Message Protocol (ICMP)

You can display ICMP statistics, including the number of messages received, bad messages received, and destination unreachable messages received.

Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) transports multi-protocol packets over point-to-point links. PPP encapsulates the data packet, allows the server to inform the dial-up client of its IP address (or client to request the IP address), authenticates the exchange, negotiates multiple protocols, and reassembles the data packet for network communication.

Advanced Digi Discovery Protocol (ADDP)

The Advanced Digi Discovery Protocol (ADDP) runs on any operating system capable of sending multicast IP packets on a network. ADDP allows the system to identify all ADDP-enabled Digi devices attached to a network by sending out a multicast packet. The Digi devices respond to the multicast packet and identify themselves to the client sending the multicast.

ADDP communicates with the TCP/IP stack using UDP. The TCP/IP stack should be able to receive multicast packets and transmit datagrams on a network.

Not all Digi devices support ADDP. You can enable or disable access to ADDP service, but you cannot change the network port number for ADDP from its default.

RealPort software

Digi devices use the patented RealPort COM/TTY port redirection for Microsoft Windows, UNIX, and Linux environments. RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host computer and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network. RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput. You can enable or disable access to RealPort services.

Encrypted RealPort

Digi devices also support RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the most efficient security algorithms. You can enable or disable access to Encrypted RealPort services. Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification. Drivers are available for a wide range of operating systems, including Microsoft Windows and Linux x32 and x64 based operating systems, as well as other versions of Unix. See the RealPort Compatibility OS List in the Digi Knowledge Base for a detailed list of supported operating systems. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

Alarms

You can configure Digi devices to issue alarms, in the form of email messages or SNMP traps, when certain device events occur, including changes in GPIO signals, data patterns detected in the data stream. Configuring Digi devices to issue alarms allows you to know when events occur. You can also forward Alarms to Device Cloud for display and management in that platform. For more information on configuring alarms, see Alarms on page 53.

Modem emulation

Digi devices include a configuration profile that allows the device to emulate a modem. Modem emulation sends and receives modem responses to a serial device over TCP/IP (including Ethernet) instead of Public Switched Telephone Network (PSTN). The modem emulation profile allows you to maintain a current software application but using it over the less expensive Ethernet network. In addition, you can enable or disable telnet processing on the incoming and outgoing modem-emulation connections. For information on the modem-emulation commands that Digi devices support, see the *Digi Connect Family Command Reference*.

Security features in Digi devices

This section covers the following information:

- Secure access and authentication
- Encryption
- SNMP security
- Network port scan cloaking

Secure access and authentication

- One password, one permission level.
- You can issue passwords to device users.
- Selective enabling/disabling network services such as ADDP, RealPort, Encrypted RealPort, HTTP/HTTPS, LPD, remote login, remote shell, SNMP, and telnet.
- Can control access to inbound ports.
- Can control access to specific devices, IP addresses, or networks through IP filtering.
- Secure sites for configuration: HTML pages for configuration have appropriate security.
- User and user group access permissions, which control user access to various features and the level of control they have over them (view settings or change settings).

Encryption

- Encrypted RealPort offers encryption for the Ethernet connection between the COM/TTY port and the Digi device. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using the Advanced Encryption Standard (AES) security algorithm.
- Strong Secure Sockets Layer (SSL) V3.0/ Transport Layer Security (TLS) V1.0-based encryption: DES (64-bit), 3DES (192-bit), AES (128-/192-/256-bit), IPsec ESP: DES, 3DES, AES.
- Wireless Digi Connect products provide Wi-Fi Protected Access (WPA/WPA2/802.11i) and Wired Equivalent Privacy (WEP) encryption (64-/128-bit). Supported WPA/WPA2/802.11i authentication methods are:

Supported WPA authentication methods		
EAP-TLS	PEAP	EAP/TTLS
LEAP (WEP only)	EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-MD5-Challenge
	EAP-PEAP/TLS (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-GTC
	EAP-PEAP/GTC (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-OTP
	EAP-PEAP/OTP (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-MSCHAPv2
	EAP-PEAP/MD5-Challenge (both PEAPv0 and PEAPv1)	EAP-TTLS/EAP-TLS
		EAP-TTLS/MSCHAPv2
		EAP-TTLS/MSCHAP
		EAP-TTLS/PAP
		EAP-TTLS/CHAP

SNMP security

You can disable SNMP "set" commands to use SNMP read-only. Changing public and private community names is recommended to prevent unauthorized access to the device.

Configuration management

Once a Digi device is configured and running, you need to periodically perform the following configuration-management tasks:

- Upgrading firmware
- Copying configurations to and from a remote host
- Software and factory resets
- Rebooting the device
- Memory management
- File management

For more information on these configuration-management tasks, see Device administration on page 89.

Customization capabilities

You can customize several aspects of Digi devices. For example, you can:

- Customize the appearance of the device interface by changing the company logo or screen colors.
- Run custom Python applications.
- Define the custom factory defaults that the devices use to restore factory default settings.

The *Digi Device Customization and Integration Guide* describes customization and integration tools and processes. Contact Digi International for more information on the Digi Connect Integration Kit customization tools and resources and for assistance with customization efforts.

The Digi Connect Integration Kit also provides a platform for evaluation, rapid prototyping, and integration of Digi Connect embedded modules with plug-and-play firmware. It includes tools, sample code, and documentation to help with product integration and web-based customization efforts.

Supported connections and data paths in Digi devices

Digi devices allow for several kinds of connections and paths for data flow between the Digi device and other entities. You can group these connections into two main categories:

- **Network services**, in which a remote entity initiates a connection to a Digi device.
- **Network/serial clients**, in which a Digi device initiates a network connection or opens a serial port for communication.

The following section describes the effects of enabling certain features and choosing certain settings when configuring Digi products.

Network services

A network service connection is a situation where a remote entity initiates a connection to a Digi device. There are several categories of network services:

- Network services associated with specific serial ports

- Network services associated with serial ports in general
- Network services associated with the command-line interface (CLI)

Network services associated with specific serial ports

- **Reverse telnet**: A remote entity establishes telnet connection to a Digi device. Data passes transparently between the telnet connection and a named serial port.
- **Reverse raw socket**: A remote entity establishes a raw TCP socket connection a Digi device. Data passes transparently between the socket and a named serial port.
- **Reverse TLS socket**: An remote entity establishes an encrypted raw TCP socket to a Digi device. Data passes transparently to and from a named serial port.
- **LPD**: A remote entity establishes a TCP connection to a named serial port. The Digi device interprets the LPD protocol and sends a print job out of the serial port.
- **Modem emulation**, also known as **pseudo-modem (pmodem):** A remote entity establishes a TCP connection to a named serial port. This connection is "interpreted" as an incoming call to the pseudo-modem.

Network services associated with serial ports in general

- **RealPort:** A single TCP connection manages (potentially) multiple serial ports.
- **Modem emulation**, also known as **pseudo-modem (pool)**: A TCP connection to the "pool" port is interpreted as an incoming call to an available pseudo-modem in the "pool" of available port numbers.
- **rsh**: Digi devices support a limited implementation of the remote shell (rsh) protocol, in that a single service listens to connections and allows a command to be executed. Only one class of commands is allowed: a single integer that specifies which serial port to connect to. Otherwise, the resulting connection is somewhat similar to a reverse telnet or reverse socket connection.
- **Reverse SSH**: An encrypted tcp socket is available for each port that provides a direct connection to the designated serial port.
- **Reverse telnet**: A telnet unencrypted socket is available for each serial port that provides a telnet style connection directly to the serial port.
- **Raw TCP**: A raw TCP unencrypted socket is available for each serial port that provides an 8 bit clean connection to the serial port
- **SSL**: An SSL encrypted Raw TCP raw TCP socket is available for each serial port that provides an 8 bit clean connection to the serial port.

Network services associated with the command-line interface

- **Telnet**: A user can telnet directly to a Digi device's command-line interface.
- **Rlogin**: A user can perform a remote login (rlogin) to a Digi device's command-line interface.

Network/serial clients

A network/serial client connection is a situation where a Digi device initiates a network connection or opens a serial port for communication. There are several categories of network/serial client connections:

- Autoconnect behavior client connections
- Command-line interface (CLI)-based clients
- Modem emulation (pseudo-modem) client connections

Autoconnect behavior client connections

In client connections that involve autoconnect behaviors, a Digi device initiates a network connection based on timing, serial activity, or serial modem signals. Autoconnect-related client connections include:

- **Raw TCP connection**: The Digi device initiates a raw TCP socket connection to a remote entity.
- **Telnet connection**: The Digi device initiates a TCP connection using the telnet protocol to a remote entity.
- **Raw TLS encrypted connection**: The Digi device initiates an encrypted raw TCP socket connection to a remote entity.
- **Rlogin connection**: The Digi device initiates a TCP connection using the rlogin protocol to a remote entity.

Command-line interface (CLI)-based client connections

Command-line interface based client connections are available for use once a user has established a session with the Digi device's CLI. CLI-based client connections include:

- **Telnet**: A connection is made to a remote entity using the telnet protocol.
- **Rlogin**: A connection is made to a remote entity using the rlogin protocol.
- **Connect**: Begin communicating with a local serial port.

Modem emulation (pseudo-modem) client connections

When a port is in the modem-emulation or pseudo-modem mode, it can initiate network connections based on AT command strings received on the serial port. See the *Digi Connect Family Command Reference* for modem emulation AT commands.

Interfaces for configuring, monitoring, and administering Digi devices

There are several interfaces for configuring, monitoring, and administering Digi devices.

Configuration capabilities

Device configuration involves setting values and enabling features for such areas as:

- Network configuration: Specifying the device's IP address settings, network-service settings, and advanced network settings.
- Serial port configuration: Specifying the serial port characteristics for the device.
- GPIO pin configuration (for Connect ME and Connect EM devices): Specifying how to use the various GPIO pins for the device.
- Alarms: Defining when to issue alarms, the conditions that trigger alarms, and how to deliver the alarms.
- Security/Users configuration: Configuring security features, such as whether to require password authentication for device users.
- System configuration: Specifying system-identifying information, such as a device description, contact person, and physical location.

Configuration interfaces

Several interfaces are available for configuring Digi devices, including:

- The Digi Device Discovery Utility, which locates Digi devices on a network, and allows you to open the web interface for the devices.

- Device Cloud, a configuration interface to manage and monitor devices. Device Cloud cannot assign an IP address but it can change one.
- A web-based interface embedded with the product, providing device configuration profiles for quick serial-port configuration and other settings.
- A command-line interface (CLI).
- Remote Command-line Interface (RCI) protocol.
- Simple Network Management Protocol (SNMP).

Digi Device Discovery utility

The Digi Device Discovery utility locates Digi devices on a network and allows you to open the web interface for discovered devices, configure network settings, and reboot the device. It uses a Digi International-proprietary protocol, Advanced Digi Discovery Protocol (ADDP), to discover the Digi devices on a network, and displays the discovered devices in a list.

Digi Device Discovery quickly locates Digi devices and basic device information, such as the device's address, firmware revision, and whether it has been configured. It runs on any operating system that can send multicast IP packets to a network. It sends out a User Datagram Protocol (UDP) multicast packet to all devices on the network. Devices supporting ADDP reply to this UDP multicast with their configuration information. Even devices that do not yet have an IP address assigned or are misconfigured for the subnet can reply to the UDP multicast packet and be displayed in device discovery results.

Not all Digi devices support ADDP. Note that personal firewalls can block device discovery, Virtual Private Network (VPN) software, and certain network equipment. Firewalls will block UDP ports **2362** and **2363** that ADDP uses to discover devices. You can enable or disable access to the ADDP service, but you cannot change the network port number for ADDP. For information on launching and using Digi Device Discovery, see Alternative configuration options for Digi Connect Wi-SP on page 73.

Device Cloud interface

Digi Device Cloud is a software-as-a-service platform that empower IT, network operations and customer support organizations to manage the vast array of equipment in their device networks. As a network grows, the complexity of effectively managing the network assets grows exponentially. Device Cloud provides functionality that helps to manage the universal problems of a dynamic device network:

- Centralized control over large numbers of devices
- Reducing service complexity
- Maintaining high levels of security
- Provisioning and decommissioning of equipment
- Adding functionality to device networks

Additionally, you can group devices together, schedule various operations, and set alarm notifications. For example, you can set an alarm to send a notification if a device disconnects or remains connected longer than a specified period.

Some things to note about using Device Cloud:

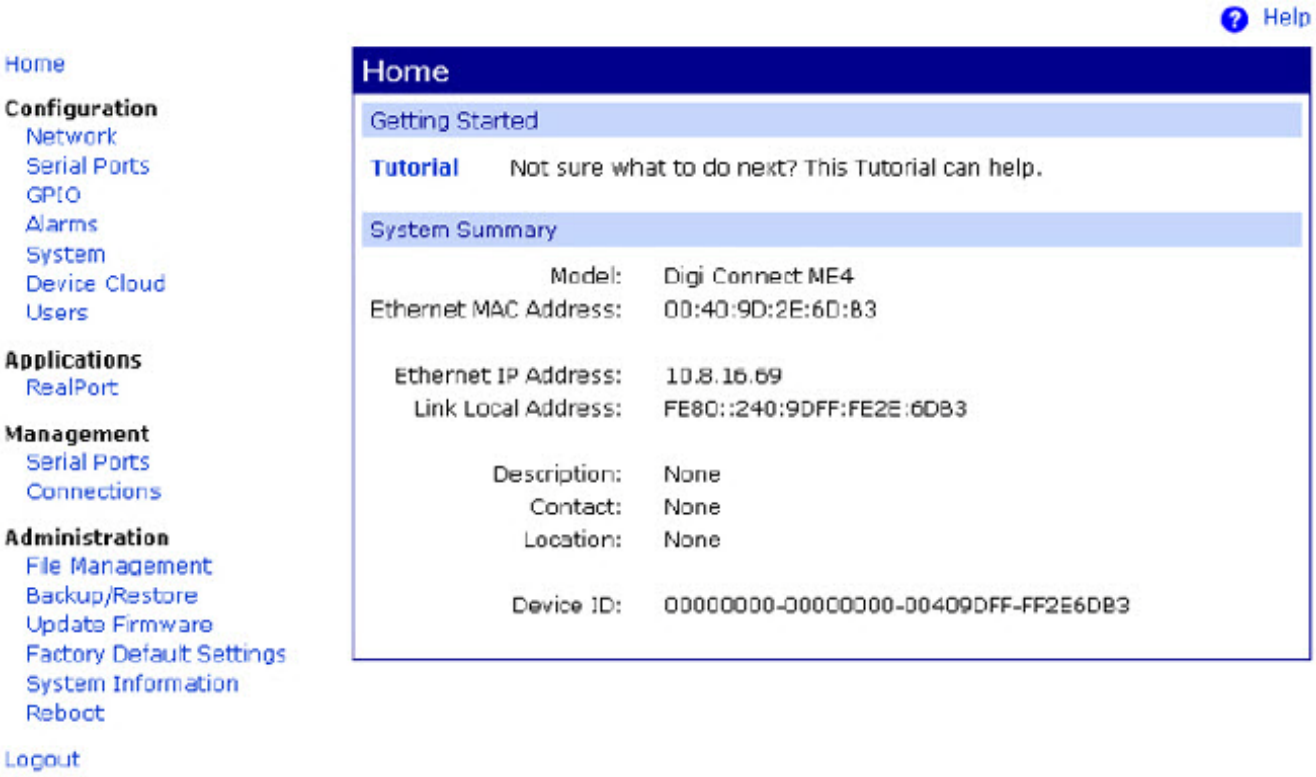
- Devices must be registered in a Device Cloud account before you can access them.
- To minimize network traffic, Device Cloud uses caching. As a result, device settings can be out-of-sync between the device and the settings viewed on the console.
- Device information refreshes on demand when the device is connected, and refreshes automatically when a device connects.

For more information on Device Cloud as a remote device network management solution, see these resources:

- *Device Cloud User Guide*
- *Device Cloud Programming Guide*
- Device Cloud tutorials and other documents available on Digi's Knowledge Base

Web interface

Digi provides a web interface that you can use to configure and monitor Digi devices. Configurable features are grouped into several categories. These categories vary by product; examples include Network, Serial Port, Alarms, and System. Most of the configurable features are arranged by most basic settings on a page, with associated and advanced settings accessible from that page. Serial-port configurations are classified into port profiles, or configuration scenarios that best represents the environment in which you use the Digi device. Selecting a particular port profile configures the serial port parameters that are needed. To access the web interface, type the Digi device's IP address or host name in a browser's URL window. The main menu on the web interface appears. For more information, see Configuration through the web interface on page 28. From web interface, you can access a tutorial from the Home page and the online help from the Help link on each page. Not all settings provided by the command-line interface appears in the web interface. However, the configuration settings in the web interface should be sufficient for most users. If necessary, you can modify settings later from the command line.



Command-line interface

You can configure Digi devices by issuing commands from the command line. The command-line interface allows communication directly with a Digi device without a graphical interface. To access the command line from the Digi Device Discovery utility, click **Telnet to command line**.

For example, you can issue the following command from the command line to set general serial configuration options:

```
#> set serial baudrate=9600 flowcontrol=hardware
```

The command-line interface provides flexibility for making precise changes to device configuration settings and operation. It requires you to have experience issuing commands and access to command documentation.

You can access the command line through telnet or SSH TCP/IP connections, or through serial port using terminal emulation software such as Hyperterminal. Access to the command line from serial ports depends on the port profile in use by the port. By default, serial port command-line access is allowed.

See Configuration through the command line on page 75 for more information on this interface. See the *Digi Connect Family Command Reference* for command descriptions and examples of entering configuration commands from the command-line interface. In addition, you can access online help for the commands by issuing the help and '?' commands.

Remote Command Interface (RCI)

The Remote Command Interface (RCI) is a programmatic interface for configuring and controlling Digi devices. RCI is an XML-based request/response protocol that allows a caller to query and modify device configurations, access statistics, reboot the device, and reset the device to factory defaults. Unlike other configuration interfaces that are designed for a user, such as the command-line or web interfaces, a program can use RCI. RCI access consists of program calls. For example, a custom application running on a computer that monitors and controls an installation of many Digi devices.

You can use RCI to create a custom configuration user interface, or utilities that configure or initialize devices through external programs or scripts.

RCI uses HTTP as the underlying transport protocol. Depending on the network configuration, use of HTTP as a transport protocol could be blocked by some firewalls.

RCI is quite complex to use, requiring users to phrase configuration requests in Extensible Markup Language (XML) format. It is a "power-user" option, intended for users who develop their own user interfaces, or implement embedded control (and thus potentially using RCI over serial) than for end-users with limited knowledge of device programming.

Not all actions in the web interface have direct equivalents in RCI.

For more details on RCI, see the Digi Connect Integration Kit and the *Remote Command Interface (RCI) Specification*.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) manages and monitors network devices. The SNMP architecture enables a network administrator to manage:

- Nodes—servers, workstations, routers, switches, hubs, etc.—on an IP network
- Network performance, find and solve network problems, and plan for network growth.

Digi devices support SNMP Versions 1 and 2.

SNMP is easy to implement in extensive networks. You can program new variables and "drop in" new devices in a network. SNMP is widely used. It is a standard interface that integrates well with network management stations in an enterprise environment.

However, because device communication is UDP-based, the communication is not secure. If you require more secure communications with a device, use an alternate device interface. SNMP does not allow for certain task that can be performed from the web interface, such as file management, uploading firmware, or backing up and restoring configurations. Compared to the web or command-line interfaces, SNMP is limited in its ability to set specific parameters, such as set port profile, is not possible.

Accessing the SNMP interface requires a tool, such as a network management station. The management station relies on an agent at a device to retrieve or update the information at the device, including Device configuration, status, and statistical information. This information is viewed as a logical database, called a Management Information Base (MIB). MIB modules describe MIB variables for a variety of device types and computer hardware and software components.

A variety of resources about SNMP are available, including reference books, overviews, and other files on the Internet. For an overview of the SNMP interface and the components of MIB-II, go to http://www.rfc-editor.org/search/rfc_search.php, and search for MIB-II. From the results, locate the text file describing the SNMP interface, titled Management Information Base for Network Management of TCP/IP-based internets: MIB-II. You can also display the text of the Digi enterprise MIBs. The product page for each product on the Digi website provides a link to the Digi-provided MIBs for that product. See Simple Network Management Protocol (SNMP) on page 57 for a list of supported MIBs.

For additional discussion on using SNMP as a device monitoring interface, see Monitoring Capabilities from SNMP on page 88.

Monitoring capabilities and interfaces

Monitoring Digi devices includes such tasks as checking device status, viewing information on a device's GPIO pins, checking runtime state, viewing serial port operations, and reviewing network statistics, and managing their connections. There are several interfaces for monitoring Digi devices and managing their connections.

As with device configuration, there are several interfaces available for monitoring Digi devices, including, the web interface embedded with the product, SNMP, command-line interface, and Device Cloud. Monitoring and management on page 79 describes these interfaces in detail.

Device Cloud device management

In Device Cloud's device management view, you can sort monitoring capabilities by the server and the devices managed by the server. The information is available in logs and generated reports. When available, the reports post linked totals that you can use to drilled back to the original devices.

Web interfaces

The web interface has several screens for monitoring Digi devices:

- Network Status
- Serial Port Management: for each port, the port's description, current profile, and current serial configuration.
- Connections Management: A display of all active system connections.
- System Information: general device information; current GPIO pin states; serial port information for each port, including the port's description, current profile, and current serial configuration (the same information displayed by choosing Serial Port Management); and network statistics.

Command-line interface

You can issue several commands from the command line to monitor devices. For a review of these commands and what they can provide from a device-monitoring perspective, see Monitoring capabilities from the command line on page 86.

SNMP

Monitoring capabilities of SNMP include managing network performance, gathering device statistics, and finding and solving network problems. For more information on using SNMP for device-monitoring purposes, see Monitoring Capabilities from SNMP on page 88.

Device administration

Periodically, administrative tasks need to be performed on Digi devices, such as uploading and managing files, changing the password for logging onto the device, backing up and restoring device configurations, updating firmware, restoring the configuration to factory defaults, and rebooting.

As with configuration and monitoring, you can perform administration from a number of interfaces, including the web interface, command line, and Device Cloud. See Device administration on page 89 for more information and procedures.

Hardware

This section details requirements and recommendations for installing ConnectPort TS Family products. See also Specifications and certifications on page 99 and System status LEDs on page 107.

For the Digi Connect ES, see the *Digi Connect ES Hardware Setup Guide*. For all other Digi Connect Family products, see their *Hardware Reference Manuals* for hardware-installation details.

Rack mounting (ConnectPort TS 16 models)

You can optionally mount ConnectPort TS 16 models to an industry standard 48.260 cm (19 in) equipment rack using the mounting bracket ears provided with the product.

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.

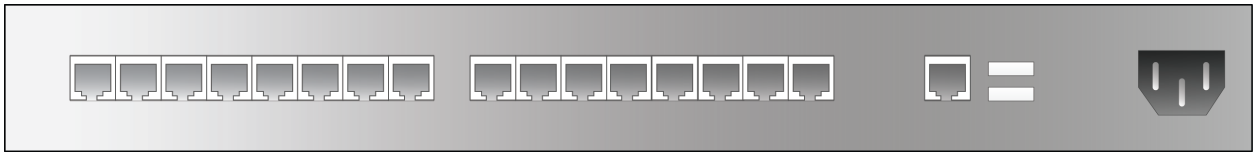
Temperature

- 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 ConnectPort TS 8 16 Rack provides 1/16" = 2mm between devices).
- For a rack setup with no forced air, 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.

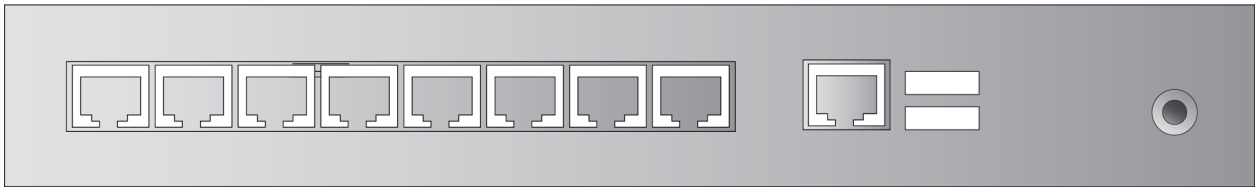
Power and wiring

- For all systems:
  - This equipment is for indoor use and all the communication wirings are limited to inside of the building.
  - Check equipment nameplate ratings before connecting to the supply circuit to avoid overloads that may damage over-current protection devices and supply wiring.
  - As needed maintain reliable earthing of rack-mounted equipment.
- For AC Supply Systems:
  - Locate the AC supply source within the same premises as the equipment you are using.

  The following image shows a ConnectPort TS 16 VAC with an AC plug.



The following image shows a ConnectPort TS 8 VAC with a barrel jack.



- For DC Supply Systems:
  - Connect equipment to a DC supply source (reliably earthed) that is electrically isolated from the AC source.
  - 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.
  - 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. In DC supply systems, the protective grounding wire must be a minimum 18AWG.

  The following image shows the ConnectPort TS 16 48VDC with a terminal block.

Configuring

This chapter describes how to configure a Digi device. It covers these topics:

IP address assignment

Default IP address and DHCP settings

All products that have a cellular (WAN) interface ship with static IP address for the Ethernet port of 192.168.1.1 and DHCP *server* enabled by default. The Ethernet port of the laptop should be configured to automatically receive an IP address and DNS server address.

All products that only have an Ethernet or Wi-Fi (LAN) interface ship with DHCP *client* enabled by default. Accessing the web interface on these products is most easily done by connecting it to a LAN that has a DHCP server.

To discover which IP address has been assigned to the device, use the Device Discovery Utility for Windows. See installation instructions on page 27.

Alternative methods of assigning IP addresses

There are several methods to assign an IP address to a Digi device, described on the following pages:

- Use Dynamic Host Configuration Protocol (DHCP) from the web interface.
- Use the command-line interface.
- Use Automatic Private IP Addressing (APIPA), also known as Auto-IP.

Note For the Digi Connect ES 4/8 SB with Switch device, special considerations apply when assigning IP addresses, owing to the two Ethernet interfaces on the product. See Ethernet IP Settings (for Digi Connect ES 4/8 SB with Switch only) on page 33 for more information.

Configure an IP address using DHCP

You can configure an IP address using Dynamic Host Configuration Protocol (DHCP). DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP. You can use DHCP to automatically assign IP addresses and deliver TCP/IP stack configuration parameters.

As mentioned previously, all products that have a cellular (WAN) interface ship with static IP address for the Ethernet port of 192.168.1.1 and DHCP *server* enabled by default. All products that only have an Ethernet or Wi-Fi (LAN) interface ship with DHCP *client* enabled by default.

This procedure assumes that you configured the Digi device as a DHCP client. The Digi devices discussed in this document are configured as a DHCP client by default.

1. sure the Digi device is not powered on.
2. If desired, set up a permanent entry for the Digi device on a DHCP server. While this is not necessary to obtain an IP address via DHCP, setting up a permanent entry saves the IP address after the device is rebooted.
3. Connect the Digi device to the network and power it on. The IP address configured in step 2 is assigned automatically.

Configure an IP address using Auto-IP

The standard protocol Automatic Private IP Addressing (APIPA or Auto-IP) automatically assigns the IP address from a group of reserved IP addresses to the device on which Auto-IP is installed. Use Digi Device Discovery or DHCP to find the Digi device and assign it a new IP address that is compatible with your network. Once the unit is plugged in, Auto-IP automatically assigns the IP address. Auto-IP addresses are typically in the 169.254.x.x address range.

Configure an IP address from the command-line interface

The **set network** command configures an IP address from the command line. Include the following parameters:

- **ip=*device ip***: The IP address for the device.
- **gateway=*gateway***: The network gateway IP address.
- **submask=*device submask***: The device subnet mask.
- **dhcp=off**: Turns off use of the Dynamic Host Configuration Protocol (DHCP), so that the IP address assigned is permanent.
- **static=on**: Specifies that the IP address is static, and will remain as the specified IP address, gateway, and submask.

For example:

```
set network ip=10.0.0.100 gateway=10.0.0.1 submask=255.255.255.0 dhcp=off static=on
```

To configure the Digi Connect SP through the command line, the DIP switches must be changed. See Command line access on page 74 for an illustration of the DIP switch settings.

IP addresses and Device Cloud

From the Device Cloud interface, you can only change the Ethernet/LAN address for a Digi device; you cannot assign an address. The mobile/cellular device is typically provided by the mobile service provider; check with your mobile service provider on how they handle addresses. To change the IP address, open the web interface for based on the IP address the device has and go **Configuration > Network > IP Settings**. On the IP Settings page, type the new IP address, subnet mask, and gateway.

Test the IP address configuration

Once the IP address is assigned, sure it works as configured.

1. Access the command line of a computer or other networked device.

2. Issue the following command:

   ping *ip-address*

   where *ip-address* is the IP address assigned to the Digi device. For example:

   ping 192.168.2.2

Locate the Digi Device through the Digi Device Discovery utility

Use the Digi Device Discovery utility to locate the Digi device and open its web interface.

Download and run the Digi Device Discovery utility

The Digi Device Discovery utility is available for downloading from the Digi Support site. To download and run the Digi Device Discovery utility.

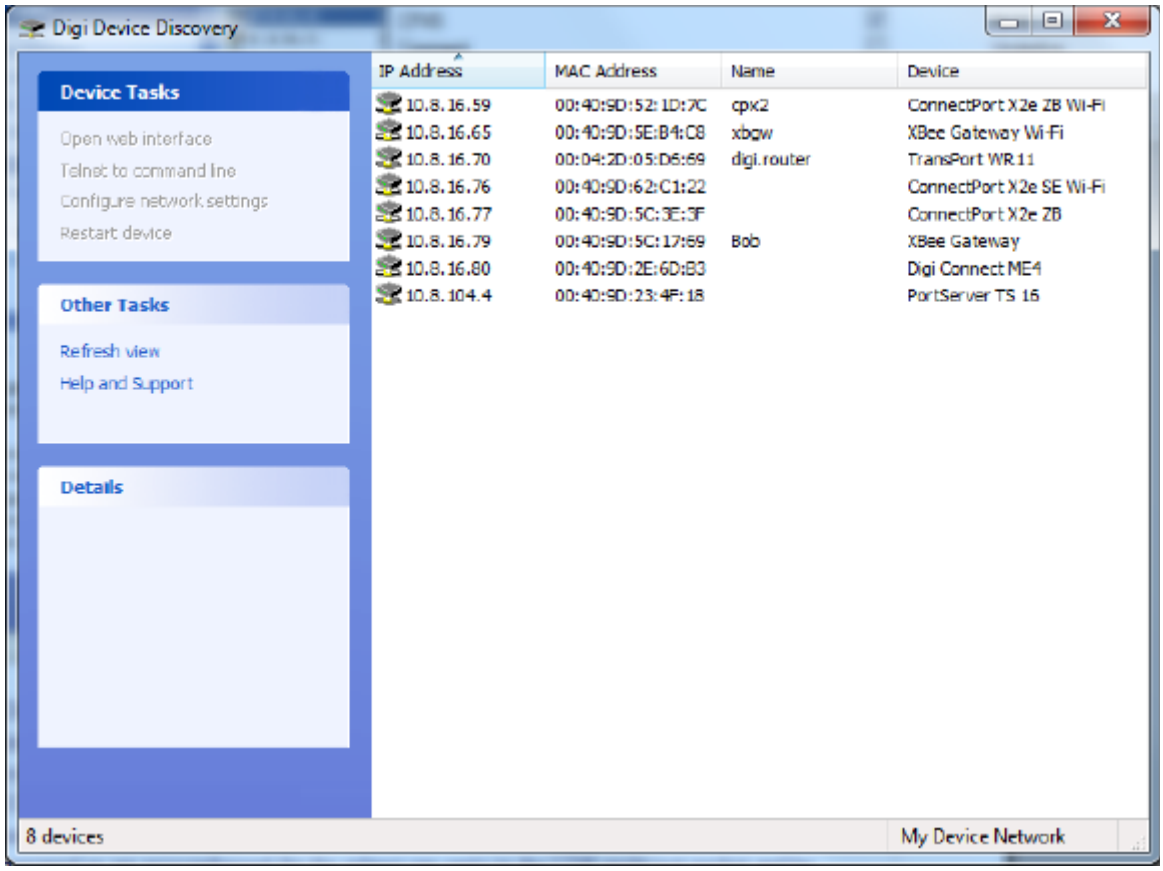
1. From a browser, go to www.digi.com.
2. Click the **Support** link and select **Diagnostics, Utilities and MIBs.**
3. Under **Select Your Product for Support,** select your Digi device from the product list and click **Submit**.
4. Under **Active Products**, select your Digi device from the product list.
5. Under **OS Specific Diagnostics, Utilities and MIBs**, Select the operating system for your computer from the list.
6. Select either **Device Discovery Utility for Windows - Standalone version** or **Device Discovery Utility for Windows - Installable version**. The standalone version runs the utility immediately after the download is complete. The installable version installs the utility on your computer and adds it to a program group in the **Start menu** named **Digi > Digi Device Discovery**
7. Click **Run** on the two dialogs. The standalone version of the utility starts immediately.

   For the installable version, an installation wizard appears. Follow the prompts to complete the installation. To start the utility, select
   Start > Programs > Digi > Digi Device Discovery > Digi Device Discovery

Discover devices

From the start menu, select **Start > Programs > Digi Connect > Digi Device Discovery**. The Digi Device Discovery application appears.

Locate the device in the list of devices, and double-click it, or select the Digi device from the list and select **Open web interface** in the **Device Tasks** list.



Depending on whether a system administrator has configured password authentication for the device, you may be required to sign in. If a login dialog appears, type the user name and password for the Digi device. The default user name is root and the default password is dbps. If these defaults do not work, contact the system administrator who initially set up the device. Now configure the Digi device, as described on the following pages.

Configuration through the web interface

Open the web interface

To open the web interface, either type the Digi device's URL in a web browser and sign in to the device, if required, or use the Digi Device Discovery utility to locate it and open its web interface.

By entering the Digi device's IP address in a web browser

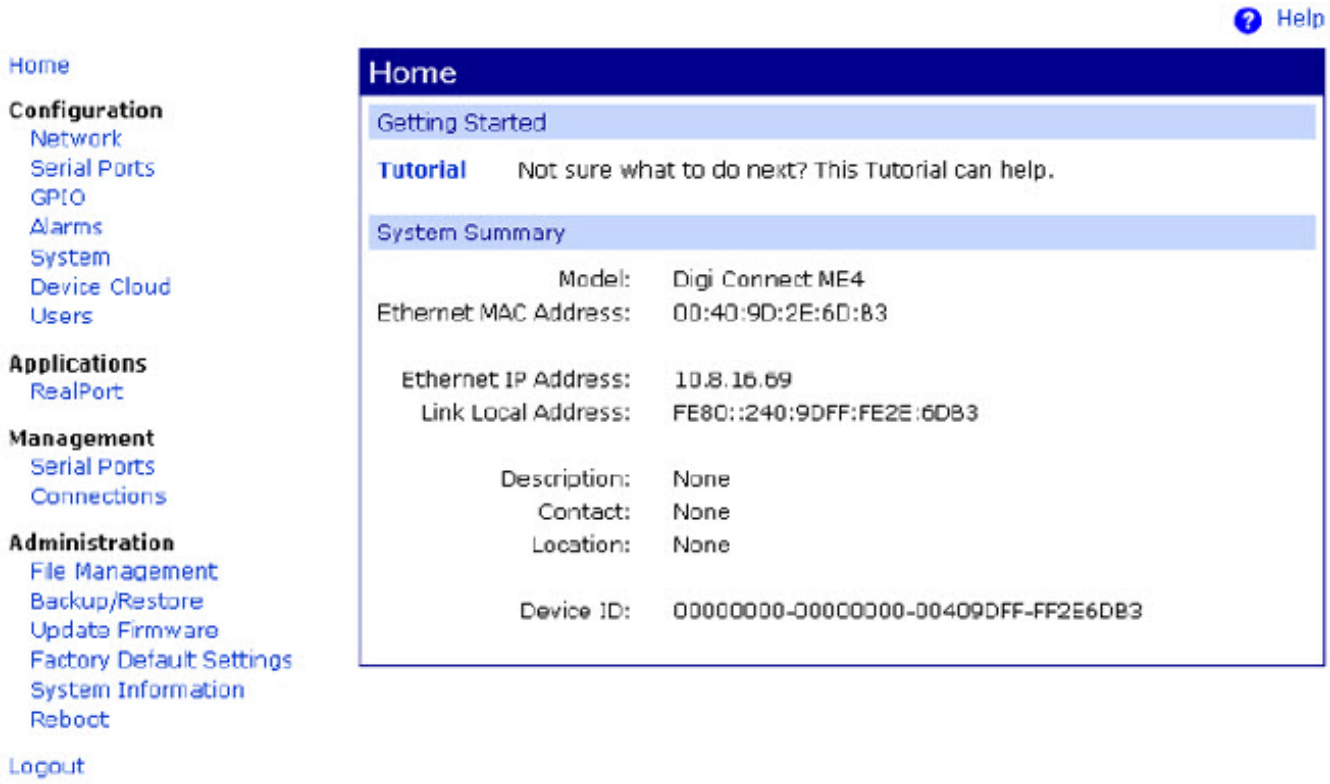
1. In the URL address bar of a web browser, type the IP address of the device.
2. If password authentication for the Digi device is not enabled, the Home page of the web interface appears. If password authentication for the Digi device is enabled, a login dialog appears. Type the user name and password for the device. The default user name is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who set up the device. See Web interface organization on page 29 for an overview of the Home page and other linked pages.

Note The idle timeout automatically logs users out of the web interface after **5** minutes of inactivity if password authentication has been enabled for the device.

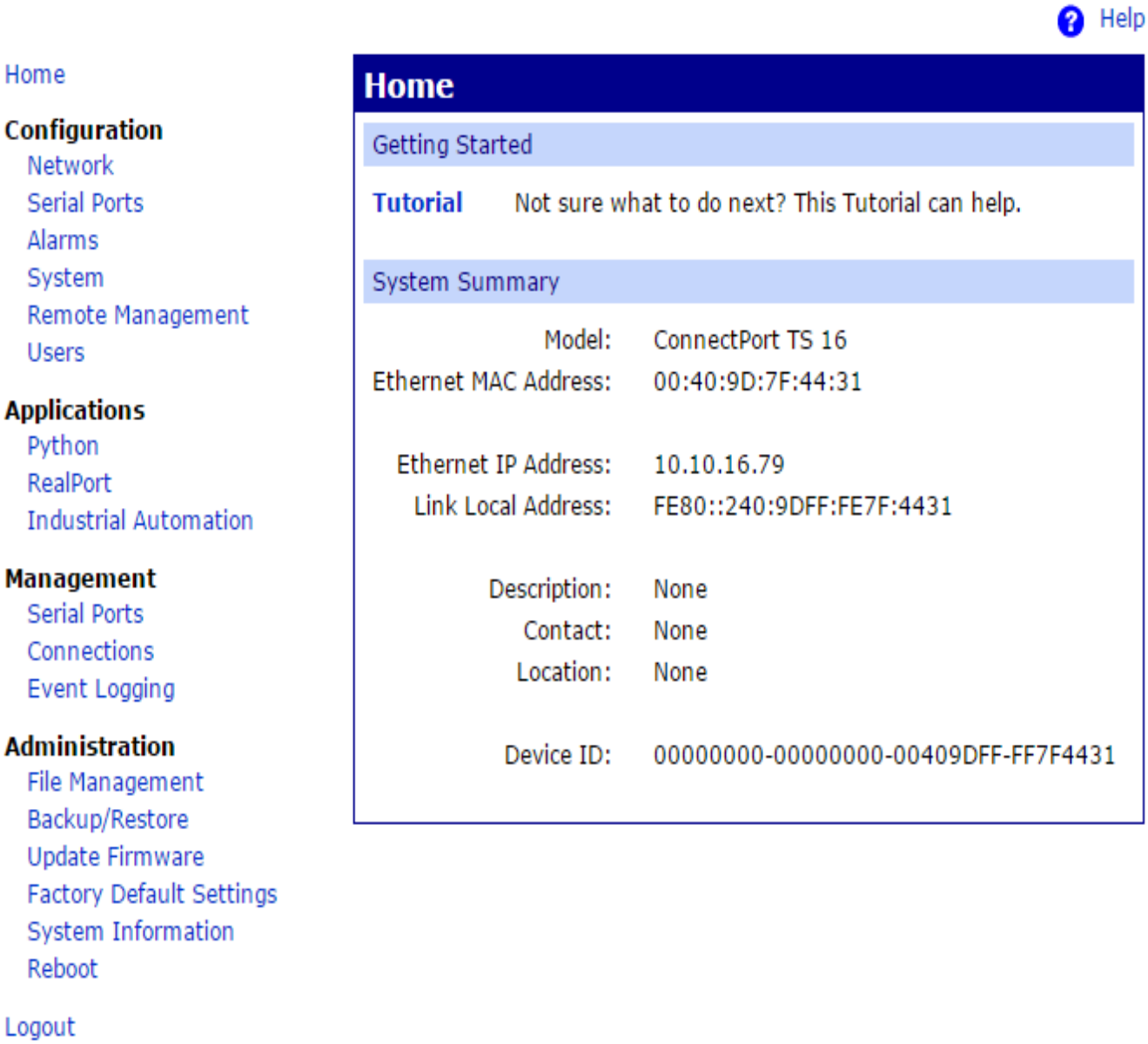
Web interface organization

The Home page

When you access the web interface, the Home page appears. Here is the Home page for Digi Connect ME



The following example shows the Home page for a ConnectPort TS 16 product:



The left side of the Home page displays a menu. This chapter focuses on the options under **Configuration** and **Applications**. For details on monitoring Digi devices and the options under **Management**, see Monitoring and management on page 79. For details on the tasks under **Administration**, see Device administration on page 89.

To log out of a configuration and management session with a Digi device, click **Logout**. A logout window appears. To finish logging out of the web interface and prevent access by other users, close the browser window. Or, click the link on the screen to log in to the device again. After 5 minutes of inactivity, the idle timeout also automatically performs a user logout.

The **Getting Started** section displays a link to a tutorial on configuring and managing Digi device.

The **System Summary** section displays all available device-description information.

Configuration pages

The choices under **Configuration** in the menu display pages for configuring settings for various features, such as network settings and serial port settings. Some of the configuration settings are organized on sets of linked screens. For example, the Network Configuration screen initially displays the IP Settings, and provides links to Network Services Settings, Advanced Settings, and other network settings appropriate to the Digi device.

Applications pages

Depending on the Digi device, there may be an **Applications** menu item for configuring various applications available for use in the device.

- **Python**: For loading and running custom programs authored in the Python programming language onto Connect and ConnectPort devices that support Python.
- **Ekahau Client:** For Digi Connect wireless devices, configures Ekahau Client™ device-location software. See page 71.
- **RealPort**: Configures RealPort settings. See RealPort configuration on page 70 for more information.
- **Industrial Automation:** Configures the Digi device for use in industrial automation applications.

Apply and save changes

The web interface runs locally on the device, which means that the interface always maintains and displays the settings in the Digi device. On each screen, use the **Apply** button to save any changes to the configuration settings to the Digi device.

Cancel changes

To cancel changes to configuration settings, click the **Refresh** or **Reload** button on the web browser. This causes the browser to reload the page. Any changes made since the last time the **Apply** button was clicked are reset to their original values.

Restore the Digi device to factory defaults

You can reset device configuration to the factory defaults as needed during the configuration process. See Restore a device configuration to factory defaults on page 91.

Online help

Online help is available for all screens of the web interface, and for common configuration and administration tasks. There is also tutorial available on the Home page.

Change the IP address from the web interface, as needed

Normally, IP addresses are assigned to Digi devices through DHCP.

This procedure assumes that the Digi device already has an IP address and you simply want to change it.

1. Open a web browser and type the Digi device's current IP address in the URL address bar.
2. If you enabled security on the Digi device, a login prompt appears. Type the user name and password for the device. The default user name is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who set up the device.
3. Click **Network** to access the Network Configuration page.

4. On the IP Settings page, select **Use the following IP address**.
5. Type an IP address (and other network settings), then click **Apply** to save the configuration.

Network configuration settings

The Network configuration pages include:

- **Ethernet IP settings:** For viewing IP address settings and changing as needed. See Ethernet IP settings or Ethernet Switch IP Settings Ethernet Uplink IP Settings (for Digi Connect ES 4/8 SB with Switch) on page 33 for more information.
- **WiFi IP settings:** For setting the IP address used for wireless LAN communication. See WiFi IP settings on page 35 for more information.
- **WiFi LAN settings:** For setting basic options for wireless LAN devices such as network name and network connection options. See WiFi LAN settings on page 35 for more information.
- **WiFi Security settings:** For setting authentication and encryption options for wireless LAN devices. See WiFi security settings on page 36 for more information.
- **WiFi 802.1x Authentication settings:** Detailed authentication settings for IEEE 802.1x authentication for wireless LAN devices. See WiFi 802.1x authentication settings on page 37 for more information.
- **Network Services settings:** Enable and disables access to various network services, such as ADDP, RealPort and Encrypted RealPort, telnet, HTTP/HTTPS, and other services. See Network services settings on page 38 for more information.
- **IP Filtering settings:** For configuring the Digi Cellular Family device to only accept connections from specific and known IP addresses or networks. See IP filtering settings on page 40 for more information.
- **IP Forwarding settings:** For configuring the Digi Cellular Family device to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding. See IP forwarding settings on page 41 for more information.
- **Advanced Network Settings**: Configures the Ethernet Interface speed and mode, TCP/IP settings, TCP keepalive settings, and DHCP settings. See Advanced network settings on page 43 for more information.

Alternatives for configuring network communications

You can use the following methods to configure the Digi device on the network.

- **Using dynamic settings**: All network settings are assigned automatically by the network, using a protocol called DHCP. Contact your network administrator to find out if a DHCP server is available.
- **Using static settings**: All network settings are set manually and will not change. The IP address and subnet mask are mandatory. The rest are not mandatory, but may be needed for some functions. Contact your network administrator for the required values.
- **Using Auto-IP**: Auto-IP assigns an IP address to the Digi device immediately after it is plugged in. If running DHCP or ADDP, the Auto-IP address is overridden and a network compatible IP address is assigned, or a static IP address can be assigned.

Even if a DHCP server is available, the device configuration may work better with static settings. Once set, static settings will not change, so you and other network devices can always find the Digi deviceby its IP address. With dynamic settings, the DHCP server can change the IP address. This can happen frequently or infrequently depending on how your network administrator has configured the network.

When the IP address does change, you and other network devices configured to talk to the Digi devicean no longer access the device. In this case, the Digi device must be located the Digi Device Discovery utility, and other network devices that need to communicate with the Digi device must be reconfigured.

Ethernet IP settings
or
Ethernet Switch IP Settings
Ethernet Uplink IP Settings (for Digi Connect ES 4/8 SB with Switch)

The Ethernet IP Settings page configure how the IP address of the Digi device is obtained, either by DHCP or by using a static IP address, subnet mask, and default gateway. For more information about how these settings are assigned and used in your organization, contact your network administrator.

Ethernet IP Settings

The Ethernet IP settings for all Digi devices but Digi Connect ES 4/8 SB with Switch are as follows.

- Obtain an IP address automatically using DHCP: When the Digi device is rebooted, it will obtain new network settings.
- Use the following IP Address: Choose this option to supply static settings. An IP address and Subnet mask must be entered. Other items are not mandatory, but may be needed for some functions (such as talking to other networks).
- IP Address: An IP address is like a telephone number for a computer. Other network devices talk to this Digi device using this ID.

  The IP address is a 4-part ID assigned to network devices. IP addresses are in the form of 192.168.2.2, where each number is between 0 and 255.
- **Subnet Mask**: The Subnet Mask is combined with the IP address to determine which network this Digi device is part of. A common subnet mask is 255.255.255.0.
- **Default Gateway**: IP address of the computer that enables this Digi device to access other networks, such as the Internet.
- **Enable AutoIP address assignment**: With AutoIP enabled, the Digi device will automatically self-configure an IP address when an address is not available from other methods, for example, when the Digi device is configured for DHCP and a DHCP server is not currently available.

Ethernet IP Settings (for Digi Connect ES 4/8 SB with Switch only)

This section describes configuring and deploying Digi Connect ES4/8 SB with Switch devices in a network.

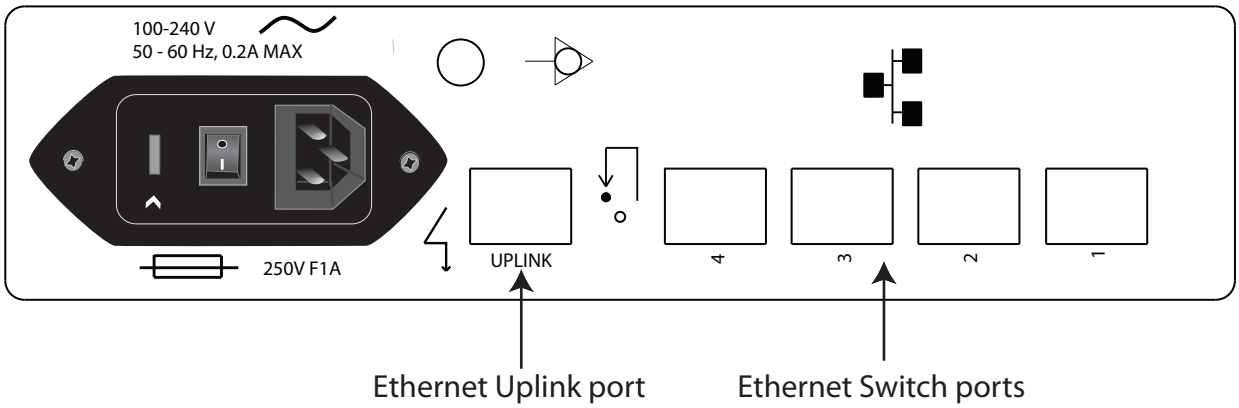
The Digi Connect ES4/8 SB with Switch has two Ethernet interfaces:

- **Ethernet Uplink**: An uplink interface, that connects to the central data management system network.

  The uplink interface provides a single Internet Protocol (IP) address for all communication to and from the devices at a single location. Network Address Translation (NAT) and port forwarding provide seamless network access through the Digi Connect ES SB SW for all Ethernet and serial devices at that location. DHCP or static addresses are used for IP address assignment of the uplink interface.
- **Ethernet Switch**: A four-port switch that creates a Local Area Network (LAN)

  The LAN switch can provide network connectivity to up to four network devices, in addition to the Digi Connect ES SB SW itself, which provides four or eight isolated RS-232 serial ports. The default IP address for the LAN interface of the Digi Connect ES 4/8 SB with Switch is **192.168.1.1**. The other network devices connected to the Digi Connect ES 4/8 SB with Switch share this same Class C network address scheme (192.168.1.*x*).
  A Dynamic Host Configuration Protocol (DHCP) server is provided on this interface to allow dynamic assignment of devices as well.

The following figure shows the location of the Ethernet Uplink and Switch ports on the product:



Because the LANs attached to each Digi Connect ES 4/8 SB with Switch are typically not connected to each other, equipment can have static network addresses and be moved from one location to another without needing to be reconfigured. The central data management system can easily communicate with the equipment by addressing the appropriate Digi Connect ES 4/8 SB with Switch device. The Digi Connect ES 4/8 SB with Switch uses NAT and port forwarding to make the connection.

Assuming the network topology just described, here are the steps for configuring the Ethernet interfaces of each Digi Connect ES 4/8 SB with Switch device for installation. These steps apply to a single Digi Connect ES 4/8 SB with Switch and its connected Ethernet and serial devices, and must be performed for each Digi Connect ES 4/8 SB with Switch deployed.

1. Connect a laptop to one of the Ethernet Switch ports on the Digi Connect ES 4/8 SB with Switch and open the web interface.

   The recommended Ethernet IP address settings for the laptop are:

   IP Address: 192.168.1.99

   Subnet: 255.255.255.0

   Default Gateway: 192.168.1.1

2. In the web interface, go to **Configuration > Network > Ethernet Switch IP Settings**. page. This page assigns IP address numbers for devices connected to the Ethernet Switch. It is recommended that you leave the settings here as-is. The IP address for the Ethernet Switch on the unit is set to 192.168.1.1. You can set fixed IP addresses starting at 192.168.1.2, 192.168.1.3, and so on. The DHCP server assigns 192.168.1.101 and higher for devices that have their IP addresses dynamically assigned.

3. Choose an IP address assignment mechanism and strategy for the uplink interface. Use one or the other of these assignment mechanisms:

   - Assign an IP address in the DHCP configuration file in the network's DHCP server. In this case, no configuration change on the Digi device is necessary. The device will request a DHCP address from any visible DHCP server at startup.

     Or, in the command line interface, type the following:

   set network if=eth1 dhcp=on static=off autoip=off
   Where **eth1** is the network interface of the uplink. The **autoip=off** option avoids unintentional network address problems through automatic IP address assignment if DHCP servers are temporarily unavailable.

   - Assign a static IP address. In the web interface, go to **Configuration > Network > Ethernet Uplink IP settings** and type the static IP address.

Or, in the command line interface, type the following:

set network if=eth1 ip=<*static ip address*> sub=<*subnet mask*> gate=<*gateway*> static=on

Where **eth1** is the network interface of the uplink. DNS server addresses and other attributes may also need to be configured on statically assigned interfaces.

4. Enable NAT and port forwarding for any protocols that must be forwarded to the LAN. See IP forwarding settings on page 41. You can also configure NAT and port forwarding from the command line; see the **set nat** and **set forwarding** commands in the *Digi Connect Family Command Reference*.

   Network configuration is complete.

Deploy the Digi Connect ES 4/8 SB with Switch

To deploy the Digi Connect ES 4/8 SB with Switch after network configuration:

1. Install the Digi Connect ES 4/8 SB with Switch in the desired location.
2. Connect the Digi Connect ES 4/8 SB with Switch to the main/business Ethernet network through the Ethernet Uplink connection, using a straight-through Ethernet cable.
3. Connect the network devices to the Ethernet Switch ports, using straight-through Ethernet cables.
4. Connect the serial devices to the serial ports.
5. Power on the Digi Connect ES 4/8 SB with Switch and all connected devices.

WiFi IP settings

The WiFi IP settings configure how the IP address of a Wi-Fi-enabled Digi device is obtained. It has the same settings as the Ethernet IP settings page.

WiFi LAN settings

Digi devices with Wi-Fi (wireless LAN) capability contain a wireless network interface that you may find useful to communicate to wireless networks using 802.11b8 technology. Contact your administrator or consult wireless access point documentation for the settings required to setup the wireless LAN configuration. Different devices and firmware settings may not support all of the settings and options listed below. Settings include:

- **Network name:** The name of the wireless network to which the wireless device should connect. In situations with multiple wireless networks, this setting allows the device to connect to and associate with a specific network. The network name is the SSID (service set identifier). If the network name remains blank, the device will search for wireless networks and connect to the first available network. This is useful when you do not need use a specific network name as the device will select the first available network.
- **Connection method:** The type of connection method this device uses to communicate on wireless networks. Choose from:
  - **Connect to any available wireless network:** Use this setting to allow the device to access any network. The device can either access point networks or peer-to-peer wireless networks.
  - **Connect to access point (infrastructure) networks only:** Use this setting if the wireless network that this device needs to connect to is composed of wireless access points. This is typically the most popular method for connecting to wireless networks.
  - **Connect to peer-to-peer (ad-hoc) networks only:** Use this setting if all devices on the wireless network connect to and communicate with each other. This is known as peer-to-peer in that there is no central server or access point. Each system communicates directly with each other system.
- **Country:** The country where this wireless device resides. The channel settings are restricted to the legal set for the selected country.

- **Channel:** The frequency channel that the wireless radio will use. Select Auto-Scan to have the device scan all frequencies until it finds one with an available access point or wireless network it can join.
- **Transmit Power:** The transmit power level in dBm.
- **Enable Short Preamble:** Enables transmission of wireless frames using short preambles. If Short Preamble is supported in the wireless network, enabling it can boost overall throughput.

WiFi security settings

The WiFi security settings specify the wireless security settings that the wireless network uses. Multiple security and authentication modes may be chosen depending on the configuration of the access point or wireless network. The wireless device will automatically select and determine the authentication and encryption methods to use while associating to the wireless network. If the wireless network does not use security and uses an *Open Network* architecture, these settings do not need to be modified.

Note that WPA settings require that the device communicate to Access Points and is not valid when the **Connection Method** is set to **Connect to wireless systems using peer-to-peer (ad-hoc)**. Also, WPA pre-shared key (WPA-PSK) security is only valid when you use a specific **Network Name** or SSID.

- **Network Authentication:** The authentication method or methods used for wireless communications.
  - **Use any available authentication method**: Enables all of the methods. The capabilities of the wireless network determines the actual method used.
  - **Use the following selected method(s)**: Selects one or more authentication methods for wireless communications.

    Open System: Uses IEEE 802.11 open system authentication to establish a connection.

    Shared Key: Uses IEEE 802.11 shared key authentication to establish a connection. At least one WEP key must be specified in order to use shared key authentication.

    WEP with 802.1x authentication: Uses IEEE 802.1x authentication (EAP) to establish a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless network.

    WPA with pre-shared key (WPA-PSK): Uses the Wi-Fi Protected Access (WPA) protocol with a pre-shared key (PSK). The PSK is calculated using a passphrase and the network SSID.

    WPA with 802.1x authentication: Uses the WPA protocol and IEEE 802.1x authentication (EAP) to establish a connection with an authentication server or access point. Encryption keys are dynamically generated to encrypt data over the wireless link.

    Cisco LEAP: Uses Lightweight Extensible Authentication Protocol (LEAP) to establish a a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless link. A user name and password must be specified to use LEAP.
- **Data Encryption:** You an select multiple encryption methods.
  - **Use any available encryption method**: Enables all of the methods. The capabilities of the wireless network determines the actual method used.
  - **Use the following selected method(s)**: Selects one or more encryption methods.

    Open System: Does not use encryption over the wireless link. Open System encryption is valid only with Open System and Shared Key authentication.

    WEP: Uses Wired Equivalent Privacy (WEP) encryption over the wireless link. You can use WEP encryption with any of the above authentication methods.

    TKIP: Uses Temporal Key Integrity Protocol (TKIP) encryption over the wireless link. You can use TKIP encryption with WPA-PSK and WPA with 802.1x authentication.

CCMP: Uses CCMP (AES) encryption over the wireless link. You can use CCMP WPA-PSK and WPA with 802.1x authentication.

- **WEP Keys**
  - **Transmit Key:** Specify the corresponding key of the encryption key that should be used when communicating with wireless networks using WEP security.

    This device allows up to four wireless keys to be set of either 64-bit or 128-bit encryption. These keys allow the wireless network to traverse different wireless networks without having to change the wireless key. Instead, only the transmit key setting has to be changed to specify which wireless key to send.
  - **Encryption Keys:** Specify 1 to 4 encryption keys to use when communicating with wireless networks using WEP security.

    The encryption keys is a set of 10 (64-bit) or 26 (128-bit) hexadecimal characters. The encryption key only contains the characters A-F, a-f, or 0-9. Optionally, you can use separator characters, such as '-', '_', or '.' to separate the set of characters.
- **WPA PSK (Pre-Shared Key) Passphrase/Confirm**: The passphrase that the Wi-Fi network uses with WPA pre-shared keys. The pre-shared key is calculated using the passphrase and the SSID. Therefore, a valid network name must have been previously specified. In the Confirm field, reenter the passphrase.
- **Username/Password/Confirm**: The user name and password combination used to authenticate on the network when using these authentication methods: WEP with 802.1x authentication, WPA with 802.1x authentication, or LEAP. In the Confirm field, reenter the password.

WiFi 802.1x authentication settings

These settings are not required based on the current Wi-Fi authentication settings. They are only configurable when **WEP with 802.1x authentication** or **WPA with 802.1x authentication are** enabled on the WiFi Security Settings tab.

- **EAP Methods:** These are the types of Extensible Authentication Protocols (EAP) or outer protocols that are allowed to establish the initial connection with an authentication server or access point. These are used with WEP with 802.1x authentication and WPA with 802.1x authentication.
  - **PEAP:** Stands for “Protected Extensible Authentication Protocol.” A user name and password must be specified to use PEAP.
  - **TLS:** Stands for “Transport Layer Security.” A client certificate and private key must be installed in order to use TLS.
  - **TTLS:** Stands for “Tunneled Transport Layer Security.” A user name and password must be specified to use TTLS.
- **PEAP/TTLS Tunneled Authentication Protocols:** These are the types of inner protocols that you can use within the encrypted connection established by PEAP or TTLS.

  You can use these **Extensible Authentication Protocols (EAP)** with PEAP or TTLS.
  - **GTC:** Generic Token Card
  - **MD5:** Message Digest Algorithm.
  - **MSCHAPv2:** Microsoft Challenge response Protocol version 2.
  - **OTP:** One Time Password

  You can use these **non-EAP protocols** that with TTLS.
  - **CHAP:** Challenge Response Protocol
  - **MSCHAP:** Microsoft Challenge response Protocol
  - **TTLS MSCHAPv2:** TTLS Microsoft Challenge response Protocol version 2.

- **PAP:** Password Authentication Protocol

- **Client Certificate Use:** When the TLS is protocol is enabled, a client certificate and private key must be installed on the Digi device.
  - **Certificate:** Click **Browse** to select a client certificate file. Then click the next **Browse** to select a private key file.
  - **Private Key File**: If the private key file is encrypted, a password must be specified.
- **Trusted Certificates:** Adds and lists trusted certificates.
  - **Verify server certificates:** Enable to verify that certificates received from an authentication server or access point are signed by a trusted certificate authority (CA). Standard CAs are built in. Additional trusted certificates may be added.
  - **Trusted Certificate File:** To add additional trusted certificates, click **Browse** to select a certificate file to upload to the Digi device, then click **Upload**.
- **Installed Certificates:** Shows which client certificates have been added and are in use.

Network services settings

The Network Services page shows a set of common network services that are available for Digi devices, and the network port on which the service is running.

You can enable and disable common network services and configure the TCP port on which the network service listens. Disabling services may be done for security purposes. That is, you can disable certain services so the device runs only those services specifically needed. To improve device security, you can disable non-secure services such as telnet.

It is usually best to use the default network port numbers for these services because they are well known by most applications.

CAUTION! Exercise caution in enabling and disabling network services, particularly disabling them. Changing certain settings can render a Digi Connect device inaccessible. For example, disabling Advanced Digi Discovery Protocol (ADDP) prevents a network from discovering the device, even if it is actually connected. Disabling HTTP and HTTPS disables access to the web interface. Disabling basic services such as telnet, rlogin, etc. makes the Command-Line interface inaccessible.

Supported network services and their default network port numbers

In Digi devices that have multiple serial ports, the network port number defaults for various services are set based on the following formula:

base network port number + serial port number

For example, the telnet passthrough service is set to network port 2001 for serial port 1, 2002 for serial port 2, 2003 for serial port 3, etc.

If a network port is changed for a particular service, that is the only network port number that changes. That change does not carry over to the other network ports. For example, if the network port number for telnet passthrough is changed from 2001 to 3001, that does not mean that the other network ports will change to 3002, 3003, etc.

There are two types of network services available:

- **Basic services,** which are accessed by connecting to a particular well-known network port.
- **Passthrough services**, in which a particular serial port is set up for a particular type of service. To use the service, users must both use the correct protocol and specify the correct network port. For example, assuming default service ports and using a Linux host, here is how a user would access the SSH and telnet passthrough services:

```
#> ssh -l fred digi16 -p 2501
#> telnet digi16 2101
```

The table shows network services, services provided, and the default network port number for each service.

Service	Services provided	Default network port number
Device Discovery, also known as Advanced Digi Discovery Protocol (ADDP)	Discovery of Digi devices on a network. Disabling this service disables use of the Digi Device Discovery utility to locate the device. The network port number for ADDP cannot be changed from its default.	2362
Encrypted (Secure) RealPort	Secure Ethernet connections between COM or TTY ports and device servers or terminal servers.	1027
RealPort	A virtual connection to serial devices no matter where they reside on the network.	771
Line Printer Daemon (LPD)	Allows network printing over a serial port.	515
Modem Emulation Pool (pmodem)	Allows the Digi device to emulate a modem. Modem emulation sends and receives modem responses to the serial device over the Ethernet instead of Public Switched Telephone Network (PSTN). You can enable or disable telnet processing on the incoming and outgoing modem-emulation connections. The pmodem service is for connecting to whatever serial port will answer.	50001
Modem Emulation Passthrough	Allows the Digi device to emulate a modem. This service is for dialing in to a particular serial port that has been set up for modem emulation.	50001
Remote login (rlogin)	Allows users to log in to the Digi device and access the command-line interface through rlogin.	513
Remote shell (Rsh)	Allows users to log in to the Digi device and access the command-line interface through Rsh.	514
Secure Shell Server (SSH)	Allows users secure access to log in to the Digi device and access the command-line interface.	22
Secure Shell (SSH) Passthrough	Accessing a specific serial port set up for SSH.	2501
Secure Socket Service	Authentication and encryption for Digi devices.	2601
Simple Network Management Protocol (SNMP)	Managing and monitoring the Digi device. To run SNMP in a more secure manner, SNMP allows for “sets” to be disabled.This securing is done in SNMP itself, not through Network Services settings. If disabled, SNMP services such as traps and device information are not used.	161
Telnet Server	Allows users an interactive telnet session to the Digi device’s command-line interface. If disabled, users cannot telnet to the device.	23

Service	Services provided	Default network port number
Telnet Passthrough	Allows a telnet connection directly to the serial port, often called reverse telnet.	2001
Transmission Control Protocol (TCP) Echo	Used for testing the ability to send and receive over a TCP connection, similar to a ping.	7
Transmission Control Protocol (TCP) Passthrough	Allows a raw socket connection directly to the serial port, often called reverse sockets.	2101
User Datagram Protocol (UDP) Echo	Used for testing the ability to send and receive over a UDP connection, similar to a ping.	7
User Datagram Protocol (UDP) Passthrough	Allows raw data to be passed between the serial port and UDP datagrams on the network.	2101
Web Server, also known as HyperText Transfer Protocol (HTTP)	Access to web pages for configuration that can be secured by requiring a user to sign in. HTTP and HTTPS, below, are also called Web Server or Secure Web Server. These services control the use of the web interface. If HTTP and HTTPS are disabled, device users cannot use the web interface to configure, monitor, and administer the device.	80
Secure Web Server, also known as HyperText Transfer Protocol over Secure Socket Layer (HTTPS)	Access to web pages for configuration that can be secured by requiring a user to sign in with encryption for greater security.	443

IP filtering settings

You can restrict your device on the network by only allowing certain devices or networks to connect. This is better known as IP Filtering or Access Control Lists (ACL). By enabling IP filtering, you are telling the device to only accept connections from specific and known IP addresses or networks. You can filter devices on a single IP address or restrict device to a group of devices using a subnet mask that only allows specific networks to access to the device.

CAUTION! Plan and review your IP filtering settings before applying them. If the settings are incorrect, the Digi device will be inaccessible from the network.

IP Filtering Settings settings include:

- **Only allow access from the following devices and networks:** Enables IP filtering so that only the specified devices or networks are allowed to connect to and access the device. Note that if you enable this feature and the system from which you are connecting to the Digi device is not included in the list of allowed devices or networks, then you will instantly no longer be able to communicate or configure the device from this system.
  - **Automatically allow access from all devices on the local subnet:** Specifies that all systems and devices on the same local subnet or network of the device should be allowed to connect to the device.

    Allow access from the following devices: A list of IP addresses of systems or devices that are allowed to connect to this device.

    Allow access from the following networks: A list of networks based on an IP address and matching subnet mask that are allowed to connect to this device. This option allows grouping several devices that exist on a

particular subnet or network to connect to the device without having to manually specific each individual IP address.

IP forwarding settings

When a Digi device acts as a router and communicates on both a private and public network with different interfaces, it is sometimes necessary to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding. When an incoming connection is made to the device on the private network, the IP port is searched for in the table of port forwarding entries. If the IP port is found, that connection is forwarded to another specific device on the public network. The options and features described in this section are only supported on some products and some firmware versions.

Port Forwarding/NAT is useful when external devices can not communicate directly to devices on the public network of the Digi device. For example, this may occur because the device is behind a firewall. By using port forwarding, the connections can pass through the networks transparently. Also, Port Forwarding/NAT allows multiple devices on the private network to communicate to devices on the public network by using a shared private IP address that is controlled by Port Forwarding/NAT.

Use port forwarding to connect from a Digi device to a RealPort device. For this type of connection to occur, your mobile wireless provider must be mobile-terminated.

IP Forwarding settings include:

- **Enable IP Routing:** Enables or disables IP forwarding.
- **Apply the following static routes to the IP routing table:** You can configure the Digi device with permanent static routes. These routes are added to the IP routing table when this device boots, or afterward when network interfaces become active or changes are made to this list of static routes. Use static routes to route IP datagrams to a network that is not a local network or accessible through the default route.
- **Network Address Translation (NAT) Settings**: A list of instances of NAT settings appears. For each instance, the settings are:
  - **Enable Network Address Translation (NAT):** Permit the translation and routing of IP packets between private (internal) and public (external) networks. Refer to NAT configuration options below. Some Digi device models permit the configuration of NAT instances for more than one network interface.
  - **NAT Public Interface**: The name of the network interface for which NAT will perform address and port translations. The list of interfaces available for NAT configuration varies according to the capabilities of your Digi device model.
  - **NAT Table Size Maximum**: The maximum number of entries that can be added to the NAT table. These entries include the configured port and protocol forwarding rules (see Forward TCP/UDP/FTP Connections and Forward Protocol Connections below), the DMZ Forwarding rule (see Enable DMZ Forwarding to this IP address below), as well as dynamic rules for connections that are created and removed during the normal operation of NAT. You can configure the NAT table size maximum value for any value in the range 64 through 1024, with the default value of 256 entries. Note that this setting does not control the maximum number of port or protocol forwarding rules that can be configured in their respective settings.
  - **Enable DMZ Forwarding to this IP address**: DMZ Forwarding allows you to specify a single host (DMZ Server) on the private (internal) network that is available to anyone with access to the NAT Public Interface IP address, for any TCP- and UDP-based services that haven't been configured. Services enabled directly on the Digi device take precedence over (are not overridden by) DMZ Forwarding. Similarly, TCP and UDP port forwarding rules take precedence over DMZ Forwarding (please see **Forward TCP/UDP/FTP Connections** below). DMZ Forwarding is effectively a lowest priority default port forwarding rule that doesn't permit the same remapping of port numbers between the public and private networks, as is possible if you use explicit port forwarding rules.

    If enabled, the incoming TCP and UDP packets from the public (external) network uses the DMZ Forwarding rule, for which there is no other rule. These other rules include explicit port forwarding rules or existing

dynamic rules that were created for previous communications, be those outbound (private to public) or inbound (public to private). Also, the DMZ Forwarding rule is not used if there is a local port on the Digi device to which the packet may be delivered. This includes TCP service listener ports as well as UDP ports that are open for various services and clients. DMZ forwarding does not interfere with established TCP or UDP connections, either to local ports or through configured or dynamic NAT rules. Outbound communications (private to public) from the DMZ Server are handled in the same manner as the outbound communications from other hosts on that same private network.

WARNING! DMZ Forwarding presents security risks for the DMZ Server. Configure the DMZ Forwarding option only if you understand and are willing to accept the risks associated with providing open access to this server and your private network.

- **Forward protocol connections from external networks to the following internal devices:** Enables protocol forwarding to the specified internal devices. Currently, the only IP protocols for which protocol forwarding is supported are:

  Generic Routing Encapsulation (GRE, IP protocol 47)

  Encapsulating Security Payload (ESP, IP protocol 50, tunnel mode only).

  These are routing protocols that route (tunnel) various types of information between networks. If your network needs to use the GRE or ESP protocol between the public and private networks, enable this feature accordingly.

- **Forward TCP/UDP/FTP connections from external networks to the following internal devices:** Specifies a list of connections based on a specific IP port and where those connections should be forwarded to. Typically the connecting devices come from the public side of the network and are redirected to a device on the private side of the network.

  It is possible to forward a single port or a range of ports. To forward a range of ports, specify the number of ports in the range, in the **Range Port Count** field for the port forwarding entry. When a range is configured, the first port in the range is specified, and the full range is indicated in the displayed entry information.

  Note that FTP connections require special handling by NAT. This is because the FTP commands and replies are character-based, and some of them contain port numbers in this message text. Those embedded port numbers potentially need to be translated by NAT as messages pass between the private and public sides of the network. In consideration of these needs, one should select FTP as the protocol type when configuring a rule for FTP connection forwarding to an FTP server on the private network side. If you use TCP, FTP communications may not work correctly. Note also that TCP port 21 is the standard port number for FTP. Finally, the use of port ranges for FTP forwarding is not supported; a port count of 1 is required.

Example

For example, to enable port forwarding of RealPort data (network port 771) on a Digi Connect WAN VPN to a Digi Connect SP with an IP address of 10.8.128.10, you would do the following:

- Select the **Enable IP Routing** check box.
- In the **Forward TCP/UDP connections from external networks to the following internal devices** section, type the port forwarding information as follows, and click Add:

Socket tunnel settings

You can use a socket tunnel to connect two network devices: one on the Digi device's local network and the other on the remote network. This is especially useful for providing SSL data protection when the local devices do not support the SSL protocol.

One of the endpoint devices is configured to initiate the socket tunnel. The tunnel is initiated when that device opens a TCP socket to the Digi device device on the configured port number. The Digi device then opens a separate connection to the specified destination host. Once the tunnel is established, the Digi device acts as a proxy for the data between the remote network socket and the local network socket, regardless of which end initiated the tunnel.

Socket Tunnel settings include:

- **Enable:** Enables or disables the configured socket tunnel.
- **Timeout:** The timeout (specified in seconds) controls how long the tunnel will remain connected when there is no tunnel traffic. If the timeout value is zero, then no timeout is in effect and the tunnel will stay up until some other event causes it to close.
- **Initiating Host:** The hostname or IP address of the network device which will initiate the tunnel. This field is optional.
- **Initiating Port:** Specify the port number that the Digi device will use to listen for the initial tunnel connection.
- **Initiating Protocol:** The protocol used between the device that initiates the tunnel and the Digi device. Currently, TCP and SSL are the two supported protocols.
- **Destination Host:** The hostname or IP address of the destination network device.
- **Destination Port:** Specify the port number that the Digi device will use to make a connection to the destination device.
- **Destination Protocol:** This is the protocol used between Digi device and the destination device. Currently, TCP and SSL are the two supported protocols. This protocol does not need to be the same for both connections.
- Click the **Add** button to add a socket tunnel. Click the Apply button to save the settings. Once the socket tunnel is configured, check the **Enable** check box to enable the socket tunnel.

Advanced network settings

The Advanced Network Settings define the network interface. These settings rarely need to be changed. Contact your network administrator for more information about these settings.

IP Settings

Use the IP settings to manage IP address configuration.

- **Host Name**: The host name to be placed in the DHCP Option 12 field. This is an optional setting which is only used when DHCP is enabled.

  The host name is validated and must contain only specific characters. These restrictions are as defined in RFCs 952, 1035, 1123 and 2132. The following characters are permitted:

  - Alphabetic: upper and lower case letters A through Z and a through z
  - Numeric: digits 0 through 9
  - Hyphen (dash): -
  - Period (dot): .

  The host name value can be a single name, or a fully qualified domain name, whose parts are separated with a period character. Each part must follow the following rules:

  - Must begin with a letter or digit
  - Must end with a letter or digit

- Interior characters may be a letter, digit or hyphen
- Each part of the name may be from 1 to 63 characters in length, and the full host name may be up to 127 characters in length. An IP address is not permitted for use in this host name setting.

- **Static Primary DNS**
  Static Secondary DNS: The IP address of Domain Name Servers (DNS) used to resolve computer host names to IP addresses. Static DNS servers are specified independently of any network interface and its connection state. An IP address of 0.0.0.0 indicates no server is specified.
- **DNS Priority**: A list of DNS servers in priority order used to resolve computer host names. Each type of server is tried, starting with the first in the list. For each server type, the primary server is tried first. If no response is received, then the secondary server is tried. If neither server can be contacted, the next server type in the list is tried.

  A network interface may obtain a DNS server from DHCP or other means when it is connected. If an interface does not obtain a DNS server, it will be skipped and the next server in the priority list will be tried.

  To change the priority order, select an item from the list and press the up or down arrow.

Ethernet Interface

- **Speed**: The Ethernet speed the Digi device uses on the Ethernet network.
  - **10**: The device operates at 10 megabits per second (Mbps) only.
  - **100**: The device operates at 100 Mbps only.
  - **auto**: The device senses the Ethernet speed of the network and adjusts automatically.

  The default is **auto**. If one side of the Ethernet connection is using auto (negotiating), the other side can set the Ethernet speed to whatever value is desired. Or, if the other side is set for 100 Mbps, this side must use 100 Mbps.
- **Duplex Mode:** The mode the Digi device uses to communicate on the Ethernet network. Specify one of the following:
  - **half**: The device communicates in half-duplex mode.
  - **full**: The device communicates in full-duplex mode.
  - **auto**: The device senses the mode used on the network and adjusts automatically.

  The default is **half**. If one side of the Ethernet connection is using auto, the other side can set the duplex value to whatever is desired. If one side uses a fixed value (for example, half-duplex), the other side has to use the same.
- **MDI**: The connection mode for the Ethernet cable.
  - **Auto**: Enables Auto-MDIX mode, where the required cable connection type (straight through or crossover) is automatically detected. The connection is configured appropriately without the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, you can use either type of cable and the interface automatically corrects any incorrect cabling. For this automatic detection to operate correctly, the “speed” and “duplex” options must both be set to “auto.”
  - **MDI**: The connection is wired as a Media Dependent Interface (MDI), the standard wiring for end stations.
  - **MDIX**: The connection is wired as a Media Dependent Interface with Crossover (MDIX), the standard wiring for hubs and switches.

TCP Keep-Alive Settings

The DHCP server assigns these network settings, unless they are manually set here.

- **Idle Timeout**: The period of time that a TCP connection has to be idle before a keep-alive is sent.
- **Probe Interval**: The time in seconds between each keep-alive probe.

- **Probe Count**: The number of times TCP probes the connection to determine if it is alive after the keep-alive option has been activated. The connection is assumed to be lost after sending this number of keep-alive probes.

WiFi Interface

Digi products with Wi-Fi capability display this setting:

- **Maximum transmission rate**: The maximum transmission rate that the device will use, in megabits per second. The complete range of transmission rates is available on all devices except the ConnectPort X2 - XBee® to Wi-Fi model. For that model, the allowed transmission rates are: 1, 2, 5.5, 11.

Serial port settings

Use the Serial Port Configuration page to establish a port profile for the serial port of the Digi device. The Serial Port Configuration page includes the currently selected port profile for the serial port, detailed configuration settings for the serial port, dependent on the port profile selected, and links to basic and advanced serial settings.

About port profiles

Port profiles simplify serial port configuration by displaying only those items that are relevant to the currently selected profile.

There are several port profile choices, but not all port profiles are supported in all products. Support of port profiles varies by Digi product. If a profile listed in this description is not available on the page, it is not supported in the Digi product.

If a port profile has already been selected, it is shown at the top of the screen. You can change or retain the profile and adjust individual settings.

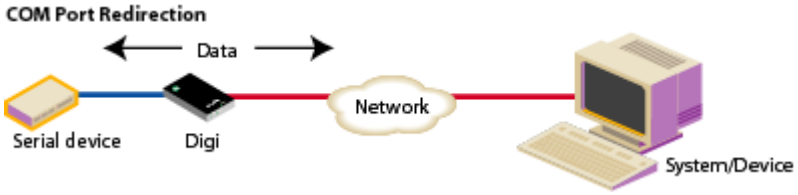
Everything displayed on the Serial Port Configuration screen between **Port Profile Settings** and the links to the **Basic Serial Settings** and **Advanced Serial Settings** depends on the port profile selected.

Select and configure a port profile

1. To configure any profile select **Serial Ports.**
2. Click the port to be configured.
3. Click **Change Profile.**
4. Select the appropriate profile and Click **Apply**.
5. Enter the appropriate parameters for each profile. Descriptions of each profile follow. See also the online help for more details about settings and values on the configuration screens.
6. Click **Apply** to save the settings.

RealPort profile

The RealPort profile maps a COM or TTY port to a serial port. This profile configures a Digi device to create a virtual COM port on a computer, known as COM Port Redirection. The computer applications send data to this virtual COM port and RealPort sends the data across the network to the Digi device.

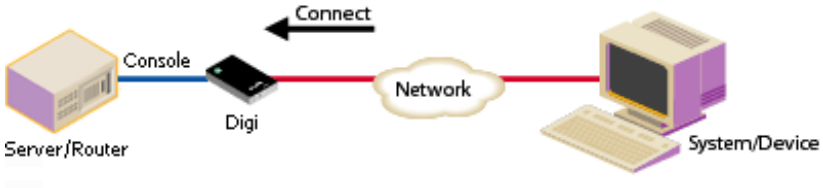


Data is routed to the serial device connected to the Digi device's serial port. The network is transparent to both the application and the serial device.

Important: On each computer that will use RealPort ports, RealPort software must be installed from the Digi Support site or the Software and Documentation CD, if provided with the Digi device, and then configured. Installation instructions are on page 70. type the IP address of the Digi device and the RealPort TCP port number 771.

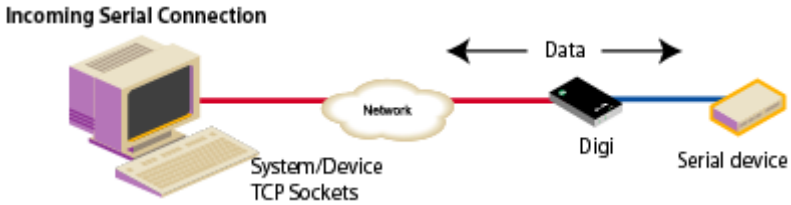
Console Management profile

The Console Management profile allows access to a device's console port over a network connection. Most network devices such as routers, switches, and servers offer one or more serial ports for management. Instead of connecting a terminal to the console port, cable the console port to the serial port of the Digi device. Then using telnet features, network administrators can access these consoled serial ports from the LAN by addressing the appropriate TCP port.



TCP Sockets profile

The TCP Sockets profile allows serial devices to communicate over a TCP network. The TCP Server allows other network devices to initiate a TCP connection to the serial device attached to the serial port of the Digi device.



Automatic TCP connections (autoconnection)

The TCP Client allows the Digi device to automatically establish a TCP connection to an application or a network, known as autoconnection. Autoconnection is enabled through the TCP Sockets profile's setting labeled **Automatically establish TCP connections**. When the TCP Sockets profile is set, the DTR flow-control signal indicates when a TCP socket connection has been established. This information can be useful in monitoring the serial line and using it as a flow-control mechanism to determine when the Digi device is connected to a remote device with which communication is being established. You can combine this mechanism with the DCD signal to close the connection and the DSR signal to do RCI over serial. Together, you can use these signals to the Digi device auto connect to many devices, deterministically, on the network.

RFC 2217 support

Digi devices support RFC 2217, an extension of the telnet protocol used to access serial devices over the network. RFC 2217 implementations enable applications to set the parameters of remote serial ports (baud rate, flow control, etc.), detect line signal changes, as well as receive and transmit data. The configuration information provided in this section applies to Digi device functioning as RFC 2217 servers. If using the RFC 2217 protocol, do not modify the port settings from the defaults. If the port settings have been changed, restore the factory default settings (see Restore a device configuration to factory defaults on page 91). No additional configuration is required.

TCP and UDP network port numbering conventions

Digi devices use these conventions for TCP and UDP network port numbering.

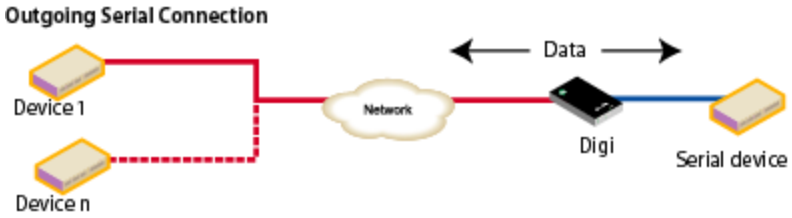
For this connection type...	Use this Port
Telnet to the serial port	2001 (TCP only)
Raw connection to the serial port	2101(TCP and UDP)

The application or Digi device that initiates communication must use these network ports numbers. If they cannot be configured to use these network port numbers, change the network port on the Digi device.

UDP Sockets profile

The UDP Sockets profile allows serial devices to communicate using UDP. The UDP Server configuration allows the serial port to receive data from one or more systems or devices on the network. The UDP Client configuration allows the automatic distribution of serial data from one host to many devices at the same time using UDP sockets.

The port numbering conventions shown in the TCP Sockets Profile also apply to UDP sockets.



Serial Bridge profile

The Serial Bridge profile configures one side of a *serial bridge*. A serial bridge connects two serial devices over the network, each of which uses a Digi device, as if they were connected with a serial cable. The serial devices “think” they are communicating with each other across a serial cable using serial communication techniques. There is no need to reconfigure the server or the serial device. Neither is aware of the intervening network. Serial bridging is also known as *serial tunneling*.

This profile configures each side of the bridge separately. Repeat the configuration for the second Digi device of the bridge, specifying the IP address of the first Digi device.

Local Configuration profile

The Local Configuration profile allows for connecting standard terminals or terminal emulation programs to the serial port in order to use the serial port as a console to access the command line interface. Profile settings enable and disable access to the command line.

Modem Emulation profile

The Modem Emulation profile allows a Digi device to sends and receive modem responses to the serial device over the Ethernet instead of PSTN (Public Switched Telephone Network). This profile allows maintaining the current software application but using it over a less-expensive Ethernet network. The commands that you can issue in a modem-emulation configuration are described in the *Digi Connect Family Command Reference*.

Industrial Automation profile

This port profile is available in Digi devices that support Industrial Automation (IA) and the Modbus protocol. It has serial port settings appropriate for the Digi Connect WAN IA's use in IA applications. It allows you to control and monitor various IA devices and PLCs. Serial ports for Digi Connect WAN IA devices are set to use this port profile by default. The default settings for the Digi Connect WAN IA and in this port profile should be sufficient for most IA applications. If you need to change the settings from the defaults, use the "set ia" command, documented in the *Digi Connect Family Command Reference*.

Dialserv Profile

The DialServ Profile allows connecting a Digi DialServ™ device to the serial port. Digi DialServ is an RJ-11 phone line simulator that allows legacy devices with built-in modems to communicate across LANs/WANs. This profile configures the Digi device to connect/tunnel serial data to an external host when the DialServ receives an incoming call, causes the DialServ to make outgoing calls, and tunnels TCP data from the incoming connection over the Dialserv when TCP traffic is received on the configured ports on the Digi device.

Important: Use of this profile is **required** for DialServ interoperation.

Custom Profile

The Custom port profile displays all serial-port settings that you can adjust as needed. Use the Custom profile only if the use of the serial port does not fit into any of the predefined port profiles, for example, if network connections involve a mix of TCP and UDP sockets.

Basic serial settings

When you select a port profile, the profile settings appear. Choose the appropriate features for your environment. Here are brief descriptions of the fields in the Basic Serial Settings; see the online help for detailed information about each setting.

- The **Description** field specifies an optional character string for the port that you can use to identify the device connected to the port.
- **Basic Serial Settings** include **Baud Rate**, **Data Bits**, **Parity**, **Stop Bits**, and **Flow Control**. The basic serial port settings must match the serial settings of the connected device. If you do not know these settings, consult the documentation that came with your serial device. These serial settings may be documented as 9600 8N1, which means that the device is using a baud rate of 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

  When using RealPort (COM port redirection) or RFC 2217, these settings are supplied by applications running on the computer or server, and the default values on the Digi device do not need to be changed.

Multiple Electrical Interface (MEI) Serial Settings

For Digi devices with Multiple Electrical Interface (MEI) switch-setting capability, these settings configure MEI settings on a per-port basis, and display the current MEI settings for the port. MEI settings include the type of electrical interface (EIA-232 or EIA-485), the number of differential wires used for communication, and whether termination and biasing resistors are used.

- EIA-232: Sets the electrical interface for the serial port to EIA-232. This is the default setting. This interface uses independent wires to transmit and receive data, which allows data to be sent and received between devices simultaneously.
- **EIA-422/EIA-485**: The serial port uses electrical interface EIA-485. You can use this mode for EIA-422 connections. This interface uses two wires to both transmit and receive data. This interface also allows for multiple transmitters and receivers to be easily connected together.

  For EIA-485 mode, there are several additional settings:

  - **2 wires | 4 wires**: Selects the number of differential wires used for communication and implicitly determines the duplex of the connection.

    2 wires: The serial port operates in two-wire mode. This mode is a half-duplex connection with *shared* transmit and receive wires.

    4 wires: The serial port operates in four-wire mode. This mode is a full-duplex connection with *independent* transmit and receive pairs.

    The default is **4 wires**.

  - **Enable termination**: Determines whether termination and biasing resistors are used across the lines. If enabled, termination and biasing resistors are enabled across the lines. Termination should be enabled if terminal/server port is an endpoint node of the 485 network. Biasing should be used in at least one unit in a two-wire environment. If disabled, termination and biasing resistors are disabled across the lines. The default is disabled.

Advanced serial settings

The advanced serial settings further define the serial interface, including whether port buffering (also known as port logging), RTS Toggle, and RCI over Serial are enabled as general serial interface options. You can also define how specific aspects of TCP and UDP serial communications should operate, including timeouts and whether a socket ID is sent.

Serial Settings

The **Serial Settings** part of the page includes these options:

- **Enable Port Logging:** Enables the port-buffering feature, which allows you to monitor incoming ASCII serial data in log form. The Log Size field specifies the size of the buffer that contains the log of ASCII serial data.
- **Enable RTS Toggle:** When enabled, the RTS (Request To Send) signal is forced high (on) when sending data on the serial port.
- **Enable RCI over Serial (DSR):** This choice allows the Digi Connect device to be configured through the serial port using the RCI protocol. See the RCI specification in the Digi Connect Integration Kit for further details.

  RCI over Serial uses the DSR (Data Set Ready) serial signal. Verify that the serial port is not configured for autoconnect, modem emulation, or any other application which is dependent on DSR state changes.
- **Enable alternate pinout (altpin)**: Enables or disables the altpin option, which swaps DCD with DSR so that you can use eight-wire RJ-45 cables with modems. By default, the altpin is disabled.

TCP settings

The **TCP Settings** only appear when the current serial port is configured with the TCP Sockets or the Custom Profile.The settings are as follows:

- **Send Socket ID:** Include an optional identifier string with the data sent over the network. The Socket ID can be 1 to 256 ASCII characters. To enter non-printable characters, use these key sequences:

Character	Key Sequence
backspace	\b
formfeed	\f
tab	\t
new line	\n
return	\r
backslash	\\
hexadecimal values	\xhh

- **Send data only under any of the following conditions:** Enable if it is required to set conditions on whether the Digi device sends the data read from the serial port to the TCP destination. Conditions include:
  - **Send when data is present on the serial line:** Send the data to the network destinations when a specific string of characters is detected in the serial data. Enter the string 1 to 4 characters in the Match String field. To enter non-printable characters, use these key sequences:

Character	Key Sequence
hexadecimal values	\xhh
tab	\t
line feed	\n
backslash	\\

- **Strip match string before sending:** Match string before sending to strip the string from the data before it is sent to the destination.
- **Send after the following number of idle:** Send the data after the specified number of milliseconds has passed with no additional data received on the serial port. You can specify a value from 1 to 65,535 milliseconds.
- **Send after the following number of bytes:** Send the data after the specified number of bytes has been received on the serial port. You can specify a value from 1 to 65,535 bytes.

- **Close connection after the following number of idle seconds:** Enable to close an idle connection. Type the number of seconds in the Timeout field that the connection will be idle before it is closed. Valid values are 1 to 65000 seconds.
- **Close connection when DCD goes low:** When selected, the connection will be closed when the DCD (Data Carrier Detected) signal goes low.
- **Close connection when DSR goes low:** When selected, the connection will be closed when the DSR (Data Set Ready) signal goes low.

UDP settings

The UDP Settings only appear when the current serial port is configured with the UDP Sockets or the Custom Profile.

- **Send Socket ID:** Include an optional identifier string with the data sent over the network. The Socket ID supports 1 to 256 ASCII characters. To enter non-printable characters, use these key sequences:

Character	Key Sequence
backspace	\b
formfeed	\f
tab	\t
new line	\n
return	\r
backslash	\\
hexadecimal values	\xhh

Display current serial port settings

To display the current serial port settings for a Digi device, type the **display techsupport** command from the command line interface.

GPIO pins

This section applies only to embedded products. All Digi Connect Family embedded devices have several General Purpose IO (GPIO) pins. In normal operation, GPIO pins are used for the serial signals CTS, DCD, DSR, DTR, and RTS. On Digi Connect EM and Wi-EM, both sets of RXD/TXD signals are also configured. You can use these GPIO pins for either standard serial communication signalling or a user-defined purpose, such as when a significant event occurs in the device. In the latter case, you can configure the Digi device so that when an event occurs, an alarm is sent as an email message to an administrator or technician, or as an SNMP trap. The number of GPIO pins varies by device. Digi Connect ME and Wi-ME devices have five GPIO pins, while Digi Connect EM and Wi-EM devices have nine GPIO pins. You can view the configuration and current state of GPIO pins through the web interface or by issuing commands from the command line.

GPIO pin settings

The GPIO Configuration page configures GPIO pin settings. You can configure GPIO pins configured for one of three modes: serial, input, and output.

- **Serial:** Use the GPIO pin for standard serial communication signaling. Each pin maps to a different serial signal: DCD, CTS, DSR, etc. Default serial settings for the GPIO pins on a Digi device follow. Depending on the device, there are five or nine pins.

Pin Number	Default Serial Signal	Signal Direction
GPIO 1	DCD	Input
GPIO 2	CTS	Input
GPIO 3	DSR	Input
GPIO 4	RTS	Output
GPIO 5	DTR	Output
GPIO 6	TXD	Output
GPIO 7	RXD	Input
GPIO 8	TXD for port 2	Output
GPIO 9	RXD for port 2	Input

- **In:** Allows input of GPIO signals. Use the GPIO pin for user-defined signal input from the connected device to the Digi device. Alarms can be issued when GPIO pins change state. You can use input mode in with alarms to trigger email notifications or SNMP traps when a particular signal change is detected, as discussed in Alarms on page 53.
- **Input mode**: allows input of GPIO signals.
- **Out:** Allows output of GPIO signals. You can use the GPIO pin for user-defined signal output from the Digi device to the connected device. You can use this mode to toggle the output of GPIO signals between high and low.

Additional implementation required for input and output choices

Changing the GPIO pin settings from Serial to Input or Output means you are responsible for implementing how the pins and signals will work, including developing any applications, signal-handling, and hardware.

Set alarms for GPIO pin changes, as needed

To issue alarms in the form of email notifications or SNMP traps when a GPIO pin signals that an event has occurred on the Digi device, go to the Alarms page and configure those alarms. See Alarms on page 53.

Test GPIO pins

After you configure the GPIO pins and any alarms associated with them, test the GPIO pins to ensure they work as desired.

Test GPIO input

You can use input signals on GPIO pins to trigger an email alarm, which tells an administrator or technician that a significant event occurred within the device. To test GPIO input:

1. On the SW2 bank of switches on the development board, ensure that one of the GPIO pins is set to High.
2. On the SW1 bank of switches, set the same GPIO pin to IO.

3. Configure the GPIO pin for input. See GPIO pins on page 51.
4. Configure an email alarm for the GPIO pin. See Alarms on page 53.
5. Toggle the SW2 switch several times to generate several email alarms.

Test GPIO output

To test GPIO output, a GPIO signal from the configuration application is raised that in turn causes an LED on the development board to turn on.

1. On the SW2 bank of switches on the development board, ensure that one of the GPIO pins is set to High.
2. On the SW1 bank of switches, set the same GPIO pin to IO.
3. In the web interface for the Digi device, click the **GPIO** link. On the GPIO page, configure one or more GPIO pins for output. See GPIO pins on page 51 for details.
4. Under **Administration**, click the **System Information** link. On the **System Information** page, click the **GPIO** link.
5. Choose **Asserted** to raise the signal, and then click **Set Pins**. An LED on the development board is turned on.

   Note that this process does not configure the Digi device. Settings are not saved. If the module reboots, perform steps 2 and 3 again.

Alarms

The **Alarms** page is for configuring device alarms and displaying alarm settings. Device alarms send email messages or SNMP traps when certain device events occur. These device events include changes in GPIO signals, data patterns detected in the data stream

Alarm notification settings

On the Alarms page, the Alarm Notification Settings control the following:

- **Enable alarm notifications:** Enables or disables all alarm processing for the Digi Connect device.
- **Send all alarms to the Remote Management server:** enables or disables sending of alarm notifications to a server that handles remote management of devices, such as Device Cloud.

  Enabling this setting sends all alarm notifications to Device Cloud. Enable this option if the Digi device is managed by a remote management server, such as Device Cloud. Enabling this option is useful because it allows all alarms to be monitored from one location. Enabling this option also allows Digi devices to send alarms to clients that would otherwise be unreachable from the Digi device, either because the Digi device is behind a firewall or not on the same network as the alarm destination.

  Disabling this settings disables sending of alarm notifications to Device Cloud. Disable this option if devices are not managed by a Device Cloud server or if alarms should be sent from the device, for example, because an SNMP trap destination is local to the device, not Device Cloud.
- **Mail Server Address (SMTP):** Specifies the IP address of the SMTP mail server. Ask your network administrator for this IP address.
- **From:** Specifies the text that used in the “From:” field for all alarms that are sent as emails.

Alarm conditions

The **Alarm Conditions** part of the Alarms page shows a list of all of the alarms. You can configure up to 32 alarms for a Digi device, and you can individually enabled and disabled these alarms.

Alarm list and status

The alarm list displays the current status of each alarm. You can use this list to view alarm status at a glance, then view more details for each alarm as needed.

- **Enable:** check box indicates whether the alarm is currently enabled or disabled.
- **Alarm:** The number of the alarm.
- **Status:** The current status of the alarm, which is either enabled or disabled.
- **Type:** The basis for the alarm. whether it is based on GPIO pin state changes or serial data pattern matching.
- **Trigger:** The conditions that trigger the alarm.
- **SNMP Trap:** Indicates whether the alarm is sent as an SNMP trap.
  - If the **SNMP Trap** field is disabled, and the **Send To** field has a value, the alarm is sent as an email message only.
  - If the **SNMP Trap** field is enabled and the **Send To** field is blank, the alarm is sent as an SNMP trap only.
  - If the **SNMP Trap** field is enabled, and a value is specified in the **Send To** field, that means the alarm is sent both as an email and as an SNMP trap.
- **Send To:** The email address to which the alarm is sent.
- **Email Subject:** Text to include in the **Subject** line of alarms sent as email messages.

Alarm configuration

To configure an alarm, click it. The configuration page for individual alarms has two sections.

Alarm conditions

For specifying the conditions on which the alarm is based, such as GPIO pin state changes, serial data pattern matching, signal strength (RSSI), or data usage. Alarm conditions include:

- **Send alarms based on GPIO pin states:** Click this radio button to specify that this alarm is sent when the specified GPIO pin states are detected. Then specify the following:
  - **Pins:** An alarm is sent when the specified combination of pin states is detected.

    High - pin is asserted.

    Low - pin is not asserted.

    Ignore - pin state is ignored.
  - **Alarm recurrence time:** Defines how often to send a new alarm. For example, if the alarm recurrence time is 10 seconds then even if the pin states are detected 5 times within a 10 second period only one alarm will be sent.
  - **Send reminders while GPIO pins remain in this state:** If enabled, reminders will be sent if the pins remain in the defined state for an extended period of time.
  - **Every:** The number of seconds the pins must remain in the defined state for a reminder to be sent.
- **Send alarms based on serial data pattern matching:** Click this radio button to specify that this alarm is sent when the specified serial data pattern is detected. Then specify the following:
  - **Serial Port:** The serial port to monitor for the data pattern. This field appears for devices where more than one serial port is available.
  - **Pattern:** When the serial port receives this data pattern it sends an alarm. You can include special characters such as carriage return carriage return (\r) and new line (\n) in the data pattern.

Alarm destinations

Alarm Destinations defines how alarm notifications are sent, either as an email message or an SNMP trap, or both, and where the alarm notification is sent.

- **Send E-mail to the following recipients when alarm occurs:** Select the check box to specify that the alarm should be sent as an email message. Then specify the following information:
  - **To:** The email address to which this alarm notification email message will be sent.
  - **CC:** The email address to which a copy of this alarm notification email message will be sent (optional).
  - **Priority:** The priority of the alarm notification email message.
  - **Subject:** The text to be included in the Subject: line of the alarm-notification email.
- **Send SNMP trap to the following destination when alarm occurs:** Specifies whether to send the alarm as an SNMP trap. To send alarms as SNMP traps, you must specify the IP address of the destination for the SNMP traps in the SNMP settings (**Configuration > System > Simple Network Management Protocol**); see SNMP Configuration settings: on page 59. That destination IP address appears below the "Send alarm to SNMP destination" check box. You can also specify a secondary or backup SNMP destination.
- To configure an alarm notification to be sent as both an email message and an SNMP trap, select both **Send E-Mail** and **Send SNMP trap** check boxes.
- Click **Apply** to apply alarm settings and return to the Alarms Configuration page.

Enable and Disable Alarms

Once alarm conditions are configured, enable and disable individual alarms by selecting or deselecting the **Enable** check box for each alarm.

System settings

The System Configuration page configures device identity and description information, date and time settings, and settings for Simple Network Management Protocol (SNMP).

Device identity settings

The device identity settings create a description of the Digi device's name, contact, and location. Use this information to identify a specific Digi device when working with a large number of devices in multiple locations.

- **Description**: The network name assigned to the Digi device.
- **Contact**: The SNMP contact person (often the network administrator).
- **Location**: A text description of the physical location of the Digi device.
- **Device ID**: The device ID assigned to this device that corresponds to the Connectware server's device ID. This option only applies when Device Cloud is being used to configure and manage the device.

Date and Time settings

The Date and Time settings set the Coordinated Universal Time (UTC) and/or system time and date on a device, or sets the offset from UTC for the device's system time.

Set Date and Time

Click the **Set** button to configure the hours, minutes, seconds, month, day, and year on the device.

If offset is set to 00:00, the device's system time and UTC are the same. Setting time and date with an offset of 00:00 results in both UTC and system time being set to the specified value. If offset is not 00:00, setting time sets the system time to the specified value and UTC is adjusted accordingly.

Offset from UTC

Specifies the offset from UTC for this device. Offset can range from -12 hours to 14 hours. Very rarely, a time zone can also have an offset in minutes (15, 30, or 45). You can use this value to modify the time and date (generally expected to be UTC) to compensate for time zones and daylight savings time. Wikipedia provides a list of time zone offsets at: http://en.wikipedia.org/wiki/List_of_time_zones

On a device with no real-time clock (RTC) and no configured time source, time and date are completely local to the device and have limited usefulness since they are not persistent over reboots/power-cycles.

On a device with a real-time clock and no configured clock source, time and date are also local to the device but they are meaningful because they are persistent. The offset option could be useful in adjusting for daylight savings time. Setting the date and time to standard time and setting offset to 1 whenever daylight savings time is in effect would serve that purpose.

On a device with a configured clock source, time and date received from a clock source is expected to be UTC. For users with several devices in different time zones, keeping offset=00:00 might be useful for comparing logs or traces from different devices, since all would be using UTC.

Time Source Settings

The time source settings configure access to up to five external time sources that you can use to set and maintain time on the device.

- **Type**: Specifies the type of time source for this entry.
  - **sntp server**: The device uses its SNTP client to poll the NTP/SNTP server, specified by the FQDN, for time.
  - **cellular**: The device polls the cellular service for time.
- **Interval**: Specifies the interval in seconds between polls of a time source. Interval can range from 1 second to 31536000 seconds. If more than one time source is specified, time sources with shorter intervals have greater influence on the device's time than do sources with longer intervals.
- **FQDN**: Specifies the fully-qualified domain name or IP address for the time source. Use FQDN only if the time source is SNTP.

The only time source that is guaranteed to be present on all products at all times is the system clock. It counts uptime and displays system time as the UNIX Epoch (00:00:00 on January 1, 1970) plus uptime. Any source that is not the system clock is considered an external source. This includes the RTC.

Devices which have an RTC but have no external time sources configured will display system time as the UNIX Epoch plus the time since power was initially applied to the device until system time is set manually. You can manually set system time via the CLI, Web UI, etc. Once system time is set manually, the RTC will continue to maintain system time but, due to variations in the accuracy of the RTC, system time can diverge from external time.

Specifying an external time source allows the device to compare its system time to the time reported by the configured time sources and appropriate adjustments to system time. This allows system time to stay consistent over long durations.

The polling interval for an external source establishes its priority relative to other sources; the more samples taken from a time source, the greater influence that time source has on system time.

Any time adjustment will update the RTC automatically. All time sources are assumed to be UTC.

Time Source Global Settings

The Time Source Global settings configures global settings that control time source management.

- **Time Adjustment Threshold**: a value in seconds that defines a range around the current time value maintained by the device. If a time update is received from a best (smallest value) ranking time source and the new time is within that range, the device's time is not changed. However, if the new time falls outside the defined threshold range, the device's time is updated immediately using the new time value.

  The Time Adjustment Threshold value can range from 0 to 300 seconds. For example, if the configured threshold is 60 seconds, the device's time will be updated using a new time value that is 60 seconds or more different than the device's current time value. If the new time value differs from the device's current time by less than 60 seconds, the device's time is not updated using that new time.

- **Enable Lost Time Source Recovery**: If multiple external time sources are available and configured in the Time Source Settings, normally only the best-ranking (smallest value) source(s) will be used to maintain the device's time. If the best-ranking source stops reporting new time values, it is considered “lost”.

  Enabling Lost Time Source Recovery allows one or more worse-ranking (higher value) time sources to be consulted in an effort to obtain a fresh time value. This prevents the best-ranking configured time source from blocking time updates if that source stops providing acceptable time samples.

  The interval of time that must pass for Lost Time Source Recovery to begin varies according to the best ranking time source that is reporting a value. For a time source of type “sntp server”, the missing sample update interval is three NTP/SNTP intervals configured for that time source, plus one minute. For a time source other than “sntp server”, the missing sample update interval is 61 minutes. These interval values cannot be user-configured

The Time Adjustment Threshold is useful in limiting the amount of drift that will be tolerated before the device's time is updated using a new sample. An appropriate value should be selected with consideration for the reliability of the time sample sources.

In the case of NTP/SNTP server sources, the latency, round-trip timing and reliability of the network connection (between the device and the server) also should be considered.

For example, if the communications path between device and server involves a cellular network connection, the performance and behavior characteristics of the cellular network should be taken into account. In a cellular network, intermittent packet delays are possible in either the transmit or receive direction (or both). Frequently these delays are asymmetric, such that the delay is greater in one direction than in the other.

In such conditions, the round-trip timing (of the request/reply) skews the time sample adjustment to determine the time value to use for the device. Therefore configuring an aggressively small (short) threshold value may cause the device to adjust its time frequently and unnecessarily, such that the time value “jumps” forward or backward as a consequence of asymmetric packet delays.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol that you can use to manage and monitor network devices. You can configure Digi devices to use SNMP features, or you can disable SNMP entirely for security reasons. To configure SNMP settings, click the **Simple Network Management Protocol** link at the bottom of the System Configuration page.

Supported standard RFCs and MIBs

Digi devices support these standard SNMP-related Request for Comments (RFCs) and Management Information Bases (MIBs)

Name	Location	Description
RFC 1213	http://www.ietf.org/rfc/rfc1213.txt	Management Information Base (MIB) II; a MIB for managing a TCP/IP network. It is an update of the original MIB, now called MIB-I. MIB-II contains variable definitions that describe the most basic information needed to manage a TCP/IP network. Variable definitions are organized into several groups, such as groups for managing the system, network interfaces, address translation, transmission media, and various protocols, including IP, ICMP, TCP, UDP, EGP, and SNMP.
RFC 1215	http://www.ietf.org/rfc/rfc1215.txt	Generic Traps (coldStart, linkUp, authenticationFailure only)
RFC 1316	http://tools.ietf.org/html/rfc1316	Character MIB
RFC 1317	http://tools.ietf.org/html/rfc1317	RS-232 MIB
RFC 2790	https://tools.ietf.org/html/rfc2790	Host Resources MIB for use with managing host systems, where "host" means any computer that communicates with other similar computers attached to the Internet.

Supported Digi enterprise MIBs

Digi devices support the following Digi enterprise MIBs.

To download these MIBs, go to the Digi Support site, click **Diagnostics, Utilities & MIBs**, select your product, and in the list displayed under **General Diagnostics, Utilities and MIBs** click the links for the MIBs.

Name	Description	Digi part number
Digi Connect Device Info MIB	Digi enterprise MIB for handling and displaying basic device information, such as firmware revisions in use, device name, IP network information, memory use, and CPU statistics.	40002410_*x*.mib
Digi Connect Mobile Information MIB	Digi enterprise MIB for handling and displaying device information for mobile devices.	40002593_*x*.mib
Digi Connect Wireless LAN MIB	Digi enterprise MIB for handling and displaying basic device information for wireless devices.	40002325_*x*.mib
Digi Serial Alarm Traps Management	Digi enterprise MIB for sending alarms as SNMP traps.	40002411_*x*.mib
Digi Login Traps MIB	Indicates when users attempt to sign into the device, and whether the attempt was successful.	40002339_*x*.mib
Digi Structures of Management (SMI) MIB	Data structures for managing hosts and gateways on a network.	40002195_*x*.mib

Name	Description	Digi part number
Digi Connect Mobile Traps MIB	A Digi enterprise MIB for sending alarms as SNMP traps for mobile devices.	40002594_*x*.mib
Digi Connectware Notifications MIB	This MIB may be required by some SNMP import facilities, as other MIBs may refer to it.	40002514_*x*.mib

Supported SNMP traps

You can enable or disable SNMP traps. Supported traps include:

- Authentication failure
- Login
- Cold start
- Link up

You can issue alarms in the form of SNMP traps.

A large set of MIBs define these various trap types (unsolicited status message from the device).

All products support MIBs for serial alarms / login traps/RFC 1215.

Products with the geofencing/GPS feature support MIBs for geofencing.

Products with mobile/cellular capability support MIBs for mobile alarms.

In the web interface, traps are enabled/disabled at **Configuration > System > SNMP > Enable Simple Network Management Protocol (SNMP) traps**

Alarms are configured at **Configuration > Alarms > Alarm Conditions > Alarm *n* > Alarm Destinations > Send SNMP trap to following destination when alarm occurs**

SNMP Configuration settings:

- **Enable Simple Network Management Protocol (SNMP):** This check box enables or disables use of SNMP.
  - The **Public community** and **Private community** fields specify passwords required to get or set SNMP-managed objects. Changing public and private community names from their defaults is recommended to prevent unauthorized access to the device.

    Public community: The password required to get SNMP-managed objects. The default is **public**.

    Private community: The password required to set SNMP-managed objects. The default is **private**.
  - **Allow SNMP clients to set device settings through SNMP:** This check box enables or disables the capability for users to issue SNMP “set” commands uses use of SNMP read-only for the Digi device.
- **Enable Simple Network Management Protocol (SNMP) traps:** Enables or disables the generation of SNMP traps.
  - **Trap Destinations:** Configures the IP address or fully qualified domain name (FQDN) of the system where the SNMP agent should send traps. The primary destination is required. The secondary destination is optional.
  - **Primary/Secondary**: The IP address of the system to which the SNMP agent should send traps. To enable any of the traps, a non-zero value must be specified. The primary destination is required. The secondary destination is optional. For Digi devices that support alarms, this field is required in order for alarms to be sent in the form of SNMP traps. See Alarms on page 53.

You can use the following SNMP trap check boxes:

- **Generate authentication failure traps**: The SNMP agent will send SNMP authentication traps when there are authentication failures.
- **Generate login traps**: The SNMP agent will send SNMP login traps on login attempts.
- **Generate cold start traps**: The SNMP agent will send traps on cold starts of the Digi device.
- **Generate link up traps**: The SNMP agent will send link up traps when network connections are established.

Device Cloud settings

In this discussion:

- The term *Device Cloud* refers to the Digi machine-to-machine cloud-based network operating platform.
- *Device Management* refers to a web based device management application that allows a user to manage their inventory of devices.
- *Device Cloud-registered device* is device that connects to the Device Cloud platform which implements the EDP protocol in order to establish and maintain this connection.

For more information about Device Cloud, these terms, and how to remotely configure and manage this device, please visit www.digi.com/cloud/digi-device-cloud and see the *Device Cloud User Guide*.

The Device Cloud configuration page sets up the connection to the Device Management remote management server so the Digi device can connect to the server. Device Management allows Device Cloud-registered devices to be configured and managed from remote locations.

Requirement: configuring the Digi device with a Device ID

An Device Cloud-registered device must be configured to properly communicate with Device Cloud. To do so, you must configure the Device Cloud-registered device to have a proper Device ID. By default, the Device ID is created from the MAC address of the device. You can configure the Device ID in the web interface on the **Configuration > System > Device Identity Settings** page; see System settings on page 55 for those settings. Typically, it is not necessary or recommended that the Device ID be modified from its default value.

After configuring the device's Device ID, you must configure the Device Cloud settings. There are three pages of settings: **Connection Settings, Short Messaging**, and **Advanced Settings**.

Connection settings

The Connection settings configure how the Device Cloud-registered device connects to Device Cloud. These settings how the Device Cloud-registered device and Device Cloud communicates with each other.

About Device Cloud connections

You can choose how your Device Cloud-registered device connects to and communicates with Device Cloud: through a *device-initiated Device Cloud connection* or a (device-initiated) *timed connection*. To illustrate how these types of connections work, here is a configuration scenario featuring Device Cloud-registered devices communicating over a cellular network.

Addresses for Device Cloud-registered devices can be publicly known, or private and dynamic, or handled through Network Address Translation (NAT). NAT reduces the need for a large amount of publicly known IP addresses by creating a separation between publicly known and privately known IP addresses. NAT allows a single device, such as a router, to act as an agent between a public network, such as the Internet or a wireless network, and a private, or local, network. This means that only one unique IP address is needed to represent an entire group of computers. Addresses handled through NAT can access the rest of "the world," but "the world" cannot access them.

In a *device-initiated Device Cloud connection*, the Device Cloud-registered device tries to connect to the network, and will continue attempts to reach Device Cloud to establish the connection. To maintain the connection, the Device Cloud-registered device sends *keep-alive messages* over the connection. You can configure the frequency in which keep-alive messages are sent. You can use device—initiated Device Cloud connections in any cellular network, whether using public or private IP addresses, or even if using NAT. Note that your cellular/mobile service plan may charge you, depending on your cellular/mobile service plan, when the Device Cloud-registered device sends keep-alives messages.

A *timed* connection is another form of a device-initiated connection. For a timed connection, the Device Cloud-registered device tries to connect to the Device Cloud Server at a configured, regular interval (period). If a connection to an Device Cloud Server is already established, the timed connection will not be attempted. The next attempt for a timed connection will occur at the next scheduled interval.

Device IP address updates

Changes to the IP address for an Device Cloud-registered device present a challenge in Device Cloud server-initiated connections, because Device Cloud needs to locate the Device Cloud-registered device by its new IP address. Device Cloud devices handle address changes by sending a *device IP address update* to Device Cloud. An IP address update permits Device Cloud to connect back to the Device Cloud-registered device, or to dynamically update a DNS with the IP address of the Device Cloud-registered device.

Device-Initiated Device Cloud Connection settings

- **Enable Device-Initiated Device Cloud Connection:** Configures the connection to Device Cloud to be initiated by the Device Cloud-registered device.
- **Device Cloud Server Address:** The IP address or hostname of the Device Cloud platform.
- **Automatically reconnect to Device Cloud after being disconnected**
  Reconnect after: Whether to automatically reconnect to Device Cloud after being disconnected and waiting for the specified amount of time.

Timed Device Cloud Connection

- **Enable Timed Device Cloud Connection**: When enabled, this device will initiate the connection to the Device Cloud Server at the configured interval (period). A timed connection defers to (will not disrupt) an Device Cloud connection that is already established. If a timed connection defers to an existing Device Cloud connection, or if the timed connection cannot be successfully established, the Digi device server will try again at the next interval.
- **Device Cloud Server Address**: The IP address or hostname of the Device Cloud Server.
- **Connect every: H hrs M mins**: The interval (period) in hours and minutes at which the Digi device server will attempt a timed connection to the specified Device Cloud Server.
- **After boot, wait before first timed connection**: When the Digi device server boots (start-up), a delay may be observed before the first timed connection is attempted. There are three choices for this delay:
  - **Immediate**: The first timed connection is attempted immediately.
  - **One Interval**: The first timed connection is attempted after one configured interval (period) has elapsed.
  - **Random Delay**: The first timed connection is attempted some random interval of time between zero (immediate) and the configured interval (period). A random delay may be helpful for such cases as when a number of devices are deployed in a single location, and it is desired to distribute their first Device Cloud timed connection attempts over time when power is restored following an outage.

Advanced Device Cloud settings

The default settings for Device Cloud remote management usually work for most situations. The Advanced settings configure the idle timeout for the connection between the Device Cloud-registered device and Device Cloud, and the keep-alive settings of the various interfaces (TCP and HTTP for mobile and Ethernet network connections). These settings should only be changed when the defaults do not properly work.

- Connection Settings: These settings configure the idle timeout for the connection between the Device Cloud-registered device and Device Cloud.
  - **Disconnect when the Device Cloud Connection is idle**
    Idle Timeout: Enables or disables the idle timeout for the connection. If enabled, an idle connection will be ended, after the amount of time specified in the **Idle Timeout** setting.
  - Authenticate to Device Cloud with a password
    Password: These fields are only applicable if your Device Cloud account has been configured to expect a password from the Device Cloud-registered device. Typically, this option is set through Device Cloud, as both the Device Cloud-registered device and Device Cloud need to be configured identically.
- Mobile (Cellular) Settings:
  Ethernet Settings
  WiFi Settings: These settings apply to device-initiated Device Cloud connections over mobile/cellular, Ethernet, and Wi-Fi networks. Each network type has these settings:
  - **Device Cloud Connection Keep-Alive Settings**: These settings control how often keep-alive packets are sent over the device-initiated connection to Device Cloud, and whether the Device Cloud-registered device waits before dropping the connection. Keep-alives for the Device Cloud connection serve three basic purposes:

    1. Keep the Device Cloud connection alive through network infrastructure such as routers, NATs and firewalls.

    2. Inform the other (remote) side of the Device Cloud connection that its peer is still active.

    3. Test the Device Cloud connection to detect whether it has stopped responding and should be abandoned. Recovery actions are taken as configured in other settings.

    The Device Cloud-registered device and Device Cloud each perform their own independent monitoring of the Device Cloud connection state (active, idle and missed keep-alives). If Device Cloud protocol messages or data other than keep-alives is exchanged over the Device Cloud connection, the idle timers that trigger keep-alives are reset, and the consecutive missed keep-alive counts are cleared to zero.

    The interval settings are used with the Assume connection is lost after *n* timeouts setting to signal when the connection has been lost.

    Device Send Interval: Specifies how frequently the device sends a keep-alive packet to Device Cloud if the Device Cloud connection is idle. Device Cloud expects to receive either Device Cloud protocol messages or keep-alive packets from the device at this interval.

    Server Send Interval: Specifies how frequently the Device Cloud-registered device sends a keep-alive packet to Device Cloud if the Device Cloud connection is idle. Device Cloud expects to receive either Device Cloud protocol messages or keep-alive packets from the Device Cloud-registered device at this interval.

    Important: It is recommended that this interval value be set as long as your application can tolerate to reduce the amount of data traffic.

    Assume connection is lost after *n* timeouts (Wait Count): After the number of consecutive expected keep-alives specified by this setting are missed according to the configured intervals, the connection is considered lost and is closed by the device and Device Cloud.
- **Connection Method:** Specifies the method by which the associated interface connects to Device Cloud.
  - **TCP:** Connect using TCP. This is the default connection method, and is typically good enough for most connections. It is the most efficient method of connecting to Device Cloud in terms of speed and transmitted data bytes.

Automatic: Automatically detect the connection method. This connection method is less efficient than TCP, but it is useful in situations where a firewall or proxy may prevent direct connection via TCP. Automatic will try each combination until a connection is made. This connection method requires the HTTP over Proxy Settings to be specified.

None: This value has the same effect as selecting TCP.

HTTP: Connect using HTTP.

HTTP over Proxy: Connect using HTTP.

HTTP over Proxy Settings: The settings required to communicate over a proxy network using HTTP. These settings apply when **Automatic** or **HTTP over Proxy** connection methods are selected.

Hostname: The name of the proxy host.

TCP Port: The network port number for the TCP network service on the proxy host.

Username:
Password: The user name and password for logging on to the proxy host.

Enable persistent proxy connections: Specifies whether the Device Cloud-registered device should use HTTP persistent connections. Not all HTTP proxies correctly handle HTTP persistent connections. Using persistent connections can improve performance when exchanging messages between the Device Cloud-registered device and Device Cloud using HTTP/proxy connection. You can reuse the same HTTP connection for multiple consecutive HTTP requests and replies, eliminating the overhead of establishing a new TCP connection for each individual HTTP request/reply, then closing that connection when the request is complete.

Manually configure a Device Cloud-registered device to connect to Device Cloud

To use the Device Management service for your Device Cloud-registered device, manually configure the device to connect to Device Cloud.

1. Open the web interface for the Device Cloud device and go to **Configuration > Device Cloud**.
2. On the **Device Cloud Configuration** settings page, type the URL of the Device Cloud platform, for example, **devicecloud.digi.com**, in the **Device Cloud Server Address** field under **Device -Initiated Management Connection**.
3. Click the check box labeled
   Automatically reconnect to Device Cloud after being disconnected.
4. Click **Apply**.

Managing alarms through Device Cloud

You can configure alarms to be sent to Device Cloud where they can be displayed and managed from the Device Cloud interface. See Alarms on page 53.

Users settings

Users settings involve several areas:

- User authentication: whether authentication is required for users accessing the Digi device, and the information required to access it. Depending on the Digi product, you can define multiple users and their authentication information. User authentication settings are on the Users settings page.
- User access settings**:** the device interfaces that a user can access, such as the command line or web interface.
- User permissions settings**:** the permissions a user has to access and configure the Digi Connect device.

- Several settings on the Network Configuration pages are available to further secure the Digi device. For example, you can disable unused network services on the Network Services page.

About user models and user permissions

The Digi Connect Family products provides the following user models:

- Two-user model
- More than two-user model

To determine which user model is implemented:

- In the web interface, if the menu includes **Users**, the Digi Connect device uses either the two-user model or the more than two users model.
- In the command-line interface, issue a **show user** or **set user** command. In the command output, note how many user IDs are defined: one, two, or more than two. Or, issue a **set user ?** command and note the range for the **id=*range*** option. If the **id=*range*** is not listed, there is only one user. Otherwise, the range for user IDs appears. These commands are described in the *Digi Connect Family Command Reference*.

Two-user model

- User 1 has a default name of **root**. This user is also known as the administrative user.
- User 1 has default permissions that enables it to issue all commands.
- You can change permissions for User 1 to be less than the default root permissions.
- User 2 is undefined. That is, the user does not exist by default, but you can define User 2.
- Use the User Permissions settings in the web interface or the **set permissions** command in the command-line interface (see the *Digi Connect Family Command Reference* for command description) to configure the permissions for User 2.
- You can change permissions for User 2 to be either greater than or less than its default.
-

CAUTION! Exercise caution in setting permissions for devices with this user model. A user cannot set another user's permission level higher than their own permission level, nor can a user raise their own permission level.

More-than-two-user model

User definitions are exactly the same as the two-user model, with the addition of user groups and more users. The **set group** command defines user groups; see the *Digi Connect Family Command Reference* for command description. Currently, there is no web interface page for defining user groups.

Special feature for Digi Connect ME only

Digi Connect ME uses the two-user model, but you can disable the login prompt (password authentication).

Password authentication

By default, password authentication is enabled for Digi Connect Family devices. That means a login prompt appears when you access the device by opening the web interface or issuing a **telnet** command.

Disable password authentication

You can disable password authentication as needed.

In the web interface:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, check the **Enable password authentication** check box.
3. Click **Apply**.

From the command line:

Issue a **newpass** command with a zero-length password.

Change the password for administrative user

To increase security, change the password for the administrative user from its default. By default, the administrative user name is **root**.

Note Record the new password. If the changed password is lost, the Digi device must be reset to the default firmware settings.

In Digi devices with a single-user model, changing the root password also changes the password for Advanced Digi Discovery Protocol (ADDP). In Digi devices with the multi-user model, changing the root password has no effect on ADDP. To change the ADDP password, type **newpass name=addp** from the command line.

In the web interface:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, click **root**.
3. Type the new password in the **New Password** and **Confirm Password** edit boxes. You can specify a case-sensitive password from 4 through 16 characters long. Click **Apply**.
4. You are immediately logged off. Log in to the web interface using the new values.

From the command line:

Issue the **newpass** command.

Add users

Digi devices allow multiple users to be defined. For those products, the **Users Configuration** page shows the currently defined users and allows you to add more user definitions. To add a user definition:

1. On the Main menu, click **Users**.
2. On the **Users Configuration** page, click **New**.
3. On the **Add New Users** page, specify the user name and password for a user. You can specify a case-sensitive password from 4 through 16 characters long. Confirm the password, and click **Apply**. The changes take effect immediately. No logout/login is necessary.

User access settings

For Digi devices with the two-user or more-than-two-users model, you can configure user access to the device interfaces. For example, the administrative user can access both the command line and web interface, but other users can be restricted to the web interface only.

Take care in changing access settings. If you are signed in as the administrative user and disable web interface, you will not be able to log in to the Digi device on your next attempt, and there is no way to raise your user permissions to enable the web interface again. You must reset the device to factory defaults to enable the web interface access.

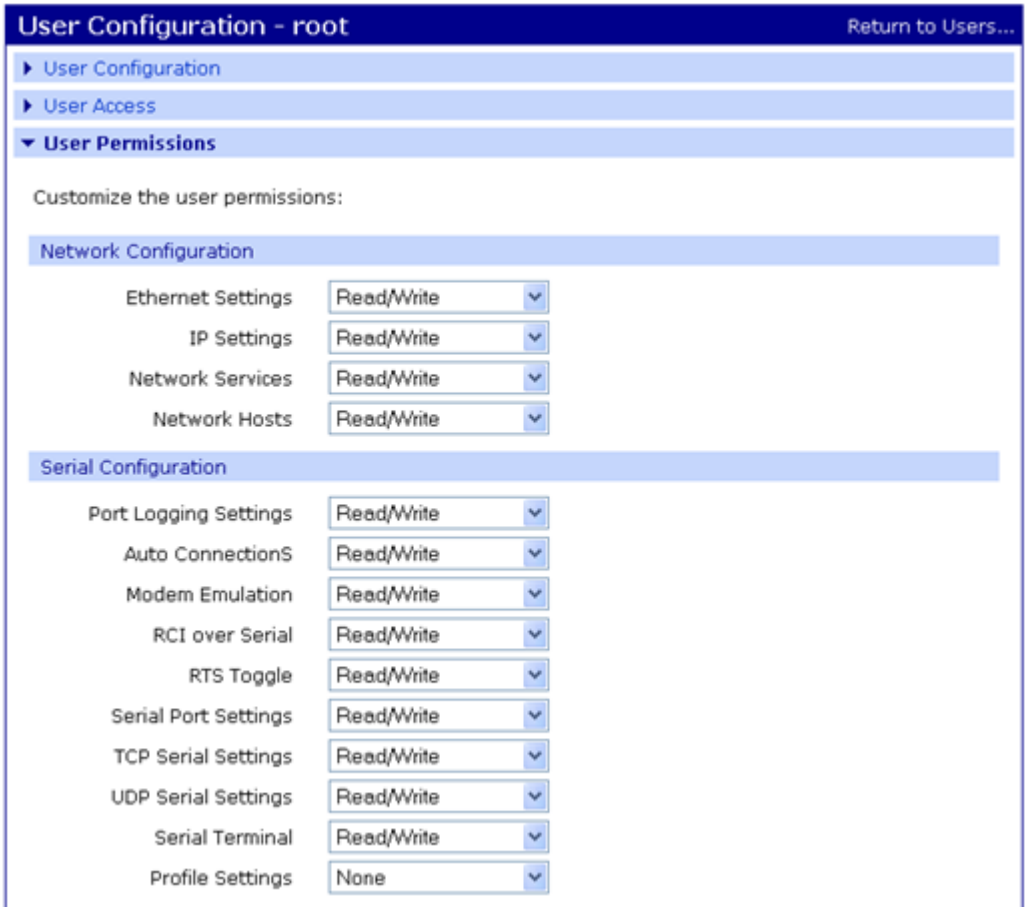
To set access settings:

1. On the Main menu, click **Users**.
2. On the Users Configuration page's list of users, click the user.
3. On the User Access page, enable or disable the device interface access as desired:
   - **Allow command line access:** Enables or disables access to the command line.
   - **Allow web interface access:** Enables or disables access to the web interface.
4. Click **Apply**. The changes take effect immediately. No logout/login is necessary.

User permissions settings

Use the User Permissions page to define whether and how users can use services and configuration settings for the Digi device. For example, you can disable a user's access to certain parts of the web interface, or allow them to display settings only but not change them.

The list of services and the user permissions available for them vary by Digi device and the features supported in the product.There are several groups of services, such as Network Configuration, Serial Configuration, System Configuration, Command Line Applications, and System Administration, with user permissions for various features. For example here are the Network Configuration and Serial Configuration user permissions for Digi Connect ME:



User permissions and effects

Permission Setting	Effect
None	The user does not have permission to execute this setting.
Read Self	The user can display their own settings, but cannot display settings for other users.
Read	The user can read the setting for all users, but does not have permission to modify or write the setting.
Read/Write Self	The user can read and write their own setting, but does not have permission to modify or write the setting for other users.
Read All/Write Self	The user can read the setting for all users and can modify their own setting.
Read/Write	The user has full permission to read and write the setting for all users.
Execute	The user has full permission to execute this setting.

Restrictions on setting user permissions

A user cannot set another user's permission level higher than their own permission level, nor can a user raise their own permission level.

Set user permissions from the web interface

1. On the Main menu, click **Users**.
2. On the Users Configuration page's list of users, click the user.
3. Click **User Permissions**.
4. A list of feature groupings and the user permissions for them appears. Customize these settings as needed.
5. Click **Apply**.

Set user permissions from the command-line interface

You can set user permissions from the command-line interface by the **set permissions** command. See the *Digi Connect Family Command Reference* for the command description.

Additional ways to control user access

Disable unused and non-secure network services

To further secure the Digi device, you can disable network services not necessary to the device, particularly non-secure or un-encrypted network services such as telnet. See Network services settings on page 38.

Applications

Most Digi devices support additional configurable applications. For most devices, these applications are accessed from the main menu under **Applications**. Some devices have an **Applications** link under **Configuration**.

Python® program management and programming resources

Digi incorporates a Python development environment into Digi devices. Python is a dynamic, object-oriented language that you can use to develop a wide range of software applications, from simple programs to more complex embedded applications. It includes extensive libraries and works well with other languages. A true open-source language, Python runs on a wide range of operating systems, such as Windows, Linux/Unix, Mac OS X, OS/2, Amiga, Palm Handhelds, and Nokia mobile phones. Python has also been ported to Java and .NET virtual machines. Unlike proprietary embedded development platforms, Digi's integration of the universal Python programming language allows customers a truly open standard for complete control of connections to devices, the manipulation of data, and event based actions.

Digi provides several resources to help you get started developing software solutions in Python:

Recommended distribution of Python interpreter

The current version of the Python interpreter embedded in Digi devices is 2.4.3. Please use modules known to be compatible with this version of the Python language only.

Digi Python Programmer's Guide

Digi incorporates a Python development environment into each ConnectPort X gateway. Unlike proprietary embedded development platforms, the integration of the universal Python programming language allows customers a truly open standard for complete control of connections to devices, the manipulation of data, and event based actions. Python is a dynamic object-oriented programming language that you can use to develop many kinds of software. It offers strong support for integration with other languages and tools, comes with extensive standard libraries, and you can learn how to use it in a few days.

The *Digi Python Programmer's Guide* introduces the Python programming language by showing how to create and run a simple Python program. It reviews Python modules, particularly modules with Digi-specific behavior. It describes how to load and run Python programs onto Digi devices, either through the command-line or web user interfaces, and how to run several sample Python programs. Find this guide at the Digi Python Wiki page—in the **Start Here** section, click the link titled **Digi Python Programmer's Guide**

http://www.digi.com/wiki/developer/index.php/Digi_Python_Programmer%27s_Guide

General Python programming language information is available at http://www.python.org/
Click the **Documentation** link.

Digi Developer Community Wiki

The Digi Developer Community Wiki is a place to learn about developing solutions using Digi's communications portfolio, software and services, including Python, Device Cloud, DIA, and more.

Digi's Developer Wiki is where you'll learn about developing solutions using Digi's communications product, software and services. The Wiki includes how-to's, example code, and M2M information to speed application development. Digi encourages an active developer community and welcomes your contributions.

http://www.digi.com/wiki/developer/index.php/Main_Page

Digi Python Custom Development Environment page

Use Python functions to obtain data from attached and integrated sensors on Digi products that have embedded XBee RF modules, such as the Drop-in Networking Accessories. See Digi Python wiki for more information.

http://www.digi.com/wiki/developer/index.php/Python_Wiki

Python Support Forum on digi.com

Find answers to common questions and exchange ideas and examples with other members of the Digi Python development community at:

http://www.digi.com/support/forum/categories/python

Device Integration Application (DIA)

The Device Cloud Device Integration Application (DIA) is software that simplifies connecting devices (sensors, PLCs, etc.) to communication gateways. DIA includes a comprehensive library of plug-ins that work out-of-the-box with common device types and you can extend it to include new devices. Its unique architecture allows the user to add most devices in under a day.

The DIA architecture provides the core functions of remote device data acquisition, control and presentation between devices and information platforms. It collects data from any device that can communicate with a Digi gateway, and is supported over any gateway physical interface. DIA presents this data to upstream applications in fully customizable formats, significantly reducing a customer's time to market.

Written in the Python® programming language for use on Digi devices, DIA may also be executed on a computer for prototyping purposes when a suitable Python interpreter is installed.

DIA is targeted for applications that need to gather samples of data from a set of devices (ZigBee® sensors, wired industrial equipment, GPS devices, etc.). It is an integral component of the Device Cloud platform, which customers can deploy with DIA software to build flexible, robust solutions with unprecedented speed.

Device Cloud and the Device Management service

Device Management allows for device management and access to device data within Device Cloud Designed as an on-demand solution, Device Management customers pay only for services consumed, conserving capital and requiring no infrastructure. Device Management includes:

- Device connector software that simplifies remote device connectivity and integration
- Management application (configure, upgrade, monitor, alarm, analyze) for Digi connectivity products including ZigBee nodes
- Application messaging engine with broadcast and receipt notification for application-to device interaction
- Cache and permanent storage options for generation-based storage and ad hoc access to historical device samples
- Application-focused bundles with ready-to-use illustrative applications

You can monitor and manage Digi devices from Device Management; for example.

- Displaying detailed state information and statistics about a device, such as device up time, amount of used and free memory, network settings, XBee network overview and detailed information on network nodes.
- Displaying and modifying mobile settings
- Monitoring the state of the device's connection and see a connection report and connection history statistics.
- Redirecting devices to a to a different destination
- Disconnecting devices
- Removing devices from the network.
- Alarms and Notifications feature that fires an alarm and sends an email notification should a specified event occur

To learn more about the Device Management and the services it provides, see the *Device Cloud User Guide* or go to www.digi.com/cloud/digi-device-cloud.

Python configuration pages

Selecting **Applications > Python** from the main menu for a Python-enabled Digi device displays the Python Configuration pages. These pages manage Python program files including uploading them to Digi devices and

deleting them as needed, and configure Python programs to execute when the Digi device boots, also known as auto-start programs.

Python files

The Python Files page is for uploading and managing Python programs on a Digi device.

- **Upload Files**: Click **Browse** to select a file to upload to and click **Upload**.
- **Manage Files**: Select any files to remove from the Digi device and click **Delete**.

Auto-start settings

The **Auto-start Settings** page configures Python programs to execute when the Digi device boots. You an configure up to four auto-start programs.

- **Enable:** When checked, the program specified in the Auto-start command line field will be run when the device boots.
- **Auto-start command line:** Specify the Python program filename to be executed and any arguments to pass to the program. The syntax is:

  filename [*arg1 arg2*...]

Manually execute uploaded Python programs

To manually execute an uploaded Python program on a Digi device, access the command line of the device and type the following command:

```
python filename [arg1 arg2...]
```

View and manage executing Python programs

To view Python threads running on the Digi device, access the command line and type the **who** command.

RealPort configuration

RealPort software must be installed and configured on each computer that uses the RealPort ports on the Digi device. This RealPort software is available for downloading from the Digi Support site. For products that ship with a Software and Documentation CD, the RealPort software is on the CD.

Install RealPort software

From the Digi Support site:

1. From a browser, go to **www.digi.com**.
2. Click the **Support** link and select **Drivers**.
3. Under **Select Your Product for Support**, select your Digi device from the product list and click **Submit**.
4. Under **Active Products**, select your Digi device from the product list.
5. Under **OS Specific Diagnostics, Utilities and MIBs,** select the operating system for your computer from the list.
6. Under **RealPort for Windows**, click the zip file.
7. Unzip the zip file.
8. Run the RealPort setup wizard.

From the Software and Documentation CD:

1. On the main page of the Software and Documentation CD, click **Software - install optional software**.

2. Select **RealPort** and click **Install**.
3. Follow the prompts of the Setup Wizard to install RealPort.

RealPort configuration settings

Applications > RealPort displays a page for configuring the RealPort application. Settings on this page include:

- **RealPort Settings**
  - **Enable Keep-Alives:** Enables sending of RealPort keep-alives. These keep-alives are messages inside the RealPort protocol, sent approximately every 10 seconds, to tell whoever is connected that the connection is still alive. RealPort keep-alives are different from TCP keep-alives, which are done at the TCP layer.

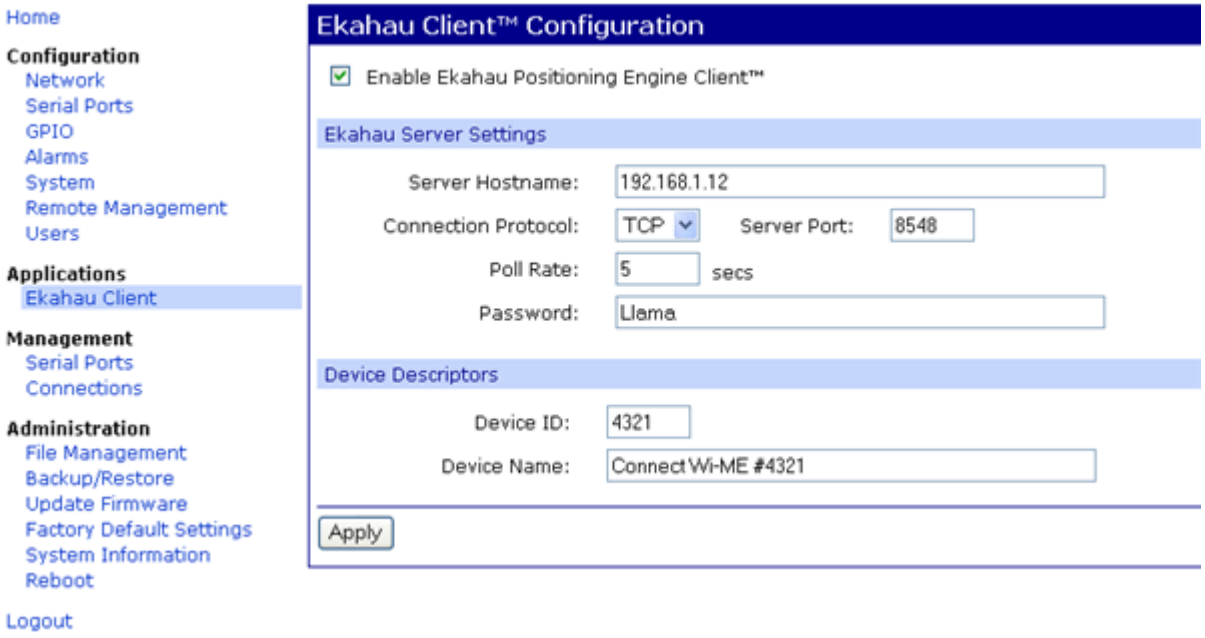
    Note that RealPort keep-alives generate additional traffic which may be undesirable in situations where traffic is measured for billing purposes.
  - **Enable Exclusive Mode:** Exclusive mode allows a single connection from any one RealPort client ID to be connected only. If this setting is enabled and a subsequent connection occurs that has the same source IP as an existing connection, the old existing connection is forcibly reset under the assumption that it is stale.
- **Device Initiated RealPort Settings**:
  - **Index**: An empty list means that no device initiated RealPort connections have been configured
  - **Host or IP Address**: The IP address or DNS name of the client to connect to.
  - Port: The network port to connect to on the client. The default port for VNC servers is 8771.
  - Retry Time: The amount of time in seconds to wait before reattempting a failed connection to the client.

Ekahau Client™

For Digi devices with Wi-Fi capability, clicking **Ekahau Client** displays a page for configuring Ekahau Client device-location software.

The Ekahau Client feature provides integrated support for Ekahau's Wi-Fi device-location solution, called the Ekahau Positioning Engine, on the Digi Connect Wi-ME, Digi Connect Wi-EM, and Digi Connect Wi-SP products. Ekahau offers a complete access point vendor-independent real-time location system for wireless LAN devices that is capable of pinpointing wireless LAN devices such as the Digi Connect products, laptops, PDAs, or other intelligent Wi-Fi enabled devices. The solution provides floor-, room- and door-level accuracy of up to 3.5 feet (1 m). The patented Ekahau positioning technology is based on simple signal-strength calibration maps, and enables customers to fully leverage an existing wireless LAN infrastructure without any need for proprietary hardware components.

Visit www.ekahau.com for additional information, including free evaluation licenses for the Ekahau Positioning Engine and Ekahau Site Survey software products.



Ekahau Client configuration settings include:

- **Enable Ekahau Positioning Engine Client™:** Enables or disables the Ekahau Positioning Engine Client feature.
  - **Ekahau Server Settings:** Configures how the Ekahau Positioning Engine Client communicates with the server.
  - **Server Hostname:** The hostname or IP address of the Ekahau Positioning Engine. The maximum length of this option is 50 characters. The default is 8548.
  - **Connection Protocol:** Specifies whether to use TCP or UDP as the network transport. The default is TCP.
  - **Server Port:** The network port used for communication. In the default Ekahau configuration, port 8548 uses TCP, and port 8549 uses UDP.
  - **Poll Rate:** The time in seconds between each scan or wireless access points and communication with the server. Once the Ekahau Client is enabled, every time the Digi device scans the network, it is essentially disassociated with the access point (AP) providing its network connectivity. In addition, during the time, or scanning interval, set by the poll rate, it will not be receiving or transmitting wireless packets. This could lead to packet loss. Set the poll rate as slow as acceptable in the application that uses the Digi device. The default is five seconds.
  - **Password:** A password to authenticate with the server. The maximum length of this option is 50 characters. The default for Digi and the Ekahau Positioning Engine is **Llama**.
- Device Descriptors:
  - **Device ID:** A numeric identifier for the Digi device, used internally by the Ekahau Positioning Engine for device tracking over time. Each Digi device located on the network requires a unique identifier.
  - **Device Name:** A descriptive name to identify the Digi device to users. The maximum length of this option is 50 characters.

Industrial Automation/Modbus Bridge

Industrial Automation is supported in these Digi devices: Digi Connect SP, Digi Connect Wi-SP, Digi Connect ME 4 MB, Digi Connect Wi-ME, Digi Connect EM, Digi Connect Wi-EM, and ConnectPort TS 8 and 16.

Currently, from the web interface, it is only possible to select a different port profile than **Industrial Automation**, or change the serial port settings, such as baud rate and parity. If changes are needed from the settings established by the Industrial Automation port profile, use the **set ia** command from the command-line interface.

Known limitations

- You can use Digi RealPort only if the Modbus Bridge function is disabled. You cannot use RealPort with Modbus/RTU or ASCII to access the Modbus Bridge function.
- The outgoing slave idle time used for remote Modbus IP-based slaves does not always close idle sockets predictably.
- While the Modbus bridge is active, do not attempt to "Port Forward" TCP 502 or UDP 502 to local Modbus/TCP servers while the Modbus Bridge is active. This causes neither function to work. Disable the Modbus Bridge if traditional Router/NAT function for Modbus/TCP port 502 is desired.

Disabling and enabling the Modbus Bridge

To disable the Modbus Bridge, select a different port profile than Industrial Automation. To enable it, reselect the Industrial Automation port profile. Any specialized settings that had been set through "set ia" commands are lost by disabling the Modbus bridge. They must be reconfigured when you reselect the Industrial Automation profile.

More information on Industrial Automation/Modbus

For more information on Industrial Automation, see the "set ia" command description in the *Digi Connect Family Command Reference,* and the application note *Remote Cellular TCP/IP Access to Modbus Ethernet and Serial Devices,* part number 90000773, available on the digi.com Support page at http://www.digi.com/support.

Configuration through Device Cloud

Device Cloud is an on-demand service. After creating a Device Cloud account, you can connect to Device Cloud. There are no infrastructure requirements. Remote devices and enterprise business applications connect to Device Cloud via standards-based Web Services.

See the *Device Cloud User Guide* for details on:

- Using Device Cloud as a management interface
- Creating a Device Cloud account
- Adding your ConnectPort X Family device to the Device Cloud device list so you can manage it from that interface

Alternative configuration options for Digi Connect Wi-SP

If configuring the Digi Connect Wi-SP with a serial connection, there are several configuration options.

Configure with an Access Point - Infrastructure Mode

1. Configure the network using an access point with the SSID - Connect and all encryption disabled (such as WEP & WPA).
2. Power up the device.
3. Launch the Discovery program and proceed with the configuration.

Configure without an Access Point - Laptop with a Wireless Card Ad-Hoc Mode

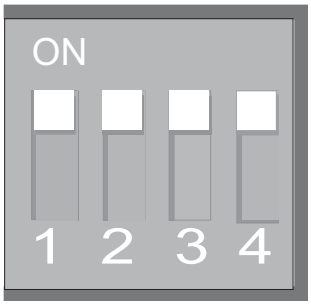
1. Configure the wireless card to operate in Ad-Hoc mode with the SSID - Connect.
2. Power up the device.

3. Launch the Discovery application on the laptop and proceed with the configuration.

Command line access

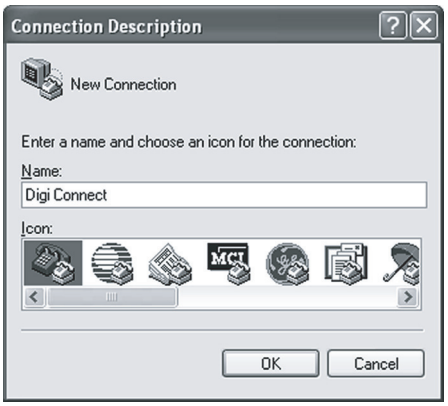
Note To set the DIP switches on the Digi Connect Wi-SP (or SP), ALWAYS disconnect the power supply before resetting the switches. See the following procedure for more details.

1. Disconnect the power supply.
2. Set the Digi Connect Wi-SP DIP switches in the On or up position. The figure shows DIP Switch settings for Command Line access for both the Digi Connect Wi-SP and the Digi Connect SP.



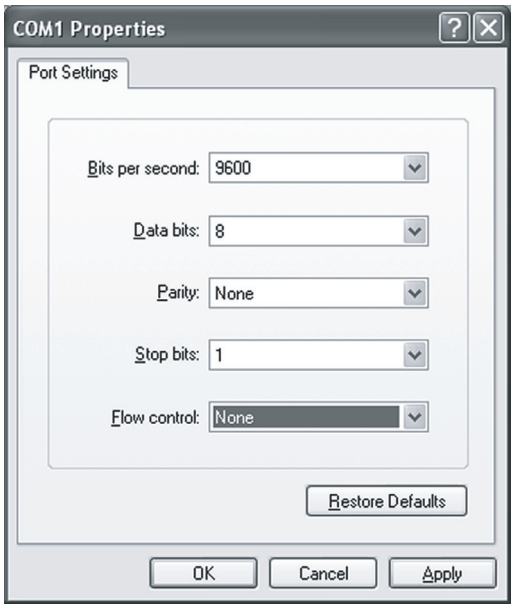
3. Connect the Digi Connect Wi-SP to a computer with a serial cable.
4. Access a terminal emulation program such as HyperTerm.

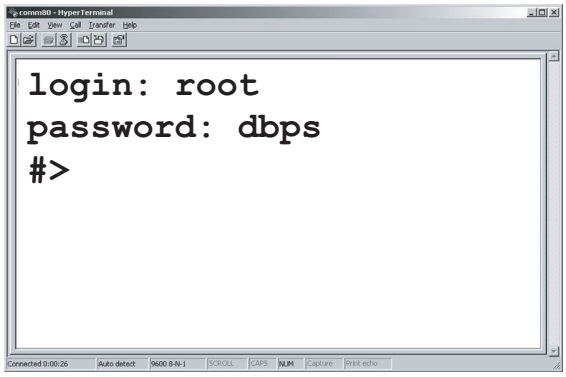
   Choose **Start > Accessories > Communication > Hyperterm** and type a name for the connection.
5. Select COM1 and click **OK**.



6. Set the port settings to 9600, 8, None, 1, None (default settings) click Apply then OK.
7. Type the default user name: **root**

   and the default password: **dbps**
8. Use the **set wlan** command to configure wireless network settings. This command is described in the *Digi Connect Family Command Reference*, available for download from the Digi Support site and, for products that ship with a Software and Documentation CD, on the CD.
9. After configuring the Digi Connect Wi-SP parameters to function within your network, disconnect the power supply and the serial cable from the Digi Connect Wi-SP.





10. Reset the DIP switch settings according to serial device requirements (EIA-232/422/485).

11. Connect the antenna and the power supply to the Digi Connect Wi-SP.

12. Start the Digi Device Setup Wizard to discover and the configure the Digi Connect Wi-SP for your network.

Note See also Digi support site at www.digi.com/support/eservice for additional command resources.

Configuration through the command line

Configuring a Digi devicethrough the command-line interface consists of entering a series of commands to set values in the device. The *Digi Connect Family Command Reference* describes the commands used to configure, monitor, administer, and operate Digi devices.

Access the command line

To configure devices using commands, first access the command line. Launch the command-line interface by using the **telnet** command. Type the following **telnet** command from a command prompt on another networked device, such as a server:

```
#> telnet ip-address
```

where *ip-address* is the IP address of the Digi device. For example:

```
#> telnet 192.3.23.5
```

If security is enabled for the Digi device, (that is, a user name and password have been set up for logging on to it), a login prompt appears. If the user name and password for the device are unknown, contact the system administrator who originally configured the device.

Verify device support of commands

To verify whether a Digi devicesupports a particular command, online help is available. For example:

- **help** displays all supported commands for a device.
- **?** displays all supported commands for a device
- **set** ? displays the syntax and options for the **set** command. Use this command to determine whether the device includes a particular "set" command variant to configure various features.
- **help set** displays syntax and options for the **set** command.
- **set serial ?** displays the syntax and options for the **set serial** command.
- **help set serial** displays the syntax and options for the **set serial** command.

Examples of configuration commands

Here are some examples of commands used to configure Digi device.

This set does not represent the complete set of configuration commands. See the *Digi Connect Family and ConnectPort TS Family Command Reference* for the complete command set.

To configure or display:	Use this command:
alarms	set alarms
autoconnection behaviors for serial port connections	set autoconnect
Device Cloud settings	set mgmtconnection set mgmtglobal set mgmtnetwork
Ethernet communications parameters	set ethernet
IP forwarding	**set forward**
GPIO pins	set gpio
group attributes: create or establish group attributes, update or remove groups or group attributes	**set group**
host name	set host
modem emulation	set pmodem
network options	set network

To configure or display:	Use this command:
network services	**set service**
Point-to-Point (PPP) outbound connections	set pppoutbound
port buffering	set buffer
port profile for a serial port	set profiles
system-identifying information	set system
serial port options—general	set serial
serial TCP and serial UDP	**set tcpserial** and **set udpserial**
RealPort configuration options	set realport
RTS toggle	set rtstoggle
SNMP	set snmp
Telnet control commands: send telnet control command to last active telnet session; set telnet operating options	send mode
users, user groups, and passwords	set user **set group** newpass
user permissions for various services and command line interface commands	set permissions
wireless devices	set wlan

Configuration through Simple Network Management Protocol (SNMP)

Configuring Digi devices through Simple Network Management protocol uses a subset of standard MIBs for network and serial configuration, plus several Digi enterprise MIBs for device identification and alarm handling. These MIBs are listed and described under Supported standard RFCs and MIBs on page 57, and must be loaded into a network management station (NMS). The standard and Digi Enterprise MIBs allow for very basic network and serial configuration. For more detailed configuration settings, use the command-line interface or web interface instead.

Some elements of SNMP configuration can only be configured from the web interface or command line, such as the setting to send alarms as SNMP traps. In the web interface, this setting is located at **Configuration > Alarms > *alarm* > Alarm Destinations > Send SNMP trap to following destination when alarm occurs**. See Alarms on page 53. In the command-line interface, this setting is configured by the **set alarm** option **typescript**. See the **set alarm** command description in the *Connect Family Command Reference*.

For information on SNMP as a monitoring interface, see Monitoring Capabilities from SNMP on page 88.

Batch capabilities for configuring multiple devices

If you need configure multiple Digi devices at a time, use the batch configuration capabilities to upload configuration files are available through the Digi Connect Programmer utility. The Digi Connect Programmer utility is a command-

line-based interface to Digi devices. Use this utility to upload firmware, files, configuration settings and factory defaults to a Digi device. You can run it from the command line on a computer that uses the Microsoft Windows operating system.

You can download the Digi Connect Programmer utility from the Digi website.

The following table list some of the available commands. For details and command descriptions, see the *Digi Device Customization and Integration Guide.*

Command	Description
connectprog /help	Displays the complete list of available command options.
connectprog /discover	Discovers devices on the local LAN. This is equivalent to using the Digi Device Discovery utility.
connectprog set /mac=<*mac address*> /ip=<*ip address*>	Sets the IP address for the device at the identified MAC address.
connectprog /info /destip=<*ip address*> /username=root /password=dbps	Displays device information for the specific device.
connectprog /backup /destip=<*ip address*> /username=root /password=dbps	Backs up the complete device configuration to config.rci in the local directory.
connectprog /upload /destip=<*ip address*> /config=<*directory path*>\<*file name*>.txt /username=root /password=dbps	Uploads the configuration file to the device.

The following example displays the results for the discover command:

```
connectprog /discover

Digi Connect Programmer
Version 1.6.25.0
Copyright 2003-2009 Digi International Inc.

Searching for devices. Please wait...

 IP Address      | MAC Address       | Model
-----------------+-------------------+------------------------------
    192.168.1.4   00:40:9D:12:34:56   ConnectPort TS 16
-----------------+-------------------+------------------------------
1 device found.
```

Monitoring and management

You can monitor the port, device, system, and network activities of Digi devices from a variety of interfaces. Changes in data flow may indicate problems or activities that may require immediate attention. In addition, you can manage connections and network services.

This chapter discusses monitoring and connection-management capabilities and tasks in Digi devices. It covers these topics:

Monitoring capabilities from Device Cloud

You can monitor and manage Digi devices from Device Cloud; for example.

- Displaying detailed state information and statistics about a device, such as device up time, amount of used and free memory, network settings, XBee network overview and detailed information on network nodes.
- Mobile settings
- Monitoring the state of the device's connection and see a connection report and connection history statistics.
- Redirecting devices to a to a different destination
- Disconnecting devices
- Removing devices from the network.

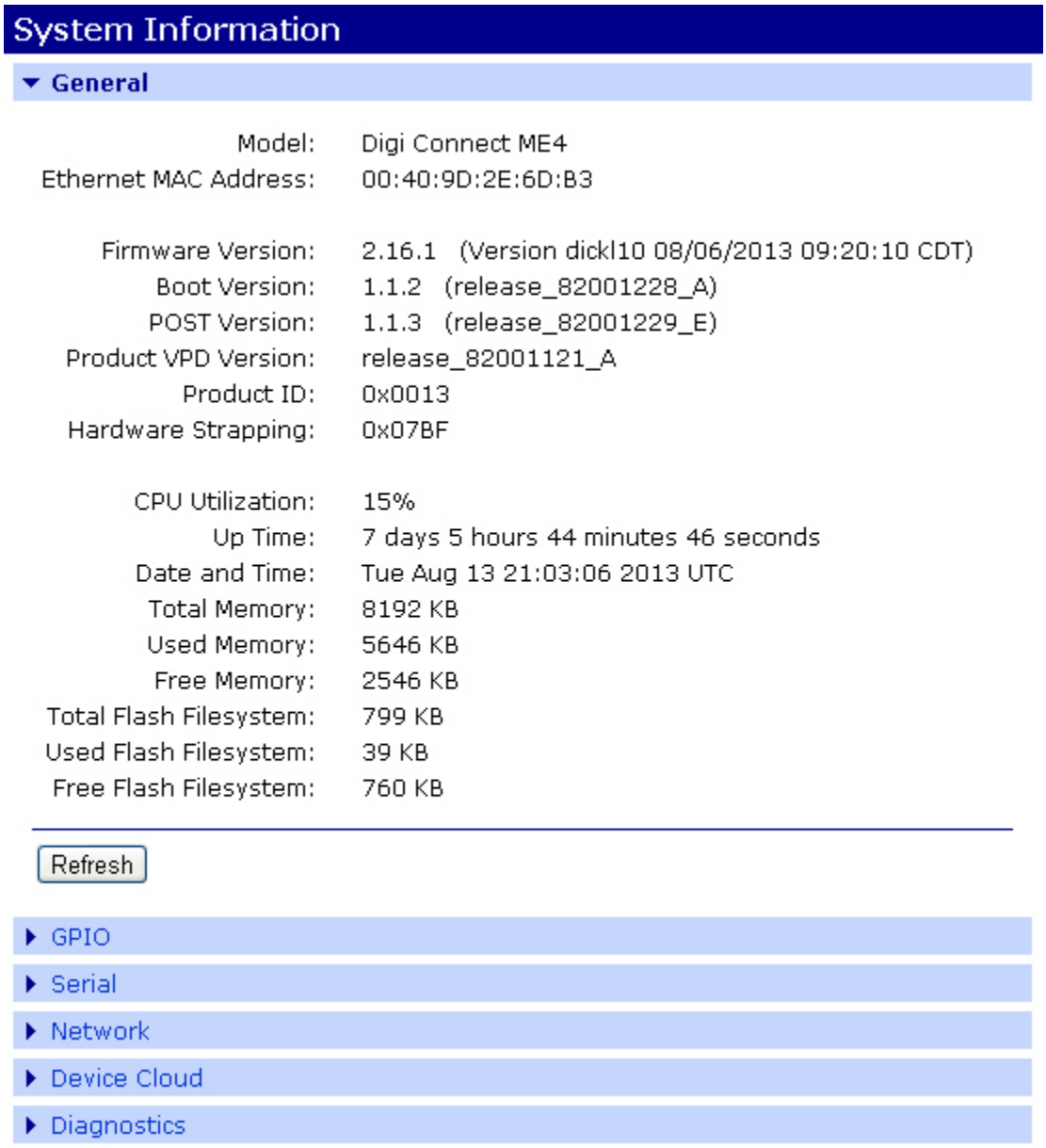
To learn more about Device Cloud and the services it provides, see the *Device Cloud User Guide.*

Monitoring capabilities in the web interface

Several device monitoring and connection-management capabilities are available in the web interface, including system information and statistics, and connection management information.

System information

The System Information pages display general system information, GPIO pin information, including the current state of GPIO pins, serial port information, system statistics, and diagnostics. Technical support uses this information to troubleshoot problems. To display these pages, go to **Administration > System Information**.



General system information

The General pane displays the following general system information.

Field	Description
Model	The model of the Digi device.
MAC Address	A unique network identifier required for all network devices. The MAC address is on a sticker on the Digi device and appears as 12 hexadecimal digits, usually starting with 00:40:9D.
Firmware Version	The current firmware version running in the Digi device. Use this information to locate and download new firmware. You can download firmware updates from: http://support.digi.com/support/firmware

Field	Description
Boot Version	The current boot code version running in the Digi device.
POST Version	The current Power-On Self Test (POST) code version running in the Digi device.
CPU Utilization	The amount of CPU resources the Digi device uses. **Important:** 100% CPU Utilization may indicate encryption key generation is in-progress. On initial boot, the Digi device generates some encryption key material: an RSA key for SSL/TLS operations, and a DSA key for SSH operations. This key-generation process can take as long as 40 minutes. Until the RSA or DSA key is generated, the Digi device will be unable to initiate or accept that type of encrypted connection. The Digi device reports itself as 100% busy, but since key generation occurs at a low priority, the device will still function normally. On subsequent reboots, the Digi device will use its existing keys and not need to generate another unless a reset to factory defaults is done, which will cause a new key to be generated on the next reboot.
Up Time	The amount of time the Digi device has been running since it was last powered on or rebooted.
Total/Used/Free Memory	The amount of memory (RAM) available, currently in use, and currently not being used.

GPIO information

The GPIO pane displays the current state of the General Purpose I/O pins on the Digi device. You can change the state of pins configured for output, as discussed in GPIO pins on page 51. Alarms can b issued when GPIO pins change state, as discussed in Alarms on page 53.

Serial port information

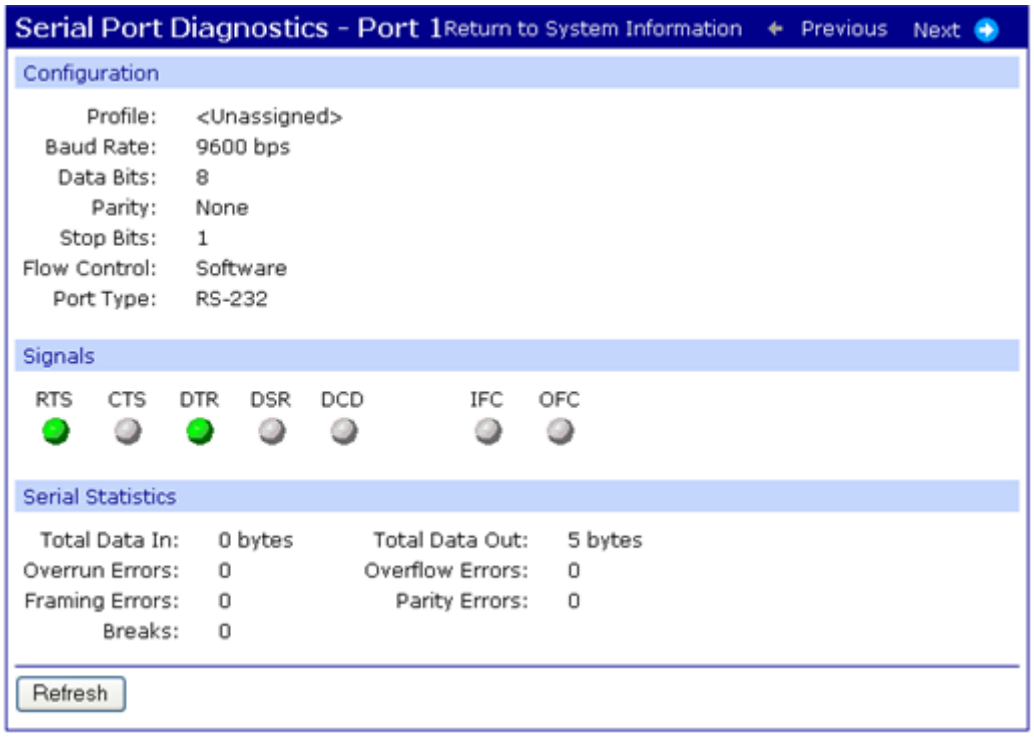
The **Serial** pane lists the serial ports that are configured for the Digi device. Click a port to view the detailed serial port information.

Serial port diagnostics

The Serial Port Diagnostics page provides details that may aid in troubleshooting serial communication problems.

Configuration

The Configuration pane displays the electrical interface (Port Type) and basic serial settings.



Signals

The Signals pane shows the state of serial port signals. Signals are green when asserted (on) and gray when not asserted (off). The following table defines signals:

Signal	Description
RTS	Request To Send.
CTS	Clear To Send.
DTR	Data Terminal Ready.
DSR	Data Set Ready.
DCD	Data Carrier Detected.
OFC	Output Flow Control. Indicates that flow control is enabled on the remote side of the serial-port connection, and that the Digi device should stop sending data.
IFC	Input Flow Control. Indicates that the Digi device is operating as if flow control is enabled for incoming data sent from the remote side of the serial-port connection. This signal is more of an indication that flow control is intended or expected rather than true state information. If the remote side has a flow-control mechanism enabled, the Digi device will use it.

Serial statistics

The Serial Statistics pane displays data counters and error tracking that will help determine the quality of data that is being sent or received. If the error counters are accumulating, there may be a problem in the Digi device.

Field	Description
Total Data In	Total number of data bytes received.
Total Data Out	Total number of data bytes transmitted.
Overrun Errors	Number of overrun errors - the next data character arrived before the hardware could move the previous character.
Overflow Errors	Number of overflow errors - the receive buffer was full when additional data was received.
Framing Errors	Number of framing errors received - the received data did not have a valid stop bit.
Parity Errors	Number of parity errors - the received data did not have the correct parity setting.
Breaks	Number of break signals received.

Network statistics

Network pane provide details about network and protocol activity that may aid in troubleshooting network communication problems. Statistics displayed are those gathered since the unit was last rebooted. If an error counter accumulates at an unexpected rate for that type of counter, there may be a problem in the Digi device.

Ethernet Connection Statistics

Field	Description
Speed	Ethernet link speed: 10 or 100 Mbps. N/A if link integrity is not detected, for example, if the cable is disconnected.
Duplex	Ethernet link mode: half or full duplex. N/A if link integrity is not detected, for example, if the cable is disconnected.
Bytes Received Bytes Sent	Number of bytes received or sent.
Unicast Packets Received	Number of unicast packets received and delivered to a higher-layer protocol. A unicast packet is one directed to an Ethernet MAC address.
Unicast Packets Sent	Number of unicast packets requested to be sent by a higher-layer protocol. A unicast packet is one directed to an Ethernet MAC address.
Non-Unicast Packets Received	Number of non-unicast packets received and delivered to a higher-layer protocol. A non-unicast packet is one directed to either an Ethernet broadcast address or a multicast address.
Non-Unicast Packets Sent	Number of non-unicast packets requested to be sent by a higher-layer protocol. A non-unicast packet is one directed to either an Ethernet broadcast address or a multicast address.
Unknown Protocol Packets Received	Number of received packets discarded because of an unknown or unsupported protocol.

IP Statistics

Field	Description
Datagrams Received Datagrams Forwarded	Number of datagrams received or forwarded.
Forwarding	Displays whether forwarding is enabled or disabled.
No Route	Number of outgoing datagrams for which no route to the destination IP could be found.
Routing Discards	Number of outgoing datagrams which have been discarded.
Default Time-To-Live	Number of routers an IP packet can pass through before being discarded.

TCP statistics

Field	Description
Segments Received Segments Sent	Number of segments received or sent.
Active Opens	Number of active opens. In an active open, the Digi device is initiating a connection request with a server.
Passive Opens	Number of passive opens. In a passive open, the Digi device is listening for a connection request from a client.
Bad Segments Received	Number of segments received with errors.
Attempt Fails	Number of failed connection attempts.
Segments Retransmitted	Number of segments retransmitted. Segments are retransmitted when the server does not respond to a packet sent by the client. This is to handle packets that might get lost or discarded somewhere in the network.
Established Resets	Number of established connections that have been reset.

UDP statistics

Field	Description
Datagrams Received Datagrams Sent	Number of datagrams received or sent.
Bad Datagrams Received	Number of bad datagrams received. This number does not include the value contained by **No Ports**.
No Ports	Number of received datagrams that were discarded because the specified port was invalid.

ICMP statistics

Field	Description
Messages Received	Number of messages received.
Bad Messages Received	Number of received messages with errors.
Destination Unreachable Messages Received	Number of destination unreachable messages received. A destination unreachable message is sent to the originator when a datagram fails to reach its intended destination.

WiFi LAN statistics

The WiFi LAN Statistics section displays detailed wireless statistics that may aid in troubleshooting network communication problems in wireless Digi devices.

Field	Description
Status	The current status of the wireless Digi device, which may include: • **Not Connected**: not associated or connected w/ any access point, perhaps because the wireless device has not fully initialized, is out of range, or the wireless interface is disconnected because the Ethernet interface is enabled. • **Searching for Network**: searching for a wireless network or access point for connection. • **Associated with Network**: successfully associated with the network w/ the proper network settings and encryption. • **Authenticated with Network**: successfully authenticated a user name and password with the network when WPA is enabled. • **Joined Ad Hoc Network**: successfully connected to and joined an ad-hoc network. • **Started Ad Hoc Network**: successfully created, started, and joined an ad-hoc network.
Network Name	The name of the wireless network to which the Digi device is connected.
Network ID	The ID of the wireless network to which the Digi device is connected and communicating.
Channel	The frequency channel that the wireless LAN radio uses for the Digi device.
Transmit Rate	The current transmission rate for the wireless LAN radio.
Signal Strength	The current receive signal strength as reported by the wireless LAN radio. Ranges are from 0 to 100.

Device Cloud status

Use the Device Cloud status section to view the connection status for the Device Cloud service.

Diagnostics

The **Diagnostics** page has a ping utility to determine whether the Digi device can access remote devices over the network. Type the hostname of the remote device to attempt to access, and click **Ping**.

Manage connections and services

The **Management** menu is for viewing and managing connections and services for the Digi device.

Manage serial ports

Management > Serial Ports provides an overview of the serial ports and their connections. Clicking **Connections** displays the active connections for that serial port. You can refresh the view to see new serial-port connections list, and you can disconnect serial-port connections as needed.

Manage connections

Management > Connections displays active system connections.

Manage active system connections

The Active System Connections list provides an overview of connections associated with various interfaces, such as user connections to the device's web interface, connections to the command line through the local shell, or Python threads currently running; the protocols used for the connections; and the number of active sessions for each connection. Use this list to determine whether any connections are no longer needed and can be disconnected.

Event logging

Management > Event Logging displays the event log for the Digi device. This log records events throughout the Digi device's system, such as starting or resetting the Digi device, configuring features, actions performed by various interfaces and subsystems, starting applications, etc. The event log is always enabled and is not user-configurable. When the Digi device operates in an unexpected manner, you can send the log entries to Digi for analysis by Technical Support and Engineers. The event log cannot be turned off, so that Digi receives an accurate view of all aspects of the operation of the device.

The event log is maintained in RAM, and there is no history across reboots of the device. When the log "overflows" the oldest entries are overwritten with new ones, so the history is incomplete.

The **Clear** button clears the event log.

Monitoring capabilities from the command line

There are several commands for monitoring Digi devices and managing their connections. For complete descriptions of these commands, see the *Digi Connect Family Command Reference*.

Commands for displaying device information and statistics

display commands

The **display** commands display real-time information about a device, such as:

- General product information, including the product name, MAC address, boot, post, and firmware versions, memory usage, utilization, and uptime, or the amount of time since the device was booted (**display device**).
- Active interfaces on the system, for example, the web interface, command line interface, Point to Point Protocol (PPP), and Ethernet interface, and their status, such as "Closed" or "Connected." (**display netdevice**).
- GPIO signals (**display gpio**).
- The event log (**display logging**).
- Memory usage information (**display memory**).

- Serial modem signals. (**display serial**).
- General status of the sockets resource (**display sockets**).
- Active TCP sessions and active TCP listeners (**display tcp**).
- Current UDP listeners (**display udp**).
- Point-to-Point Protocol (PPP) information.
- Uptime information (**display uptime**).

info commands

The **info** commands displays statistical information about a device over time. The statistics displayed are those gathered since the tables containing the statistics were last cleared. Statistics include:

- Device statistics. **info device** displays such details as product, MAC address, boot, POST, and firmware versions, memory usage, utilization, and uptime.
- Ethernet statistics. **info ethernet** displays statistics regarding the Ethernet interface, including the number of bytes and packets sent and received, the number of incoming and outgoing bytes that were discarded or that contained errors, the number of Rx overruns, the number of times the transmitter has been reset, and the number of incoming bytes when the protocol was unknown.
- ICMP statistics. **info icmp** displays the number of messages, bad messages, and destination unreachable messages received.
- Serial statistics. **info serial** displays the number of bytes received and transmitted, signal changes, FIFO and buffer overruns, framing and parity errors, and breaks detected.
- TCP statistics. **info tcp** displays the number of segments received or sent, the number of active and passive opens, the number of bad segments received, the number of failed connection attempts, the number of segments retransmitted, and the number of established connections that have been reset.
- UDP statistics. **info udp** displays the number of datagrams received or sent, bad datagrams received, and the number of received datagrams that were discarded because the specified port was invalid.
- Wireless statistics. **info wlan** displays detailed statistics for wireless devices that may aid in troubleshooting network communication problems with a wireless network.

set alarm

set alarm displays alarm settings, including conditions that trigger alarms, and how alarms are sent, either as an email message, an SNMP trap, or both. You can configure the alarms as needed.

set gpio

set gpio displays current GPIO pin settings. You can reconfigure the pin settings as needed.

set buffer and display buffers

set buffer configures buffering parameters on a port and displays the current port buffer configuration. **display buffers** displays the contents of a port buffer, or transfers the port-buffer contents to a server running Trivial File Transfer Protocol (TFTP).

set snmp

set snmp configures SNMP, including SNMP traps, such as authentication failure, cold start, link up, and login traps, and displays current SNMP settings.

show

The **show** commands display current settings in a device.

Commands for managing connections and sessions

- **close**: Closes active sessions that were opened by **connect**, **rlogin**, and **telnet** commands.
- **connect**: Establishes a connection, with a serial port.
- **exit** and **quit**: These commands terminate a currently active session.
- **who** and **kill**: The **who** command displays a global list of connections. The list of connections includes those associated with a serial port or the command-line interface. who is particularly useful in conjunction with the kill command, which terminates active connections. Use who to determine any connections that are no longer needed, and end the connections by issuing a kill command.
- **ping**: Tests whether a host or other device is active and reachable.
- **reconnect**: Reestablishes a previously established connection; that is, a connection opened by a **connect**, **rlogin**, or **telnet** command; the default operation is to reconnect to the last active session.
- rlogin: Performs a login to a remote system.
- **send**: Sends a telnet control command, such as break, abort output, are you there, escape, or interrupt process, to the last active telnet session.
- **status**: Displays a list of sessions, or outgoing connections made by **connect**, **rlogin**, or **telnet** commands for a device. Use the **status** command to determine which of the current sessions to close.
- **telnet**: Establishes an outgoing telnet connection, also known as a session.

Monitoring Capabilities from SNMP

Device monitoring capabilities from SNMP include, among other things:

- Network statistics, defined in RFC 1213, MIB-II
- Port statistics, defined in RFCs 1316 and 1317
- Device information, defined in Digi enterprise MIB DIGI-DEVICE-INFO.mib

For more information on the statistics available through the standard RFCs listed above, refer to the RFCs available on the IETF web site (www.ietf.org). For enterprise MIBs, refer to the description fields in the MIB text.

Device administration

This chapter discusses the administration tasks that need to be performed on Digi devices periodically, such as file management, changing the password used for logging onto the device, backing up and restoring device configurations, updating firmware and Boot/POST code, restoring the device configuration to factory defaults, and rebooting the device. As with device configuration and monitoring, it covers performing administrative tasks through a variety of device interfaces, including web, and command-line interfaces.

Administration from the web interface

The Administration section of the web interface main menu provides the following choices:

- **File Management:** For uploading and managing files, such as custom web pages, applet files, and initialization files. See File management on page 89 for more information.
- **Python Program File Management:** For uploading custom programs in the Python programming language to Digi devices and configuring the programs to execute automatically at startup. See Python® program management and programming resources on page 67 for more information.
- **Backup/Restore:** For backing up or restoring a device's configuration settings. See Backup/restore device configurations on page 90 for more information.
- **Update Firmware:** For updating firmware, including Boot and POST code. See Update firmware and Boot/POST Code on page 90 for more information.
- **Factory Default Settings:** For restoring a device to factory default settings. See Restore a device configuration to factory defaults on page 91 for more information.
- **System Information:** For displaying general system information for the device and device statistics. See Display system information on page 93 for more information.
- **Activate Find Me LED**: On the Digi Connect ES model only, turns on/off the Find Me or locator LED to aid in locating a specific Digi device. See Activate Find Me LED on page 93 for more information.
- **Reboot:** For rebooting the device. See Reboot the Digi device on page 93 for more information.

These administrative tasks are organized elsewhere in the web interface:

- Enable and disable network services. See Network services settings on page 38 for more information.
- Enable password authentication for the Digi device. See Users settings on page 63 for more information.

File management

The **File Management** page of the web interface uploads custom files to a Digi device, such as an image file of your company logo. Custom applets allow the flexibility to alter the interface either by adding a different company logo, changing colors, or moving information to different locations. If custom applets is not used, using this feature is not necessary.

Uploading files

To upload files to a Digi device, type the file path and name for the file, or click **Browse** to locate and select the file, and click **Upload**.

Delete files

To delete files from a Digi device, select the file from the list under **Manage Files** and click **Delete**.

Custom files are not deleted by device reset

Any files uploaded to the file system of a Digi device from the File Management page are not deleted by restoring the device configuration to factory defaults, or by pressing the Reset button on the device (see Restore a device configuration to factory defaults on page 91). This deletion is prevented so that customers with custom applets and custom factory defaults can retain them on the device and not have them deleted by a reset. Such files can only be deleted by the Delete operation, described above.

Backup/restore device configurations

After you configure a Digi device, back up the configuration settings. You can restore the backup configuration settings if a problem occurs when updating the firmware or adding hardware. If you need to configure multiple devices, you can use the backup/restore feature to load the backup configuration settings from the first device onto the other devices.

This procedure shows how to back up or restore the configuration to a server and download a configuration from a server to a file or TFTP.

If using TFTP, ensure that the TFTP program is running on a server.

1. From the Main menu, click **Administration > Backup/Restore**. The Backup/Restore page appears.
2. Choose the appropriate option (**Backup** or **Restore**) and select the file.

Update firmware and Boot/POST Code

You can update the firmware and/or boot/POST code for a Digi device from a file on a computer or through TFTP. The recommended method is to download the firmware to a local hard drive. TFTP is supported for those using UNIX systems. Both the firmware and the boot/POST code are updated using the same set of steps.The Digi device automatically determines the type of image being uploaded. Before uploading the firmware or the boot/POST code, it is very important to read the Release Notes supplied with the firmware to check if the boot/POST code must be updated before updating the firmware.

Prerequisites

These procedures assume that:

- You downloaded the firmware file from digi.com.
- If you are using TFTP, that the TFTP server is running.

Update firmware from a file on a computer

1. From the Main menu, click **Administration > Update Firmware**. The Update Firmware page appears.
2. Type the name of the firmware or POST file in the **Select Firmware** edit box, or click **Browse** to locate and select the firmware or POST file.
3. Click **Update**.

   Important: DO NOT close the browser until the update completes and a reboot prompt appears.

Update firmware from a TFTP Server

Updating firmware from a TFTP server is done from the command-line interface using the **boot** command. It cannot be done from the web interface. For details, see Administration from the command-line interface on page 94.

Restore a device configuration to factory defaults

There are several ways to reset the device configuration of a Digi device to the factory default settings: using the **Administration > Factory Defaults** page in the web interface; using the **boot** command from the command line; and using the Reset button, or, on some models, a Reset signal The first two reset methods are a soft reset, while the reset button/signal method is a hard reset.

Using the Administration > Factory Defaults page on the web interface

The **Restore Factory Defaults** operation from the web interface clears all current settings, resets password for the administrative/root user, and restores the settings to the factory defaults. If a Digi device has custom factory default settings, the settings will revert to those custom defaults instead. This method is the best way to reset the configuration, because you can back up the settings using the Backup/Restore operation, which provides a means for restoring it after the configuration issues have been resolved.

1. Create a backup copy of the configuration using the Backup/Restore operation. See Backup/restore device configurations on page 90 for more information.
2. From the Main menu, click **Administration > Factory Default Settings**. The Factory Default Settings page appears.
3. Check the **Keep network setting**s check box to keep the current network settings such as the IP address and host key settings. In addition, any files that were loaded into the device through the File Management page such as custom-interface files and applet files are retained. See File management on page 89 for information on loading and deleting files.
4. Click **Restore.**

Using the boot command

The **boot action=factory** command clears all current configuration settings, except the IP address settings, host key settings, and password for the administrative/root user; restores the settings to the factory defaults; then reboots the device. If a Digi device has custom factory default settings, the settings will revert to those custom defaults instead.

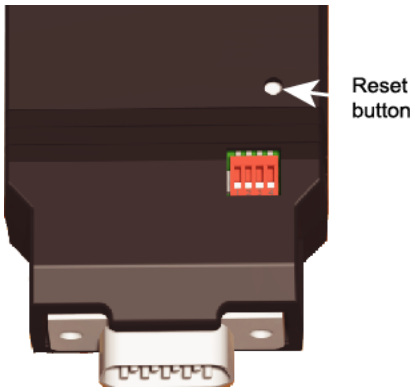
```
#> boot action=factory
```

There are several other options for using the **boot** command to load configuration settings. See the **boot** command description in the *Digi Connect Family Command Reference*.

Using the Reset button

If you cannot access the Digi device from the web interface, you can restore the configuration to factory defaults by using the Reset button.This reset clears all configuration settings.

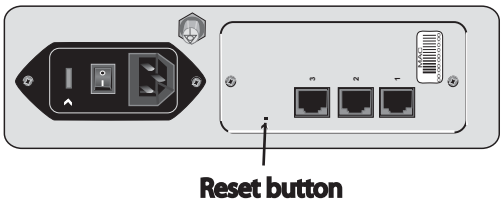
1. Power off the Digi device.
2. Locate the Reset button or pin on your device.Here is the reset button for a Digi Connect SP unit.



For Digi Connect EM or Digi Connect Wi-EM, the Reset button is located between P3 and CR1, as shown:

Digi Connect ME and Digi Connect Wi-ME do not have a reset button. Instead, pin 20 (the /init pin) is shorted to ground.

For Digi Connect ES, the reset switch is on the side panel.



3. Hold the **Reset** button down gently with a non-conductive, small diameter tool (such as wood or plastic) with a blunt end (NOT SHARP or the button could be damaged). Power on the device while holding the Reset button down. On some models, after a few seconds you may see the Status LED blink a 1-1-1 pattern once.

   For Digi Connect ME and Digi Connect Wi-ME, short pin 20 (the /init pin) to ground during boot up to restore the module to factory defaults. Note that shorting pin 14 simply reboots the unit but does not restore the configuration.

4. After 30 seconds, release the Reset button. At this point, on some models, the Status LED will blink a 1-5-1 pattern. Wait for the device to boot up. At this time, the configuration is returned to factory defaults. Now, if desired, power off the device, though this is not necessary.

Note Powering off the device *before* releasing the Reset button guarantees the configuration will NOT be reverted. Powering off the device *just after* releasing the Reset button will result in an unknown configuration, possibly having some or all settings reverted to defaults.

Display system information

System information displays the model, MAC address, firmware version, boot version, and POST version of the Digi device. It also displays memory available: total, used, and free, and tracks CPU percent utilization and the uptime.

From the web interface menu, select **Administration > System Information**. Select **General**, **GPIO**, **Serial, Network,** or **Diagnostics** for the appropriate information. For descriptions of the information displayed on these screens, see System information on page 79.

Activate Find Me LED

For Digi Connect ES products, use the Find Me LED to aid in finding a specific Digi device server among a group of devices. The locator LED is shown on page 113.

- **Activate**: Clicking this button causes the Find Me locator LED to blink.
- **Stop**: Clicking this button causes the Find Me locator LED to stop blinking.

Reboot the Digi device

Changes to some device settings require saving the changes and rebooting the Digi device. To reboot a Digi device:

1. From the web interface menu, select **Administration > Reboot**.
2. On the **Reboot** page, click the **Reboot** button. Wait approximately 1 minute for the reboot to complete.

Enable/disable access to network services

As needed, enable and disable access to various network services, such as ADDP, RealPort, SNMP, and telnet. For example, for performance and security reasons, it may be desirable to disable access to all network services not necessary for running or interfacing with the Digi device. In the web interface, enabling and disabling network services is done on the **Network Services** settings page for a Digi device. See Network services settings on page 38.

Restore device configuration to factory defaults

There are two ways to restore the device configuration to the factory default settings:

- Reset the configuration from a web browser, which clears all current device configuration settings except the IP address settings and administrator password. This is the best way to reset the configuration as it allows for backing up the settings, providing a means for restoring the settings after any configuration issues are resolved. See Using the Administration > Factory Defaults page on the web interface on page 91 for more information.
- Reset the configuration using the reset button on the Digi device. Use this method if the device cannot be accessed from a web browser. The location of the reset button may vary. See Using the Reset button on page 91.

Settings cleared and retained during factory reset

Restoring the Digi device to its factory default settings clears all current settings *except* the IP address settings and the administrator password. Any files such as custom-interface files and applet files that were loaded through the web interface's **File Management** page are retained. See File management on page 89 for information on loading and deleting files.

Restore the configuration from a web browser

1. From the main menu, click **Administration > Factory Default Settings**.

2. Click **Restore.**

Administration from the command-line interface

You can perform administrative tasks for Digi devices from the command line. Here are several device-administration tasks and the commands used to perform them. See the *Digi Connect Family Command Reference* for more complete command descriptions. For descriptions of these commands, see the *Digi Connect Family Command Reference*.

Administrative task	Command
Backup/restore a configuration from a TFTP server on the network	backup
Update firmware	boot Telnet to the Digi device's command line interface using a telnet application or hyperterm. If security is enabled for the Digi device, a login prompt appears. The default user name is **root** and the default password is **dbps.** If these defaults do not work, contact the system administrator who set up the device. Issue the command: #> boot load=*tftp-server-ip*:*filename* where ***tftp-server-ip*** is the IP address of the TFTP server that contains the firmware, and ***filename*** is the name of the file to upload.
Reset configuration to factory defaults	**revert** or **boot action=factory**
Display system information and statistics	info
Reboot the device	boot
Enable/disable network services	**set service**

Latency Tuning

What is Latency?

This section discusses latency and a recommended process for defining and addressing latency issues in your network and application.

Latency is the amount of time a packet takes to travel from source to destination. Together, latency and bandwidth define the speed and capacity of a network. Several factors influence latency, including the traffic pattern and traffic generated by an application, the physical wiring for the network, using various TCP/IP timers, and the amount of additional traffic on the network besides that generated by the application.

Recommended Process for Deterministic Ethernet/IP Performance

Following is a process recommended to achieve deterministic Ethernet/IP networking behavior. It uses Digi commercial off-the-shelf firmware and hardware, and not any specialized products that specifically reduce latency. By following this process, you can define and address latency issues at multiple levels in your network and application. The process involves these steps:

1. Determine the characteristics of your application, in terms of traffic pattern and amount of traffic generated.
2. Determine the latency budget and the type of latency in which you are interested.
3. Depending on the results produced in steps 1 and 2 and if applicable, optimize the physical layer.
4. Depending on the results produced in steps 1, 2, and 3 and if applicable, optimize the network and transport layer.
5. Depending on the results produced in steps 1, 2, 3, and 4 and if applicable, optimize the application layer.

Best-case scenario for achieving deterministic Ethernet/IP networking behavior

The best-case scenario for achieving deterministic Ethernet/IP networking behavior with Digi firmware and hardware is a unidirectional master-slave application running over an isolated Ethernet network that is built around Ethernet switches instead of Ethernet hubs. In other words, a network that eliminates unnecessary traffic and minimizes Ethernet collisions.

Step 1: Determine the characteristics of your application

Consider your application in terms of traffic pattern and amount of traffic generated.

- What is the main purpose of the application, and the primary activities?
- What is the traffic pattern: Is it peer-to-peer or master-slave application?
- Amount of traffic generated (*x* bytes every *y* minutes): How much data is being transmitted from and received by the application, and over what amount of time? For example, 200 bytes of data sent over 500 milliseconds.

Step 2: Determine the latency budget and type of latency

Next, determine the latency budget and type of latency in which you are interested. Identifying the latency budget for your application involves defining what latency means for your network and the application running on it. Consider

how much latency is acceptable and whether the latency is one-way or round-trip. This latency budget influences how much optimization you may need to perform at the physical, data link/network, and application layers.

Step 3: Optimize the physical layer

Depending on the results produced in steps 1 and 2, optimize the physical layer; that is, address the physical-layer characteristics that can affect latency. Optimizing the physical layer may include, but is not limited to, these recommendations:

- Use Ethernet switches instead of Ethernet hubs to minimize unnecessary traffic and minimize collisions.
- Use industrial-strength cabling and sure the wiring is sound. Bad wiring can result in increased collisions.
- Eliminate impedance mismatches.
- Avoid running communications cabling on the same tracks with power cabling or other cabling exhibiting fast voltage swings
- Use a smaller less noise-induced error-prone Ethernet or data rate. Lower Ethernet speeds have higher voltages, where background noise is less relevant and has less impact on latency. Voltages associated with 10, 100, and 1000 mbps Ethernet speeds are:
  - 10 mbps: 2.3V (CAT5)
  - 100 mbps: 0.8V (CAT5)
  - 1000 mbps: 0.5V (CAT5E/CAT6)
- Ground to earth all your networking equipment, including the Digi device.
- Use only networking equipment that is certified or known to operate well within the required ranges for vibrations, shock, operating temperature, relative humidity, etc.

Step 4: Optimize the network and transport layers

Depending on the results produced in steps 1, 2, and 3, optimize the network and transport layers. Optimizing the network and transport layers, may include, but is not limited to, these recommendations:

- Isolate any unnecessary TCP/IP traffic from the network.
- Choose smaller packets to reduce transit times through intermediate networking devices, as most of these devices are store-and-forward.
- Increase the TCP/IP responsiveness to incoming/outgoing traffic by choosing appropriate values for various TCP/IP timers, such as the retransmission timer, the gratuitous ARP timer, the delayed acknowledgment timer, or by using the **nodelay** option in conjunction with TCP sockets.
- Avoid using time-consuming encryption facilities.

Command options for optimizing network and transport layers

A major contributor to latency for the network and transport layers is unnecessary retransmissions of data. The command-line interface has several command options to help you reduce these unnecessary retransmissions. These

options are available through the command-line interface only, not the Web user interface. See the *Digi Connect Family Command Reference* for command descriptions.

Command	Option	Description
set network	garp=30-3600 (seconds)	Frequency of Gratuitous ARP (GARP) announcements, which are a broadcast announcement to the network of a device's MAC address and the IP address being used for it. These allow the network to update its ARP cache tables without performing an ARP request on the network. Gratuitous ARP announcements can affect latency in a limited way, because some systems stall or dispose of data that is transmitted during an ARP cache refresh. If this happens, setting the Gratuitous ARP frequency to be more often than the problem system's time-to-live variable can cause it to refresh the cache without needing to perform a request.
set network	rto_min=30-1000	The TCP maximum retransmission time out (RTO) in seconds. TCP uses progressively larger retransmit values, starting at a minimum value calculated from a sliding window of ACK response round-trip times bounded at the bottom by **rto_min.** Essentially, **rto_min** is not necessarily the timeout that will be used as the starting retransmit timeout, but the smallest such value that could be used. This affects latency, because lowering **rto_min** can ensures that retransmits, if they occur, take place in less time. By occurring sooner, the network can recover lost data in less time at the expense of possibly retransmitting data still in-flight or successfully received by the other side, but unacknowledged due to a "delayed ACK" mechanism or something similar.
set service	range=*range*	The index number associated with the service.
set service	nodelay={on|off}	Allows unacknowledged or smaller-than-maximum-segment-sized data to be sent for the specified range of network services. **nodelay=off** disables Nagle's algorithm, which is on by default, for some TCP services. Nagle's algorithm reduces the number of small packets sent. It establishes not sending outgoing data when there is unacknowledged sent data, or is less-than-maximum segment size (typically around 1500 bytes for Ethernet) worth of data to be sent. While Nagle's algorithm allows efficient data transmission, there are times where it is desirable to disable it.
set service	delayed_ack=0-1000	Time, in milliseconds, to delay sending ACK packets in response to received data for the specified range of network services. Default is 200 milliseconds. Setting this option to 0 (zero) sends an ACK packet back acknowledge the received data immediately. Setting this option to any other value than 0 means that the ACK packet will be sent after the specified time. If the network services generate new data during that time, the ACK packet is sent along with the data packet. You can use this setting to avoid congestion and reduce network traffic, However, do not change this option from its default setting unless you have a solid understanding of network services and data transmission, or have been instructed to the change.

Considerations for using latency-related command options

There are several considerations for using these latency-related command options:

- Changing the options from their defaults may violate RFCs.

- Decrementing the values for these options increases the amount of network activity, for example, there will be increased retransmissions.
- For a peer-to-peer application, you need to consider both sides of the connection and how options are set. For example, if the setting for the **rto_min** option for the Digi device is set to a value that is less than the setting for the **delayed_ack** option for the other side of the connection, then there will be a forced retransmission of every packet of data. For a master-slave application, this consideration does not apply.

Step 5: Optimize the application layer

Optimizing the application layer may include, but is not limited to, these recommendations:

- Avoid having more than one application/network node generating time-sensitive traffic in the network Have one traffic generator in a master-slave setup on the network.
- Avoid running other (management) applications, such as email, image or mp3 downloading while time-sensitive traffic is running.
- Verify the application itself has timers that cause retransmissions of data.
- Use firewalls.

Specifications and certifications

This chapter provides hardware specifications, additional feature detail, and regulatory statements and certifications for Digi devices.

For more detailed hardware specifications, see the *Hardware Reference* and datasheet for your Digi Connect product.

Hardware specifications

Following are hardware specifications for all products in the Digi Connect Family.

See hardware references for some Connect Family product specifications

Several Digi Connect products have *Hardware Reference Manuals*, which include hardware specifications. The specifications listed here are for products that do not have an accompanying *Hardware Reference Manual*.

Digi Connect ES specifications

Specification		Value
Environmental	Ambient temperature	0 to 55 C (32 to 130 F)
	Relative humidity	Relative humidity not to exceed 95% non-condensing over the temperature range of from 4C to 45C. Above 45C, constant absolute humidity shall be maintained.
	Storage and transport temperature	30 to 85 C (-122 to 185 F)
	Altitude	2000 meters (6560 feet)
	Serial Port Protection (ESD)	Serial Port Protection (ESD): +15 kV human body model
Power requirements	External	100-240V
	Input frequency	50-60 Hz
	Input current protection	1.0 A / 250 V(Time Lag) rated fuse
	UL certified	Yes
	Surge protection	• 4 kV burst (EFT) per EN61000-4-4 • 4 kV isolation input to output • 2 kV surge per EN61000-4-5

Specification		Value
Dimensions	Length	23.5 cm (9.3 in)
	Width	26.9 cm (10.6 in)
	Depth	4.2 cm (2.1 in)
	Weight	1.36 kg (3.00 lb)

RJ-45 Pinout

Pin assignments for the RJ-45 connector on the ConnectPort ES are as follows:

Pin Number	EIA-232 Signal
01	RI
02	DSR
03	RTS
04	CGND
05	TxD
06	RxD
07	SGND
08	CTS
09	DTR
10	DCD

ConnectPort TS 8 specifications

Specification		Value
Environmental	Ambient temperature	0 to 60C3 (2 to 140F)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6560 feet)
	Serial port protection (ESD)	+15 kV human body model

Specification		Value
Power requirements	DC power range	9-30V
	Typical power consumption DC Current @ 120 Vdc (mA)	6W (500mA @ 12Vdc)
	Maximum power consumption (watts)	12W (1A @ 12Vdc)
	Recommended power supply input rating (watts)	17W (120 VAC @ .14A) External power supply provided with product purchase
		For units that have a 48VDC DC supply: 13W (48VDC @ .25A)
	UL certified	Yes
Dimensions	Length	10.5 cm (4.15 in)
	Width	19.6 cm (7.7 in)
	Depth	3.3 cm (1.3 in)
	Weight	1.86 kg (4.1 lb)
USB interface	Input	500mA max

ConnectPort TS 16 specifications

Specification		Value
Environmental	Ambient temperature	0 to 55C (32 to 131F)
	Relative humidity	5 to 95% (non-condensing)
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6500 feet)
	Serial Port Protection (ESD)	+15 kV human body model
Power requirements	Input power range	AC: 100-240 VAC, 50/60 Hz, 0.4A DC: 36-72VDC .700A (MAX)
	Typical power consumption	8 W
	Maximum power consumption	15 W
	UL certified	Yes

Specification		Value
Dimensions	Length	43.18 cm (17 in)
	Width	17.65 cm (6.95 in)
	Depth	4.1 cm (1.62 in)
	Weight	2.3 kg (5 lb)
USB interface	Input	500mA max

ConnectPort TS 4x4 and ConnectPort TS 4x2 specifications

Specification		Value
Environmental	Operating temperature	0 to 60C3 (2 to 140F)
	Storage and transport temperature	-40 C to 85 C (-40F to 185F)
	Relative humidity	5 to 95% (non-condensing)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
	Altitude	2000 meters (6500 feet)
	Serial Port Protection (ESD)	+8 kV air discharge and +4 kV direct discharge per EN61000-4-2
Power requirements	Power input	9-30VDC
	Power consumption	Idle: 3.1 W Max: 11.5 W
	Surge protection (with included power supply)	4 kV burst (EFT) per EN61000-4-4 2 kV surge per EN61000-4-5
Dimensions	Width	10.40 cm (4.11 in)
	Height	3.30 cm (1.30 in)
	Length	19.7 cm (7.75 in)
	Weight	0.64 kg (1.4 lb)

Wireless networking features

The following table shows key wireless-networking features that you can configure in Wi-Fi-enabled Digi products. For more details and up-to-date information on support of these features, see the readme file for your Digi product.

Wireless feature	Specification
Standard	802.11bg
Frequency	2.4 GHz
Data Rates	Up to 54 Mbps with automatic rate fallback
Modulation	DBPSK (1 Mbps), DQPSK (2 Mbps), CCK (11, 5.5 Mbps), BPSK (6, 9 Mbps), QPSK (12,18 Mbps), 16-QAM (24, 36 Mbps), 64-QAM (48, 54 Mbps)
Country Code	Specifies the country where the product resides.
Network Mode	• Open • Infrastructure Mode • Ad-Hoc Mode
Channel	Can use automatic channel search-and-select or a user-configurable channel number.
Service Set Identifier (SSID)	A user-configurable SSID string or auto-connect option.
Wireless Security	• Wi-Fi Protected Access (WPA/WPA2/802.11i) • Wired Equivalent Privacy (WEP)
Authentication Options	• Open • Shared • Wi-Fi Protected Access (WPA2—/802.11i) • WPA/WPA2 with pre-shared key (WPA-PSK)
802.1x (WPA2—/802.11i) Authentication	• LEAP (WEP), PEAP, TTLS, TLS, EAP-FAST • GTC, MD5, OTP, PAP, CHAP, MSCHAP, MSCHAPv2, TTLS-MSCHAPv2
Encryption	• Temporal Key Integrity Protocol (TKIP) • Counter mode CBC MAC Protocol (CCMP) • Wired Equivalent Privacy (WEP) • Use of encryption can be disabled.
Network Key	A shared key (ASCII or Hexadecimal) used for WEP or WPA-PSK.
Username	Specify the user name to use for 802.1x -based authentication (WPA).
Password	Specify the password to use for 802.1x based authentication (WPA).

Wireless feature	Specification
Ekahau Client™	Provides integrated support for Ekahau's Wi-Fi device-location solution. Ekahau offers a complete access point vendor-independent real-time location system for wireless LAN devices that is capable of pinpointing wireless LAN devices such as the Digi Connect products, laptops, PDAs, or other intelligent Wi-Fi enabled devices. The solution provides floor-, room- and door-level accuracy of up to 3.5 feet (1 m). The patented Ekahau positioning technology is based on simple signal-strength calibration maps, and enables customers to fully leverage an existing wireless LAN infrastructure without any need for proprietary hardware components.
Wireless Networking Status Features	The following status information can be displayed for Wireless Digi devices. For more detailed descriptions, see WiFi LAN statistics on page 85.
Connection Status	The status of the wireless network connection.
Network Mode	The network mode currently in use: • Infrastructure Mode • Ad-Hoc Mode
Data Transfer Rate	The data transfer rate of the current connection.
Channel	The wireless network channel currently in use.
SSID	The selected SSID of the wireless network.
Wireless Security: Wi-Fi Protected Access (WPA/ WPA2/802.11i), Wired Equivalent Privacy (WEP) security and encryption	The status of the WEP/WPA/WPA2 security features, including the Authentication Method currently in use and whether authentication is enabled or disabled
Signal Strength	A statistic that indicates the strength of the radio signal between 0 and 100 percent.

Regulatory information and certifications

RF exposure statement

Digi Connect Wi-SP, Digi Connect Wi-EM, and Digi Connect Wi-ME

The Digi Connect Family wireless devices Digi Connect Wi-SP, Digi Connect Wi-EM, and Digi Connect Wi-ME comply with the RF exposure limits for humans as called out in RSS-102.

These devices are exempt from RF evaluation based on its operating frequency of 2400 MHz, and effective radiated power of 100 milliwatts. This would be less than the 3 watt requirement for a mobile device (>20 cm separation) operating at 2400 MHz.

FCC certifications and regulatory information (USA only)

The FCC certifications in this section are for Digi Connect ES and ConnectPort TS products. For certifications for other Digi Connect devices, see the device's *Hardware Reference*.

FCC Part 15 Class A

These devices comply with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) These devices may not cause harmful interference, and (2) These devices must accept any interference received, including interference that may cause harmful operation.

Radio Frequency Interference (RFI) (FCC 15.105)

This equipment has been tested and found to comply with the limits for Class A digital devices pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Labeling Requirements (FCC 15.19)

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Modifications (FCC 15.21)

Changes or modifications to this equipment not expressly approved by Digi may void the user's authority to operate this equipment.

Cables (FCC 15.27)

Shielded cables *must* be used to remain within the Class A limitations.

Industry Canada (IC) certifications

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

International EMC (Electromagnetic Emissions/Immunity/Safety) standards

These products comply with the requirements of following Electromagnetic Emissions/Immunity/Safety standards. There are no user-serviceable parts inside the product. Contact your Digi representative for repair information.

Product	Emissions	Immunity	Safety
Digi Connect ES	• EN60601-1-2:2001 • EN55011:1998 • EN55022:1998 • AS/NZS CISPR 22: 2002 • ICES-003, Issue 3:1997 • FCC Part 15 Subpart B Class A	EN55024:1998	• UL60950-1 • CAN/CSA C22.2 No. 60950-1-3 • IE60950-1 • IEC60601-1
ConnectPort TS 8 ConnectPort TS 8 MEI	• EN55022 • AS/NZS CISPR 22: 2004 • ICES-003, Issue 3:1997 • FCC Part 15 Subpart B Class A	EN55024	• UL60950-1 • IEC60950-1 • CAN/CSA C22.2 No 60950-1-3
ConnectPort TS 16 ConnectPort TS 16 MEI	• EN55022:2006 • AS/NZS CISPR 22:2006 • ICES-003 Iss. 4:2004 • FCC P15 subpart B Class A	EN55024:1998 +A1:2001+A2:2003	• EN/IEC60950-1 • UL 60950-1 • CUL 60950-1-03
ConnectPort TS 4x4 ConnectPort TS 4x2	• CE • FCC Part 15 subpart B, Class A • AS/NZS CISPR 22 • EN55022, Class A	EN55024	• UL 60950-1 • CSA 22.2 No. 60950 • EN60950

Troubleshooting

This chapter provides information on resources and processes available for troubleshooting your Digi device.

Troubleshooting Resources

There are several resources available to you for support of your Digi product or resolving configuration difficulties on Digi Support site, www.digi.com/support/eservice
Try these troubleshooting steps to eliminate your problem. After working through these steps and your problem is not solved, try the resources listed below.

1. Visit Digi's Support knowledge bases at www.digi.com/support/kbase to look for articles related to your situation.
2. Visit our support forums at www.digi.com/support/forum/ and search for possible posts from other users with similar situations.
3. If the knowledge base or support forums do not have the information you need, fill out an Online Support Request via: www.digi.com/support/eservice/
   You will need to create a user account if one is not already set up.

System status LEDs

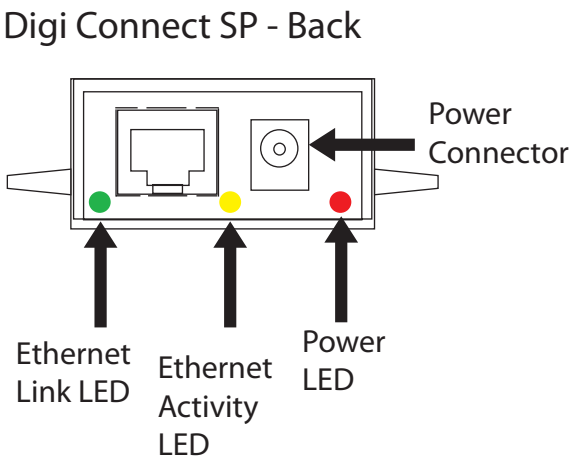
Digi devices have several LEDs that indicate system status, link integrity, and link activity.

Digi Connect Family LEDs

Digi Connect LEDs provide information on port activity, diagnostics, and Ethernet activity.

Digi Connect SP

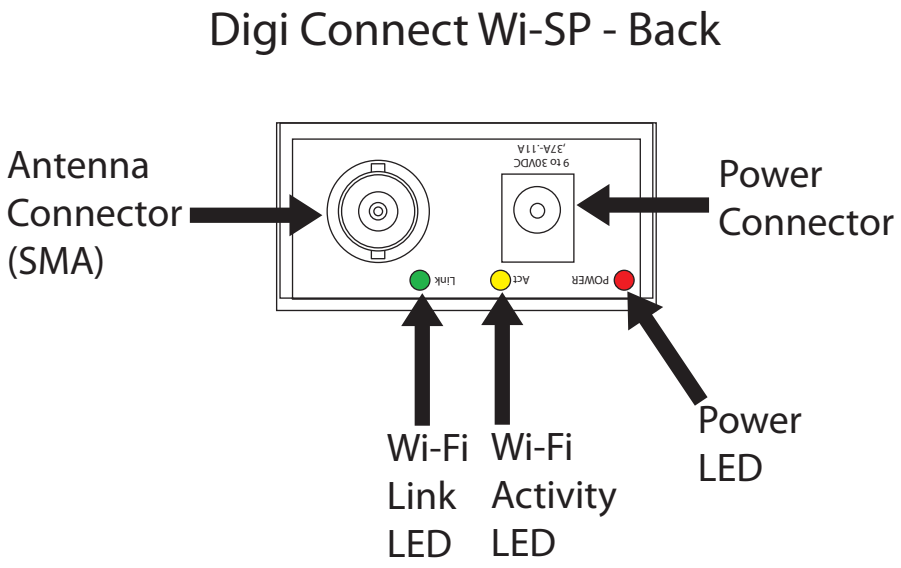
Digi Connect SP has three LEDs: Ethernet Link and Ethernet Activity, which are connected directly to the hardware; and the Power LED, which is software programmable.



LED/button	Color and Light Pattern	Description
Ethernet Link LED	Off	Ethernet link is not powered or down.
	Solid green	Ethernet link is up.
Ethernet Activity LED	Blinking yellow	Ethernet traffic is on the link.
Power LED	Red (labeled PWR)	This LED is software programmable. The default is that this LED indicates power (and is therefore always on).

Digi Connect Wi-SP

Digi Connect Wi-SP has three LEDs: Wi-Fi Link and Wi-Fi Activity, which are connected directly to the hardware; and the Power LED, which is software programmable.

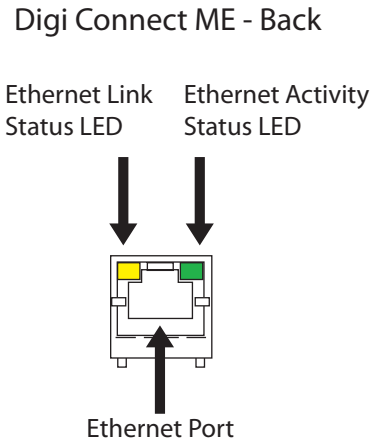


LED/button	Color and Light Pattern	Description
Wi-Fi Link Status LED	Solid green	Unit is associated with an access point.
	Green, blinking slowly	Unit is in ad hoc mode.
	Green, blinking quickly	Unit is scanning for a network
Wi-Fi Activity Status LED	Solid yellow	Bad initialization
	Off	The Wi-Fi link is idle.
	Blinking yellow	Traffic is on the Wi-Fi link.
Power LED	Red (labeled PWR)	This LED is software-programmable. The default is that this LED indicates power (and is therefore always on).

Digi Connect ME

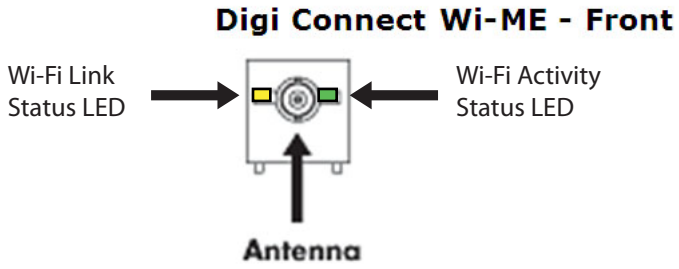
The Digi Connect ME module has two LEDs that are located near the upper corners of the Ethernet port (see the following figure).

Note The LEDs are the same for a module with or without a JTAG connector.



LED/button	Color and Light Pattern	Description
Ethernet Link LED	Solid yellow	Ethernet link is up.
Ethernet Activity LED	Blinking green	Ethernet traffic is on the link.

Digi Connect Wi-ME

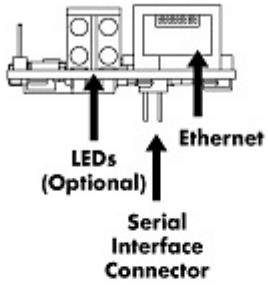


LED/button	Color and Light Pattern	Description
Wi-Fi Link Status LED	Solid yellow	Unit is associated with an access point.
	Yellow, blinking slowly	Unit is in ad hoc mode.
	Yellow, blinking quickly	Unit is scanning for a network.
Wi-Fi Activity Status LED	Off	The Wi-Fi link is idle.
	Blinking green	Wi-Fi traffic is on the link.

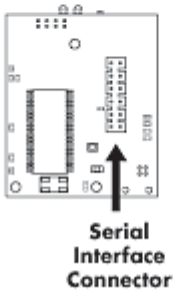
Digi Connect EM and Digi Connect Wi-EM

Digi Connect EM and Digi Connect Wi-EM modules provide two hardware options for LEDs, with or without on board LED array. The integration kit provides predefined LED behavior. With the development kit, your implementation determines some LED behavior. See the following table for more information.

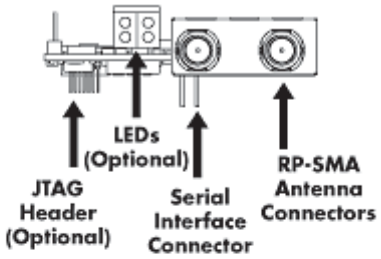
■ Digi Connect EM - Front



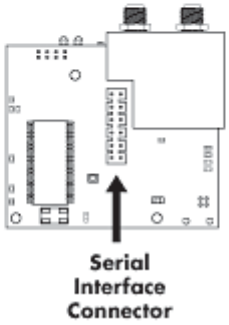
■ Digi Connect EM - Bottom



■ Digi Connect Wi-EM



■ Digi Connect Wi-EM - Bottom

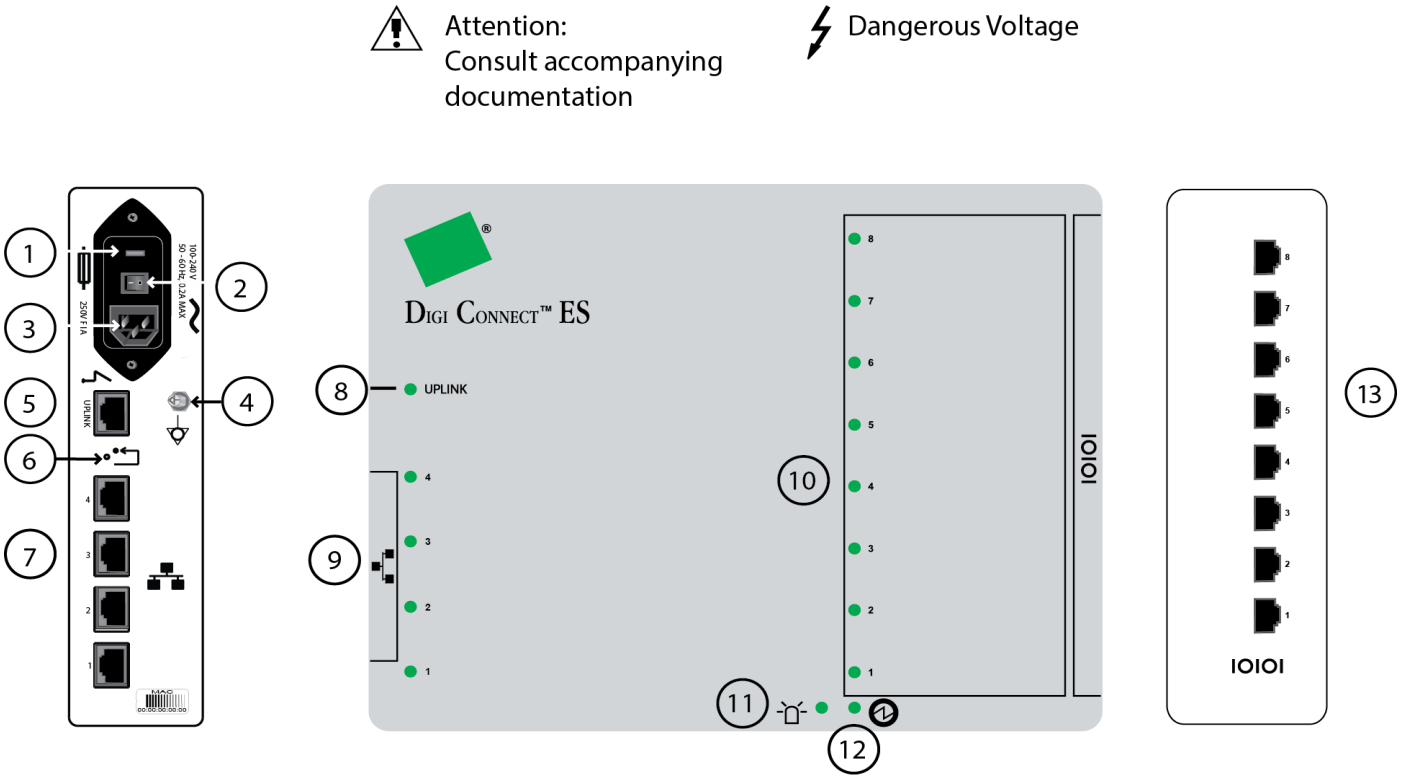


LED Behaviors				
LED	Pin Header EM	Integration Kit Digi Connect EM	Integration Kit Digi Connect Wi-EM	Development Kit
Top left (green)	1 (+) 3(-)	Serial port activity: Off - the serial channel is idle. Blinking - serial data is transmitted or received.		This LED is software programmable
Top right (green)	5 (+) 7 (-)	Network link status: Off - no link has been detected. On - a link has been detected.	Network link status: On - unit is associated with an access point. Blinking slowly - unit is in ad hoc mode. Blinking quickly - unit is scanning for a network.	Same as Integration Kit (Network link status)

LED Behaviors				
LED	Pin Header EM	Integration Kit Digi Connect EM	Integration Kit Digi Connect Wi-EM	Development Kit
Bottom left (red)	2 (+) 4 (-)	Diagnostics: Blinking 1-1-1 - starting the operating system. Blinking 1-5-1 - configuration has been returned to factory defaults. **Note** If other blinking patterns occur, contact Digi Technical Support.		This LED is software programmable
Bottom right (yellow)	6 (+) 8 (-)	Blinking - network data is transmitted or received		This LED is software programmable

Digi Connect ES 4/8 SB and Digi Connect 4/8 SB with Switch

DigiConnect ES connectors, LEDs, and controls



1 - Fuse (250V F1A)

2 - On/Off switch (Off / On)

3 - Power input (100-240V 50 - 60 Hz, 0.2 A MAX)

4 - Grounding stud

5 - Ethernet Uplink port

6 - Reset switch

7 - Ethernet Switch ports

8 - Ethernet Uplink LED

9 - Ethernet Switch LEDs

10 - Serial LEDs

11 - Find Me/Locator LED

12 - Power LED

13 - Serial ports - 4 or 8

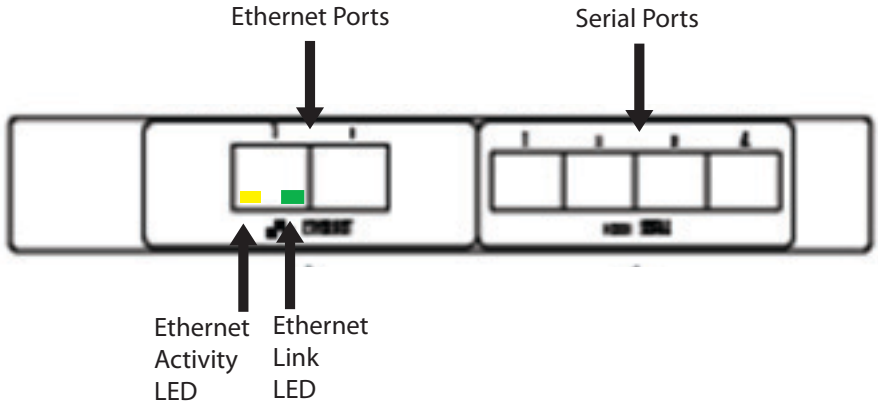
LED/button	Color and Light Pattern	Description
Ethernet Uplink LED	Solid green	Ethernet Uplink connection is up but no traffic is on the line.
	Blinking green	Traffic is on the Ethernet Uplink connection.
	Off	Ethernet Uplink connection is disconnected.

LED/button	Color and Light Pattern	Description
Ethernet Switch LEDs	Solid green	Ethernet Switch connection is up but there is no activity on the line.
	Blinking green	Ethernet activity is on the Ethernet Switch connection
	Off	Ethernet Switch connection is not in use.
Serial LED	Solid green	Serial connection is up but no traffic is on the line.
	Blinking green	Serial connection is up and traffic is on the serial port.
	Off	Serial connection is not in use
Find Me/Locator LED	Blinking amber	Use the LED as an aid in finding a specific device among a group of devices. You can turn LED on or off from the Digi device's command line and web interfaces. From the command line, issue the **findme blink={on|off}** command. From the web interface, go to **Administration > Activate Find Me LED**. Once the LED is enabled, the menu item changes to **Stop Find Me LED** which you can use to turn off the LED.
	Off	Find Me LED is deactivated.
Power	Green	Power is on.
	Off	Power is off.

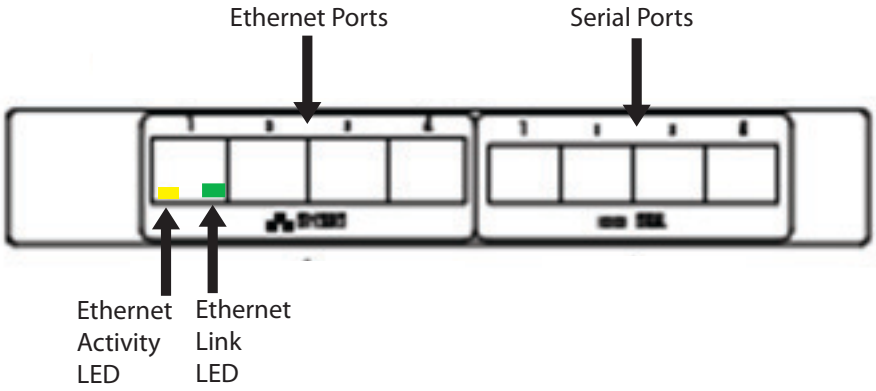
ConnectPort TS Family Products

ConnectPort TS 4x4

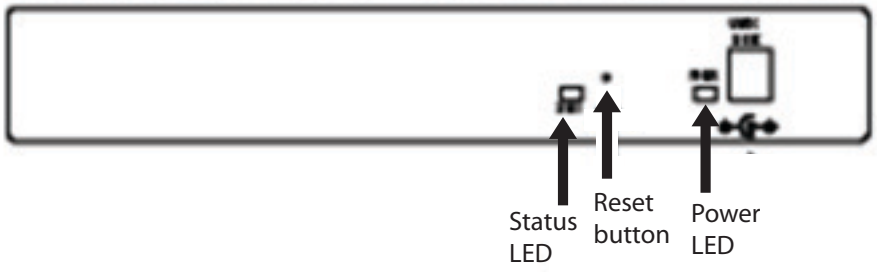
ConnectPort TS 4x2 - Back



ConnectPort TS 4x4 - Back



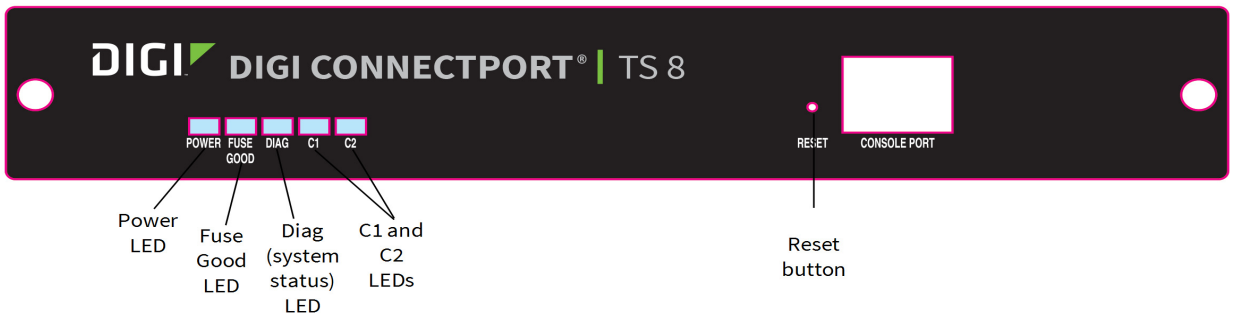
ConnectPort TS 4x4 and ConnectPort TS 4x2 - Front



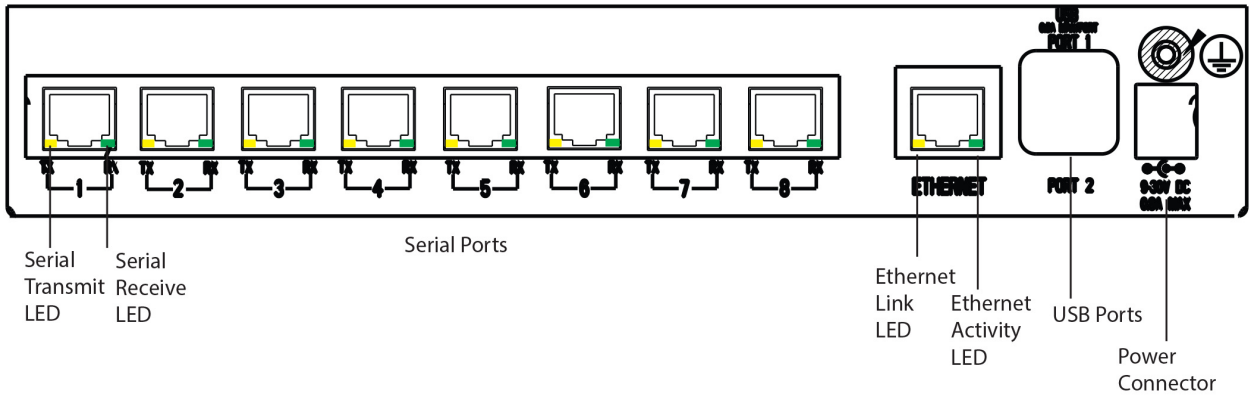
LED/button	Color and Light Pattern	Description
Power LED	Solid Green	Power is applied.
Fuse Good LED	Solid Green	Power is applied and the fuse is good. If this LED is not illuminated when power is applied, the fuse is blown and needs to be replaced.
Diag LED	Amber	Blinks during product initialization and factory reset, using the light patterns below. This LED should never blink during normal operation. If it blinks constantly, contact Digi Technical Support.
	1-1-1 blinking amber	Firmware is initializing.
	1-5-1 blinking amber	Device configuration has been restored to its factory defaults.
	Other blinking amber	Contact Digi Technical Support.
	Solid amber	Device is powered on and ready for operation.
C1 & C2 LEDs	Green	These LEDs are provided for use by custom Linux applications running on the unit.
Reset button	N/A	Performs equivalent of a power-cycle.
Serial TX	Yellow	On when data is being transmitted out of a serial port.
Serial RX	Green	On when data is being received on a serial port.
Ethernet Link LED	Solid green	Ethernet link is up. Will light solid green when an active LAN connection is plugged into the Ethernet port.
Ethernet Activity LED	Blinking yellow	Blinks when active traffic is on the LAN connection.

ConnectPort TS 8 and ConnectPort TS 8 MEI

ConnectPort TS 8 and ConnectPort TS 8 MEI - Serial Port Side

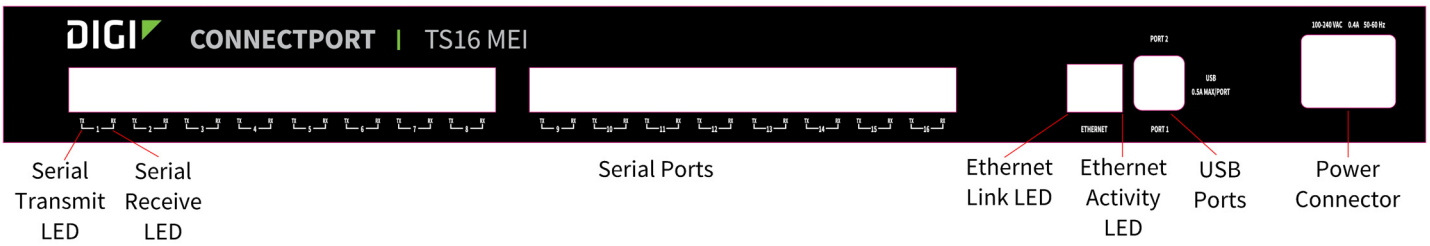


ConnectPort TS 8 and ConnectPort TS 8 MEI - Back Panel

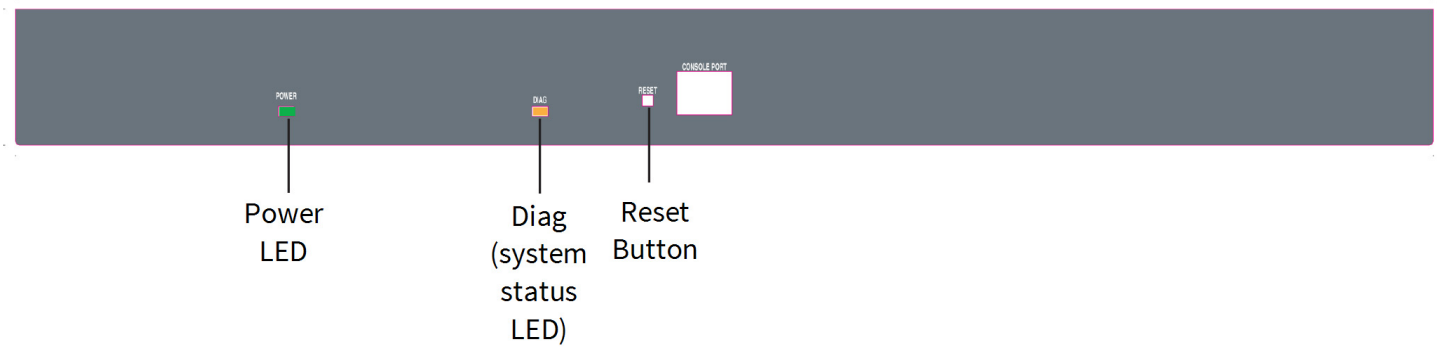


ConnectPort TS 16 and ConnectPort TS 16 MEI

ConnectPort TS 16 and ConnectPort TS 16 MEI - Serial Port Side



ConnectPort TS 16 and ConnectPort TS 16 MEI -



LED/button	Color and Light Pattern	Description
Power LED	Solid Green	Power is applied.

LED/button	Color and Light Pattern	Description
Diag LED	Amber	Blinks during product initialization and factory reset, using the light patterns below. This LED should never blink during normal operation. If it blinks constantly, contact Digi Technical Support.
	1-1-1 blinking amber	Firmware is initializing.
	1-5-1 blinking amber	Device configuration has been restored to its factory defaults.
	Other blinking amber	Contact Digi Technical Support.
	Solid amber	Device is powered on and ready for operation.
C1 and C2 LEDs	Green	You can use these LEDs with custom applications running on the unit.
Reset button	N/A	Performs equivalent of a power-cycle.
Serial TX	Yellow	On when data is being transmitted out of a serial port.
Serial RX	Green	On when data is being received on a serial port.
Ethernet Link LED	Solid green	Ethernet link is up. Will light solid green when an active LAN connection is plugged into the Ethernet port.
Ethernet Activity LED	Blinking yellow	Blinks when active traffic is on the LAN connection.

ConnectPort TS 16 48VDC

ConnectPort TS 16 48VDC - Side Panel