Digi Connect® Family and ConnectPort® TS Family

User Guide

Revision history—90000565

Revision	Date	Description
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.
T	February 2017	Updated and rebranded the documentation with minor updates. Added X.509 Certificate/Key Management information. Added international EMC standards information.
U	December 2019	Added information about the unique web interface password for each device. Added get started information for Connect SP.
V	February 2020	Added information about the USB ports on the ConnectPort TS 8/16.
W	June 2020	Added information about the RADIUS feature.

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 warranty information, go to the following website:

www.digi.com/howtobuy/terms

Send comments

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

Customer support

Digi Technical Support: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Contents

Overview: Configuration, monitoring, and administration

Using the Digi Connect and ConnectPort TS Family web interface

Configure the device using the web interface

Configure and manage the device using the Digi Connect and ConnectPort TS Family command line interface

Remote Manager monitoring capabilities

SNMP device monitoring capabilities

Latency tuning

Hardware

Specifications and certifications

Troubleshooting

About this guide

This guide describes how to install, provision, configure, monitor, and administer Digi Connect and ConnectPort TS Family. The guide covers the following products:

- 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
- Digi Connector 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

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.

Where to find information

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

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

For product support resources visit the following support pages:

- Digi Connect Family and ConnectPort TS Family serial servers

For 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, including:
  - Support forum
  - Knowledge Base
  - Datasheets/product briefs
  - Application/solution guides
  - Carrier-specific documents

Digi Connect and ConnectPort TS Family features

This section provides an overview of Digi Connect and ConnectPort TS Family features.

User interfaces

You can use the following user interfaces to configure, monitor, and administer Digi devices:

- Digi Remote Manager
- Web-based interface
- Command-line interface available via local serial port, telnet or SSH
- Remote Command Interface (RCI) over the serial port
- Simple Network Management Protocol (SNMP)

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)
- RealPort
- Encrypted RealPort
- HTTP/HTTPS
- Line Printer Daemon (LPD)
- Remote login (rlogin)
- Remote shell (rsh)
- SNMP
- Telnet
- Socket connectivity to the serial ports (for example, reverse telnet, reverse SSH, raw socket, and UDP)

You can enable or disable access to network services from the **Network Services Settings** page in the web interface. For more information, see Network Services Settings.

You can use the **set service** command to enable and disable network services from the command-line interface. See the *Digi Connect® Family Command Reference* on www.digi.com for a description of the **set service** command.

IP protocol support

All Digi Connect and ConnectPort TS Family 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)
- 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)

Serial data communication over TCP and UDP

Digi Connect and ConnectPort TS Family products support serial data communication over TCP and UDP. The key features include:

- Serial data communication over TCP can automatically perform the following functions:
  - Establish bi-directional 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 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 IP stack configuration parameters such as the subnet mask and default router, and provide other configuration information. For more details, see Assign an IP address using DHCP.

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 Assign an IP address using Auto-IP.

Simple Network Management Protocol (SNMP)

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

- Nodes—servers, workstations, routers, switches, and hubs—on an IP network.
- Network performance, such as finding and solving network problems, and planning for network growth.

Digi devices support SNMP Versions 1 and 2.

For a list of SNMP-related of supported Request for Comments (RFCs) and Management Information Bases (MIBs), see Supported RFCs and MIBs.

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

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) provides authentication and encryption for Digi Connect and ConnectPort TS Family products. For more information, see Security features in Digi devices.

Telnet

Digi Connect and ConnectPort TS Family 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 Network connections and data paths. You can enable or disable access to telnet network services.

Remote login (rlogin)

You can enable or disable access to rlogin service. When enabled, users can use rlogin to remotely sign in to systems.

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 provides web pages that you can use to configure the Digi Connect and ConnectPort TS Family product. You can secure these web pages by requiring a user login.

Internet Control Message Protocol (ICMP)

You can display ICMP statistics, including the number of:

- Messages received
- Bad messages received
- 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 is responsible for:

- Encapsulating the data packet
- Allowing the server to inform the dial-up client of its IP address (or client to request the IP address)
- Authenticating the exchange
- Negotiating multiple protocols
- Reassembling the data packet for network communication

Advanced Digi Discovery Protocol (ADDP)

The 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 Connect and ConnectPort TS Family products attached to a network by sending out a multicast packet. The Digi Connect and ConnectPort TS Family products respond to the multicast packet and identify themselves to the client sending the multicast.

ADDP communicates with the IP stack using UDP. The IP stack can receive multicast packets and transmit datagrams on a network.

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's RealPort software leverages the TCP/IP network infrastructure to provide a virtual connection to serial devices. The software is installed directly on the server and allows applications to talk to devices via a Digi device server or terminal server over a network.

RealPort software is a COM port redirector that allows multiple connections to multiple ports over a single TCP/IP connection. This means RealPort supports the maximum number of remote devices. The number is restricted only by the operating system and server processing power.

Other unique features include full hardware and software flow control, as well as tunable latency and throughput. With these, RealPort ensures optimum performance since data transfer is adjusted according to specific application requirements. It also provides connection recovery—after a network interruption RealPort automatically reconnects the device to the COM port without the application knowing there was a failure.

Encrypted RealPort

Digi Connect and ConnectPort TS Family 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 an SSL connection and encrypting the data using Advanced Encryption Standard (AES).

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 Connect and ConnectPort TS Family products to issue alarms, in the form of email messages or SNMP traps, when certain device events occur, including:

- Changes in GPIO signals (on embedded products)
- Data patterns detected in the data stream

Configuring Digi devices to issue alarms allows you to know when events occur. For more information on configuring alarms, see Alarms Configuration.

Modem emulation

Digi Connect and ConnectPort TS Family 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 Connect and ConnectPort TS Family products support, see the *Digi Connect® Family Command Reference*. See Select Port Profile for more information.

Security features in Digi devices

This section covers Digi Connect and ConnectPort TS Family security features.

Secure access and authentication

Security features include the following:

- Provide customized permissions controls to locally defined users. The local definitions apply irrespective of whether Radius is used for authentication.
- Unique default password for each device.
- Issue passwords for device users.
- Selectively enable/disable network services such as ADDP, RealPort, Encrypted RealPort, HTTP/HTTPS, LPD, remote login, remote shell, SNMP, and telnet.
- Control access to inbound ports.
- Control access to specific devices, IP addresses, or networks through IP filtering.
- Secure sites for configuration: HTML pages for configuration have appropriate security.
- Control user and user group access permissions. These permissions control user access to various features and the level of control they have over them (view settings or change settings).
- Enable secure remote login through Remote Authentication Dial-In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP).

Encryption

Encrypted RealPort offers encryption for the Ethernet connection between the COM/TTY port and the Digi Connect and ConnectPort TS Family product. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in an SSL connection and encrypting the data using the Advanced Encryption Standard (AES) security algorithm.

Encryption methods are as follows:

- Strong TLS V1.0-based encryption:
  - DES (64-bit)
  - 3DES (192-bit)
  - AES (128/192/256-bit)

- 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 include:

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

SNMP security

You can configure SNMP **set** commands to use SNMP read-only. Digi recommends changing the public and private community names to prevent unauthorized access to the Digi device.

Configuration management

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

- Copy configurations to and from a remote host
- Perform the following on the Digi device:
  - Update the firmware
  - Reset the factory settings
  - Manage the device files and memory
  - Reboot the device

For more information on these configuration-management tasks, see Administration.

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.

Network connections and data paths

Digi Connect and ConnectPort TS Family devices allow for several kinds of connections and paths for data flow between Digi Connect and ConnectPort TS Family devices 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 topics describe the effects of enabling features and selecting settings when configuring Digi Connect and ConnectPort TS Family devices.

Network services

A network service connection occurs when a remote entity initiates a connection to a Digi device. There are several categories of network services:

- Network services associated with specific ports
- Network services associated with serial ports in general
- Network services associated with the command-line interface

Network services associated with specific ports

The following list details network services associated with specific ports.

- **Reverse telnet**: A remote entity establishes a telnet connection to a Digi serial port. Data passes transparently between the telnet connection and a named serial port.
- **Reverse raw socket**: A remote entity establishes a raw TCP socket connection to a Digi serial port. Data passes transparently between the socket and a named serial port.
- **Reverse TLS socket**: A remote entity establishes an encrypted raw TCP socket connection to a Digi serial port. 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

The following list details 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 Connect and ConnectPort TS Family products 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.
- **DialServ**: Connecting a DialServ device to the serial port. DialServ simulates a public switched telephone network (PSTN) to a modem and forwards the data to the serial port. The Digi device sends and receives the data over an IP network.
- **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
- **TLS/SSL**: An TLS/SSL encrypted 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

The following list details network services associated with the command line interface (CLI).

- **Telnet**: Use telnet to directly access a Digi Connect and ConnectPort TS Family command-line interface.
- **Rlogin**: Perform a remote login (rlogin) to a Digi Connect and ConnectPort TS Family command-line interface.

Network/serial clients

A network/serial client connection occurs when a Digi Connect and ConnectPort TS Family product 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 client connections
- Modem emulation (pseudo-modem) client connections

Autoconnect behavior client connections

In client connections that involve autoconnect behaviors, a Digi Connect and ConnectPort TS Family product initiates a network connection based on timing, serial activity, or serial modem signals. Autoconnect-related client connections include:

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

Command-line interface (CLI)-based client connections

CLI-based client connections are available for use when you establish a session with the Digi Connect and ConnectPort TS Family product's CLI. CLI-based client connections include:

- **ssh**: Allows you to connect to a remote entity using the ssh protocol.
- **telnet**: Allows you to connect to a remote entity using the telnet protocol.
- **rlogin**: Allows you to connect to remote entity using the rlogin protocol (bash only).
- **scp**: Allows you to transfer files (bash only).
- **connect**: Begin communicating with a local serial port.

Note Additional communication methods include using a bash shell such as scp, tftp, nc, or using Python.

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* on www.digi.com for modem emulation AT commands.

Get started with Digi Connect and ConnectPort TS Family products

This section walks you through configuring an IP address and signing in to your Digi Connect and ConnectPort TS Family device.

Connect SP: Verify the components and connect the hardware

Note Perform this step only if you have a Connect SP device.

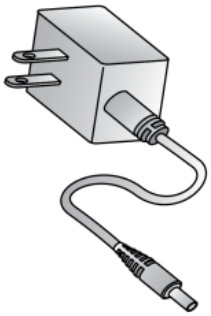
Verify the components

Verify that you have all included equipment. If any item is missing or damaged, contact your supplier.

Included equipment

Digi Connect SP

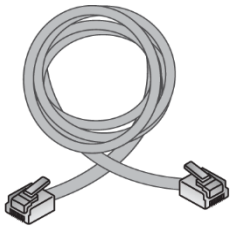
One of the devices shown above



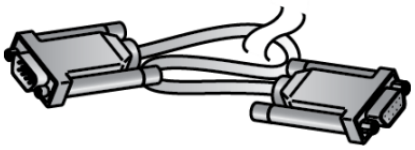
Power supply

Loopback plug

Required additional equipment



Ethernet cable



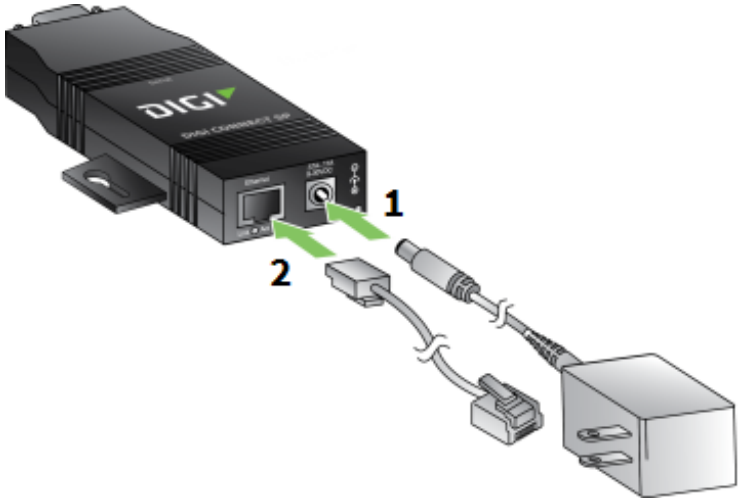
Null modem for serial configuration

Personal computer

Note A loose label sticker that includes the unique device password is included in the box. Retain this label sticker with your hardware records. This default password will be needed if the device is factory reset and you want to access the web UI on the device or to register the device with Digi Remote Manager®. If the device was already registered with Remote Manager at the time of the factory reset, you do not need the unique password to access the device in Remote Manager.

Connect the hardware

1. Connect the power supply to the power connector.
2. Connect the Ethernet cable to the Ethernet port.



Assign an IP address

This section describes how to assign an IP address to Digi Connect and ConnectPort TS Family products and manage that IP address.

Default IP address and DHCP settings

All products that have a cellular (WAN) interface ship with a static IP address for the Ethernet port of 192.168.1.1 and DHCP *server* enabled by default. Configure the Ethernet port on the laptop 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 the IP address assigned to the device, use the Device Discovery Utility for Windows. See Use Digi Device Discovery utility to sign in to the web interface for more information.

Configuring IP addresses

You can use any of the following methods to assign an IP address to a Digi device:

- 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 an Ethernet switch device, special considerations apply when assigning IP addresses. See IP Settings (for Connect ES 4/8 SB with Ethernet switch only) for more information.

Assign an IP address using Auto-IP

The standard Automatic Private IP Addressing (APIPA or Auto-IP) protocol 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 ADDP to find the Digi device and assign it a new IP address that is compatible with your network. When you plug in the device, Auto-IP automatically assigns the IP address. Auto-IP addresses are typically in the 169.254.x.x address range. See Use Digi Device Discovery utility to sign in to the web interface for instructions on using Digi Device Discovery.

Assign an IP address from the command-line interface

Use the **set network** command to configure an IP address from the command line. The **set network** command includes the following parameters:

- **ip=*device ip***: The IP address for the device.
- **gateway=*gateway***: The network gateway IP address.
- **garp=*seconds***: The frequency of Gratuitous ARP (GARP) announcements, in seconds, which are a broadcast announcement to the network of a device's MAC address and the IP address.
- **submask=*device submask***: The device subnet mask for the IPaddress.
- **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, you must change the DIP switches. See Set DIP switches on Digi Connect SP\Wi-SP for an illustration of the DIP switch settings.

Assign an IP address from the web interface

Normally, you assign IP addresses to Digi Connect and ConnectPort TS Family devices through DHCP. This procedure assumes that the Digi Connect and ConnectPort TS Family device already has an IP address and you simply want to change it.

To change the IP address from the web interface:

1. Open a web browser and type the current IP address of the Digi Connect and ConnectPort TS Family device in the address bar. A login dialog displays.

2. Enter the default user name and password for the device.
   - **User name**: The default user name is **root**.
   - **Password**: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.

   Note If this is the first time you have logged into the web interface, you are required to change the password.

3. Click **Network** to access the **Network Configuration** page.
4. On the **IP Settings** page, select **Use the following IP address**.
5. Type the IP address, subnet mask, and gateway settings.
6. Click **Apply** to save the configuration.

IP addresses and Remote Manager

From the Remote Manager 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.

Assign an IP address using DHCP

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

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.

The following 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.

To configure an IP address using DHCP:

1. Verify 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. DHCP assigns the IP address configured in step 2 automatically.

Test the IP address assignment

To verify the IP address 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
   ```

Sign in to the web interface

After you successfully assign an IP address to your device, you can sign in to the device's web interface using either of the following:

- Web browser
- Digi Device Discovery utility

Use a web browser to sign in to the web interface

To access the web interface for a Digi device using a browser:

1. Open a web browser and type the current IP address of the Digi Connect and ConnectPort TS Family device in the address bar. A login dialog displays.
2. Enter the default user name and password for the device.
   - **User name**: The default user name is **root**.
   - **Password**: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.

   Note If this is the first time you have logged into the web interface, you are required to change the password.

3. The **Home** page appears. See Home page for an overview of the Home page and other linked pages.

   Note If password authentication is enabled, the idle timeout automatically logs users out of the web interface after 5 minutes of inactivity.

Use Digi Device Discovery utility to sign in to the web interface

To discover the Digi device and open the web interface:

1. Go to your product's support page:
   - Digi ConnectPort X2
   - Digi ConnectPort X4
   - Digi Connect SP
2. Under **Product Support**, click the **Utilities** tab.

3. Under **Operating System Specific Utilities**, choose an operating system.
4. Under **Utilities** or **Operating System Specific Diagnostics, Utilities and MIBs**, 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**.
5. 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** > **All Programs** > **Digi** > **Digi Device Discovery** > **Digi Device Discovery**.
6. From the Digi Device Discovery utility, locate the Digi device in the list of devices, and choose one of the following options:
   - Double-click the Digi device to open the web interface.
   - Select the Digi device from the list and select **Open web interface** in the **Device Tasks** list.
7. A login dialog displays. Enter the default user name and password for the device.
   - **User name**: The default user name is **root**.
   - **Password**: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.

Note If this is the first time you have logged into the web interface, you are required to change the password.

Overview: Configuration, monitoring, and administration

This section provides an overview for configuring, monitoring, and administering Digi devices.

Configuration capabilities

Configuration options provide settings for the following features:

- **Network Configuration**: Specifies IP address settings, network service settings, and advanced network settings.
- **Serial Ports Configuration**: Specifies serial port characteristics for the device.
- **GPIO Pin Configuration (for Connect ME and Connect EM devices)**: Specifies how to use GPIO pins for the device.
- **Alarms**: Defines conditions that trigger alarms and notifications for alarms.
- **System Configuration**: Provides system-identifying information, such as a device description, device location, and contact information.
- **Security/Users**: Configures security features, such as enabling password authentication for device users.

Digi Device Discovery utility

The Digi Device Discovery utility:

- Locates Digi devices on a network
- Allows you to open the web interface for discovered devices
- Allows you to configure network settings and reboot the device

Download the Digi Device Discovery utility.

In addition to quickly locating devices, the utility also lists device information, such as the device address, firmware version, 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 Digi devices on the network. Digi devices that support ADDP reply to the UDP multicast with their configuration information. Even Digi devices that do not yet have an assigned IP address or are misconfigured for the subnet can reply to the UDP multicast packet and appear in the device discovery results.

Note Personal firewalls, Virtual Private Network (VPN) software, and certain network equipment can block device discovery. Firewalls 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.

See Use Digi Device Discovery utility to sign in to the web interface for instructions on using the utility to sign in to the Digi Connect and ConnectPort TS Family web interface.

Remote Manager interface

Digi Remote Manager 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. Remote Manager 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 Remote Manager:

- Devices must be registered in a Remote Manager account before you can access them.
- To minimize network traffic, Remote Manager 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 Remote Manager as a remote device network management solution, see these resources:

- *Remote Manager User Guide*
- *Remote Manager Programmer Guide*
- Remote Manager tutorials and other documents available on Digi's Knowledge Base

Web interface

Digi Connect and ConnectPort TS Family devices provide a web interface for configuring and monitoring devices. See Using the Digi Connect and ConnectPort TS Family web interface.

You are required to log in to the web interface.

- **User name**: The default user name is **root**.
- **Password**: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**.

If the default user name and password does not work, they may have been updated. Contact your system administrator. You are required to change the password from the default the first time you log into the web interface.

Note Not all configuration options provided by the command-line interface (CLI) appears in the web interface. If you need to configure more advanced options, see the Accessing the command-line interface for instructions on accessing the CLI.

Accessing the command-line interface

You can configure Digi devices by issuing commands from the command line. The command-line interface allows direct communication with a Digi device.

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 a 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 Configure and manage the device using the Digi Connect and ConnectPort TS Family command line interface for more information on this interface. See the *Digi Connect® Family Command Reference* on www.digi.com 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*.

SNMP

Use SNMP to manage and monitor network devices. SNMP architecture allows you to:

- Manage nodes on an IP network, including servers, workstations, routers, switches and hubs
- Manage network performance, find and solve network problems, and plan for network growth

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 you to perform certain tasks 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) for a list of supported MIBs.

For more information about using SNMP as a device monitoring interface, see SNMP device monitoring capabilities.

Device administration

Periodically, you need to perform administrative tasks on a Digi Connect and ConnectPort TS Family device, such as:

- Uploading and managing files
- Changing the password for logging onto the device
- Backing up and restoring the configuration
- Updating firmware
- Restoring the configuration to factory defaults
- Rebooting the module

As with configuration and monitoring, you can perform administration from a number of interfaces, including the web interface, command line, and Remote Manager. See Administration for more information and procedures.

Using the Digi Connect and ConnectPort TS Family web interface

This section describes how to configure and manage a Digi Connect and ConnectPort TS Family device using the web interface.

Home page

When you access the web interface, the Home page appears. The Home page provides a tutorial and a system summary.

Menu

The left side of the web interface displays a menu. Use the menu to:

- Configure the Digi device, peripheral devices, and applications
- Manage serial ports and connections
- Administer the Digi device

Getting started

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

System summary

The System Summary page displays the details for this Digi Connect and ConnectPort TS Family.

- **Model**: The model type for this Digi Connect and ConnectPort TS Family product.
- **IPv6 Address (Link)**: The IPv6 address (link) associated with this Digi device.
- **IPv6 Address (Global)**: The IPv6 address (global) associated with this Digi device.
- **IPv4 Address**: The IPv4 address associated with this Digi device.
- **MAC Address**: The MAC address associated with this Digi device.
- **Description**: A description of this Digi device.
- **Contact**: Contact information for the Digi device.
- **Location**: The location of this Digi device.
- **Device ID**: The serial number associated with this Digi device. The serial number appears on a label on the Digi device.

Apply and save changes

The web interface runs locally on the Digi device, which means that the interface always maintains and displays the current settings in the Digi device. When you change the configuration settings, click **Apply** to save your changes to the Digi device.

Cancel changes

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

Online help

The web interface provides online help for all pages. The Home page provides a tutorial.

Management

Use the **Management** menu to view and manage connections and services for the Digi Connect and ConnectPort TS Family product.

You can monitor the port, device, system, and network activities of Digi Connect and ConnectPort TS Family devices from a variety of interfaces. Changes in data flow may indicate problems or activities that may require immediate attention.

This chapter discusses monitoring and connection-management capabilities and tasks in Digi Connect and ConnectPort TS Family products.

Web interface

The web interface has several screens for monitoring Digi Connect and ConnectPort TS Family devices:

- Network status
- Serial Port Management: for each port, the port's description, current profile, port logs (if activated), 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, current serial configuration. The same information appears when you choose Serial Port Management.
  - Network statistics: statistics for IP, TCP, UDP, and ICMP.

Manage connections and services

Use the **Management** menu to view and manage connections and services for the Digi Connect and ConnectPort TS Family product.

Serial Port Management

The Serial Port Management page (**Management** > **Serial Ports**) provides an overview of the serial ports and their connections. Click **Connections** to display the active connections for a serial port. You can refresh the view to see new serial-port connections, and you can disconnect serial-port connections as needed.

Port Connections Management

The Port Connections Management page (**Management** > **Serial Ports** > **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

- Python threads currently running
- Protocols used for the connections
- The number of active sessions for each connection

Use this list to determine which connections are no longer needed. You can disconnect connections that are no longer needed.

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, or starting applications. 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. You cannot disable the event log. Digi uses the event log to get an accurate view of all operational aspects 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.

Manage network services

Management > Network Services displays information about active network services. Currently, the only network-service management task possible from this page is managing the DHCP server.

Administration

You can periodically perform administration tasks on Digi Connect and ConnectPort TS Family products, 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
- Rebooting the device

The Administration section in the web interface provides the following options:

- **X.509 Certificate/Key Management**: Load and manage X.509 certificates and public/private host key pairs that are public key infrastructure (PKI) based security. See X.509 Certificate/Key Management for more information.

Note Only the ConnectPort TS 8/16 supports X.509 certificate/key Management.

- **File Management**: Upload and manage files, such as custom web pages, applet files, and initialization files. See File Management for more information.

- **Python Program File Management**: Upload custom programs in the Python programming language to Digi devices and configuring the programs to execute automatically at startup. See Python Configuration for more information.
- **Backup/Restore**: Back up or restore device configuration settings. See Backup/Restore for more information.
- **Update Firmware:** Update the firmware, including Boot and POST code. See Update the firmware and boot/POST code for more information.
- **Factory Default Settings**: Restore a device to factory default settings. See Factory default settings for more information.
- **System Information**: Display general system information for the device and device statistics. See System information for more information.
- **Activate Find Me LED**: On the Digi Connect ES model only, turn on/off the Find Me or locator LED to aid in locating a specific Digi device. See Activate the Find Me LED for more information.
- **Reboot**: Reboot the device. See Reboot for more information.

These administrative tasks are organized elsewhere in the web interface:

- Enable and disable network services. See Reboot for more information.

File Management

Use the **File Management** page to upload custom files to a Digi Connect and ConnectPort TS Family product, such as an image file containing your company logo. You can use custom applets and HTML files to alter the interface either by adding a different company logo, changing colors, or moving information to different locations.

If you upload an index.htm or index.html file, that file automatically loads when you sign in to a Digi device from the web browser.

Upload files

To upload files to a device:

1. Select **Administration** > **File Management**.
2. Click **Choose File** to locate and select the file.
3. Click **Upload**.

Delete files

To delete files from a device:

1. Select **Administration** > **File Management**.
2. Select the **Action** check boxes next to files that you want to delete.
3. Click **Delete**.

Factory reset does not delete custom files

A factory reset does not delete files uploaded to the File Management page. When you restore the Digi device to factory defaults or press the **Reset** button on the device (see Factory default settings), the

uploaded files remain. This allows you to retain custom applets and custom factory defaults. If you want to remove custom files you must manually delete them (see Delete files).

X.509 Certificate/Key Management

Use the X.509 Certificate/Key Management page to upload and manage entries in the database of certificate and private key data. This feature supports displaying, loading, saving, removing, certificate database entries, and importing a private key for the Digi device into the database. Certificates and public/private host key pairs are an integral part of public key infrastructure (PKI) based security.

Supported security implementations

The X.509 Certificate/Key Management manages several kinds of certificate databases and security implementations, including:

- **X.509 Certificate Authority/Certificate Revocation**—A trusted third party issues digital certificates for use by other parties.
- **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**—Use SSL and TLS security to secure access to web pages for configuration purposes, secure serial port connections, and SSL autoconnect, an automatic connection (autoconnection) between a serial port on the device and a remote network destination.
- **Secure Shell (SSHv2)**—Use SSHv2 to secure access to a device's console and serial ports for configuration purposes.

Benefits of certificates

You gain the following benefits when you use certificates to manage security:

- Certificates are more secure than Digi self-signed certificates.
- Certificate management allows you to push your own certificates out to Digi device.
- The key sizes are more flexible.
- When you manage certificates through the web interface, it creates a repository of certificates that other applications and processes can use.

Additional information on certificate management

Implementing certificate management requires selecting a security type and understanding its technical details and key operations. If you are tasked with certificate management for your organization and need more background information, a good place to start is Wikipedia articles for the security types (X.509 CA/CRL, SCEP, VPN, SSL/TLS), and SSH). These articles reference resources such as standards, Request For Comments pages (RFCs), and articles that provide more technical detail.

Tables managed by the X.509 Certificate/Key Management feature

Certificate and key management information is stored in the following database tables:

Security type	Table	Used to load
X.509 Certificate Authority/Certificate Revocation	CA (Certificate Authority)	Certificate authority digital certificates. A certificate authority (CA) is a trusted third party that issues digital certificates for use by other parties. Digital certificates issued by the CA contain a public key. The certificate contains information about the individual or organization to which the public key belongs. A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.
	CRL (Certificate Revocation List)	Certificate revocation lists for loaded CAs. A certificate revocation list (CRL) is a file that contains the serial numbers of digital certificates issued by a CA which have been revoked, and should no longer be trusted. Like CAs, CRLs are a vital part of a public key infrastructure (PKI). You must install the digital certificate of the corresponding CA before you load the CRL.
Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	SSL Identity	SSL/TLS identity certificates. A default key is generated automatically but can be overridden by a user. Note that this default key is not secure.
	SSL Identity Keys	SSL/TLS identity private keys.
	SSL Peer	SSL/TLS peer certificates.
	SSL Revoked	Verbatim revoked SSL/TLS certificates.
Secure Shell (SSHv2)	SSH Host Keys Table	SSHv2 identity private keys. Used for authentication with SSHv2 clients and secure key exchange. A default 1024-bit DSA key is generated automatically if none exists when the device boots. There is no certificate for SSHv2, just private key data.

Behavior of SSH/SSL private keys on Digi device

Digi devices generate their SSH/SSL self-signed private keys automatically. While this automatic generation is convenient for device users, as they are not required perform any actions regarding the private keys, it presents some security loopholes.

- With self-signed private keys, you must establish trust in a secure environment. That is, if you cannot guarantee that the environment is secure, you must pull the private keys off the Digi device.
- You must know about the certificate before you connect, as opposed to third-party signed certificates, where you only need the third-party certificate.
- The length of a Digi device's self-signed private keys is 1024 bits. While this length is adequate for 99.9% of all applications, some people or applications prefer a shorter or longer key.

Using TFTP to load and store certificate information

Use TFTP to load and store PEM-formatted certificates into the certificate and private key management tables.

Using HTTP/HTTPS to transfer certificate and key data

You can use HTTP or HTTPS to transfer certificate and private key data on a web browser.

Data retained after factory reset

When you reset a Digi device to factory defaults, it retains certificates and private key data loaded onto it.

Certificate management settings

There are separate pages of settings for the certificate databases and key management for certificates and key data for the different types of security implementations.

Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs)

Upload CAs and CRLs

Use this section to upload and manage certificate authority (CA) certificates, or certificate revocation list (CRL) files. You can install up to 8 CA certificates and up to 8 CA revocations. You can also obtain CA certificates from a SCEP server. You can install up to 8 SCEP CA certificates.

You an use files in ASN.1 DER or PEM Base64 encoded formats. Click Choose File and type or browse to the name of the file to upload. Click the **Upload** button to upload the file.

Installed Certificate Authority Certificates

The table lists any certificate authority certificates that are loaded in the Certificate Authority database.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate. This is expressed as the value entered in a browser's URL field; typically a Fully Qualified Domain Name (FDQN) if using DNS or an IP address.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Delete** button: Click to delete the CA certificates selected in the **Action** column from the database.

Installed Certificate Authority Certificate Revocation Lists

The table lists any certificate authority certificate revocation lists that are loaded in the Certificate Revocation List database.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Issuer**: The entity that issued the certificate.
- **Last Update**: The last date and time the certificate revocation list was issued.

- **Next Update**: The effective or expiration date and time of the certificate revocation list. At this date, a new one must be obtained.
- **Delete** button: Click to delete the CA certificate revocation lists selected in the **Action** column from the database.

Secure Socket Layer (SSL) / Transport Layer Security (TLS) Certificates

Use the **Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Certificates** page to load host certificates and keys, as well as peer certificates and revocations.

Identity certificates and keys

You can install up to two SSL/TLS identity certificates. You can also install up to 2 SSL/TLS identity keys.

Upload SSL/TLS Identity Keys and Certificates

Use this section to upload SSL/TLS RSA or DSA identity keys and certificates.

You can use identity certificate and key files in ASN.1 DER or PEM Base64 encoded formats.

Enter or browse to the name of the file to upload in the **Upload File** field. A password is required in the **Password** field only if the host key file is encrypted. Click the **Upload** button to upload the file.

Installed SSL and TLS Identity Certificates

This table lists the identity certificates that are installed in the SSL and TLS databases.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Matching Key**: The private key associated with the certificate, if any exists.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Installed SSL/TLS identity keys

This table lists the identity keys that are installed in the SSL and TLS databases.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Type**: The type of encryption of the identity key: RSA (public key cryptography algorithm) or DSA (digital signature algorithm).
- **Matching Certificate**: The certificate associated with the private key, if any exists.
- **Delete** button: Deletes all keys selected in the **Action** column from the database.

Trusted peer certificate

Use this section to upload and manage SSL and TLS trusted peer certificates.

Upload SSL/TLS trusted peer certificates

Use this section to upload SSL/TLS trusted peer certificates. Certificate files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. Click the **Upload** button to upload the file.

Installed SSL/TLS trusted peer certificates

This table lists the installed SSL and TLS trusted peer certificates. You can install up to 8 SSL/TLS trusted peer certificates.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Untrusted revoked certificate

Use this section to upload and manage SSL/TLS untrusted revoked certificates. You can install up to 8 SSL/TLS untrusted revoked certificates.

Upload SSL/TLS untrusted revoked certificates

Use this section to upload SSL/TLS untrusted revoked certificates. Certificate files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. Click the **Upload** button to upload the file.

Installed SSL/TLS untrusted revoked certificates

The table lists the installed SSL and TLS untrusted revoked certificates.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: The entity that received the certificate.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Delete** button: Deletes all certificates selected in the **Action** column from the database.

Secure Shell (SSH) Host Keys

Use the Secure Shell (SSH) Host Keys page to upload and manage SSH host keys.

Upload SSH Host Keys

Use this section to upload SSH RSA or DSA hostkeys. Key files can be in ASN.1 DER or PEM Base64 encoded formats. Enter or browse to the name of the file to upload in the **Upload File** field. A password is required in the **Password** field only if the host key file is encrypted. Click the **Upload** button to upload the file.

Installed SSH host keys

The table lists the installed SSH host keys. You can install up to 2 SSH host keys.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Type**: The type of encryption of the identity key: RSA (public key cryptography algorithm) or DSA (digital signature algorithm).
- **Fingerprint**: The fingerprint of the SSH host key. This fingerprint is in the form of a hash code consisting of several hexadecimal bytes to identify the SSH host key.
- **Delete** button: Deletes the selected SSH host keys in the **Action** column from the database.

Secure Shell (SSH) hostkeys

Use the **Secure Shell (SSHv2) Hostkeys database** to load host private keys. You can use SSHv2 host keys for authentication with SSHv2 clients and secure key exchange. The Digi device automatically generates a default 1024-bit DSA key if none exists when the Digi device boots.

- **Upload SSH Host Keys**: Use this section to upload SSH RSA or DSA hostkeys. Key files may be in ASN.1 DER or PEM Base64 encoded formats. If the host key file is encrypted, a password is required.
- **Installed SSH Host Keys**: Lists the host keys loaded into the SSH Hostkeys database.

Backup/Restore

After you configure a Digi Connect and ConnectPort TS Family 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.

Back up or restore a device configuration from the web interface

You can back up or restore a device configuration to a server from the web-interface and download a configuration from a server to a file or TFTP.

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

To backup a device configuration:

1. Click **Administration** > **Backup/Restore**. The Backup/Restore page appears.
2. Select the storage location type.
3. Click **Backup**.

To restore a device configuration:

1. Click **Administration** > **Backup/Restore**. The Backup/Restore page appears.
2. Select the storage location type.
3. Select the file to restore from the **Restore From File** field or click **Choose File** to locate and select the file.
4. Click **Restore**.

Update the 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 to upload.

Important Read the Release Notes supplied with the firmware to see if the boot/POST code must be updated before updating the firmware or the boot/POST code.

Update the firmware from a file on a computer

To update the firmware from a file on a computer:

1. Select **Administration** > **Update Firmware**. The Update Firmware page appears.
2. Type the name of the firmware or POST file in the **Select Firmware** field, 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 the firmware from a TFTP Server

You can update firmware from a TFTP server through the command-line interface using the **boot** command. You cannot update the firmware from the web interface. For details, see Administration.

Factory default settings

Restoring a Digi Connect and ConnectPort TS Family device to its factory default settings clears all current configuration settings, except the IP address settings and administrator password with some exceptions. See the following topics for more information:

- Settings cleared and retained during a factory reset
- File Management

There are several ways to reset the device configuration of a Digi Connect and ConnectPort TS Family product to the factory default settings:

- From the web interface using the Restore Factory Defaults operation

  This method is the best way to reset the configuration, because you can back up the settings using the Backup/Restore operation. The Backup/Restore operation provides a means to restore the configuration after the configuration issues have been resolved. See Reset the factory settings on a Digi Connect and ConnectPort TS Family product from the web interface for more information.

- From the command-line interface, using the **boot** command

- Using the reset button on the Digi Connect and ConnectPort TS Family device

  Use this method if you cannot access the device from a web browser. The location of the reset button may vary. See Reset the factory settings on a Digi Connect and ConnectPort TS Family product using the Reset button for more information.

Settings cleared and retained during a factory reset

A factory reset does not delete files uploaded to the File Management page. See Factory reset does not delete custom files for more information.

If a Digi device has custom default settings, the settings revert to those custom defaults instead of the factory defaults.

Restoring the Digi device to its factory default settings clears all current settings *except* the IP address settings and the administrator password. All custom-interface files and applet files that you uploaded from the **File Management** page are retained. See File Management for information on uploading and deleting files.

Reset the factory settings on a Digi Connect and ConnectPort TS Family product from the web interface

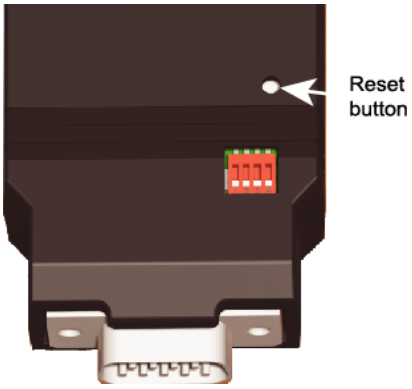
To reset the factory settings on the Digi Connect and ConnectPort TS Family device from the web interface:

1. Create a backup copy of the configuration using the Backup/Restore operation. See Backup/Restore for more information.
2. Select **Administration** > **Factory Default Settings**. The Factory Default Settings page appears.
3. To keep the network settings for the device, such as the IP address, select the **Keep network settings** check box.
4. Click **Restore**.

Reset the factory settings on a Digi Connect and ConnectPort TS Family product using the Reset button

To reset the factory settings on a Digi Connect and ConnectPort TS Family product using the Reset button:

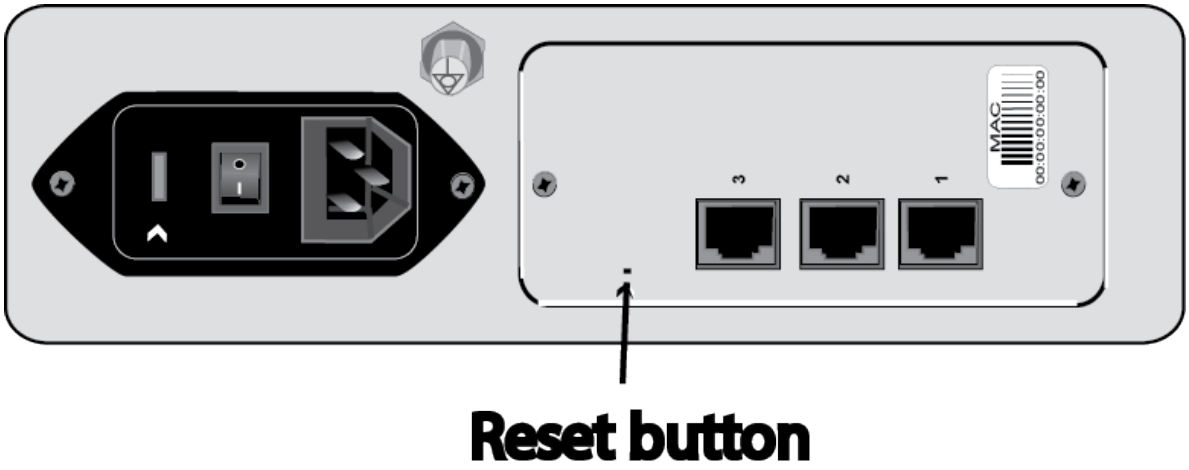
1. Power off the Digi Connect and ConnectPort TS Family.
2. Locate the Reset button or pin on your Digi device. Here is the reset button for a Digi Connect SP unit.



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 causing some or all settings to revert to defaults.

System information

The System Information page displays general system information about the Digi Connect and ConnectPort TS Family device. Technical support uses this information to troubleshoot problems. To display these pages, go to **Administration** > **System Information**.

General

The General page displays the following general system information:

- **Model**: The model of the Digi Connect and ConnectPort TS Family product.
- **MAC Address**: A unique network identifier required for all network devices. The MAC address appears on a sticker on the Digi device and consists of 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 the Digi Support site.
- **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.

- **Power status**: For models with dual power supply, **Power status** shows the status of the power supplies. For example, if power supply 1 for a *Digi Connect and ConnectPort TS Family* 16 MEI unit is disconnected but power supply 2 is connected, the power status appears as follows:

Power status:	Dual power (1 - Fail, 2 - Normal)

Serial

The **Serial** page under **Administration** > **System Information** lists the serial ports and their configuration status. Click a port to view detailed serial port information on the **Serial Port Diagnostics** page.

Note The ConnectPort LTS serial ports behave like DTE ports.

- Outputs from the device: TxD (in 422/485 Full duplex TxD+ and TxD-), RTS, and DTR
- Inputs to the device: RxD (in 422/485 Full duplex RxD+ and RxD-), CTS, DSR, and DCD

For pin-out information, see *ConnectPort® LTS 8/16/32 Quick Start Guide*.

Serial Port Diagnostics

The Serial Port Diagnostics page displays information on the current state of a serial port on your Digi device.

- **Configuration**: The Configuration page displays the electrical interface (Port Type) and basic serial settings.
- **Signals**: The Signals pane shows the state of serial port signals. The serial port signals are green when asserted (on) and gray when not asserted (off). These signals are defined as follows:
  - **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 Statistics section includes 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, you may have a problem with your Digi device server.
  - **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.
  - **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.

GPIO

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. Alarms can be issued when GPIO pins change state, as discussed in Alarms Configuration.

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 Connect and ConnectPort TS Family product.

Ethernet Connection Statistics

- **Speed**: Ethernet link speed: 10 or 100 Mbps. N/A if link integrity is not detected. For example, the cable is disconnected.
- **Duplex**: Ethernet link mode: half or full duplex. N/A if link integrity is not detected. For example, 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 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 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 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

- **Datagrams Received/Datagrams Forwarded**: Number of received or forwarded datagrams.
- **Forwarding**: Displays whether forwarding is enabled or disabled.
- **No Routes**: Number of outgoing datagrams for which no route to the destination IP can be found.
- **Routing Discards**: Number of discarded outgoing datagrams.
- **Default Time-To-Live**: Number of routers an IP packet can pass through before it is discarded.

TCP Statistics

- **Segments Received/Segments Sent**: Number of received or sent segments.
- **Active Opens**: Number of active opens. In an active open, the Digi Connect and ConnectPort TS Family product initiates a connection request with a server.
- **Passive Opens**: Number of passive opens. In a passive open, the Digi Connect and ConnectPort TS Family listens 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 retransmitted segments. Segments are retransmitted when the server does not respond to a packet sent by the client. A retransmit limits the number of lost and discarded packets.
- **Established Resets**: Number of established connections that have been reset.

UDP Statistics

- **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

- **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.

Wi-Fi LAN Statistics

- **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.

Remote Manager status

Use the Remote Manager status section to view the connection status for the Remote Manager service.

Diagnostics

Use the ping utility on the **Diagnostics** page to determine whether the Digi device can access remote devices over the network. Type the host name of the remote device you want to access, and click **Ping**.

Activate the 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 Digi Connect 48 SB and Digi Connect 4/8 SB with switch.

- **Activate**: Click this button to activate the Find Me locator LED. The Find Me locator LED starts blinking.
- **Stop**: Click this button to deactivate the Find Me locator LED. The Find Me locator LED stops blinking.

Reboot

Changes to some device settings require saving the changes and rebooting the Digi Connect and ConnectPort TS Family. Use the Reboot page to reboot the Digi Connect and ConnectPort TS Family.

To reboot a Digi Connect and ConnectPort TS Family from the web interface:

1. Select **Administration** > **Reboot**.
2. Click the **Reboot** button. Wait approximately one minute for the reboot to complete.

Enable/disable access to network services

You can enable and disable access to various network services, such as ADDP, RealPort, SNMP, and telnet. For example, you can disable access to all network services that are not required for running or interfacing with the Digi Connect and ConnectPort TS Family product for performance and security reasons. From the web interface, you can enable and disable network services on the **Network Services Settings** page for a Digi Connect and ConnectPort TS Family product. See Network Services Settings.

Configure the device using the web interface

Use the options under **Configuration** to configure settings for various features, such as network settings and serial port settings.

Network configuration

The Network Configuration page includes:

- **IP settings**: For viewing IP address settings and changing as needed.
- **WiFI IP settings**: Configure the IP address used for wireless LAN communication. See Wi-Fi IP settings for more information.
- **WiFI LAN settings**: Configure basic settings for wireless LAN devices such as network name and network connection options. See Wi-Fi LAN settings for more information.
- **WiFi Security settings**: Configure authentication and encryption settings for wireless LAN devices. See Wi-Fi security settings for more information.
- **WiFi 802.1x Authentication settings**: Configure IEEE 802.1x authentication settings for wireless LAN devices. See Wi-Fi 802.1x authentication settings for more information.
- **Network Services settings:** Configure access to various network services, such as ADDP, RealPort and Encrypted RealPort, telnet,HTTP/HTTPS, and other services. See Network Services Settings for more information.
- **IP Filtering settings**: Configure the IP settings for a Digi Connect and ConnectPort TS Family device to only accept connections from specific and known IP addresses or networks. See IP filtering settings for more information.
- **IP Forwarding settings**:
  - Configure the IP forwarding settings for a Digi Connect and ConnectPort TS Family device to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding.
  - Configure the built-in firewall functionality to limit IP traffic to and from certain networks, TCP or UDP ports, and interfaces. This feature is based on Linux tool iptables. See IP filtering settings for more information.
- **Advanced Network Settings**: Configure the Ethernet Interface speed and mode, IP settings, TCP keepalive settings, and DHCP settings. See Advanced Network Settings for more information.

IP SettingsEthernet Uplink IP Settings (for Connect ES 4/8 SB with Switch)

The IP Settings page allows you to configure how to obtain the IP address of the Digi Connect and ConnectPort TS Family device. You can use one of the following methods to obtain the IP address:

- DHCP
- Static IP address
- Subnet mask
- Default gateway

For more information on how to assign and use these settings in your organization, contact your network administrator.

IP settings

The 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.

IP Settings (for Connect ES 4/8 SB with Ethernet 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:

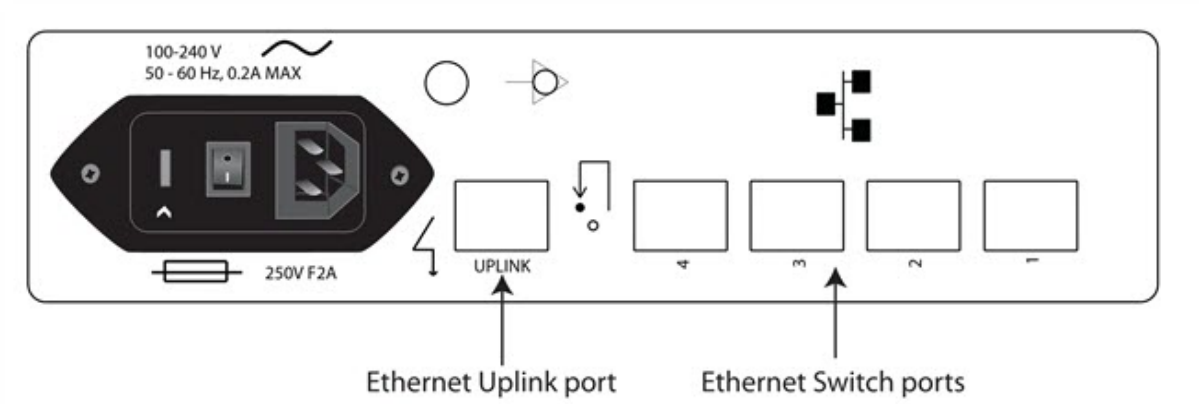
- **Ethernet Uplink**: An uplink interface that connects to the central data management system network.

  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 provides network connectivity for up to four network devices, in addition to the Digi Connect ES SB SW 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.

See Configure the Ethernet interface for Connect ES 4/8 SB with Switch for instructions on configuring the network topology just described.

Configure the Ethernet interface for Connect ES 4/8 SB with Switch

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.

To configure the Ethernet interface for each Connect ES 4/8 SB with Switch:

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 IP address settings for the laptop are as follows:

   - **IP Address**: 192.168.1.99
   - **Subnet**: 255.255.255.0
   - **Default Gateway**: 192.168.1.1

2. From the web interface, select **Configuration** > **Network** > **Ethernet Switch IP Settings**, This page assigns IP address numbers to devices connected to the Ethernet Switch. Digi recommends 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 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 command:

     ```
     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. From the web interface, select **Configuration** > **Network** > **Ethernet Uplink IP settings** and type the static IP address.

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

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

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

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

   Network configuration is complete.

Deploy the 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.

Wi-Fi IP settings

Use the Wi-Fi IP Settings page to configure how to obtain the IP address of a Wi-Fi-enabled Digi device. It has the same settings as the IP Settings page.

Wi-Fi 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 802.11b 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.

Wi-Fi security settings

Use the Wi-Fi Security Settings page to 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 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 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.

Wi-Fi 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 Settings page shows a set of common network services that are available for Digi Connect and ConnectPort TS Family products, and the network port on which the service is

running.

You can enable and disable common network services and configure the TCP/UDP port on which the network service listens. You can disable services as needed 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.

Best practice Use the default network port numbers for basic network services because the port numbers are used by most applications.

CAUTION! Exercise caution when 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, and so on makes the Command-Line interface inaccessible.

Supported basic network services and their default port numbers

For Digi devices with 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

The assumed default base is 2000. For example, the telnet passthrough service is set to network port 2001 for serial port 1, 2002 for serial port 2, and 2003 for serial port 3, and so on.

If you change a network port 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 you change the network port number for telnet passthrough from 2001 to 3001, that does not mean that the other network ports changes to 3002, 3003, and so on.

There are two types of network services available:

- **Basic services**: You can access these services by connecting to a particular well-known network port.
- **Passthrough services**: You can set up a specific type of service for a specific serial port. To use the service, you must 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 on port 1:

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

The following table shows the 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. You cannot change the network port number for ADDP 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.	50000
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 sign in to the Digi device and access the command-line interface through rlogin.	513
Remote shell (Rsh)	Allows users to sign in to the Digi device and access the command-line interface through Rsh.	514
Secure Shell Server (SSH)	Allows users secure access to sign 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 **set** commands 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

Service	Services provided	Default network port number
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
Telnet Passthrough	Allows a telnet connection directly to the serial port, often called reverse telnet. The format for this port number is as follows: 20<serial port number> Replace <serial port number> with the Digi serial port number. For example, 2001 applies to serial port 1, 2010 applies to serial port 10, and 2016 applies to serial port 16.	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. The format for this port number is as follows: 21<serial port number> Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	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. The format for this port number is as follows: 21<serial port number> Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	2101
Web Server, also known as HyperText Transfer Protocol (HTTP)	You can establish secure access to configuration web pages by requiring a user to sign in. HTTP and HTTPS 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

Service	Services provided	Default network port number
Secure Web Server, also known as HyperText Transfer Protocol over Secure Socket Layer (HTTPS)	You can secure access to configuration web pages by requiring a user to sign in with encryption for greater security.	443

IP filtering settings

Some Digi devices support built-in firewall functionality to limit TCP/IP traffic to and from certain networks, TCP ports, and interfaces. The functionality implemented is based on the **iptables** tool.

You can restrict your Digi 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 Digi 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.

The settings for IP Filtering 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 are 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 cannot 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 you can add 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 you can configure 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.

  You can 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. For this reason, you 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, using port ranges for FTP forwarding is not supported; a port count of 1 is required.

IP forwarding 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:

1. Select the **Enable IP Routing** check box.
2. 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 Connect and ConnectPort TS Family product'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 Connect and ConnectPort TS Family product on the configured port number. The Digi Connect and ConnectPort TS Family product then opens a separate connection to the specified destination host. Once the tunnel is established, the Digi Connect and ConnectPort TS Family product acts as a proxy for bi-directional 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 (seconds):** 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 product 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 server. Currently, TCP and SSL are the two supported protocols.
- **Destination Host:** The hostname or IP address of the destination network device.
- **Destination Port:** The port number that the Digi device will use to make a connection to the destination device.
- **Destination Protocol:** 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 **Add** to add a socket tunnel. Click **Apply** to save the settings. Once the socket tunnel is configured, select 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): .

  You can specify the host name value as 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 keepalive 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 settings

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 ports configuration

Use the Serial Ports Configuration page to establish a port profile for each serial port on the Digi Connect and ConnectPort TS Family product. The Serial Ports 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.

The Serial Port Configuration page includes the **Port Settings** pane that lists the available ports and allows you to configure or copy selected ports.

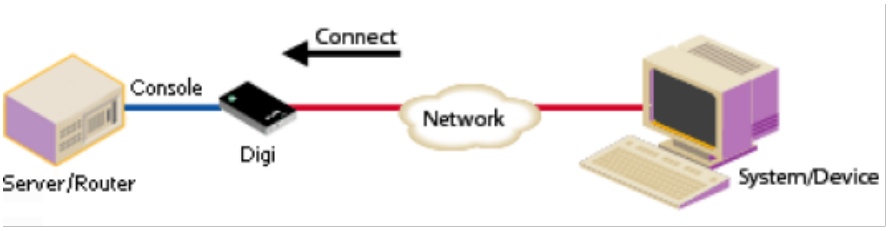
Select Port Profile

The Select Port Profile page appears when you click **Change Profile** on the **Port Profile Settings** pane.

A port profile allows you to easily configure a serial port based on how you intend to use that port. By selecting one of the pre-defined profiles, the configuration options are focused only on the settings required for that particular profile.

The Digi Connect and ConnectPort TS Family supports the following port profiles:

- **Console Management**: Manage a serial device's console port over a network connection. The Console Management profile allows you to access a Digi 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 Connect and ConnectPort TS Family product. Then using TCP/IP utilities like reverse telnet, network administrators can access these consoled serial ports from the LAN.



  See Assign a profile to a serial port for more information.

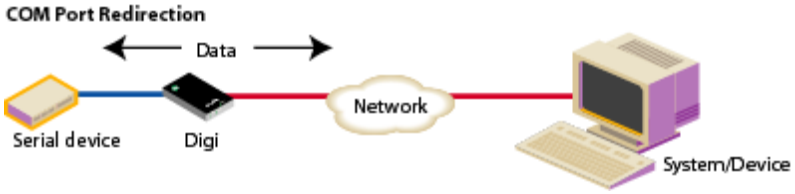
- **Custom**: The Custom profile is an advanced option to allow full configuration of the serial port. Use the Custom profile only if the serial port does not fit into any of the predefined port profiles. For example, when network connections involve a mix of TCP and UDP sockets. See Assign a profile to a serial port for more information.

- **DialServ**: 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 DialServ interoperation **requires** this profile.

- **Local Configuration**: The Local Configuration profile allows you to sign in and access the command line interface when connecting directly to a serial port on a Digi device. This profile provides a login from the Digi device. See Assign a profile to a serial port for more information.
- **Modem Emulation**: The Modem Emulation profile allows you to configure the serial port to act as a modem. The Digi device server emulates modem responses to a serial device and seamlessly sends and receives data over an Ethernet network instead of a PSTN (Public Switched Telephone Network). This allows you to retain legacy software applications without modification and use a less expensive Ethernet network in place of public telephone lines. See Assign a profile to a serial port for more information.
- **RealPort**: Use RealPort to map a COM or TTY port to this serial port of your Digi device. The COM/TTY port appears and behaves as a local port to the PC or server. RealPort is also known as COM Port Redirection. See Assign a profile to a serial port for more information. Refer to Install RealPort software for basic RealPort installation instructions. Refer to *RealPort Installation User's Guide* for more detailed instructions on installing and configuring the RealPort driver on your PC or server.

  When you configure a RealPort profile, the Digi Connect and ConnectPort TS Family product relinquishes control of the serial port to the host that has the RealPort driver installed. The computer applications send data to this virtual COM or TTY port and the RealPort driver sends the data across the network to the corresponding serial port on the Digi Connect and ConnectPort TS Family product.



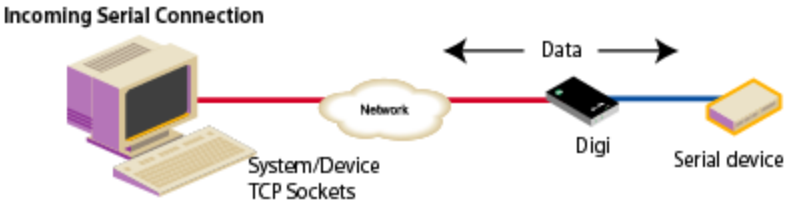
The network is transparent to both the application and the serial device.

Important Install and configure the RealPort software on each computer that uses RealPort ports. See Assign a profile to a serial port for installation instructions. You need to configure the RealPort software with the IP address of the Digi Connect and ConnectPort TS Family product.

- **Serial Bridge**: The Serial Bridge Profile configures one side of a serial bridge. A bridge connects two serial devices over the network as if they were connected with a serial cable. This is also referred to as serial tunneling. Each serial device is connected to the serial port of a Digi device server. You must configure one Digi device as the client and the other Digi device as the server. This profile configures each side of the bridge separately.

See Assign a profile to a serial port for more information.

- **TCP Sockets**: Auto-Connect (TCP client) to another host on the network or allow incoming connections on this serial port (TCP server). 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 Connect and ConnectPort TS Family product. The TCP client will establish a TCP connection to a defined IP address and port number.



For more information about the TCP Sockets, see the following:

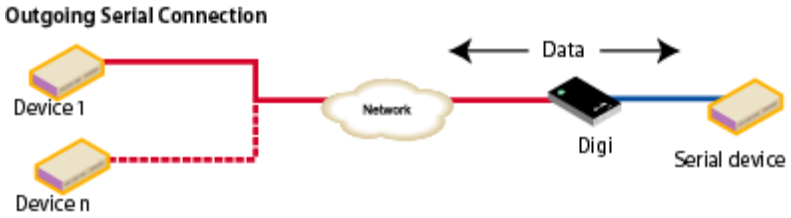
- Automatic TCP connections (Automatic Connection)
- TCP and UDP network port numbering conventions

See Assign a profile to a serial port for more information about assigning a profile.

- **UDP Sockets**: Allows the automatic distribution of serial data from one host to many devices at the same time. 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. See Assign a profile to a serial port for more information.

  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.



Not all port profiles are supported in all products. Supported port profiles varies by Digi Connect and ConnectPort TS Family model. If a profile listed in this description is not available on the page, it is not supported in the Digi Connect and ConnectPort TS Family product.

If you selected a port profile, the port number associated with the port profile appears at the top of the page. You can change or retain the profile and adjust individual settings.

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

Assign a profile to a serial port

To assign a profile to a serial port:

1. Select **Configuration** > **Serial Ports**.
2. Click a ***port number*** from the **Port** column.
3. Click **Change Profile**.
4. On the **Select Port Profile** page, select a port profile option and then click **Apply**.

5. Complete the steps based on the selected profile option:
   - **Console Management**: 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 your Digi device server. Then using TCP/IP utilities like reverse telnet, network administrators can access these consoled serial ports from the LAN.
     a. Record the TCP (or SSH) port number listed under **TCP Server Settings**. You will need the TCP port number when configuring an application or device that accesses the serial port from the network.
     b. To log inbound serial data, click **Advanced Serial Settings**, select **Enable port logging**, and then click **Apply**.
     c. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device, and then click **Apply**.

     Note Configure the application or device that initiates communication to the serial port from the network with the following information:
     - IP address of this Digi device server.
     - TCP or (SSH) port number for the serial port recorded above in Step a.

   - **Local Configuration** (Console Port): Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device or terminal, and then click **Apply**.
   - **Custom**: Complete the fields under **Serial Port Configuration** and then click **Apply**.
   - **Modem Emulation**: Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device and then click **Apply**.

     Modem emulation enables a system administrator to configure the serial port to act as a modem. The Digi device server emulates modem responses to a serial device and seamlessly sends and receives data over an Ethernet network instead of a PSTN (Public Switched Telephone Network). The advantage for a user is the ability to retain legacy software applications without modification and use a less expensive Ethernet network in place of public telephone lines.

- **RealPort**: COM port redirection is provided with the RealPort software installed on your network-based computer. RealPort creates a virtual COM port on your computer. When your computer applications send data to this virtual COM or TTY port, RealPort sends the data across the network to the Digi device server. The Digi device server routes the data to the serial device connected to its serial port. The network is transparent to both the application and the serial device.

  Prerequisite RealPort software must be installed on each computer that you want to connect to. See Install RealPort software for more information.

  RealPort will set the serial port settings as directed by the computer application, so there is no need to modify the Basic Serial Port Settings.

- **Serial Bridge**: A bridge connects two serial devices over the network as if they were connected with a serial cable. This is also referred to as serial tunneling. Each serial device is connected to the serial port of a Digi device server. Configure one Digi device as the TCP server and the other Digi device as the TCP client. Once you establish a connection between the two Digi devices the communication is bi-directional.

  To assign a Serial Bridge (Serial Tunneling) to a serial port on a Digi device acting as the TCP client (which initiates the connection to the TCP server):

  a. Select **Initiate serial bridge to the following device** and provide the following information:
     - Type the **IP Address** of the other Digi device server.
     - In the **TCP Port** field, type the Raw TCP port number for the destination serial port. If the serial port is the first or only port on the device server, the value is 2101.

  b. Click **Apply** to save the configuration.

  c. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device and then click **Apply**.

  Follow the same steps to configure the Digi device server on the other side of the bridge, with the following exceptions:

  - Select **Allow other devices to initiate serial bridge**. The default **TCP Port** rarely needs to be changed.
  - Clear the **Initiate serial bridge to the following device** check box.

- **TCP Sockets** for TCP client (Automatic Connection): In a TCP client configuration, the Digi device server automatically establishes a TCP connection to an application or network device. See Automatic TCP connections (Automatic Connection) for more information.

  To assign a TCP Client (Automatic Connection) profile to a serial port:

  a. Under **TCP Client Settings**, select the **Automatically establish TCP connections** check box.

  b. Select the **Connect** option that describes when the TCP connection will be initiated.

  c. Type the IP address or DNS name of the destination server in the **Server (name or IP)** field.

  d. Select one of the following options from the **Service** drop-down list:

  - Raw TCP
  - Rlogin
  - Secure Sockets
  - Telnet
  - SSH

e. Specify the destination TCP port number in the **TCP Port** field. The port number depends on the conventions used on the remote server or device. The following table provides the common TCP port number conventions.

Connection Service	Common TCP Port Number
Telnet	23
Rlogin	513
Reverse Telnet to the port of the Digi device server The format for this port number is as follows: 20<serial port number> Replace <serial port number> with the Digi serial port number. For example, 2001 applies to serial port 1, 2010 applies to serial port 10, and 2016 applies to serial port 16.	2001
Raw connection to the port of the Digi device server The format for this port number is as follows: 21<serial port number> Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	2101

f. Click **Apply** to save the configuration.

g. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device or terminal, and then click **Apply**.

- **TCP Sockets** for TCP server: A TCP Server configuration allows other network devices to initiate a TCP connection to the serial device attached to a serial port of the Digi device server. This is also referred to as reverse telnet, console management or device management.
    a. Record the TCP (or SSH) port number listed under **TCP Server Settings**. You will need the TCP port number when configuring an application or device that accesses the serial port from the network.
    b. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device or terminal, and then click **Apply**.

Note Configure the application or device that initiates communication to the serial port from the network with the following information:

- IP address of this Digi device server.
- TCP or (SSH) port number for the serial port recorded above in Step a.

- **UDP Sockets** for UDP client (data distribution): UDP client configuration allows the automatic distribution of serial data from one host to many devices at the same time using UDP sockets. This is also referred to this as UDP Multicast.
    a. Under **UDP Client Settings**, provide the following information for each UDP destination:
        - A description of the destination.
        - The destination IP Address or DNS name.
        - The destination UDP port.

        When finished, click **Add**.
    b. Select the options that define when to send data and click **Apply**.
    c. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device or terminal, and then click **Apply**.
- **UDP Sockets** for a UDP server:
    a. Record the UDP port number listed under **UDP Server Settings**. You will need the UDP port number when configuring an application or device that accesses the serial port from the network.
    b. Click **Basic Serial Settings**, complete the fields to match the settings of the attached serial device, and then click **Apply**.

Note Configure the application or device that initiates communication to the serial port from the network with the following information:

- IP address of this Digi device server.
- UDP port number for the serial port recorded previously in Step a.

Automatic TCP connections (Automatic Connection)

The TCP Client allows the Digi Connect and ConnectPort TS Family product to automatically establish a TCP connection to an application or a network, known as autoconnection. You can enable autoconnection through the TCP Sockets profile's setting labeled **Automatically establish TCP connections**. When you set the TCP Sockets profile, the DTR flow-control signal indicates when a TCP socket connection has been established. You can use this information when monitoring the serial line. You can use it as a flow-control mechanism to determine when the Digi device connects to a remote device establishes communication. 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 to auto connect to many devices, deterministically, on the network.

TCP and UDP network port numbering conventions

Digi devices use the following conventions for TCP and UDP network port numbering:

For this connection type...	Use this Port
Telnet to the serial port The format for this port number is as follows: `20<serial port number>` Replace <serial port number> with the Digi serial port number. For example, 2001 applies to serial port 1, 2010 applies to serial port 10, and 2016 applies to serial port 16.	2001 (TCP only)
Raw connection to the serial port The format for this port number is as follows: `21<serial port number>` Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	2101 (TCP and UDP)

The application or Digi Connect and ConnectPort TS Family device that initiates communication must use these network ports numbers. If you cannot configure the application or Digi Connect and ConnectPort TS Family product to use these network port numbers, change the network port on the Digi Connect and ConnectPort TS Family product.

RFC 2217

Use the RFC 2217 protocol to access serial devices over the network. RFC 2217 implementations enable applications to set the parameters of remote serial ports (for example, baud rate or flow control), 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 Factory default settings). No additional configuration is required.

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 is 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*.

Basic serial settings

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) these settings are supplied by applications running on the PC or server, and the default values on your Digi device server do not need to be changed.

The possible settings are as follows:

- **Description**: Specifies an optional character string for the port which can be used to identify the device connected to the port.
- **Baud Rate**: Select the baud rate value for the serial device.
- **Data Bits**: Select the data bits value for the serial device.
- **Parity**: Select the parity for the serial device.
- **Stop Bits**: Select the stop bit value for the serial device.
- **Flow Control**: Select the flow control value for the serial device.

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. Enable termination if the terminal/server port is an endpoint node on the 485 network. Use biasing 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

Use **Advanced Serial Settings** to configure the serial interface and the access to the serial interface. The default settings work in most situations.

Serial settings

- **Enable Port Logging**: Port logging allows you to save serial data to the memory of the Digi device server. Once enabled, the port log can be viewed by selecting **Port Logs** on the Serial Port Management page (**Management** > **Serial Ports**). Port Logging is enabled in the CLI via the set buffer command.
- **Log Size**: The size in kilobytes of the memory buffer used to save serial data when port logging is enabled.
- **Automatic backup**: The port data is stored to specified location automatically.
- **Unlimited automatic backup size**: When enabled, the automatic backup size is not limited.
- **Automatic backup size**: This option defines the amount of the log to backup at a time.
- **Enable SYSLOG service**: The port data can be stored to the SYSLOG server in addition to the port log storage location at the same time.
- **Enable RTS Toggle:** When enabled, the Digi device asserts RTS (Request To Send) when sending data on the serial port.

- **Enable RCI over Serial (DSR):** This choice allows configure the Digi Connect device 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

These TCP Settings are available only when you configure the current port with the Console Management, Custom, or TCP Sockets profile.

- **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. Enter non-printable characters as follows:

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

- **Send data only under any of the following conditions**: Enable if you need to specify the conditions when the Digi device server will send the data read from the serial port to the TCP destination.

- **Send when data is present on the serial line**: Send the data to the network destinations when a string of characters is detected in the serial data. To enter non-printable characters, use these key sequences:

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

- **Match string**: A 1 to 4 character string. This is usually the newline character sequence but can also be a custom string of 1 to 4 characters.
- **Strip match string before sending:** Search for the string specified in the Match String field before sending the data and strip the string from the string from the data before it is sent to the destination.
- **Send after the following number of idle milliseconds**: Send the data after the specified number of milliseconds have passed with no data received on the serial port.
- **Send after the following number of bytes**: Send the data after the specified number of bytes have been received on the serial ports.
- **Close connection after the following number of idle seconds**: Enable to close an idle connection. Use the **Timeout** field to enter the number of seconds that the connection will be idle before it is closed. This can be 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.

  Note If you are using 8-wire cabling, you must apply the altpin for DCD functionality.

- **Close connection when DSR goes low**: When selected, the connection will be closed when the DSR (Data Set Ready) signal goes low.

UDP settings

These UDP Settings are available only when the current port is configured with the Console management, 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 can be 1 to 256 ASCII characters. Enter non-printable characters as follows:

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

Display current serial port settings

To display the current serial port settings for a Digi device, type **display techsupport** 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 signaling 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, and so on. The following table lists the default serial settings for the GPIO pins on a Digi device. 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 are issued when GPIO pins change state. You can use input mode with alarms to trigger email notifications or SNMP traps when a particular signal change is detected, as discussed in Alarms Configuration.
- **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

You can configure the Digi Connect and ConnectPort TS Family to send alarms in the form of email notifications or SNMP traps when a GPIO pin signals an event has occurred on the Digi device. See Alarms Configuration for more information.

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.
4. Configure an email alarm for the GPIO pin. See Alarms Configuration.
5. Toggle the SW2 switch several times to generate several email alarms.

Test GPIO output

To test GPIO output, you must send a GPIO signal from the configuration application that turns on an LED on the development board.

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. Access and log in to the web interface.
4. Click **GPIO** . On the GPIO page, configure one or more GPIO pins for output. See GPIO pins for details.
5. Under **Administration**, click **System Information**.
6. On the **System Information** page, click **GPIO**.
7. Choose **Asserted** to raise the signal, and then click **Set Pins**. An LED on the development board is turned on.

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

Alarms Configuration

Use the Alarms Configuration page to configure 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

Use the Alarm Notification Settings page to configure the following:

- **Enable alarm notifications:** Enables or disables all alarm processing for the Digi 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 Remote Manager.

  Enabling this setting sends all alarm notifications to Remote Manager. Enable this option if the Digi device is managed by a remote management server, such as Remote Manager. 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.

  When you disable this setting alarm notifications are not sent to Remote Manager. Disable this setting if devices are not managed by a Remote Manager server or if alarms are sent from the device. For example, an SNMP trap destination is local to the device, not Remote Manager.
- **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 list and status

The **Alarm Conditions** page lists all of the alarms. You can configure up to 32 alarms for a Digi device, and you can individually enable and disable these alarms.

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**: The 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 Conditions

Use the Alarm Conditions page to specify 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

Use the Alarm Destinations page to define 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**: Enable sending the alarm 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 set the **Alarm Type** to **snmptrap** and specify the IP address of the destination for the SNMP traps in the SNMP settings (**Configuration > System > Simple Network Management Protocol**). See Simple Network Management Protocol (SNMP) Settings. 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:

1. Select both **Send E-Mail** and **Send SNMP trap** check boxes.
2. Click **Apply** to apply changes to alarm settings and return to the Alarms Configuration page.

Configure alarm conditions

To configure an alarm:

1. Select **Configuration** > **Alarms**.
2. To enable or disable an alarm, select or clear the Enable check box next to the alarm.
3. Click the alarm under the **Alarm** column that you want to configure.
4. Configure the fields in the following sections:
   - **Alarm Conditions**: These condition specify the conditions on which the alarm is based, such as serial data pattern matching or data usage.
   - **Alarm Destinations**: These conditions specify how the alarm is sent, either as an email message or an SNMP trap, or both, and where the alarm is sent.
5. Click **Apply** to save your changes.

System Configuration

Use the System Configuration page to configure device identity and description information, date and time settings, and settings for Simple Network Management Protocol (SNMP).

Device Identity Settings

Use the Device Identity Settings page to create a description of the Digi Connect and ConnectPort TS Family product's name, contact, and location. You can use this information to identify a specific Digi device product 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**: A text description of the device ID used to identify the device (for example, MAC or IP address).

Simple Network Management Protocol (SNMP) Settings

Use the Simple Network Management Protocol (SNMP) Settings page to manage and monitor network devices. You can configure Digi Connect and ConnectPort TS Family devices to use SNMP features, or you can disable SNMP for security reasons. For additional information, see Simple Network Management Protocol (SNMP).

- **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**: Provide the IP address or fully qualified domain name (FQDN) of the system where the SNMP agent sends traps. The primary destination is required. The secondary destination is optional.
  - **Primary/Secondary**: The IP address of the system to which the SNMP agent sends traps. To enable any of the traps, you must specify a non-zero value. The primary destination is required. The secondary destination is optional. If your Digi devices supports alarms, you must complete this field in order to send alarms in the form of SNMP traps. See Alarms Configuration.

  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 sends SNMP login traps on login attempts.
  - **Generate cold start traps**: The SNMP agent sends traps on cold starts of the Digi device.
  - **Generate link up traps**: The SNMP agent sends link up traps when network connections are established.

Date and Time Settings

Use the Date and Time Settings page to set the Coordinated Universal Time (UTC) and/or system time and date on a device, or set the offset from UTC for the Digi device's system time.

Set the date and time

To set the 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: https://en.wikipedia.org/wiki/Lists_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, and so on. 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

Use the Time Source Global settings to configure the 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 the Digi device receives a time update from a best (smallest value) ranking time source and the new time is within that range, the Digi device's time is not changed. However, if the new time falls outside the defined threshold range, the Digi 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 Digi device's time will be updated using a new time value that is 60 seconds or more different than the Digi device's current time value. If the new time value differs from the Digi device's current time by less than 60 seconds, the Digi 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 Digi device's time. If the best-ranking source stops reporting new time values, it is considered “lost”.

  Enabling Lost Time Source Recovery allows the Digi device to consult one or more worse-ranking (higher value) time sources 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. You cannot configure these interval values.

Use the Time Adjustment Threshold to limit the amount of drift that will be tolerated before the Digi device's time is updated using a new sample. You should select an appropriate value with consideration for the reliability of the time sample sources.

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

If the communications path between the Digi device and server involves a cellular network connection, you should consider the performance and behavior characteristics of the cellular network. 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.

Configure RADIUS authentication for a ConnectPort TS device

You can configure a ConnectPort TS to use RADIUS (Remote Authentication Dial-In User Service) servers to authenticate and maintain user profiles on dial-in users.

When RADIUS authentication is enabled, the user name and password used to log into the ConnectPort TS is sent to the RADIUS server for authentication. If the user login has been configured on the RADIUS server, then the user is allowed to access the ConnectPort TS web interface.

To configure RADIUS authentication:

1. Determine whether the RADIUS server is configured to authenticate users. See RADIUS server reference.
2. Create the required RADIUS roles locally on the ConnectPort TS. See Create RADIUS server roles.
3. Enable RADIUS authentication for a device, and then configure the Digi device to use one or more RADIUS servers to authenticate user profiles See Enable RADIUS authentication.

RADIUS server reference

Note This information applies only to the ConnectPort TS.

Before you can use the RADIUS server to authenticate users attempting to access a ConnectPort TS device, your system administrator must configure the RADIUS server with the following:

- A default set of attributes (or roles):
  - role-admin
  - role-outbound
  - role-nasprompt
- The desired permissions assigned to each attribute. The permissions determine the actions the user role is allowed to perform in the ConnectPort TS web interface.

  Note The permissions assigned to the attributes on the RADIUS server must exactly match the permissions assigned to the user on the device. See Create RADIUS server roles.

When the RADIUS server is configured and RADIUS authentication is enabled on the ConnectPort TS, then when user logs into the device using one of the default attributes, the device sends the user login information (user name, password, and attribute) to the RADIUS server. The RADIUS server logs into the device using the login information. The user is then able to perform actions in the ConnectPort TS web interface.

Create RADIUS server roles

To ensure that RADIUS authentication works as expected, you must create users locally on the ConnectPort TS for the roles that match the default set of attributes configured on the RADIUS server. These are the user names and passwords that must be used to log in to the ConnectPort TS web interface.

The required list is as follows:

- role-admin
- role-outbound
- role-nasprompt

For each of these users, you must also define the permissions that determine the actions the user is allowed to perform in the ConnectPort TS web interface.

Note The permissions assigned to the user on the device must exactly match the permissions assigned to the attributes on the RADIUS server . See RADIUS server reference.

To create the default users for RADIUS authentication:

1. Access the web interface.
2. Select **Configuration** > **Users**.
3. Add the **role-admin** user.
    a. Click **New**. The **Add New User** page displays.
    b. Enter a default name: **role-admin**
    c. Enter the password: **role-admin**
    d. Click **Apply**. The changes take effect immediately. No logout/login is necessary.
4. Add the **role-outbound** user.
    a. Click **New**. The **Add New User** page displays.
    b. Enter a default name: **role-outbound**
    c. Enter the password: **role-outbound**
    d. Click **Apply**. The changes take effect immediately. No logout/login is necessary.
5. Add the **role-nasprompt** user.
    a. Click **New**. The **Add New User** page displays.
    b. Enter a default name: **role-nasprompt**
    c. Enter the password: **role-nasprompt**
    d. Click **Apply**. The changes take effect immediately. No logout/login is necessary.
6. The three new users display in the **Users** page. You must define the access and permissions for each user.
    a. Click **role-admin**.
    b. Expand the **User Access** section and configure user access. See Change user access settings.
    c. Expand the **User Permissions** section and configure the permissions. See User permissions settings.
    d. Repeat the process for the remaining roles: **role-outbound** and **role-nasprompt**.

Enable RADIUS authentication

You can enable RADIUS authentication for a device, and then configure the Digi device to use one or more RADIUS (Remote Authentication Dial-In User Service) servers to authenticate user profiles.

1. Access the web interface.
2. Click **System** from the **Configuration** section. The **System Configuration** screen displays.
3. Select **Authenticate users via a RADIUS server** to enable RADIUS authentication.
4. Configure the primary RADIUS server.
    a. In the **Primary server's name** field, enter the name or IP address of the RADIUS server that should be queried first. If this server is down or busy, the Digi device server will query the secondary server, if one is configured.
    b. In the **Primary server's secret** field, enter the password used for encrypting messages between the RADIUS server and the Digi device server.
5. (Optional) Configure a secondary RADIUS server. If the primary RADIUS server is down or busy, the Digi device server will query the secondary RADIUS server.
    a. In the **Secondary server's name** field, enter the name or IP address of the RADIUS server that should be queried if the primary RADIUS server is down or busy.
    b. In the **Secondary server's secret** field, enter the password used for encrypting messages between the RADIUS server and the Digi device server
6. Click **Apply** to save the changes.

Remote Manager settings

The Remote Manager 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 you to configure and manage Remote Manager-registered devices from remote locations.

In this discussion:

- *Remote Manager* 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.
- *Remote Manager-registered device* is Digi device that connects to the Remote Manager platform which implements the EDP protocol in order to establish and maintain this connection.

For more information about Remote Manager, these terms, and how to remotely configure and manage this device, please visit the Remote Manager product page and see the *Remote Manager User Guide*.

Device ID requirement for the Digi device

When configuring a Digi device to be a Remote Manager-registered device, you must create a Device ID for the Digi device. The Device ID allows the Digi device to communicate with Remote Manager.

By default, the Device ID is created from the MAC address of the device. The default setting is the recommended setting for the Device ID. You can configure the Device ID from the **Configuration** > **System** > **Device Identity Settings** page on the Digi device's web interface. See System Configuration for more information.

After you configure the device's Device ID, you must sign in to Remote Manager and configure the settings on the following pages:

- **Connection Settings**
- **Short Messaging**
- **Advanced Settings**

Connection settings

The Connection settings configure how the Remote Manager-registered device connects to Remote Manager. These settings allow the Remote Manager-registered device and Remote Manager to communicates with each other.

About Remote Manager connections

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

You can specify addresses for Remote Manager-registered devices that are 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 Remote Manager connection*, the Remote Manager-registered device connects to the network, and tries to establish a connection to Remote Manager. To maintain the connection, the Remote Manager-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 Remote Manager connections in any cellular network, whether using public or private IP addresses, or even if using NAT. Note that your cellular/mobile provider may charge you, depending on your cellular/mobile service plan, when the Remote Manager-registered device sends keep-alives messages.

A *server-initiated Remote Manager connection* works the opposite way. Remote Manager opens a TCP connection, and the Remote Manager-registered device must be listening for the connection from Remote Manager to occur. An advantage of server-initiated Remote Manager connections is that you are not charged for sending the keep-alive bytes that are used in device-initiated connections. A disadvantage is that there is no way of knowing whether the devices displayed in the Remote Manager-registered device list are offline or connected. The device list shows all the devices as disconnected until Remote Manager does something to interact with them. In addition, you cannot use Remote Manager connections for devices that use private IP addresses and are behind a NAT. (Server-initiated connections are not supported.)

A *timed* connection is another form of a device-initiated connection. For a timed connection, the Remote Manager-registered device tries to connect to the Remote Manager Server at a configured, regular interval (period). If a connection to an Remote Manager 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 Remote Manager-registered device present a challenge in Remote Manager server-initiated connections, because Remote Manager needs to locate the Remote Manager-registered device by its new IP address. Remote Manager devices handle address changes by sending a *device IP address update* to Remote Manager. An IP address update permits Remote Manager to connect to the Remote Manager-registered device, or to dynamically update a DNS with the IP address of the Remote Manager-registered device.

Device-Initiated Remote Manager Connection settings

- **Enable Device-Initiated Remote Manager Connection**: When enabled, the Remote Manager-registered device initiates the connection to the Remote Manager.
- **Remote Manager Server Address**: The IP address or hostname of the Remote Manager platform.
- **Automatically reconnect to Remote Manager after being disconnected**

  Reconnect after: When enabled, the Remote Manager-registered device automatically reconnects to Remote Manager after being disconnected and waiting for the specified amount of time.

Server-Initiated Remote Manager Connection settings

Enable Server-Initiated Remote Manager Connection: Configures the connection to the Remote Manager server to be initiated by Remote Manager.

Enable Device IP Address updates to the following server: Enables or disables a connection to Remote Manager to inform Remote Manager of the IP address of the Remote Manager-registered device, known as a device IP address update. This permits Remote Manager to connect back to the Remote Manager-registered device, or to dynamically update a DNS with the IP address of the Remote Manager-registered device.

Remote Manager Server Address: The IP address or hostname of the Remote Manager platform.

Retry if the IP address update fails:

Retry after: These options specify whether another IP address update attempt should be made after a previous attempt failed, and how often the retry attempts should occur.

Timed Remote Manager connection

- **Enable Timed Remote Manager Connection**: When enabled, this Digi device initiates the connection to the Remote Manager Server at the configured interval (period). A timed connection defers to (will not disrupt) an established Remote Manager connection. If a timed connection defers to an existing Remote Manager connection, or if the Digi device server cannot successfully establish the timed connection, the Digi device server will try again at the next interval.
- **Remote Manager Server Address**: The IP address or hostname of the Remote Manager Server.

- **Connect every: H hrs M mins**: The interval (period) in hours and minutes in which the Digi device server attempts a timed connection to the specified Remote Manager Server.
- **After boot, wait before first timed connection**: When the Digi device server boots (starts up), you may observe a delay before the first timed connection is attempted. Choose one of the following options on how to handle the delay:
  - **Immediate**: Attempt first timed connection immediately.
  - **One Interval**: Attempt the first timed connection after one configured interval (period) has elapsed.
  - **Random Delay**: Attempt the first timed connection after a random interval of time between zero (immediate) and the configured interval (period). Choose this option when you have a number of Digi device deployed in a single location and you want to distribute the first Remote Manager timed connection attempt for each Digi device over time when power is restored after an outage.

Advanced Remote Manager settings

The default settings for Remote Manager remote management work for most situations. The advanced settings allow you to configure the idle timeout for the connection between the Remote Manager-registered device and Remote Manager, and the keep-alive settings of the various interfaces (TCP and HTTP for mobile and Ethernet network connections). You should only change the advanced settings when the defaults do not properly work.

- **Connection Settings**: These settings configure the idle timeout for the connection between the Remote Manager-registered device and Remote Manager.
  - **Disconnect when the Remote Manager Connection is idle**
    Idle Timeout: Enables or disables the idle timeout for the connection. When enabled, an idle connection ends after the amount of time specified in the **Idle Timeout** setting.
  - **Authenticate to Remote Manager with a password**
    Password: These fields are only applicable when your Remote Manager account was configured to expect a password from the Remote Manager-registered device. Typically, you can set this option through Remote Manager, since you need to configure the Remote Manager-registered device and Remote Manager identically.

- **Mobile (Cellular) Settings**
  Ethernet Settings
  WiFi Settings: These settings apply to device-initiated Remote Manager connections over mobile/cellular, Ethernet, and Wi-Fi networks. Each network type has these settings:

  - **Remote Manager Connection Keep-Alive settings**: These settings control how often to send keep-alive packets over the device-initiated connection to Remote Manager, and whether the Remote Manager-registered device waits before dropping the connection. Keep-alives for the Remote Manager connection serve three basic purposes:
    - Keep the Remote Manager connection alive through network infrastructure such as routers, NATs and firewalls.
    - Inform the other (remote) side of the Remote Manager connection that its peer is still active.
    - Test the Remote Manager connection to detect whether it has stopped responding and should be abandoned. Recovery actions are taken as configured in other settings.

    The Remote Manager-registered device and Remote Manager each perform their own independent monitoring of the Remote Manager connection state (active, idle and missed keep-alives). If Remote Manager protocol messages or data other than keep-alives is exchanged over the Remote Manager 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 Remote Manager if the Remote Manager connection is idle. Remote Manager expects to receive either Remote Manager protocol messages or keep-alive packets from the device at this interval.
  - **Server Send Interval**: Specifies how frequently the Remote Manager-registered device sends a keep-alive packet to Remote Manager if the Remote Manager connection is idle. Remote Manager expects to receive either Remote Manager protocol messages or keep-alive packets from the Remote Manager-registered device at this interval.

    Important Digi recommends that you set this interval value as long as your application can tolerate to reduce the amount of data traffic.

  - **Assume the 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 Remote Manager.

- **Connection Method**: Specifies the method by which the associated interface connects to Remote Manager.
  - **TCP**: Connect using TCP. This is the default connection method, and is typically good enough for most connections. It is the most efficient method for connecting to Remote Manager 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. This option tries each connection option until a connection is made. This connection method requires that you specify **HTTP over Proxy Settings**.
  - **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 you select when **Automatic** or **HTTP over Proxy** connection methods.
  - **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 used to sign in to the proxy host.
  - **Enable persistent proxy connections**: Specifies whether the Remote Manager-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 Remote Manager-registered device and Remote Manager using the 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.

Configure a Remote Manager-registered device to connect to Remote Manager

To manually configure the Device Management service for your Remote Manager-registered device to connect to Remote Manager:

1. Open the web interface.
2. Select **Configuration** > **Remote Manager**.
3. On the **Remote Manager Configuration** settings page, type the URL of the Remote Manager platform. For example, type **remotemanager.digi.com** in the **Remote Manager Server Address** field under **Device -Initiated Management Connection**.
4. Select the
   Automatically reconnect to Remote Manager after being disconnected check box.
5. Click **Apply**.

Manage alarms through Remote Manager

You can configure the alarms sent to Remote Manager. You can also view and manage alarms from the Remote Manager interface. See Alarms Configuration for more information.

Users

User settings involve several areas:

- **User authentication**: Whether authentication is required for users accessing the Digi Connect and ConnectPort TS Family device and the information required to access it. Depending on the Digi device, you can define multiple users and their authentication information. User authentication settings are on the Users settings page.
- **User access settings**: Device interfaces that a user can access, such as the command line or web interface.
- **User permissions settings**: Permissions a user has for accessing and configuring the device.
- Several settings on the **Network Configuration** pages are available to further secure the Digi Connect and ConnectPort TS Family product. For example, you can disable unused network services on the **Network Services** page.

About user models and user permissions

The Digi Connect and ConnectPort TS Family products provides the following user models:

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

To determine which user model to implement:

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.

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 and ConnectPort TS Family devices. That means a login prompt appears when you access the device by opening the web interface or issuing a **telnet** command. The default user name is **root** and the unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.

Disable password authentication

You can disable password authentication as needed.

To change a password from the web interface:

1. Select **Configuration** > **Users**.
2. On the **Users Configuration** page, select the **Enable password authentication** check box.
3. Click **Apply**.

To change a password from the command line:

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

Add a user

Digi Connect and ConnectPort TS Family devices allow you to define multiple users. For those products, the **Users Configuration** page shows the currently defined users and allows you to add users.

To add a user:

1. Select **Configuration** > **Users**.
2. Click **New user**.
3. On the **Add New User** page, complete the user authentication fields. You can specify a case-sensitive password from 4 through 16 characters long.
4. Click **Apply**. The changes take effect immediately. No logout/login is necessary.

Change user access settings

For Digi Connect and ConnectPort TS Family products 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 you can restrict other users to the web interface only.

CAUTION! Take care in changing access settings. If you sign in as the administrative user and disable the web interface, you will not be able to sign in to the Digi Connect and ConnectPort TS Family 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. Select **Configuration** > **Users**.
2. Click a user under **User Name**.
3. Click **User Access**.
4. 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.
5. 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 Connect and ConnectPort TS Family product. 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 Connect and ConnectPort TS Family product 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.

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 settings for all users, but does not have permission to modify or write the settings.
Read/Write Self	The user can read and write their own settings, but does not have permission to modify or write the settings for other users.
Read All/Write Self	The user can read the settings for all users and can modify their own settings.
Read/Write	The user has full permission to read and write the settings for all users.
Execute	The user has full permission to execute the settings.

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

To set user permissions, choose one of the following options:

- Set user permissions from the web interface:
  1. Select **Configuration** > **Users**.
  2. Click a user under **User Name**.
  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:

  Use the **set permissions** command to set permissions from the command-line interface. See the *Digi Connect® Family Command Reference* for the command description.

Control user access

This section provides information about additional methods for controlling user access.

Disable unused and non-secure network services

To further secure the Digi Connect and ConnectPort TS Family product, you can disable network services that are not required for the Digi device. You can disable non-secure or un-encrypted network services such as Telnet. See Network Services Settings.

Applications pages

Most Digi devices support additional configurable applications. Use the options under **Application** to configure applications. The application options vary depending on the Digi 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 Ekahau Client™.
- **RealPort**: Configures RealPort settings. See RealPort configuration for more information.
- **Industrial Automation**: Configures the Digi device for use in industrial automation applications.

Python Configuration

If you have a Python-enabled Digi Connect and ConnectPort TS Family device, you can manage Python files using the **Application** > **Python** menu options. Python options include:

- Uploading Python program files to the Digi Connect and ConnectPort TS Family device
- Deleting a Python program file from the device

- Configuring which Python programs to execute when the Digi Connect and ConnectPort TS Family device boots (also known as auto-start programs)

Python Files

The Python Files page allows you to upload and manage Python programs on a Digi Connect and ConnectPort TS Family device.

- **Upload Files**: Click **Choose File** to select a file to upload and click **Upload**.
- **Manage Files**: Select any files to remove from the Digi Connect and ConnectPort TS Family device and click **Delete**.

Auto-start settings

Use the **Auto-start Settings** page to configure Python programs to execute when the Digi Connect and ConnectPort TS Family device boots. You can configure up to four auto-start entries.

- **Enable:** When selected, the program specified in the Auto-start command line field runs when the device boots.
- **Auto-start command line:** Specify the name of a Python program file to be executed and any arguments to pass to the program using the following syntax:

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

Manually execute uploaded Python programs

To manually execute an uploaded Python program on a Digi Connect and ConnectPort TS Family device:

- Access the Digi device command-line interface and type the following command:

```
python filename [arg1arg2...]
```

View and manage Python programs

To view Python threads running on the Digi Connect and ConnectPort TS Family device:

- Access the Digi device command-line interface and type the **who** command.

Python program management and programming resources

Digi incorporates a Python development environment into Digi Connect and ConnectPort TS Family devices. Digi integration of the universal Python programming language allows customers an open standard for complete control of connections to devices, the manipulation of data, and event-based actions.

Recommended distribution of Python interpreter

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

Digi Python Programmer's Guide

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 those with Digi-specific behavior, and describes how to load and run Python programs onto Digi devices, and run sample Python programs.

Digi Wiki for Developers

Digi Wiki for Developers is where you can learn how to develop solutions using Digi's communications products, 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.

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. See the Digi Python wiki for more information.

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

Python support forum on www.digi.com

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

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

Device Integration Application (DIA)

The Remote Manager Device Integration Application (DIA) is software that simplifies connecting devices (for example, sensors or PLCs) 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, you can also execute DIA 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 (for example, ZigBee® sensors, wired industrial equipment, or GPS devices). It is an integral component of the Remote Manager platform, which customers can deploy with DIA software to build flexible, robust solutions with unprecedented speed.

Remote Manager and the device management service

Remote Manager allows for device management and access to device data within Remote Manager. Designed as an on-demand solution, Remote Manager customers pay only for services consumed, conserving capital and requiring no infrastructure. Remote Manager feature include:

- 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 Remote Manager. 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 Remote Manager and the services it provides, see the *Remote Manager User Guide* or go to www.digi.com/products/cloud/digi-remote-manager.

RealPort configuration

Install and configure RealPort software on each computer that uses the RealPort ports on the Digi device. The RealPort software is available for downloading from the Digi Support site. For complete information on installing and using RealPort software, see RealPort Installation Guide on the Digi Support site.

Install RealPort software

To install RealPort software from the Digi Support site:

1. Go to your product's support page:
   - Digi ConnectPort X2
   - Digi ConnectPort X4
   - Digi Connect SP
2. Click **Product Support** > **Drivers**.
3. From the **Operating System Specific Drivers** list box, select your operating system. A list of available downloads and release notes for your operating system appears.
4. Click the link for the RealPort zip file and save it to your computer.
5. Extract the files from the RealPort zip file and 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 then click **Install**.

3. Follow the Setup Wizard prompts to install RealPort.

   Enter the following information during setup of RealPort:

   - IP address of this Digi device server
   - RealPort TCP port number. (default is 771)

   See *RealPort Installation Guide* for additional information.

RealPort Settings

Use the **RealPort Configuration** page to configuring the RealPort application. The available settings are as follows:

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

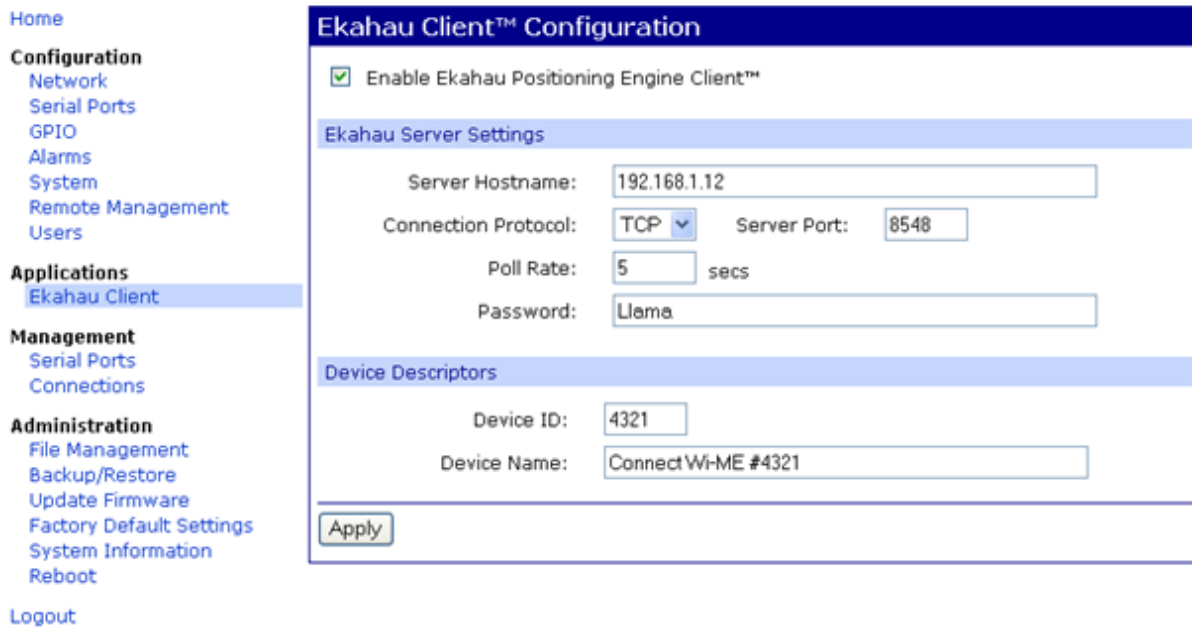
    Note that RealPort keep-alives generate additional traffic which may be undesirable in situations where traffic is measured for billing purposes.
  - **Enable Exclusive Mode**: Exclusive mode allows a single connection from any one RealPort client ID. If you enable this setting and a subsequent connection occurs that has the same source IP as an existing connection, the existing connection is forcibly reset under the assumption that it is stale.
- **Device Initiated RealPort Settings**:
  - **Index**: An empty list means there are no configured device-initiated RealPort connections.
  - **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™

Use the **Ekahau Client** page to configure Ekahau Client device-location software for a Digi devices with Wi-Fi capability.

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. When 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 does not 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**: The password used to authenticate with the server. The maximum length of this password 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 device name is 50 characters.

Industrial Automation-Modbus-Bridge

Industrial Automation is supported in the following 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.

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* available on the Digi Support site.

Known limitations

- You can use Digi RealPort only when 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 you want traditional Router/NAT function for Modbus/TCP port 502.

Enable or disable Modbus Bridge

To enable or disable Modbus Bridge, choose one of the following options:

- To disable the Modbus Bridge, select a different port profile than Industrial Automation.
- To enable Modbus Bridge, reselect the Industrial Automation port profile.

> **Note** Any specialized settings configured using the **set ia** commands are lost when you disable the Modbus bridge. You must reconfigure these settings when you re-enable the Industrial Automation port profile.

Configuration through Digi Remote Manager

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

See the *Remote Manager User Guide* for details on:

- Using Remote Manager as a management interface
- Creating a Remote Manager account
- Adding your Digi Connect and ConnectPort TS Family device to the Remote Manager device list so you can manage it from that interface

IPv6 support

Select Digi products support Internet Protocol version 6 (IPv6), electronic devices use this network layer standard to exchange data across a packet-switched network. IPv6 is provides more addresses for networked devices than IPv4.

The primary change from IPv4 to IPv6 is the length of network addresses. IPv4 address are 32 bits long. In contrast, IPv6 addresses are 128 bits long and are typically composed of two logical parts: a 64-bit network prefix and a 64-bit host part, which is either automatically generated from the interface's MAC address or assigned sequentially.

IPv6 addresses are normally written as eight groups of four hexadecimal digits. For example: 3002:0ff2:63a5:0db8:42ae:0040:02de:3560. You can omit leading zeros in a group. If a four-digit group is 0000, the zeros may be omitted, and that part of the address shortened to two consecutive colons, provided you use only one double colon in the address. You can write a sequence of four bytes at the end of an IPv6 address in decimal, using dots as separators.

IPv6 networks are written using CIDR notation.

An IPv6 network (or subnet) is a contiguous group of IPv6 addresses the size of which must be a power of two; the initial bits of addresses which are identical for all hosts in the network are called the network's prefix.

A network is denoted by the first address in the network and the size in bits of the prefix, separated with a slash. For example, 2001:1234:5678:9ABC::/64 stands for the network with addresses 2001:1234:5678:9ABC:: through 2001:1234:5678:9ABC:FFFF:FFFF:FFFF:FFFF.

Because you can see a single host as a network with a 128-bit prefix, you will sometimes see host addresses written followed with /128.

Implementation of IPv6 in Digi products means that there are more ways in which you can express addresses for devices and destinations:

- As an IPv4 address, for example 10.8.118.3.
- As an IPv6 address in any of its accepted notation formats, including address notation with special meanings, for example, 3002:0ff2:63a5:0db8:42ae:0040:02de:3560,
- As a Fully Qualified Domain Name (FQDN), for example www.myhost.com or remote3.digi.com. Use of an FQDN assumes there is a DNS server somewhere to resolve the name. For a DNS server, it does not make sense to talk about a Fully Qualified Domain Name for it, since the server itself is doing the resolving of names.

Digi's implementation of IPv6 supports a *dual stack*. That is, each Digi device will have an IPv4 address and potentially several IPv6 addresses:

- Link-local address: similar to AutoIP.
- Site-local address: router-assigned.

Important Digi's IPv6 implementation *does not* allow assignment of static IPv6 addresses. A Digi device gets either a link-local or site-local address.

Alternative configuration options for Digi Connect Wi-SP

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

Configure the network using an access point

To configure the network using an access point (infrastructure mode with SSID -Connect) for Digi Connect Wi-SP:

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 on your computer and proceed with the configuration.

Configure the wireless card without an access point

To configure the wireless card without an access point (Ad-Hoc mode with SSID - Connect) for Digi Connect SP:

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 you computer and proceed with the configuration.

Set DIP switches on Digi Connect SP\Wi-SP

Digi Connect SP and Digi Connect Wi-SP have a set of DIP switches on the underside of the device for setting the EIA mode for serial communications.

To set the DIP switches on Digi Connect Wi-SP (or SP):

1. Disconnect the power supply.

   Note ALWAYS disconnect the power supply before resetting the DIP switches.

2. Set the Digi Connect Wi-SP DIP switches in the On or up position. The following image shows the DIP Switch settings required 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. For example, select **Start** > **Accessories** > **Communication** > **Hyperterm** and type a name for the connection.
5. Select COM1 and click **OK**.

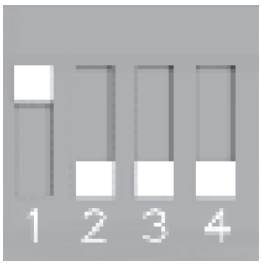
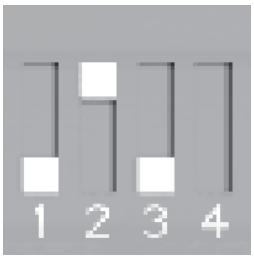
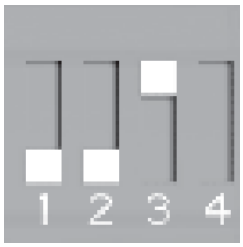
6. Set the port settings to **9600**, **8**, **None**, **1**, **None** (default settings), click **Apply** and then click **OK**.

7. Type the default user name, **root**, and the default password. The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.
8. Use the **set wlan** command to configure wireless network settings. This command is described in the *Digi Connect and ConnectPort TS 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 configure the Digi Connect Wi-SP for your network.

Note The Digi support website at www.digi.com/support provides additional command resources.

Set DIP switches example

Set these DIP switches according to your serial device requirements (EIA-232/422/485).

Up/On **Down/Off**			
DB-9 pin	**EIA-232**	**EIA-422/485 Full-duplex**	**EIA-485 Half-duplex**
1	DCD	CTS-	Not used
2	RxD	RxD+	RxD+
3	TxD	TxD+	TxD+
4	DTR	RTS-	Not used
5	GND	GND	GND
6	DSR	RxD-	RxD-
7	RTS	RTS+	Not used
8	CTS	CTS+	Not used
9	RI	TxD-	TxD-
Shell	GND		

Batch configuration capabilities

If you need configure multiple Digi devices, use the batch configuration capabilities to upload configuration files 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.

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.

Command	Description
connectprog /info /destip=<*ip address*> /username=root /password=<*password*>	Displays device information for the specific device. Where <*password*> is: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.
connectprog /backup /destip=<*ip address*> /username=root /password=<*password*>	Backs up the complete device configuration to config.rci in the local directory. Where <*password*> is: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.
connectprog /upload /destip=<*ip address*> /config=<*directory path*>\<*file name*>.txt /username=root /password=<*password*>	Uploads the configuration file to the device. Where <*password*> is: The unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator.

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.
```

Configure and manage the device using the Digi Connect and ConnectPort TS Family command line interface

You can issue commands from the command line to configure, manage, and monitor Digi Connect and ConnectPort TS Family devices. For a description of the complete command set, see *Digi Connect® Family Command Reference*.

This section gives some basics for using the command line interface, as well as listing some commonly used commands by function.

Configuration through the command line

You can configure the Digi Connect and ConnectPort TS Family product by entering a series of command to set values through the command-line interface.

Access the command-line interface

To access the command-line interface and send configuration commands to the Digi Connect and ConnectPort TS Family device:

1. Launch the command-line interface by using the **telnet** command.
2. To launch the CLI via telnet, issue the following **telnet** command from a command prompt on another networked device, such as a server:

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

Replace *ip-address* with the IP address of the Digi Connect and ConnectPort TS Family device. For example:

```
#> telnet 192.3.23.5
```

If security is enabled for the Digi Connect and ConnectPort TS Family device, a login prompt appears for telnet access. If you do not know the user name and password for the device, contact the system administrator who originally configured the device.

Basics for using the command-line interface

The Digi Connect and ConnectPort TS Family offers online help for CLI commands. Use the following command examples to get help for using commands.

- **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.

Basics for using the command-line interface

The Digi Connect and ConnectPort TS Family offers online help for CLI commands. Use the following command examples to get help for using commands.

- **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.

Management through the command line interface

This section provides information on some key commands available from the command line interface.

For more information, see the *Digi Connect Family Command Reference* on www.digi.com.

Use the following commands to display information and statistics:

- display
- flashdrv
- info
- set alarm
- set buffer and display buffer
- set gpio
- set snmp
- show

Use the following commands to manage connections and sessions:

- close
- connect
- exit and quit
- reconnect
- rlogin
- send
- status
- telnet
- who and kill

Use the following commands to configure the product:

- newpass
- send mode
- set alarm
- set autoconnect
- set buffer and display buffer
- set forward
- set gpio
- set group
- set host
- set mgmtconnection
- set mgmtglobal

- set mgmtnetwork
- set network
- set permissions
- set pmodem
- set pppoutbound
- set profiles
- set realport
- set rtstoggle
- set serial
- set service
- set snmp
- set system
- set tcpserial
- set udpserial
- set user
- set wlan

close

Use the **close** command to close active sessions that were opened by **connect**, **rlogin**, and **telnet** commands.

connect

Use the **connect** command to establish a connection with a serial port.

display

Use the **display** commands to 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. These include 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**).
- Logged serial data (**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**).
- Uptime information (**display uptime**).

exit and quit

Use the **exit** and **quit** commands to terminate a currently active session.

flashdrv

Use the **flashdrv** command to access the Memory Module connected to the USB port on the ConnetPort TS 8/16 and view the available memory size.

info

Use the **info** commands to display statistical information about a device over time. The statistics displayed are those gathered since the tables containing the statistics were last cleared. The type of statistics include:

- Device statistics. The **info device** command displays such details as product, MAC address, boot, POST, and firmware versions, memory usage, utilization, and uptime.
- Ethernet statistics. The **info ethernet** command 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 was reset
  - The number of incoming bytes when the protocol was unknown
- ICMP statistics. The **info icmp** command displays the number of messages, bad messages, and destination unreachable messages received.
- Serial statistics. The **info serial** command displays the following information:
  - Number of bytes received and transmitted
  - Signal changes
  - FIFO and buffer overruns
  - Framing and parity errors
  - Breaks detected

- TCP statistics. The **info tcp** command displays the following information:
  - 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
  - The number of established connections that were reset
- UDP statistics. The **info udp** command displays the following information:
  - The number of datagrams received or sent
  - The number of bad datagrams received
  - The number of received datagrams that were discarded because the specified port was invalid
- Wireless statistics. The **info wlan** command displays detailed statistics for wireless devices that may aid in troubleshooting network communication problems with a wireless network.

newpass

Use the **newpass** command to issue a new password to a user.

ping

Use the **ping** command to test whether a host or other device is active and reachable.

reconnect

Use the **reconnect** command to reestablish a connection opened by a **connect**, **rlogin**, or **telnet** command. By default, the **reconnect** command reestablishes the connection to the last active session.

rlogin

Use the **rlogin** command to sign in to a remote system.

send

Use the **send** command to send a telnet control command, such as break, abort output, are you there, escape, or interrupt process, to the last active telnet session.

send mode

Use the **send mode** command to configure the telnet control commands. For example, send telnet control command to last active telnet session or set telnet operating options.

set alarm

Use the **set alarm** command to display alarm settings, including conditions that trigger alarms, and how alarms are sent. You can configure alarms to be sent as either an email message, an SNMP trap,

or both. You can configure the alarms as needed.

set autoconnect

Use the **set autoconnect** command to configure the autoconnection behaviors for serial port connections.

set buffer and display buffers

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

set forward

Use the **set forward** command to configure IP forwarding.

set gpio

Use the **set gpio** to display current GPIO pin settings. You can reconfigure the pin settings as needed.

set group

Use the **set group** command to configure create, establish, update, or remove group attributes.

set host

Use the **set host** command to configure the host name for the Digi device.

set mgmtconnection

Use the **set mgmtnetwork** command to configure the Remote Manager connection settings.

set mgmtglobal

Use the **set mgmtglobal** command to configure the Remote Manager global settings.

set mgmtnetwork

Use the **set mgmtnetwork** command to configure the Remote Manager network settings.

set network

Use the **set network** command to configure the network options.

set permissions

Use the **set permissions** command to configure the user permissions for various services and command-line interface commands.

set pmodem

Use the **set pmodem** command to configure the modem emulation.

set pppoutbound

Use the **set pppoutbound** command to configure the PPP outbound connections.

set ppp

Use the **set ppp** command to configure PPP connections.

set profiles

Use the **set profiles** command to configure the port profile for a serial port.

set radius

Use the **set radius** command to start, stop, and set RADIUS authentication.

set realport

Use the **set realport** command to configure RealPort.

set rtstoggle

Use the **set rtstoggle** command to configure the RTS toggle.

set serial

Use the **set serial** command to configure the serial port options.

set service

Use the **set service** command to configure the network services.

set snmp

Use the **set snmp** command to configure SNMP, including SNMP traps, such as:

- Authentication failure
- Cold start
- Link up
- Login traps

The **set snmp** command also displays current SNMP settings.

set system

Use the **set system** command to configure the system identifying information.

set tcpserial

Use the **set tcpserial** command to configure serial TCP.

set udpserial

Use the **set udpserial** command to configure the serial UDP.

set user

Use the **set user** command to configure a user.

set wlan

Use the **set wlan** command to configure wireless devices.

set wlan

Use the **set wlan** command to configure wireless devices.

status

Use the **status** command to display a list of sessions or outgoing connections made by the **connect**, **rlogin**, or **telnet** commands for a Digi device. Use the **status** command to determine which of the current sessions to close.

show

Use the **show** commands to display current settings on a Digi device.

telnet

Use the **telnet** command to establish an outgoing telnet connection, also known as a session.

who and kill

Use the **who** command to display a global list of connections. The list of connections includes those associated with a serial port or the command-line interface.

Use the **kill** command to terminate active connections based on the ID number returned from the who results.

Use the **who** command to determine any connections that are no longer needed, and end the connections by issuing a **kill** command.

Administration

You can issue commands from the command-line interface to administer Digi Connect and ConnectPort TS Family products. The following table displays several administration tasks and the commands used to perform them. See the *Digi Connect® Family Command Reference* for more complete command descriptions.

Administrative task	Command
Backup/restore a configuration from a TFTP server on the network	**backup**
Update firmware	**boot** To update the firmware: 1. Telnet to the Digi device command-line interface using a telnet application or hyperterm. 2. A login prompt appears. The default user name is **root** and the unique default password is printed on the device label. If the password is not on the device label, the default password is **dbps**. If neither of the defaults work, the password may have been updated. Contact your system administrator. 3. If you are at the bash shell, type **configshell** to get to the config shell. 4. Issue the **boot load** command: `#> boot load=tftp-server-ip:filename` Replace *tftp-server-ip* with the IP address of the TFTP server that contains the firmware, and replace *filename* with 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**

Remote Manager monitoring capabilities

You can monitor and manage Digi Connect and ConnectPort TS Family products from Remote Manager. For example, you can:

- Display 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.
- Manage mobile settings.
- Monitor the state of the device's connection and see a connection report and connection history statistics.
- Redirect devices to a to a different destination.
- Disconnect devices.
- Remove devices from the network.

To learn more about Remote Manager and the services it provides, see the *Digi Remote Manager User Guide*.

Remote Manager device management

From the Remote Manager'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.

SNMP device monitoring capabilities

SNMP provides the following device monitoring capabilities:

- 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

You can use this information to manage network performance, gather device statistics, and find and solve network problems.

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

Supported RFCs and MIBs

Digi Connect and ConnectPort TS Family supports the following SNMP-related Request for Comments (RFCs) and Management Information Bases (MIBs):

- **Standard RFCs and MIBs**
  - RFC 1213—Management Information Base (MIB) II manages a TCP/IP network. 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. See www.ietf.org/rfc/rfc1213.txt for more information.
  - RFC 1215—Generic Traps (coldStart, linkUp, authenticationFailure, login only). See www.ietf.org/rfc/rfc1215.txt for more information.
  - RFC 2790—Host Resources MIB for use with managing host systems, where “host” means any computer that communicates with other similar computers attached to the Internet. See tools.ietf.org/html/rfc2790 for more information.

- **DIGI enterprise MIBs**
  - DIGI CONNECT DEVICE INFO MIB—A 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.
  - Digi Connect Mobile Information MIB—A Digi enterprise MIB for handling and displaying device information for mobile devices.
  - Digi Connect Wireless LAN MIB—A Digi enterprise MIB for handling and displaying basic device information for wireless devices.
  - DIGI SERIAL ALARM TRAPS MIB—A Digi enterprise MIB for sending alarms as SNMP traps.
  - Digi Login Traps MIB—A Digi enterprise MIB that indicates when users attempt to sign into the device, and whether the attempt was successful.
  - Digi Structures of Management MIB—A Digi enterprise MIB that provides data structures for managing hosts and gateways on a network.
  - Digi Connect Mobile Traps MIB—A Digi enterprise MIB for sending alarms as SNMP traps for mobile devices.
  - Digi Connectware Notifications MIB—This Digi enterprise MIB may be required by some SNMP import facilities, as other MIBs may refer to it.

  See Download a Digi MIB for instructions on downloading a Digi MIB from the Digi website.

SNMP configuration

You can configure basic network and serial configurations for Digi Connect and ConnectPort TS Family devices through SNMP:

- Use a subset of standard MIBs for network and serial configuration. See Supported RFCs and MIBs for more information on supported MIBS.
- Use Digi enterprise MIBs for device identification, alarm handling, and Digi Connect and ConnectPort TS Family-specific configurations.

To use the MIBS, you must load MIBs into a network management station (NMS).

Note that some SNMP configuration settings can be configured only from the web or command line interfaces. For example, to send alarms as SNMP traps:

- In the web interface, use the **Configuration > Alarms > *alarm* > Alarm Destinations > Send SNMP trap to following destination when alarm occurs** option. See Alarms Configuration.
- In the command-line interface, use the **set alarm** option **typescript**. See the **set alarm** command description in the *Digi Connect® Family Command Reference* on www.digi.com.

Note You cannot configure all network and serial configurations using SNMP. For more advanced configuration settings, use the web or command-line interfaces.

Download a Digi MIB

To download a Digi MIB:

1. Locate the support page for your product:
2. Under Product Support, click the **Utilities** tab.
3. Locate the MIB you want to view under **General Diagnostics, Utilities, and MIBs**.

Supported SNMP traps

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

- Authentication failure
- Login
- Cold start
- Link up
- Alarms issued in the form of SNMP traps

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.

From the web interface, you can enable/disable traps at **Configuration** > **System** > **SNMP** > **Enable Simple Network Management Protocol (SNMP) traps**.

You can configure alarms at **Configuration** > **Alarms** > **Alarm Conditions** > **Alarm *n*** > **Alarm Destinations** > **Send SNMP trap to following destination when alarm occurs**.

Latency tuning

This section discusses latency and provides 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.

Achieving deterministic IP performance

Use the following recommended process to achieve deterministic IP networking behavior. This process uses Digi commercial off-the-shelf firmware and hardware, and does not use 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. To achieve deterministic IP networking behavior:

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 IP networking behavior

The best-case scenario for achieving deterministic 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?
- What is the 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

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 ensure 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.

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 and ConnectPort TS 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. 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.

Hardware

This section details requirements and recommendations for Digi Connect and ConnectPort TS Family products. See also Specifications and certifications and System status LEDs.

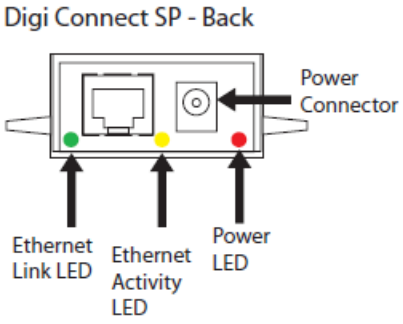
For the Digi Connect ES, see the *Digi Connect ES Hardware Setup Guide*. For all other Digi Connect and ConnectPort TS Family products, see their *Hardware Reference Manuals* for hardware-installation details.

System status LEDs

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

Digi Connect SP

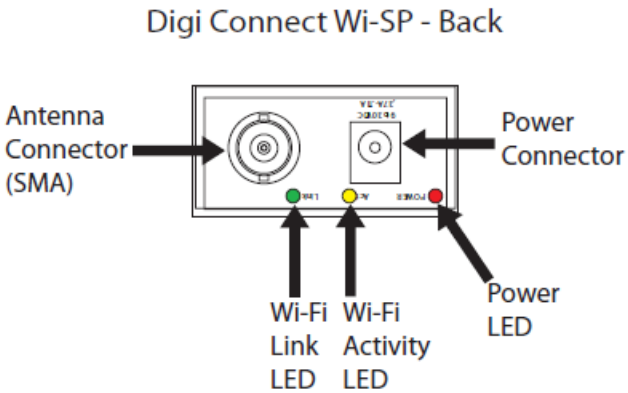
Digi Connect SP has three LEDs: Ethernet Link and Ethernet Activity, which are connected directly to the hardware; and the Power LED, which is software programmable.



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. By default, 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.

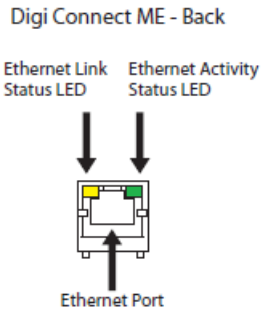


LED/button	Color and Light Pattern	Description
Wi-Fi Link Status LED	Solid green	Unit is associated with an access point.
	Green, blinking slowly	Unit is in ad hoc mode.
	Green, blinking quickly	Unit is scanning for a network
Wi-Fi Activity Status LED	Solid yellow	Bad initialization
	Off	The Wi-Fi link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

Digi Connect ME

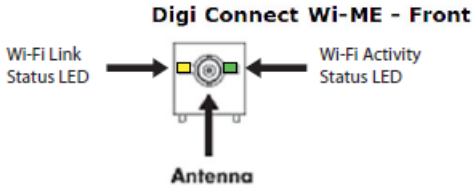
The Digi Connect ME module has two LEDs that are located near the upper corners of the Ethernet port (see the following figure).

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.

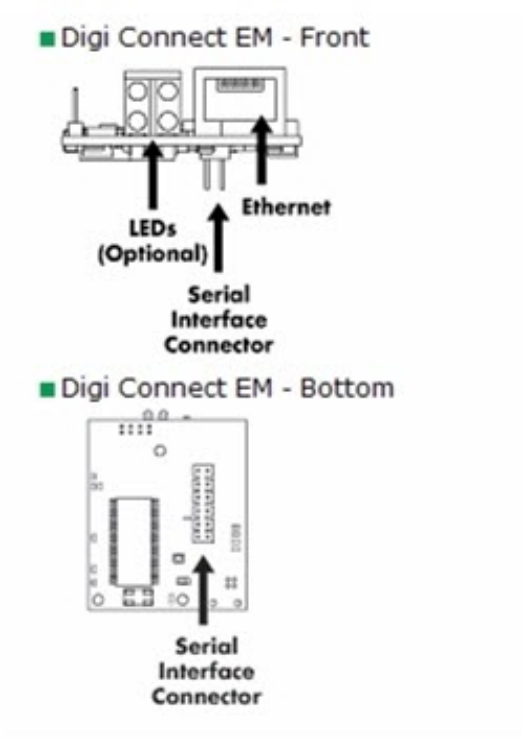
Digi Connect Wi-ME

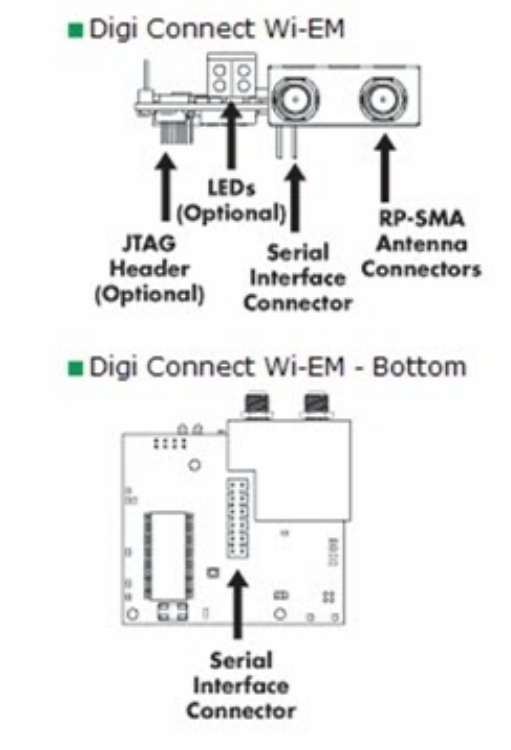


LED/button	Color and Light Pattern	Description
Wi-Fi Link Status LED	Solid yellow	Unit is associated with an access point.
	Yellow, blinking slowly	Unit is in ad hoc mode.
	Yellow, blinking quickly	Unit is scanning for a network.
Wi-Fi Activity Status LED	Off	The Wi-Fi link is idle.
	Blinking green	Wi-Fi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





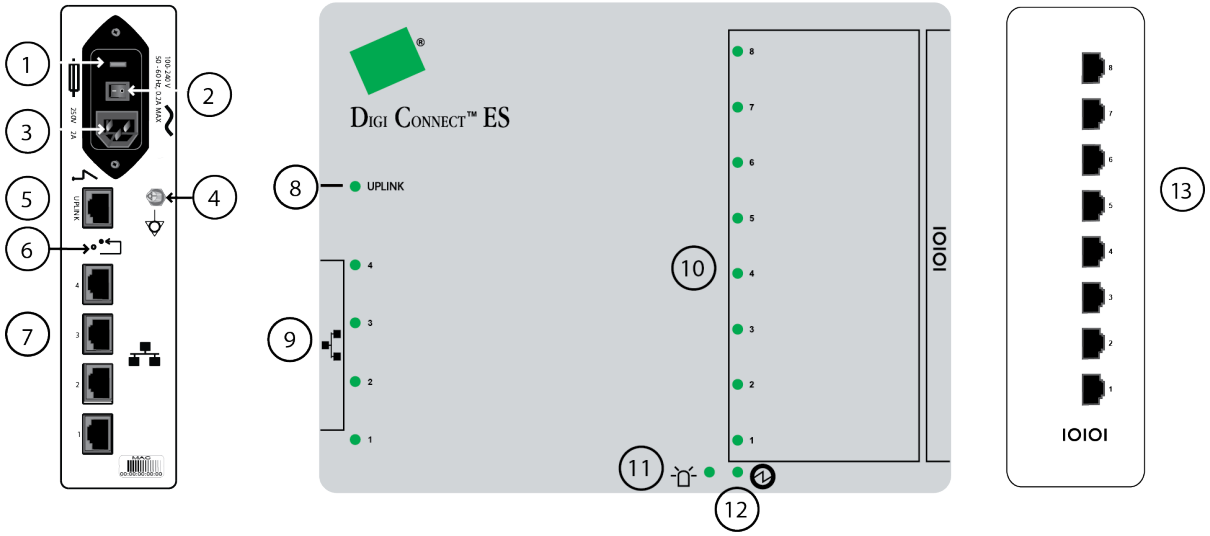
LED Behaviors				
LED	**Pin Header EM**	**Integration Kit Digi Connect EM**	**Integration Kit Digi Connect Wi-EM**	**Development Kit**
Top left (green)	1 (+) 3(-)	Serial port activity: **Off**: The serial channel is idle. **Blinking**: Serial data is transmitted or received.		This LED is software programmable
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)
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 48 SB and Digi Connect 4/8 SB with switch

Digi Connect ES connectors, LEDs, and controls

Attention: Consult accompanying documentation

Dangerous Voltage



1 - Fuse (250V 2A)

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

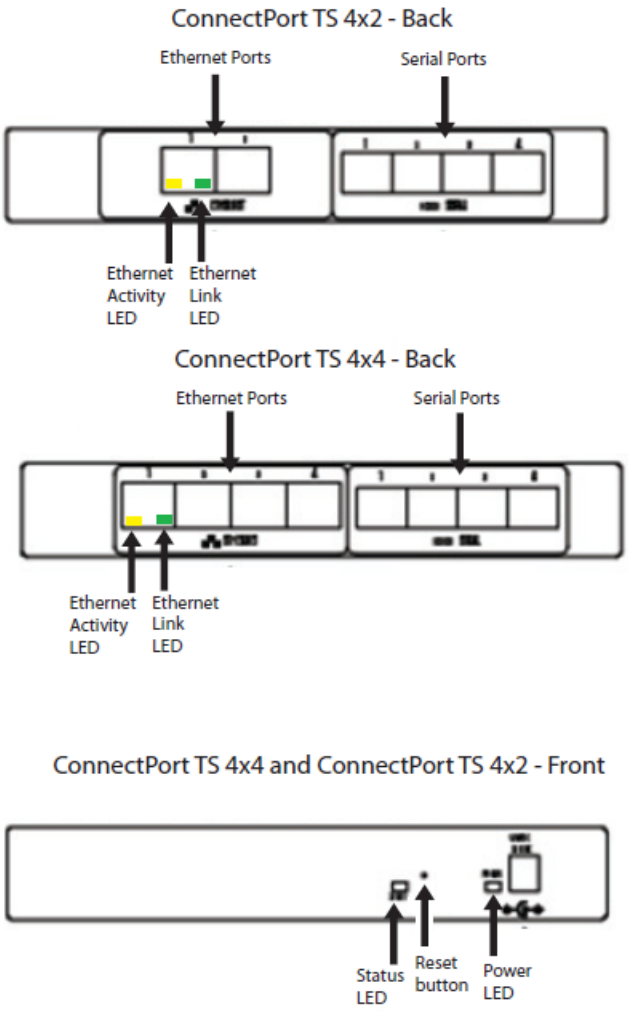
13 - Serial ports - 4 or 8

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

ConnectPort TS 4x4



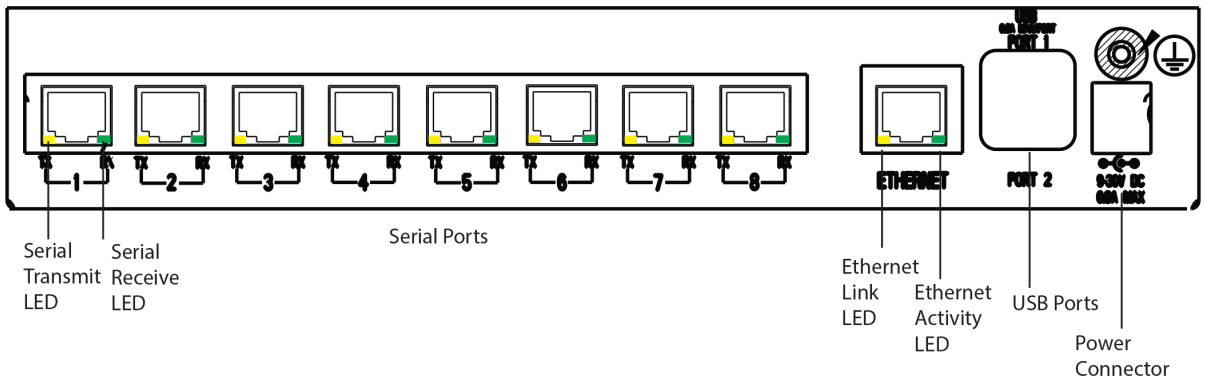
LED/button	Color and Light Pattern	Description
Power LED	Solid Green	Power on.
Fuse Good LED	Solid Green	Power on and the fuse is good. If this LED is not illuminated when power is applied, the fuse is blown and needs to be replaced.

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	Initializing firmware.
	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	Serial port is transmitting data.
Serial RX	Green	Serial port is receiving data.
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

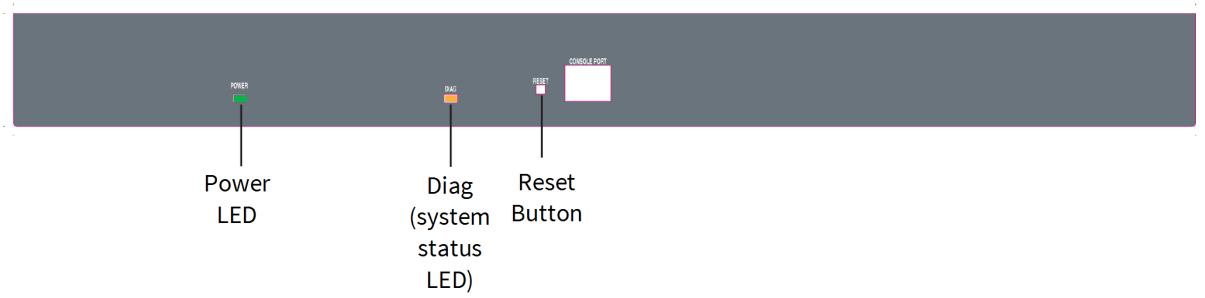
ConnectPort TS 8 and ConnectPort TS 8 MEI - Serial Port Side

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 -



Hardware: ConnectPort TS 8/16

Item	Description
Serial ports	You can configure the device to allow network administrators to access serial ports from the LAN. See Serial ports configuration.

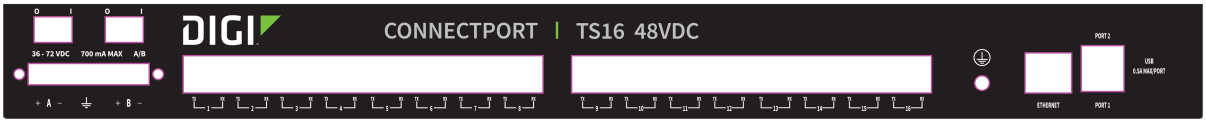
Item	Description
Ethernet port	Configure the Ethernet port.
USB ports	Use the USB port to connect a flash drive to the device. You can use the flashdrv command to view information about the flash drive.
Power Connector	Connect a power source to the device.
Reset button	Reset the factory settings on a Digi Connect and ConnectPort TS Family product using the Reset button.

LEDs: ConnectPort TS 8/16

LED/button	Color and Light Pattern	Description
Power LED	Solid Green	Power on.
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	Initializing firmware.
	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	Serial port is transmitting data.
Serial RX	Green	Serial port is receiving data.
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



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.

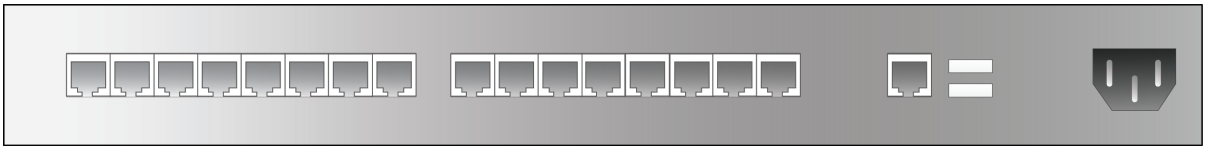
Temperature

- 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.

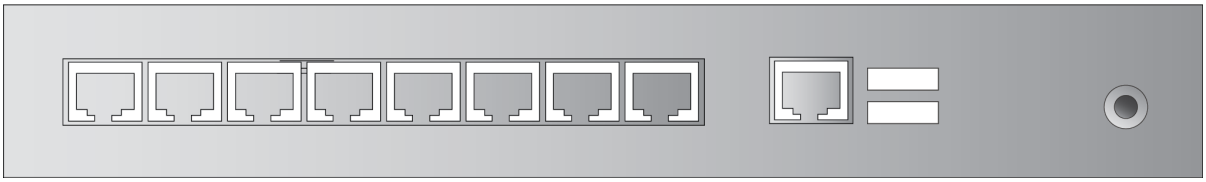
Power and wiring

- 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.

Specifications and certifications

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

Hardware specifications

This section provides the hardware specifications for all products in the Digi Connect and ConnectPort TS Family.

For more detailed hardware specifications, see the *Hardware Reference Manual* and datasheet for your Digi Connect and ConnectPort TS Family product. The specifications provided in this section apply to products that do not include a 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 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	2.0 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
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 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
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

Specification		Value
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	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 (6560 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

Wireless networking features

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

Wireless feature	Specification
Standard	802.11bg
Frequency	2.4 GHz
Data Rates	Up to 54 Mbps with automatic rate fallback

Wireless feature	Specification
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) 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 Wi-Fi LAN Statistics.
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.

Digi Connect and ConnectPort TS Family regulatory information and certifications

This section documents Digi Connect and ConnectPort TS Family regulatory information and certifications.

RF exposure statement

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

The Digi Connect and ConnectPort TS 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)

- FCC Part 15 Class B
- Radio Frequency Interface (RFI) (FCC 15.105)
- Labeling Requirements FCC (15.19)

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 Interface (RFI) (FCC 15.105)

This device has been tested and found to comply with the limits for Class B digital devices pursuant to Part 15 Subpart B, 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 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.

If the FCC ID is not visible when installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module FCC ID.

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 Emmissions/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	■ CAN/CSA C22.2 No. 60950-1-3 ■ UL60950-1 ■ 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 ■ EN/IEC 62368-1 ■ CSA/UL 62368-1:2014

Product	Emissions	Immunity	Safety
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 ■ EN/IEC 62368-1 ■ CSA/UL 62368-1:2014
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 section provides information on resources and processes available for troubleshooting your Digi device.

Troubleshooting resources

Use the troubleshooting information in this section to resolve your issue with your Digi device. If you cannot resolve the issue using the information in this section, there are several resources you can use to resolve your issue on the Digi Support site.

To resolve a problem from the Digi Support site:

1. Visit Digi's Knowledge Base at knowledge.digi.com/ and search for articles related to your situation.
2. Visit our support forums at www.digi.com/support/forum/ and search for posts from other users with similar situations.
3. Complete a support ticket via email to tech.support@digi.com.
   You will need to create a user account if one is not already set up.
4. To obtain direct assistance for your issue within a four hour time period, log in to your paid support account (or create one) at www.digi.com/support, and submit a support ticket.