ConnectPort LTS

User Guide

Revision history—90001001

Revision	Date	Description
E	May 2013	Added information on the banner feature.
F	December 2016	■ Updated the branding. ■ Added Ethernet bridging feature. ■ Expanded information under Configure the device using the ConnectPort LTS web interface.
G	May 2017	Removed the Declarations of conformity information from the Specifications and certifications chapter.
H	July 2018	Added pin-out information.
J	December 2019	Added information about the unique, default password printed on the device label.

Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2019 Digi International Inc. All rights reserved.

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

Network connections and data paths

Overview: Configuration, monitoring, and administration

Digi Device Discovery utility

Configure the device using the ConnectPort LTS web interface

Configure and manage the device using the ConnectPort LTS command line interface

Simple Network Management Protocol (SNMP)

ConnectPort LTS LCD interface

ConnectPort LTS disaster recovery

ConnectPort LTS hardware specifications

ConnectPort LTS regulatory information and certifications

About this guide

This guide describes how to install, provision, configure, monitor, and administer ConnectPort LTS devices. The guide covers the following products:

- ConnectPort LTS 8 and ConnectPort LTS 8 MEI
- ConnectPort LTS 8 W and ConnectPort LTS 8 MEI W
- ConnectPort LTS 16 and ConnectPort LTS 16 MEI
- ConnectPort LTS 16 W and ConnectPort LTS 16 MEI W
- ConnectPort LTS 16 MEI 2AC
- ConnectPort LTS 32 and ConnectPort LTS 32 MEI
- ConnectPort LTS 32 W and ConnectPort LTS 32 MEI W

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:

- *RealPort® Installation Guide*

For product support resources visit the following support pages:

For additional information, see the following resources:

- Online help and tutorials in the web interface for the Digi device
- Digi Python Wiki

- 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

ConnectPort LTS features

This section provides an overview of ConnectPort LTS features.

ConnectPort LTS Family

ConnectPort LTS (Linux Terminal Server) devices provide serial over Ethernet connectivity for applications. They support IPv4 and IPv6 Ethernet protocols. ConnectPort LTS MEI is the same size as ConnectPort LTS (RS-232 only version).

User interfaces

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

- Web-based interface
- Command-line interface available via local serial port, telnet or SSH
- Simple Network Management Protocol (SNMP)
- LCD panel

For additional details on these user interfaces, see Overview: Configuration, monitoring, and administration. You can customize some of the user interfaces.

Hardware and network interface features

For detailed hardware specifications and network interface information, go to:

www.digi.com/products/serial-servers/serial-device-servers/connectportlts#specifications

See also the datasheet for your Digi device.

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
- Secure Shell Server (SSH)

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

Serial data communication over TCP and UDP

ConnectPort LTS 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.
- 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) is a protocol for managing and monitoring network devices. SNMP architecture enables a network administrator to manage nodes—servers, workstations, routers, switches, hubs, and so on—on an IP network; manage network performance, find and solve network problems, and plan for network growth. For more information on SNMP as a device-management interface, see Simple Network Management Protocol (SNMP).

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

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

Telnet

ConnectPort LTS devices support the following types of telnet connections:

- Telnet client
- Telnet server
- Reverse telnet, often used for console management or device management
- Telnet autoconnect

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 ConnectPort LTS 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 ConnectPort LTS products attached to a network by

sending out a multicast packet. The ConnectPort LTS 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.

Secure Shell (SSH)

ConnectPort LTS products support Secure Shell (SSH) as a connection method and the following types of SSH connections: Reverse SSH and SSH Autoconnect. Limited use of SSH via SSH client is available from the Linux command line/bash shell. For more information on these connections, see Network connections and data paths. You can enable or disable access to Secure Shell network services.

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

ConnectPort LTS 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 ConnectPort LTS products to issue alarms, in the form of email messages or SNMP traps, when certain device events occur, including 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

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

Ethernet bridging

You can use Ethernet bridging to join multiple Ethernet networks together so that the joined networks appear as one Ethernet network. Ethernet bridging combines an Ethernet interface with one or more physical Ethernet interfaces under the umbrella of a single bridge interface. The Ethernet bridge is a software switch that can connect multiple Ethernet interfaces (physical or virtual) on a single machine while sharing a single IP subnet.

Use the script file, **brmode** (/etc/init.d/brmode), to enable or disable Ethernet bridging. (Ethernet bridging is supported only through the command line interface.)

To enable Ethernet bridging, run the following command:

```
# service brmode start
```

The IP address of the eth0 interface becomes the common IP address for the bridging mode interface (br0).

After enabling Ethernet bridging, the eth0 and eth1 addresses disappear. There is a delay of a few minutes while the system automatically changes the physical interface from the Ethernet 1 port to Ethernet 2 port.

Note Enable the eth1 (IP address #2) interface before starting Ethernet bridging.

To disable Ethernet bridging, run the following command:

```
# service brmode stop
```

To customize Ethernet bridging options, modify **/etc/init.d/brmode**. See the **brctl** Linux manpage for details.

To remove bridging messages from the serial console, run the following command:

```
# brctl setageing br0 0
```

To automatically start the Ethernet bridging service at each boot, add the following commands to the **rc.user** file:

```
service brmode start
brtcl set ageing br0 0
```

For more information on using the **rc.user** file, see Using the rc.user file and the Digi Knowledgebase.

Security features in Digi devices

This section covers ConnectPort LTS 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, telnet, and Secure Shell (SSH).
- Control access to inbound ports.
- 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 ConnectPort LTS 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/V1.2-based encryption:
  - DES (58/64-bit)
  - 3DES (168/192-bit)
  - AES (128/156/192/256-bit)

SNMP security

SNMP security options include:

- 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 (SNMPv1/v2c).
- You can use SNMPv3 support for enhanced security through SNMP.

Configuration management

Once a ConnectPort LTS 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.

Get started with ConnectPort LTS products

This section walks you through configuring an IP address and signing in to your ConnectPort LTS device.

Configuring IP addresses

The IP address mode determines how IP addresses are assigned. There are two modes for assigning IP addresses:

- **Dynamic:** Allows IP addresses to be automatically assigned using the Dynamic Host Configuration Protocol (DHCP) and/or Auto Private IP Addressing (APIP or AUTO IP).
- **Static:** Requires you to assign a static IP address using any available configuration interface.

By default, ConnectPort LTS devices are configured to dynamically assign addresses using DHCP.

Even if a DHCP server is available for dynamically assigning IP addresses, static addresses may work better for your network configuration. Once set, static IP addresses do not change and other network devices can always find the device by its IP address. With dynamic settings, the DHCP server can change the IP address frequently or infrequently depending on how your network administrator has configured the network.

When the IP address changes, network devices configured to talk to the ConnectPort LTS device can no longer access the device. In this case, you must locate the Digi device using the Digi Device Discovery utility and reconfigure the other network devices that need to communicate with the ConnectPort LTS device.

The following table summarizes methods for assigning an IP address.

Method	Description
Digi Device Discovery Utility	Use the Digi Device Discovery utility to search for and display Digi device, as well as change configuration settings. See Use Digi Device Discovery utility to sign in to the web interface.
LCD panel	Use the LCD panel on ConnectPort LTS products to perform basic configuration tasks, including setting the IP address, as well as monitoring and diagnostics tasks. See ConnectPort LTS LCD interface.
Dynamic Host Configuration Protocol (DHCP)	Use DHCP from the web interface to automatically assign IP addresses, to deliver IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information. All ConnectPort LTS devices have a DHCP client enabled by default. Contact your network administrator to find out if a DHCP server is available. See Assign an IP address using DHCP.
Auto Private IP Addressing (APIPA) also known as Auto-IP	Use APIPA to automatically assign an IP address to the Digi device from a reserved pool of standard Auto-IP addresses on a DHCP server. If the DHCP server is unavailable or there is no DHCP server, Auto-IP assigns the device an IP address. If DHCP is enabled or responds after ADDP is used, both override the Auto-IP address previously assigned. See Assign an IP address using Auto-IP.
Static IP	Manually assign a specific IP address to a device through the Digi Device Discovery Utility, the web interface, LCD, or the command-line interface. Once set, these settings do not change. The IP address and subnet mask are mandatory. Additional settings may be needed for some functions. Contact your network administrator for the required values.

Method	Description
Access via the console port	Use the port, labeled **console** port on ConnectPort LTS device to configure device settings. This port allows for a login with serial settings of 9600 baud, 8 data bits, and 1 stop bit. The standard serial ports do not provide a login by default and do not provide access to configuration settings. Only the console port allows access to configuration settings.
Command-line interface	Use the command-line interface to configure device settings. See Assign an IP address from the command-line interface.

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.

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.

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:

- **index=(1-4)**: The Ethernet interface index number.
- **ip_v4=*device ip***: The IP address for the device.
- **gateway_v4=*gateway***: The network gateway IP v4 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_v4=*device submask***: The device subnet mask for the IP v4 address.
- **mode_v4=(none|static|dhcp)**: The configuration mode of the IP v4 address.

- **ip_v6=*device ip***: The IP v6 address for the device.
- **gateway_v6=*gateway***: The IP address for the IP v6 network gateway.
- **submask_v6=*gateway***: The device subnet mask for the IP v6 address.
- **mode+v6=(none|static|dhcp)**: The configuration mode of the IP v6 address.

For example:

```
set network index=1 ip_v4=10.0.0.100 gateway_v4=10.0.0.1 submask_v4=255.255.255.0
mode_v4=static
```

Assign an IP address from the web interface

Normally, you assign IP addresses to ConnectPort LTS devices through DHCP. This procedure assumes that the ConnectPort LTS 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 ConnectPort LTS 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.

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
   ```

Using the rc.user file

The **/usr2/rc.user** file is a text file on the ConnectPort LTS that is accessible by logging in as the root user. You can modify the file to automatically perform various tasks at boot time, such as:

- Run advanced linux commands
- Initiate custom scripts
- Load additional configuration information

The Digi Knowledge Base contains additional information on the **rc.user** file, common examples, and advice on how to test and implement commands using the **rc.user** file. Go to http://www.digi.com/support for details.

Quick reference for configuring features

The following table provides a quick reference for configuring features and performing device tasks.

Some features are configurable from the command line interface only. For those features, the commands that configure the feature are noted. See the *ConnectPort LTS Command Reference* for descriptions of the commands.

To learn how to access the web interface, see Sign in to the web interface.

Feature/task	Path to feature in the web interface
Administration/Configuration management:	
Certificate Management	**Administration** > **Certificate Management**
File management: uploading and downloading files, such as applet files, and custom splash screens	**Administration** > **File Management**
Python program file management	**Administration** > **File Management**
Backup/restore configuration settings	**Administration** > **Backup/Restore**
Update firmware	**Administration** > **Update Firmware**
Reset configuration to factory defaults	**Administration** > **Factory Default Settings**
System information, including device identifiers and statistics	**Administration** > **System Information**
Reboot the device	**Administration** > **Reboot**
Alarms	**Configuration** > **Alarms**
Connection management:	

Feature/task	Path to feature in the web interface
Manage serial port connections	**Management** > **Serial Ports**
Manage active PPP connections	**Management** > **Connections** > **Active PPP Connections**
Manage active system connections	**Management** > **Connections** > **Active System Connections**
Domain Name System (DNS) Client	**Configuration** > **Network** > **DNS** > **Primary DNS and Secondary DNS**
Ethernet settings	**Configuration** > **Network** > **Advanced Network Settings**
Help on configuring features	**Help** button on each page.
Host name for a device	**Configuration** > **Network** > **Advanced Network Settings** > **Host Name**
IP address settings:	
Using static IP addresses	**Configuration** > **Network** > **IP Settings**
Using DHCP	**Configuration** > **Network** > **IP Settings**
IPv6 Settings	**Configuration** > **Network** > **IP Settings**
Source Based Routing	**Configuration** > **Network** > **IP Settings**
Network Bonding	**Configuration** > **Network** > **IP Settings**
Using Auto IP	**Configuration** > **Network** > **Advanced Settings**
Advanced network services settings:	
Web settings	**Configuration** > **Network** > **Network Services Settings** > **Advanced Network Service Settings**
SMTP settings	**Configuration** > **Network** > **Network Services Settings** > **Advanced Network Service Settings**
NFS settings	**Configuration** > **Network** > **Network Services Settings** > **Advanced Network Service Settings**
Samba settings	**Configuration** > **Network** > **Network Services Settings** > **Advanced Network Service Settings**
Syslog settings	**Configuration** > **Network** > **Network Services Settings** > **Advanced Network Service Settings**

Feature/task	Path to feature in the web interface
Multiple Electrical Interface (MEI)	1. Select **Configuration** > **Serial Ports** >. 2. Click a ***port number*** from the **Port** column. 3. Click **Basic Serial Settings**. 4. Complete the fields and click **Apply**.
Port logging: enabling port buffering and displaying contents of a port buffer	To enable port logging: 1. Select **Configuration** > **Serial Ports**. 2. Click a ***port number*** from the **Port** column. 3. Click **Advanced Serial Settings**. 4. Select **Enable Port Logging** and complete the fields. 5. Click **Apply**. To display the contents of a port buffer, select **Management** > **Serial Ports** > **Connections**.
Port profiles: sets of preconfigured serial-port settings for a particular connection and use scenario	1. Select **Configuration** > **Serial Ports**. 2. Click a ***port number*** from the **Port** column. 3. Click **Change Profile**. 4. Select one of the following profile options and click **Apply**: ■ **RealPort**—Configure the COM port redirection. See also the *RealPort Installation Guide*. ■ **Console Management** ■ **TCP Sockets**—The TCP server listens for TCP connections on the serial port or the TCP client to automatically establish a connection to a defined network port. See Automatic TCP connections (Automatic Connection). ■ **UDP Sockets** ■ **Serial Bridge** ■ **Modem** ■ **Modem Emulation** ■ **Printer** ■ **Local Configuration** ■ **Custom** 5. Complete the fields and click **Apply**.

Feature/task	Path to feature in the web interface
Ethernet bridging	Ethernet bridging configuration is available only through the command line interface. To enable Ethernet bridging, first enable the eth1 interface (IP address #2). Then connect to the ConnectPort LTS via serial port, ssh, or telnet and run the following command: `# service brmode start` See Ethernet bridging for more information.
Python support: loading and running custom programs authored in the Python programming language.	Configurable from command line only. See the **set python** command in the *ConnectPort LTS Command Reference*.
RealPort (COM port redirection) configuration	**Configuration** > **Serial Ports** > **port** > **Port Profile Settings** > **RealPort** 1. Select **Configuration** > **Serial Ports**. 2. Click a ***port number*** from the **Port** column. 3. Click **Change Profile**. 4. Select **RealPort** and click **Apply**. 5. Complete the fields and click **Apply**. See also the *RealPort Installation Guide*.
Reverting configuration settings	**Administration** > **Factory Default Settings**
Security/access control features:	
Control access to TCP/UDP inbound ports	1. Select **Configuration** > **Serial Ports**. 2. Click a ***port number*** from the **Port** column. 3. Click **Change Profile**. 4. Select **TCP Sockets**, **UDP Sockets**, or **Custom**, and click **Apply**. **Note** When you configure a TCP/UDP server, the configuration only applies to inbound sockets. You configure the outbound sockets when you configure the TCP/UDP client. 5. Complete the fields and click **Apply**.
Secure Shell Server (SSH)	**Configuration** > **Network** > **Network Service Settings** > **Basic Network Services Settings** > **Enable Secure Shell Server (SSH)**

Feature/task	Path to feature in the web interface
Add or modify a user's sign in credentials	1. Select **Configuration** > **Users**. 2. Select a user or click **New user** and complete the fields. 3. Click **User Access** and complete select the access options for the user. 4. Click **User Permissions** and select the user permissions for the user. 5. Click **Group Configuration** and associate a group with a user. 6. Click **Upload SSH Public key** and enable or disable SSH Public Key Authentication.
Set authentication method for port access	1. Select **Configuration** > **Serial Ports**. 2. Select ***port number*** under the **Port** column. 3. Click **Authentication Settings**.
Serial port configuration:	
Basic serial port settings	**Configuration** > **Serial Ports** > **Basic Serial Settings**
Advanced serial port settings	**Configuration** > **Serial Ports** > **Advanced Serial Settings**
Port profiles: associate a serial port with a set of preconfigured port settings for a specific use	**Configuration** > **Serial Ports** > **Port Profile Settings**
RTS Toggle	**Configuration** > **Serial Ports** > **Advanced Serial Settings**
Port Sharing: allow a serial port to be shared by multiple software applications. Supports up to four sessions per port. Only one session can be RealPort	1. Select **Configuration** > **Serial Ports**. 2. Click a ***port number*** from the **Port** column. 3. Click **Change Profile**. 4. Select **TCP Sockets**, **UDP Sockets**, or **Custom** and click **Apply**: 5. Complete the fields under **TCP Server Settings**, **UDP Server Settings**, or **Network Services** and click **Apply**.
SNMP:	
Configure SNMP through the web interface	**Configuration** > **System** > **Simple Network Management Protocol (SNMP) Settings**
Enable/disable SNMP service	**Configuration** > **Network** > **Network Service Settings** > **Basic Network Services Settings**

Feature/task	Path to feature in the web interface
Enable/disable SNMP alarm traps	**Configuration** > **Alarms** > ***alarm*** > **Send SNMP trap to following destination when alarm occurs**
Use SNMP as primary configuration interface	Basic network and serial settings configurable through standard and Digi-specific Management Information Blocks (MIBs). You can also configure advanced settings through SNMP.
System information: assign system-identifying information to a device	**Configuration** > **System** > **Device Identity Settings**
Authentication configuration for Web and CLI access	**Configuration** > **System** > **Authentication Settings**
Statistics	**Administration** > **System Information**
Status information	**Management** > **Serial Ports, Connections, Network Services**
Peripheral settings:	
SD Memory	**Peripheral** > **SD Memory**
USB	**Peripheral** > **USB**
Modem	**Peripheral** > **Modem**
LCD	**Peripheral** > **LCD**
XBee	**Peripheral** > **XBee**
Application settings:	
PPP	**Application** > **PPP**
Python	**Application** > **Python**
RealPort	**Application** > **RealPort**

Network connections and data paths

ConnectPort LTS devices allow for several kinds of connections and paths for data flow between ConnectPort LTS 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 ConnectPort LTS 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.
- **Console Mgmt**: Allows a TCP connection to a serially-attached console.

- **Modem**: The Modem Profile allows you to attach modem devices to the serial port to establish or receive connections from other systems and modems. Both the modem dial-in and bi-directional options provide a login from the Digi device.
- **Reverse SSH**: A remote entity establishes an SSH connection to a ConnectPort LTS serial port and data passes transparently between the SSH connection and a named serial port.

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**: ConnectPort LTS 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.

Network services associated with the command-line interface

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

- **SSH**: Use Secure Shell (SSH) to directly access a ConnectPort LTS command-line interface.
- **Telnet**: Use telnet to directly access a ConnectPort LTS command-line interface.
- **Rlogin**: Perform a remote login (rlogin) to a ConnectPort LTS command-line interface.

Network/serial clients

A network/serial client connection occurs when a ConnectPort LTS 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 ConnectPort LTS product initiates a network connection based on timing, serial activity, or serial modem signals. Autoconnect-related client connections include:

- **Raw TCP connection**: The ConnectPort LTS initiates a raw TCP socket connection to a remote entity.

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

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.
- **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.
- **Users**: Configures security features, such as enabling password authentication for device users.

ConnectPort LTS administration capabilities

Administrative capabilities include the following:

- 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

You can perform administration tasks using a number of interfaces, including the ConnectPort LTS web interface and command line. See Administration for more information and procedures.

ConnectPort LTS configuration interfaces

The following table lists and briefly describes ConnectPort LTS configuration interfaces.

Configuration interface	Description
Digi Device Discovery Utility	Allows you to discover devices, open the web interface for a device, configure network settings, and reboot the device. See Digi Device Discovery utility.
ConnectPort LTS web interface	Allows you to configure and monitor ConnectPort LTS devices. See Configure the device using the ConnectPort LTS 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 Access the command-line interface for instructions on accessing the CLI.

Configuration interface	Description
ConnectPort LTS command line interface	Allows you to configure ConnectPort LTS by issuing commands from the command line. See Configure and manage the device using the ConnectPort LTS command line interface.
Simple Network Management Protocol (SNMP)	Allows you to manage and monitor network devices. See Simple Network Management Protocol (SNMP).
ConnectPort LTS LCD panel	Allows you to configure, monitor status, and diagnose ConnectPort LTS issues. See ConnectPort LTS LCD interface.

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 ConnectPort LTS web interface.

Configure the device using the ConnectPort LTS web interface

This section describes how to configure and manage a ConnectPort LTS device using the web interface.

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 ConnectPort LTS 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 the ConnectPort LTS support page.
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.

Power failure message

If either of the two power connections to the ConnectPort LTS 16 2AC fails, a power failure message is displayed at the top of the page. For example, if the first power connection fails, the following message is displayed:

```
Power 1 Failure
```

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 ConnectPort LTS.

- **Model**: The model type for this ConnectPort LTS 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.

Logout and Login

To sign out of a configuration and management session:

1. Click **Logout**. The Login page appears.
2. Close the browser window to prevent access by other users.

Note After 5 minutes of inactivity, the idle timeout automatically performs a user logout.

To sign in to the device:

- Enter your user credentials on the Login page and click **Login**.

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.

Configuration through 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. See IP Settings for more information.
- **Network Services settings:** Configure access to various network services, such as ADDP, RealPort and Encrypted RealPort, telnet, SSH, HTTP/HTTPS, and other services. See Basic Network Services Settings for more information.
- **Socket Tunnel settings**: Configure a socket tunnel used to connect two network devices: one on the ConnectPort LTS device's local network and the other on the remote network. See Socket tunnel 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 Settings

The IP Settings page allows you to configure how to obtain the IP address of the ConnectPort LTS device. You can use one of the following methods to obtain the IP address:

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

Note Changes to DHCP, IP address, subnet mask, and DNS may effect your browser connection.

In addition, this page displays the IP addresses of the primary and secondary Domain Name System (DNS) server for the ConnectPort LTS device. For more information on how to assign and use these settings in your organization, contact your network administrator.

ConnectPort LTS has two Ethernet interfaces and you can enable or disable each interface separately. Each interface has following settings:

- **IPv4**: Internet Protocol version 4 configuration.
  - **Do not use this interface**: Choose this option if you do not want to enable IPv4 address on this Ethernet interface.
  - **Obtain an IP address automatically using DHCP**: Choose this option if you want to obtain new network settings after you reboot the ConnectPort LTS device.
  - **Use the following IP address**: Choose this option to supply a static IP address. You must provide the IP address and subnet mask. Other items are not mandatory, but may be needed for some functions (such as talking to other networks).
  - **IP Address**: The IP address for the ConnectPort LTS device. 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 for the ConnectPort LTS device. A common subnet mask is 255.255.255.0.

- **Gateway**: The IP address of the computer that enables the ConnectPort LTS device to access other networks, such as the Internet.

- **IPv6**: Internet Protocol version 6 configuration.
  - **Do not use this interface**: Choose this option if you do not want to enable IPv6 address on this Ethernet interface.
  - **Auto configuration**: Choose this option if you want to set IPv6 address through the stateless autoconfiguration protocol.
  - **Obtain an IP address automatically using DHCP**: Choose this option if you want to set IPv6 address through DHCPv6.
  - **Use the following IP address**: Choose this option to supply a static IPv6 address.
  - **IP address**: The IPv6 address for the ConnectPort LTS device. The IPv6 addresses are normally written as eight groups of four hexadecimal digits, where each group is separated by a colon (:).

    For example, IPv6 addresses are in the form of

    2001:0db8:85a3:0000:0000:8a2e:0370:7334

    And you must enter an IPv6 address with an IPv6 prefix length of the network. IPv6 network is written in CIDR notation which is separated by a slash "/" to IPv6 address.

    For example, an IPv6 address connected to a /64 subnet is written

    2001:0db8:85a3:0000:0000:8a2e:0370:7334/64.
  - **Gateway**: The IPv6 address of the computer that enables this ConnectPort LTS device to access other networks, such as the Internet.
  - **Use 6to4 tunneling**: Choose this option to supply 6to4 Tunneling which consists of encapsulating IPv6 packets within IPv4; in effect using IPv4 as a link layer for IPv6 so that the ConnectPort LTS device can reach the remote IPv6 Internet through the existing IPv4 infrastructure.
  - **IPv4 address of the remote 6to4 relay**: Set the IPv4 address of the remote 6to4 relay server.
  - **Overwrite local IPv4 address**: Set the public IPv4 address that you want to use for 6to4 tunneling. This is the public IPv4 address. If it is not set, the current IPv4 address of ConnectPort LTS will be used.

- **DNS**: Set the IP address of the Domain Name Server (DNS) used to resolve computer host names to IP addresses. The 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.
  - **Use Manual DNS**: Choose this option if you want to set DNS configuration manually.
  - **Primary DNS**: Set the IP address of primary DNS.
  - **Secondary DNS**: Set the IP address of secondary DNS.

- **Source Based Routing**: Choose this option to if you have two routers (gateways) in your network and you want each interface to use a different router. For example, if you enable this option, any traffic that originates from the IP address of Ethernet interface 2 (replies to traffic that came in Ethernet interface 2), will be routed back out through the same Ethernet interface 2. Please note that this option applies only to Ethernet interface 1 and 2 by default.
  - **Enable Local Routing**: Select this option to enable local routing.
- **Network Bonding**: Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a logical point-to-point link, known as a LAG (link aggregation groups), virtual link, or bundle. The MAC client can treat this virtual link like a single link. Network Bonding implements 802.3ad.
  - **Do not use this interface**: Choose this option if you do not want to enable network bonding on this Ethernet interface.
  - **Obtain an IP address automatically using DHCP**: Choose this option if you want to obtain new network settings after you reboot the ConnectPort LTS device.
  - **Use the following IP address**: Choose this option to manually enter static IP address settings.
  - **Subnet Mask**: The subnet mask for the ConnectPort LTS device. A common subnet mask is 255.255.255.0.
  - **Gateway**: The IP address of the computer that enables the ConnectPort LTS device to access other networks, such as the Internet.

Basic Network Services Settings

The Basic Network Services Settings page shows a set of common network services that are available for ConnectPort LTS 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

Service	Services provided	Default network port number
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
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

Service	Services provided	Default network port number
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
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

Advanced Network Services Settings

The Advanced Network Services Settings page shows a set of specific network services that are available for ConnectPort LTS products, and the related settings for the service.

- **Web Settings**:
  - **Login timeout (0-1440 minutes, 0 for unlimited)**: Idle timeout settings in minutes for the Web server. The Digi device prompts the user to log in again if the user tries to use the web interface after login timeout has expired. If you set this value 0, the web login will not expire.

- **SMTP Settings**:
  - **Enable SMTP service**: When enabled, the Digi device can send an email notification when an alarm occurs.
  - **SMTP server name**: IP address or DNS name of the SMTP server.
  - **SMTP with authentication**: Choose this option if your SMTP server requires a user name and password.
  - **SMTP without authentication**: Choose this option if your SMTP server does not require a user name and password.
  - **POP before SMTP**: Choose this option if you want to access your SMTP server after you successfully log in to POP service.
  - **SMTP user name**: The user name for your SMTP (or POP) server.
  - **SMTP password (new)/(confirm)**: The password for your SMTP (or POP) server.
  - **Device mail address**: The email address used to send alarms. Most SMTP servers check the sender's email address with the host domain name to verify the address as authentic. Consequently, when assigning an email address for the device email address, any arbitrary username with the registered hostname may be used. An example is username@company.com.

- **NFS Settings**:
  - **Enable NFS service**: When enabled, the Digi device can log port data to an NFS server.
  - **NFS server name**: IP address or domain name of the NFS server.
  - **Mounting path on NFS server**: The path to where the files are located on the NFS server.
  - **NFS timeout (5-3600 seconds)**: The timeout value in seconds to disconnect the Digi device from the NFS connection when the NFS server is not responding. If there is no response form the NFS server during the NFS timeout interval, The Digi device releases (unmount) a local directory which is mounted to the directory of NFS server (mounting path on NFS server).
  - **NFS mount retrying interval (5-3600 seconds)**: The retrying interval in seconds before the Digi device attempts an NFS remount again after disconnecting an NFS connection. The Digi device checks whether connecting to the NFS server is possible for every NFS mount retrying interval. And if connection to NFS server is possible, the Digi device remounts mounting path on NFS server on its local directory again and changes data logging location to NFS server automatically if it is needed.
  - **Alert Settings**:
    - **Description**: A description of the alert that will be sent to the receiver.
    - **Send E-mail alert to the following recipients for NFS disconnection**: Send an email alert if selected.
    - **Subject**: The title of the email alert.
    - **To**: The primary recipient of the email alert.
    - **CC**: The secondary recipient of the email alert.
    - **Priority**: Select one of the following priority options for this email alert: **Normal** or **High**.
  - **Send NFS disconnection trap when alarm occurs**: When selected, sends an SNMP trap when an alarm occurs.

- **Samba Settings**:
  - **Enable Samba service**: When enabled, the Digi device can log port data to a Samba server.
  - **Samba server name**: IP address or domain name of the Samba server.
  - **Mounting on path Samba server**: The path to where the files are located on the Samba server.
  - **Samba timeout (5-3600 seconds)**: Timeout interval in seconds before the Digi device disconnects Samba connection when the Samba server is not responding. If there is no response form the Samba server during the Samba timeout interval, the Digi device releases (unmount) a local directory which is mounted to the directory of the Samba server (mounting path on Samba server).
  - **Samba mount retrying interval (5-3600 seconds)**: Retrying interval in seconds when the Digi device tries to connect to the Samba server again after disconnecting the Samba connection. The Digi device checks whether connecting to the Samba server is possible for every Samba mount retrying interval. If connection to the Samba server is possible, the Digi device remounts mounting path on the Samba server on its local directory again and changes data logging location to Samba server automatically if it is needed.
  - **Samba server user**: The user name for your Samba server.
  - **Samba server password (new)/(confirm)**: The password for your Samba server.
  - **Alert Settings** :
    - **Description**: A description of the alert that will be sent to the receiver.
    - **Send E-mail alert to the following recipients for Samba disconnection**: When selected, sends an email alert when an alarm occurs.
    - **Subject**: The subject line of the e-mail notification and the description of the SNMP trap when an alarm is triggered.
    - **To**: The email address of the primary recipient of email alert.
    - **CC**: (Optional) The email address of the secondary recipient of email Alert.
    - **Send Samba disconnection trap when alarm occurs**: When selected, sends an SNMP disconnection trap when an alarm occurs.
    - **Priority**: Select one of the following priority options for this email alert: **Normal** or **High**.
    - **Send Samba disconnection trap when alarm occurs**: When selected, sends an Samba disconnection trap when an alarm occurs.

- **SYSLOG settings**:
  - **Enable SYSLOG service**: When selected, the Digi device can log port data to the SYSLOG server.
  - **SYSLOG server name**: IP address or domain name of the SYSLOG server.
  - **SYSLOG Facility**: The Digi device supports SYSLOG facilities from local0 to local7. You can employ these facilities to save messages from the Digi device separately to the SYSLOG server.

Socket tunnel settings

You can use a socket tunnel to connect two network devices: one on the ConnectPort LTS 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 ConnectPort LTS product on the configured port number. The ConnectPort LTS product then opens a separate connection to the specified destination host. Once the tunnel is established, the ConnectPort LTS 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**:
  - **Host name**: The host name that will appear the **DHCP Option 12** field. The host name can be a single name or a fully qualified domain name (FQDN). You can use this optional setting only when you enable DHCP.

    Note If you change the host name, you must sign in to the web interface again.

  - **Enable Auto IP address assignment**: Auto Private IP Addressing (APIPA), also known as Auto-IP: A standard protocol that automatically assigns an IP address from a reserved pool of standard Auto-IP addresses to the computer on which it is installed. The device is set to obtain its IP address automatically from a DHCP server. If the DHCP server is unavailable or nonexistent, Auto-IP assigns the device an IP address if one of the following instances are true:
    - You enabled DHCP or it responds later
    - You are using ADDP/Device Discovery

    Both will override the previously assigned Auto-IP address.
  - **Reuse old IP at bootup time on DHCP failure**: If the Digi device fails to receive an IP address from the DHCP server on booting up, the users can set the IP configurations of the Digi device with the previous IP configurations and connect it to the network.
- **Ethernet interface**: You can set the speed and duplex mode of each Ethernet interface.
  - **Speed**: Specify the Ethernet speed of the Digi device. Your options are as follows: **Auto**, **10 Mbit**, **100 Mbps**, or **1000 Mbps**.
  - **Mode**: Specify the duplex mode of the Ethernet interface. Your options are as follows: **Auto**, **Half-duplex**, or **Full-duplex**. Note that you cannot manually set the duplex mode if the speed is set to **Auto**.
- **TCP keep-alive settings**: The DHCP server assigns these network settings, unless you manually set them here.
  - **Idle Timeout**: The period of time that a TCP connection can remain idle before sending a keep-alive.
  - **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 activating the keep-alive option. The connection is assumed to be lost after sending this number of keep-alive probes.

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:

- **Interface**: The name of the network interface where the packet originated.
- **Option**: Determines the rule that will be applied to the specified IP address/mask or its inverse.
- **IP address/Mask**: Specifies the host range by entering the base host IP address followed by a forward slash (/) and subnet mask.
- **Protocol**: The type of protocol this port will accept or drop.
- **Port**: A TCP/IP port on the Digi device that other hosts will access.
- **Chain**: Determines whether or not hosts can access the port.

Serial ports configuration

Use the Serial Ports Configuration page to establish a port profile for each serial port on the ConnectPort LTS 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:

- **Port Group Settings**: This pane allows you to create one or more port groups and assign ports to each port group. See Port Group Settings for more information.
- **Port Settings**: This pane lists the available ports and allows you to configure or copy selected ports. See Port Settings for more information.

Port Group Settings

You can create port groups to send data to multiple ports. Instead of sending data to individual serial ports, you can send data to all ports in a group simultaneously through a port in a group. If you select an additional option, you can also see the data from multiple ports in the same group from a terminal connected to the one of serial ports in the group.

To configure a port group, you must create a port group first and then select ports to be associated with this group. You can create a maximum number of 16 port groups and a port cannot be associated with multiple groups. When you select ports to be associated with a group you can also configure following settings:

- **No.**: The group number.
- **Group name**: The name of the group.
- **Ports**: Lists the ports associated with the group.

When you click **Add**, the following settings appear:

- **Group name**: The name of the group.
- **Check all/Uncheck all**: Select or clear the check boxes for all ports.

- **Port #<number>**: Select or clear the check box associated with the port. When you select a check box, the port will be assigned to the group.
- **Show data from all ports associated with same port group**: When selected, user can see the data from other ports in the same group from a terminal connected to the one of serial ports in the group. You can control the pattern of data from other ports in the same group.

- **Send after the following number of bytes**: Send the data to the other ports in the same group after the specified number of bytes has been received on the serial port. You can specify 1 to 4096 bytes. Default is 1024 bytes.
- **Send after the following number of idle milliseconds**: Send the data to the other ports in the same group after the specified number of idle time has been passed with no additional data received on the serial port. You can specify 1 to 65,535 milliseconds. Default is 1000 milliseconds.

Port Settings

- **Port**: Lists the available port. To view or configure the port settings, click the port number. See Port Profile Settings for more information.
- **Description**: A brief description of the port.
- **Profile**: The profile assigned to the port. See Select Port Profile for more information on available port profile options.
- **Serial Configuration**: Displays the serial configuration associated with the port.
- **Action**: Select to perform allowable actions on this entry. The only allowable action is to copy the port settings for this port to other ports. See Copy Serial Port Settings for more information.

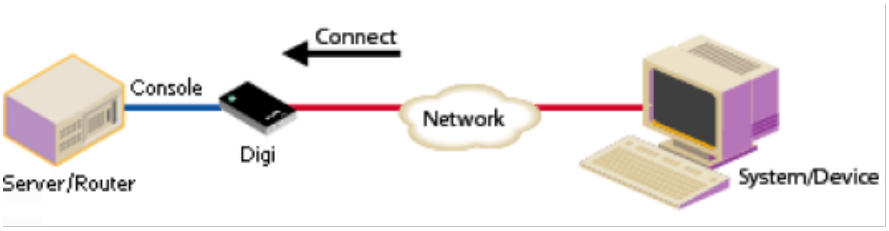
Select Port Profile

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.

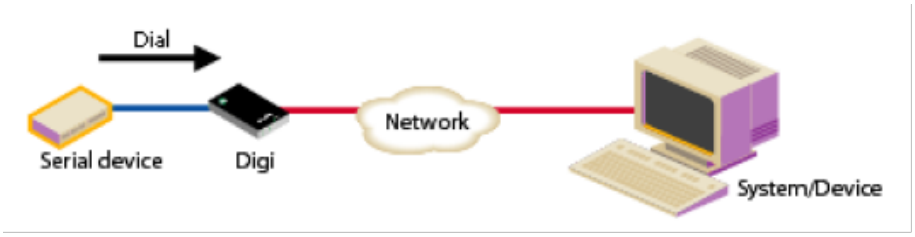
The ConnectPort LTS supports the following port profiles:

- **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 ConnectPort LTS 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. In ConnectPort LTS, the Custom profile also allows the access of a serial port through RealPort protocol. See Assign a profile to a serial port for more information.
- **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**: The Modem profile allows you to attach modem devices to the serial port to establish or receive connections from other systems and modems.



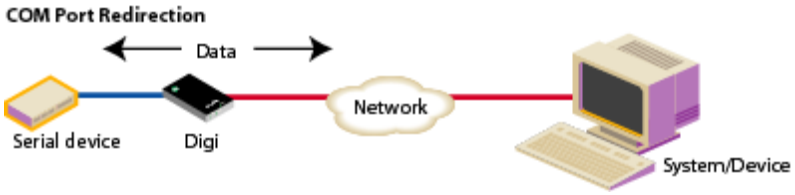
Modem dial-in and bi-directional options provide a login from the Digi device. See Assign a profile to a serial port for more information.

- **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.

- **PPP**: The PPP (Point-to-Point Protocol) profile configures an Internet PPP connection so the provider's server can respond to your requests, pass them on to the Internet, and forward requested Internet responses back to you. PPP uses the Internet protocol (IP) (and can handle others). Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they are put on the Internet.

- **Printer**: The Printer profile allows you to connect a printer to the serial port. Use this profile if you intend to print using the LPD protocol on your system. 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 ConnectPort LTS 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 ConnectPort LTS 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 ConnectPort LTS product.

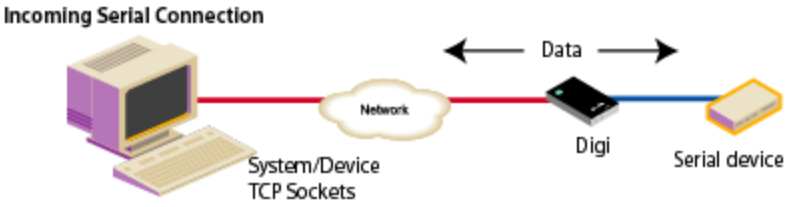
- **Serial Bridge**: The Serial Bridge Profile configures one side of a serial bridge. A bridge connects two serial devices over the network as if they were connected with a serial cable. This is also referred to as serial tunneling. Each serial device is connected to the serial port of a Digi device 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 ConnectPort LTS 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:

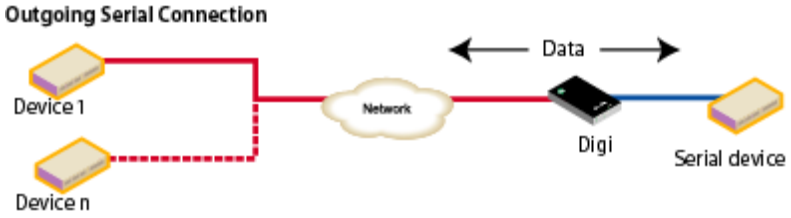
  - Automatic TCP connections (Automatic Connection)
  - TCP and UDP network port numbering conventions

  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 ConnectPort LTS model. If a profile listed in this description is not available on the page, it is not supported in the ConnectPort LTS 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**: To accommodate environments where the ConnectPort LTS is not available on the network (for security purposes) or to allow access when a network outage occurs, use externally attached serial modems for out-of-band management.
     a. Select **Incoming Connection** or **Outgoing Connection** (or **Network Bridge Connection**... if bi-directional).
     b. Select **Enable PPP Connections on this Modem** if you want to establish a PPP connection.
     c. Click **Apply**.
     d. Click **Basic Serial Settings** and configure these settings to match the settings of the attached modem. In a typical configuration, you should set the baud rate should be set to **115200** and set flow control to **Hardware**.
     e. 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.
- **Printer**: Verify that the **Basic Serial Settings** match the settings of your serial printer and then click **Apply**. See Using LDP protocol for more information.
- **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.

Using LDP protocol

The following list provides tips for configuring the print spooler on your system when you intend to print using the LPD protocol to a printer attached to device server:

- Banner pages are not supported.
- The device server's DNS name or IP address is the remote system's name.
- Queue names must conform to the following conventions:

  ```
  lp[port#]
  ```

  For example :

  ```
  lp1(port 1), lp2(port 2)
  ```

Note Ensure the LDP service is enabled in the Network Services Settings. See Basic Network Services Settings for more information.

Automatic TCP connections (Automatic Connection)

The TCP Client allows the ConnectPort LTS 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**.

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 ConnectPort LTS device that initiates communication must use these network ports numbers. If you cannot configure the application or ConnectPort LTS product to use these network port numbers, change the network port on the ConnectPort LTS product.

Copy Serial Port Settings

You can copy the port settings for this port to other ports.

To copy port settings, select a port first and then select the ports you want to copy the port settings to.

- **All**: Selects or clears all port check boxes.
- **<number>**: Select or clear the check box associated with the port number. When you select a check box, the port settings will be copied to the port.

Note The following port settings will not be copied: Port Description, Auto Connection State, TCP Socket ID, UDP Serial State, and UDP Socket ID.

Port Profile Settings

The Port Profile Settings page appears when you select a port under Port Settings on the Serial Ports Configuration page. The content on this page varies depending on the type of port profile selected. To change a port profile, click **Change Profile**. See Select Port Profile for more information the available port profiles and changing the port profile.

Console Management settings

Use the Console Management Settings pane to connect directly to the serial device using the following TCP port on the network.

- **Enable Telnet access using TCP Port**: Enable the telnet access method to connect to your serial device. The currently configured TCP port is shown.
- **Enable Secure Shell (SSH) access using TCP Port**: Enable Secure Shell access to connect to your serial device. The currently configured TCP port is shown.

Local Configuration Settings

The Local Configuration profile allows you to sign in to and the command line interface when connecting directly to a serial port. This profile provides a login from the Digi device.

- **Access the command line interface when connecting from serial terminals**: Enable access to the command-line interface when connecting from serial terminals to configure and manage the Digi device.

Modem Emulation Settings

The Modem Emulation profile allows you to configure the serial port to act as a modem.

Verify that the Basic serial settings match the settings of your modem.

Modem Settings

The Modem profile allows you to connect a modem to the serial port. When you assign the Modem profile to a serial port, the following settings appear under Modem Settings on the Port Profile Settings page:

- **Incoming Connection**: Modem receives dial-in connections, such as inbound PPP connections or to manage a device through a telephone network. The ConnectPort LTS product server will receive connections from other hosts.

- **Outgoing Connection**: The modem sends dial-out connections to establish connections with external hosts or to connect to an external PPP network.
- **Network Bridge Connection (bi-directional)**: You can use the modem to establish connections to other hosts and receive connections from other hosts.
- **Init String**: This is the modem initialization settings. Modify the init string to change the behavior of the modem as needed by your application/modem model. For more information about the supported modem commands, see the *ConnectPort LTS Command Reference*.

  Note If the modem is currently in use, the init string change will not take effect immediately. It will be used the next time the modem is initialized.

- **Enable PPP Connections on this Modem**: When enabled, modem is used for PPP connections. You will need to configure the PPP connection for incoming and/or outgoing PPP connections. See PPP (Point-to-Point Protocol) for more information.

  Note The Modem profile is most often used when you configure a Digi device server for out-of-band management and PPP.

- **Enable callback**: When enabled, the Digi device disconnects the connection from a remote site and then calls the phone number specified in the **Callback phone number** field.
- **Callback phone number**: The phone number that the Digi device calls when you enable callback.
- **Dial-in modem callback login**: The Digi device calls the phone number specified as the callback phone number after a user authentication.
- **Allow dial-in modem callback number change**: The Digi device will ask a user whether to change the callback phone number before calling.

Printer Settings

Verify that the Basic serial settings match the settings of your serial printer.

RealPort Settings

When you associate a port with the RealPort profile, you are only required to configure the altpin when using 8-wire cabling with modems or devices requiring DCD assertion. The other configuration settings are not required. RealPort will set the serial port settings as directed by the computer application.

Refer to the *RealPort Setup Guide* for instructions on installing and configuring the RealPort driver on your computer or server.

Serial Bridge Settings

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.

- **Peer-to-peer bridge**: Both sides of a peer-to-peer bridge are configured similarly. On start-up, both sides will try to initiate a connection to the serial device on the other side of the bridge.

Each side is configured with the IP address and destination TCP port of the other side acting as a TCP server. A peer-to-peer bridge is the preferred configuration for a serial bridge.

To configure a peer-to-peer bridge, enable both **Initiate serial bridge to the following device** and **Allow other devices to initiate serial bridge**.

- **Client/Server bridge**: In a client/server bridge, one side of the bridge is designated as the client. This side should enable **Initiate serial bridge to the following device**. You need to configure the client with the IP address and TCP port of the other side of the bridge.

  The other side of the bridge is designated as the server. This side should enable **Allow other devices to initiate serial bridge**.

  Note the **TCP Port** value entered under **Allow other devices to initiate serial bridge**. You will need this TCP Port number when you configure the other side of the serial bridge. Most bridges should use the suggested default TCP Port.

- **Enable Secure Socket serial bridge**: Enable to use a secure socket connection, otherwise the connection will use raw TCP.

Serial Services

Your serial device can automatically establish connections to another system or device on the network. This is also referred to as Automatic Connection or AutoConnect.

Access the command line interface: Enable access to the command-line interface when connecting from serial terminals.

TCP Settings

Automatically establish bi-directional TCP connections between the serial device and a server or other networked device.

- **Automatically establish TCP Connections**: Enable automatic connection to a system or device on the network.
  - **Establish connection under one of the following conditions**:
    - **Always connect and maintain connections**: A connection is always available. If a connection is lost it will be reconnected automatically. This type of connection is most often used in client/server configurations where this Digi device server is the client.

      Note Select this option to enable autoconnect for 3-wire devices.

    - **Connect when data is present on the serial line**: A connection is made when the serial port receives data. This type of connection is most often used for terminals and terminal emulation.
    - **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 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.

- **Connect when DCD (Data Carrier Detect) line goes high**: A connection is made when the serial port's DCD (Data Carrier Detect) signal goes high. This type of connection is most often used for modems. See the Advanced Serial Settings for the option to close the connection when the DCD signal goes low.

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

- **Connect when DSR (Data Set Ready) line goes high**: A connection is made when the serial port's DSR (Data Set Ready) signal goes high. See the Advanced Serial Settings for the option to close the connection when the DSR signal goes low.

- **Establish connection to the following network service**:
  - **Server (name or IP)**: Type the IP address or host name of the destination device.
  - **Service**: Select the service type of the connection. Your options are as follows:
    - **Raw TCP**—If you are bridging to another Digi device server use Raw TCP.
    - **Rlogin**
    - **Secure Sockets**
    - **Telnet**
    - **SSH**
  - **TCP Port**: Type the TCP port number of the destination device. The standard port numbers are 23 for telnet and 513 for rlogin. If you are bridging to another Digi device server use the raw TCP port number for its serial port. This is usually 2101 for port 1. 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.

    See Assign a profile to a serial port for more information about assigning a Serial Bridge (Serial Tunneling) profile to a serial port.
  - **Enable Keep-Alive**: When selected, enables the Keep-Alive feature.

UDP Settings

Serial data received is automatically returned to the last UDP client that sent data. You can override or lock-down the destination by entering one or more IP and port pairs below. All serial data is repeated as UDP unicast to all devices in this list.

- **Automatically send serial data**: Enable sending serial data to one or more systems or devices on the network using UDP sockets.
  - **Send data to the following network services**: A list of servers or devices to send data to using UDP. To add a new destination enter the following information and click **Add**.
    - **Description**: A description of the server or device (16 characters or less).
    - **Send To**: The IP address or DNS name to send data to.

- **UDP Port**: The port number to send data to. If you are sending data to another Digi device server use the raw UDP port number for its serial port. This is usually 2101 for port 1. The format for this port number is as follows:

```
21<serial port number>
```

Replace <serial port number> is 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.

- **Send data under any of the following conditions**:
  - **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	\\

  - **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.

Network Services

Enable the access methods that will be used to connect to your serial device. This page displays the currently configured TCP or UDP port.

- **Allow multiple connections**: Enable to allow multiple connections to the TCP server.
- **Enable Raw TCP access using TCP Port**: Enable raw TCP access method to access to the specified port. The default is 2101 for port 1. The format for this port number is as follows:

```
21<serial port number>
```

Replace <serial port number> is 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.

- **Enable Secure Shell (SSH) access using TCP Port**: Enable Secure Shell access to connect to your serial device. The currently configured TCP port is shown.
- **Enable UDP access using UDP Port**: Enable the UDP access method to access the specified port.
- **Enable RealPort access**: Enable the RealPort access method.
- **Enable LPD access**: Enable the LPD access method.
- **Enable TCP Keep-Alive**: When selected, enables the sending of the TCP Keep-Alive feature. TCP sends keep-alive messages at the TCP layer to connected devices indicating the connection is still alive.

TCP Server Settings

Other systems or devices can connect to your serial device over the network (often referred to as Reverse Telnet, Console Management or Device Management). You can enable the access methods that will be used to connect to your serial device. The default configuration enables telnet, raw TCP, Secure Shell (SSH), and Secure Socket access.

- **Allow multiple connections**: Enable to allow multiple connections to the TCP server.
- **Enable Telnet access using TCP Port**: Enable the telnet access method to connect to your serial device. The currently configured TCP port is shown.
- **Enable Raw TCP access using TCP Port**: Enable raw TCP access method to access to the specified port. The default is 2101 for port 1. The format for this port number is as follows:

  ```
  21<serial port number>
  ```

  Replace <serial port number> is 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.
- **Enable TCP Keep-Alive**: When selected, enables the sending of the TCP Keep-Alive feature. TCP sends keep-alive messages at the TCP layer to connected devices indicating the connection is still alive.

TCP Client Settings

Your serial device can automatically establish connections to another system or device on the network. This is also referred to as Automatic Connection or AutoConnect.

- **Automatically establish TCP Connections**: Enable automatic connection to a system or device on the network.

- **Establish connection under one of the following conditions**:
  - **Always connect and maintain connections**: A connection is always available. If a connection is lost it will be reconnected automatically. This type of connection is most often used in client/server configurations where this Digi device server is the client.

    Note Select this option to enable autoconnect for 3-wire devices.

  - **Connect when data is present on the serial line**: A connection is made when the serial port receives data. This type of connection is most often used for terminals and terminal emulation.
  - **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 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.
  - **Connect when DCD (Data Carrier Detect) line goes high**: A connection is made when the serial port's DCD (Data Carrier Detect) signal goes high. This type of connection is most often used for modems. See the Advanced Serial Settings for the option to close the connection when the DCD signal goes low.

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

  - **Connect when DSR (Data Set Ready) line goes high**: A connection is made when the serial port's DSR (Data Set Ready) signal goes high. See the Advanced Serial Settings for the option to close the connection when the DSR signal goes low.

- **Establish connection to the following network service**:
  - **Server (name or IP)**: Type the IP address or host name of the destination device.
  - **Service**: Select the service type of the connection. Your options are as follows:
    - **Raw TCP**—If you are bridging to another Digi device server use Raw TCP.
    - **Rlogin**
    - **Secure Sockets**
    - **Telnet**
    - **SSH**
  - **TCP Port**: Type the TCP port number of the destination device. The standard port numbers are 23 for telnet and 513 for rlogin. If you are bridging to another Digi device server use the raw TCP port number for its serial port. This is usually 2101 for port 1. 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.

    See Assign a profile to a serial port for more information about assigning a Serial Bridge (Serial Tunneling) profile to a serial port.
  - **Enable Keep-Alive**: When selected, enables the Keep-Alive feature.

UDP Server Settings

Your serial device can receive UDP data from systems or devices on the network. See Assign a profile to a serial port for more information on assigning a UDP server to a serial port.

- **Allow multiple connections**: When enabled, allows multiple connections to the UDP server.
- **Enable UDP access using UDP Port**: When enabled, allows you to specify the UDP port number to connect to when sending data to the serial device. The default is 2102.

UDP Client Settings

Your serial device can send data to one or more systems or devices on the network using UDP. This is also referred to as Data Distribution or UDP Multicast.

- **Automatically send serial data**: Enable sending serial data to one or more systems or devices on the network using UDP sockets.

- **Send data to the following network services**: A list of servers or devices to send data to using UDP. To add a new destination enter the following information and click **Add**.
  - **Description**: A description of the server or device (16 characters or less).
  - **Send To**: The IP address or DNS name to send data to.
  - **UDP Port**: The port number to send data to. If you are sending data to another Digi device server use the raw UDP port number for its serial port. This is usually 2101 for port 1. The format for this port number is as follows:

    ```
    21<serial port number>
    ```

    Replace <serial port number> is 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.
- **Send data under any of the following conditions**:
  - **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.

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.
- **MEI Type**: The MEI (multi-electronic interface) type sets the type of serial interface if the ConnectPort LTS is the MEI version. The MEI version has three kinds of serial interfaces: RS232, RS422/485 (full), and RS485Half. If the ConnectPort LTS is not the MEI version, MEI Type will be fixed to RS232 and you cannot change it.
- **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.
- **Enable termination**: When selected, enables termination.

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.
- **Pre-delay**: The number of milliseconds to wait after the RTS signal is turned on before sending data. This can be 0 to 5000 milliseconds but is usually set to 0. This setting only appears when you are configuring a Console Management, Modem, or RealPort profile.

- **Post-delay**: The number of milliseconds to wait after sending data before turning off the RTS signal. This can be 0 to 5000 milliseconds but is usually set to 0. This setting only appears when you are configuring a Console Management, Modem, or RealPort profile.
- **Enable DCD on 8-pin RJ45 connectors (Altpin)**: When enabled, the functions of DCD pin and DSR pin are swapped so that you can use eight-wire RJ-45 cables with modems. This setting only appears when you are configuring a Console Management, Modem, RealPort, and or Sockets profile.

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

Authentication settings

Note The selected profile type determines if the following settings are enabled.

- **Authentication method**: The authentication method. The default is None.

  The Digi device supports various authentication options, such as None, Local, RADIUS, LDAP.
- **Primary/Secondary authentication server**: The IP address or DNS name of the remote authentication server.
- **Authentication server socket**: The TCP port number of the authentication server.
- **Primary/Secondary account server**: The IP address or DNS name of the remote accounting server. The accounting server is only required when you set the authentication method to RADIUS.
- **Account server socket**: The TCP port number of the accounting server.
- **Shared secret**: A password string used for encryption of messages between the authentication server and the ConnectPort LTS. Only RADIUS servers require a shared secret.
- **Timeout**: The authentication timeout, in seconds. Only RADIUS servers require a timeout value.
- **Retries**: The authentication retry count. Only RADIUS servers require an authentication retry count.
- **LDAP search base**: The LDAP search base string. Only LDAP servers require a search base string.
- **Domain name for active directory**: The LDAP domain name string for Active Directory. Only LDAP servers require a domain name of Active Directory.

- **Secure LDAP**: Allows you to enable Secure LDAP for LDAP servers. The default is Disable. Only LDAP servers require this option.

  Note Default permissions for authenticated remote users are defined under the user name **ruser**.

- **PPP User**: Select the PPP user you want to allow to sign in to the serial port. Select ANYBODY if you want to allow multiple users to sign in to the serial port. This field is enabled when you assign the Modem profile to the serial port. To add PPP users to this drop-down list, configure **Incoming PPP Connections** (**Application** > **PPP** > **Incoming PPP Connections**.

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 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.

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.
- **Type**: The basis for the alarm; whether it is based on 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 Alarm conditions include:

- **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.

- **Alarm Type**: Specify the alarm type to send. Your options are as follows: [**none**|**email**|**snmptrap**|**all**]
- **Alarm Description**: The text to include in the Subject: lien of the alarm-notification email or SNMP traps description.
- **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.

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 ConnectPort LTS 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 ConnectPort LTS 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) v1/v2c**: This check box enables or disables use of SNMP version 1 or version2c.
  - **SNMPv1/v2c Get community**: The password required to get SNMP-managed objects. The default is public. Changing get and set community names from their defaults is recommended to prevent unauthorized access to the device.
  - **SNMPv1/v2c Set community**: The password required to set SNMP-managed objects. The default is private.
  - **SNMPv1/v2c Permission**: Allow SNMP clients to set device settings through SNMP:
    - **get only**: Disables the capability for users to issue SNMP set commands uses use of SNMP read-only for the ConnectPort LTS product.
    - **get/set**: Enables the capability for users to issue SNMP set commands uses use of SNMP read-only for the ConnectPort LTS product.

- **Enable Simple Network Management Protocol (SNMP) v3**: Enables or disables use of SNMP version 3.
  - **User**: The user name that is authenticated to communicate with the SNMP engine.
  - **Security level**: The security level of the user with regard to authentication and privacy: Auth_NoPriv or Auth_Priv.
  - **Authentication protocol**: The type of authentication protocol algorithm to use: MD5 or SHA.
  - **Authentication password/ Authentication password (confirm)**: Supply and confirm the password for the user.
  - **Privacy protocol**: The type of privacy protocol to use: DES or AES.
  - **Privacy password/ Privacy password (confirm)**: Supply and confirm the password for the user.
  - **SNMPv3 Permission**: Select the appropriate permission level: **get only** or **get/set**.
- **Enable Simple Network Management Protocol (SNMP) traps**: Enables or disables the generation of SNMP traps.
  - **Trap version**: The SNMP version for the trap.
  - **Trap primary IP**: The primary IP address of the system to which traps are sent. You must specify a non-zero value to enable traps. If your ConnectPort LTS product supports alarms, this field is required in order to send alarms in the form of SNMP traps. See Alarms Configuration.
  - **Trap secondary IP**: The secondary IP address of the system to which traps are sent.
  - **Trap community**: Community string for SNMP trap.
  - **Trap user**: Type the user name that is authenticated to communicate with the SNMP v3 trap engine.
  - **Trap security level**: The security level of the user with regard to authentication and privacy in case of SNMPv3 trap: **Auth_NoPriv** or **Auth_Priv**.

Select one or more of the following SNMP trap options:

- Generate cold start traps
- Generate link up traps
- Generate authentication failure traps
- Generate login traps
- Generate power traps

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.

- **Enable NTP**: Select or clear the check box to enable or disable Network Time Protocol (NTP). When enabled, the ConnectPort LTS uses NTP to set the system time.

- **NTP server**: Type the IP address or hostname for the NTP server.
- **NTP option**: Choose one of the following options:
  - **Once**:
  - **Periodically**: Synchronize the clock with NTP based on the **NTP update interval**.

- **NTP update interval**: Type the interval, in hours, between NTP updates.
- **Date (mm/dd/yyyy)**: Type the date in mm/dd/yyyy format.
- **Time (hh:mm:ss)**: Type the time in hh:mm:ss format.
- **Offset (hh:mm)**: Type the offset in hh:mm format.

Authentication Settings

Use the Authentication Settings page to set the authentication method and the related settings for web interface and command-line interface access. The command-line interface access includes access through serial console, telnet, SSH, Rlogin and Rsh. Remote authentication uses the permissions set to the default user called **ruser**.

- **Authentication method**: The authentication method. The default is None.

  The Digi device supports various authentication options, such as None, Local, RADIUS, LDAP.
- **Primary/Secondary authentication server**: The IP address or DNS name of the remote authentication server.
- **Authentication server socket**: The TCP port number of the authentication server.
- **Primary/Secondary account server**: The IP address or DNS name of the remote accounting server. The accounting server is only required when you set the authentication method to RADIUS.
- **Account server socket**: The TCP port number of the accounting server.
- **Shared secret**: A password string used for encryption of messages between the authentication server and the ConnectPort LTS. Only RADIUS servers require a shared secret.
- **Timeout**: The authentication timeout, in seconds. Only RADIUS servers require a timeout value.
- **Retries**: The authentication retry count. Only RADIUS servers require an authentication retry count.
- **LDAP search base**: The LDAP search base string. Only LDAP servers require a search base string.
- **Domain name for active directory**: The LDAP domain name string for Active Directory. Only LDAP servers require a domain name of Active Directory.
- **Secure LDAP**: Allows you to enable Secure LDAP for LDAP servers. The default is Disable. Only LDAP servers require this option.

  Note Default permissions for authenticated remote users are defined under the user name **ruser**.

Login Settings

Use the Login Settings page to configure the login settings.

- **Enable Login Banner**: Allows you to enable the login banner. A login banner is an optional message that appears above the Login page before a user signs in using the web interface or telnet/ssh command line login prompt. For example, a banner "Security Notice" followed by additional security information may appear above the Login page. The login banner is disabled by default.

  The text for the banner resides in a text file named **issue.net**. See Create the login banner for instructions on creating the banner.
- **Disable root login via telnet or ssh**: Allows you to disable the root shell access via telnet (default port 23) or ssh (default port 22). The root shell access via telnet is enabled by default.

Create the login banner

To create the login banner:

1. From the web interface, select **Configuration** > **System** > **Login Settings**.
2. Select the **Enable Login Banner** check box.
3. Open a Linux command line prompt and type the following command:

   ```
   #> bash
   ```

4. Using a text editor, such as vi, create a text file called **issue.net**:

   ```
   #> vi /usr2/issue.net
   ```

5. In **issue.net** file, type the text that you want to appear in the login banner.
6. Change the permissions of the **issue.net** file to read, write, and execute for all.

   ```
   #> chmod 777 /usr2/issue.net
   ```

Escape Character Settings

Use the Escape Character Settings page to configure the escape character settings.

- **Connect**: The escape character for users using the connect command. The default escape character is **^[** (Control key and left bracket).
- **Telnet**: The escape character for users using telnet. The default is **^]** (Control key and right bracket).
- **SSH**: The escape character for users using ssh. The default is **~**.

Users

You can configure the Digi device server to accommodate the requirements of specific users. You can configure the following user attributes:

- The user's name and password.
- The device interfaces that the user can access, such as the command-line interface or web interface.
- The permissions the user has to access and configure the device.

Multi-user model implemented in ConnectPort LTS

The user model in ConnectPort LTS device determines the commands that users can issue. ConnectPort LTS supports multiple users. ConnectPort LTS devices use a more-than-two-user model. You can define up to 32 users. Characteristics of this model include:

- The **root** user is a user name or account that by default has access to all configuration settings on the Digi device. The **root** user is responsible for system administration. By default, the all permissions for the **root** user are enabled and the **root** user can issue all commands. The **root** user is the first user to access and configure the Digi device. The first user to access the Digi device can choose to disable some of the default **root** permissions. You are prompted to change your password the first time you sign in and after a factory reset.
- The **admin** user is a user name or account that has access to configuration settings defined by the **root** user for administrative purposes. The **admin** user is initially inactive. To activate the **admin** user, you must login to the web interface as root and then assign a password to the **admin** user. See User Configuration.

- The **ruser** is a user name or account used by authentication when the user is not locally defined. The **ruser** represents the remote user. Use the user named **ruser** to set permissions for users authenticating remotely via Remote Authentication Dial-In User Service (RADIUS) and/or Lightweight Directory Access Protocol (LDAP).

  The default RADIUS user defines the permissions for all RADIUS users who do not have a local definition. You can customize the permissions for RADIUS users who do not have a local definition.

  Users that have a local definition and connect to services that are set up for RADIUS:
  - Have permission characteristics of locally-defined users.
  - User authentication uses the specified RADIUS authentication method. See description of **Authentication Method** in Authentication Settings for more information.

  The RADIUS attributes supported by ConnectPort LTS are as follows:
  - For authentications:
    - User-Name
    - User-Password
    - NAS-Port-Id
    - Framed-Protocol
  - For accounting:
    - Acct-Status-Type
    - User-Name
    - User-Password
    - NAS-Port-Id
    - Acct-Session-ID
    - Acct-Session-Time
    - Service-Type
- Users are defined by the user settings in the web interface or the **set user** command in the command-line interface.
- You can define additional users as needed.
- **set user**, **set group,** and other commands are described in detail in the *ConnectPort LTS Command Reference*.

Users

The Users page displays a list of configured users and groups. Use the page to configure users and groups.

- **Configure Users**:
  - **User Name**: Lists the configured users. To edit a user, such as change the password, click a user's name.

- **Action**: Lists the available actions per user. The possible action is as follows:
  - **Remove**: Allows you to remove the user.
- **New user**: Allows you to add a new user.

- **Configure Groups**:
  - **Group Name**: Lists the configured groups. To edit a group, click the group's name.
  - **Action**: Lists the available actions per group. The possible action is as follows:
  - **Remove**: Allows you to remove the group.
  - **New group**: Allows you to add a new group.

Add New User

Use the Users Configuration page to configure a user's login credentials.

- **User Name**: The user's login name.
- **New Password**/**Confirm Password**: The user's login password. The password must be 4 to 16 characters long.

Add a user

ConnectPort LTS 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.

User Configuration

- **User Configuration**: Use the User Configuration page to configure a user's login credentials.
  - **User Name**: The user's login name.
  - **New Password**/**Confirm Password**: The user's login password. The password must be 4 to 16 characters long.

- **User Access**: Use the User Access page to configure the user's access permissions.
  - **System Interface Access (Command Line Interface)**: Choose the interface to use when the user logs into the command line interface. Your options are as follows:
    - **None**: Disable system interface access for this user.
    - **Shell**: Allow this user to access the shell program of the command-line interface.
    - **CLI menu**: Allow this user to access the menu program of the command-line interface.
    - **Port access menu**: Allow this user to access the port access menu.
  - **Allow web interface access**: Allow this user to access the web interface for system configuration and management.
  - **Manage Serial Ports**: Select the ports that the user can access.

- **User Permissions**: Use the User Permissions page to configure a user's permissions associated with various services and configuration settings.

  To further secure the ConnectPort LTS 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 Basic Network Services Settings.

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

  The list of services and the user permissions available for them vary by ConnectPort LTS product and the features supported in the product. There are several groups of services, such as:

  - Network Configuration
  - Serial Configuration
  - System Configuration
  - User Configuration
  - Peripherals
  - Application Configuration
  - Connection Management
  - Command Line Applications
  - System Administration

  The possible selections for each permissions setting can vary, but includes the following possibilities:

  - **None**: The user does not have permission to execute this setting.
  - **Read Self**: The user can display their own settings, but not those of other users.
  - **Read**: The user can read the setting for all users, but does not have permission to modify or write the setting.
  - **Read/Write Self**: The user can read and write their own setting, but not those of other users.
  - **Read All/Write Self**: The user can read the setting for all users and can modify their own setting.
  - **Read/Write**: The user can read and write the setting for all users.
  - **Execute**: The user can execute this setting.

Change user access settings

For ConnectPort LTS 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 ConnectPort LTS 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.
5. Select the user access options that you want to enable for this user.
6. Click **Apply**. The changes take effect immediately. No logout/login is necessary.

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.

Peripheral

Use the options under **Peripheral** to configure settings for various peripheral devices on ConnectPort LTS, such as SD memory, USB, Modem, LCD, and XBee.

Note USB, Modem, and XBee are supported in ConnectPort LTS W versions only.

SD Memory

The ConnectPort LTS supports standard SD and SDHC (high-capacity) memory cards. To use an SD memory device, insert the card in the SD slot and then select **Start service** on the **SD Memory** page. After you start the SD memory card service, you can see the card information such as:

- Card Type
- File system
- Used size
- Available size

If the SD memory card is not formatted, select the format type and click the **Format** button.

The physical mounting point of SD memory device on the ConnectPort LTS is **/mnt/sd**.

USB

To use the USB device, insert the device in the USB port and then select **Start service** next to the USB device you want to start on the **USB** page.

The ConnectPort LTS W version has two USB ports. After you start the USB service, you can see the device information such as:

- Card Type
- File system
- Used size

If the USB storage device using is not formatted, select the format type and click the **Format** button.

The physical mounting point of USB device on the ConnectPort LTS is **/mnt/usb1** or **/mnt/usb2**.

Modem

Use the Modem page to configure the internal modem for ConnectPort LTS. The Modem page has the same configuration settings of Modem Profile of Serial port settings and it allows you to establish or receive connections from other systems and internal modems. Modem configuration page allows you to use the several connection types.

Modem Settings

The Modem profile allows you to connect a modem to the serial port. When you assign the Modem profile to a serial port, the following settings appear under Modem Settings on the Port Profile Settings page:

- **Incoming Connection**: Modem receives dial-in connections, such as inbound PPP connections or to manage a device through a telephone network. The ConnectPort LTS product server will receive connections from other hosts.
- **Outgoing Connection**: The modem sends dial-out connections to establish connections with external hosts or to connect to an external PPP network.
- **Network Bridge Connection (bi-directional)**: You can use the modem to establish connections to other hosts and receive connections from other hosts.

- **Init String**: This is the modem initialization settings. Modify the init string to change the behavior of the modem as needed by your application/modem model. For more information about the supported modem commands, see the *ConnectPort LTS Command Reference*.

  Note If the modem is currently in use, the init string change will not take effect immediately. It will be used the next time the modem is initialized.

- **Enable PPP Connections on this Modem**: When enabled, modem is used for PPP connections. You will need to configure the PPP connection for incoming and/or outgoing PPP connections. See PPP (Point-to-Point Protocol) for more information.

  Note The Modem profile is most often used when you configure a Digi device server for out-of-band management and PPP.

- **Enable callback**: When enabled, the Digi device disconnects the connection from a remote site and then calls the phone number specified in the **Callback phone number** field.
- **Callback phone number**: The phone number that the Digi device calls when you enable callback.
- **Dial-in modem callback login**: The Digi device calls the phone number specified as the callback phone number after a user authentication.
- **Allow dial-in modem callback number change**: The Digi device will ask a user whether to change the callback phone number before calling.

Service Settings

- **Serial Service Settings**:
  - **TCP Settings**: Your serial device can automatically establish connections to another system or device on the network. This is also referred to as Automatic Connection or AutoConnect.
    - **Automatically establish TCP Connections**: Enable automatic connection to a system or device on the network.

- **Establish connection under one of the following conditions**:
  - **Always connect and maintain connections**: A connection is always available. If a connection is lost it will be reconnected automatically. This type of connection is most often used in client/server configurations where this Digi device server is the client.

    Note Select this option to enable autoconnect for 3-wire devices.

  - **Connect when data is present on the serial line**: A connection is made when the serial port receives data. This type of connection is most often used for terminals and terminal emulation.
  - **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 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.
  - **Connect when DCD (Data Carrier Detect) line goes high**: A connection is made when the serial port's DCD (Data Carrier Detect) signal goes high. This type of connection is most often used for modems. See the Advanced Serial Settings for the option to close the connection when the DCD signal goes low.

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

  - **Connect when DSR (Data Set Ready) line goes high**: A connection is made when the serial port's DSR (Data Set Ready) signal goes high. See the Advanced Serial Settings for the option to close the connection when the DSR signal goes low.

- **Establish connection to the following network service**:
  - **Server (name or IP)**: Type the IP address or host name of the destination device.
  - **Service**: Select the service type of the connection. Your options are as follows:
    - **Raw TCP**—If you are bridging to another Digi device server use Raw TCP.
    - **Rlogin**
    - **Secure Sockets**
    - **Telnet**
    - **SSH**
  - **TCP Port**: Type the TCP port number of the destination device. The standard port numbers are 23 for telnet and 513 for rlogin. If you are bridging to another Digi device server use the raw TCP port number for its serial port. This is usually 2101 for port 1. 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.

    See Assign a profile to a serial port for more information about assigning a Serial Bridge (Serial Tunneling) profile to a serial port.
  - **Enable Keep-Alive**: When selected, enables the Keep-Alive feature.

- **UDP Settings**:
  - **Automatically send serial data**: Enable sending serial data to one or more systems or devices on the network using UDP sockets.
  - **Send data to the following network services**: A list of servers or devices to send data to using UDP. To add a new destination enter the following information and click **Add**.
    - **Description**: A description of the server or device (16 characters or less).
    - **Send To**: The IP address or DNS name to send data to.
    - **UDP Port**: The port number to send data to. If you are sending data to another Digi device server use the raw UDP port number for its serial port. This is usually 2101 for port 1. The format for this port number is as follows:

      ```
      21<serial port number>
      ```

      Replace <serial port number> is 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.
  - **Send data under any of the following conditions**:
    - **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.

- **Network Services Settings**: Enable the access methods that will be used to connect to your serial device. This page displays the currently configured TCP or UDP port.

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.
- **MEI Type**: The MEI (multi-electronic interface) type sets the type of serial interface if the ConnectPort LTS is the MEI version. The MEI version has three kinds of serial interfaces: RS232, RS422/485 (full), and RS485Half. If the ConnectPort LTS is not the MEI version, MEI Type will be fixed to RS232 and you cannot change it.
- **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.
- **Enable termination**: When selected, enables termination.

Advanced Serial Settings

The following settings are advanced settings used to fine tune the serial port and access to the serial interface. The default settings will typically work in most situations.

Note The advanced settings rarely need to be changed.

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.

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

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.

Authentications settings

- **Authentication method**: The authentication method. The default is None.

  The Digi device supports various authentication options, such as None, Local, RADIUS, LDAP.

- **Primary/Secondary authentication server**: The IP address or DNS name of the remote authentication server.
- **Authentication server socket**: The TCP port number of the authentication server.
- **Primary/Secondary account server**: The IP address or DNS name of the remote accounting server. The accounting server is only required when you set the authentication method to RADIUS.
- **Account server socket**: The TCP port number of the accounting server.
- **Shared secret**: A password string used for encryption of messages between the authentication server and the ConnectPort LTS. Only RADIUS servers require a shared secret.
- **Timeout**: The authentication timeout, in seconds. Only RADIUS servers require a timeout value.
- **Retries**: The authentication retry count. Only RADIUS servers require an authentication retry count.
- **LDAP search base**: The LDAP search base string. Only LDAP servers require a search base string.
- **Domain name for active directory**: The LDAP domain name string for Active Directory. Only LDAP servers require a domain name of Active Directory.
- **Secure LDAP**: Allows you to enable Secure LDAP for LDAP servers. The default is Disable. Only LDAP servers require this option.

Note Default permissions for authenticated remote users are defined under the user name **ruser**.

LCD

Use the LCD configuration page to configure the LCD display for *ConnectPort LTS*. The following settings are available on LCD configuration page:

- **Enable display**: When enabled, LCD display is enabled and you can use LCD menu using keypad.
  - **Background image wait time**: Specifies how much user idle time must elapse before the background image is launched on the LCD display. The default is 0 and means the background image will not be launched automatically.
- **Use default background image**: When enabled, the default background image appears on the LCD display when either the wait time is elapsed or the Exit menu is selected using keypad on the LCD display.
- **Load background image**: Upload a background image on the LCD. This product supports only 128 x 64 8 bit bitmap image. If you upload an incorrect image type, an error message appears on LCD screen. After uploading the image, toggle the **Enable display** or **Use default background image** option once to force the LCD daemon to reload the image.
- **Load custom (Python) program**: Upload a custom Python program onto the *ConnectPort LTS*.

For instructions on configuring an IP address using the LCD interface, see ConnectPort LTS LCD interface.

XBee

The XBee configuration page has very similar settings to the Custom serial port profile.

For detailed information about XBee RF modules and commands for configuring them, please refer to the *ZigBee RF Modules User Guide*.

XBee Port Settings

- **Allow direct Access from networks**: When enabled, you can access the XBee port in the same manner that the custom profile accesses a serial port. This setting is **Disabled** by default.

- **Serial Service Settings**:
  - **TCP Settings**: Your serial device can automatically establish connections to another system or device on the network. This is also referred to as Automatic Connection or AutoConnect.
    - **Automatically establish TCP Connections**: Enable automatic connection to a system or device on the network.
    - **Establish connection under one of the following conditions**:
      - **Always connect and maintain connections**: A connection is always available. If a connection is lost it will be reconnected automatically. This type of connection is most often used in client/server configurations where this Digi device server is the client.

        Note Select this option to enable autoconnect for 3-wire devices.

      - **Connect when data is present on the serial line**: A connection is made when the serial port receives data. This type of connection is most often used for terminals and terminal emulation.
      - **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 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.
      - **Connect when DCD (Data Carrier Detect) line goes high**: A connection is made when the serial port's DCD (Data Carrier Detect) signal goes high. This type of connection is most often used for modems. See the Advanced Serial Settings for the option to close the connection when the DCD signal goes low.

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

      - **Connect when DSR (Data Set Ready) line goes high**: A connection is made when the serial port's DSR (Data Set Ready) signal goes high. See the Advanced Serial Settings for the option to close the connection when the DSR signal goes low.

- **Establish connection to the following network service**:
  - **Server (name or IP)**: Type the IP address or host name of the destination device.
  - **Service**: Select the service type of the connection. Your options are as follows:
    - **Raw TCP**—If you are bridging to another Digi device server use Raw TCP.
    - **Rlogin**
    - **Secure Sockets**
    - **Telnet**
    - **SSH**
  - **TCP Port**: Type the TCP port number of the destination device. The standard port numbers are 23 for telnet and 513 for rlogin. If you are bridging to another Digi device server use the raw TCP port number for its serial port. This is usually 2101 for port 1. 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.

    See Assign a profile to a serial port for more information about assigning a Serial Bridge (Serial Tunneling) profile to a serial port.
  - **Enable Keep-Alive**: When selected, enables the Keep-Alive feature.

- **UDP Settings**:
  - **Automatically send serial data**: Enable sending serial data to one or more systems or devices on the network using UDP sockets.
  - **Send data to the following network services**: A list of servers or devices to send data to using UDP. To add a new destination enter the following information and click **Add**.
    - **Description**: A description of the server or device (16 characters or less).
    - **Send To**: The IP address or DNS name to send data to.
    - **UDP Port**: The port number to send data to. If you are sending data to another Digi device server use the raw UDP port number for its serial port. This is usually 2101 for port 1. The format for this port number is as follows:

      ```
      21<serial port number>
      ```

      Replace <serial port number> is 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.
  - **Send data under any of the following conditions**:
    - **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.

- **Network Services Settings**: Enable the access methods that will be used to connect to your serial device. This page displays the currently configured TCP or UDP port.

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.
- **MEI Type**: The MEI (multi-electronic interface) type sets the type of serial interface if the ConnectPort LTS is the MEI version. The MEI version has three kinds of serial interfaces: RS232, RS422/485 (full), and RS485Half. If the ConnectPort LTS is not the MEI version, MEI Type will be fixed to RS232 and you cannot change it.
- **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.
- **Enable termination**: When selected, enables termination.

Advanced Serial Settings

The following settings are advanced settings used to fine tune the serial port and access to the serial interface. The default settings will typically work in most situations.

Note The advanced settings rarely need to be changed.

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.

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

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.

Authentication Settings

- **Authentication method**: The authentication method. The default is None.

  The Digi device supports various authentication options, such as None, Local, RADIUS, LDAP.

- **Primary/Secondary authentication server**: The IP address or DNS name of the remote authentication server.
- **Authentication server socket**: The TCP port number of the authentication server.
- **Primary/Secondary account server**: The IP address or DNS name of the remote accounting server. The accounting server is only required when you set the authentication method to RADIUS.
- **Account server socket**: The TCP port number of the accounting server.
- **Shared secret**: A password string used for encryption of messages between the authentication server and the ConnectPort LTS. Only RADIUS servers require a shared secret.
- **Timeout**: The authentication timeout, in seconds. Only RADIUS servers require a timeout value.
- **Retries**: The authentication retry count. Only RADIUS servers require an authentication retry count.
- **LDAP search base**: The LDAP search base string. Only LDAP servers require a search base string.
- **Domain name for active directory**: The LDAP domain name string for Active Directory. Only LDAP servers require a domain name of Active Directory.
- **Secure LDAP**: Allows you to enable Secure LDAP for LDAP servers. The default is Disable. Only LDAP servers require this option.

Note Default permissions for authenticated remote users are defined under the user name **ruser**.

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.

- **PPP**: Connects incoming clients or serial devices to external networks using modems and telephony to maintain the connection.
- **Python**: For loading and running custom programs authored in the Python programming language.
- **RealPort**: Configures RealPort settings.

PPP (Point-to-Point Protocol)

PPP (Point-to-Point Protocol) provides TCP/IP communication over a modem connected to a serial port on your ConnectPort LTS server. PPP allows you to connect a device to a network using a telephone line and the device has access to the resources of the network as if it were directly connected to the network. Use the PPP (Point-to-Point Protocol) page to connect incoming clients or serial devices to an external network using modems and telephony to maintain the connection.

Basic PPP Settings

Use Basic PPP Settings to configure the most commonly used settings for incoming and outgoing PPP connections. You should configure these settings before creating any incoming or outgoing connections.

You can use Basic PPP Settings to enable or disable the Dynamic IP Address Pool. The Dynamic IP Address Pool is a set of reserved IP addresses unique to the network that are assigned to the incoming connections. You can set the first IP address to use and the number of sequential addresses (plus one) to be reserved for assignment.

- **Enable Dynamic IP Address Pool for Incoming Connections**: Enables or disables the Dynamic IP Address Pool used by incoming connections. The Dynamic IP Address Pool is a set of reserved IP addresses that can be automatically supplied to each incoming PPP connection. Each connection that is set up to automatically assign an IP address is supplied a different address from the pool. The set of addresses in the pool must to be unique to the network so that network conflicts do not occur.
- **First IP Address**: Specifies the first IP address that the address pool should start with. The IP address pool contains this address and all successive addresses up to the number of IP addresses specified plus one for the network interface. For example, if the first IP address is 10.0.0.1 and the number of addresses is 4, then the Dynamic IP Address Pool will contain 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4, and 10.0.0.5.
- **Number of Addresses**: Specifies the number of addresses to use in the pool. Note that you should verify that none of the addresses from the first IP address up to the number of addresses plus one is already in use on the network.

Configure basic PPP settings

To automatically assign an IP address for an incoming PPP client:

1. Select **Application** > **PPP**.
2. Click **Basic PPP Settings**.
3. Select **Enable Dynamic IP Address Pool for Incoming Connections**.
4. Type the IP address for the incoming PPP client in the **First IP Address** field.
5. Type the number of addresses in the **Number of Addresses** field.

6. **Incoming PPP Connections**: Use this section to make and maintain rules for incoming PPP connections. To make a new rule for incoming PPP connections.
    a. Click **New connection**.
    b. On the **Serial Port** section of the Incoming connection page, select the serial ports for this connection rule.
    c. On the **Authentication Configuration** section, type the **User Name** and **Password** to use for PPP authentication such as NONE/PAP/CHAP/BOTH.

    Note To use the **Local** authentication method for serial port authentication, you must enter the **User Name** and **Password** of an existing system user.

    If you are going to use the **None** method for serial port authentication, you can add any user, including users not in the local database of system users, and you can select a user name from the **PPP User** menu on the Authentication page of the serial port.

    d. Select the authentication method from one of following methods:

        NONE: The remote user does not require PPP authentication.

        PAP: Password Authentication Protocol (PAP) authentication is required.

        CHAP: Challenge Handshake Authentication Protocol (CHAP) authentication is required.

        BOTH: Both CHAP and PAP authentication are required.

    e. In the **Peer Configuration** section, select one of the following options for assigning the IP address of the incoming PPP client:

        Automatically assign remote IP address from IP address pool: If you select this option, the IP address for the incoming PPP client will be automatically assigned from the IP address pool set on the Basic PPP Settings page.

        Allow remote peer to specify remote IP address: If you select this option, the incoming PPP client will specify the IP address used for the PPP connection.

        Assign static remote IP address: If you select this option, the IP address for incoming PPP client will be assigned as specified by the Remote IP address.

f. In the **Peer Configuration** section, select **Allow client access to local network via PPP connection** if you want the incoming PPP client to be able to access the ConnectPort LTS or other devices on the network through the ConnectPort LTS PPP interface. Once you enable this option, you can select one of the following options for assigning the IP address of the local PPP interface:

Automatically assign local IP address from IP address pool: The IP address for the local PPP interface is automatically assigned from the IP address pool set on the Basic PPP Settings page.

Assign static local IP address: The IP address for the local PPP interface is assigned as specified by the local IP address.

g. In the **Advanced Configuration** section, select **Enable idle timeout** if you want to close the PPP connection when there is no activity from the incoming PPP client during the time specified by Timeout.

7. **Advanced PPP Settings**: If you want the incoming PPP client to be able to access the local network where the ConnectPort LTS is connected, select the **Process ARP Requests (Proxy ARP)** option.

Note Use **Advanced PPP Settings** when IP addresses assigned to the PPP link are on the same local network subnet as the local LAN.

Incoming PPP Connections

Incoming PPP connections are connections where you can dial in to the ConnectPort LTS device. You can connect to the ConnectPort LTS device using a modem to dial the phone number of the modem connected to the serial port. For example, you can use a modem to access the network associated with the Digi device server or use modems to create a network bridge by connecting two separate networks.

See Configure incoming PPP connections for more information.

- **Serial ports**: Select the serial ports or internal modem associated with incoming PPP connections.

- **Authentication Configuration**:
  - **User Name**: Specifies the user name for this connection. The user provides the user name and password when connecting to the device. This user name must be unique to the device so that no other incoming PPP connection, outgoing PPP connection, or system user uses it.
  - **Password**/**Confirm Password**: Specifies the password for this connection. This is the password that the user specifies when connecting and logging into the device.
  - **Associate with "ANYBODY"**: Select this check box when multiple PPP users will connect to one or more serial ports. When you clear this check box, there is only one user dedicated to the selected ports.
  - **Authentication**: Specifies the type of authentication required by this PPP connection. You must supply the same type of authentication for your dial-up connection as specified here in order to successfully connect.

    NONE: No authentication is required. This is the recommended default for authentication.

    CHAP: CHAP (Challenge Handshake Authentication Protocol) provides secure encrypted authentication. CHAP periodically verifies the identity of the peer using a 3-way handshake. This is done upon initial link establishment and may be repeated anytime after the link has been established. (See RFC 1334 for further details.) CHAP authentication will work between two ConnectPort LTS devices.

    Note ConnectPort LTS does not support MS-CHAP (Microsoft specific implementation of CHAP).

    PAP: Many ISPs and corporate PPP servers use PAP (Password Authentication Protocol). PAP provides a simple method for the peer to establish its identity using a 2-way handshake. This is done only upon link establishment. (See RFC 1334 for further details.)

    BOTH: CHAP authentication will work between two ConnectPort LTS products. CHAP will be negotiated to PAP for all other connections.

- **Peer Configuration**: Specifies how to assign the remote IP address that is supplied to the client.
  - **Automatically assign remote IP address from IP address pool**: Automatically assigns the remote IP address with a unique address from the IP address pool (as configured in Basic PPP Settings). The assigned address will not conflict with any other PPP connection using the Dynamic IP Address Pool.

    Note The Dynamic IP Address Pool must be enabled.

  - **Allow remote peer to specify remote IP address**: The remote peer automatically assigns the remote IP address.
  - **Assign static remote IP address**: Assigns the IP address entered in the **Remote IP Address** field to the remote IP address. This connection will always be assigned this same IP address. Use this option if the client needs to have the same IP address if it is running as a server.
  - **Remote IP Address**: Specifies the static remote IP address.
  - **Allow client access to local network via PPP connection**: Specifies whether the remote client should have access to the local Ethernet network when they dial in to the PPP connection. This option requires the ConnectPort LTS device to have a unique local IP address for each PPP connection to handle the routing between the PPP connection and the local network.
  - **Automatically assign local IP address from IP address pool**: Automatically assigns the local IP address with a unique address from the IP address pool (as configured in Basic PPP Settings). The assigned address will not conflict with any other PPP connection using the Dynamic IP Address Pool.

    Note The Dynamic IP Address Pool must be enabled.

  - **Assign static local IP address**: Assigns the IP address entered in the **Local IP Address** field to the local IP address. This connection will always be assigned this same IP address. Use this option if the client needs to have the same IP address if it is running as a server.
  - **Local IP Address**: Specifies the local IP address to use for the PPP connection. This IP address must be unique on the network and must not be the same as the remote IP address or any address in the Dynamic IP Address Pool. Digi recommends that this address should reside on a different subnet than the Ethernet IP address.

- **Advanced configuration**: Specifies how to assign the remote IP address supplied to the client.

  Enable Idle Timeout: When selected, enables idle timeout for this connection. The idle time is the elapsed time after receiving the last byte from this connection. If you clear this check box, the connection can remain idle for any amount of time. If you select this check box, the connection closes after the connection has been idle for specified number of seconds in the **Timeout** field.

- **Timeout**: The maximum allowed time (in seconds) a connection can remain idle before it is closed.

Configure incoming PPP connections

This section describes how to configure an incoming PPP connection. Use it to configure a PPP connection that will be initiated by another system dialing into the ConnectPort LTS server.

Prerequisite Assign a modem profile with an incoming connection to the Digi device server port. See Assign a profile to a serial port for more information.

To configure the rules for incoming PPP connections:

1. Select **Application** > **PPP**.
2. Click **Incoming PPP Connections**.
3. Click **New Connection**.
4. Under **Authentication Configuration**, complete the following fields:
   - **User Name**: Type the user name.
   - **Password/Confirm Password**: Type the password.
   - **Associate with "ANYBODY"**: Enable when you want the user name and password associated with any PPP user.
   - **Authentication**: Choose one of the following authentication methods:
     - **NONE**: The remote user does not require PPP authentication.
     - **CHAP**: Challenge Handshake Authentication Protocol (CHAP) authentication is required.
     - **PAP**: Password Authentication Protocol (PAP) authentication is required.
     - **BOTH**: Both CHAP and PAP authentication are required.

   PPP authentication uses this information.

   Note To use the **Local** authentication method for serial port authentication, you need to enter the user name and password of an existing system user. If not, the PPP connection will fail because you cannot specify a PPP user on the **Authentication** page of the serial port separately.

   If you choose the **None** authentication method for serial port authentication, you can add any user even if the user is not in the local database as a system user; you can select a user name from the **PPP User** menu on the Authentication page for the serial port.

5. Under **Peer Configuration**, select one of the following options for assigning the IP address of an incoming PPP client:
    - **Automatically assign remote IP address from IP address pool**: Select this option if you want to automatically assign the IP address for the incoming PPP client from the IP address pool set on the Basic PPP Settings page. If you want the IP address to be assigned dynamically, you must first configure a pool of IP addresses on the Basic PPP Settings page. See Basic PPP Settings for more information.
    - **Allow remote peer to specify remote IP address**: Select this option if you want the incoming PPP client to specify the IP address to use for the PPP connection.
    - **Assign static remote IP address**: Select this option if you want to assign the IP address for incoming PPP client as specified by the Remote IP address.
6. Under **Peer Configuration**, select **Allow client access to local network via PPP connection** if you want the incoming PPP client to access the ConnectPort LTS or other devices on the network through the ConnectPort LTS PPP interface. If you enable this option, select one of the following options for assigning the IP address of the local PPP interface.
    - **Automatically assign local IP address from IP address pool**: Automatically assign the IP address for the local PPP interface from the IP address pool set on the Basic PPP Settings page. If you choose this option, type the IP address in the **Remote IP Address** field.
    - **Assign static local IP address**: Assign the IP address for the local PPP interface is as specified in the **Local IP Address** field. If you choose this option, type the IP address in the **Local IP Address** field.
7. Under **Advanced Configuration**, select **Enable idle timeout** if you want to close the PPP connection when there is no activity from the incoming PPP client after a specified number of seconds and type the number of seconds in the **Timeout secs** field.

The dial-in user will need to know the following:

- The phone number for the modem attached to this Digi device server.
- The **Username**, **Password**, and type of **Authentication** configured in the preceding task.

Setting up incoming PPP connections

To correctly configure the settings for incoming PPP connections:

1. Select **Application** > **PPP**.
2. Configure the PPP settings.
3. Select **Configuration** > **Serial Ports**.
4. Configure the serial port settings.

Outgoing PPP Connections

Use **Outgoing PPP Connections** to configure outgoing PPP connections.

The ConnectPort LTS device uses the outgoing PPP connections to connect to an external modem or ISP. Outgoing PPP connections typically automatically connect the Digi device server to an external

modem or ISP network when the main Ethernet network goes down. This allows the device to continue communication on the network or allow connections from the network when the main Ethernet network is down.

- **Username**: The username for this connection.
- **Phone Number 1**: The phone number used to connect to the remote system.
- **Phone Number 2**: Alternate phone number used to connect to the remote system.
- **Action**: Lists the available actions per user. The **Remove** action allows you to remove the user.

Configure outgoing PPP connections

This section describes how to configure an outgoing PPP connection. Use it to configure a PPP connection that will be initiated by another system dialing into the ConnectPort LTS server.

Prerequisite Assign a modem profile with an outgoing connection to the Digi device server port. See Assign a profile to a serial port for more information.

To create or modify the rules for outgoing PPP connections:

1. Select **Application** > **PPP**.
2. Click **Outgoing PPP Connections**.
3. Choose one of the following options:
   - To create a new rule, click **New Connection**.
   - To modify an existing rule, click a user name under the **Username** column.
4. Under **Serial Ports**, select the serial ports to which you want the connection rule to apply.

5. Under **Authentication Configuration**, complete the following fields:
   - **User Name**: Type the user name.
   - **Password/Confirm Password**: Type the password.
   - **Phone Number 1**: Specifies the phone number used to connect to the remote system.
   - **Phone Number 2**: Specifies the alternate phone number used to connect to the remote system.
   - **Authentication**: Choose one of the following authentication methods:
     - **NONE**: The remote user does not require PPP authentication.
     - **CHAP**: Challenge Handshake Authentication Protocol (CHAP) authentication provides secure encrypted authentication. CHAP periodically verifies the identity of the peer using a 3-way handshake. This is done upon initial link establishment and may be repeated anytime after the link has been established. (See RFC 1334 for details.) CHAP authentication will work between two ConnectPort LTS devices.

       Note MS-CHAP (Microsoft specific implementation of CHAP) is not supported.

     - **PAP**: Password Authentication Protocol (PAP) authentication is required. PAP provides a simple method for the peer to establish its identity using a 2-way handshake. This is done only upon link establishment. (See RFC 1334 for further details.)
     - **BOTH**: Both CHAP and PAP authentication are required (recommended).
   - **Use login script**: Enable when you want to use a login script and type the path to the login script in the **Dial chat script** field.

   PPP authentication uses this information.
6. Under **Peer Configuration**, select one of the following options for assigning the IP address of an incoming PPP client:
   - **Automatically obtain remote IP address remote peer**: Select this option if you want to automatically assign the IP address supplied by the remote peer.
   - **Request specific address**: Select this option if you want to request the specified **IP Address** from the remote peer. There is no guarantee this IP address is assigned to this connection. The address is only requested. Some service providers do not allow you to request IP addresses and others only allow you to assign a certain range of addresses. Ask the service provider of the system you want to connect to if you can request an IP address.

Advanced PPP Settings

The ConnectPort LTS product uses advanced PPP settings to enable the routing table to use and process ARP requests received by this device. Process ARP requests are also known as Proxy ARP. ARP requests inform devices how and where to connect to a specific device. PPP connections use this setting. The setting is disabled by default.

Configure advanced PPP settings

To enable or disable Proxy ARP:

1. Select **Application** > **PPP**.
2. Click **Advance PPP Connections**.
3. Select or clear the **Process ARP Requests (Proxy ARP)** check box to enable or disable Proxy ARP.
4. Click **Apply** to save your changes.

Configure settings on serial ports

To configure the settings on serial ports:

1. Select a port from **Configuration** > **Serial ports** > **Ports Settings**.
2. Click **Change Profile** and change the port profile to **modem**.
3. In the **Port Profile Settings** > **Modem Settings** section, select **Incoming Connections**.
4. Select **Enable PPP connections on this modem** if you want to establish a PPP connection.
5. Set configurations on **Basic Serial Settings** and **Advanced Serial Settings** sections according to your environment.
6. Select the authentication method of the serial port in the **Authentication Settings** section. If the port profile is set to **modem**, you can only select **None** or **Local** authentication method.
7. Select **PPP User** from the list if you set authentication method to None.

   If you select the **Local** authentication method, you cannot select a PPP user separately. To make the correct PPP connection with the **Local** serial port authentication method, you need to have the PPP connection configuration with the same user name and password as in the local system user database set on **Configuration** > **Users**. (See Configure incoming PPP connections.)

   Note If your serial port or internal modem uses local authentication with a user in the local database, you must use the Show Terminal window on your PPP client. When the terminal window opens, log in to the serial port and then close the terminal window. PPP negotiation will start once you close the terminal window.

Python Configuration

If you have a Python-enabled ConnectPort LTS device, you can manage Python files using the **Application** > **Python** menu options. Python options include:

- Uploading Python program files to the ConnectPort LTS device
- Deleting a Python program file from the device
- Configuring which Python programs to execute when the ConnectPort LTS device boots (also known as auto-start programs)

Python Files

The Python Files page allows you to upload and manage Python programs on a ConnectPort LTS device.

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

Auto-start settings

Use the **Auto-start Settings** page to configure Python programs to execute when the ConnectPort LTS 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 ConnectPort LTS 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 ConnectPort LTS 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 ConnectPort LTS 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 2.6.2. Use modules known to be compatible with this version of the Python language only.

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 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.

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

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 the ConnectPort LTS support page.
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.

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.

Management

Use the **Management** menu to view and manage connections and services for the ConnectPort LTS product.

You can monitor the port, device, system, and network activities of ConnectPort LTS 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 ConnectPort LTS products.

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 PPP connections

The **Active PPP Connections** list provides an overview of connections associated with PPP interfaces.

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.

Port Logging Management

The Port Logging Management page displays the logs for a selected port.

- Logging: Displays one of the following options:
  - **On**: Logging is enabled.
  - **Off**: Logging is disabled.
- **Buffer Utilization**: Displays the percentage of buffer utilization.
- **Pause Logging**/**Start Logging**: Allows you to stop and start logging.
- **Refresh**: When clicked, displays the latest log information.
- **Clear Log**: When clicked, deletes the log information.

Administration

You can periodically perform administration tasks on ConnectPort LTS 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:

- **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.
- **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.
- Enable password authentication for the ConnectPort LTS device. See Users for more information.

Certificate Management

Use the Certificate Management page to upload your certificates and private key to the Digi device server.

CAUTION! You must restart the web server for changes to take effect. To restart the web server, click **Restart Web Server**.

You can also generate a temporary self-signed certificate for testing purposes. To generate a temporary certificate, click **Generate**.

File Management

Use the **File Management** page to upload custom files to a ConnectPort LTS 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). The root user also can delete custom files by accessing the command-line interface.

Backup/Restore

After you configure a ConnectPort LTS 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

To backup a device configuration:

1. Click **Administration** > **Backup/Restore**. The Backup/Restore page appears.
2. Select the storage location type. The ConnectPort LTS basic version supports NFS/Samba/User space/Local machine for the location. The default filename for the backup file is backup.cfg.
3. Click **Backup**.

To restore a device configuration:

1. Click **Administration** > **Backup/Restore**. The Backup/Restore page appears.
2. Select the storage location type. The ConnectPort LTS basic version supports NFS/Samba/User space/Local machine for the location. The default filename for the backup file is backup.cfg.
3. Select the **Keep Network Settings** check box if you want to retain the basic network settings, such as IP address, subnet mask, and gateway.

   Note If the restored configuration modifies the network settings, your Digi device server will dynamically switch to the new settings. You will need to manually redirect your browser to the new IP address.

4. Select the file to restore from the **Restore From File** field or click **Choose File** to locate and select the file.
5. Click **Restore**.

Backup or restore a device configuration from a TFTP or BOOTP server from the command line

From the command-line interface, the **backup** command backs up the device configuration to a TFTP or BOOTP server located on the network or a storage device in the ConnectPort LTS device, or restores the configuration.

The format for the **backup** command is as follows:

```
backup [to=serveripaddress[:filename]|
[to={sd|usb|nfs|samba|userspace}[:filename]]
[from=serveripaddress[:filename] print]|
[from={sd|usb|nfs|samba|userspace}[:filename]]
```

Parameters

- **to=*serveripaddress*[:*filename*]**: The IP address of the TFTP server where you save the configuration file and the name of the configuration file. If you do not specify a filename, the default filename is config.rci.
- **to=(sd|usb|nfs|samba|userspace)[:*filename*]**: The location of the storage device where you save the configuration file and the name of the configuration file. If you do not specify a filename, the default filename is config.rci.
- **from=*serveripaddress*[:*filename*]**: The IP address of the TFTP server where the configuration file resides and the name of the configuration file you want to restore. If you do not specify a filename, the default filename config.rci is used. In ConnectPort LTS, after you restore the configuration file the system will be rebooted.
- **from=(sd|usb|nfs|samba|userspace)[:*filename*]**: The location of the storage device where the configuration file resides and the name of the configuration file you want to restore. If you do not specify a filename, the default filename config.rci is used.
- **print**: Prints the current device configuration.

Example:

```
#> backup from=10.0.0.1:config.rci
```

Update Firmware

To update the firmware for a ConnectPort LTS device, choose one of the following options:

- Updated the firmware from **Administration** > **Update Firmware** page in the web interface.
- Update the firmware from the command-line interface via TFTP or BOOTP.

Digi recommends downloading the firmware to a local hard drive before upgrading the firmware.

Update the firmware from the web interface

Before you update the firmware from the web interface:

1. Download the latest firmware from http://www.digi.com/support.
2. Read the release notes to determine if there are any special steps to complete before updating the firmware.

To update the firmware from the web interface:

1. Sign in to the web interface.
2. Click **Administration** > **Update Firmware**. The Update Firmware page appears.
3. Click **Choose File** to locate and select the firmware file.
4. Click **Update**.

> **Important** DO NOT close the browser until the update is complete and a reboot prompt appears.

Update the firmware from the command-line interface on a TFTP or BOOTP server

Before you update the firmware from the web interface:

1. Download the latest firmware from http://www.digi.com/support.
2. Read the release notes to determine if there are any special steps to complete before updating the firmware.
3. Ensure the TFTP or BOOTP server is running before you start this task.

To update the firmware from a TFTP or BOOTP server:

- From the command-line interface on a TFTP or BOOTP server, issue the following command:

```
boot load=host ip address:loadfile
```

See the description of the **boot** command in the *ConnectPort LTS Command Reference* for more information.

Update the BIOS code

You can only update the BIOS code through the boot loader. To update BIOS code, see ConnectPort LTS disaster recovery.

Important Before uploading the firmware, read the firmware Release Notes to see if you need to update the BIOS code before updating the firmware.

Factory default settings

Restoring a ConnectPort LTS device to its factory default settings clears all current configuration settings 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 ConnectPort LTS 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 ConnectPort LTS product from the web interface for more information.

- From the command-line interface, using the **boot** or **revert** commands
- Using the reset button on the ConnectPort LTS 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 ConnectPort LTS product using the Reset button for more information.

- From the LCD display under **Miscellaneous**

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.

- **Restore**: Returns the configured settings on the Digi device to the factory defaults.
- **Keep network settings**: Select this check box to retain the IP address settings.
- **Restore Only Serial Port Settings**: Select this check box to restore only the serial settings to their factory defaults. The other configuration settings remain as-is.

Reset the factory settings on a ConnectPort LTS product from the web interface

To reset the factory settings on the ConnectPort LTS 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. (Optional) Choose one or both of the following options:
   - To keep the network settings for the device, such as the IP address, select the **Keep network settings** check box.
   - To reset the serial port settings only, select the **Restore Only Serial Port Settings** check box.
4. Click **Restore**.

Reset the factory settings on a ConnectPort LTS *product using the Reset button*

To reset the factory settings on a ConnectPort LTS product using the Reset button:

1. Locate the **Factory Reset** button on the front of device, as shown in the following image.

2. Gently press the Factory Reset button with a non-conducive, small diameter tool (such as wood or plastic) with a blunt end. Do not use a sharp-ended tool or the button could be damaged.
3. Hold down the **Factory Reset** button for 2~3 seconds and then release it.
4. Check the status of the **Ready** LED. When the restoration is complete, the **Ready** LED will turn on again.

System information

The System Information page displays general system information about the ConnectPort LTS 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 ConnectPort LTS product.
- **Ethernet 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.
- **Bios 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.
- **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.

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.
- **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.

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 ConnectPort LTS product.

Ethernet Connection Statistics

- **Speed**: Ethernet link speed: 10, 100, or 1000 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.
- **Packets Received**: Number of packets received and delivered to a higher-layer protocol.
- **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 ConnectPort LTS product initiates a connection request with a server.
- **Passive Opens**: Number of passive opens. In a passive open, the ConnectPort LTS 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.
- **Currently Established**: The number of established connections that have been reset.
- **Resets Sent**: The number of sent resets.

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.
- **Messages Sent**: Number of ICMP messages sent.
- **Dest. Unreachable Messages Sent**: Number of ICMP destination unreachable messages sent.
- **IPv6 Messages Received**: Number of IPv6 messages received.
- **IPv6 Bad Messages Received**: Number of IPv6 messages received with errors.
- **IPv6 Destination Unreachable Messages Received**: Number of IPv6 destinations unreachable messages received. A destination unreachable message is sent to the originator when a datagram fails to reach its intended destination.
- **IPv6 Messages Sent**: Number of IPv6 messages sent.
- **IPv6 Dest. Unreachable Messages Sent**: Number of IPv6 destination unreachable messages sent.

XBee Network

Use this section to view XBee module activity and detailed statistics. This information may aid in troubleshooting network communication problems with your XBee network.

Gateway Device Details

This Gateway Device Details page displays the current PAN ID, channel, and gateway address used by the XBee network.

Network View of the XBee Devices

Use the **Discover XBee Devices** button to refresh the list of devices that joined the XBee network. (Note that the discovery operation may take a few seconds.) Click an entry in the device's table to

view detailed information about the state of that device on the XBee Device State page.

Field	Description
Node ID	The user assigned identifier of the node.
Network Address	The 16-bit network address of the node.
Extended Address	The unique 64-bit MAC address of the node.
Node Type	The role that the XBee module in the gateway serves in the XBee network. For a gateway, the XBee module is a coordinator.
Product Type	The product type of the XBee module.
Clear list before device discovery	Clears the network view of XBee devices of any previously discovered nodes prior to any new discovery/display XBee network actions.

Python Application XBee Socket Counter

The Python Application XBee Socket Counter pane displays data counters that are specific to ZigBee Sockets implemented using a Python application.

Field	Description
Frames Sent	The total number of transmitted frames.
Frames Received	The total number of received frames.
Bytes Sent	The total number of bytes sent.
Bytes Received	The total number of bytes received.

Python Application XBee Socket Error Counters

This Python Application XBee Socket Error Counters pane displays data counters that are specific to XBee Sockets implemented using a Python application. Use these values to determine the quality of sent or received data.

Field	Description
Transmit Frame Errors	The total number of transmitted frames that could not be transmitted due to an I/O error.
Receive Frame Errors	The total number of received frames where an error occurred.
Received Bytes Dropped	The total number of bytes dropped due to an exhaustion of internal buffers.
Received Bytes Truncated	Number of received bytes that were dropped because the user buffer passed to recvfrom() was not large enough to contain the entire packet.

XBee Device State

Use the XBee Device State page to see detailed information on the state of the wireless node. The parameters that appear on this page will vary based on the capabilities supported by the node's RF

module.

Reboot

Changes to some device settings require saving the changes and rebooting the ConnectPort LTS. Use the Reboot page to reboot the ConnectPort LTS. To reboot a ConnectPort LTS 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, SSH, and telnet. For example, you can disable access to all network services that are not required for running or interfacing with the ConnectPort LTS 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 ConnectPort LTS product. See Basic Network Services Settings.

Configure and manage the device using the ConnectPort LTS command line interface

You can issue commands from the command line to configure, manage, and monitor 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.

Access the command-line interface

To access the command-line interface and send configuration commands to the ConnectPort LTS device:

1. Choose one of the following options:
   - Launch the command-line interface from the Digi Device Discovery Utility.
   - Use the **telnet**/**ssh** command to launch the command-line interface.
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 ConnectPort LTS device. For example:

   ```
   #> telnet 192.3.23.5
   ```

   For secure connections, use the **ssh** command as follows:

   ```
   #> ssh username@ip-address
   ```

   Replace username with the user name used to sign in to the ConnectPort LTS device and replace ip-address with the IP address of the device. For example:

   ```
   #> ssh root@192.3.23.5
   ```

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

   After you successfully sign in to the command-line interface, you can access the configuration shell interface (configshell) or the general bash-shell, according to the your user settings for system interface access. When the user system interface access option is set to Shell, you can access the general bash-shell directly and run various system commands. In addition, you can run the configshell command to enter the configuration-specific shell interface. If the your system interface access option is set to CLI menu, the you can access the configuration shell interface directly, but you cannot access the general bash-shell.

Basics for using the command-line interface

The ConnectPort LTS 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
- info
- set alarm
- set buffer and display buffer
- 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 ConnectPort LTS product:

- newpass
- set alarm
- set autoconnect
- set buffer and display buffer
- set group
- set host
- set ippool
- set lcd
- set modem
- set network

- set nfs
- set permissions
- set pmodem
- set portauth
- set ppp
- set profiles
- set python
- set realport
- set rtstoggle
- set samba
- set sdmemory
- set serial
- set service
- set smtp
- set snmp
- set socket_tunnel
- set switches
- set sysauth
- set syslog
- set system
- set tcpserial
- set trace
- set udpserial
- set user
- set web
- set xbee

backup print

Print the configuration file in command-line format. You can use this to cut and paste into scripts.

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**).
- Logged serial data (**display buffers**).
- 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.

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, bios, and firmware versions, memory usage, utilization, and uptime. For models with dual power supplies, such as ConnectPort LTS 16 MEI 2AC, this command displays the status of the power supplies.
- 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
- ZigBee statistics. The **info zigbee_sockets** command displays the following information:
  - The number of frames received or sent
  - The number of bad frames received or sent
  - The number of bytes received or sent
  - The number of received bytes dropped or truncated

newpass

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

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.

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 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 ippool

Use the **IP pool** command to configure the IP pool for the PPP connection.

set lcd

Use the **set lcd** command to configure the LCD.

set modem

Use the **set modem** command to configure the modem profile.

set network

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

set nfs

Use the **set nfs** command to configure NFS.

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 portauth

Use the **set portauth** command to enable authentication for serial ports.

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 python

Use the **set python** command to configure Python.

set realport

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

set rtstoggle

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

set samba

Use the **set samba** command to configure the Samba server.

set sdmemory

Use the **set sdmemory** command to configure the SD memory.

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 smtp

Use the **set smtp** command to configure SMTP.

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 socket_tunnel

Use the **set socket_tunnel** command to configure the socket tunnel.

set switches

Use the **set switches** command to configure the MEI type and termination.

set sysauth

Use the **set sysauth** command to enable authentication for the web interface and command-line interface.

set syslog

Use the **set syslog** command to configure the system log.

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 trace

Use the **set trace** command to configure the trace log.

set udpserial

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

set user

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

set web

Use the **set web** command to configure the web timeout value in minutes.

set xbee

Use the **set xbee** command to configure the XBee.

show

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

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.

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 ConnectPort LTS 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 to=*serveripaddress*[:*filename*]**
Update firmware	**boot** To update the firmware: 1. Telnet or ssh to the Digi device command-line interface using a telnet/ssh application. 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**
Configure device server for tracing and display tracing information	**set trace**

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) manages and monitors network ConnectPort LTS 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.

About Simple Network Management Protocol (SNMP)

SNMP is a widely-used standard protocol that allows you to manage all device nodes on an IP network, solve network problems, and improve network performance.

Most Digi devices support SNMP versions 1 and 2.

ConnectPort LTS supports SNMP versions 1, 2, and 3.

SNMP is easy to implement in extensive networks because the standard architecture allows you to easily program new variables and drop in new devices into a network.

However, because device communication is UDP-based, the communication is not secure. If you require secure communications with a device, use an alternate device interface. Also, SNMP does not allow you to perform all the tasks available from the ConnectPort LTSweb or command line interfaces, such as file management, uploading firmware, or backing up and restoring configurations. Compared to the web or command-line interfaces, SNMP offers a limited set of management and configuration options.

Management Information Bases (MIBs)

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.

Viewing MIB-II components

For an overview of the SNMP interface and the MIB-II components:

1. Go to www.rfc-editor.org/search/rfc_search.php.
2. Search for **MIB-II**.

3. From the results, select the text file *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*.

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.

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**.

SNMP configuration

You can configure basic network and serial configurations for ConnectPort LTS 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 ConnectPort LTS-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.

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

Supported RFCs and MIBs

ConnectPort LTS 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.

- **DIGI enterprise MIBs**
  - DIGI 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 SERIAL ALARM TRAPS MIB—A Digi enterprise MIB for sending alarms as SNMP traps.
  - DIGI ConnectPort LTS MIB—A Digi enterprise MIB for configuring ConnectPort LTS.

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

ConnectPort LTS LCD interface

This section discusses how to configure, monitor or diagnose a ConnectPort LTS device using the LCD interface.

Keys

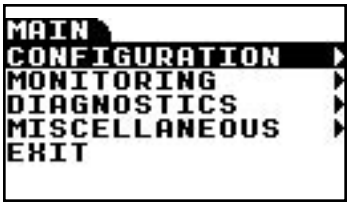
Use the keys on the right side of LCD display to select menu options. The selected menu option is displayed with white characters on black background.

- **Up**: Move up.
- **Dn**: Move down.
- **Sel**: Select the current menu item. If the item has a submenu, a black triangle mark is displayed at the end of line. If the item does not have a submenu, the action assigned to the menu item is performed.
- **Ext**: Go to the upper menu or run the action assigned to the selected menu item. The current menu level appears on the top left top of the LCD screen. The upper menu appears on the top right of the LCD screen.

Keypad operations

When you turn on the ConnectPort LTS, the following image appears on the LCD screen by default:

Press any key to display the LCD main menu.



If a menu item has submenus, a black triangle appears to the right of the menu item. Use the **Up** or **Dn** keys to navigate the menu.

Press the **Sel** key to display the submenu associated with the selected menu item. The name of the submenu appears on the left at the top of the screen. For example, the **CONFIG** tab indicates you are on the CONFIGURATION menu. The **MAIN** tab is the upper menu. To return to the upper menu, press **Ext**.)

Configuring the ConnectPort LTS using the LCD interface

You can configure the following ConnectPort LTS settings using the LCD interface:

- **IP settings #1**: Sets IP mode, IP address, subnet mask, and the default gateway of network interface #1.
- **IP settings #2**: Sets IP mode, IP address, subnet mask, and the default gateway of network interface #2.
- **Host name**: Specifies the host name of the device.
- **DNS**: Specifies the primary DNS of the device.

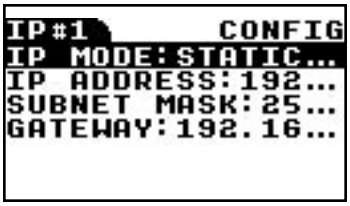
Note You can only set IPv4 mode. You cannot configure IPv6 using the LCD interface.

Change the IP settings

You can change the IP mode, as well as the IP address, subnet mask, and default gateway settings.

To set the IP Mode:

1. From the LCD main menu, select **CONFIGURATION**.
2. Select either **IP SETTINGS #1** or **IP SETTINGS #2**. The following IP menu appears:

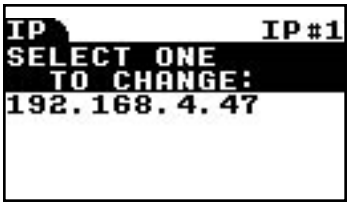


3. Select **IP MODE** and then select one of the following options:

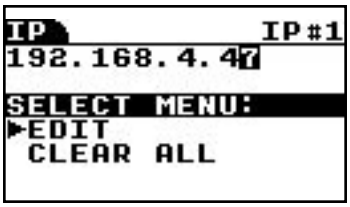
- **DISABLE**: Disable this Ethernet interface.
- **STATIC IP**: Set the IP mode to STATIC. If you set the IP address mode to STATIC, you can set the static IP address, subnet mask, and gateway addresses.
- **DHCP**: Set the IP mode to DHCP.

To change the IP address:

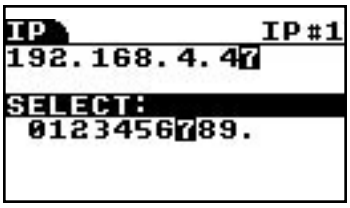
1. Select **IP ADDRESS** from the **IP** menu.



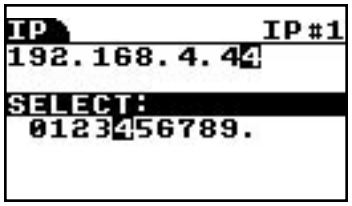
2. Select the IP address that you want to change.



3. Choose one of the following options:
   - Select the **EDIT** menu to change the IP address.



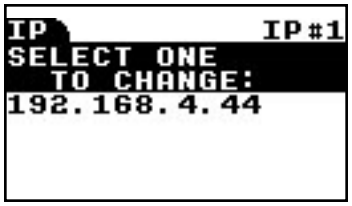
     a. From this menu, choose a character under **SELECT** using the **Up** (Left) and **Dn** (Right) keys. The following image shows how the IP address on the upper line changes as you select each number:



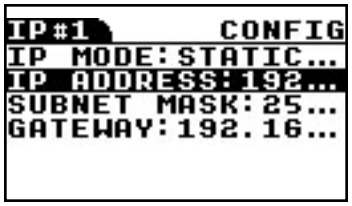
     Note that you can choose the null character (first letter) to clear a selected letter.

     b. Choose another character by pressing **Ext** key twice. Repeat the steps to change the letter as described above.

     c. When you finish changing the characters, press the **Ext** key.



     d. Enter the IP settings menu again to change the **SUBNET MASK** or **GATEWAY** in the manner described above.



     e. Press the **Ext** key when the **IP SETTINGS** menu is displayed.

f. Choose one of following options:
- **SAVE APPLY**: Save and apply configuration changes.
- **DISCARD CHANGES**: Discard all changes.
- **CANCEL**: Discard all changes and return to **IP SETTINGS** menu.

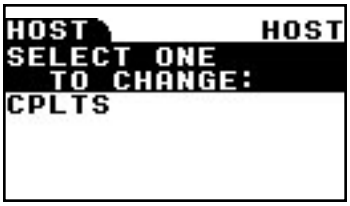
- Select the **CLEAR ALL** menu to clear the entire IP address.

Change the hostname

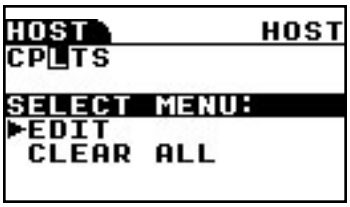
To change the hostname:

1. Access the host name menu by selecting **CONFIGURATION** and then **HOST NAME**.

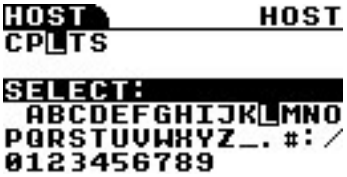
2. Press the **Sel** key again.



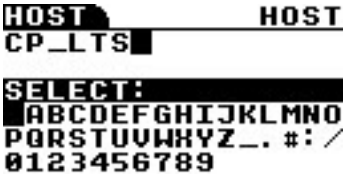
3. Move cursor position using the **Up** (Left) and **Dn** (Right) keys. Once you position the cursor to the item you want to change, press the **Sel** key to enter the editing submenu.



4. On the editing submenu screen, select **EDIT** to change the selected letter or **CLEAR ALL** to clear all host names displayed on the screen. Selecting **EDIT** displays the following submenu:



5. On the submenu, choose a character using **Up** (Left) and **Dn** (Right) keys. The host name on the upper line changes automatically as follows:



6. After changing the selected letter, choose another letter by pressing the **Ext** key twice. Repeat the steps as needed until you have finished entering the host name. When you have finished changing letters, press the **Ext** key several times until you see the following screen.

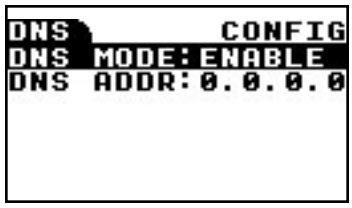
7. Choose one of following options:
   - **SAVE APPLY**: Save and apply configuration changes.
   - **DISCARD CHANGES**: Discard all changes.
   - **CANCEL**: Discard all changes and return to the HOST NAME menu.

Change the DNS configuration

1. Select **CONFIGURATION** and then **DNS**.

2. Press the **Sel** key again.

3. Choose **ENABLE** and press the **Ext** key.



4. Set the IP address of the DNS server in the same manner as setting the IP address.

Monitoring the status using the LCD interface

You can monitor the following status information through the LCD interface:

- **Serial port**
  - **Configuration**: Profile, Baudrate, Data Bit, Parity Bit, Stop Bit, Flow control, Port Type
  - **Signal status**: RTS, CTS, DTR, DSR, DCD
  - **Statistics**: Data In, Data out, Parity Error, Framing Error, Overrun error
- **Ethernet**
  - Speed, Duplex, Bytes Received, Bytes Sent, Packets Received, Packet Sent
- **System**
  - Product Model, F/W version, Bios version, IP Address, MAC address, CPU Utilization, UP Time, Memory (Total, Used, Free)

Running diagnostics using the LCD interface

You can run the following diagnostics run through the LCD interface:

- **Auto Test**: Run all possible hardware tests and show the results.
- **Individual Test**: Run the following tests by selection or manually: EEPROM, UART (Internal and External), Ethernet, USB, SD Memory, Modem, XBee.

Miscellaneous functions in the LCD interface

You can run the following functions from the Miscellaneous menu.

- **Factory Reset**: Restore the configuration to factory defaults.
- **LCD setting:** Reset the LCD configuration or select a background image.

Run the Factory Reset

To run the Factory Reset from the LCD interface:

1. Select **Miscellaneous** and then **FACTORY RESET**.

2. Select **APPLY** to restore the device configuration to factory default values and automatically reboot the device.

LCD settings

Select the LCD setting menu by selecting **MISCELLANEOUS** and then **LCD SETTINGS**.

You can select the following functions:

- **RESET**: Restore the LCD configuration, including the background image, to the factory defaults.
- **SELECT IMAGE**: Choose a background image.

Change the LCD settings

To change the LCD settings:

1. Select **MISCELLANEOUS** and then **LCD SETTINGS**. The LCD settings menu appears.

2. Choose one of the following options:
   - To reset the LCD configuration settings, select **RESET** and then click **APPLY** to confirm your changes when you see the following confirmation message:

   - To change the background image, select **SELECT IMAGE** and choose one of the following options.
     - **DEFAULT IMAGE**: Restore the original background image.
     - **USER IMAGE**: Select a new background image and follow the prompts.

ConnectPort LTS disaster recovery

The Digi ConnectPort LTS provides a disaster recovery procedure in the event the configuration data is destroyed or corrupted. The Digi ConnectPort LTS automatically restores a corrupted configuration file system to the factory default settings. If the Digi ConnectPort LTS device fails to boot after you run a factory reset to restore the factory default settings, you can restore the firmware from the Bios menu.

Restore *ConnectPort LTS* to Factory Default Settings

To restore the ConnectPort LTS to the factory default configuration settings, use a TFTP or BOOTP server. To use the **Bios menu** to flash new firmware and/or new BIOS code revision:

1. Connect the console port on the rear panel of the Digi ConnectPort LTS unit to a serial port on a workstation. Use the supplied RJ45/DB9F console adapter and an Ethernet cable.
2. Set up a terminal emulation program such as HyperTerminal. Use the following port parameters:
   - **bps**=9600
   - **data bits**=8
   - **parity**=none
   - **stop bits**=1
   - **flow control**=none
3. Reboot or power on the ConnectPort LTS unit.
4. Press the ESC key within three seconds of applying power to the device. The following screen appears. Use the ESC key to return to a previous menu screen, and then press the Enter key to refresh the menu screen.

```
Press <ESC> key to enter the bios menu :  0
-------------------------------------------------------------------------------
 Welcome to Bios Configuration page
-------------------------------------------------------------------------------
 Select menu
 1. RTC configuration [ Apr 28 10 -  20:40:00 ]
 2. Hardware test
 3. Firmware upgrade [S/W Version : v1.0.0rc13t1(82002228_A)]
 4. Exit and boot from flash
 5. Exit and boot from flash in emergency mode
 6. Exit and reboot
  <ESC> Back, <ENTER> Refresh
 ----->
```

5. Choose **Firmware upgrade** by entering 3. The following screen appears.

```
Firmware upgrade
-------------------------------------------------------------------------------
Select menu
1. Protocol [TFTP]
2. IP address assigned to Ethernet interface [192.168.55.120]
3. Server's IP address [192.168.55.128]
4. Default Ethernet interface [ETHERNET1]
5. Firmware File Name [pp.bin]
6. Auto firmware Upgrade on next boot[OFF]
7. Start firmware upgrade
 <ESC> Back, <ENTER> Refresh
----->
```

6. Enter the information for the first menu items.
    - **Protocol**: The choices are BOOTP or TFTP.
    - **IP address assigned**: Type the IP address of the Digi ConnectPort LTS unit.
    - **Server's IP address**: The IP address of the BOOTP or TFTP server.
    - **Firmware File Name**: The filename for the firmware.
    - **Ethernet interface**: 1 or 2.
7. Use the ESC key to return to previous menu screens.
8. Select **Start firmware upgrade**. The firmware upgrade can take 15 to 20 minutes to process. Do not interact with the ConnectPort LTS unit until the firmware update is complete.
9. When the upgrade process is complete, the device will reboot and the factory default settings will be restored.

ConnectPort LTS hardware specifications

To get ConnectPort LTS hardware specifications, visit www.digi.com/products/serial-servers/serial-device-servers/connectportlts#specifications.

ConnectPort LTS regulatory information and certifications

This section documents ConnectPort LTS regulatory information and certifications.

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 B

These devices comply with the standards cited in this section:

- ConnectPort LTS 16
- ConnectPort LTS 32

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.

Industry Canada (IC) certifications

This digital apparatus does not exceed the Class B 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 B prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

China regulatory information

Linux Terminal Server

Digi 串口服务器 LTS 16 MEI 2AC

用户须知

当系统出现故障时可能会导致严重的后果，为了应对这些后果，采用备份系统和安全装置保护生命和财产安全是必不可少的。用户承担对保护系统故障所造成后果的责任。

该设备在室内使用，所有通信线路仅限于建筑物内。

该设备未被批准不得用于生命支持系统或医疗系统。

塞纳科技没有明确批准该设备的变更或修改，用户将无权操作该设备。

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

警告!

要断开关危险电压应断开所有的输入插座!

没有电源线设备将被出售

机架式

1. 高架工作环境温度—如果安装在一个封闭或多单元机架组件上，其机架环境的操作环境温度也许高于室温。因此，应考虑设备安装的环境应与制造商的最高额定环境温度兼容。
2. 空气流通减少—在机架中安装的设备应该是这样的:其操作设备所需的空气流动量不会影响设备的安全。
3. 机械载荷—由于机械负荷的不平衡性，在机架上安装设备不应该在危险的条件下进行。
4. 电路过载—应考虑连接设备的供电线路和电路超载可能产生对过量电流的保护以及对电源线的影响。解决这一问题，应适当考虑设备的铭牌额定值。
5. 应保持可靠的接地—保持机架安装设备接地的可靠性。应特别注意将连接头而不是直流电的连接头连到分支电路上。
6. **锂蓄电池**

“警告”

如果电池更换不当，会有发生爆炸的危险。

请仅使用制造商推荐的同一或者同等型号的产品。

(制造商：索尼福岛公司，型号：CR2032)

按照国家标准或回收计划，处理废旧电池。

Safety statements

5.10 Ignition of Flammable Atmospheres

Warnings for Use of Wireless Devices

CAUTION! Observe all warning notices regarding use of wireless devices.

Potentially Hazardous Atmospheres

Observe restrictions on the use of radio devices in fuel depots, chemical plants, and areas where the air contains chemicals or particles, such as grain, dust, or metal powders, and any other area where you would normally be advised to turn off your vehicle engine.

Safety in Aircraft

Switch off the wireless device when instructed to do so by airport or airline staff. If the device offers a ”flight mode” or similar feature, consult airline staff about its use in flight.

Safety in Hospitals

Wireless devices transmit radio frequency energy and may affect medical electrical equipment. Switch off wireless devices wherever requested to do so in hospitals, clinics, or healthcare facilities. These requests are designed to prevent possible interference with sensitive medical equipment.

Pacemakers

Pacemaker manufacturers recommended that a minimum of 15cm (6 inches) be maintained between a handheld wireless device and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with independent research and recommendations by Wireless Technology Research.

Persons with Pacemakers

- ALWAYS keep the device more than 15cm (6 inches) from their pacemaker when turned ON.
- Do not carry the device in a breast pocket.
- If you have any reason to suspect that the interference is taking place, turn OFF your device.

Rack-mountable

1. **Elevated Operating Ambient Temperature**: If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in a environment compatible with the manufacturer’s maximum rated ambient temperature (Tmra).
2. **Reduced Air Flow**: Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
3. **Mechanical Loading**: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

4. **Circuit Overloading**: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
5. **Reliable Earthing**: Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit.

Lithium Battery

Danger of explosion if battery is incorrectly replaced.
Replace only with the same or equivalent type recommended by the manufacturer.
(Manufacturer: SONY FUKUSHIMA CORP., Model: CR2032.)
DISPOSE OF USED BATTERIES ACCORDING TO THE NATIONAL CODE OR RECYCLING PROGRAM.

Modem

CAUTION! To reduce the risk of fire, use only No. 26AWG or larger telecommunication line cord.

Cabling

To determine the proper cable requirements for your application, please refer to the *Cable Guide for all PortServer® TS*, *Digi Connect®*, and *Digi One®* Products (Digi part number 90000253).