Digi Connect® WAN Family User Guide

User Guide

Revision history—90000753

Revision	Date	Description
J	September 2013	Added memory specification for the external flash drive.
K	May 2016	Resolved link issues. Deleted references to the Digi Device Setup Wizard.
L	March 2017	Rebranded with minor updates.
M	June 2017	Modified regulatory and certification information as required by RED (Radio Equipment Directive).

Trademarks and copyright

Disclaimers

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

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Send comments

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

Customer support

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

Contents

Configuration, monitoring, and administration

Hardware

Digi Connect WAN Family web interface

Digi Connect WAN Family command-line interface

Remote Manager monitoring capabilities

SNMP device monitoring capabilities

Specifications and certifications

Troubleshooting

About this guide

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

- Digi Connect WAN Family
- Digi Connect WAN Family GPRS
- Digi Connect WAN Family GSM-R
- Digi Connect WAN Family VPN
- Digi Connect WAN Family IA
- Digi Connect WAN Family 3G
- Digi Connect WAN Family 3G IA
- Digi Connect WAN Family 4G

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:

- Digi Connect WAN Family

For additional information, see the following resources:

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

- Product information available on the Digi website, www.digi.com, and the Digi support site, including:
  - Support forum
  - Knowledge Base
  - Datasheets/product briefs
  - Application/solution guides
  - Carrier-specific documents

Digi Connect WAN Family features

This section provides an overview of Digi Connect WAN Family features.

User interfaces

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

- Digi Remote Manager
- Web-based interface

  For Digi devices that ship with a default IP address, connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration.
- Command-line interface available via local serial port, telnet or SSH
- Simple Network Management Protocol (SNMP)

Network services

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

- Advanced Digi Discovery Protocol (ADDP)
- RealPort
- Encrypted RealPort
- HTTP/HTTPS
- Line Printer Daemon (LPD)
- Remote login (rlogin)
- Remote shell (rsh)
- SNMP
- Telnet

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

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

IP protocol support

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

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Dynamic Host Configuration Protocol (DHCP)
- Simple Network Management Protocol (SNMP)
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- Remote login (rlogin)
- Line Printer Daemon (LPD)
- HyperText Transfer Protocol (HTTP)/HyperText Transfer Protocol over Secure Socket Layer (HTTPS)
- Simple Mail Transfer Protocol (SMTP)
- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)
- Address Resolution Protocol (ARP)
- Advanced Digi Discovery Protocol (ADDP)
- Point-to-Point Protocol (PPP)
- Network Address Translation (NAT)/Port Forwarding (only some products have NAT)
- Secure Shell (SSHv2)
- Generic Routing Encapsulation (GRE) passthrough
- IPsec Encapsulating Security Payload (ESP) on most models
- ESP passthrough

Serial data communication over TCP and UDP

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

- Serial data communication over TCP can automatically perform the following functions:
  - Establish bi-directional TCP connections, known as autoconnections, between the serial device and a server or other network device. Autoconnections are based on data and/or serial hardware signals.
  - Control forwarding characteristics based on size, time, and pattern.
  - Allow incoming raw, telnet, and SSL/TLS (secure-socket) connections.
  - Support RFC 2217, an extension of the telnet protocol.

- Serial data communication over UDP can automatically perform the following functions:
  - Digi Connect products can automatically send serial data to one or more devices or systems on the network using UDP sockets. Options for sending data include whether specific data is on the serial line, a specific time period has elapsed, or after the specified number of bytes has been received on the serial port.
  - Control forwarding characteristics based on size, time, and patterns.
  - Support incoming datagrams from multiple destinations.
  - Support outgoing datagrams sent to multiple destinations.
- TCP/UDP forwarding characteristics.
- Extended communication control on TCP/UDP data paths.
  - Timeout
  - Hangup
  - User-configurable Socket ID string (text string identifier on autoconnect only)

Dynamic Host Configuration Protocol (DHCP)

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

Auto IP

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

Simple Network Management Protocol (SNMP)

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

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

Digi devices support SNMP Versions 1 and 2.

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

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

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

Telnet

Digi Connect WAN Family devices support the following types of telnet connections:

- Telnet client
- Telnet server

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

For more information on these connections, see Network connections and data paths. You can enable or disable access to telnet network services.

Remote login (rlogin)

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

Line Printer Daemon (LPD)

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

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

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

Internet Control Message Protocol (ICMP)

You can display ICMP statistics, including the number of:

- Messages received
- Bad messages received
- Destination unreachable messages received

Point-to-Point Protocol (PPP)

The Point-to-Point Protocol (PPP) transports multi-protocol packets over point-to-point links. PPP is responsible for:

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

Digi Connect WAN Family devices support PPP as the connection protocol from the Digi device to the cellular IP network with NAT (Network Address Technology).

Network Address Translation (NAT)/port forwarding

Network Address Translation (NAT) reduces the need for a large amount of publicly known IP addresses by creating a separation between publicly known and privately known IP addresses.

Advanced Digi Discovery Protocol (ADDP)

The ADDP runs on any operating system capable of sending multicast IP packets on a network. ADDP allows the system to identify all ADDP-enabled Digi Connect WAN Family products attached to a network by sending out a multicast packet. The Digi Connect WAN Family products respond to the multicast packet and identify themselves to the client sending the multicast.

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

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

Generic Routing Encapuslation (GRE passthrough/Encapsulating Security Payload (ESP) passthrough

GRE and ESP are routing protocols that route (tunnel) various types of information between networks.

GRE applies to the encapsulation of IP datagrams tunneled through the Internet. The encapsulation includes security, typically in the form of IPsec (IP security), and is most commonly found in VPN (Virtual Private Network) implementation. RFC (Request For Comment) 1701 and 1702 define these standards. Similarly, you can use ESP in conjunction with IPsec as a possible way of carrying IP packets for a Virtual Private Network (VPN) setup. ESP is defined in RFC 2406.

In ESP passthrough and GRE passthrough, inbound IPsec ESP or GSP protocol traffic is forwarded to a VPN device connected to the Digi device's Ethernet port.

Note If you are using an Auto-key Internet Key Exchange (IKE)-based VPN, UDP port 500 must also be forwarded.

Mobile/cellular features and protocol support

Key cellular features in cellular-enabled Digi devices include:

- GSM: GPRS, EDGE, UMTS, HSPA, SMS
- CDMA: 1xRTT, EV-DO (Revs 0 and A)
- IPsec ESP / IKE
- IP passthrough, also known as bridge mode
- 3-5 volt SIM card
- Signal-strength LEDs

Provisioning wizard

For Digi devices equipped with a Code-Division Multiple Access (CDMA)-based cellular modem, the Mobile Device Provisioning Wizard is available in the web interface to properly configure the Digi device with the required configuration used to access the mobile network. The wizard allows for both automatic and manual provisioning for a variety of mobile service providers.

Digi SureLink™

Digi Connect WAN Family support the Digi SureLink feature. Digi SureLink provides an "always-on" mobile network connection to ensure that a Digi device is in a state where it can connect to the network. It does this through hardware reset thresholds and periodic tests of the connection.

Mobile/cellular protocols

Mobile/cellular protocols supported include, unless otherwise noted:

- Global System for Mobile communication (GSM).
- General Packet Radio Service (GPRS).
- Enhanced Data Rates for GSM Evolution (EDGE).
- Universal Mobile Telecommunications Service (UMTS).
- High Speed Packet Access (HSPA).
- Code-Division Multiple Access (CDMA).
- Evolution-Data Optimized (EV-DO, EVDO, or 1xEV-DO).
- Short Message Service (SMS), currently for GSM cellular products only. Digi cellular gateways implement an SMS-based protocol that allows managing devices by sending SMS commands from anywhere SMS messages can be sent. See Short Message Service (SMS) settings.
- Wi-MAX.

RealPort software

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

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

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

Encrypted RealPort

Digi Connect WAN Family devices also support RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server. Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in an SSL connection and encrypting the data using Advanced Encryption Standard (AES).

Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification.

Drivers are available for a wide range of operating systems, including Microsoft Windows and Linux x32 and x64 based operating systems, as well as other versions of Unix. See the RealPort Compatibility OS List in the Digi Knowledge Base for a detailed list of supported operating systems. It is ideal for financial, retail/point-of-sale, government, or any application requiring enhanced security to protect sensitive information.

Alarms

You can configure Digi Connect WAN Family 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
- Cellular alarms for signal strength and amount of cellular traffic for a given period of time

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

Modem emulation

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

Security features in Digi devices

This section covers Digi Connect WAN Family security features.

Secure access and authentication

Security features include the following:

- Provide customized permissions controls to locally defined users. The local definitions apply irrespective of whether Radius is used for authentication.
- Issue passwords for device users.
- Selectively enable/disable network services such as ADDP, RealPort, Encrypted RealPort, HTTP/HTTPS, LPD, remote login, remote shell, SNMP, and telnet.
- Control access to inbound ports.
- Control access to specific devices, IP addresses, or networks through IP filtering.
- Secure sites for configuration: HTML pages for configuration have appropriate security.

Encryption

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

Encryption methods are as follows:

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

- AES (128/192/256-bit)
- IPsec ESP: DES, 3DES, AES

- Wireless Digi Connect products provide Wi-Fi Protected Access (WPA/WPA2—/802.11i) and Wired Equivalent Privacy (WEP) encryption (64-/128-bit). Supported WPA/WPA2—/802.11i authentication methods include:

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

SNMP security

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

Network Port Scan Cloaking

The Network Port Scan Cloaking feature allows you to configure this Digi device to ignore (discard) received packets for services that are hidden or not enabled and network ports that are not open. You can use this feature to protect your Digi device from malicious software or denial of service attacks. For more information, see Network Port Scan Cloaking.

Configuration management

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

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

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

Customization capabilities

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

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

Getting started with Digi Connect WAN Family products

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

Assign an IP address

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

Default IP address and DHCP settings

All products that have a cellular (WAN) interface ship with a static IP address for the Ethernet port of 192.168.1.1 and DHCP *server* enabled by default. Therefore, simply connecting a laptop computer to the Ethernet port of these products allows direct access to the web interface for configuration. Configure the Ethernet port on the laptop to automatically receive an IP address and DNS server address.

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

To discover the IP address assigned to the device, use the Device Discovery Utility for Windows. See Use Digi Device Discovery utility to sign in to the web interface for more information.

Configuring IP addresses

There are several alternate methods to assign an IP address to a Digi device:

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

Digi Connect WAN Family devices have two IP addresses: one for Ethernet and one for cellular. The pre-defined default Ethernet Port IP address is **192.168.1.1**.

Assign an IP address using DHCP

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

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

If desired, set up a permanent entry for the Digi device 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 when the device is rebooted.

For more information on DHCP server configuration, see DHCP server settings.

Assign an IP address using Auto-IP

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

Assign an IP address from the command-line interface

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

- **ip=*device ip***: The IP address for the device.
- **gateway=*gateway***: The network gateway IP address.
- **garp=*seconds***: The frequency of Gratuitous ARP (GARP) announcements, in seconds, which are a broadcast announcement to the network of a device's MAC address and the IP address.
- **submask=*device submask***: The device subnet mask for the IPaddress.
- **dhcp=off**: Turns off use of the Dynamic Host Configuration Protocol (DHCP), so that the IP address assigned is permanent.
- **static=on**: Specifies that the IP address is static, and will remain as the specified IP address, gateway, and submask.

For example:

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

Assign an IP address from the web interface

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

To change the IP address from the web interface:

1. Open a web browser and type the current IP address of the Digi Connect WAN Family device in the address bar.
2. Type the user name and password for the device. The default user name is **root** and the default password is **dbps**. If these defaults do not work, contact the system administrator who set up the device.
3. Click **Network** to access the **Network Configuration** page.
4. On the **IP Settings** page, select **Use the following IP address**.
5. Type the IP address, subnet mask, and gateway settings.
6. Click **Apply** to save the configuration.

IP addresses and Remote Manager

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

Test the IP address assignment

To verify the IP address works as configured:

1. Access the command line of a computer or other networked device.
2. Issue the following command:

   ```
   ping ip-address
   ```

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

   ```
   ping 192.168.2.2
   ```

Sign in to the web interface

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

- Web browser
- Digi Device Discovery utility

Use a web browser to sign in to the web interface

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

1. In the web browser address bar, type the IP address of the device.
2. If you are prompted for login credentials, type the user name and password for the Digi device. The default user name is **root** and the default password is **dbps**. If the default user name and password do not work, contact the system administrator who set up the Digi device.

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

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

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

To discover the Digi device and open the web interface:

1. Go to your product's support page:
   - DigiConnectPort X2
   - DigiConnectPort X4
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.

   If you are prompted for login credentials, type the user name and password for the Digi device. The default user name is **root** and the default password is **dbps**. If the default user name and password do not work, contact the system administrator who set up the Digi device.

Network connections and data paths

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

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

The following topics describe the effects of enabling features and selecting settings when configuring Digi Connect WAN Family devices.

Network services

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

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

Network services associated with specific ports

The following list details network services associated with specific ports.

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

Network services associated with serial ports in general

The following list details network services associated with serial ports in general.

- **RealPort**: A single TCP connection manages (potentially) multiple serial ports.
- **Modem emulation**, also known as **pseudo-modem (pool)**: A TCP connection to the "pool" port is interpreted as an incoming call to an available pseudo-modem in the "pool" of available port numbers.
- **rsh**: Digi Connect WAN Family products support a limited implementation of the remote shell (rsh) protocol, in that a single service listens to connections and allows a command to be executed. Only one class of commands is allowed: a single integer that specifies which serial port to connect to. Otherwise, the resulting connection is somewhat similar to a reverse telnet or reverse socket connection.
- **DialServ**: Connecting a DialServ device to the serial port. DialServ simulates a public switched telephone network (PSTN) to a modem and forwards the data to the serial port. The Digi device sends and receives the data over an IP network.
- **Reverse SSH**: An encrypted TCP socket is available for each port that provides a direct connection to the designated serial port.

Network services associated with the command-line interface

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

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

Network/serial clients

A network/serial client connection occurs when a Digi Connect WAN Family product initiates a network connection or opens a serial port for communication. There are several categories of network/serial client connections:

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

Autoconnect behavior client connections

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

- **Raw TCP connection**: The Digi Connect WAN Family initiates a raw TCP socket connection to a remote entity.
- **Telnet connection**: The Digi Connect WAN Family initiates a TCP connection using the telnet protocol to a remote entity.

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

Command-line interface (CLI)-based client connections

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

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

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

Modem emulation (pseudo-modem) client connections

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

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.
- **Mobile (Cellular) Configuration**: Specifies the mobile service provider and mobile connection settings for the device.
- **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.
- **Security/Users**: Configures security features, such as enabling password authentication for device users.

Digi Device Discovery utility

The Digi Device Discovery utility:

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

Download the Digi Device Discovery utility from www.digi.com/support/productdetail?pid=5574.

In addition to quickly locating devices, the utility also lists device information, such as the device address, firmware version, and whether it has been configured. It runs on any operating system that can send multicast IP packets to a network. It sends out a User Datagram Protocol (UDP) multicast packet to all Digi devices on the network. Digi devices that support ADDP reply to the UDP multicast with their configuration information. Even Digi devices that do not yet have an assigned IP address or are misconfigured for the subnet can reply to the UDP multicast packet and appear in the device discovery results.

Note Personal firewalls, Virtual Private Network (VPN) software, and certain network equipment can block device discovery. Firewalls block UDP ports **2362** and **2363** that ADDP uses to discover devices. You can enable or disable access to the ADDP service, but you cannot change the network port number for ADDP.

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

Remote Manager interface

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

- Centralized control over large numbers of devices
- Reducing service complexity

- Maintaining high levels of security
- Provisioning and decommissioning of equipment
- Adding functionality to device networks

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

Some things to note about using Remote Manager:

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

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

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

Web interface

Digi Connect WAN Family devices provide a web interface for configuring and monitoring devices. See Digi Connect WAN Family web interface.

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

Accessing the command-line interface

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

To access the command line from the Digi Device Discovery utility, click **Telnet to command line**.

For example, here is a command issued from the command line to assign the IP address to the Ethernet interface:

```
#> set network ip=192.168.1.1
```

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

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

See Digi Connect WAN Family command-line interface for more information on this interface. See the *Digi Connect® Family Command Reference* on www.digi.com for command descriptions and examples of

entering configuration commands from the command-line interface. In addition, you can access online help for the commands by issuing the **help** and **?** commands.

Remote Command Interface (RCI)

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

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

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

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

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

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

SNMP

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

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

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

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

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

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

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

Device administration

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

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

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

Hardware

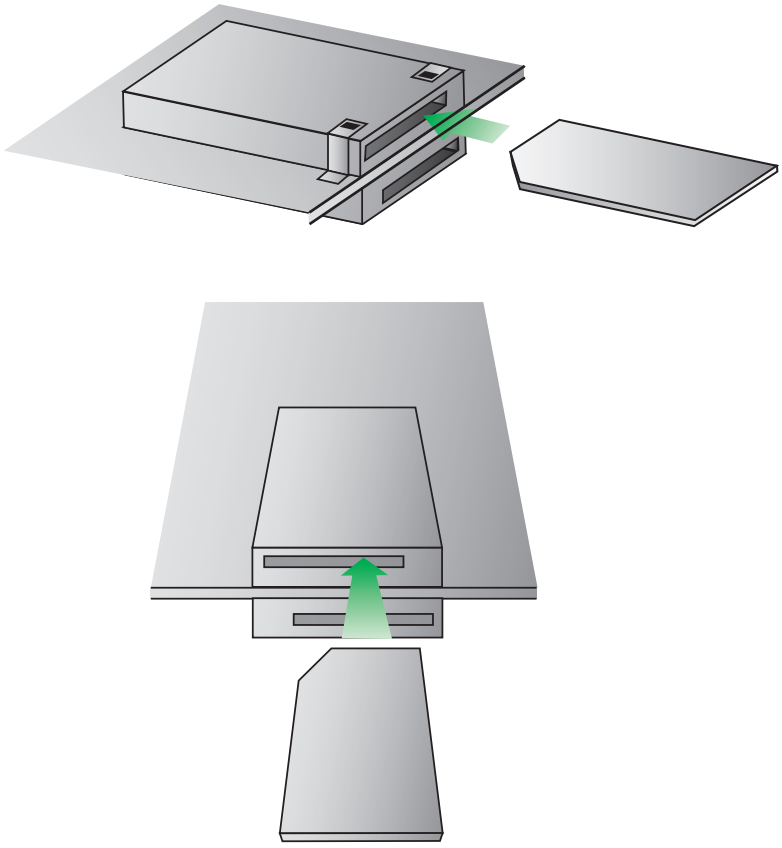
This section details requirements and recommendations for select Digi Connect WAN Family hardware. See also Specifications and certifications and System status LEDs.

SIM card slots

There are two SIM card slots on the circuit board. If you are only using one SIM, insert it into the primary SIM slot (the slot closer to the top of the product) as shown.

Note For ConnectPort X4 H, the SIM cards slots are on the underside of NEMA enclosure cover. When the cover is opened to insert the SIM card, the primary SIM card slot is the *lower* of the two slots, and may be difficult to access for inserting the card. Consider using the secondary card slot.

The metal contacts on the SIM card should face down. Insert the chamfered edge first. When properly inserted, the SIM card clicks into place. If operation outside of a standard office temperature is desired, use high-temperature SIM cards to ensure cellular connectivity throughout the lifetime of the product.



SIM card activation

The SIM card must be activated for cellular service. Contact your mobile service provider and see Mobile (Cellular) Settings.

Configuration settings and status information

There are several firmware settings for SIM cards, for selecting between dual SIM cards, designating primary and secondary SIM cards, setting ID and phone numbers, and viewing status. See SIM card selection and settings.

Digi Connect WAN Family web interface

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

Home page

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

Menu

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

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

Getting started

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

System summary

The System Summary page displays the details for this Digi Connect WAN Family.

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

Apply and save changes

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

Cancel changes

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

Online help

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

Configuration through the web interface

Use the options under **Configuration** to configure settings for various features, such as network settings, mobile 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.
- **WiFI IP settings**: Configure the IP address used for wireless LAN communication. See Wi-Fi IP settings for more information.
- **WiFI LAN settings**: Configure basic settings for wireless LAN devices such as network name and network connection options. See Wi-Fi LAN settings for more information.
- **WiFi Security settings**: Configure authentication and encryption settings for wireless LAN devices. See Wi-Fi security settings for more information.
- **WiFi 802.1x Authentication settings**: Configure IEEE 802.1x authentication settings for wireless LAN devices. See Wi-Fi 802.1x authentication settings for more information.
- **DHCP Server settings**: Configure a DHCP server to allow other devices or hosts on this network to be assigned dynamic IP addresses. See DHCP server settings for more information.
- **Network Services settings:** Configure access to various network services, such as ADDP, RealPort and Encrypted RealPort, telnet,HTTP/HTTPS, and other services. See Network Services Settings for more information.
- **Dynamic DNS Update settings:** Configure a Dynamic DNS (DDNS) service that allows a user whose IP address is dynamically assigned to be located by a host or domain name. See Dynamic DNS update settings for more information.
- **IP Filtering settings**: Configure the IP settings for a Digi Connect WAN Family device to only accept connections from specific and known IP addresses or networks. See IP filtering settings for more information.
- **IP Forwarding settings**:
  - Configure the IP forwarding settings for a Digi Connect WAN Family device to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding.
  - Configure the built-in firewall functionality to limit IP traffic to and from certain networks, TCP or UDP ports, and interfaces. This feature is based on Linux tool iptables. See IP filtering settings for more information.
- **IP Network Failover settings**: Provides a dynamic method for selecting and configuring the default gateway for the Digi device using a set of rules and link tests to determine whether you can use a particular network interface to communicate with a specified destination. See IP Network Failover settings for more information.

- **Socket Tunnel settings**: Configure a socket tunnel used to connect two network devices: one on the Digi Connect WAN Family device's local network and the other on the remote network. See Socket tunnel settings for more information.
- **Virtual Private Network (VPN) settings**: Configure the Virtual Private Network that securely connect two private networks together so that devices may connect from one network to the other network using secure channels. See Virtual Private Network (VPN) settings for more information.
- **IP Pass-through settings**: Configure a Digi Connect WAN Family device to pass its mobile IP address directly through and to the Ethernet device (router or computer) to which it is connected through the Ethernet port. The Digi Connect WAN Family device becomes transparent (similar to the behavior of a cable or DSL modem) to provide a bridge from the mobile network directly to the end device attached to the Digi Connect WAN Family device. See IP Pass-through settings for more information.
- **Host List settings**: Add or remove entries from the host list. For DialServ, the host list provides a means to map a phone number (in the local name field) to a network destination, (in the "resolves_to" field). See Host List Settings for more information.
- **Virtual Router Redundancy Protocol (VRRP) settings**: Configure a number of routers to represent a virtual router, which simplifies configuration of hosts on a network.
- **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 Digi Connect WAN Family device. You can use one of the following methods to obtain the IP address:

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

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

IP settings

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

- **IP Address**: An IP address is like a telephone number for a computer. Other network devices talk to this Digi device using this ID.

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

Wi-Fi IP settings

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

Wi-Fi LAN settings

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

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

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

Wi-Fi security settings

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

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

- **Network Authentication:** The authentication method or methods used for wireless communications.
  - **Use any available authentication method**: Enables all of the methods. The capabilities of the wireless network determines the actual method used.
  - **Use the following selected method(s)**: Selects one or more authentication methods for wireless communications.
  - **Open System**: Uses IEEE 802.11 open system authentication to establish a connection.
  - **Shared Key**: Uses IEEE 802.11 shared key authentication to establish a connection. At least one WEP key must be specified in order to use shared key authentication.
  - **WEP with 802.1x authentication**: Uses IEEE 802.1x authentication (EAP) to establish a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless network.
  - **WPA with pre-shared key (WPA-PSK)**: Uses the Wi-Fi Protected Access (WPA) protocol with a pre-shared key (PSK). The PSK is calculated using a passphrase and the network SSID.
  - **WPA with 802.1x authentication**: Uses the WPA protocol and IEEE 802.1x authentication (EAP) to establish a connection with an authentication server or access point. Encryption keys are dynamically generated to encrypt data over the wireless link.
  - **Cisco LEAP**: Uses Lightweight Extensible Authentication Protocol (LEAP) to establish a connection with an authentication server or access point. Wired Equivalent Privacy (WEP) keys are dynamically generated to encrypt data over the wireless link. A user name and password must be specified to use LEAP.

- **Data Encryption:** You an select multiple encryption methods.
  - **Use any available encryption method**: Enables all of the methods. The capabilities of the wireless network determines the actual method used.
  - **Use the following selected method(s)**: Selects one or more encryption methods.
  - **Open System**: Does not use encryption over the wireless link. Open System encryption is valid only with Open System and Shared Key authentication.
  - **WEP**: Uses Wired Equivalent Privacy (WEP) encryption over the wireless link. You can use WEP encryption with any of the above authentication methods.
  - **TKIP**: Uses Temporal Key Integrity Protocol (TKIP) encryption over the wireless link. You can use TKIP encryption with WPA-PSK and WPA with 802.1x authentication.
  - **CCMP:** Uses CCMP (AES) encryption over the wireless link. You can use CCMP WPA-PSK and WPA with 802.1x authentication.
- **WEP Keys**
  - **Transmit Key:** Specify the corresponding key of the encryption key used when communicating with wireless networks using WEP security.

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

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

Wi-Fi 802.1x authentication settings

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

- **EAP Methods:** These are the types of Extensible Authentication Protocols (EAP) or outer protocols that are allowed to establish the initial connection with an authentication server or

access point. These are used with WEP with 802.1x authentication and WPA with 802.1x authentication.

- **PEAP:** Stands for “Protected Extensible Authentication Protocol.” A user name and password must be specified to use PEAP.
- **TLS:** Stands for “Transport Layer Security.” A client certificate and private key must be installed in order to use TLS.
- **TTLS:** Stands for “Tunneled Transport Layer Security.” A user name and password must be specified to use TTLS.

- **PEAP/TTLS Tunneled Authentication Protocols:** These are the types of inner protocols that you can use within the encrypted connection established by PEAP or TTLS.

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

  You can use these **non-EAP protocols** that with TTLS.
  - **CHAP:** Challenge Response Protocol.
  - **MSCHAP:** Microsoft Challenge response Protocol.
  - **TTLS MSCHAPv2:** TTLS Microsoft Challenge. response Protocol version 2.
  - **PAP:** Password Authentication Protocol.
- **Client Certificate Use:** When the TLS is protocol is enabled, a client certificate and private key must be installed on the Digi device.
  - **Certificate:** Click **Browse** to select a client certificate file. Then click the next **Browse** to select a private key file.
  - **Private Key File**: If the private key file is encrypted, a password must be specified.
- **Trusted Certificates:** Adds and lists trusted certificates.
  - **Verify server certificates:** Enable to verify that certificates received from an authentication server or access point are signed by a trusted certificate authority (CA). Standard CAs are built in. Additional trusted certificates may be added.
  - **Trusted Certificate File:** To add additional trusted certificates, click **Browse** to select a certificate file to upload to the Digi device, then click **Upload**.
- **Installed Certificates:** Shows which client certificates have been added and are in use.

DHCP server settings

You can enable the DHCP server feature in a Digi device to allow other devices or hosts on this network to be assigned dynamic IP addresses. This DHCP server supports a single subnetwork scope.

For the DHCP server to operate, the Digi device must be configured to use a static IP address. For information on how to configure static IP settings, see IP Settings.

DHCP terminology

Some key terms involved in configuring a DHCP server include:

scope

A scope is the full consecutive range of possible IP addresses for a network and typically defines a single physical subnet on your network, where DHCP services are offered. A scope is the primary way for the DHCP server to manage distribution and assignment of IP addresses and related configuration parameters to its clients on the network.

exclusion range

An exclusion range is a limited sequence of IP addresses within a scope, excluded from DHCP service offerings. Exclusion ranges assure that any addresses in these ranges are not offered by the server to DHCP clients on your network.

address pool

After the scope is defined and exclusion ranges are applied, the remaining addresses form the available address pool within the scope. The addresses in this pool are available for dynamic assignment by the server to DHCP clients on your network.

lease

A lease is the length of time that the DHCP server specifies, during which a client host can use an assigned IP address. When the DHCP server grants a lease to a client, the lease is active.

Before the lease expires, the client typically needs to renew its address lease assignment with the DHCP server. A lease becomes inactive when it expires or it is deleted at the server, or if the client actively releases the lease. The duration of a lease determines when it will expire and how often the client needs to renew it with the DHCP server in order to retain the lease.

A DHCP server never grants a lease to its own address. There is no need for its own address to be in the exclusion range; the DHCP server simply protects its address from being offered.

grace period

When a DHCP client actively releases a lease, or when the lease expires without being renewed by the client, the DHCP server does not immediately delete the lease record and return the associated IP address to the available address pool. A grace period is the interval of time for which the lease record is retained before the DHCP server automatically deletes the record from its lease list, thereby making the IP address available for lease assignment to another client. The grace period is not a configurable value.

For more about the grace period and what it means when the DHCP server is running, see View and manage the current DHCP leases.

reservation

You may use a reservation to create a permanent address lease assignment by the DHCP server. Reservations assure that a specified hardware device on the subnet can always use the same IP address. Address lease reservations associate a specific IP address with a specific client's Ethernet MAC address.

options

Options are other client configuration parameters that the DHCP server can assign when serving leases to DHCP clients. Most options are defined in RFC 2132. The DHCP server in the Digi device supports a limited set of options:

- Option 3: Routers on Subnet
- Option 6: DNS Servers

Addresses in the DHCP server settings

The IP address and subnet mask of the DHCP server's scope are the static IP configuration settings for the Digi Connect WAN Family itself.

The default gateway (router) provided to a client with the lease information is the IP address of the Digi device.

The DNS servers provided to a client with the lease information are the DNS server addresses configured in the Digi device. These addresses include any DNS server addresses that the Digi device acquires when it connects to the mobile network.

DHCP server configuration settings

Here are the configuration settings for the DHCP server. Typically, you can modify these settings without restarting the DHCP server for the changes to become effective on the running server.

- **Enable Dynamic Host Configuration Protocol (DHCP) Server:** Enables the DHCP server feature on this Digi device. Note that for the DHCP server to operate, the Digi device must be configured to use a static IP address. For information on how to configure static IP settings, see IP Settings.
  - **Scope Name**: The name of the physical network interface associated with the subnet being served by the DHCP server. Most Digi device models have a single network interface, so there is no choice for the scope name. For models that have multiple network interfaces, such as an Ethernet interface and a Wi-Fi (802.11) interface, this DHCP Server may be configured to provide services on either of those interfaces.
  - **IP Addresses:** The starting and ending IP addresses for the scope being served by this DHCP server. These addresses must be in the same subnet as the Digi device itself.
  - **Lease Duration:** The length of the leases for the scope being served by this DHCP server. The default lease duration is 24 hours. A DHCP client may request a lease duration other than this setting, and the DHCP server will grant that request if possible.
- **Wait specified delay before sending DHCP offer reply:** The interval of time in milliseconds to delay before offering a lease to a new client. The default delay is 500ms, and the range is 0 to 5000ms. Use of this delay permits this Digi device to reside on a network with other DHCP servers, yet not offer leases to new clients unless the other DHCP servers do not make such an offer. This provides a measure of protection against inadvertently connecting a Digi device to a network that is running its own DHCP server(s), and offering leases to clients in a manner inconsistent with that network.
- **Check that an IP address is not in use before offering it:** When a DHCP client requests a new IP address lease, before offering an IP address to that client, use “ping” to test whether that IP address is already in use by another host on the network but is unknown to the DHCP server. If an IP address is determined to be in use, it is marked as **Unavailable** for a period of time, and it will not be offered to any client while in this state. Enabling this test adds approximately one second of delay before the IP address is offered to the client, since the “ping” test must not receive a valid reply for that test to successfully determine that the IP address is not already in use. This option is off (disabled) by default. This option does not apply to Static Lease Reservations, since the “ping” test is not used for them.

- **Send the DHCP Server IP address as a DNS Proxy Server**: This option configures the DHCP Server to send its IP address to a DHCP client as the first DNS server in its lease information. This Digi device supports a DNS Proxy feature that will relay DNS requests and responses between DNS clients and servers. The DNS Proxy is not a feature of the DHCP Server itself, but rather it is managed elsewhere in the configuration settings for this Digi device. For DHCP client to use DNS Proxy effectively, you must enable DNS proxy in the DHCP server configuration and the DNS Proxy settings. For more information, see the description of the Enable DNS Proxy Service setting in Advanced Network Settings. This option is on (enabled) by default.
- **Static Lease Reservations:** A static lease reservation is a specific IP address paired with a client's MAC address, which reserves the IP address for that client's use only. This assures that a client always receives a lease for the same IP address and that no other client obtains a lease for that address.

  To add a reservation, type the IP address and MAC Address values, select or clear the **Enable** check box, and then press the **Add** button.

  After adding a reservation, you may click the IP address or MAC address of that entry in the table, permitting you to specify or modify the lease duration for this reservation.

  The **Enable** check box for the entry permits a reservation to be disabled without actually removing the entry, then enabled again at a later time.

  Use the **Remove** link to permanently remove a reservation from the DHCP server configuration.

  Use the **Remove All** link to permanently remove all reservations from the DHCP server configuration.
- **Address Exclusions:** A specific set of IP addresses to exclude from the scope. The DHCP server will not grant leases to clients for any IP address in the exclusion range.

  To add an exclusion, type the starting and ending IP addresses, select or clear the **Enable** check box, and then press the **Add** button.

  The **Enable** check box for the entry permits an exclusion to be disabled without actually removing the entry, then enabled again at a later time.

  Use the **Remove** link to permanently remove an exclusion from the DHCP server configuration.

  Use the **Remove All** link to permanently remove all exclusions from the DHCP server configuration.
- **Apply button**: You must click **Apply** to save changes you make to the DHCP server settings. If you leave this page without applying the changes, those changes will be discarded.

Manage the DHCP server

To manage the DHCP server and view/manage the lease status, go to **Management** > **Network Services**. See Manage DHCP server operation for more information.

Network Services Settings

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

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

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

Several services have a setting that allows network services to send TCP keep-alives. You can configure TCP keep-alives in more detail on the **Advanced Network Settings** page.

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

Supported basic network services and their default port numbers

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

```
base network port number + serial port number
```

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

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

There are two types of network services available:

- **Basic services**: You can access these services by connecting to a particular well-known network port.
- **Passthrough services**: You can set up a specific type of service for a specific serial port. To use the service, you must use the correct protocol and specify the correct network port. For example, assuming default service ports and using a Linux host, here is how a user would access the SSH and telnet passthrough services on port 1:

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

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

Service	Services provided	Default network port number
Device Discovery, also known as Advanced Digi Discovery Protocol (ADDP)	Discovery of Digi devices on a network. Disabling this service disables use of the Digi Device Discovery utility to locate the device. You cannot change the network port number for ADDP from its default.	2362
Encrypted (Secure) RealPort	Secure Ethernet connections between COM or TTY ports and device servers or terminal servers.	1027
RealPort	A virtual connection to serial devices no matter where they reside on the network.	771
Line Printer Daemon (LPD)	Allows network printing over a serial port.	515
Modem Emulation Pool (pmodem)	Allows the Digi device to emulate a modem. Modem emulation sends and receives modem responses to the serial device over the Ethernet instead of Public Switched Telephone Network (PSTN). You can enable or disable telnet processing on the incoming and outgoing modem-emulation connections. The pmodem service is for connecting to whatever serial port will answer.	50000
Modem Emulation Passthrough	Allows the Digi device to emulate a modem. This service is for dialing in to a particular serial port that has been set up for modem emulation.	50001
Remote login (rlogin)	Allows users to sign in to the Digi device and access the command-line interface through rlogin.	513
Remote shell (Rsh)	Allows users to sign in to the Digi device and access the command-line interface through Rsh.	514
Secure Shell Server (SSH)	Allows users secure access to sign in to the Digi device and access the command-line interface.	22
Secure Shell (SSH) Passthrough	Accessing a specific serial port set up for SSH.	2501
Secure Socket Service	Authentication and encryption for Digi devices.	2601
Simple Network Management Protocol (SNMP)	Managing and monitoring the Digi device. To run SNMP in a more secure manner, SNMP allows for **set** commands to be disabled. This securing is done in SNMP itself, not through Network Services settings. If disabled, SNMP services such as traps and device information are not used.	161

Service	Services provided	Default network port number
Telnet Server	Allows users an interactive telnet session to the Digi device's command-line interface. If disabled, users cannot telnet to the device.	23
Telnet Passthrough	Allows a telnet connection directly to the serial port, often called reverse telnet. The format for this port number is as follows: `20<serial port number>` Replace <serial port number> with the Digi serial port number. For example, 2001 applies to serial port 1, 2010 applies to serial port 10, and 2016 applies to serial port 16.	2001
Transmission Control Protocol (TCP) Echo	Used for testing the ability to send and receive over a TCP connection, similar to a ping.	7
Transmission Control Protocol (TCP) Passthrough	Allows a raw socket connection directly to the serial port, often called reverse sockets. The format for this port number is as follows: `21<serial port number>` Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	2101
User Datagram Protocol (UDP) Echo	Used for testing the ability to send and receive over a UDP connection, similar to a ping.	7
User Datagram Protocol (UDP) Passthrough	Allows raw data to be passed between the serial port and UDP datagrams on the network. The format for this port number is as follows: `21<serial port number>` Replace <serial port number> with the Digi serial port number. For example, 2101 applies to serial port 1, 2110 applies to serial port 10, and 2116 applies to serial port 16.	2101
Web Server, also known as HyperText Transfer Protocol (HTTP)	You can establish secure access to configuration web pages by requiring a user to sign in. HTTP and HTTPS are also called Web Server or Secure Web Server. These services control the use of the web interface. If HTTP and HTTPS are disabled, device users cannot use the web interface to configure, monitor, and administer the device.	80

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

Network services and IP passthrough

The IP pass-through feature (**Configuration** > **Network** > **IP Pass-through**) causes the Digi device to be bridged transparently between Ethernet and mobile data links. Enabling IP Pass-through disables many device features, including many network services. To provide access to the device for configuration and management purposes, you can configure a subset of network services to terminate at the Digi device instead a connected device such as a router. In the IP pass-through feature, these network services are called *pinholes*. Services that you can configured as pinholes include HTTP, HTTPS, telnet, SSH, and SNMP. See IP Pass-through settings for more information.

Dynamic DNS update settings

A Dynamic DNS (DDNS) service allows a user whose IP address is dynamically assigned to be located by a host or domain name. Before a DDNS service may be used, you must create an account with the DDNS service provider. The provider will give you account information such as user name and password. You will use this account information to register your IP address and update it as it changes.

A DDNS service provider typically supports the registration of only public IP addresses. When using such a service provider, if your Digi device has a private IP address (such as 192.168.x.x or 10.x.x.x), your update requests will be rejected.

The Digi device monitors the IP address it is assigned. It will typically update the DDNS service or server automatically, but only when its IP address has changed from the IP address it previously registered with that service.

DDNS service providers may consider frequent updates to be an abuse of their service. In such a circumstance, the service provider may act by blocking updates from the abusive host for some period of time, or until the customer contacts the provider. Please observe the requirements of the DDNS service provider to ensure compliance with possible abuse guidelines.

The Dynamic DNS Update Settings page includes both settings and status information.

Settings

- **Current IP address**: The IP address of the Digi device.
- **Use the following dynamic DNS service**: Disables DDNS updates, or selects the DDNS service provider to use to register the IP address of this Digi device. When you select a specific DDNS service provider, you must also provide the related account information for that service provider.

  To force an update request to be sent to a particular DDNS service.

  1. Select **None** to disable DDNS updates, and then click **Apply** to save that change.
  2. Select the DDNS service you wish to update.
  3. Click **Apply** to save that change.

     An update request will be sent to that service after you configure and validate the settings for the selected DDNS service.

- **DynDNS.org DDNS Service**: You must create your account at DynDNS.org before you can successfully register the IP address of your Digi device with their service. Please familiarize yourself with their service options and requirements, in order to most effectively use this feature of your Digi device.

  This DDNS service supports only public IP addresses. If you have a private IP address (such as 192.168.x.x or 10.x.x.x), your update requests will be rejected.

  - **Host and Domain Name**: The fully qualified host and domain name you have registered with your service provide (for example: myhost.dyndns.net).
  - **DynDNS User Name**: The user name of the account you that you created with your service provider.
  - **DynDNS Password**: The password for the account you that you created with your service provider.
  - **DynDNS DDNS System**: The system for the account you that you created with your service provider. DynDNS.org supports a number of different services, which vary by the system you select. The available choices are:
    - Dynamic DNS
    - Static DNS
    - Custom DNS
  - **Use Wildcards**: Enables/disables wildcards for this host. The options are as follows:
    - Disable wildcards
    - Enable wildcards
    - No change to service setting

    According to wildcard documentation at DynDNS.org: “The wildcard aliases *.yourhost.ourdomain.tld to the same address as yourhost.ourdomain.tld.”

    Using this option in the settings for your Digi device has the same effect as selecting the wildcard option on the DynDNS.org website. To leave the wildcard option unchanged from the current selection on their web site, use the “no change” option in the device settings. Note that DynDNS.org support for this option may vary according to the DynDNS system you are registered to use.
  - **Connection Method**: The connection method to try when connecting to your service provider to register your IP address. DynDNS.org supports three methods to connect. The options are as follows:
    - Standard HTTP port 80
    - Alternate HTTP port 8245
    - Secure HTTPS port 443

Status and history information

The following settings show status and history information for the DDNS service.

- **Most Recent DDNS Service Update Status**: This section provides the status of the most recent attempt to update a DDNS service or server. The displayed information confirms the success of an update request, or it may offer information as to the reason an update request was rejected by the service or server.

  A number of status appear. Some of them are specific to the updated DDNS service. Use this information when trying to resolve update failures with the DDNS service provider.
  - **Service**: The name of the updated DDNS service provider or server.
  - **Reported**: The IP address of your Digi device that is registered with the DDNS service provider or server.
  - **Update Status**: A simple indication of success or failure for this last update request.
  - **Result Information**: A DDNS service-specific status message, helpful when consulting technical support.
  - **Raw Result Data**: DDNS service-specific update result data returned by the service provider, helpful when consulting technical support.
- **Last Logged Action or Result**: The last attempted, logged action or result for the DDNS feature, helpful for troubleshooting possible problems with DDNS updates. This information helps identify problems with settings, network connection failures, and other issues that prevent a DDNS update from completing successfully. Successful results also are reported here.

IP filtering settings

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

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

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

The settings for IP Filtering Settings include:

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

- **Allow access from the following devices:** A list of IP addresses of systems or devices that are allowed to connect to this device.
- **Allow access from the following networks:** A list of networks based on an IP address and matching subnet mask that are allowed to connect to this device. This option allows grouping several devices that exist on a particular subnet or network to connect to the device without having to manually specific each individual IP address.

IP forwarding settings

When a Digi device acts as a router and communicates on both a private and public network with different interfaces, it is sometimes necessary to forward certain connections to other devices. This is also known as Network Address Translation (NAT) or Port Forwarding.

When an incoming connection is made to the device on the private network, the IP port is searched for in the table of port forwarding entries. If the IP port is found, that connection is forwarded to another specific device on the public network. The options and features described in this section are only supported on some products and some firmware versions.

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

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

IP Forwarding settings include:

- **Enable IP Routing:** Enables or disables IP forwarding.
- **Apply the following static routes to the IP routing table:** You can configure the Digi device with permanent static routes. These routes are added to the IP routing table when this device boots, or afterward when network interfaces become active or changes are made to this list of static routes. Use static routes to route IP datagrams to a network that is not a local network or accessible through the default route.

- **Network Address Translation (NAT) Settings**: A list of instances of NAT settings appears. For each instance, the settings are:
  - **Enable Network Address Translation (NAT):** Permit the translation and routing of IP packets between private (internal) and public (external) networks. Refer to NAT configuration options below. Some Digi device models permit the configuration of NAT instances for more than one network interface.
  - **NAT Public Interface**: The name of the network interface for which NAT will perform address and port translations. The list of interfaces available for NAT configuration varies according to the capabilities of your Digi device model.
  - **NAT Table Size Maximum**: The maximum number of entries that you can add to the NAT table. These entries include the configured port and protocol forwarding rules (see Forward TCP/UDP/FTP Connections and Forward Protocol Connections below), the DMZ Forwarding rule (see Enable DMZ Forwarding to this IP address below), as well as dynamic rules for connections that are created and removed during the normal operation of NAT. You can configure the NAT table size maximum value for any value in the range 64 through 1024, with the default value of 256 entries. Note that this setting does not control the maximum number of port or protocol forwarding rules that you can configure in their respective settings.

- **Enable DMZ Forwarding to this IP address**: DMZ Forwarding allows you to specify a single host (DMZ Server) on the private (internal) network that is available to anyone with access to the NAT Public Interface IP address, for any TCP- and UDP-based services that haven't been configured. Services enabled directly on the Digi device take precedence over (are not overridden by) DMZ Forwarding. Similarly, TCP and UDP port forwarding rules take precedence over DMZ Forwarding (please see **Forward TCP/UDP/FTP Connections** below). DMZ Forwarding is effectively a lowest priority default port forwarding rule that doesn't permit the same remapping of port numbers between the public and private networks, as is possible if you use explicit port forwarding rules.

  If enabled, the incoming TCP and UDP packets from the public (external) network uses the DMZ Forwarding rule, for which there is no other rule. These other rules include explicit port forwarding rules or existing dynamic rules that were created for previous communications, be those outbound (private to public) or inbound (public to private). Also, the DMZ Forwarding rule is not used if there is a local port on the Digi device to which the packet may be delivered. This includes TCP service listener ports as well as UDP ports that are open for various services and clients. DMZ forwarding does not interfere with established TCP or UDP connections, either to local ports or through configured or dynamic NAT rules. Outbound communications (private to public) from the DMZ Server are handled in the same manner as the outbound communications from other hosts on that same private network.

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

- **Forward protocol connections from external networks to the following internal devices:** Enables protocol forwarding to the specified internal devices. Currently, the only IP protocols for which protocol forwarding is supported are:
  - Generic Routing Encapsulation (GRE, IP protocol 47).
  - Encapsulating Security Payload (ESP, IP protocol 50, tunnel mode only).

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

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

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

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

IP forwarding example

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

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

IP Network Failover settings

The IP Network Failover feature provides a dynamic method for selecting and configuring the default gateway for the Digi device. Failover uses of a set of rules and link tests to determine whether you can use a particular network interface to communicate with a specified destination. The user configures these rules, link tests and the priority order of the interfaces.

Failover maintains a network interface list, ordered by the configured Failover Interface Priority, and containing information on the state of the network interface and recent success or failure of the link tests for that interface. The failover status for a network interface is one of the following:

- **1 - Responding:** The interface is Up and configured in the system. It is currently responding to the link tests. This interface is suitable for use as the default gateway.
- **2 - Up:** The interface is Up and configured in the system. Its status has not been determined by the link tests, or no link tests are configured. This interface may be suitable for use as the default gateway.

- **3 - Not Responding:** The interface is Up and configured in the system. However, it is not currently responding to the link tests, and the number of consecutive test failures has reached the threshold number configured in the Network Failover settings. This interface may be suitable for use as the default gateway.
- **4 - Down:** The interface is Down or not configured in the system. However, it is not currently responding to the link tests. This interface is not suitable for use as the default gateway.
- **5 - Unknown:** The interface is Unknown (does not exist) in the system. This interface is not suitable for use as the default gateway.

The number shown above for each status value, indicates the priority of that status, failover uses in selecting the interface to use as the default gateway. Status priority 1 is the most suitable for use, with lower priorities considered suitable if there are no interfaces at the highest priority.

When any network interface changes status, the interface list is examined for the interface that has the highest status priority, nearest the start of the list. The default gateway is the highest priority interface with a Responding status. If no interface is marked Responding then the default gateway is highest Up interface.

When Network Failover performs a link test, it adds a temporary static host route to the destination IP address for the link test, using the network interface that the link test is configured to test. The static host route is removed when the link test completes. Avoid manually configuring static host routes to any of the failover link test destinations, as such host routes may interfere with failover's link testing. Static IP routes are configured on the IP Forwarding Settings page. For additional information, see IP forwarding settings.

In the Advanced Network Settings, the Gateway Priority selection provides a simpler method for selecting the default gateway. However, if failover is properly configured and enabled, it overrides the Gateway Priority selection in the Advanced Network Settings. For a description of this non-failover Gateway Priority selection and information on how to configure it, see Advanced Network Settings.

For IP Network Failover status and statistics, see IP Network Failover statistics.

Network Failover general settings

- **Enable IP Network Failover**: Enable the Network Failover feature in the Digi device. Click the check box to turn failover on or off.
- **Enable fallback to the non-failover default gateway priority method**: The Network Failover uses the fallback option if it cannot configure a default gateway. Failure to configure a default gateway could occur if one or more interfaces are not enabled (On) for Network Failover use, or if the enabled interfaces are not Up or do not have a gateway associated with them. Click the check box to turn fallback on or off.

- **Failover Interface Priority**: Failover uses the list of available network interfaces in priority order to determine the default gateway. The default gateway routes IP packets to an outside network, unless controlled by another route.

  A network interface may have a static gateway configured for it, or it may obtain a gateway from DHCP or other means when the interface is configured. The first interface in this list that supplies a gateway will be used as the default gateway. The default gateway may change as interfaces connect and disconnect, and as failover link tests determine that an interface is providing the desired IP packet routing to a remote network destination.

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

- **Link Test Settings for each of the network interfaces**: The options that follow configure the link tests for the network interfaces. Each network interface has its own set of options. Failover can support Ethernet, Wi-Fi and Mobile (cellular) network interfaces. The available interfaces vary among different Digi products.
  - **Enable IP Network Failover for the XXX Interface**: Enable use of the XXX interface for failover, where XXX is Ethernet, Wi-Fi, or Mobile. Click the check box to turn failover on or off. If a network interface is not enabled for use by failover, it will not be considered by failover for use in selecting the default gateway.
  - **No Test**: Click the radio button to select no link tests will be used for this interface. Since no link tests are run, failover will only be aware of the Up or Down status of the interface.
  - **Ping Test**: Click the radio button to select the Ping Test as the link test to use for this interface. The Ping Test sends ICMP Echo Request packets to the configured destination IP address. If you receive an ICMP Echo Reply (ping reply), the link test successfully demonstrated that you can use the network interface to communicate with the specified destination.
  - **Primary Destination** (Ping Test): The primary, or first, destination to ping. The destination must be a valid IPv4 address. If the destination is remains empty, no Primary Destination link test will be attempted.
  - **Secondary Destination** (Ping Test): The secondary, or second, destination to ping. The destination must be a valid IPv4 address. If the destination is remains empty, no Secondary Destination link test will be attempted.
  - **Send Count** (Ping Test): The maximum number of ping requests to send for a ping link test. When a reply is received, the ping test ends successfully and does not continue to send ping requests. If no ping reply is received after Send Count ping requests have been sent, the link test ends in failure.
  - **Send Interval** (Ping Test): The time interval in seconds between sending ping requests during a ping link test. The ping tests sends a ping request. If no ping reply is received before the Send Interval expires, another ping request is sent.
  - **TCP Connection Test**: Click the radio button to select the TCP Connection Test as the link test to use for this interface. The TCP Connection Test tries to establish a TCP connection to the configured destination IP address and port number. If a connection is successfully established, or if the remote host actively rejects (resets) the connection attempt, the link test successfully demonstrated that you can use the network interface communicate with the specified destination. If a TCP connection is successfully established, it is immediately closed.
  - **Primary TCP Port** (TCP Connection Test): The destination TCP port to use to connect to the Primary Destination address.

- **Primary Destination** (TCP Connection Test): The primary, or first, destination used to establish a TCP connection. The Primary Destination uses the Primary TCP Port when testing the connection to the Primary Destination. The destination must be a valid IPv4 address. If the destination is empty, no Primary Destination link test will be attempted.
- **Secondary TCP Port** (TCP Connection Test): The destination TCP port to use to connect to the Secondary Destination address.
- **Secondary Destination** (TCP Connection Test): The secondary, or second, destination used establish a TCP connection. The Secondary Destination uses the Secondary TCP Port when testing the connection to the Secondary Destination. The destination must be a valid IPv4 address. If the destination is empty, no Secondary Destination link test will be attempted.
- **Connection Timeout** (TCP Connection Test): The time in seconds to wait for a TCP connection to be established or rejected by the destination host.

The following four Link Test options are used if the Ping or TCP Connection Link Test is selected.

- **Repeat the test every: N seconds**: The time interval (N) in seconds between the end of a successful link test and the start of the next link test for the network interface. This interval occurs only after a successful test.

  Shorter intervals verify the link more often, but they also increase the packet traffic over the network interface during the text. Consider the frequency of tests carefully for network connections such as Mobile (cellular) connections, which may be expensive, depending on the service plan in effect with your mobile service provider.

- **On test failure, retry every: N seconds**: The time interval (N) in seconds between the end of a failed link test and the start of the next link test for the network interface. This interval occurs after a failed test and continues until the “Not Responding” (consecutive failures) threshold has been reached.

  A possible strategy is to configure a shorter Retry interval than the Success interval, to more quickly test the network connection to determine whether it is truly not working or there was just a transient test failure. Determining the validity of the link helps failover determine whether it is necessary to reconfigure the default gateway.

- **Report *Not Responding* after: N consecutive failures**: The threshold (N) in consecutive link test failures at which time the network interface is reported to failover as “Not Responding”. Upon receiving such a report, failover may determine that the default gateway must be reconfigured. The count of consecutive failures is reset to zero when a successful link test completes, or when the network interface is reconfigured or its connection is restarted (such as a mobile PPP connection).

- **When *Not Responding*, retry every: N seconds**: The time interval (N) in seconds between the end of a failed link test and the start of the next link test for the network interface. This interval occurs after a failed test, but *only after* the “Not Responding” (consecutive failures) threshold has been reached.

Socket tunnel settings

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

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

Socket tunnel settings include:

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

Virtual Private Network (VPN) settings

Use a Virtual Private Networks (VPN) to securely connect two private networks together so that devices may connect from one network to the other network using secure channels. VPN uses IP Security (IPsec) technology to protect the transferring of data over the Internet. All Digi Connect WAN Family products except Digi Connect WAN support VPNs.

The Digi device is responsible for handling the routing between networks. Devices within the local private network served by the Digi device can connect to devices on the remote network as if they are in the local network. The VPN tunnels are configured using various security settings and methods to ensure the networks are secured.

Uses for a VPN-enabled Digi device

VPN-enabled Digi devices, such as Digi Connect WAN VPN, are cellular-enabled routers that securely connect remote subnets using IPsec VPN technology. Devices in the Digi device's private network can

connect directly to devices on the other private network with which the VPN tunnel is established. You configure VPN tunnels using security settings and methods to ensure the networks are secured.

Use the Digi device for primary or backup remote site connectivity. The Digi device routes secured IPsec VPN traffic over the cellular IP network and a VPN appliance terminates it at the host end.

You can use a VPN-enabled Digi device in several scenarios; for example:

- As the *primary* router where the remote site does not use another WAN router.
- As a *backup* router where the remote site has a primary WAN connection through DSL, Frame Relay, or other means.
- To provide secure access to remote serial and/or Ethernet devices.

This section describes using a Digi device as a *primary* remote site router using IPsec Encapsulated Security Payload (ESP) and Internet Key Exchange (IKE)/Internet Security Association and Key Management Protocol (ISAKMP) pre-shared key methods.

VPN global settings

- **General Security Settings**
  - **Enable Antireplay**: Antireplay allows the IPsec tunnel receiver to detect and reject packets that have been replayed. Set this field to match that at the remote VPN gateway. The default is Enabled.

    Important Disable Antireplay if you use manual keyed tunnels.

- **Miscellaneous Settings**
  - **Suppress SA lifetime during IKE Phase 1**: In most cases, clear this check box. Some VPN equipment do not negotiate the ISAKMP Phase 1 lifetimes. Such equipment may refuse to negotiate with the Digi device if it includes lifetime values in Phase 1 negotiation messages. If the Digi device must communicate with such equipment, enable this option to prevent the Phase 1 lifetimes from being included in the ISAKMP Phase 1 messages.
  - **Suppress Delete Phase 1 SA Message For PFS**: In most cases clear this check box. VPN devices usually send a delete notification for any phase 2 SAs that are left over from previous sessions when they start to negotiate quick mode. However, some devices do not handle this notification correctly and will terminate the connection when they receive it. If you have trouble connecting to the remote VPN device, select this check box to suppress sending this message.
  - **IP addresses of remote VPN peers may change on the fly (Dynamic DNS)**: Enable when you are specifying the address of the remote VPN device with a DNS name, and that device uses dynamic DNS because its public IP address can change. Selecting this check box will cause the Digi device to poll the DNS server once a minute to see if the remote VPN device's IP address has changed. The IPsec software will be restarted with the new IP address if it does change. Selecting this check box increases network traffic since the unit will be polling the DNS server once a minute.

VPN tunnel configuration settings

- **Description**: Type a short, one-line description of the VPN tunnel.
- **VPN Tunnel**: Displays settings for encryption and authentication keys. Selecting ISAKMP is recommended; almost all VPN devices use this standard protocol. ISAKMP is more secure than manually setting the keys The only time to set the keys manually is when connecting with an old VPN device that does not support ISAKMP, in which case you should replace the obsolete box with one that does.
- **Local Endpoint Type**:

  Select **Local endpoint is a subnet** to allow devices on the remote network to see devices on the local network. This is the standard way IPsec works and the correct choice in most cases.

  Select **Local endpoint is an internal interface** to not allow devices on the remote network to see devices on the local network. This causes the Digi device to create a virtual endpoint and assign it the IP address specified later in the settings on this page. Devices on the remote network will only see the IP address of this endpoint, and cannot see the IP addresses of any devices on the local private network. This feature must be used in combination with NAT. If you select it, then you must update the NAT settings on the **Network >IP Forwarding** page. You must enable NAT translation for the VPN interface that corresponds to the tunnel. Tunnel 1 uses interface vpn0, tunnel 2 uses vpn1, and so on.
- **VPN Mode**:

  If a single remote VPN device will be used for this VPN tunnel, select
  Initiate client connections to and accept connections from the remote VPN device at and type the remote device's IP address or DNS name in the field below. If the Digi device should accept connections from any remote VPN device for this tunnel, select the **Accept connections from any VPN device** option.

- **Identity settings**
  - **Network Interface: mobile|0eth0**: Select the network interface used to communicate with the remote VPN device. The mobile0 device is the one with the cellular modem. In most cases, this is the correct device to use to communicate with a remote VPN device on the Internet.
  - Negotiate tunnel as soon as interface comes up: Check if the Digi device should establish the VPN tunnel as soon as the selected network interface is ready to use. Clear this check box if the Digi device should wait until a device on the local private network tries to communicate with a device on the remote network before establishing the VPN tunnel.
  - **Use the following as the identity**: Use this option to control how the Digi device identifies itself to the remote VPN device. The Digi device must identify itself to the remote VPN device when it negotiates the tunnel. You must ensure both devices agree on what the identification is. Select the **Use the following as the identity** option to enter a string such as a DNS name or an FQDN. Select the **Use the interface IP address** if the Digi device should send the IP address of the interface you selected above as its identity. Select **Use the identify certificate X.509...** to use a PKI certificate. If using a PKI certificate, remember to load it in the **Administration >X.509 Certificate/Key Management** web page.
- **Local Endpoint**:

  If you set the Local Endpoint Type to **Local endpoint is an internal interface**, the following prompts appear:
  - Host address for tunnel's internal VPN interface: In the IP Address field, type the IP address for the virtual network interface. This is the IP address which will be visible to devices on the remote private network.
  - Discard packets sent to the remote subnet unless they come from this local subnet: Select this option if the Digi device should discard IP packets transmitted from a device on the local network and addressed to the remote network which do not come from the subnet you specify below.

    IP Address: Type the IP address of the subnet.

    Subnet Mask: Type the mask for the subnet.
  - As indicated on the settings page, use the local endpoint as an internal interface in combination with NAT. Click here to configure the Network Address Translation (NAT) settings. Select the interface name of vpn0 to configure NAT for this tunnel.

  If you set the Local Endpoint Type to **Local endpoint is a subnet**, prompts for entering the network address and mask for the private network appear. Both the Digi unit and the remote VPN device must be configured to use the same values.
  - **IP Address**: Type the IP address of the local private network.
  - **Subnet Mask**: Type the mask for the local private network.

- **Remote Endpoint**: Type the IP address and subnet mask of the remote network. Both the Digi device and the remote VPN device must be configured to use the same values.
  - **Tunnel Network Traffic to the following Remote Network**:

    IP Address: Type the IP address of the remote network.

    Subnet Mask: Type the subnet mask of the remote network.

    Digi devices support a mode of VPN tunnel operation called *VPN tunnel all mode*, where all traffic that is not directed to the local subnet is sent across a VPN tunnel to a remote network. This mode is different from the normal mode of VPN tunnel operation, where the range of the remote subnet is explicitly set VPN tunnel all mode is supported when the Digi device is the initiator of the VPN connection. It is not supported when the Digi device is the server.

    For example, in the normal mode of operation, a user might set up a VPN tunnel between the local subnet at 192.168.1.0/24 to a remote subnet at 172.16.1.0/24. In this case, the remote subnet range is the subnet at 172.16.1.x. In VPN tunnel all mode, the remote subnet is any address that is not on the local subnet, or in this case, anything not in the subnet 192.16.1.x.

    The local subnet must be defined as a specific range, for example 192.168.1.0/24. This is specified in the VPN settings by setting the IP address of the local subnet to 192.168.1.0, and the subnet mask to 255.255.255.0. VPN tunnel all mode is specified by setting the remote IP address to 0.0.0.0, and the remote subnet mask to 0.0.0.0.

    With the configuration described above, any frames sent from the 192.168.1.x network to any IP address not in the 192.168.1.x subnet will be set over the VPN tunnel to the remote subnet.

    When configuring a Digi device for VPN tunnel all mode and the device allows for setting the gateway priority, set the gateway priority. The gateway priority is set on the **Configuration > Network > Advanced Network Settings** page in the **Gateway Priority** setting. Set the gateway priority to **Ethernet** for Ethernet-enabled Digi devices, or **WiFi** for a wireless Digi devices. If the Digi device's IP address on the Ethernet (or wireless) interface is statically configured, specify the address for the gateway on that interface. The gateway address is set in the **Configuration > Network > Ethernet IP Settings** page.

- **Pre-Shared Key Settings**:

  If you select the pre-shared key authentication method in one or more of your ISAKMP Phase 1 Policies, then you will be prompted to supply the ID of the VPN device and the preshared key used for authentication.

  - **Use the following IP address, FQDN, or username for the remote VPN's ID**: Type the remote VPN device's ID in this field. Ensure the remote VPN device is configured to send this ID.
  - **Use the following pre-shared key to negotiate IKE security settings**: Type the preshared key in this field. This value must match exactly with the preshared key set on the remote VPN device.

- **ISAKMP Phase 1 Settings**:
  - **General Security Settings for Phase 1**

    Connection Mode: Main|Aggressive: Set the connection mode to match that configured on the remote VPN device. If aggressive mode is selected, then the VPN device will try aggressive mode first, and then try main mode if aggressive mode fails.

    Enable Perfect Forward Secrecy (PFS): Set this option to enable PFS. PFS guarantees that if one key is broken by an attacker, that does not help him to break another key. PFS is more secure, but slows down the negotiation process. Both the Digi device and the remote VPN device must be configured the same way.

  - **NAT-T Settings**

    Enable NAT Traversal (NAT-T): Set this option if there is a NAT firewall between the two VPN devices.

    Keep Alive Interval: The amount of time in seconds between NAT keep alive messages. Once a connection is established through a firewall, the VPN devices have to send keep alive messages to prevent the NAT firewall from timing out the connection. Set the interval to a value less than the connection timeout of the NAT firewall.

  - **ISAKMP Phase 1 Policies**:

    Keys are negotiated in two phases. The first phase negotiates the keys and authentication method used to establish the initial ISAKMP connection. During this phase, the two VPN devices verify each other's identity and create a security association (encrypted connection). Phase 2 uses the encrypted connection. The encryption and authentication settings you specify determine the level of security in the connection the two VPN devices used to communicate with each other.

    Select the policies to use during phase 1 of the ISAKMP negotiation. Ensure that the Digi device and the remote VPN device use the same policies. If more than one policy is specified, the VPN devices will use the most secure policy that they both have been configured to support.

    Pre-shared Key: Using DSS and RSA signatures is more secure than using a pre-shared key.

    Encryption: The encryption type and the length of the key. The longer the key the more secure it is.

    Integrity: The authentication algorithm. The SHA1 algorithm is more secure than MD5.

    SA Lifetime: The maximum length of the phase 1 security association.

    Diffie-Hellman: The Diffie-Hellman group to use for key generation. The larger the group the more secure it is.

- **ISAKMP Phase 2 Settings**:

  The SAs used for bulk data transfer are created during phase 2. The phase 2 settings you specify will determine the level of security used when devices on the local private network communicate with devices on the remote private network. As with the other settings, the both the Digi device and the remote VPN device must be configured to use the same values. If more than one policy is specified, the VPN devices will use the most secure policy that they both have been configured to support.

- **General Security Settings for Phase 2**:

  Diffie-Hellman: Select the Diffie-Hellman group used to generate keys. Larger groups are more secure.

- **ISAKMP Phase 2 Policies**:

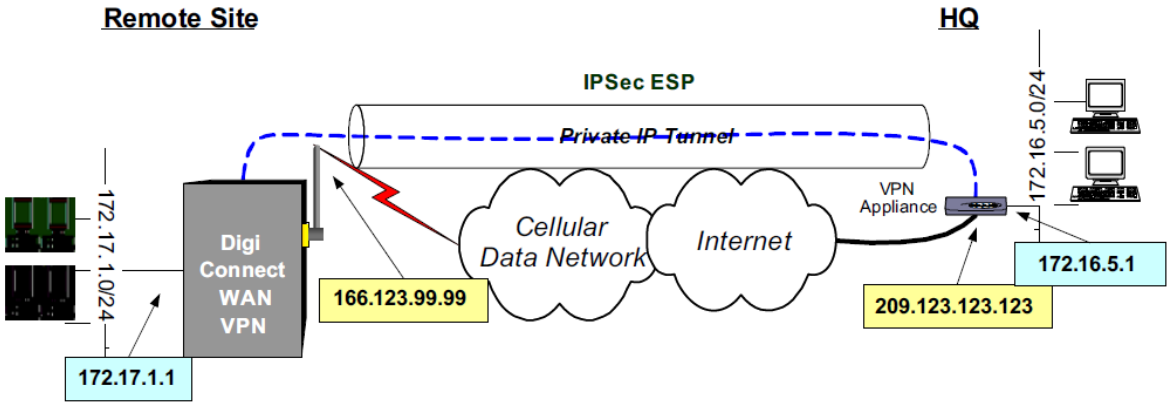
  Encryption: The encryption algorithm used for encrypting data and the length of the key. The longer the key the more secure it is. There are three supported encryption algorithms including DES, 3-DES, and AES. DES encryption uses 64-bit keys, 3-DES encryption uses 192-bit keys, and AES encryption uses 256-bit keys.

  Authentication: The authentication algorithm used in authenticating clients. There are two supported authentication algorithms including MD5 and SHA1. MD5 authentication uses 128-bit keys and SHA1 uses 160-bit keys. The SHA1 algorithm is more secure than MD5.

  SA Lifetime: The maximum length of the Phase 2 security association (SA), in seconds. After the SA has been negotiated, the SA lifetime begins. Once the lifetime has completed, a new set of SA policies are negotiated with the remote VPN endpoint.

Example VPN configuration

The diagram shows a Digi Connect WAN VPN used as a primary remote site router:



How VPN tunnels work

The Digi device's Ethernet port usually connects to a switch or hub, which then connects to other Ethernet devices. The mobile/cellular carrier provides only one IP address to the mobile interface. The

Digi device uses Network Address Translation (NAT), where only the mobile IP address is visible to the outside. Private IP addresses are typically used on the remote site LAN connected to the Digi device's Ethernet port. All outgoing traffic, except the tunneled VPN traffic, uses the mobile IP address of the Digi device. Using the example network above, the process for initiating VPN tunnels works like this:

1. Typically, a host or device on the remote subnet (in this case, 172.17.1.0) requests information from a host on the main site (HQ) subnet (172.16.5.0). For example, a computer at 172.17.1.20 needs a file from 172.16.5.100.
2. The Digi device sees the request is on the HQ subnet and verifies a VPN tunnel exists between the two sites.
3. If no tunnel exists, the Digi device initiates a VPN tunnel request to its peer — the VPN concentrator at HQ. The VPN policy settings are compared, and if they match, an IPsec tunnel is created between the Digi device and the VPN concentrator. Traffic is encrypted as defined in the VPN policies.

VPN tunnel requirements

To establish an IPsec VPN tunnel, the IP address of the mobile interface must be publicly accessible. You can specify either a static or dynamic IP address depending on the requirements of your VPN end point. However, the you cannot specify an IP address a private range of addresses (for example, 10.0.0.0, 172.16.0.0 or 192.168.0.0). If the mobile IP address is within one of the private IP address ranges, the mobile carrier is using a NAT (Network Address Translation) server between your mobile IP address and the Internet.

GSM-GPRS/EDGE APN type requirements

If the VPN end points require static (persistent) IP addresses, you may need a custom access point name (APN). An Internet APN can work in these cases:

- The main site (HQ) VPN appliance can support Dynamic DNS names.
- Use another form of authentication (for example, FQDN).

Be aware that these APNs are based on AT&T; other carrier APNs may have similar requirements.

CDMA carrier requirements

The CDMA (Code-Division Multiple Access) carrier requirements are similar to GSM in that static IP addresses may be required depending on the host site concentrator VPN implementation. In both cases, the Digi device's mobile IP address will likely need to support mobile terminated data; that is, the ability to accept incoming data connections.

HQ router / VPN appliance configuration

For supported protocols, see the IPsec specifications your Digi device. Security policies on the HQ VPN device must match those on the Digi device. The HQ VPN appliance's peer address is the Digi device's mobile IP address.

Console port

You can configure the Digi device's console port for Console Management to provide SSH or telnet access. You can connect the Digi device's console port to the router or VPN appliance's console port to provide true diverse out-of-band console access.

Configuring and managing VPN settings from the command line

In the command-line interface, the **set vpn** command configures VPN connections, and the **vpn** command manages them. These commands are described in the *Digi Connect WAN Family Command*

Reference. Generally, configuring VPN connections from the web interface is simpler. Review the settings descriptions in this procedure (also available in the online help) to determine whether you need to gather any information before you start setting up the VPN.

IP Pass-through settings

There are many application scenarios where you can use a router to decide upon alternative routes using a primary and a secondary (or backup) interface. In many of these configurations require a router to use a public IP address as assigned by the network over which it communicates. This requirement is mostly owing to the router needing to establish a VPN tunnel over that interface and using the public IP address as part of the VPN authentication. (For more on VPN tunnels, see How VPN tunnels work.)

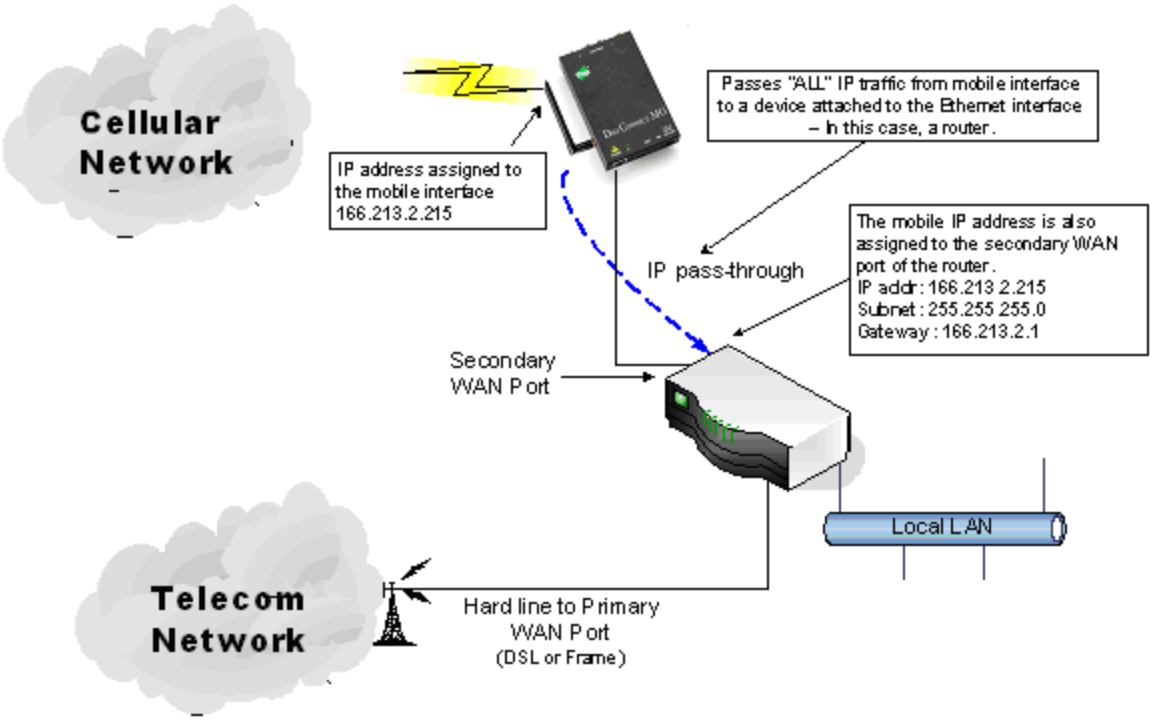
The IP pass-through feature allows a Digi device to provide bridging functionality similar to that of a cable or DSL modem, where the Digi device becomes “transparent” to the router or connected device. In this case; the router’s WAN interface believes it is connected directly to the mobile network and has no knowledge that the Digi device is the mechanism providing that connectivity.

How IP pass-through works

A Digi device configured for IP pass-through, such as a ConnectPort WAN or Digi Connect WAN, passes its mobile IP address directly through and to the Ethernet device (router or computer) to which it is connected through the Ethernet port. From the perspective of the connected device, the Digi device essentially becomes transparent (similar to the behavior of a cable or DSL modem) to provide a bridge from the mobile network directly to the end device attached to the Digi device.

Since the mobile network address is effectively “passed-through” to the local device connected to the Ethernet port of the Digi device, all network access to it is bypassed, with some specific exceptions.

Here is an example of a Digi device configured for IP pass-through in a network with a third-party router.



If the third-party router's WAN interface is attached to the Digi device's Ethernet port, and the Digi device's mobile interface receives the IP address 166.213.2.215, the router's WAN port is assigned the same IP address 166.213.2.215. If the router is receiving the IP address dynamically; the DNS server addresses, subnet mask, and default gateway information will be filled in automatically. If you configured the router manually; you need to obtain the DNS information from the mobile service provider and enter that manually. The subnet mask is 255.255.255.0 and the default gateway is the same as the mobile IP address with ".1" for the last octet. In other words: if the mobile IP address is 166.213.2.215, the default gateway is 166.213.2.1.

Effect of IP pass-through on network access to Digi device

When IP pass-through is enabled, the Digi device effectively disables all router and IP service functionality. Services that are disabled are:

- NAT
- Port forwarding
- VPN
- DDNS updates
- Socket tunnel
- Network Services configuration

The Digi device is effectively transparent to all IP activity and network access by other devices, with these exceptions:

- You can access it via the serial port for configuration using the command line interface.
- It accepts TCP/IP connections for purposes of configuration by means of a "pinhole" on the mobile interface.
- Other devices can access it on the local Ethernet segment via the default IP address of 192.168.1.1.

Using pinholes to manage the Digi device

IP pass-through uses a concept called *pinholes*. You can configure a Digi device to listen on specific TCP ports, and terminate those connections at the Digi device for purposes of managing it. Those ports are called pinholes, and they are not passed on to the device connected to the Ethernet port of the Digi device. You can configure network services and ports as pinholes include (see Network Services Settings to configure these settings):

- **HTTP**: for accessing the device through HTTP and the web interface.
- **HTTPS**: for accessing to the device through HTTPS and the web interface.
- **Telnet**: for accessing the device through a telnet login and the command-line.
- **SSH**: for accessing the device through a Secure Shell (SSH) login and the command-line.
- **SNMP**: for monitoring and managing the device through SNMP.
- **Ping**: for accessing the device through ICMP echo (ping) requests.

Remote Manager and Digi SureLink ports are automatically set up as pinholes so that they continue to work with the Digi device. In addition, the Digi device uses a private address on the Ethernet interface strictly for use in configuration or local access. This allows a user on the local network to gain access to the web interface or a telnet session in order to make configuration changes.

Remote device management and IP pass-through

As illustrated above, the Digi device allows you to enable pinholes for specific ports to allow remote users to manage the Digi device from the mobile network or open Internet. The Digi device retains its remote management capabilities using Remote Manager. The necessary pinholes are automatically defined when the Digi device is configured for IP Pass-through. This provides administrators with the same remote-management capabilities that exist in Digi remote devices.

Configuring IP pass-through

To configure IP Pass-through from the web interface for your Digi device:

Note Ensure you have completed at least the first three steps.

1. Set a static IP address for the Digi device. Go to **Configuration** > **Network** > **IP Settings**.
2. Set up the DHCP server. Go to **Configuration** > **Network** > **DHCP Server Settings**. See DHCP server settings and the online help for DHCP Server Settings.
3. Turn on the DHCP server. Go to **Management** > **Network Services**. In **DHCP Server Management**, click the **Start** button.
4. Configure IP pass-through settings. Go to **Configuration** > **Network** > **IP Pass-through**.

   IP pass-through settings include:
   - **Enable IP Pass-through**: Enables or disables IP Pass-through.
   - **Pinhole Configuration**: Specifies whether specific network services/ports are configured as pinholes for purposes of managing the Digi device.
5. Click **Apply**.

Host List Settings

Use the Host List Settings page to add or remove entries from the host list. For Digi devices using the DialServ feature, the host list provides a means to map a phone number to a network destination.

The Host List settings are:

- **Local Name**: A phone number.
- **Resolves To**: a network destination.
- **Add** button: Adds the entry to the host list.

When accessing a device by name, the Digi device tries to locate the name within the host list. When it finds a match, it maps the host name to the alias. Typically, you can use this as a first means of locating the destination address before using the domain name system (DNS).

Each host list entry consists of a local name string which is mapped to an resolves to destination. You can specify a destination that is either an IP Address or Fully Qualified Domain Name (FQDN). By creating several entries, the host list will allow a many-to-one mapping of multiple host names to a single destination, as well as a one-to-many mapping of a host name to multiple destinations. The one-to-many mapping allows a fail-over option; that is, a connection to the IP address first tries to resolve to the first name in the host list. If that connection attempt fails, then it tries to resolve to the next name in the host list.

Virtual Router Redundancy Protocol VRRP settings

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol for routers. VRRP allows several routers on a subnet to use the same virtual IP address, with the physical routers representing a

"virtual router." Two or more physical routers are configured to stand for the virtual router, with only one doing the actual routing at any given time. The virtual router has a unique You can share IP address and MAC address with all routers in a VRRP group. Using a virtual router redundancy protocol allows you to configure systems with a single default gateway, rather than running an active routing protocol.

There are two roles in VRRP: master, and backup. The master represents the virtual router and forwards IP traffic. The physical router that is currently routing the data is known as the Master. If the Master router fails, another Backup router automatically replaces it. Backup routers monitor the health of the master router, and in the event that the master stops sending advertisements, backup routers stage an election to determine which one will be the next master, and take over the virtual router IP address. The time required to make the determination that the master is down and hold elections depends on configuration, but typically occurs in about 3 seconds.

You can configure a number of VRRP groups (up to 255) on a LAN. A router may participate in multiple groups. All routers must be within one hop of each other (does not route).

VRRP settings include:

- **Virtual Router Identifier (VRID)**: The virtual router ID. All routers in the same VRID communicate with each other. Specify a VRID value between 1 and 255. All routers that are to communicate must have the same VRID.
- **Priority**: Determines which router is the master. The router with the highest priority is the master. The default priority is 100.
- **Advertisement Interval**: The amount of time in milliseconds between VRRP master advertisements. Set all routers in the virtual routing group to the same value. 3000 msec (3 seconds) is typically used.
- **Enable Preempt**: This settings controls whether a higher priority Backup router preempts a lower priority Master. Select the check box to enable preemption; clear the check box to prohibit preemption. The default setting is enabled.
- **IP Address**: The IP Address of the virtual router. All routers in the same VRID should use the same virtual IP address. Configure clients to use this value as their default gateway.

Advanced Network Settings

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

IP settings

Use the IP settings to manage IP address configuration.

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

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

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

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

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

- **Static Primary DNS**

  Static Secondary DNS: The IP address of Domain Name Servers (DNS) used to resolve computer host names to IP addresses. Static DNS servers are specified independently of any network interface and its connection state. An IP address of 0.0.0.0 indicates no server is specified.

- **DNS Priority**: A list of DNS servers in priority order used to resolve computer host names. Each type of server is tried, starting with the first in the list. For each server type, the primary server is tried first. If no response is received, then the secondary server is tried. If neither server can be contacted, the next server type in the list is tried.

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

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

- **Gateway Priority**: List of network interfaces in priority order used to determine the default gateway. Use the default gateway to route IP packets to an outside network, unless controlled by another route.

  A network interface may have a static gateway configured, or obtain a gateway from DHCP or other means when it is connected. The first interface in this list that supplies a gateway will be used as the default gateway. The default gateway may change as interfaces connect and disconnect.

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

  The IP Network Failover feature provides a dynamic method for selecting the default gateway. If failover is properly configured and enabled, it overrides the Gateway Priority selection in the Advanced Network Settings. For a description of the failover feature and information on how to configure it, please see IP Network Failover settings.

DNS proxy settings

- **Enable DNS Proxy Service**: Enables the DNS Proxy feature on this Digi device. DNS Proxy permits DNS client hosts to communicate with this Digi device as if it were a DNS Server. It forwards the DNS client's request to one of the DNS servers configured in its network settings. The response from the actual DNS server will be relayed to the requesting client when it is

received by the DNS Proxy. The DNS Proxy does not cache the actual detailed client requests nor the responses received from the DNS servers. Rather, it acts as a request/response relay agent between the DNS clients and servers.

The DNS Proxy will cycle through the DNS servers that are configured in the Digi device. DNS client requests are identified by the client's IP address and the unique Query ID in the DNS request message. For each new DNS client request (new Query ID), the DNS Proxy uses the first DNS server in its list of DNS servers. If the client retries the same request (same Query ID), the DNS Proxy will recognize that retry message and will either send the retry request to the same DNS server as the previous request for this client, or it will move to the next DNS server in its list of DNS servers. The DNS Proxy feature determines when to retry the same DNS server, or move to the next DNS server, according to the **DNS Proxy: Request Retries Per DNS Server** configuration setting (see below). The DNS Proxy itself does not perform unsolicited retries of DNS client requests.

Note The DHCP Server feature on the Digi device may be configured to use the DNS Proxy feature. For more information, see DHCP server settings. The DNS server list may be dynamic in its content. For example, when DNS server IP addresses are received from a mobile service provider's network, they are added to the DNS server list of this Digi device. Those DNS server IP addresses may or may not be configured when the DHCP Server offers a lease to a DHCP client. As a result, the DHCP client may have no DNS servers provided to it in the lease, and domain name resolution may fail for that client. A significant benefit of the DNS Proxy feature is that the DHCP Server can offer its own IP address as a DNS server in the client lease, and the DNS Proxy will forward DNS requests and responses as stated above. Since the DHCP protocol does not allow a DHCP Server to force an unsolicited DNS server list update to its clients, the DNS Proxy feature provides an indirect method by which such updates may be made effective for the client.

- **Request Cache Size Maximum**: Specifies the maximum number of DNS client request records that the DNS Proxy will maintain concurrently in its cache. A large cache consumes more system resources than does a small cache. However, if the maximum cache size is too small, new DNS client requests may be quietly discarded until the cache has room to add new client request records, or existing cache entries may be replaced by the new requests. If a large number of concurrent DNS client lookups is anticipated, configuring a larger maximum cache size is recommended. See also the setting **For new client requests received when the request cache is full** below.
- **Request Idle Time-To-Live**: Specifies the period of time, in seconds, that a DNS client request will remain in the DNS Proxy cache, before it is deleted. This is a period of idle time, during which neither a DNS client request retry is received by the DNS Proxy, nor a DNS server response is received by the DNS Proxy, for a specific DNS client request. A shorter **Idle TTL** results in the DNS Proxy using resources more efficiently, since the client request cache is reduced in size and the request buffers are released more quickly for future use for other DNS client requests.

- **Request Retries Per DNS Server**: Specifies the number of retries using the same DNS server, for a specific DNS client request that is retried (retransmitted) by the DNS client. There is always one "try" but the number of retries is configurable.

  For new client requests received when the request cache is full:
  Specifies how to handle new client requests when the maximum number of client request entries is already being serviced (the request cache is full). There are two choices for this option:
  Replace the Least Recently Used (LRU) client request with the new request: Remove the least recently used entry from the cache, and add an entry for the new client request.

  Discard (ignore) new requests until some existing requests have expired:
  Silently discard the new client request, and do this for all future new requests until one or more entries have expired and been removed from the request cache.

Network Port Scan Cloaking

The Network Port Scan Cloaking feature allows you to configure this Digi device to ignore (discard) received packets for services that are hidden or not enabled and network ports that are not open.

Malicious software on the Internet may scan IP addresses, protocols, and ports to try to gain access to hosts. You can use the Network Port Scan Cloaking feature to prevent sending responses to the originator for ping and for TCP and UDP ports that do not have an associated service. The default operation is that, when a TCP connection request is received for a port that is not open/bound, the Digi device will send a TCP reset reply to inform the originator that the service is not available. Similarly, the default operation when a UDP datagram is received for a port that is not open/bound, the Digi device will send an ICMP port unreachable packet to inform the originator that the service is not available. For the DNS Proxy feature, you can configure specific network interfaces to ignore (discard) requests that are received from that interface, without otherwise acting on them.

These actions, which are common behaviors in accordance with established protocol standards, effectively inform the originator that it has found a valid IP destination. The originator may continue to probe other ports to gain access to the Digi device. In addition, such reply packets may have a monetary cost for mobile network services such as cellular or WiMAX. Enabling the cloaking feature can help manage both the port scanning threat and reduce overall data costs.

You can configure your Digi device to activate cloaking on a global basis, as well as for individual network interfaces that are available on your Digi device. By enabling the cloak for individual protocols and interfaces, you prevent the possibility of sending reply packets to the originator under the conditions described above.

Note If you enable cloaking on a global basis for a particular protocol, that selection overrides the selections for the interface-specific settings. For example, enabling cloaking for ping in the global group, overrides a disabled selection for the eth0 (Ethernet) interface.

- **Enable Network Port Scan Cloaking**: Enables the Network Port Scan Cloaking feature on this Digi device.
- **Scan Cloaking: Ping**: Enables/disables cloaking for ping requests. Replies will not be sent for received ping requests.
- **Scan Cloaking: TCP**: Enables/disables cloaking for TCP connection requests for which no service is available.

- **Scan Cloaking: UDP**: Enables/disables cloaking for UDP packets for which no service is available.
- **Scan Cloaking: DNS Proxy**: Enable/disable cloaking for DNS Proxy requests for a specific network interface.

Note There is no global cloaking selection for DNS Proxy. To cloak the DNS Proxy feature altogether, simply disable it.

Ethernet interface

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

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

  The default is **half**. If one side of the Ethernet connection is using auto, the other side can set the duplex value to whatever is desired. If one side uses a fixed value (for example, half-duplex), the other side has to use the same.
- **MDI**: The connection mode for the Ethernet cable.

  Auto: Enables Auto-MDIX mode, where the required cable connection type (straight through or crossover) is automatically detected. The connection is configured appropriately without the need for crossover cables to interconnect switches or connecting PCs peer-to-peer. When it is enabled, you can use either type of cable and the interface automatically corrects any incorrect cabling. For this automatic detection to operate correctly, the “speed” and “duplex” options must both be set to “auto.”

  MDI: The connection is wired as a Media Dependent Interface (MDI), the standard wiring for end stations.

  MDIX: The connection is wired as a Media Dependent Interface with Crossover (MDIX), the standard wiring for hubs and switches.

TCP keepalive settings

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

- **Idle Timeout**: The period of time that a TCP connection has to be idle before a keep-alive is sent.

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

WiFi Interface settings

Digi products with Wi-Fi capability display this setting:

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

Mobile (Cellular) Settings

The Mobile Settings pages configure how to connect to mobile (cellular) networks using the mobile connection, including the service provider, service plan, and connection settings used in connecting to the mobile network. If your Digi device has not already been provisioned for use in the mobile network, you can launch a wizard to provision it from these pages. In addition, you can configure settings for Digi SureLink, a feature that provides an "always-on" mobile network connection to ensure rapid on-demand communication. The SureLink configuration settings allow you to customize how SureLink detects when a connection has been lost, in order to re-establish the link. These settings also load a preferred roaming list (PRL) into the cellular module.

Information required from your mobile service provider

To connect to the mobile network, you must get a set of network settings from the mobile service provider including service plan and authentication details. For more information, consult the documentation that came with your mobile service provider's information.

Different processes used for CDMA and GSM provisioning

The process for provisioning your Digi device and the settings displayed on the Mobile Configuration page vary according to whether the mobile service provider network used with your Digi Connect WAN Family product is based on CDMA (Code-Division Multiple Access) or GSM (Global System for Mobile communication).

CDMA-based mobile service providers

Device provisioning for a CDMA-based mobile service provider consists of selecting the service provider from a list and either automatically or manually entering mobile settings provided by the mobile service provider Examples of CDMA-based mobile service providers include Sprint or Verizon.

GSM-based mobile services providers

Device provisioning for a GSM-based mobile service provider involves inserting a Subscriber Identity Module (SIM) card into the Digi device, which makes subscription data available in the cellular network. Examples of GSM-based mobile service providers include AT&T and T-Mobile.

Set mobile configuration settings to factory defaults

The **Set to Defaults** button on the Mobile Configuration page sets all the mobile settings to factory defaults and sets the Service Provider selection back to deselected.

SIM card selection and settings

The Digi device may be equipped with one or two Subscriber Identity Module (SIM) cards. A SIM card contains the account information associated with a particular mobile service provider.

All of the settings available on the Mobile Configuration page are stored individually for each SIM card.

SIM card settings include:

- **SIM**: Select the SIM card identified by the slot number.
- **Set as Primary**: Click to make this the preferred SIM to use to establish mobile connections.
- **IMSI**: The International Mobile Subscriber Identity (IMSI) number that uniquely identifies the SIM card.
- **Phone Number**: The phone number associated with the mobile account, if available.

  Note that the IMSI and phone number may not be available until the SIM attempts a connection.
- **Status**: The configuration status of the SIM. It may be one of these values:
  - **Not configured:** A mobile service provider has not been configured. Select a provider from the list under **Mobile Service Provider Settings.**
  - **Disabled:** The SIM will not be used to establish a mobile connection. To enable, click **Apply** under **Mobile Settings.**
  - **Not installed**: The SIM card is not plugged into the Digi device server.
  - **Primary:** This is the preferred SIM to use to establish mobile connections.
  - **Secondary:** If you cannot establish a connection the primary SIM, a connection will be established with the secondary SIM.

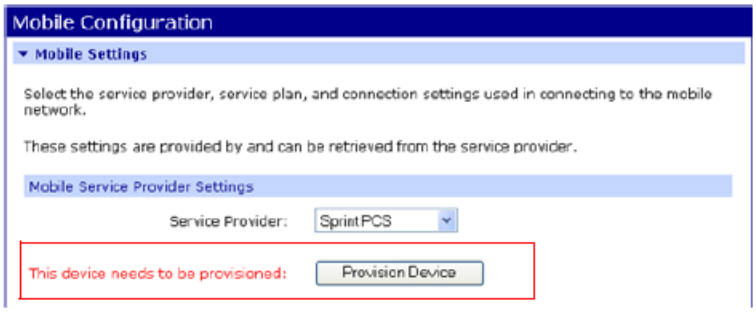
Mobile settings

Mobile service provider settings

The Mobile Service Provider settings identify the service provider to use in connecting to the mobile network. Information displayed varies by product and whether the remote service provider is GSM- or CDMA-based. Settings that may be displayed on this screen include:

- **Service Provider:** For GSM-based mobile service providers, this is the service provider to use in connecting to the mobile network. The service provider must match the provider that supplied the SIM card. This must match the provider that supplied the SIM card. (Not displayed for CDMA products.)
- **Service Plan:** For GSM-based mobile service providers, this is the service plan to use in connecting to the mobile network. This setting must match the plan that the service provider has supplied to you. This is also sometimes known as the APN (Access Point Name).
- **Username** and **Password:** For GSM-based mobile service providers, these settings are the user name and password of the mobile connection needed to access the mobile network.

- **Device provisioning state:** For CDMA-based mobile service providers, the text below the **Service Provider** selection list states whether the device has already been provisioned. If the device has not yet been provisioned, clicking the **Provision Device** button launches a wizard for provisioning the device. Mobile device provisioning is described next.



  If the device has been provisioned, text similar to the following appears: "This device has been properly provisioned. No further settings are necessary to communicate on the network. To re-provision this device for any reason (please use caution), **click here**".

Provisioning a mobile device

Mobile device provisioning is needed to properly configure the Digi device with the required information used to access the mobile network. The device must be provisioned before you will be able to create a data connection to the mobile network. The device only needs to be provisioned once. This type of provisioning applies only to Digi devices that have a CDMA cellular module.

For Digi devices, provisioning is done through the Mobile Device Provisioning Wizard, which is launched from the Mobile Configuration page.

Automatic versus manual provisioning

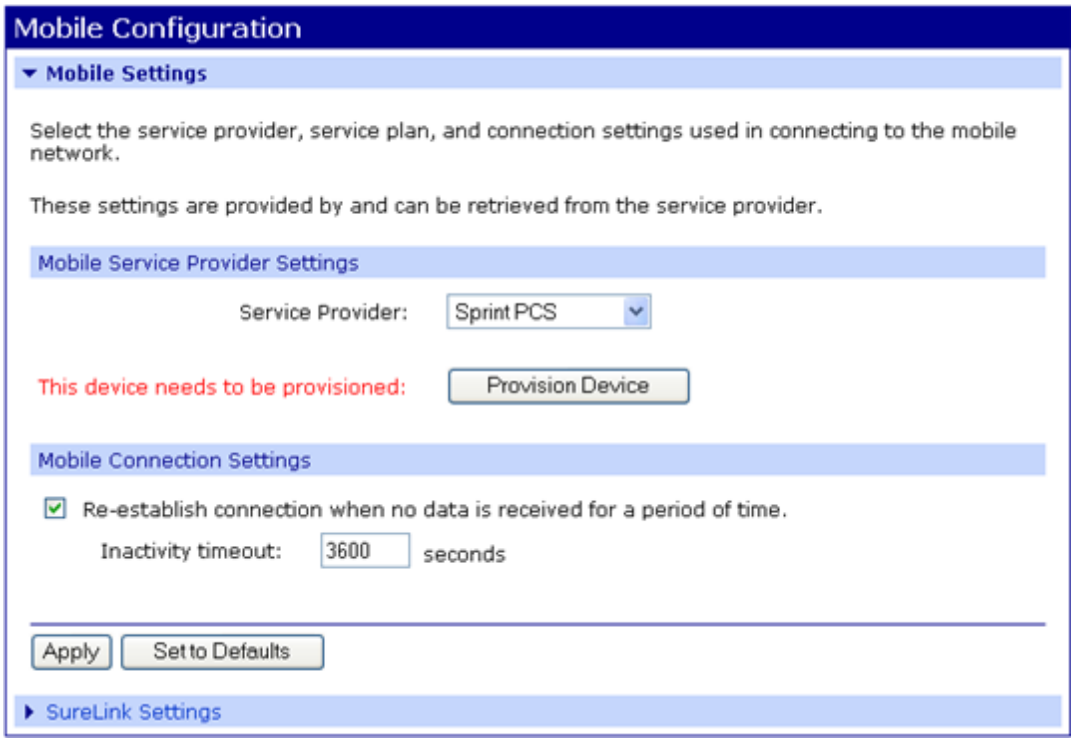
There are different types of provisioning methods depending upon your mobile provider. The Mobile Device Provisioning Wizard will provide the appropriate choices based on the mobile provider selected. Two main provisioning methods are:

- Automatic Provisioning: Typically, an automatic provisioning process called IOTA (IP-Based Over the Air) provisions the device. Note that automatic provisioning requires the modem device to communicate over the mobile network and requires a good signal to ensure proper provisioning.
- Manual Provisioning: Alternatively, you can use a manual provisioning method to manually specify the required fields needed to access the mobile network. The manual provisioning method is an advanced configuration normally used only for custom network access or providers. This method is not available for all mobile providers, and will not be available in the Mobile Device Provisioning Wizard if your mobile provider does not support it.

Launch the Mobile Device Provisioning Wizard

Below the **Service Provider** selection list is a line of text that states whether or not the device has already been provisioned or needs to be provisioned. If a device has not yet been provisioned, the Mobile Configuration page displays a message, as shown below. Click the **Provision Device** button to

launch the Mobile Device Provisioning Wizard. For example, here is how the **Mobile Settings** page looks when a device has not yet been provisioned.

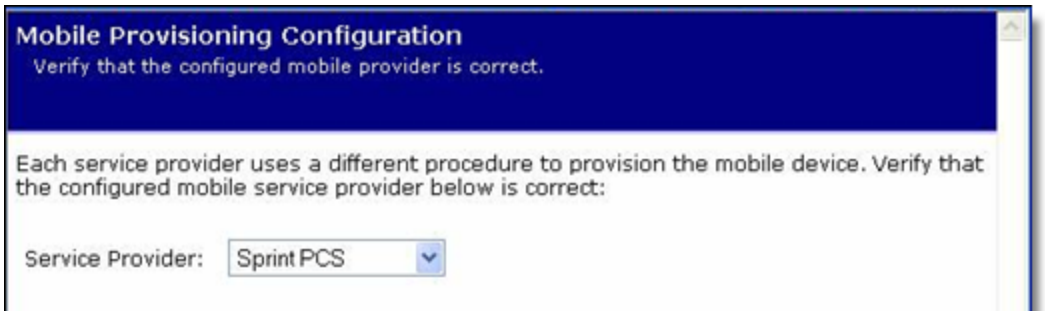


Example: provisioning a Digi device for Sprint PCS

The sequence of Mobile Device Provisioning Wizard screens displayed and the settings on them vary by product and mobile service provider.

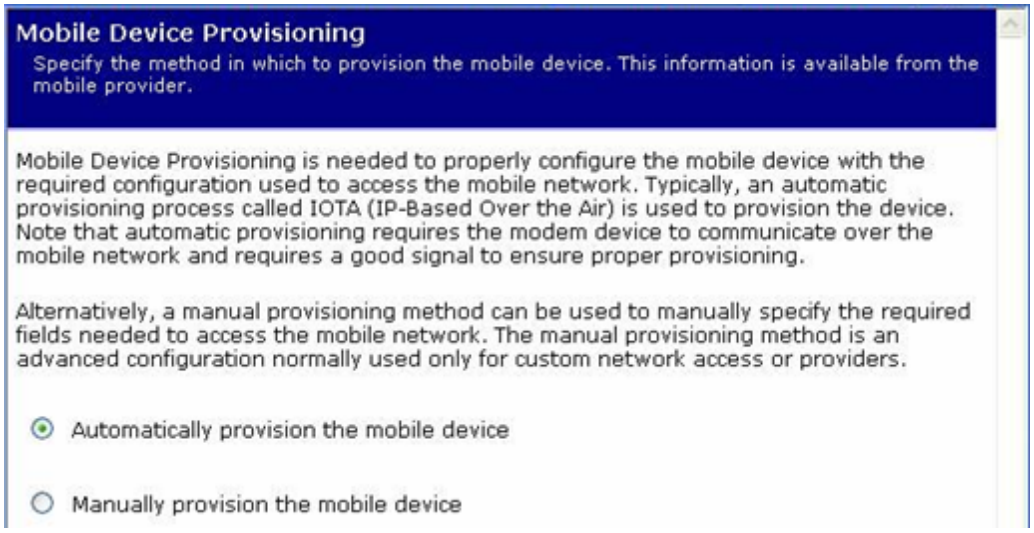
The following example shows how to provision a Digi device when Sprint PCS is the mobile service provider.

1. Select a mobile service provider from the list.



2. Select automatic or manual provisioning.

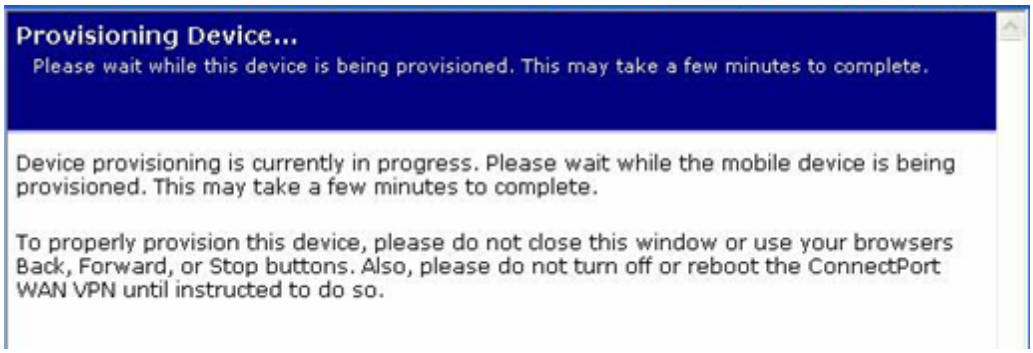
   The main difference between automatic and manual provisioning is that manual provisioning involves entering more information. You will have received all of this information from your mobile service provider during account setup.



3. As needed, enter device provisioning information provided by your mobile service provider.

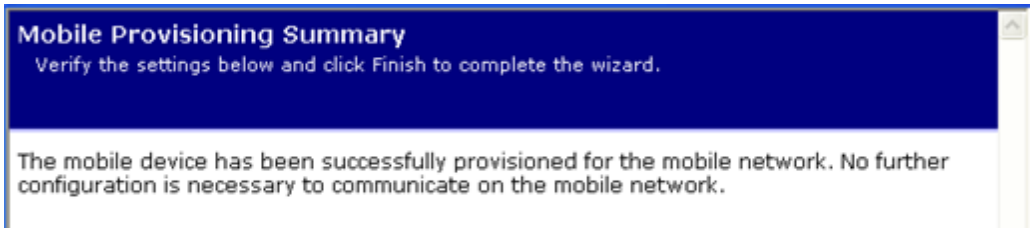
   On some modules, the provisioning information is already obtained and automatically entered. If the following screen appears, enter the provisioning information.

4. Device provisioning in progress...



5. Provisioning complete.

   Upon successful completion of provisioning, a screen appears stating that the provisioning was successful. Click **Finish.**



   If provisioning fails:

   The first screen of the provisioning wizard appears again. Instead, you must perform manual provisioning.

6. Click **Apply** on the **Mobile Configuration** page to complete the provisioning.

Reprovision a Digi device

To reprovision a Digi device, simply run the Mobile Device Provisioning Wizard again.

Mobile connection settings

Mobile connection settings configure how the mobile connection is established and maintained.

Re-establish connection when no data is received for a period of time:
Inactivity timeout: Whether the mobile connection will be disconnected and re-established after no data has been received over the link for the specified amount of time, in seconds.

SIM Selection Settings

The following options control how the Digi device chooses a SIM card to establish mobile connections.

The primary SIM will used first to try to establish a connection. If the connection is unsuccessful, the secondary SIM will be used instead. If it is also unsuccessful, the primary and then secondary SIMs will be tried again repeatedly.

Stop using this SIM and switch to the next SIM

These settings determine when a connection attempt is unsuccessful, at which point the Digi device should switch to the next SIM card to establish mobile connections.

- **If this SIM is not registered after *n* seconds**: The SIM has not registered with the mobile service provider after a specified number of seconds.
- **If roaming with this SIM**: The SIM is registered, but is roaming to another service provider. Your provider may apply additional connection charges when roaming.
- **After *n* connection failures**: A connection could not be established after the specified number of attempts.

Disconnect this SIM and return to the primary SIM

Once a connection has been successfully established with this SIM, these settings determine when to end the connection and return to using the primary SIM.

- **When the connection is dropped**: The connection has ended for any reason.
- **If the connection is idle for *n* seconds**: No data has been received over the mobile link for the specified number of seconds.
- **After a maximum of *n* seconds**: The connection has been established for the specified number of seconds.

Advanced settings

The following options configure advanced settings to manage the mobile PPP connection established by the Digi device. Unless otherwise stated, the mobile PPP connection is not restarted with the new settings when the changes are applied (saved). The changes are applied the next time the mobile PPP connection is restarted. Settings vary between CDMA and GSM cellular modems.

CDMA cellular modem advanced settings

- **Mobile Technology Settings**: Selects the CDMA technology to use for the mobile service connection. The available service depends on the mobile service provider and the geographic location of the Digi device server.

  Note The mobile PPP connection is not automatically restarted when a technology selection is configured.

  - **Automatic**: Enables automatic selection of a technology for the mobile service connection, whichever service is available. The modem will look for EvDO (3G) or 1xRTT (2G) service, whichever is available in that location.
  - **1xRTT**: Restrict the modem to find 1xRTT (2G) service only.
  - **EvDO**: Restrict the modem to find EvDO (3G) service only.

- **Mobile Antenna Settings**: Selects the mobile antenna configuration.
  - **Antenna diversity (two antennas)**: Automatically receive on either the main or auxiliary antenna, depending on which antenna has a better signal. Use this setting if two antennas are connected.
  - **Primary antenna only**: Always receive on the main antenna. Use this setting if only one antenna is connected.

GSM cellular modem advanced settings

- **Mobile Band Settings**: Select the mobile service frequency bands that you want to configure in the modem.

  Note The mobile PPP connection is not automatically restarted when a band selection is configured.

  - **Automatic**: Enables automatic service band selection by the modem. Automatic is the default value. Digi recommends using the default setting unless there is a reason to configure specific bands.
  - **2G Only**
  - **3G Only**
  - **Manual**: Selects the individual service bands that you want to configure. Improper selection or combinations may result in a failure to establish a mobile connection. Select one or more of these values: 850 MHz, 900 MHz, 1800 MHz, 1900 MHz.

- **Mobile Carrier Settings**: Mobile carrier selection allows you to configure the mobile device to use a specific mobile service only. The recommended and normal operation is for the mobile device to automatically find service with an available carrier. However, you can configure a manual selection to use a specific carrier. Please be aware that use of a manual carrier selection can result in a significantly longer time interval for the unit to find service on the specified network. Both the mobile network and the mobile device (modem) may influence this behavior. Therefore it is recommended that the **Automatic** selection be used wherever possible.

  WARNING! The scan for available carriers requires that you terminate the mobile PPP connection before you perform the scan. You cannot perform and complete a successful scan if it is initiated over the mobile connection, since the scan procedure requires user interaction that is not possible after the mobile PPP connection has been terminated.

  - **Automatic**: Enables automatic selection of a carrier for the mobile service connection. The mobile PPP connection is not automatically restarted if automatic carrier selection is configured.
  - **Manual**: Enables manual selection of the Network ID of a carrier for the mobile service connection. The carrier selection is the concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) value for a carrier. The MCC is always a three-digit decimal value, and the MNC is either a two- or three-digit decimal value. A properly entered Network ID is composed of five or six decimal digits, with no other characters in that value.

    The **Scan available carriers...** link initiates a wizard that instructs the modem to scan for available carriers and display a list from which the desired carrier may be selected. The scan may take as little as 20 seconds or up to two minutes to complete. Scanning for carriers requires that the mobile PPP connection be terminated so the scan may be performed. Upon completion of the wizard, the mobile PPP connection is restarted using the selected carrier.

    Note If the **Mobile Band Settings** selection in use by the modem is other than **Automatic**, the list of carriers returned by the scan may include only a subset of the carriers available in the area.

    You can manually enter the Network ID from a carrier selection from the list. However, the mobile PPP connection does not automatically restart if you are using the manual entry method.

Digi SureLink settings

Use the Mobile Connection Settings to configure Digi SureLink settings for a Digi device. SureLink can ensure that a Digi device is in a state where it can connect to the mobile network, and you can use them to monitor the integrity of the established mobile connection.

There are two groups of SureLink settings:

- **Hardware Reset Thresholds**: You can configure these settings to clear any error states that were resident in the Digi device's cellular module, so the device can once again connect to the network, if the connection is lost. It does this by first resetting the cellular module after a default or specified number of consecutive failed connection attempts, and then resetting the Digi device after a default or specified number of failed consecutive connection attempts. You can also disable each of these connection-failure settings.
- **Link Integrity Monitoring settings**: You can configure these settings to perform a selected test that examines the functional integrity of the network connection, and take action to recover the connection in the event that it is lost.

Hardware reset thresholds

- **Hard reset the modem module after the following number of consecutive failed connections:** Enables or disables a hard reset of the cellular modem module after the specified number of failed connection attempts. Specify a value between 1 and 255. The default is 3.
- **Power-cycle the device after the following number of consecutive failed connections:** Enables or disables a power-cycle of the Digi device after the specified number of failed connection attempts. Specify a value between 1 and 255. The default is 0, or off.

Link integrity monitoring settings

- **Enable Link Integrity Monitoring using the test method selected below:** Enables or disables the link integrity monitoring tests. If this setting is enabled, the other Link Integrity Monitoring settings may be configured and verify the functional integrity of the mobile connection. The default is off (disabled).

  There are three tests available:
  - Ping Test
  - TCP Connection Test
  - DNS Lookup Test

  You can use these tests to demonstrate that two-way communication is working over the mobile connection. Several tests are provided because different mobile networks or firewalls may allow or block Internet packets for various services. Select the appropriate test may be selected according to mobile network constraints and your preferences.

  The link integrity tests are performed only while the mobile connection is established. If the mobile connection is disconnected, the link integrity tests are suspended until the connection is established again.

  For the link integrity tests to provide meaningful results, the remote or target hosts must be accessible over the mobile connection and not through the LAN interface of the device (if it has one). That is, the configure the settings to guarantee that the mobile connection is actually tested.

  The link integrity test settings may be modified at any time. The changes are used at the start of the next test interval.

- **Ping Test:** Enables or disables the ability to use “ping” (ICMP) as a test to verify the integrity of the mobile connection. The test is successful if a valid ping reply is received in response to the ping request sent. The ping test actually sends up to three ping requests, at three second intervals, to test the link. When a valid reply is received, the test completes successfully and immediately. If a reply is received for the first request sent, there is no need to send the other two requests.

  Two destination hosts may be configured for this test. If the first host fails to reply to all three ping requests, the same test is attempted to the second host. If neither host replies to any of the ping requests sent, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.
  - **Primary Address**: First host to test.
  - **Secondary Address**: Second host to test (if the first host fails).
- **TCP Connection Test:** Enables or disables the creation of a new TCP connection as a test to verify the integrity of the mobile connection. The test is successful if a TCP connection is established to a specified remote host and port number. If the remote host actively refuses the connection request, the test is also considered to be successful, since that demonstrates successful two-way communication over the mobile connection. The TCP connection test waits up to 30 seconds for the connection to be established or refused. When the TCP connection is established, the test completes successfully, and the TCP connection is closed immediately.

  Two destination hosts may be configured for this test. If the first host fails to establish (or refuse) the TCP connection, the same test is attempted to the second host. If neither host successfully establishes (or refuses) the TCP connection, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.
  - **TCP Port**: The TCP port number to connect to on the remote host (default 80).
  - **Primary Address**: The address of the first host to test.
  - **Secondary Address**: The address of the second host to test (if the first host fails).

- **DNS Lookup Test:** Enables or disables the ability to use a Domain Name Server (DNS) lookup as a test to verify the integrity of the mobile connection. The test is successful if a valid reply is received from a DNS server. Typically, this means the hostname is successfully "resolved" to an IP address by a DNS server. But even a reply such as "not found" or "name does not exist" is acceptable as a successful test result, since that demonstrates successful two-way communication over the mobile connection. When a valid reply is received, the test completes successfully and immediately.

  The DNS servers used in this test for the hostname lookup, are the primary and secondary DNS servers obtained from the mobile network when the mobile PPP connection is first established. You can view these addresses by going to **Administration > System Information > Mobile**.

  Note that this DNS test is independent of the normal DNS client configuration and lookup cache, which is used for other hostname lookups. This test specifically requires communication over the mobile connection for each lookup, and to avoid being "short-circuited" by previously cached information. Also, this test does not interfere in any way with the normal DNS client configuration of this device.

  Two hostnames may be configured for this test. If the first hostname fails to get a reply, the same test is attempted for the second hostname. If no reply is received for either hostname, the test fails. The primary and secondary DNS names must be fully qualified domain names. Note that the reverse lookup of an IP address is possible, but that is usually unlikely to succeed in returning a name. Still, you can use a reverse lookup to demonstrate the integrity of the mobile connection.
  - **Primary DNS Name**: The first hostname to look up.
  - **Secondary DNS Name**: The second hostname to look up (if the first hostname fails).
- **Repeat the selected link integrity test every *N* seconds:** Specifies the interval, in seconds, at which the selected test is initiated (repeated). A new test will be started every ***N*** seconds while the mobile connection is established. This value must be between 10 and 65535. The default is 240.

  If the configured interval is less time than it takes a test to complete, the next test will not be initiated until the previous (current) test has completed.
- **Test only when idle:** Initiate the selected link integrity test only after no data has been received for the specified interval of time. This changes the behavior of the test in that the test interval varies according to the presence of other data received from the mobile connection.

  Although using this idle option may result in less data exchanged over the mobile connection, it also prevents the link integrity tests from running as often to verify the true bi-directional state of that connection.

- **Reset the link after the following number of consecutive link integrity test failures:** Disconnects and reestablishes the mobile connection after the configured number of consecutive link integrity test failures. This value must be between 1 and 255. The default is 3. When the mobile connection is reestablished, the "consecutive failures" counter is reset to zero.

  If the mobile connection is disconnected for any reason (including not as a result of a link integrity test failure), the consecutive failures count is reset to zero when the mobile connection is reestablished.

Status and statistical information for mobile connections

Once the mobile settings have been configured, you can monitor the status of mobile connections by going to **Administration** > **System Information** > **Mobile**. See Mobile Information and Statistics.

From the command line, this mobile information appears when you issue the **display mobile** and **display pppstats** commands.

Update PRL settings

Note These settings apply to Digi cellular-enabled products that use the Sierra Wireless MC57xx series CDMA/EVDO modules.

The Update PRL page is for loading a preferred roaming list (PRL) into the cellular module on the Digi device. A PRL is a database that resides in a mobile device that contains information used during the system selection and acquisition process. It is built by the mobile service provider, and is normally not accessible to users. The PRL indicates which bands, sub bands and service provider identifiers will be scanned and in what priority order. Without a PRL, a mobile device may not be able to roam, or obtain service outside of the home area. There may be cases where missing or corrupt PRLs can lead to not having service at all.

On many networks, regularly updating the PRL is advised if the subscriber uses the device outside the home area frequently, particularly if they do so in multiple different areas. This allows the mobile device to choose the best roaming carriers, particularly "roaming partners" with whom the home carrier has a cost-saving roaming agreement, rather than using non-affiliated carriers. You can use the PRL files to identify home networks along with roaming partners, thus making the PRL an actual list that determines the total coverage of the subscriber, both home and roaming coverage.

To load a PRL, fill in values for these settings:

- **PRL File**: The location and name of the PRL file to be loaded into the cellular module. Type the PRL file's pathname or click the Browse button and use the browse dialog to select the file.
- **MSL/OTSL**: The master subsidy lock (MSL) or a one-time subsidy lock (OTSL) associated with the module. This value is a six-digit activation or unlock code supplied by the mobile service provider.

Click the Upload button to upload the PRL file to the cellular module.

If the PRL loading/updating operation was successful, the status message PRL update successful appears in a blue box above the settings.

If an error occurs, a red box with a message describing the error appears above the settings.

You can update PRL over the air **by dialing the over-the-air (OTA) feature code *228.**

Short Message Service (SMS) settings

The following options configure the cellular Short Message Service (SMS) capabilities of the mobile module of the Digi device.

Important Notes:

- To determine whether the cellular modem in a Digi device supports SMS, telnet to the command line and type the **show smscell** command. If an error message is returned (**error: show option not found**), then SMS is not supported for that Digi device.
- SMS is a feature that may be available as part of your mobile service agreement. However, sending and receiving short messages (or "text messages") may have additional costs. Before using the SMS capabilities of your Digi device, verify with your mobile service provider that your agreement includes SMS as part of your service plan. Understand the costs of SMS before you enable the SMS features on this Digi device.
- Please read Supported character set.
- You can configure Digi devices to be managed by Remote Manager via SMS commands. These configuration settings are on the **Configuration > Remote Manager > Remote Manager SMS Settings** page and described in Short Messaging/Remote Manager SMS settings. This Remote Manager SMS functionality must be enabled through the Global SMS settings, described below.

Global SMS settings

- **Enable cellular Short Message Service (SMS) capabilities**: Enable SMS features on this Digi device. When this option is enabled, the remaining SMS options may be configured. This option is disabled (off) by default.
- **Send ACK reply via SMS when command is accepted**: When a command message is received via SMS, send an acknowledgment (ACK) message via SMS to the originator of the command message, indicating that the command has been accepted and will be processed. This option is disabled (off) by default.
- **Send NAK reply via SMS if password validation fails**: When a command message is received via SMS, and a required password is either missing or incorrect, send a negative acknowledgment (NAK) message via SMS to the originator of the command message, indicating that the command has been rejected due to password validation failure. This option is disabled (off) by default.
- **Global SMS Command Password**: When a command message is received via SMS, and a global password is specified in these settings, that password must be provided by the originator of the command message or the message will be rejected by the Digi device. If a command-specific password is configured, that command-specific password must be provided instead of this global command password. Specifically, a command-specific password overrides the global password, and the global password is not considered if a command-specific password is configured in the settings. This option is disabled (no global password required) by default. To remove the password, simply clear the password field on the settings page.

- **Default Message Receiver**: When **Default Message Receiver** receives a message via SMS, the **Default Message Receiver** determines which SMS **"**user**"** will receive the message and process it. This handling pertains to messages that are not enabled commands for which command processing is performed. The choices for this option are:
  - **Log Only:** The received message is logged but otherwise not processed (default option).
  - **Python:** The received message is passed to the standard Python receiver. Further processing of the message text is the responsibility of the Python program that is implemented to receive SMS messages. Note that these messages are logged when they are placed on the Python read queue.
- **Enable extended detail for SMS event logging (verbose)**: The SMS feature normally records limited, relevant activities to the system event log. These log entries identify SMS initialization, reconfiguration, and message send/receive activities. For troubleshooting purposes, you can enable this option to record the message send and receive activity logging in greater detail. However, this can result in filling the event log with more SMS activity records than are useful for normal operation. Digi recommends enabling this option only when detail is required for a limited period of time. This option is disabled (off) by default.

Python settings

Python-related settings for the SMS feature include:

- **Enable SMS support for Python**: Enable SMS features for Python on this Digi device. When this option is enabled, the remaining Python-specific SMS options may be configured. This option is enabled (on) by default.
- **Received Message Queue Maximum**: The number of received messages that may be placed on the dedicated Python SMS message read queue awaiting processing by Python. Once this limit is reached, new received messages are logged but discarded until the read queue falls below this configured maximum message count. The default value for this setting is 100 messages.
- **Received Message Hold Time Maximum**: The maximum amount of time in seconds that a received message will be held on the dedicated Python SMS message read queue while waiting for Python SMS message processing to be brought into service. This setting allows messages to be received and queued for Python before the Python program that processes them is ready to receive such messages, thereby eliminating loss of messages that are received before the Python program is ready to handle them. The default value for this setting is 600 seconds (10 minutes).

- **Python SMS Password**: Although this use is not typical, a message may be directed for deliver to Python by sending "**#python**" as a command to this Digi device. In such a case, this Python password may be configured to validate the acceptance of such a command message before it is accepted and placed on the dedicated Python SMS message read queue for further processing. When Python is configured as the **Default Message Receiver**, it is not necessary to use the Digi device command message syntax, since all otherwise unhandled messages will be delivered to the Python read queue. However, password validation is not performed for non-command messages. This option is disabled (no Python password required) by default. To remove the password, simply clear the password field on the settings page.

Built-in command settings

Several built-in commands are supported for execution via SMS messages sent to your Digi device. Descriptions of built-in command-related settings for the SMS feature follow. Full detailed descriptions of the SMS command syntax and supported command options is available on the Digi support web site.

Supported commands

The following table displays the supported commands.

Built-in command	Description
#help (alias **#?**)	The Digi device replies to the sender via SMS with a message that specifies the command syntax and a list of the supported, available commands that may be sent to this device. You may obtain further help for a specific command by sending that command as a parameter. For example, send **#help ping** to request a help reply for the **#ping** built-in command.
#cli	Request that a CLI command be run on the Digi device. The output from the CLI command is returned to the sender via SMS, with a limit of around 2000 characters for the number of CLI output characters returned in the reply.
#idigi (alias **#cwm**)	Manage or obtain status for a device connection to a Remote Manager server. The Digi device replies to the sender via SMS with a message that contains the status or result of the requested action.
#ping	Request that the Digi device reply to the sender via SMS to verify two-way SMS communication between the sender and the Digi device.

Command options

For each built-in command, the following options are supported:

- **Enable**: Enable the command for use via SMS. All commands are enabled by default.
- **Password**: Specify required password for the command message. The command message requires this password in order to be accepted for further processing. If you configure a command-specific password, you must provide that command-specific password instead of the global command password (if one is configured (see Global SMS settings for more information). A command-specific password overrides the global password and the global password will not be use if you configure a command-specific password in the settings. This option is disabled (no command password required) by default. To remove the password, simply clear the password field on the settings page.

Sender Control List (SCL) settings

The SCL allows you to select the addresses (or phone numbers) from which SMS messages will be accepted. This is in effect a "Caller ID" capability in which the Digi device screens message senders and either processes or discards the message according to the configured SCL rules.

Following are descriptions of the SCL-related settings for the SMS feature.

- **Enable SMS Sender Control List**: Enable the SCL capabilities on this Digi device. When you enable this option, you can configure the remaining SCL-specific SMS options. This option is disabled (off) by default.
- **Send NAK reply via SMS if received message is rejected by SCL**: Sends a negative acknowledgment (NAK) message via SMS to the originator of the command message indicating that the original message was rejected due to the configured SCL rules. This occurs when the Digi device receives a message via SMS from a sender who was blocked by the SCL rules. This option is disabled (off) by default.

For each SCL rule, you can configure the following options:

- **Enable**: Enables the rule for use by SMS. You can enable and disable rules without removing them from the SCL. Digi device ignores disabled rules when examining received messages.
- **Sender Address (Phone Number)**: The address (phone number) of the sender for which this rule applies. If the sender's address matches this configured address, the Digi device accepts the SMS message for further processing. If the sender's address does not match any of the enabled SCL rule addresses, the Digi device rejects it and no further processing is performed. To remove the address, simply clear the address field on the settings page.

- **Match Type**: Specifies the type of address match test to perform for this rule. The supported match types are as follows:
  - **Exact**: The sender's address must exactly match the address configured for this rule.
  - **Right**: The sender's address must match the address configured for this rule when comparing the rightmost characters to the shorter of the two strings (sender address, rule address). For example, “5551212” matches “13125551212” since the rightmost characters match to the length of the shorter string, “5551212”. This is the default match type.
  - **Left**: The sender's address must match the address configured for this rule when comparing the leftmost characters to the shorter of the two strings (sender address, rule address). For example, “1312555” matches “13125551212” since the leftmost characters match to the length of the shorter string, “1312555”.
  - **Partial**: The sender's address must match the address configured for this rule when comparing the consecutive characters to the shorter of the two strings (sender address, rule address). For example, “312555” matches “13125551212” since the shorter string “312555” is a substring of the longer string “13125551212”.

Supported character set

For SMS via GSM service, the Digi device has to translate between the GSM 03.38 7-bit alphabet and ASCII. ASCII is the native character set for the Digi device and is the character set used in the CLI and web UI.

The ASCII and GSM 03.38 characters do not map one-to-one, and in fact some ASCII characters must be represented in GSM 03.38 as multi-character escape sequences (per extensions to the original GSM 03.38 alphabet). In the following table, such characters are shown as “0x1Bhh” under the “GSM 03.38 Code” column. This notation indicates a two-character sequence, where “hh” is a pair of hexadecimal digits.

In the reverse translation (from GSM 03.38 to ASCII), some of the GSM 03.38 characters have no ASCII counterpart. These are replaced with ASCII space characters. One exception is the INVERTED QUESTION MARK (0x60 in GSM 03.38) which is replaced with an ASCII QUESTION MARK (0x3F) character.

The following table documents the supported characters and the mapping used between these two alphabets. Note that “unknown” characters are replaced with space characters during the translation. In the table below, such characters appear as “0x20 *” under the “GSM 03.38 Code” column.

Notes for the table:

- The GRAVE ACCENT character (0x60) in ASCII has no counterpart in GSM 03.38. The Digi device substitutes the GRAVE ACCENT with the APOSTROPHE (0x27).
- The characters marked with * indicate a substitution since the ASCII characters have no counterpart in GSM 03.38. The Digi device replaces these characters with the SPACE (0x20) character. As such, the Digi Connect WAN Family product does not support these characters in GSM short messages.

The following table displays the supported character set:

ASCII Code	GSM 03.38 Code	ASCII Character	Description
0x00	0x20 *	NUL	NULL
0x01	0x20 *	SOH	START OF HEADING
0x02	0x20 *	STX	START OF TEXT
0x03	0x20 *	ETX	END OF TEXT
0x04	0x20 *	EOT	END OF TRANSMISSION
0x05	0x20 *	ENQ	ENQUIRY
0x06	0x20 *	ACK	ACKNOWLEDGE
0x07	0x20 *	BEL	BELL
0x00	0x20 *	NUL	NULL
0x01	0x20 *	SOH	START OF HEADING
0x08	0x20 *	BS	BACKSPACE
0x09	0x20 *	HT	HORIZONTAL TABULATION
0x0A	0x0A	LF	LINE FEED
0x0B	0x20 *	VT	VERTICAL TABULATION
0x0C	0x1B0A	FF	FORM FEED
0x0D	0x0D	CR	CARRIAGE RETURN
0x0E	0x20 *	SO	SHIFT OUT
0x0F	0x20 *	SI	SHIFT IN
0x10	0x20 *	DLE	DATA LINK ESCAPE
0x11	0x20 *	XON	DEVICE CONTROL ONE
0x12	0x20 *	DC2	DEVICE CONTROL TWO
0x13	0x20 *	XOFF	DEVICE CONTROL THREE
0x14	0x20 *	DC4	DEVICE CONTROL FOUR
0x15	0x20 *	NAK	NEGATIVE ACKNOWLEDGE
0x16	0x20 *	SYN	SYNCHRONOUS IDLE
0x17	0x20 *	ETB	END OF TRANSMISSION BLOCK
0x18	0x20 *	CAN	CANCEL
0x19	0x20 *	EM	END OF MEDIUM
0x1A	0x20 *	SUB	SUBSTITUTE

ASCII Code	GSM 03.38 Code	ASCII Character	Description
0x1B	0x20 *	ESC	ESCAPE
0x1C	0x20 *	FS	FILE SEPARATOR
0x1D	0x20 *	GS	GROUP SEPARATOR
0x1E	0x20 *	RS	RECORD SEPARATOR
0x1F	0x20 *	US	UNIT SEPARATOR
0x20	0x20	SP	SPACE
0x21	0x21	!	EXCLAMATION MARK
0x22	0x22	"	QUOTATION MARK
0x23	0x23	#	NUMBER SIGN
0x24	0x02	$	DOLLAR SIGN
0x25	0x25	%	PERCENT SIGN
0x26	0x26	&	AMPERSAND
0x27	0x27	'	APOSTROPHE
0x28	0x28	(	LEFT PARENTHESIS
0x29	0x29	)	RIGHT PARENTHESIS
0x2A	0x2A	*	ASTERISK
0x2B	0x2B	+	PLUS SIGN
0x2C	0x2C	,	COMMA
0x2D	0x2D	-	HYPHEN-MINUS
0x2E	0x2E	.	FULL STOP (PERIOD)
0x2F	0x2F	/	SOLIDUS (SLASH)
0x30	0x30	0	DIGIT ZERO
0x31	0x31	1	DIGIT ONE
0x32	0x32	2	DIGIT TWO
0x33	0x33	3	DIGIT THREE
0x34	0x34	4	DIGIT FOUR
0x35	0x35	5	DIGIT FIVE
0x36	0x36	6	DIGIT SIX
0x37	0x37	7	DIGIT SEVEN

ASCII Code	GSM 03.38 Code	ASCII Character	Description
0x38	0x38	8	DIGIT EIGHT
0x39	0x39	9	DIGIT NINE
0x3A	0x3A	:	COLON
0x3B	0x3B	;	SEMICOLON
0x3C	0x3C	<	LESS-THAN SIGN
0x3D	0x3D	=	EQUALS SIGN
0x3E	0x3E	>	GREATER-THAN SIGN
0x3F	0x3F	?	QUESTION MARK
0x40	0x00	@	COMMERCIAL AT
0x41	0x41	A	LATIN CAPITAL LETTER A
0x42	0x42	B	LATIN CAPITAL LETTER B
0x43	0x43	C	LATIN CAPITAL LETTER C
0x44	0x44	D	LATIN CAPITAL LETTER D
0x45	0x45	E	LATIN CAPITAL LETTER E
0x46	0x46	F	LATIN CAPITAL LETTER F
0x47	0x47	G	LATIN CAPITAL LETTER G
0x48	0x48	H	LATIN CAPITAL LETTER H
0x49	0x49	I	LATIN CAPITAL LETTER I
0x4A	0x4A	J	LATIN CAPITAL LETTER J
0x4B	0x4B	K	LATIN CAPITAL LETTER K
0x4C	0x4C	L	LATIN CAPITAL LETTER L
0x4D	0x4D	M	LATIN CAPITAL LETTER M
0x4E	0x4E	N	LATIN CAPITAL LETTER N
0x4F	0x4F	O	LATIN CAPITAL LETTER O
0x50	0x50	P	LATIN CAPITAL LETTER P
0x51	0x51	Q	LATIN CAPITAL LETTER Q
0x52	0x52	R	LATIN CAPITAL LETTER R
0x53	0x53	S	LATIN CAPITAL LETTER S
0x54	0x54	T	LATIN CAPITAL LETTER T

ASCII Code	GSM 03.38 Code	ASCII Character	Description
0x55	0x55	U	LATIN CAPITAL LETTER U
0x56	0x56	V	LATIN CAPITAL LETTER V
0x57	0x57	W	LATIN CAPITAL LETTER W
0x58	0x58	X	LATIN CAPITAL LETTER X
0x59	0x59	Y	LATIN CAPITAL LETTER Y
0x5A	0x5A	Z	LATIN CAPITAL LETTER Z
0x5B	0x1B3C	[	LEFT SQUARE BRACKET
0x5C	0x1B2F	\	REVERSE SOLIDUS (BACKSLASH)
0x5D	0x1B3E	]	RIGHT SQUARE BRACKET
0x5E	0x1B14	^	CIRCUMFLEX ACCENT
0x5F	0x11	_	LOW LINE (UNDERSCORE)
0x60	0x27 (1)	`	GRAVE ACCENT
0x61	0x61	a	LATIN SMALL LETTER A
0x62	0x62	b	LATIN SMALL LETTER B
0x63	0x63	c	LATIN SMALL LETTER C
0x64	0x64	d	LATIN SMALL LETTER D
0x65	0x65	e	LATIN SMALL LETTER E
0x66	0x66	f	LATIN SMALL LETTER F
0x67	0x67	g	LATIN SMALL LETTER G
0x68	0x68	h	LATIN SMALL LETTER H
0x69	0x69	i	LATIN SMALL LETTER I
0x6A	0x6A	j	LATIN SMALL LETTER J
0x6B	0x6B	k	LATIN SMALL LETTER K
0x6C	0x6C	l	LATIN SMALL LETTER L
0x6D	0x6D	m	LATIN SMALL LETTER M
0x6E	0x6E	n	LATIN SMALL LETTER N
0x6F	0x6F	o	LATIN SMALL LETTER O
0x70	0x70	p	LATIN SMALL LETTER P
0x71	0x71	q	LATIN SMALL LETTER Q

ASCII Code	GSM 03.38 Code	ASCII Character	Description
0x72	0x72	r	LATIN SMALL LETTER R
0x73	0x73	s	LATIN SMALL LETTER S
0x74	0x74	t	LATIN SMALL LETTER T
0x75	0x75	u	LATIN SMALL LETTER U
0x76	0x76	v	LATIN SMALL LETTER V
0x77	0x77	w	LATIN SMALL LETTER W
0x78	0x78	x	LATIN SMALL LETTER X
0x79	0x79	y	LATIN SMALL LETTER Y
0x7A	0x20	z	LATIN SMALL LETTER Z
0x7B	0x1B28	{	LEFT CURLY BRACKET
0x7C	0x1B40	|	VERTICAL LINE (PIPE)
0x7D	0x1B29	}	RIGHT CURLY BRACKET
0x7E	0x1B3D	~	TILDE
0x7F	0x20 *	DEL	DELETE

WiMAX settings

For Digi devices equipped with WiMAX radios, the WiMAX settings configure the WiMAX radio and how it connects to a network.

Radio settings

These settings control the current state of the WiMAX radio, and its behavior when you start the Digi device.

- **Enable the WiMAX radio**: Turn on the radio, scan for available networks, and be ready to connect. If the radio is disabled, it will not transmit or receive over the air.
- **Automatically connect to the selected subscription**: Establish a connection when the Digi device server starts, and re-establish a connection if it is lost. Select an entry from the subscription list to automatically connect.

- **WiMAX Subscriptions**: A list of configured subscriptions or accounts. The service provider establishes these subscriptions when you sign up for network service.
  - **Operator**: The name of the network service provider (NSP) company that provides the network services and accounting.
  - **Name**: The name of the subscription or account with the network service provider.
  - **NSP-ID**: The identifier of the network service provider.
  - **Activated**: When activated, enables full service for a subscription. If not activated, you may need to establish service with the provider, usually by visiting their web site. If service has already been established, connect to the subscription to update the activation status.
- **Authentication**: log in to the network with the specified authentication and user credentials. If your service provider gave you account login information, select the authentication type and type the user name, password, and realm values.

  If you have a login of the form of ***username@realm***, type the user name and realm in separate fields, without the @ sign.

Network connection

You can use these options to explicitly control which subscription and network is connected.

- **Connect with automatic network selection**: Select the subscription you want to use from the subscription list. The Digi device chooses the best available network automatically.
- **Connect to a specific network**: Select the subscription you want to use from the subscription list. Also select the network to which you want to connect from the network list.

  Note Some networks may not allow a connection with the selected subscription.

- **WiMAX Networks:** A list of networks that are available for connections. The radio discovers these networks over the air during the scanning process. While connected, this list shows the networks found prior to connecting and will not be updated.
  - **Name**: The name of the network access provider (NAP) that provides network connectivity.
  - **Type**: The relationship to the subscribed network service provider. The possible relationship types are as follows:
    - **Home**: The network service provider operates the network.
    - **Partner**: A partner of the network service provider operates this network.
    - **Roaming**: The network provides roaming access for the network service provider.
    - **Unknown**: The network may not allow connections for the network service provider.
  - **NAP-ID**: The identifier of the network access provider.
  - **RSSI**: Received signal strength indicator. A measure of the signal level of the network.
  - **CINR**: Carrier to interference and noise ratio. A measure of the signal quality of the network.
  - **Refresh**: Update the list of available networks. Use this to see latest results of the scanning process.
  - **Scan**: Perform a wide-area scan for additional networks. Use scan to find unused networks on channels in the subscriptions list. The current network will be disconnected.

    The scan takes a few minutes to complete. During this time, you can update the list of networks by clicking **Refresh** and you can restart a connection by clicking **Connect**.
  - **Connect**: Click to connect to the selected subscription and network. The connection process takes a few seconds to complete. If a connection cannot be made, the Digi device will try to connect repeatedly until a it establishes a connection or you click **Disconnect**.
  - **Disconnect**: Click to disconnect from the Digi device from the current network. The radio will scan for available networks while not connected.

Additional WiMAX configuration information

For additional information on configuring and activating WiMAX settings, see *Digi Quick Note: Digi Connect WAN 4G and ConnectPort Sprint/CLEAR 4G Configuration*, available on the Digi support site.

Serial ports configuration

Use the Serial Ports Configuration page to establish a port profile for each serial port on the Digi Connect WAN Family product. The Serial Ports Configuration page includes the currently selected port profile for the serial port, detailed configuration settings for the serial port, dependent on the port profile selected, and links to basic and advanced serial settings.

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

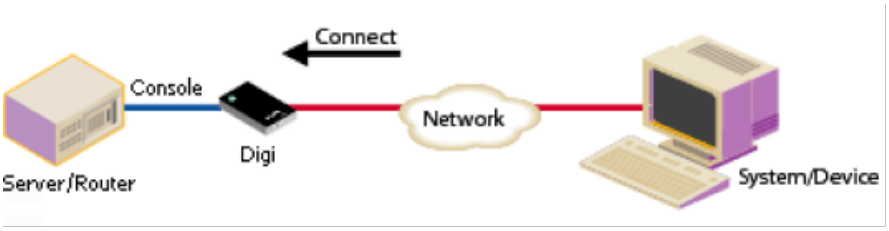
Select Port Profile

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

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

The Digi Connect WAN Family supports the following port profiles:

- **Console Management**: Manage a serial device's console port over a network connection. The Console Management profile allows you to access a Digi device's console port over a network connection. Most network devices such as routers, switches, and servers offer one or more serial ports for management. Instead of connecting a terminal to the console port, cable the console port to the serial port of the Digi Connect WAN Family product. Then using TCP/IP utilities like reverse telnet, network administrators can access these consoled serial ports from the LAN.



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

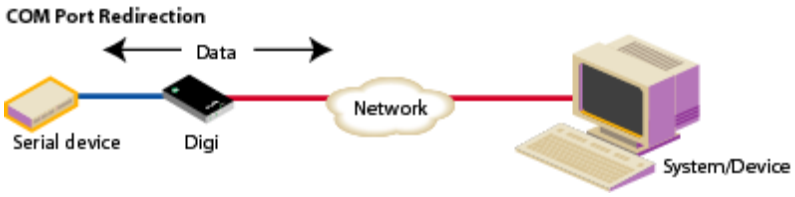
- **Custom**: The Custom profile is an advanced option to allow full configuration of the serial port. Use the Custom profile only if the serial port does not fit into any of the predefined port profiles. For example, when network connections involve a mix of TCP and UDP sockets. See Assign a profile to a serial port for more information.
- **DialServ**: The DialServ profile allows connecting a Digi DialServ™ device to the serial port. Digi DialServ is an RJ-11 phone line simulator that allows legacy devices with built-in modems to communicate across LANs/WANs. This profile configures the Digi device to connect/tunnel serial data to an external host when the DialServ receives an incoming call, causes the DialServ to make outgoing calls, and tunnels TCP data from the incoming connection over the Dialserv when TCP traffic is received on the configured ports on the Digi device.

  Important DialServ interoperation **requires** this profile.

- **GPS**: The GPS profile allows the Digi device to make use of an NMEA-0183 compliant GPS data stream for location and geofencing.
- **Local Configuration**: The Local Configuration profile allows you to sign in and access the command line interface when connecting directly to a serial port on a Digi device. This profile provides a login from the Digi device. See Assign a profile to a serial port for more information.

- **Modem Emulation**: The Modem Emulation profile allows you to configure the serial port to act as a modem. The Digi device server emulates modem responses to a serial device and seamlessly sends and receives data over an Ethernet network instead of a PSTN (Public Switched Telephone Network). This allows you to retain legacy software applications without modification and use a less expensive Ethernet network in place of public telephone lines. See Assign a profile to a serial port for more information.
- **RealPort**: Use RealPort to map a COM or TTY port to this serial port of your Digi device. The COM/TTY port appears and behaves as a local port to the PC or server. RealPort is also known as COM Port Redirection. See Assign a profile to a serial port for more information. Refer to the *RealPort Setup Guide* for instructions on installing and configuring the RealPort driver on your PC or server.

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



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

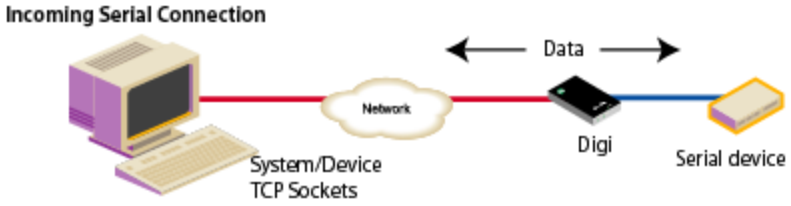
  Important Install and configure the RealPort software on each computer that uses RealPort ports. You can download and install the RealPort software from the Digi Support site. See Assign a profile to a serial port for installation instructions. You need to configure the RealPort software with the IP address of the Digi Connect WAN Family product.

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

  This profile configures each side of the bridge separately.

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

- **TCP Sockets**: Auto-Connect (TCP client) to another host on the network or allow incoming connections on this serial port (TCP server). The TCP Sockets profile allows serial devices to communicate over a TCP network. The TCP server allows other network devices to initiate a TCP connection to the serial device attached to the serial port of the Digi Connect WAN Family product. The TCP client will establish a TCP connection to a defined IP address and port number.



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

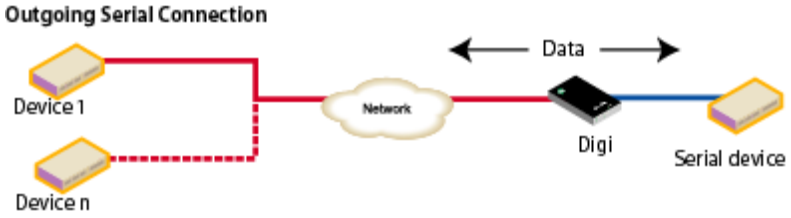
- Automatic TCP connections (Automatic Connection)
- RFC 2217
- TCP and UDP network port numbering conventions

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

- **UDP Sockets**: Allows the automatic distribution of serial data from one host to many devices at the same time. The UDP Sockets profile allows serial devices to communicate using UDP. The UDP Server configuration allows the serial port to receive data from one or more systems or devices on the network. See Assign a profile to a serial port for more information.

  The UDP Client configuration allows the automatic distribution of serial data from one host to many devices at the same time using UDP sockets.

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



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

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

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

Assign a profile to a serial port

To assign a profile to a serial port:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Automatic TCP connections (Automatic Connection)

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

TCP and UDP network port numbering conventions

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

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

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

RFC 2217

Use the RFC 2217 protocol to access serial devices over the network. RFC 2217 implementations enable applications to set the parameters of remote serial ports (for example, baud rate or flow control), detect line signal changes, as well as receive and transmit data. The configuration information provided in this section applies to Digi device functioning as RFC 2217 servers. If using the RFC 2217 protocol, do not modify the port settings from the defaults. If the port settings have been changed, restore the factory default settings (see Factory Default Settings). No additional configuration is required.

Industrial automation profile

This port profile is available in Digi devices that support Industrial Automation (IA) and the Modbus protocol. It has serial port settings appropriate for the Digi Connect WAN IA's use in IA applications. It

allows you to control and monitor various IA devices and PLCs. Serial ports for Digi Connect WAN IA devices are set to use this port profile by default. The default settings for the Digi Connect WAN IA and in this port profile is sufficient for most IA applications. If you need to change the settings from the defaults, use the "set ia" command, documented in the *Digi Connect® Family Command Reference*.

Basic serial settings

The basic serial port settings must match the serial settings of the connected device. If you do not know these settings consult the documentation that came with your serial device. These serial settings may be documented as 9600 8N1, which means that the device is using a baud rate of 9600 bits per second, 8 data bits, no parity, and 1 stop bit.

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

The possible settings are as follows:

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

Advanced serial settings

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

Serial settings

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

- **Enable RCI over Serial (DSR):** This choice allows configure the Digi Connect device through the serial port using the RCI protocol. See the RCI specification in the Digi Connect Integration Kit for further details.

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

TCP Settings

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

- **Send Socket ID**: Include an optional identifier string with the data sent over the network.

  The Socket ID can be 1 to 256 ASCII characters. Enter non-printable characters as follows:

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

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

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

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

- **Match string**: A 1 to 4 character string. This is usually the newline character sequence but can also be a custom string of 1 to 4 characters.
- **Strip match string before sending:** Search for the string specified in the Match String field before sending the data and strip the string from the string from the data before it is sent to the destination.
- **Send after the following number of idle milliseconds**: Send the data after the specified number of milliseconds have passed with no data received on the serial port.
- **Send after the following number of bytes**: Send the data after the specified number of bytes have been received on the serial ports.
- **Close connection after the following number of idle seconds**: Enable to close an idle connection. Use the **Timeout** field to enter the number of seconds that the connection will be idle before it is closed. This can be 1 to 65000 seconds.
- **Close connection when DCD goes low**: When selected, the connection will be closed when the DCD (Data Carrier Detected) signal goes low.

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

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

UDP settings

These UDP Settings are available only when the current port is configured with the Console management, the UDP Sockets, or the Custom Profile.

- **Send Socket ID**: Include an optional identifier string with the data sent over the network.

  The Socket ID can be 1 to 256 ASCII characters. Enter non-printable characters as follows:

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

Display current serial port settings

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

Camera

Digi Connect WAN Family products support connecting a WatchPort® Camera to one of its USB host ports. One Digi WatchPort V2 USB camera is supported.

Camera settings

Use the following settings to configure the camera operation and handling of images captured by the camera.

- **Enable Camera** Enables and disables camera. When disabled, all camera activity stops and all used memory is freed.
- **Resolution**: The resolution level for images.
- **Frame Delay**: The minimum time between frames in milliseconds. The actual delay time between frames will be this number or greater. The camera automatically increases this value as needed, such as in low light conditions. This delay time is the inverse of frames per second. For instance, if you want to set the camera to process at a maximum of 5 frames per second, the frame delay is set to 200 (1/5 = 0.2 second = 200 ms).
- **Quality**: Image quality. Choose a quality from 0 to 100; with 0 being the lowest quality and smallest image size and 100 being the best image quality and largest image size. Digi recommends a quality range from 30 to 80. Quality above 80 results in larger images, which result in lower overall performance and increased memory use.

- **Send Images to TCP Server**: Enables sending camera images to a TCP server. The TCP server application must conform to the protocol sent by this device, which is: on connect, the TCP client sends a protocol id of four bytes: 0x85ce4a71, followed by a protocol version of 4 bytes: 0x00000010. After this, images are sent repeatedly in the form of 4 bytes containing the length of the JPEG image to follow, and the JPEG image.
  - **TCP Server**: Name of the server to receive image data.
  - **TCP Port**: Type the TCP port number. The default port is 22222.
- **Current Image**: Displays a snapshot of the current camera image. Click the image to display a new window with the full-size image. If **No Camera Available** appears, the camera is disabled, no camera is attached to the Digi device, or some other problem is causing the camera to work incorrectly. You can access the current snapshot by typing the following URL in any web browser:

  ```
  http://device-ip/FS/dev/camera/0
  ```

  where *device-ip* is the IP address for the Digi device.
- **Advanced Settings**: All settings from **Automatic Gain Control** on are advanced camera settings. Digi recommends using the default camera settings listed under **Advanced Settings**. Advanced users can modify them as needed, but most users do not need to modify them.

Camera operation

Once you connect and configure the camera, the current snapshot image from the camera is available directly from the device at the following URL:

```
http://device-ip/FS/dev/camera/0
```

where *device-ip* is the IP address for the Digi device.

You can view video from the camera by streaming the camera data to a TCP server application. To stream camera data over a TCP server application, complete the configuration settings under **Send Images to TCP Server**. For more information, see the installation guide for your Watchport Camera.

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, alarms for signal strength and amount of cellular traffic for a given period of time.

Alarm notification settings

Use the Alarm Notification Settings page to configure the following:

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

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

  When you disable this setting alarm notifications are not sent to Remote Manager. Disable this setting if devices are not managed by a Remote Manager server or if alarms are sent from the device. For example, an SNMP trap destination is local to the device, not Remote Manager.
- **Mail Server Address (SMTP):** Specifies the IP address of the SMTP mail server. Ask your network administrator for this IP address.
- **From:** Specifies the text that used in the “From:” field for all alarms that are sent as emails.

Alarm list and status

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

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

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

Alarm Conditions

Use the Alarm Conditions page to specify the conditions on which the alarm is based, such as 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.
- **Send alarms based on average RSSI level below threshold for amount of time:** Send alarms based on the average signal strength falling below a specified threshold for a specified amount of time.
  - **RSSI:** The threshold signal strength, measured in dB (typically -120 dB to -40 dB).
  - **Time:** The amount of time, in minutes, that the signal strength falls below the threshold.

Note The **set alarms** command has an option, **optimal_alarms_enabled={yes|no}** that, when enabled, causes an optimal alarm to be sent when the signal strength returns to a value above the specified threshold. This feature is only available through the command line. The default is **no**; it must be explicitly enabled if desired.

- Send alarms based on cellular data exchanged in an amount of time:
  - **Data:** The number of bytes of cellular data.
  - **Time:** The number of minutes.
  - **Cell Data Type:** Type of cellular data exchanged: receive data, transmit data, total data.

Alarm Destinations

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

- **Send E-mail to the following recipients when alarm occurs**: Enable sending the alarm as an email message. Then specify the following information:
  - **To**: The email address to which this alarm notification email message will be sent.
  - **CC**: The email address to which a copy of this alarm notification email message will be sent (optional).
  - **Priority**: The priority of the alarm notification email message.
  - **Subject**: The text to be included in the Subject: line of the alarm-notification email.
- **Send SNMP trap to the following destination when alarm occurs**: Specifies whether to send the alarm as an SNMP trap. To send alarms as SNMP traps, you must set the **Alarm Type** to **snmptrap** and specify the IP address of the destination for the SNMP traps in the SNMP settings (**Configuration > System > Simple Network Management Protocol**). See Simple Network Management Protocol (SNMP) Settings. That destination IP address appears below the “Send alarm to SNMP destination” check box. You can also specify a secondary or backup SNMP destination.

To configure an alarm notification to be sent as both an email message and an SNMP trap:

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

Configure alarm conditions

To configure an alarm:

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

System Configuration

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

Device Identity Settings

Use the Device Identity Settings page to create a description of the Digi Connect WAN Family product's name, contact, and location. You can use this information to identify a specific Digi device product when working with a large number of devices in multiple locations.

- **Description**: The network name assigned to the Digi device.
- **Contact**: The SNMP contact person (often the network administrator).
- **Location**: A text description of the physical location of the Digi device.
- **Device ID**: A text description of the device ID used to identify the device (for example, MAC or IP address).

Simple Network Management Protocol (SNMP) Settings

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

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

- **Private community**: The password required to set SNMP-managed objects. The default is **private**.
- **Allow SNMP clients to set device settings through SNMP:** This check box enables or disables the capability for users to issue SNMP **set** commands uses use of SNMP read-only for the Digi device.

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

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

Date and Time Settings

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

Set the date and time

To set the date and time, click the **Set** button to configure the hours, minutes, seconds, month, day, and year on the device.

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

Offset from UTC

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

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

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

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

Time source settings

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

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

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

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

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

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

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

Time Source Global settings

Use the Time Source Global settings to configure the global settings that control time source management.

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

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

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

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

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

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

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

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

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

Remote Manager settings

The Remote Manager configuration page sets up the connection to the Device Management remote management server so the Digi device can connect to the server. Device Management allows you to configure and manage Remote Manager-registered devices from remote locations.

In this discussion:

- *Remote Manager* refers to the Digi machine-to-machine cloud-based network operating platform.
- *Device Management* refers to a web based device management application that allows a user to manage their inventory of devices.

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

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

Device ID requirement for the Digi device

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

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

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

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

Connection settings

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

About Remote Manager connections

If you enable Short Message Service (SMS) capabilities on your Remote Manager-registered device, a device-initiated connection may be requested through a *paged connection*. To illustrate how these types of connections work, the following image shows a configuration scenario featuring Remote Manager-registered devices communicating over a cellular network.

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

In a *device-initiated Remote Manager connection*, the Remote Manager-registered device connects to the network, and tries to establish a connection to Remote Manager. To maintain the connection, the Remote Manager-registered device sends *keep-alive messages* over the connection. You can configure

the frequency in which keep-alive messages are sent. You can use device—initiated Remote Manager connections in any cellular network, whether using public or private IP addresses, or even if using NAT. Note that your cellular/mobile provider may charge you, depending on your cellular/mobile service plan, when the Remote Manager-registered device sends keep-alives messages.

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

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

A *paged connection* is another form of a device-initiated connection. An on-demand request, such as a Short Message (SM) received via a cellular modem from a mobile service provider, initiates this type of connection. The request message may specify the Remote Manager platform with which the Remote Manager-registered device should connect, or it may simply request that the device connect to the Remote Manager platform configured in the **Paged Remote Manager Connection** settings. Paged Remote Manager Connections require both the global SMS configuration (**Configuration** > **Mobile** > **Short Message Service Settings** > **Enable cellular Short Message Service (SMS)** capabilities to be enabled, and the **Configuration** > **Remote Manager** > **Short Messaging** > **Remote Manager SMS Settings** > **Enable Remote Manager SMS** settings, along with the current Phone Number and Service ID settings.

Device IP address updates

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

Device-Initiated Remote Manager Connection settings

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

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

Server-Initiated Remote Manager Connection settings

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

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

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

Retry if the IP address update fails:

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

Timed Remote Manager connection

- **Enable Timed Remote Manager Connection**: When enabled, this Digi device initiates the connection to the Remote Manager Server at the configured interval (period). A timed connection defers to (will not disrupt) an established Remote Manager connection. If a timed connection defers to an existing Remote Manager connection, or if the Digi device server cannot successfully establish the timed connection, the Digi device server will try again at the next interval.
- **Remote Manager Server Address**: The IP address or hostname of the Remote Manager Server.
- **Connect every: H hrs M mins**: The interval (period) in hours and minutes in which the Digi device server attempts a timed connection to the specified Remote Manager Server.
- **After boot, wait before first timed connection**: When the Digi device server boots (starts up), you may observe a delay before the first timed connection is attempted. Choose one of the following options on how to handle the delay:
  - **Immediate**: Attempt first timed connection immediately.
  - **One Interval**: Attempt the first timed connection after one configured interval (period) has elapsed.
  - **Random Delay**: Attempt the first timed connection after a random interval of time between zero (immediate) and the configured interval (period). Choose this option when you have a number of Digi device deployed in a single location and you want to distribute the first Remote Manager timed connection attempt for each Digi device over time when power is restored after an outage.

Paged Remote Manager Connection settings

- **Enable Paged Remote Manager Connection**: When enabled, the Remote Manager-registered device initiates a paged connection to Remote Manager when requested to do so from an external communication, such as a Short Message received via a mobile service provider. The external communication may specify the Remote Manager platform with which the Remote Manager-registered device should connect, or it may simply request that the Remote Manager-

registered device connect to the Remote Manager platform that is configured in the **Paged Remote Manager Connection** settings.

Paged Remote Manager connections provide emergency access to your Remote Manager-registered device that directs it to connect to Remote Manager so that you can perform management or application operations.

You can configure a paged Remote Manager connection to disconnect an established connection to Remote Manager and establish a connection to the Paged Remote Manager connection, or you can configure it to defer to an established Remote Manager connection.

If you do not enable paged Remote Manager connections, the Remote Manager-registered device refuses to receive paged connection requests via external communication. This setting fully controls whether or not paged Remote Manager connections are allowed.

- **Remote Manager Server Address**: The IP address or hostname of the Remote Manager platform. For a paged Remote Manager connection, you do not have to provide the Remote Manager address in the configuration settings. You can specify the Remote Manager address in the external communication that requests the paged connection. The external communication can override this configuration option with its own Remote Manager address selection. This allows you to use a paged Device connection to support emergency Remote Manager device management.
- **Disconnect the current Remote Manager connection before making a paged connection**: When enabled, the Remote Manager-registered device terminates an established connection to Remote Manager, and then it connects to the Remote Manager platform specified in the Paged Remote Manager Connection settings or specified in the external communication (such as a Short Message). The external communication can disconnect an established Remote Manager connection, thereby overriding this configuration option. This allows you to use a paged Device connection to support emergency Remote Manager device management.

Short Messaging/Remote Manager SMS settings

Use the **Remote Manager SMS Settings** page to configure the Remote Manager-registered device to be managed by Remote Manager via Short Message Service (SMS) messages.

For these Remote Manager SMS settings to work, you must enable the global SMS settings under Mobile SMS settings. See Global SMS settings.

- **Enable Remote Manager SMS**: Select this option to enable Remote Manager SMS support.
- **Phone Number**: The phone number or short code of the Remote Manager platform. For more information about the Remote Manager SMS Phone Number and Service ID fields, contact your Digi sales Representative, or use the Remote Manager **Provision** command.
- **Service Identifier**: The Service Identifier (prefix) for Remote Manager. This field is an optional setting that you can use when you are using a shared short code. Redirecting the message to a specific service under that short code requires an identifier (prefix).

- **Adjust Device SMS Settings to Remote Manager recommended values**: This setting applies several Global SMS configuration options (as described in Global SMS settings) that are required by the Remote Manager SMS feature.
- **Restrict Sender**: Only process inbound messages for Remote Manager from the number specified in the **Phone Number** setting. Messages from other phone numbers will be passed on to other SMS Services on the device.

Advanced Remote Manager settings

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

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

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

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

    The interval settings are used with the Assume connection is lost after *n* timeouts setting to signal when the connection has been lost.
  - **Device Send Interval**: Specifies how frequently the device sends a keep-alive packet to Remote Manager if the Remote Manager connection is idle. Remote Manager expects to receive either Remote Manager protocol messages or keep-alive packets from the device at this interval.
  - **Server Send Interval**: Specifies how frequently the Remote Manager-registered device sends a keep-alive packet to Remote Manager if the Remote Manager connection is idle. Remote Manager expects to receive either Remote Manager protocol messages or keep-alive packets from the Remote Manager-registered device at this interval.

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

  - **Assume the connection is lost after *n* timeouts (Wait Count)**: After the number of consecutive expected keep-alives specified by this setting are missed according to the configured intervals, the connection is considered lost and is closed by the device and Remote Manager.

- **Connection Method**: Specifies the method by which the associated interface connects to Remote Manager.
  - **TCP**: Connect using TCP. This is the default connection method, and is typically good enough for most connections. It is the most efficient method for connecting to Remote Manager in terms of speed and transmitted data bytes.
  - **Automatic**: Automatically detect the connection method. This connection method is less efficient than TCP, but it is useful in situations where a firewall or proxy may prevent direct connection via TCP. This option tries each connection option until a connection is made. This connection method requires that you specify **HTTP over Proxy Settings**.
  - **None**: This value has the same effect as selecting TCP.
  - **HTTP**: Connect using HTTP.
  - **HTTP over Proxy**: Connect using HTTP.
  - **HTTP over Proxy Settings**: The settings required to communicate over a proxy network using HTTP. These settings apply when you select when **Automatic** or **HTTP over Proxy** connection methods.
  - **Hostname**: The name of the proxy host.
  - **TCP Port**: The network port number for the TCP network service on the proxy host.
  - **Username**:
    Password: The user name and password used to sign in to the proxy host.
  - **Enable persistent proxy connections**: Specifies whether the Remote Manager-registered device should use HTTP persistent connections. Not all HTTP proxies correctly handle HTTP persistent connections. Using persistent connections can improve performance when exchanging messages between the Remote Manager-registered device and Remote Manager using the HTTP/proxy connection. You can reuse the same HTTP connection for multiple consecutive HTTP requests and replies, eliminating the overhead of establishing a new TCP connection for each individual HTTP request/reply, then closing that connection when the request is complete.

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

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

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

Manage alarms through Remote Manager

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

Users

User settings involve several areas:

- **User authentication**: Whether authentication is required for users accessing the Digi Connect WAN Family device and the information required to access it. You specify whether the user authentication is a user name and password or an SSH public key. Depending on the Digi device, you can define multiple users and their authentication information. User authentication settings are on the Users settings page.
- **User access settings**: Device interfaces that a user can access, such as the command line or web interface.
- **User permissions settings**: Permissions a user has for accessing and configuring the device.
- **Network configuration settings to further secure your device**: Digi devices with cellular capability present additional security considerations, mainly involving securing the border between the Digi device and the cellular network. Several settings on the **Network Configuration** pages are available to further secure the Digi Connect WAN Family product. For example, you can disable unused network services on the **Network Services** page. On the IP Filtering page, you can allow access from a specified devices and networks, and drop all other connection attempts.

About user models and user permissions

For Digi devices that have a one-user model:

- By default, there is no login prompt.
- The default name for user 1 is **root**. This user is also known as the administrative user.

The Digi Connect WAN Family products provides the following user models:

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

To determine which user model to implement:

In the web interface, if the menu includes **Users**, the Digi Connect device uses either the two-user model or the more than two users model.

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

Two-user model

- User 1 has a default name of **root**. This user is also known as the administrative user.
- User 1 has default permissions that enables it to issue all commands.
- You can change permissions for User 1 to be less than the default root permissions.
- User 2 is undefined. That is, the user does not exist by default, but you can define User 2.

- Use the User Permissions settings in the web interface or the **set permissions** command in the command-line interface (see the *Digi Connect® Family Command Reference* for command description) to configure the permissions for User 2.
- You can change permissions for User 2 to be either greater than or less than its default.

More-than-two-user model

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

Password authentication

By default, there is no password authentication for Digi Connect WAN Family devices. When you access the Digi device by opening the web interface or issuing a telnet command, no login prompt appears.

Enable password authentication

To enable password authentication from the web interface:

1. Select **Configuration** > **Security**.
2. On the Security Configuration page, select the **Enable password authentication** check box.
3. Type the new password in the **New Password** and **Confirm Password** edit boxes.
4. Click **Apply**.
5. A prompt appears to immediately log back in to the web interface using the new values.

To enable password authentication for a Digi device that uses the one-user model from the command line:

- Issue a **newpass** command with a password length of one or more characters.

Disable password authentication

You can disable password authentication as needed.

To change a password from the web interface:

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

To change a password from the command line:

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

Change the password for an administrative user

To increase security, change the administrative user's password from its default. The default administrative password is **root**.

Note Record the new password. If you lose this password, you must reset the Digi Connect WAN Family product to the default firmware settings.

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

To change the administrative password from the web interface:

1. Select **Configuration** > **Security**.
2. Select the **Enable password authentication** check box.
3. Type the new password in the **New Password** and **Confirm Password** fields. You can specify a case-sensitive password from 4 to 16 characters long.
4. Click **Apply**. You are immediately logged off. Sign in to the web interface using the new values.
5. Sign in to the web interface using the administrative password.

To change the administrative password from the command line:

- Issue a **newpass** command.

Upload and SSH public key

You can configure SSH to sign in to servers without having to provide a password. This is called "public key authentication" and is more secure than using a normal password.

You can generate a public/private key using a program called ssh-keygen, and store a copy of the public key on the server(s) that you wish to use for authentication. When you sign in, the server sends you a message encrypted with your public key. Your machine decrypts it and sends back the original message, proving your identity.

To upload an SSH public key:

1. On the Main menu, click **Security**.
2. On the **Security Configuration** page, select the **Enable SSH public key authentication** check box.
3. Type or paste the SSH public key in the edit box.
4. Click **Apply**.

Add a user

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

To add a user:

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

Change user access settings

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

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

To set access settings:

1. Select **Configuration** > **Users**.
2. Click a user under **User Name**.
3. Click **User Access**.
4. Enable or disable the device interface access as desired:
   - **Allow command line access:** Enables or disables access to the command line.
   - **Allow web interface access:** Enables or disables access to the web interface.
5. Click **Apply**. The changes take effect immediately. No logout/login is necessary.

User permissions settings

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

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

User permissions and effects

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

Restrictions on setting user permissions

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

Set user permissions

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

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

3. Click **User Permissions**.
4. A list of feature groupings and the user permissions for them appears. Customize these settings as needed.
5. Click **Apply**.

- Set user permissions from the command-line interface:

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

Control user access

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

Disable unused and non-secure network services

Depending on your mobile service provider, other users can access your Digi Connect WAN Family product over the Internet, through various network services enabled on your Digi Connect WAN Family product. To further secure the Digi Connect WAN Family product, you can disable network services that are not required for the Digi device. You can disable non-secure or un-encrypted network services such as Telnet. See Network Services Settings.

Use IP filtering

You can restrict your Digi device on the network by only allowing certain devices or networks to connect to it. This is known as IP filtering or Access Control Lists (ACL). IP filtering allows you to configures a Digi device to accept connections from specific and known IP addresses or networks only, and silently drop other connections. You can filter the Digi devices on a single IP address or restricted as a group of Digi devices using a subnet mask that only allows specific networks to access to the Digi device. IP Filtering settings are a part of the Network configuration settings. See IP filtering settings.

Important Plan and review your IP filtering settings before applying them. If you apply the settings incorrectly the Digi device will be inaccessible from the network.

Use the Network Port Scan Cloaking feature

The Network Port Scan Cloaking feature allows you to configure this Digi device to ignore (discard) received packets for services that are hidden or not enabled and network ports that are not open. You can use this feature to protect your Digi device from malicious software or denial of service attacks. For more information, see Network Port Scan Cloaking.

Position and GPS support

Certain Digi devices have native GPS support with a geofence application. There are two groups of position settings. Static position settings define the latitude and longitude coordinates for the Digi device. GPS geofence settings define perimeters around a point. If the Digi device moves into, out of, or is outside of the perimeter is reported to the Digi device's event log, an SNMP server, or reported via e-mail. You must configure a supported GPS receiver use by the Digi device.

A GPS drive allows GPS data to be read from devices providing an NMEA-0183-compliant serial stream via serial or USB. Python, the web interface, command line, Remote Manager, and the geofencing application can use this data.

Static position settings

The static position settings define latitude and longitude coordinates for the Digi device. You can query these parameters with the RCI protocol and applications, such as the Remote Manager, can use this information.

- **Latitude**: The static latitude of the device, in degrees (-90.0 - 90.0).
- **Longitude**: The static longitude of the device, in degrees (-180.0 - 180.0).

Geofence settings

You can define up to 16 geofences. To add a geofence, click the **Add** button. The configuration settings for the geofence appear.

General settings

- **Name**: A name to reference this geofence. This name will appear in the event log, SNMP trap, and/or e-mail report.
- **Latitude**: Latitude of the center of the geofence, in degrees (-90.0 - 90.0).
- **Longitude**: Longitude of the center of the geofence, in degrees (-180.0 - 180.0).
- **Maximum HDOP**: This is the maximum tolerated horizontal dilution of precision that is allowed for reporting a geofence event. When the reported HDOP is greater than this value, fence event log reports, SNMP traps, and e-mail reports will not be sent. HDOP tolerances vary by receiver.
- **Entry Radius**: The entry radius, in meters, is the distance from the center of the fence for entry. That is, if the device is less than this distance from the defined center, an entry event has occurred.
- **Exit Radius**: The exit radius, in meters, is the distance from the center of the fence for exit. That is, if the device is more than this distance from the defined center, an exit event has occurred. This is also the distance used to determine if the device is outside of the fence for update events.
- **Location Update Interval**: The location update interval, in seconds, specifies the amount of time to wait between reporting that the device is outside of the geofence. This applies to event log, SNMP, and e-mail reports.

Email settings

- **Notify on Fence Entry**: An email will be sent to the defined recipients via the configured SMTP servers when the device has entered the geofence defined by the geofence center and entry radius.
- **Notify on Fence Exit**: An email will be sent to the defined recipients via the configured SMTP servers when the device has left the geofence defined by the geofence center and exit radius.

- **Send Location Update Notifications When Outside Fence**: An email will be sent to the defined recipients via the configured SMTP servers when the device is outside of the geofence defined by the geofence center, and exit radius. Emails will be sent at the interval defined by the location update interval parameter.
  - **Primary SMTP Server Address**: The IPv4 address of the primary SMTP email server.
  - **Secondary SMTP Server Address**: The IPv4 address of the secondary SMTP email server.
  - **Recipient**: The email address of the recipient of the geofence report email.
  - **CC: Recipient**: The email address of the carbon copy (CC:) recipient of the geofence report email .
  - **From**: The email (return) address of the originator of the geofence report email .
  - **Subject**: The subject line that will appear on the geofence report email.
  - **Priority**: The priority of the email . You can specify normal and high priority.
- **Include Location Data in Body**: Selecting this check box indicates that the current location of the device is included in the geofence email .
  - **Body Text**: This parameter specifies the body text for the email .

SNMP settings

- **Trap on Fence Entry**: An SNMP trap will be sent to the defined SNMP servers when device has entered the geofence defined by the geofence center, and entry radius.
- **Trap on Fence Exit**: An SNMP trap will be sent to the defined SNMP servers when the device has left the geofence defined by the geofence center, and exit radius.
- **Send Location Update Traps When Outside Fence**: An SNMP trap will be sent to the defined SNMP servers when the device is outside of the geofence defined by the geofence center, and exit radius. SNMP traps will be sent at the interval defined by the location update interval parameter.

Event log settings

- **Send Fence Entry Events to Event Log**: A log entry will be written when device has entered the geofence defined by the geofence center, and entry radius.
- **Send Fence Exit Events to Event Log**: A log entry will be written when the device has left the geofence defined by the geofence center, and exit radius.
- **Send Location Update to the Event Log When Outside of the Fence**: A log entry will be written when the device is outside of the geofence defined by the geofence center, and exit radius. Log entries will be written at the interval defined by the location update interval parameter.

Applications pages

Most Digi devices support additional configurable applications. Use the options under **Application** to configure applications. The application options vary depending on the Digi device.

- **Python**: For loading and running custom programs authored in the Python programming language onto Connect and ConnectPort devices that support Python.
- **RealPort**: Configures RealPort settings.
- **Industrial Automation**: Configures the Digi device for use in industrial automation applications.

Python Configuration

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

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

Python Files

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

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

Auto-start settings

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

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

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

Manually execute uploaded Python programs

To manually execute an uploaded Python program on a Digi Connect WAN Family device:

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

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

View and manage Python programs

To view Python threads running on the Digi Connect WAN Family device:

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

Python program management and programming resources

Digi incorporates a Python development environment into Digi Connect WAN Family devices. Digi integration of the universal Python programming language allows customers an open standard for

complete control of connections to devices, the manipulation of data, and event-based actions.

Recommended distribution of Python interpreter

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

Digi Wiki for Developers

Digi Wiki for Developers is where you can learn how to develop solutions using Digi's communications products, software and services. The wiki includes how-to's, example code, and M2M information to speed application development. Digi encourages an active developer community and welcomes your contributions.

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

Digi Python Custom Development Environment page

Use Python functions to obtain data from attached and integrated sensors on Digi products that have embedded XBee RF modules. See the Digi Python wiki for more information.

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

Python support forum on www.digi.com

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

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

Device Integration Application (DIA)

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

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

Written in the Python programming language for use on Digi devices, you can also execute DIA on a computer for prototyping purposes when a suitable Python interpreter is installed.

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

Remote Manager and the device management service

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

- Device connector software that simplifies remote device connectivity and integration.
- Management application (configure, upgrade, monitor, alarm, analyze) for Digi connectivity products including ZigBee nodes.

- Application messaging engine with broadcast and receipt notification for application-to device interaction.
- Cache and permanent storage options for generation-based storage and ad hoc access to historical device samples.
- Application-focused bundles with ready-to-use illustrative applications

You can monitor and manage Digi devices from Remote Manager. For example:

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

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

RealPort configuration

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

Install RealPort software

To install RealPort software from the Digi Support site:

1. Go to your product's support page:
   - Digi ConnectPort X2
   - Digi ConnectPort X4
2. Under Product Support, click the **Drivers** tab.
3. Select the operating system for your computer from the **Operating System Specific Drivers** list.
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.
- **Device Initiated RealPort Settings**:
  - **Index**: An empty list means there are no configured device-initiated RealPort connections.
  - **Host or IP Address**: The IP address or DNS name of the client to connect to.
  - **Port**: The network port to connect to on the client. The default port for VNC servers is 8771.
  - **Retry Time**: The amount of time in seconds to wait before reattempting a failed connection to the client.

Industrial Automation-Modbus-Bridge

Industrial Automation is supported in these Digi devices: Digi Connect WAN IA and Digi Connect WAN 3G IA.

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

For more information on Industrial Automation, see the **set ia** command description in the *Digi Connect® Family Command Reference* and the application note *Remote Cellular TCP/IP Access to Modbus Ethernet and Serial Devices* available on the Digi Support site.

Known limitations

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

Enable or disable Modbus Bridge

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

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

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

Configuration through Digi Remote Manager

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

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

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

Manage Remote Manager through SMS commands

You can configure Digi devices managed by Remote Manager through Short Message Service (SMS) commands. See Users.

Batch configuration capabilities

If you need configure multiple Digi devices, use the batch configuration capabilities to upload configuration files through the Digi Connect Programmer utility. The Digi Connect Programmer utility is a command-line-based interface to Digi devices. Use this utility to upload firmware, files, configuration settings and factory defaults to a Digi device. You can run it from the command line on a computer that uses the Microsoft Windows operating system.

Management

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

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

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

Web interface

The web interface has several screens for monitoring Digi Connect WAN Family devices:

- Network status
- Mobile connection status

- Serial Port Management: for each port, the port's description, current profile, port logs (if activated), and current serial configuration.
- Connections Management: A display of all active system connections.
- System Information:
  - General device information.
  - Serial port information: for each port, including the port's description, current profile, and current serial configuration. The same information appears when you choose Serial Port Management.
  - Network statistics: statistics for IP, TCP, UDP, and ICMP.

Manage connections and services

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

Serial Port Management

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

Port Connections Management

The Port Connections Management page (**Management** > **Serial Ports** > **Connections**) displays active Virtual Private Network (VPN) and system connections.

Manage Virtual Private Network (VPN) connections

To monitor a VPN connection from the web interface, select **Management** > **Connections**. The VPN settings appear.

Note that the **Connect** and **Disconnect** functions do not work if VPN the uses a Pre-Shared Key (PSK).

Manage active system connections

The **Active System Connections** list provides an overview of connections associated with various interfaces, such as:

- User connections to the device's web interface
- Connections to the command line through the local shell
- Python threads currently running
- Protocols used for the connections
- The number of active sessions for each connection

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

Event logging

Management > **Event Logging** displays the event log for the Digi device. This log records events throughout the Digi device's system, such as starting or resetting the Digi device, configuring features,

actions performed by various interfaces and subsystems, or starting applications. The event log is always enabled and is not user-configurable. When the Digi device operates in an unexpected manner, you can send the log entries to Digi for analysis by Technical Support and Engineers. You cannot disable the event log. Digi uses the event log to get an accurate view of all operational aspects of the device.

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

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

Manage network services

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

Manage DHCP server operation

DHCP server management operations include:

- View DHCP server status.
- Start/stop/restart the DHCP server.
- View and manage current DHCP leases.

Start, stop, and restart the DHCP server

The DHCP Server Management page shows the current status of the DHCP server. Depending on the current status, there are buttons to start, stop, or restart the DHCP server. Click the appropriate button to perform your request.

Note Stopping, restarting, or rebooting the DHCP server causes all information on IP address leases to be lost. All leased addresses except for reservations will be returned to the available address pool and may be served in a new lease to a DHCP client.

View and manage the current DHCP leases

The DHCP server maintains a current list of its leases, reservations and unavailable addresses. The displayed lease list may contain entries that report a variety of status descriptions. The Lease Status types are identified and described below.

Even after a lease has expired or is released by a DHCP client, the associated IP address is not immediately returned to the available address pool. Rather, there is a non-configurable **grace period** during which the lease record is retained by the DHCP server. At the end of that grace period, the lease record is automatically deleted and the associated IP address is returned to the available address pool. Where a grace period is observed, this is indicated in the Lease Status descriptions below.

The grace period is incorporated in the DHCP server to increase the consistency of offering the same IP address to a DHCP client, even if that client is rebooted or off the network for a period of time that does not exceed the grace period.

You can move leases from the DHCP server while the server is running. To remove a lease, select the check box to the left of the lease information in the table of leases, then click the **Remove** button below the lease table. To remove all leases, select the check box to the left of the descriptive headings at the top of the table, then click the **Remove** button below the lease table.

Note Removing a lease will cause the associated IP address to be returned immediately to the available address pool. Any IP address in this available address pool may be served in a new lease to a DHCP client. Static lease reservations will always display in the lease list. These reservation leases may be removed, but a new lease will be created immediately. To disable or permanently remove a reservation, use the DHCP Server Settings page in the Network Configuration area.

Lease status types

Here are the Lease Status values that are displayed in the lease list, including how long a lease table entry will remain in each state. Note that after a lease is deleted, the associated IP address is returned to the available address pool.

- **Assigned (active)**: A lease is currently assigned and active for the given client. The client may renew the lease, in which case the lease remains in this state.
- **Assigned (expired)**: A lease has expired and is no longer active for the given client. A lease in this state will remain for a 4-hour grace period, after which it is deleted. If the same client requests an IP address before the lease is deleted, it will be given the same IP address previously served to it.
- **Reserved (active)**: A lease for an address reservation is currently active for the given client. A reservation lease will remain indefinitely, although the status may alternate between active and inactive.
- **Reserved (inactive)**: A lease for an address reservation is currently inactive for the given client. A reservation lease will remain indefinitely, although the status may alternate between active and inactive.
- **Reserved (unavail)**: A lease for an address reservation was offered to a client, but that client actively declined to use the IP address. Typically this is because the client determined that another host on the same subnetwork is already using that IP address. Upon receiving the client's decline message, the DHCP server will mark the address as unavailable. The lease will remain in this state for 4 hours, after which it is reverts to the Reserved (inactive) status.
- **Offered (pre-lease)**: A lease has been offered to the given client, but that client has not yet requested that the lease be acknowledged. It may be that the client also received an offer from another DHCP server, in which case this offer will expire in approximately 2 minutes. If the client requests this lease before that 2-minute interval elapses, this lease will change status to Assigned. If the 2-minute interval expires, the offer record is deleted and the associated IP address is returned immediately to the available address pool.
- **Released**: A lease was previously assigned to the given client, but that client has proactively released it. A lease in this state will remain for a 1-hour grace period, after which it is deleted. If the same client requests an IP address before the lease is deleted, it will be given the same IP address previously served to it.

- **Unavailable Address**: A lease was offered to a client, but that client actively declined to use the IP address. Typically this is because the client determined that another host on the same subnetwork is already using that IP address. Upon receiving the client's decline message, the DHCP server will mark the address as unavailable. The lease will remain in this state for a 4-hour grace period, after which it is deleted. This status may also occur if the DHCP server determines that the IP address is in use before it offers the address to a client (see the DHCP server setting **Check that an IP address is not in use before offering it**).

Administration

You can periodically perform administration tasks on Digi Connect WAN Family products, such as:

- File management
- Changing the password used for logging onto the device
- Backing up and restoring device configurations
- Updating firmware and Boot/POST code
- Restoring the device configuration to factory defaults
- Rebooting the device

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

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

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

- **File Management**: Upload and manage files, such as custom web pages, applet files, and initialization files. See File Management for more information.
- **Python Program File Management**: Upload custom programs in the Python programming language to Digi devices and configuring the programs to execute automatically at startup. See Python Configuration for more information.
- **Backup/Restore**: Back up or restore device configuration settings. See Backup/Restore for more information.
- **Update Firmware:** Update the firmware, including Boot and POST code. See Update the firmware and boot/POST code for more information.
- **Factory Default Settings**: Restore a device to factory default settings. See Factory Default Settings for more information.
- **System Information**: Display general system information for the device and device statistics. See System Information for more information.
- **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 Digi Connect WAN Family device. See Users for more information.

File Management

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

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

Upload files

To upload files to a device:

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

Delete files

To delete files from a device:

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

Factory reset does not delete custom files

A factory reset does not delete files uploaded to the File Management page. When you restore the Digi device to factory defaults or press the **Reset** button on the device (see Factory Default Settings), the uploaded files remain. This allows you to retain custom applets and custom factory defaults. If you want to remove custom files you must manually delete them (see Delete files).

X.509 Certificate/Key Management

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

Supported security implementations

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

- **X.509 Certificate Authority/Certificate Revocation**—A trusted third party issues digital certificates for use by other parties.

- **Simple Certificate Enrollment Protocol (SCEP)**—Use SCEP to obtain certificates used in Virtual Private Networking (VPN) security. Large enterprises use SCEP. SCEP allows for provisioning from the field.
- **VPN**—Use the IPsec protocol in VPN to securely connect a device to a network, connect two networks together, and allow a device to perform proxy VPN.
- **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**—Use SSL and TLS security to secure access to web pages for configuration purposes, secure serial port connections, and SSL autoconnect, an automatic connection (autoconnection) between a serial port on the device and a remote network destination.
- **Secure Shell (SSHv2)**—Use SSHv2 to secure access to a device's console and serial ports for configuration purposes.

Benefits of certificates

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

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

Additional information on certificate management

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

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

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

Security type	Table	Used to load
X.509 Certificate Authority/Certificate Revocation	CA (Certificate Authority)	Certificate authority digital certificates. A certificate authority (CA) is a trusted third party that issues digital certificates for use by other parties. Digital certificates issued by the CA contain a public key. The certificate contains information about the individual or organization to which the public key belongs. A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates, and the information contained therein, issued by that CA.
	CRL (Certificate Revocation List)	Certificate revocation lists for loaded CAs. A certificate revocation list (CRL) is a file that contains the serial numbers of digital certificates issued by a CA which have been revoked, and should no longer be trusted. Like CAs, CRLs are a vital part of a public key infrastructure (PKI). You must install the digital certificate of the corresponding CA before you load the CRL.
Simple Certificate Enrollment Protocol (SCEP)	SCEP CA (Certificate Authority)	SCEP certificate authority digital certificates that have been approved and issued. Tables are populated using SCEP commands and data is obtained from a SCEP server, rather than populated by a user.
	SCEP Pending Enrollment Requests	SCEP certificate requests that are pending approval.
Virtual Private Networking (VPN)	VPN Identity	VPN identity certificates. Identity certificates and keys allow for IPsec authentication and secure key exchange with ISAKMP/IKE using RSA or DSA signatures. The VPN identity certificate must be issued by a CA trusted by the peer.
	VPN Identity Keys	VPN RSA or DSA identity private keys.
Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	SSL Identity	SSL/TLS identity certificates. A default key is generated automatically but can be overridden by a user. Note that this default key is not secure.
	SSL Identity Keys	SSL/TLS identity private keys.
	SSL Peer	SSL/TLS peer certificates.
	SSL Revoked	Verbatim revoked SSL/TLS certificates.

Security type	Table	Used to load
Secure Shell (SSHv2)	SSH Host Keys Table	SSHv2 identity private keys. Used for authentication with SSHv2 clients and secure key exchange. A default 1024-bit DSA key is generated automatically if none exists when the device boots. There is no certificate for SSHv2, just private key data.

Behavior of SSH/SSL private keys on Digi device

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

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

Using TFTP to load and store certificate information

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

Using HTTP/HTTPS to transfer certificate and key data

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

Data retained after factory reset

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

Certificate management settings

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

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

Upload CAs and CRLs

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

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

About Simple Certificate Enrollment Protocol (SCEP) CA certificates

Managing Simple Certificate Enrollment Protocol (SCEP) CA certificates involves two types of certificates and settings on several pages:

- The *SCEP CA certificate*. This is the globally trusted certificate.
- The *VPN identity certificate*; that is, the certificate that identifies the particular device.

The process for managing these two types of certificates is as follows:

Step	Location in X.509 Certificate and Key Management settings
1. Get the SCEP CA certificate.	**Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs) > Obtain CA certificates from a SCEP Server** fields and **Get CA** button See Obtain CA certificates from a SCEP Server.
2. Accept the SCEP CA certificates.	Certificate Authorities (CAs) / Certificate Revocation Lists (CRLs) > Installed SCEP Certificate Authority Certificates See Installed Certificate Authority Certificates.
3. Enroll the VPN identity certificate.	Virtual Private Network (VPN) Identities > Key Generation / Enrollment fields and Enroll button This step moves the VPN identity certificate into the pending enrollment database, which is the database that indicates which certificate enrollment requests are outstanding. See Key generation / enrollment.
4. Verify enrollment of the VPN identity certificate.	Virtual Private Network (VPN) Identities > Installed VPN Identity Certificates The VPN identity certificate is automatically added when it comes back from the SCEP server. Verify that it is in the table. See Installed VPN identity certificates.

Installed Certificate Authority Certificates

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

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

Installed Certificate Authority Certificate Revocation Lists

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

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Issuer**: The entity that issued the certificate.
- **Last Update**: The last date and time the certificate revocation list was issued.
- **Next Update**: The effective or expiration date and time of the certificate revocation list. At this date, a new one must be obtained.
- **Delete** button: Click to delete the CA certificate revocation lists selected in the **Action** column from the database.

Obtain CA certificates from a SCEP Server

This section performs step 1 of the process for managing SCEP CA certificates. It involves specifying the SCEP server where you can obtain CA certificates.

Note You must accept CA Certificates before you can use it for any purpose.

- **SCEP Server URL**: The URL of the SCEP server from which to get the CA certificate.
- **CA Identifier**: The ID of the CA certificate to be obtained from the SCEP server. Get this value from the SCEP administrator.
- **Get CA button**: Click to get the specified CA certificate from the specified SCEP server URL.

Installed SCEP Certificate Authority Certificates

This section performs step 2 of the process for managing SCEP CA certificates. It lists any installed Simple Certificate Enrollment Protocol (SCEP) CA certificates. To enter any new certificates, obtain the certificate information from the SCEP administrator. Click the **Accept** button to accept SCEP CA certificates in the list.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **Subject**: A text description of the SCEP CA.
- **Issuer**: The entity that issued the certificate.
- **Expiration**: The expiration date of the certificate.
- **Fingerprint**: The fingerprint of the received CA certificate. This fingerprint is in the form of a hash code consisting of several hexadecimal bytes that allow the SCEP administrator to verify the CA certificate.
- **Delete** button: Deletes all the SCEP CA certificates selected in the **Action** column from the database.
- **Accept** button: Accepts the SCEP CA certificates selected in the **Action** column into the database. This action moves the CA certificate from the SCEP CA to the X.509 CA table.

Virtual Private Network (VPN) identities

Upload VPN identity keys and certificates

Use this section to upload VPN RSA or DSA identity keys and certificates. You can install up to 5 VPN identity certificates. You can install up to 5 VPN identity keys.

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

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

Installed VPN identity certificates

This table lists any VPN identity certificates that are loaded in the VPN Identities database.

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

Installed VPN identity keys

Lists any VPN identity keys that are in the VPN Identities database.

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

Key generation / enrollment

Use this section to set parameters for handling SCEP enrollment requests. A SCEP enrollment request creates a private key and sends a request to the SCEP server to generate a SCEP CA certificate. You can install up to 4 pending SCEP enrollment requests.

Enrollment request parameters are as follows:

- **SCEP Enrollment Server URL**: The URL for the SCEP server.
- **CA Certificate**: The name of the CA certificate to be obtained from the SCEP server.
- **Encryption Certificate**

  Signing Certificate: There are roles in a certificate enrollment request: The CA that signs the enrollment request, and the CA that encrypts the request. These two options are indices into the CAs in the Digi device's certificate database, and both sign and encrypt the request. This information is typically downloaded from the SCEP CA table.
- **RSA Key Length (bits)**: The number of characters in the key.

- **Enrollment Password:** A one-time, short-lived password used for the SCEP enrollment process. Get this password from the SCEP administrator.
- **Common Name (CN)**: A name that identifies the device associated with the SCEP CA certificate; for example, the device name or a FQDN.
- **Country Code (C)**: A two-letter abbreviation for the country in which the device associated with the SCEP CA certificate resides; for example, US for United States.
- **State or Province (ST)**: The state or province abbreviation for the physical location of the device associated with the SCEP CA certificate.
- **Locality (L)**: The city or town for the physical location of the device associated with the SCEP CA certificate.
- **Organization (O)**: Company or organizational name for the device associated with the SCEP CA certificate.
- **Organizational Unit (OU)**: Organizational sub-descriptor for the device associated with the SCEP CA certificate; for example “Engineering” or “IT.”
- **E-mail (SubjectAltName)**: Email address for the device associated with the SCEP CA certificate.
- **FQDN (SubjectAltName)**: Fully Qualified Domain Name (FQDN) for the device associated with the SCEP CA certificate.
- **Enroll** button: Sends the enrollment request to the SCEP server.

Pending SCEP Enrollment Requests

This table lists SCEP enrollment requests that are pending approval. These are requests that have saved at the SCEP server console but not yet approved. If the SCEP administrator does not approve these requests, they will remain in this pending state forever until deleted.

- **Action**: Select to perform allowable actions on the entry. The only allowable action is to delete the entry.
- **URL**: This value must be the same as the **SCEP Enrollment Server URL** in the SCEP enrollment request.
- **Issuer**: The entity that issued the certificate.
- **Delete** button: Deletes all SCEP enrollment requests selected in the **Action** column from the database.

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

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

Identity certificates and keys

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

Upload SSL/TLS Identity Keys and Certificates

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

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

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

Installed SSL and TLS Identity Certificates

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

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

Installed SSL/TLS identity keys

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

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

Trusted peer certificate

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

Upload SSL/TLS trusted peer certificates

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

Installed SSL/TLS trusted peer certificates

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

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

Untrusted revoked certificate

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

Upload SSL/TLS untrusted revoked certificates

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

Installed SSL/TLS untrusted revoked certificates

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

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

Secure Shell (SSH) Host Keys

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

Upload SSH Host Keys

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

Installed SSH host keys

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

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

Secure Shell (SSH) hostkeys

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

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

required.

- **Installed SSH Host Keys**: Lists the host keys loaded into the SSH Hostkeys database.

Backup/Restore

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

Back up or restore a device configuration from the web interface

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

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

To backup a device configuration:

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

To restore a device configuration:

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

Update the firmware and boot/POST code

You can update the firmware and/or boot/POST code for a Digi device from a file on a computer or through TFTP. The recommended method is to download the firmware to a local hard drive. TFTP is supported for those using Unix systems. Both the firmware and the boot/POST code are updated using the same set of steps. The Digi device automatically determines the type of image to upload.

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

Update the firmware from a file on a computer

To update the firmware from a file on a computer:

1. Select **Administration** > **Update Firmware**. The Update Firmware page appears.
2. Type the name of the firmware or POST file in the **Select Firmware** field, or click **Browse** to locate and select the firmware or POST file.

3. Click **Update**.

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

Update the firmware from a TFTP Server

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

Factory Default Settings

Restoring a Digi Connect WAN Family 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 Digi Connect WAN Family product to the factory default settings:

- From the web interface using the Restore Factory Defaults operation

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

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

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

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

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

- Using the reset button on the Digi Connect WAN Family device

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

Settings cleared and retained during a factory reset

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

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

Reset the factory settings on a Digi Connect WAN Family product from the web interface

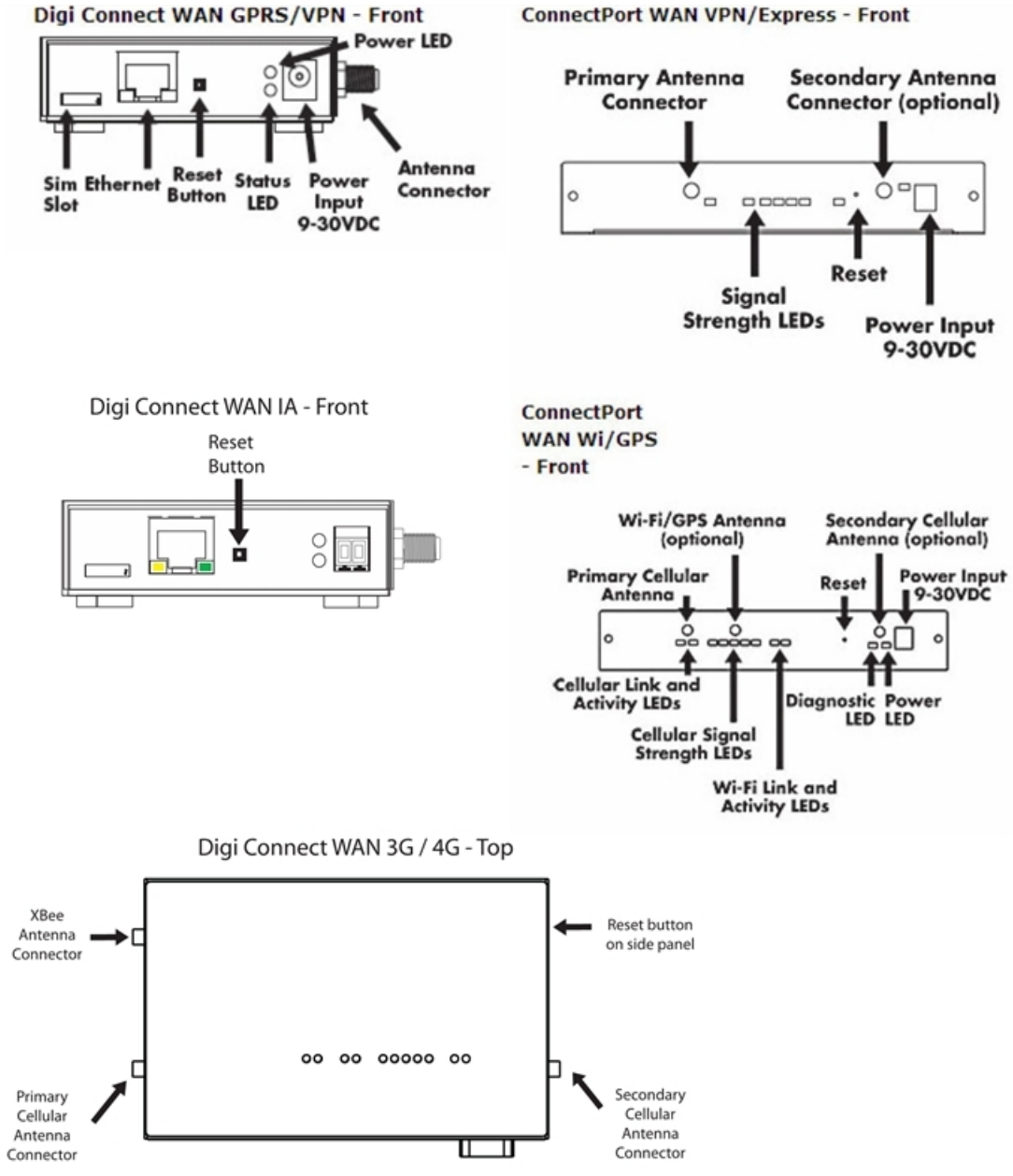
To reset the factory settings on the Digi Connect WAN Family device from the web interface:

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

Reset the factory settings on a Digi Connect WAN Family *product using the Reset button*

To reset the factory settings on a Digi Connect WAN Family product using the Reset button:

1. Power off the Digi Connect WAN Family.
2. Locate the Reset button or pin on your Digi device.



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

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

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

System Information

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

General

The General page displays the following general system information:

- **Model**: The model of the Digi Connect WAN Family product.
- **MAC Address**: A unique network identifier required for all network devices. The MAC address appears on a sticker on the Digi device and consists of 12 hexadecimal digits, usually starting with 00:40:9D.
- **Firmware Version**: The current firmware version running in the Digi device. Use this information to locate and download new firmware. You can download firmware updates from the Digi Support site.
- **Boot Version**: The current boot code version running in the Digi device.
- **POST Version**: The current Power-On Self Test (POST) code version running in the Digi device.
- **CPU Utilization**: The amount of CPU resources the Digi device uses.

  Important: 100% CPU utilization may indicate encryption key generation is in-progress. On initial boot, the Digi device generates some encryption key material: an RSA key for SSL/TLS operations, and a DSA key for SSH operations. This key-generation process can take as long as 40 minutes. Until the RSA or DSA key is generated, the Digi device will be unable to initiate or accept that type of encrypted connection. The Digi device reports itself as 100% busy, but since key generation occurs at a low priority, the device will still function normally. On subsequent reboots, the Digi device will use its existing keys and not need to generate another unless a reset to factory defaults is done, which will cause a new key to be generated on the next reboot.

- **Up Time**: The amount of time the Digi device has been running since it was last powered on or rebooted.
- **Total/Used/Free Memory**: The amount of memory (RAM) available, currently in use, and currently not being used.

Serial

The **Serial** page under **Administration** > **System Information** lists the configured serial ports for the Digi Connect WAN Family products. Click a port to view detailed serial port information on the **Serial Port Diagnostics** page.

Serial Port Diagnostics

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

- **Configuration**: The Configuration page displays the electrical interface (Port Type) and basic serial settings.
- **Signals**: The Signals pane shows the state of serial port signals. The serial port signals are green when asserted (on) and gray when not asserted (off). These signals are defined as follows:
  - **RTS**: Request To Send.
  - **CTS**: Clear To Send.
  - **DTR**: Data Terminal Ready.
  - **DSR**: Data Set Ready.
  - **DCD**: Data Carrier Detected.
  - **OFC**: Output Flow Control. Indicates that flow control is enabled on the remote side of the serial-port connection, and that the Digi device should stop sending data.
  - **IFC**: Input Flow Control. Indicates that the Digi device is operating as if flow control is enabled for incoming data sent from the remote side of the serial-port connection. This signal is more of an indication that flow control is intended or expected rather than true state information. If the remote side has a flow-control mechanism enabled, the Digi device will use it.
- **Serial Statistics**: The Statistics section includes data counters and error tracking that will help determine the quality of data that is being sent or received. If the error counters are accumulating, you may have a problem with your Digi device server.
  - **Total Data In**: Total number of data bytes received.
  - **Total Data Out**: Total number of data bytes transmitted.
  - **Overrun Errors**: Number of overrun errors—the next data character arrived before the hardware could move the previous character.
  - **Framing Errors**: Number of framing errors received—the received data did not have a valid stop bit.
  - **Parity Errors**: Number of parity errors—the received data did not have the correct parity setting.
  - **Breaks**: Number of break signals received.

Network statistics

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

Ethernet Connection Statistics

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

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

IP statistics

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

TCP Statistics

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

UDP Statistics

- **Datagrams Received/Datagrams Sent**: Number of datagrams received or sent.
- **Bad Datagrams Received**: Number of bad datagrams received. This number does not include the value contained by **No Ports**.

- **No Ports**: Number of received datagrams that were discarded because the specified port was invalid.

ICMP Statistics

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

Wi-Fi LAN Statistics

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

Mobile Information and Statistics

The Mobile Information and Statistics Page displays detailed mobile statistics that may aid in troubleshooting network communication problems with your mobile network. The statistics displayed depend on whether your mobile service provider is GSM- or CDMA-based.

SIM Information

- **Slot**: The number of the socket containing the SIM card.
- **IMSI**:The International Mobile Subscriber Identity (IMSI) number that uniquely identifies the SIM card.
- **Phone Number**: The phone number associated with the mobile account, if available.

- **Status**: The configuration status of the SIM. It may be one of these values:
  - **Not configured**: A mobile service provider has not been configured. Select a provider on the Mobile Configuration page.
  - **Disabled**: The SIM will not be used to establish a mobile connection. To enable, click **Apply** on the Mobile Configuration page.
  - **Not installed**: The SIM card is not plugged into the Digi device server.
  - **Primary**: This is the preferred SIM to use to establish mobile connections.
  - **Secondary**: If a mobile connection cannot establish connection with the primary SIM, the mobile connection will establish a connection with the secondary SIM.
- **PIN Status**: The status of the PIN code that may be needed to use the SIM. It may be one of these values:
  - **Ready**: The PIN is correct, or no PIN is required.
  - **Waiting for PIN**: A PIN is required, but has not been configured. Type a PIN on the Mobile Configuration page.
  - **PIN incorrect**: The PIN is not correct. It will not be tried again to prevent locking the SIM. Type a new PIN on the Mobile Configuration page.
  - **Waiting for PUK**
    Waiting for PIN2
    Waiting for PUK2: An unlock code is required. This SIM must be unlocked before you can use it in the Digi device server.
- **Active**: The SIM used to establish a mobile connection.

Mobile Connection Statistics

- **Registration Status**: The status of the modem's connection to the cellular network:
  - **Not Registered**: Digi device is not currently searching a new operator to register to.
  - **Registered**: Home network.
  - **Not Registered**: Digi device is currently searching a new operator to register to.
  - **Registration Denied**.
  - **Unknown**.
  - **Registered - Roaming**.
- **Location Area Code (aka "LAC")**: The modem reports this value as a 4-hex-digit string. In the mobile statistics it appears both as hex and decimal representations. For example "00C3 (195)."
- **Cell ID**: The modem's identifier in hexadecimal and decimal, for example: "00C3 (195)."

- **Signal Strength (RSSI)**: The relative signal strength, displayed as signal strength LEDs.
  - **0 LEDs**: Unacceptable; Signal strength is not known or not detectable.
  - **1 LED**: Weak.
  - **2 LEDs**: Moderate.
  - **3 LEDs**: Good.
  - **4: LEDs**: Excellent.

Mobile Statistics

Mobile statistics include the interface status, bytes received and sent, baud rate, modem resets, and inactivity timer.

- **IP Address**: The IP address of the PPP connection provided by the mobile service.
- **Primary DNS Address/Secondary DNS Address**: The IP addresses of the DNS nameservers. The nameserver specified on “dns1” performs the name lookups first, and if that fails, the nameserver specified on “dns2” performs the name lookups.
- **Data Received**: Total number of data bytes received.
- **Data Sent**: Total number of data bytes sent.
- **Idle Resets**: The number of times the modem has been reset because no data was received for a period of time.
- **Inactivity Timer**: The time, in seconds, after which if no data has received over the link, the mobile connection will be disconnected and re-established.

Mobile Information

The Mobile Information section items are specific to a cellular modem or service provider account. These vary in the information reported from modem to modem and also differ between CDMA and GSM services. You will find this information useful when troubleshooting an issue and contacting technical support. Some of the common information items include (but are not limited to):

- **Mobile Version**: Version number of the cellular modem.
- **IMSI**: International Mobile Subscriber Identifier (IMSI), a unique 15-digit number which designates the subscriber. This ID is the subscriber's code to access the cellular network. The network uses this code for provisioning and to admit the device/user to its provisioned services.
- **Phone Number**: The phone number used to call the modem module. Two numbers are displayed: the Mobile Directory Number (MDN) and the Mobile Identification Number (MIN).
- **Modem Manufacturer**: The manufacturer of the modem module.
- **Model**: The model name of the modem module.
- **Modem Serial Number**: The serial number of the modem module.
- **Modem Revision**: The firmware revision in the modem module.
- **Other Mobile Information**: Depending on your mobile service provider, other mobile information and settings may be provided after the modem revision.

IP Network Failover statistics

The **IP Network Failover** page displays detailed IP Network Failover status and statistics that may aid in troubleshooting network communication problems. The IP Network Failover feature provides a dynamic method for selecting the default gateway. If IP Network Failover is properly configured and enabled, it overrides the **Gateway Priority** setting in the **Advanced Network Settings**. If failover is off/disabled, the non-failover gateway configuration is enabled. To configure IP Network Failover, use the **Network** > **IP Network Failover** page; see IP Network Failover settings. To configure the non-failover default gateway priority list, use the **Configuration** > **Network** > **Advanced Network Settings** page; see Advanced Network Settings.

Field	Description
Current Default Gateway Status	The current status of the default gateway, including the interface name, default gateway IP address, and how the default gateway was configured (Failover or Non-Failover).

Field	Description
Current Network Failover Status	The current status of the Network Failover feature's management of the default gateway. **Failover State**: The current configured state of IP Network Failover (On or Off). **Fallback to Non-Failover**: The current configured state of the IP Network Failover option to fall back to Non-Failover (On or Off). When an IP Network Failover cannot configure a default gateway, it uses the fallback option. Failure to configure a default gateway could occur if one or more interfaces are not enabled (On) for IP Network Failover use, or if those enabled interfaces are not Up or do not have a gateway associated with them. **Interface Table**: The current status of all available IP network interfaces. The table is displayed in order of the interface priority configured in the IP Network Failover settings. For each network interface, the following information is displayed: **Priority:** The interface priority that Network Failover uses. The highest priority is 1, which is the first interface in the configured Failover Interface Priority list. **Interface:** The name of the network interface. **Status:** The current failover status of this network interface. Status values include: ■ **1 - Responding:** The interface is up and configured in the system. It is currently responding to the link tests. This interface is suitable for use as the default gateway. ■ **2 - Up:** The interface is up and configured in the system. Its status has not been determined by the link tests, or no link tests are configured. This interface may be suitable for use as the default gateway. ■ **3 - Not Responding:** The interface is up and configured in the system. However, it is not currently responding to the link tests, and the number of consecutive test failures has reached the threshold number configured in the **IP Network Failover** settings. This interface may be suitable for use as the default gateway. ■ **4 - Down:** The interface is down or not configured in the system. However, it is not currently responding to the link tests. This interface is not suitable for use as the default gateway. ■ **5 - Unknown:** The interface is unknown (does not exist) in the system. This interface is not suitable for use as the default gateway.

Field	Description
	The number displayed for each status value indicates the priority of that status. Failover uses this value to select the interface for the default gateway. Status priority 1 is the most suitable for use, with lower priorities considered suitable if there are no interfaces at the highest priority. The interface list is maintained in the interface priority order configured in the Network Failover settings. When any interface changes status, the interface list is examined for the interface that has the highest status priority, nearest the start of the list. The highest priority interface with a Responding status becomes the default gateway. If there is no interface marked as Responding then the highest Up interface becomes the default gateway. **Gateway**: The gateway IP address associated with the interface, or 0.0.0.0 if the interface does not have an associated gateway. An interface with no gateway is not suitable for use as the default gateway. **State**: The Network Failover enabled state (On or Off) for this interface. The On state means failover is monitoring this interface, and the Off state means failover is not using this interface for failover purposes. **Tests**: The number of Link Tests (0, 1 or 2) that are configured for this interface.

Field	Description
Current Network Gateway Status (Non-Failover)	This information reports the status of the non-failover management of the default gateway. If Network Failover is enabled (On) and can successfully configure a default gateway, failover always overrides the non-failover Gateway Priority configuration. **Interface Table**: The current status of all available IP network interfaces. The table is displayed in order of the interface priority configured in the Advanced Network Settings. For each network interface, the following information is displayed: **Priority**: The priority of the interface configured in the Advanced Network Settings. The highest priority is 1, which is the first interface in the configured Advanced Network Settings Interface Priority list. **Interface**: The name of the network interface. **Status**: The current status of this network interface. Possible status values and their meanings: ■ **1 - Up**: The interface is up and configured in the system. This interface is suitable for use as the default gateway. ■ **0 - Down**: The interface is down or not configured in the system. This interface is not suitable for use as the default gateway. The Interface Priority order configured in the Advanced Network Settings maintains the interface list. When any interface changes status, the interface list is examined for the interface that has the highest status priority, nearest the start of the list. The highest priority interface with an Up status becomes the default gateway. **Gateway**: The gateway IP address associated with the interface, or 0.0.0.0 if the interface does not have an associated gateway. An interface with no gateway is not suitable for use as the default gateway.

Field	Description
Current Failover Link Test Statistics	These statistics indicate the successes and failures of the configured link tests. The Network Failover feature uses these statistics to manage the default gateway. For each network interface, the following counters are maintained and reported. The values indicate the total number for each interface and category, since the Digi device was last powered on or rebooted. **Test Success**: The total number of successful link tests. A link test is successful if either of the configured tests (primary or secondary destination) succeeds. When a link test succeeds, the interface is reported as “Responding”. **Test Failure**: The total number of failed link tests. A link test fails if both of the configured tests (primary or secondary destination) fail, or if only one link test is configured and it fails. If two link tests are configured, and both of them fail, that is counted as a single link test failure for the purpose of counting failures. **Bypass Test**: The total number of bypassed link tests that did not run for a number of possible reasons. A link test is bypassed if no destinations are configured, if the interface has no associated gateway, if the interface goes down while a test is in progress, or if failover is disabled (turned off) while a test is running (disabled as a feature or for the interface being tested). **Consecutive Failures**: The current number of consecutive link test failures for the interface. When the number of consecutive failures reaches the threshold configured in the Network Failover settings, the interface is reported as “Not Responding” and the default gateway may be changed as a result. When a link test is successful, or when the interface goes down and comes back up, the consecutive failures counter is reset to zero. **Link Not Responding**: The total number of link test failures that occurred for the interface after it has been reported as “Not Responding”. This counter allows you to determine how much time an interface is in the “Not Responding” state.

Remote Manager status

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

Position/GPS statistics

The Position statistics show information gathered from attached NMEA-0183 compliant GPS receivers attached to the Digi device, and statically configured position parameters.

Watchport Sensor statistics

To be provided.

SureLink statistics

Digi SureLink provides an “always-on” mobile network connection to ensure that a Digi device is in a state where it can connect to the network. The statistics displayed for Digi SureLink pertain to the periodic tests, known as Link Integrity Monitoring tests, that run over the established PPP connection to ensure that end-to-end communication is possible. There are three Link Integrity Monitoring tests

available: Ping Test, TCP Connection Test, and DNS Lookup Test. For descriptions of these tests, see Link integrity monitoring settings. In these SureLink statistics, a “session” is a PPP session. The session statistics are reset to zero at the start of a new PPP connection. The “total” statistics are the accumulated totals for all sessions since the device booted. The “tests” are the SureLink Link Integrity Monitoring tests that you configured to be run when establishing the mobile network connection.

- **Session Successes**: The number of times a configured test ran and succeeded in the current PPP session.
- **Session Failures**: The number of times a configured test ran and failed in the current PPP session.
- **Session Consecutive Failures**: The number of consecutive failures for a test, with no success. When a test is successful, the consecutive failures counter resets to zero. The consecutive failures counter indicates a device's “progress” toward the configured maximum number of consecutive failures, after which the PPP link goes down (and restarts).
- **Session Bypasses**: SureLink testing bypasses a test when a configuration parameter is bad. This means the test was not run. If the PPP connection goes down while a test is in progress, the SureLink testing classifies the test as bypassed, since it could not be run. (Note that the PPP link may go down for many reasons, independent of SureLink testing.)
- **Total Successes**: The total number of times a configured test ran and succeeded since you started the Digi device.
- **Total Failures**: The total number of times a configured test ran and failed since your started the Digi device.
- **Total Link Down Requests**: The number of times the SureLink feature failed consecutively, the configured number of failures and, as a result, requested that PPP shut down and restart its connection. This statistic counts such occurrences during the current device boot. SureLink itself does do the PPP stop/start; it sends a message to PPP asking it to do so, owing to a SureLink test failure.
- **Total Bypasses**: The total number of test bypasses (see “session bypasses”) since you started the Digi device.

Diagnostics

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

Reboot

Changes to some device settings require saving the changes and rebooting the Digi Connect WAN Family. Use the Reboot page to reboot the Digi Connect WAN Family. To reboot a Digi Connect WAN Family from the web interface:

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

Enable/disable access to network services

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

Digi Connect WAN Family command-line interface

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

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

Configuration through the command line

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

Access the command-line interface

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

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

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

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

```
#> telnet 192.3.23.5
```

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

Basics for using the command-line interface

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

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

Management through the command line interface

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

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

Use the following commands to display information and statistics:

- display
- info
- set alarm
- set buffer and display buffer

- set snmp
- show

Use the following commands to manage connections and sessions:

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

Use the following commands to configure the product:

- backup print
- display mobile (cellular)
- display provisioning
- display wimax
- newpass
- send mode
- set accesscontrol
- set alarm
- set autoconnect
- set buffer and display buffer
- set forward
- set host
- set ia
- set mgmtconnection
- set mgmtglobal
- set mgmtnetwork
- set mobile
- set nat
- set network
- set pmodem

- set pppoutbound
- set profiles
- set realport
- set rtstoggle
- set serial
- set service
- set snmp
- set system
- set tcpserial
- set udpserial
- set user
- set wimax

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.

dhcp

The **dhcp** command manages DHCP server operation.

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 logging/**).
- Memory usage information (**display memory**).
- Serial modem signals (**display serial**).
- Mobile connection information and statistics (**display mobile**).
- Network Address Translation (NAT) information (**display nat**).
- General status of the sockets resource (**display sockets**).

- Active TCP sessions and active TCP listeners (**display tcp**).
- Current UDP listeners (**display udp**).
- Provisioning information currently in the Digi device device's CDMA module (**display provisioning**).
- Uptime information (**display uptime**).
- Virtual Private Network (VPN) connection information (**display vpn**).

display mobile (cellular)

Use the **display mobile** command to display mobile (cellular) statistics.

display provisioning

Use the **display provisioning** command to provision CDMA cellular modules.

display wimax

Use the **display wimax** command to display Wi-MAX information and statistics.

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, boot, POST, and firmware versions, memory usage, utilization, and uptime.
- Ethernet statistics. The **info ethernet** command displays statistics regarding the Ethernet interface, including:
  - The number of bytes and packets sent and received
  - The number of incoming and outgoing bytes that were discarded or that contained errors
  - The number of Rx overruns
  - The number of times the transmitter was reset
  - The number of incoming bytes when the protocol was unknown
- ICMP statistics. The **info icmp** command displays the number of messages, bad messages, and destination unreachable messages received.

- Serial statistics. The **info serial** command displays the following information:
  - Number of bytes received and transmitted
  - Signal changes
  - FIFO and buffer overruns
  - Framing and parity errors
  - Breaks detected
- TCP statistics. The **info tcp** command displays the following information:
  - The number of segments received or sent
  - The number of active and passive opens
  - The number of bad segments received
  - The number of failed connection attempts
  - The number of segments retransmitted
  - The number of established connections that were reset
- UDP statistics. The **info udp** command displays the following information:
  - The number of datagrams received or sent
  - The number of bad datagrams received
  - The number of received datagrams that were discarded because the specified port was invalid
- To display mobile statistics, use the **display mobile** command instead of the **info** command.

newpass

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

ping

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

reconnect

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

rlogin

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

send

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

send mode

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

set accesscontrol

Use the **set accesscontrol** command to limit network access (IP filtering) to the Digi device.

set alarm

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

set autoconnect

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

set buffer and display buffers

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

set forward

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

set host

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

set ia

Use the **set ia** command to configure the Industrial Automation/Modbus information.

set mgmtconnection

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

set mgmtglobal

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

set mgmtnetwork

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

set mobile

Use the **set mobile** command to configure the cellular communication settings.

set nat

Use the **set nat** command to configure the router and Network Address Translation (NAT) settings.

set network

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

set pmodem

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

set pppoutbound

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

set ppp

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

set profiles

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

set realport

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

set rtstoggle

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

set serial

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

set service

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

set snmp

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

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

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

set system

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

set tcpserial

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

set user

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

set wlan

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

set wimax

Use the **set wimax** command to configure the Wi-MAX communication settings.

set wlan

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

status

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

show

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

telnet

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

vpn

Use the **vpn** command to manage Virtual Private Network (VPN) connections.

who and kill

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

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

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

Administration

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

Administrative task	Command
Backup/restore a configuration from a TFTP server on the network	**backup**
Update firmware	**boot** To update the firmware: 1. Telnet to the Digi device command-line interface using a telnet application or hyperterm. 2. If security is enabled for the Digi device, a login prompt appears. The default user name is **root** and the default password is **dbps.** If these defaults do not work, contact the system administrator who set up the device. 3. If you are at the bash shell, type **configshell** to get to the config shell. 4. Issue the **boot load** command: `#> boot load=tftp-server-ip:filename` Replace *tftp-server-ip* with the IP address of the TFTP server that contains the firmware, and replace *filename* with the name of the file to upload.
Reset configuration to factory defaults	**revert** or **boot action=factory**
Display system information and statistics	**info**
Reboot the device	**boot**
Enable/disable network services	**set service**

Remote Manager monitoring capabilities

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

- Display detailed state information and statistics about a device, such as device up time, amount of used and free memory, network settings, XBee network overview and detailed information on network nodes.
- Manage mobile settings.
- Monitor the state of the device's connection and see a connection report and connection history statistics.
- Redirect devices to a to a different destination.
- Disconnect devices.
- Remove devices from the network.

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

Remote Manager device management

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

Remote Manager is well-suited to managing Digi Connect WAN Family devices and the networks in which the devices reside. Advantages include the ability to view an entire network, and multiple networks, at once, and ease in viewing signal strength, link quality, and alarms.

SNMP device monitoring capabilities

SNMP provides the following device monitoring capabilities:

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

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

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

Supported RFCs and MIBs

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

- **Standard RFCs and MIBs**
  - RFC 1213—Management Information Base (MIB) II manages a TCP/IP network. MIB-II contains variable definitions that describe the most basic information needed to manage a TCP/IP network. Variable definitions are organized into several groups, such as groups for managing the system, network interfaces, address translation, transmission media, and various protocols, including IP, ICMP, TCP, UDP, EGP, and SNMP. See www.ietf.org/rfc/rfc1213.txt for more information.
  - RFC 1215—Generic Traps (coldStart, linkUp, authenticationFailure, login only). See www.ietf.org/rfc/rfc1215.txt for more information.
  - RFC 2790—Host Resources MIB for use with managing host systems, where “host” means any computer that communicates with other similar computers attached to the Internet. See tools.ietf.org/html/rfc2790 for more information.

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

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

SNMP configuration

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

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

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

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

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

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

Download a Digi MIB

To download a Digi MIB:

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

Supported SNMP traps

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

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

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

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

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

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

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

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

Specifications and certifications

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

Hardware specifications

This section provides the hardware specifications for all products in the Digi Connect WAN Family.

Digi Connect WAN specifications

Specification		Value
Environmental	Ambient temperature	-30 to +70C (-22 to 158F) for GSM models -30 to +60C (-22 to 140F) for CDMA models
	Relative humidity	Relative humidity not to exceed 95% non-condensing over the temperature range from 4C to 45C. Above 45C, constant absolute humidity shall be maintained.
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6560 feet)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263

Specification		Value
Power requirements	DC power input	■ Voltage input: 6-30VDC ■ Power consumption: Idle: 1.5W Max: 10.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply (domestic SKUs)	Can be powered by an external power supply. ■ Certifications: UL /c-UL Listed ITE or Class II power supply ■ Input voltage: 120 VAC +/- 10% ■ Input frequency: 60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 500 mA ■ Temperature range: +32 to 104F (0 to 40C). If you use a power supply with an ambient rating less than that specified by the product, then reduce the allowed ambient temperature range of the product to the rating of the power supply chosen. ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.

Specification		Value
	AC power supply (international SKUs)	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: +32 to 104F (0 to 40C). If you use a power supply with an ambient rating less than that specified by the product, then reduce the allowed ambient temperature range of the product to the rating of the power supply chosen. ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	13.3 cm (5.25 in)
	Width	8.5 cm (3.35 in)
	Depth	2.5 cm (0.97 in)
	Weight	0.45 g (1.00 lb)

ConnectPort WAN specifications

Specification		Value
Environmental	Ambient temperature	-30 to 60C (-22 to 140F)
	Relative humidity	Relative humidity not to exceed 95% non-condensing over the temperature range from 4C to 45C. Above 45C, constant absolute humidity shall be maintained.
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6560 feet)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263

Specification		Value
Power requirements	DC power input	■ Voltage input: 9-30VDC ■ Power consumption: Idle: 1.2W Max: 3.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: (32 to 104F (0 to 40C). If you use a power supply with an ambient rating less than that specified by the product, then reduce the allowed ambient temperature range of the product to the rating of the power supply chosen. ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	19.7 cm (7.75 in)
	Width	10.40 cm (4.11 in)
	Height	3.30 cm (1.30 in)
	Weight	Without a module: 0.64 kg (1.40 lb) With a module: 0.68 kg (1.50 lb)

Digi Connect WAN 3G / Digi Connect WAN 4G specifications

Specification		Value
Environmental	Ambient temperature	0 to +40C (+32 to 104F)
	Relative humidity	Relative humidity not to exceed 95% non-condensing over the temperature range from 4C to 45C. Above 45C, constant absolute humidity shall be maintained.
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6560 feet)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ Voltage input: 6-30VDC ■ Power consumption: Idle: 1.5W Max: 10.4W ■ Connector: 2.35mm x 5.7mm, locking barrel, center pin positive.
	AC power supply	■ Certifications: CE/UL /c-UL Listed ITE (LPS) or Class II power supply ■ Input voltage: 100 VAC to 240 VAC ■ Input frequency: 50-60 Hz ■ Output voltage: 12 VDC +/- 5% ■ Max output current: 1.66 A ■ Temperature range: 0 to 40C (+32 to 104F) ■ Connector: 2.1mm x 5.5mm, locking barrel, center pin positive.
Dimensions	Length	13.3 cm (5.25 in)
	Width	8.5 cm (3.35 in)
	Depth	2.5 cm (0.97 in)
	Weight	0.45 kg (1.00 lb)

Digi Connect WAN 3G IA specifications

Specification		Value
Environmental	Ambient temperature	-40 to +85C (-40 to 185F) **Notes:** ■ The ambient temperature of the unit may be further limited by the ambient temperature limits of the internal modules. ■ The ambient temperature of the internal modules must not be exceeded for proper operation. Refer to the installed module's specifications.
	Relative humidity	Relative humidity not to exceed 95% non-condensing over the temperature range from 4C to 45C. Above 45C, constant absolute humidity shall be maintained.
	Storage and transport temperature	-40 to 85C (-40 to 185F)
	Altitude	2000 meters (6560 feet)
	Ethernet isolation	1500VAC min per IEEE802.3/ANSI X3.263
Power requirements	DC power input	■ Voltage input: 6-30VDC ■ Power consumption: Idle: 1.5W Max: 10.4W ■ Connector: Tension clamp connector, 5.08mm spacing ■ Positive terminal - Left ■ Negative terminal - Right
Dimensions	Length	13.3 cm (5.25 in)
	Width	8.5 cm (3.35 in)
	Depth	2.5 cm (0.97 in)
	Weight	0.45 kg (1.00 lb)

Wireless networking features

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

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

Wireless feature	Specification
Wireless Networking Status Features	The following status information can be displayed for Wireless Digi devices. For more detailed descriptions, see Wi-Fi LAN Statistics.
Connection Status	The status of the wireless network connection.
Network Mode	The network mode currently in use: ■ Infrastructure mode ■ Ad-Hoc mode
Data Transfer Rate	The data transfer rate of the current connection.
Channel	The wireless network channel currently in use.
SSID	The selected SSID of the wireless network.
Wireless Security: Wi-Fi Protected Access (WPA/WPA2/802.11i), Wired Equivalent Privacy (WEP) security and encryption	The status of the WEP/WPA/WPA2 security features, including the Authentication Method currently in use and whether authentication is enabled or disabled.
Signal Strength	A statistic that indicates the strength of the radio signal between 0 and 100 percent.

Digi Connect WAN Family regulatory information and certifications

This section documents Digi Connect WAN Family regulatory information and certifications.

RF exposure statement

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

In order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antenna or antennas and the user should not be less than 20 cm.

FCC certifications and regulatory information (USA only)

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

FCC part 15 Class A

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

Radio Frequency Interface (RFI) (FCC 15.105)

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

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

Labeling Requirements FCC (15.19)

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

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

Modifications (FCC 15.21)

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

Cables (FCC 15.27)

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

Industry Canada (IC) certifications

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

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

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.

Class I Division 2, Groups A,B,C,D Hazardous Location

The following models are suitable for use in Class I, Division 2, Groups A, B, C and D or Non-hazardous locations only.

- Digi Connect WAN IA
- Digi Connect WAN 3G IA EVDO Sprint

- Digi Connect WAN 3G IA HSDPA EU
- Digi Connect WAN 3G IA Cell Ready
- Digi Connect WAN 3G IA HSDPA Generic
- Digi Connect WAN 3G IA HSDPA ATT
- Digi Connect WAN 3G IA EVDO VZW

Warning: Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2.

Avertissement: Risque d'Exlposion - La substitution de composants peut rendre ce matérial inacceptable pour les emplacements de Classe I, Division 2.

Warning: Explosion Hazard - Do not replace power supply unless power has been switched off or the area is known to be non-hazardous.

Avertissement: Risque d'Exlposion - Ne remplace power supply pas d'alimentation eletrique á moins que le pouvoir n'ait été éteint ou on connu que la région soit non-hasardeuse.

Warning: Explosion Hazard - Do not disconnect equipment unless power has been switched off or the area is know to be non-hazardous.

Avertissement: Risque d'Exlposion - Avant de déconnecter l'equipment, couper le courant ou s'assurer que l'emplacement est désigné non dangereux.

International EMC (Electromagnetic Emmissions/Immunity/Safety) standards

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

Product	Emissions	Immunity	Safety
Digi Connect WAN/ RG/VPN - CDMA	EN55022:1994 +A1:1995 +A2:1997 Class A FCC Part 15 Subpart B Class A VCCI-V-3/2005.04 AS/NZS CISPR 22:2002 FCC Part 22 Subpart H, section 107,109 and FCC Part 24 subpart E IC RSS-129 and IC RSS-133	EN55024:1998 +A1:2001 +A2:2003	UL/CUL 60950-1 UL1604, Class 1 Div 2 haz Loc IEC/EN60950-1 1st Ed.
Digi Connect WAN/ RG/VPN - GSM	EN55022:1998 FCC Part 15 Subpart B TS018	EN55024:1998	UL/CUL 60950-1 UL1604, Class 1 Div 2 haz Loc IEC/EN60950-1 1st Ed.

Product	Emissions	Immunity	Safety
Digi Connect WAN 3G	FCC Part 15 Subpart B Class B IEC-003 AS/NZS CISPR 22:2006 VCCI V-3 2007.04	EN55024	IEC/EN60950 UL/CUL 60950
Digi Connect WAN 3G IA	FCC Part 15 Subpart B Class B IEC-003 AS/NZS CISPR 22:2006 VCCI V-3 2007.04	EN55024	IEC/EN60950 UL/CUL 60950

Europe

The Digi Connect WAN Family is certified for use in several European countries. For information, visit www.digi.com/resources/certifications.

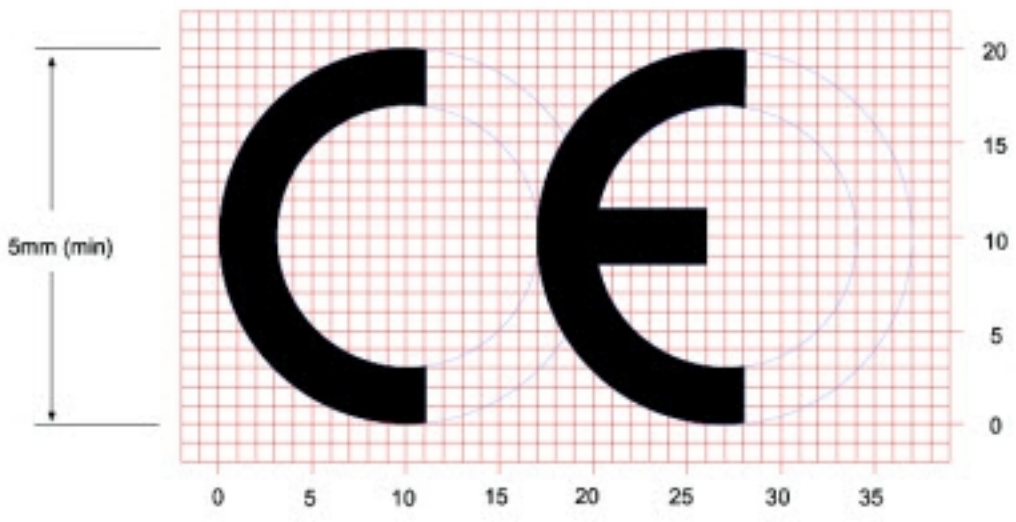
If the Digi Connect WAN Family is incorporated into a product, the manufacturer must ensure compliance of the final product with articles 3.1a and 3.1b of the RE Directive (Radio Equipment Directive). A Declaration of Conformity must be issued for each of these standards and kept on file as described in the RE Directive (Radio Equipment Directive).

Furthermore, the manufacturer must maintain a copy of the Digi Connect WAN Family user manual documentation and ensure the final product does not exceed the specified power ratings, antenna specifications, and/or installation requirements as specified in the user manual. If any of these specifications are exceeded in the final product, a submission must be made to a notified body for compliance testing to all required standards.

OEM labeling requirements

The 'CE' marking must be affixed to a visible location on the OEM product.

CE labeling requirements



The CE mark shall consist of the initials “CE” taking the following form:

- If the CE marking is reduced or enlarged, the proportions given in the above graduated drawing must be respected.
- The CE marking must have a height of at least 5mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for the Digi Connect WAN Family concerning emissions, EMC, and safety. For more information, see www.digi.com/resources/certifications.

Important note

Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

Maximum power and frequency specifications

Connect WAN 3G /IA

Maximum power	Frequencies
2 W	Cellular 850 and 900 MHZ Bands.
1 W	Cellular 1800 and 1900 MHZ Bands

Troubleshooting

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

Troubleshooting resources

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

To resolve a problem from the Digi Support site:

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

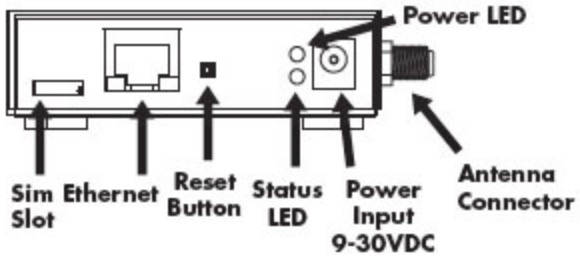
System status LEDs

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

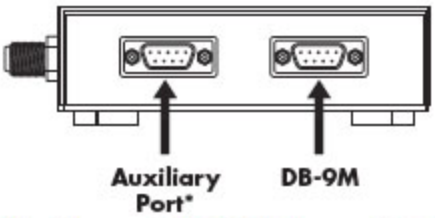
Digi Connect WAN Family LEDs and buttons

Digi Connect WAN and Digi Connect WAN IA

Digi Connect WAN GPRS/VPN - Front

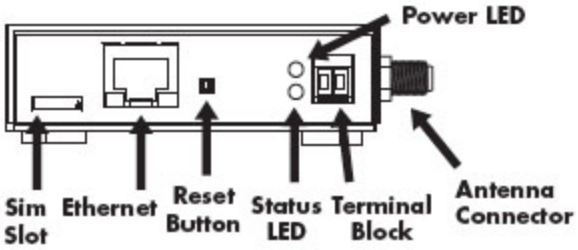


Digi Connect WAN GPRS//VPN - Back

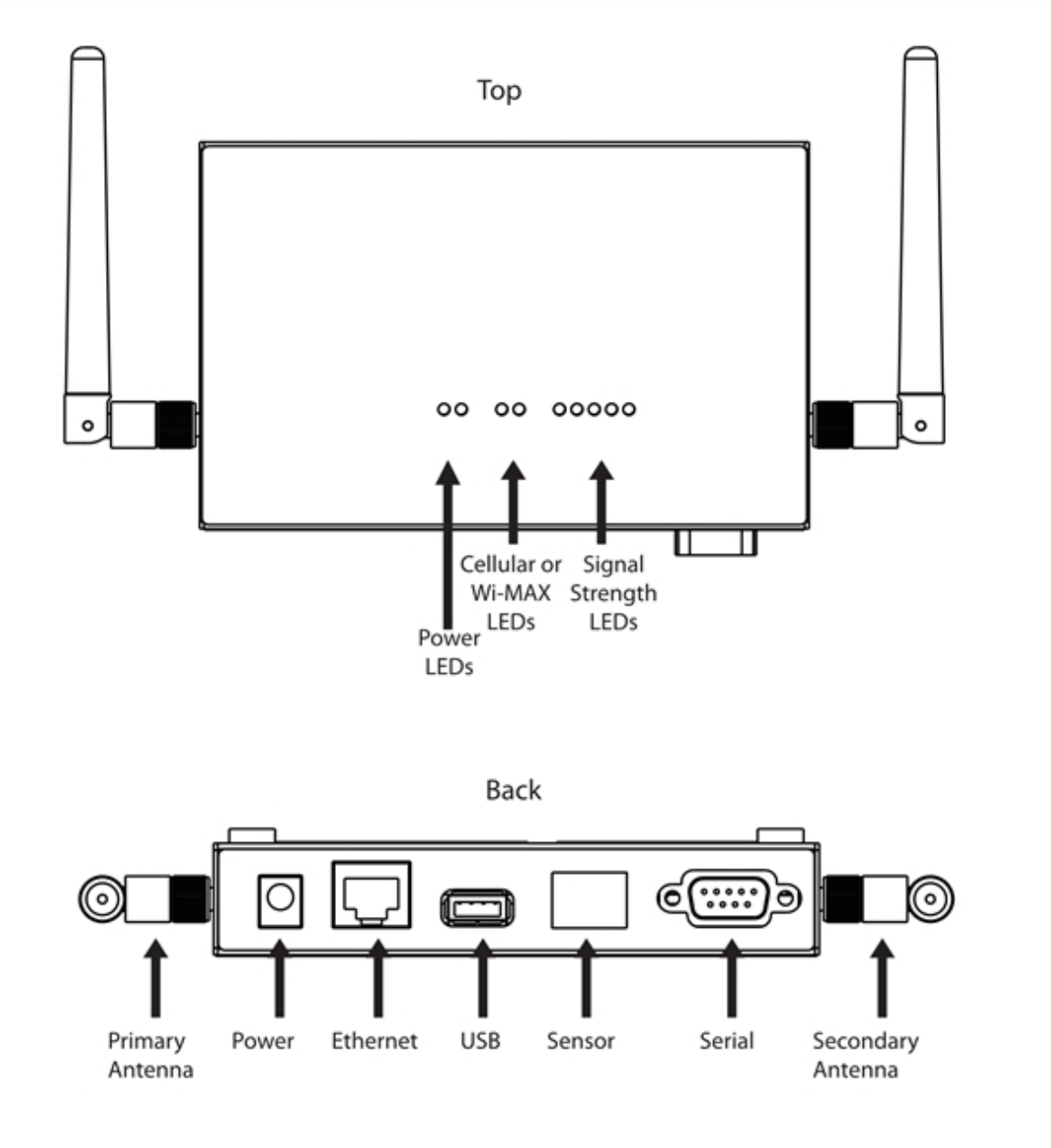


*Digi Connect WAN IA does not include an auxillary port

Digi Connect WAN IA - Front



Digi Connect WAN 3G and Digi Connect WAN 4G



Digi Connect WAN Family LEDs and buttons

LED/button	Color and Light Pattern	Activity Indicated
Power LED	Green	Power on.
	Not illuminated	Power off.

LED/button	Color and Light Pattern	Activity Indicated
Ethernet Link LED	Solid yellow	Ethernet link is available.
	Blinking green	Ethernet traffic is on Digi Connect WAN Family LEDs and buttons the link.
Cellular or WiMAX Link LED	Solid yellow	Cellular or Wi-MAX link is available.
Cellular or WiMAX Activity LEDs	Blinking green	Cellular or Wi-MAX traffic is on the link
Signal Strength LEDs	0-4 LEDs Amber or green depending on cellular signal type	Relative signal strength indicator (RSSI), shown as a number of LEDs. ■ 0: signal strength unknown or unacceptable ■ 1: signal strength low/weak ■ 4: signal strength high/excellent You can find specific dB values for the signal via the web interface; go to **Administration** > **System Information** > **Mobile**. Under **Mobile Connection**, the signal strength appears in bars and dBm. From the command line, type the **display mobile** command. Digi Connect WAN models have a feature where the signal strength LEDs change colors to indicate which type of cellular signal is detected. Amber = 2G network Green = 3G network
Status LED		Blinks during product initialization and factory reset, using the light patterns below. This LED should never blink during normal operation. If it blinks constantly, contact Digi Technical Support.
	Solid red	Initializing hardware.
	1-1-1 blinking green	Initializing firmware.
	1-5-1 blinking green	Device configuration has been restored to its factory defaults.
	Other blinking green	Contact Digi Technical Support.
	Solid green	Device is powered on and ready for operation.
Reset button		**Single press**: Performs equivalent of a power-cycle. **Press and hold**: Resets device configuration settings to factory defaults (factory reset).