



# Connect EZ Mini

## User Guide

---

Firmware version 24.3

## Revision history—90002409

Revision	Date	Description
M	April 2024	<p>Release of Digi Connect EZ firmware version 24.3:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">WireGuard VPN</a> - Configure a WireGuard VPN where your device can act as a client or as a server.</li> <li>▪ <a href="#">System watchdog</a> - Two new configuration settings: <ul style="list-style-type: none"> <li>• <b>Interface tests</b> - Configure a reboot of the interfaces you configure after a specified amount of time.</li> <li>• <b>Modem monitoring</b> - Configure a power cycle of the modem after an initial timeout instead of that timeout being reported as a failure.</li> </ul> </li> <li>▪ <a href="#">SNMP trap</a> and <a href="#">email notification</a> for events - Configure an SNMP v2 trap and/or email notification to be sent when an event occurs.</li> <li>▪ <a href="#">Configure a GRE tunnel</a> - Configure your tunnel to use Ethernet over GRE (<b>GRETAP</b> setting).</li> <li>▪ <a href="#">Serial disconnect</a> - Disconnect any users connected to a serial port configured for one of these modes: <a href="#">Login</a>, <a href="#">Remote Access</a>, <a href="#">PPP Dial-in</a>, or <a href="#">Modem Emulator</a>.</li> <li>▪ <a href="#">Serial port information</a> - Display information about the serial ports on the Dashboard.</li> </ul> <hr/> <p><b>Tip</b> For more information about this release, see the blog post called, "<a href="#">Announcing the Latest Digi Software Solutions for DAL OS 24.3 Firmware</a>" on <a href="#">digi.com</a>.</p> <hr/> <p><b>Additional changes</b></p> <ul style="list-style-type: none"> <li>▪ Added a step for <a href="#">device registration</a>.</li> </ul>
L	February 2024	Updated baud rate information. See <a href="#">Default serial port configuration</a> .
K	January 2024	<p>Release of Digi Connect EZ firmware version 23.12:</p> <ul style="list-style-type: none"> <li>▪ FIPS feature is available for all DAL devices. <a href="#">Enable FIPS mode</a></li> <li>▪ Link OSPF routes through a DMVPN tunnel and allow for redirection of packets between spokes. <a href="#">Configure a DMVPN spoke</a>.</li> <li>▪ New setting which allows device to initiate a Realport connection to a remote server. <a href="#">Configure the RealPort service</a>.</li> <li>▪ Renamed SureLink <b>Attempts</b> configuration setting to <b>Surelink test failures</b> to better indicate what this setting does.</li> <li>▪ New <b>Telnet Login</b> setting to control whether a user must supply</li> </ul>

Revision	Date	Description
		<p>credentials when opening a Telnet connection to access a serial port on a service. <a href="#">Configure serial authentication</a>.</p> <ul style="list-style-type: none"> <li>■ New Advanced watchdog <b>Modem check and recovery</b> setting to control whether watchdog will monitor initialization of the Connect EZ cellular modem. <a href="#">Configure the system watchdog</a>.</li> </ul> <hr/> <p><b>Tip</b> For more information about this release, see <a href="#">Announcing the Latest Digi Software Solutions for DAL OS 23.12 Firmware and Digi Remote Manager</a> on <a href="#">digi.com</a>.</p> <hr/>
J	October 2023	<p>Release of DigiConnect EZ firmware version 23.9:</p> <ul style="list-style-type: none"> <li>■ Register a device to DRM: <ul style="list-style-type: none"> <li>• Added a link to the Dashboard of the local web UI to register and add the device to Digi Remote Manager.</li> </ul> </li> <li>■ Updated Dashboard: <ul style="list-style-type: none"> <li>• Updated the layout of the Dashboard page of the web UI to combine the network interface and cellular modem details into a single Network Activity panel.</li> </ul> </li> <li>■ Domain allow list: <ul style="list-style-type: none"> <li>• Added a Domain allow list feature to control what domains are accessible through the Digi device.</li> </ul> </li> <li>■ Fallback: <ul style="list-style-type: none"> <li>• Added a fallback server setting to control which DNS server is used as the fallback in the event that no configured or DHCP-obtained DNS servers are available.</li> </ul> </li> <li>■ MACsec tunnel: <ul style="list-style-type: none"> <li>• Added information about adding a MACsec tunnel.</li> </ul> </li> </ul> <p><b>Additional changes</b></p> <ul style="list-style-type: none"> <li>■ Added <a href="#">Configure an email notification for a system event</a> and <a href="#">Configure an SNMP trap for a system event</a>.</li> </ul>
H	July 2023	<p>Release of DigiConnect EZ firmware version 23.6:</p> <ul style="list-style-type: none"> <li>■ Serial port options: <ul style="list-style-type: none"> <li>• For <b>PPP Dial-in</b> mode, added the <b>Default Route</b> option to control whether a default route gets added for the PPP interface.</li> <li>• Documented the new <b>Modem emulator</b> mode, which allows serial ports to act as a dial-up modem emulator for handling incoming AT dial-ins.</li> </ul> </li> <li>■ Advanced Watchdog options:</li> </ul>

Revision	Date	Description
		<ul style="list-style-type: none"> <li>• Added <b>System &gt; Advanced Watchdog</b> options to all devices.</li> <li>▪ Digi Remote Manager support: <ul style="list-style-type: none"> <li>• Each time a device connects to Digi Remote Manager after the device boots (or re-boots), the device now immediately uploads all health metrics.</li> </ul> </li> <li>▪ VPN: <ul style="list-style-type: none"> <li>• Added new <b>Enable open routing</b> configuration setting (<b>VPN &gt; IP tunnels</b>) to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel.</li> </ul> </li> <li>▪ Networking: <ul style="list-style-type: none"> <li>• Added new <b>TCP retries2</b> configuration setting (<b>Network &gt; Advanced</b>) to control the number of times an unacknowledged TCP data packet will be retransmitted before the connection is considered lost.</li> </ul> </li> </ul> <p><b>Additional changes</b></p> <ul style="list-style-type: none"> <li>▪ Updated RealPort sharing mode options description. See <a href="#">Configure the serial port for RealPort mode</a>.</li> </ul>

## Trademarks and copyright

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

© 2024 Digi International Inc. All rights reserved.

## Disclaimers

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

## Warranty

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

[www.digi.com/howtobuy/terms](http://www.digi.com/howtobuy/terms)

## Customer support

**Gather support information:** Before contacting Digi technical support for help, gather the following information:

- ✓ Product name and model
- ✓ Product serial number (s)

- ✓ Firmware version
- ✓ Operating system/browser (if applicable)
- ✓ Logs (from time of reported issue)
- ✓ Trace (if possible)
- ✓ Description of issue
- ✓ Steps to reproduce

**Contact Digi technical support:** Digi offers multiple technical support plans and service packages. Contact us at +1 952.912.3444 or visit us at [www.digi.com/support](http://www.digi.com/support).

## Feedback

To provide feedback on this document, email your comments to

[techcomm@digi.com](mailto:techcomm@digi.com)

Include the document title and part number (Digi Connect EZ Mini User Guide, 90002409 A) in the subject line of your email.

# Contents

---

## Digi Connect EZ Mini User Guide

Digi Connect EZ Mini .....	16
----------------------------	----

## Get started with Connect EZ

Before you begin: Register your Connect EZ .....	17
Step 1: Verify product components .....	17
Included equipment .....	18
Step 2: Connect the power supply .....	18
Step 3: Connect to site network using an Ethernet LAN .....	19
Step 4: Discover the IP address using the Digi Navigator .....	19
Step 5: Configure RealPort from the Digi Navigator .....	20
Step 6: Connect to the web UI and update the Connect EZ firmware .....	21
Step 7: Connect to Digi Remote Manager .....	22

## Hardware

Top panel and LEDs .....	23
Bottom panel .....	24
Back panel .....	25
Change the password on the Connect EZ .....	26
Connect equipment to the Connect EZ serial port .....	27
Connect equipment to a serial port .....	27
Serial connector pinout: Connect EZ Mini .....	27
Mount the Connect EZ device .....	28
Attach to a mounting surface using the two mounting tabs .....	28
Attach to DIN rail with clip .....	28
Power loss and Connect EZ configuration .....	29
Use the ERASE button to reset your device to the factory defaults .....	29
Discover the IP address using the Digi Navigator .....	30
Discover the device's IP address: Additional methods .....	30
Discover the IP address using a Micro USB cable .....	31
Manually configure the PC and assign an IP address to the device .....	31
Connect to the local Web UI on the Connect EZ .....	33
Device label sticker sample .....	33

## Firmware configuration

Review Connect EZ default settings .....	36
--	----

Local WebUI .....	36
Digi Remote Manager .....	36
Default interface configuration .....	36
Other default configuration settings .....	36
Change the default password for the admin user .....	37
Configuration methods .....	38
Using Digi Remote Manager .....	39
Access Digi Remote Manager .....	39
Using the local web interface .....	40
Review the dashboard .....	40
Log out of the web interface .....	41
Use the local REST API to configure the Connect EZ device .....	41
Use the GET method to return device configuration information .....	41
Use the POST method to modify device configuration parameters and list arrays .....	43
Use the DELETE method to remove items from a list array .....	44
Access the terminal screen from the web UI .....	45
Using the command line .....	46
Access the command line interface .....	46
Log in to the command line interface .....	46
Exit the command line interface .....	47

## Interfaces

Define a static IP address .....	48
IP address and netmask .....	49
Wide Area Networks (WANs) .....	49
Wide Area Networks (WANs) .....	50
Configure WAN priority and default route metrics .....	50
Configure SureLink active recovery to detect WAN failures .....	52
Configure the device to reboot when a failure is detected .....	66
Disable SureLink .....	73
Configure a Wide Area Network (WAN) .....	82
Show WAN status and statistics .....	87
Delete a WAN .....	89
Show SureLink status and statistics .....	90
Show SureLink State .....	91
Show SureLink status for all interfaces .....	91
Show SureLink status for a specific interface .....	92
Show SureLink status for all IPsec tunnels .....	92
Show SureLink status for a specific IPsec tunnel .....	93
Show SureLink status for all OpenVPN clients .....	93
Show SureLink status for a specific OpenVPN client .....	94
Configure a TCP connection timeout .....	94

## Serial port

Default serial port configuration .....	96
Serial mode options .....	96
View serial port information .....	96
Default serial port configuration .....	96
Baud rate options .....	97
Configure Login mode for a serial port .....	97
Configure Remote Access mode for a serial port .....	102
Configure Application mode for a serial port .....	120

Configure PPP dial-in mode for a serial port .....	122
Configure UDP serial mode for a serial port .....	129
Configure Modem emulator mode for a serial port .....	142
Configure Modbus mode for a serial port .....	145
Configure RealPort mode using the Digi Navigator .....	149
Installation and configuration process .....	149
Digi Navigator features .....	149
Install the Digi Navigator .....	149
Configure RealPort on a Digi device from the Digi Navigator .....	151
Digi Navigator device discovery process .....	152
Services used to discover a device when connected to a network .....	153
Digi Navigator application features .....	157
Advanced RealPort configuration without using the Digi Navigator .....	161
Windows Operating System .....	161
Linux Operating System .....	161
Download the RealPort driver .....	161
Configure RealPort on your laptop .....	161
Configure the serial port for RealPort mode .....	163
Configure the RealPort service .....	168
Disconnect a user from a serial port .....	170
Show serial port status and statistics .....	172
Serial Status page .....	172
Review the serial port message log .....	174

## Virtual Private Networks (VPN)

IPsec .....	177
IPsec data protection .....	177
IPsec mode .....	177
IPsec modes .....	177
Internet Key Exchange (IKE) settings .....	177
Authentication .....	178
Configure an IPsec tunnel .....	178
Configure IPsec failover .....	206
Configure SureLink active recovery for IPsec .....	209
Show IPsec status and statistics .....	225
Debug an IPsec configuration .....	226
Configure a Simple Certificate Enrollment Protocol client .....	227
Example: SCEP client configuration with Fortinet SCEP server .....	234
Show SCEP client status and information .....	239
OpenVPN .....	242
Configure an OpenVPN server .....	243
Configure an OpenVPN Authentication Group and User .....	252
Configure an OpenVPN client by using an .ovpn file .....	256
Configure an OpenVPN client without using an .ovpn file .....	259
Configure SureLink active recovery for OpenVPN .....	263
Show OpenVPN server status and statistics .....	280
Show OpenVPN client status and statistics .....	281
Generic Routing Encapsulation (GRE) .....	283
Configuring a GRE tunnel .....	284
Show GRE tunnels .....	289
Example: GRE tunnel over an IPsec tunnel .....	290
Dynamic Multipoint VPN (DMVPN) .....	305
Configure a DMVPN spoke .....	306
L2TP .....	312



Configure a PPP-over-L2TP tunnel .....	312
L2TP with IPsec .....	322
Show L2TP tunnel status .....	322
L2TPv3 Ethernet .....	324
Configure an L2TPv3 tunnel .....	324
Show L2TPv3 tunnel status .....	328
MACsec .....	330
Configure a MACsec tunnel .....	330
WireGuard VPN .....	332
Configure the WireGuard VPN .....	332

## Services

Allow remote access for web administration and SSH .....	339
Configure the web administration service .....	342
Configure SSH access .....	351
Use SSH with key authentication .....	358
Generating SSH key pairs .....	358
Configure telnet access .....	361
Configure DNS .....	366
Show DNS server .....	371
Simple Network Management Protocol (SNMP) .....	373
SNMP Security .....	373
Configure Simple Network Management Protocol (SNMP) .....	373
Download MIBs .....	378
Location information .....	380
Configure the location service .....	381
Configure the device to use a user-defined static location .....	383
Configure the device to accept location messages from external sources .....	385
Forward location information to a remote host .....	389
Configure geofencing .....	396
Show location information .....	408
Modbus gateway .....	409
Configure the Modbus gateway .....	410
Show Modbus gateway status and statistics .....	423
System time .....	426
Configure the system time .....	426
Manually set the system date and time .....	430
Network Time Protocol .....	430
Configure the device as an NTP server .....	431
Show status and statistics of the NTP server .....	436
Configure a multicast route .....	437
Enable service discovery (mDNS) .....	440
Use the iPerf service .....	443
Example performance test using iPerf3 .....	447
Configure the ping responder service .....	447
Example performance test using iPerf3 .....	451

## Applications

Develop Python applications .....	453
Set up the Connect EZ for Python development .....	454
Create and test a Python application .....	454
Python modules .....	458

Set up the Connect EZ to automatically run your applications .....	489
Configure scripts to run automatically .....	489
Show script information .....	496
Stop a script that is currently running .....	497
Start an interactive Python session .....	498
Run a Python application at the shell prompt .....	499
Configure scripts to run manually .....	500
Task one: Upload the application .....	501
Task two: Configure the application to run automatically .....	502
Start a manual script .....	506

## User authentication

Connect EZ user authentication .....	509
User authentication methods .....	509
Add a new authentication method .....	511
Delete an authentication method .....	513
Rearrange the position of authentication methods .....	514
Authentication groups .....	516
Change the access rights for a predefined group .....	518
Add an authentication group .....	520
Delete an authentication group .....	524
Local users .....	526
Change a local user's password .....	527
Configure a local user .....	529
Delete a local user .....	537
Terminal Access Controller Access-Control System Plus (TACACS+) .....	540
TACACS+ user configuration .....	541
TACACS+ server failover and fallback to local authentication .....	542
Configure your Connect EZ device to use a TACACS+ server .....	542
Remote Authentication Dial-In User Service (RADIUS) .....	547
RADIUS user configuration .....	548
RADIUS server failover and fallback to local configuration .....	548
Configure your Connect EZ device to use a RADIUS server .....	549
LDAP .....	552
LDAP user configuration .....	554
LDAP server failover and fallback to local configuration .....	555
Configure your Connect EZ device to use an LDAP server .....	555
Disable shell access .....	560
Set the idle timeout for Connect EZ users .....	562
Example user configuration .....	564
Example 1: Administrator user with local authentication .....	564
Example 2: RADIUS, TACACS+, and local authentication for one user .....	566

## Firewall

Firewall configuration .....	574
Create a custom firewall zone .....	574
Configure the firewall zone for a network interface .....	576
Delete a custom firewall zone .....	577
Port forwarding rules .....	579
Configure port forwarding .....	579
Delete a port forwarding rule .....	584
Packet filtering .....	586

Configure packet filtering .....	586
Enable or disable a packet filtering rule .....	590
Delete a packet filtering rule .....	591
Configure custom firewall rules .....	593
Configure Quality of Service options .....	595
Web filtering .....	604
Configure web filtering with Cisco Umbrella .....	604
Configure web filtering with manual DNS servers .....	607
Verify your web filtering configuration .....	610
Show web filter service information .....	612

## System administration

Review device status .....	614
Configure system information .....	615
Update system firmware .....	617
Manage firmware updates using Digi Remote Manager .....	617
Certificate management for firmware images .....	618
Downgrading .....	618
Dual boot behavior .....	622
Reboot your Connect EZ device .....	623
Reboot your device immediately .....	623
Schedule reboots of your device .....	623
Erase device configuration and reset to factory defaults .....	625
Custom factory default settings .....	628
Locate the device by using the Find Me feature .....	631
Enable FIPS mode .....	632
Configuration files .....	634
Save configuration changes .....	634
Save configuration to a file .....	635
Restore the device configuration .....	636
Schedule system maintenance tasks .....	639
Disable device encryption .....	644
Re-enable cryptography after it has been disabled. ....	645
Configure the speed of your Ethernet port .....	646
Configure the system watchdog .....	648

## Monitoring

intelliFlow .....	653
Enable intelliFlow .....	654
Configure service types .....	656
Configure domain name groups .....	658
Use intelliFlow to display average CPU and RAM usage .....	661
Use intelliFlow to display top data usage information .....	662
Use intelliFlow to display data usage by host over time .....	664
Configure NetFlow Probe .....	665

## Central management

Digi Remote Manager support .....	671
Certificate-based enhanced security .....	671
Configure your device for Digi Remote Manager support .....	671

Collect device health data and set the sample interval .....	678
Enable event log upload to Digi Remote Manager .....	681
Reach Digi Remote Manager on a private network .....	682
Pinhole method .....	682
Proxy server method .....	683
VPN Tunnel method .....	683
Log into Digi Remote Manager .....	683
Use Digi Remote Manager to view and manage your device .....	684
Add a device to Remote Manager .....	684
Add a device to Remote Manager using information from the label .....	684
Add a device to Remote Manager using your Remote Manager login credentials .....	685
Configure multiple Connect EZ devices by using Digi Remote Manager configurations .....	686
View Digi Remote Manager connection status .....	687
Learn more .....	688

## File system

The Connect EZ local file system .....	690
Display directory contents .....	690
Create a directory .....	691
Display file contents .....	692
Copy a file or directory .....	692
Move or rename a file or directory .....	693
Delete a file or directory .....	694
Upload and download files .....	695
Upload and download files by using the WebUI .....	695
Upload and download files by using the Secure Copy command .....	696
Upload and download files using SFTP .....	697

## Diagnostics

Perform a speedtest .....	700
Generate a support report .....	700
Support report overview .....	701
View system and event logs .....	705
View System Logs .....	705
View Event Logs .....	707
Configure syslog servers .....	710
Configure options for the event and system logs .....	712
Configure an email notification for a system event .....	716
Configure an SNMP trap for a system event .....	717
Analyze network traffic .....	719
Configure packet capture for the network analyzer .....	720
Example filters for capturing data traffic .....	729
Capture packets from the command line .....	730
Stop capturing packets .....	731
Show captured traffic data .....	732
Save captured data traffic to a file .....	733
Download captured data to your PC .....	734
Clear captured data .....	735
Use the ping command to troubleshoot network connections .....	737
Ping to check internet connection .....	737
Stop ping commands .....	737
Use the traceroute command to diagnose IP routing problems .....	737

## Digi Connect EZ regulatory and safety statements

RF exposure statement .....	739
Federal Communication (FCC) Part 15 Class A .....	739
European Community - CE Mark Declaration of Conformity (DoC) .....	739
CE and UKCA OEM labeling requirements .....	739
CE labeling requirements .....	739
UK Conformity Assessed (UKCA) labeling requirements .....	740
RoHS compliance statement .....	741
Cautionary statements for Connect EZ .....	741
Residential environment warnings .....	741
Product disposal instructions .....	741

## Command line interface

Access the command line interface .....	744
Log in to the command line interface .....	744
Exit the command line interface .....	745
Execute a command from the web interface .....	745
Display help for commands and parameters .....	746
The help command .....	746
The question mark (?) command .....	746
Display help for individual commands .....	747
Use the Tab key or the space bar to display abbreviated help .....	748
Auto-complete commands and parameters .....	748
Available commands .....	749
Use the scp command .....	750
Display status and statistics using the show command .....	752
show config .....	752
show system .....	752
show network .....	753
Device configuration using the command line interface .....	753
Execute configuration commands at the root Admin CLI prompt .....	753
Display help for the config command from the root Admin CLI prompt .....	753
Configuration mode .....	755
Enable configuration mode .....	755
Enter configuration commands in configuration mode .....	755
Save changes and exit configuration mode .....	756
Exit configuration mode without saving changes .....	756
Configuration actions .....	756
Display command line help in configuration mode .....	757
Move within the configuration schema .....	760
Manage elements in lists .....	761
The revert command .....	763
Enter strings in configuration commands .....	765
Example: Create a new user by using the command line .....	765
Command line reference .....	768
analyzer clear .....	768
analyzer save .....	768
analyzer start .....	768
analyzer stop .....	768
cat .....	768
clear dhcp-lease ip-address .....	769
clear dhcp-lease mac .....	769

cp .....	769
grep .....	769
help .....	770
ls .....	771
mkdir .....	772
modem sms send .....	772
modem sms send-binary .....	772
monitoring metrics upload .....	772
monitoring .....	773
monitoring metrics upload .....	773
more .....	773
mv .....	773
ping .....	773
poweroff .....	774
reboot .....	774
rm .....	774
scp .....	775
show analyzer .....	775
show arp .....	775
show cloud .....	775
show config .....	776
show dhcp-lease .....	776
show dns .....	776
show eth .....	776
show event .....	776
show hotspot .....	777
show ipsec .....	777
show l2tp lac .....	777
show l2tp lns .....	777
show l2tpeth .....	778
show location .....	778
show log .....	778
show manufacture .....	778
show modbus-gateway .....	778
show nemo .....	779
show network .....	779
show ntp .....	779
show openvpn client .....	779
show openvpn server .....	780
show route .....	780
show scep-client .....	780
show scripts .....	780
show serial .....	781
show surelink interface .....	781
show surelink ipsec .....	781
show surelink openvpn .....	781
show surelink state .....	781
show system .....	782
show version .....	782
show vrrp .....	782
show web-filter .....	782
speedtest .....	783
ssh .....	783
system backup .....	783
system cloud register .....	784

system disable-cryptography .....	784
system duplicate-firmware .....	784
system factory-erase .....	784
system find-me .....	785
system firmware ota check .....	785
system firmware ota list .....	785
system firmware ota update .....	785
system firmware update .....	785
system power ignition off_delay .....	786
system restore .....	786
system script start .....	786
system script stop .....	786
system serial clear .....	786
system serial restart .....	787
system serial save .....	787
system serial show .....	787
system support-report .....	787
system time set .....	788
system time sync .....	788
system time test .....	788
tail .....	788
telnet .....	789
traceroute .....	789
vtys .....	790

## Digi Connect EZ Mini User Guide

---

This guide provides reference and usage information for the Connect EZ.

Digi Connect EZ is Digi's next generation Device Server product line, providing connectivity for existing critical assets in business, commercial, and industrial automation applications. This product line builds on and extends the capabilities of our previous PortServer and Digi One products along with enhanced manageability, security, intelligence, and performance, while offering seamless connectivity for existing applications.

### Digi Connect EZ Mini

The Digi Connect EZ Mini has 1 serial port and is specifically designed to make it simple to implement and support machine-to-machine automation applications to allow enterprises to monitor and manage their critical equipment at scale.

The Connect EZ Mini offers a small form factor that can be easily deployed on a DIN rail, mounted on a wall or panel, or as a "bump in the cable". The Connect EZ Mini leverages Digi's DAL firmware and TrustFence security framework to extend Digi's critical infrastructure management offerings with enhanced deployment flexibility.

The Connect EZ Mini supports connectivity through RealPort, TCP Sockets, SSH, TLS, and UDP connectivity.



## Get started with Connect EZ

---

This section explains what comes with each Connect EZ model, how to install the necessary software, and how to connect the hardware.

[Before you begin: Register your Connect EZ](#)

[Step 1: Verify product components](#)

[Step 2: Connect the power supply](#)

[Step 3: Connect to site network using an Ethernet LAN](#)

[Step 4: Discover the IP address using the Digi Navigator](#)

[Step 5: Configure RealPort from the Digi Navigator](#)

[Step 6: Connect to the web UI and update the Connect EZ firmware](#)

[Step 7: Connect to Digi Remote Manager](#)

### Optional

- [Change the password on the Connect EZ](#)
- [Mount the Connect EZ](#)
- [Connect equipment to the Connect EZ serial port](#)

### Administrators only

- [Additional configuration](#) to the device can be done in Remote Manager or in the device's local web user interface.

## Before you begin: Register your Connect EZ

Welcome to the Digi family! Register your new Connect EZ today and start enjoying a suite of exclusive benefits, including centralized management and 24/7 technical support. [Click here to register now!](#)

## Step 1: Verify product components

Verify that you have the following included equipment.

---

**NEXT STEP:** If you are performing the initial device set-up, proceed to the next step after verifying the components: [Step 2: Connect the power supply](#).

---

## Included equipment

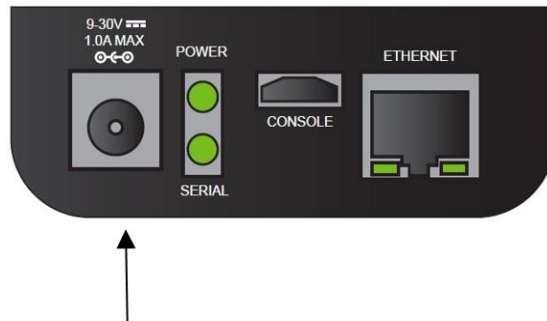
Equipment	Description
<b>Connect EZ Mini</b>	For detailed information about the panels, see: <ul style="list-style-type: none"> <li>▪ <a href="#">Top panel and LEDs</a></li> <li>▪ <a href="#">Bottom panel</a></li> <li>▪ <a href="#">Back panel</a></li> </ul>
<b>Power supply</b>	Each kit includes a power supply. The power supply is a Direct Plugin Class 2 output transformer rated 18 W, 12 VDC, and with a 1.5 A output. For information about connecting the power supply, see <a href="#">Step 2: Connect the power supply</a> .
<b>Ethernet cable</b>	Connect to a site network using an Ethernet cable. See <a href="#">Step 3: Connect to site network using an Ethernet LAN</a> .
<b>DIN rail clip kit</b>	The DIN rail clip connects to the back of the device and is used to mount the device onto a DIN rail. See <a href="#">Attach to DIN rail with clip</a> . The kit includes a DIN rail clip and two screws that meet these requirements: <ul style="list-style-type: none"> <li>▪ M4 in diameter</li> <li>▪ 5 mm in length</li> <li>▪ Countersunk</li> <li>▪ Phillips #2</li> <li>▪ Black Steel</li> </ul>
<b>Loose label</b>	A loose label sticker that includes information about the device is included in the box. You should retain this label sticker with your hardware records. For more information about the label, see <a href="#">Device label sticker sample</a> . <hr/> <p><b>Note</b> This label includes the unique default password for the device. This unique password will be needed if the device is factory reset and you want to access the web UI on the device.</p> <hr/>
<b>Global plug kit</b>	If you purchased the GLB version of the device, a kit that includes global outlet plugs is included.

## Step 2: Connect the power supply

The power supply is included with the device.

The power supply is a Direct Plugin Class 2 output transformer rated 18 W, 12 VDC, with 1.5 A output.

1. Orient the device so the top of the device is facing you.



2. Connect the twist-lock end of the power supply cord to the device.
3. Plug the other end of the power supply cord to a main power supply.

---

**NEXT STEP:** If you are performing the initial device set-up, proceed to the next step: [Step 3: Connect to site network using an Ethernet LAN](#).

---

## Step 3: Connect to site network using an Ethernet LAN

This section explains how to connect to a site network using an Ethernet cable.

1. Connect one end of an Ethernet cable to your site network.
2. Connect the other end of the Ethernet cable to the **Ethernet** port on the Connect EZ. By default a DHCP request will be sent to the local Ethernet network.

---

**Note** If you do not have a DHCP server on your network, you can connect locally over 192.168.210.1. See [Using the local web interface](#).

---

---

**NEXT STEP:** If you are performing the initial device set-up, proceed to the next step: [Step 4: Discover the IP address using the Digi Navigator](#).

---

## Step 4: Discover the IP address using the Digi Navigator

You can use the [Digi Navigator](#) to quickly discover the IP address for the Connect EZ.

---

**Note** If you don't have access to the **Digi Navigator**, you can use a manual method to discover the IP address. See [Discover the device's IP address: Additional methods](#).

---

1. To ensure that your computer and device are connected to each other and your local network, make the following connections:
  - Connect the device to your computer with an Ethernet cable.
  - Connect the device to your local network with an Ethernet cable.
  - Connect your computer to your local network with an Ethernet cable.
2. [Download and install](#) the **Digi Navigator**.
3. Launch the **Digi Navigator**.

4. The tool discovers the Connect EZ devices that are powered on and connected to your network. When the process is complete, a list of the devices appears.
  - **Connected to a network:** By default, the HTTPS service is enabled and used to find an IP address for the Connect EZ. Other services can be enabled if needed from the **Filters** section. See [Services used to discover a device when connected to a network](#).
  - **Connected directly to a device or on a network with no DHCP server:** In either of these situations, a default IP address is assigned to the device. You can specify the filters used to assign an IP address. See [Use the autodiscovery protocol to discover a device](#) and [Assign a generic IP address to the device](#).
5. Expand a device to display the IP address.

---

**NEXT STEP:** If you are performing the initial device set-up, you should proceed to the next step after getting the device's IP address: [Step 5: Configure RealPort from the Digi Navigator](#).

---

## Step 5: Configure RealPort from the Digi Navigator

You can configure the Connect EZ to communicate with your computer using RealPort from the **Digi Navigator**. You must enable RealPort on the device and then configure your computer for RealPort. In this step, all serial ports on the device are set to RealPort mode and the RealPort service is enabled. The COM ports on your laptop are also configured.

**Note** You can also manually configure the device for RealPort by logging into the device's web UI. See [Advanced RealPort configuration without using the Digi Navigator](#).

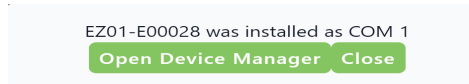
---

1. [Download and install](#) the **Digi Navigator**.
2. Make sure the Connect EZ is powered connected your local network or computer with an Ethernet cable.
3. Launch the **Digi Navigator**.
4. A list of the devices discovered by the **Digi Navigator** displays. Click on the device that you want to configure. For information about how devices are discovered and how to add a device to the list, see [Digi Navigator device discovery process](#).
5. Configure RealPort on the device.
  - a. Click the **Configure device for RealPort** button. A login screen displays.
  - b. Enter the device's default user name and password in the appropriate fields. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
  - c. Click **Submit**. A progress message displays.
  - d. When RealPort configuration is complete, the **Success** message displays.
 

A small dialog box with a white background and a thin border. At the top, the word "Success" is written in a small font. Below it, there is a green button with the word "Close" in white text.
  - e. Click **Close** to close the message.
6. Configure RealPort on your computer. The RealPort service is installed during this process.
  - a. Click **Configure this PC for RealPort**.
  - b. From the **Select starting COM** list box, select the COM port that should be configured for RealPort. The first available COM port is selected by default. The number of COM ports

configured matches the number of serial ports on the Connect EZ device.

- c. Click **Submit**. A series of progress messages displays.
- d. When the configuration is complete, a message displays.



- e. Determine your final step:
  - **Close:** Click **Close** to close the message. Configuration is complete.
  - **Open Device Manager:** Click **Open Device Manager** if you want to do further configuration to the COM ports. The Windows **Properties** dialog displays.

---

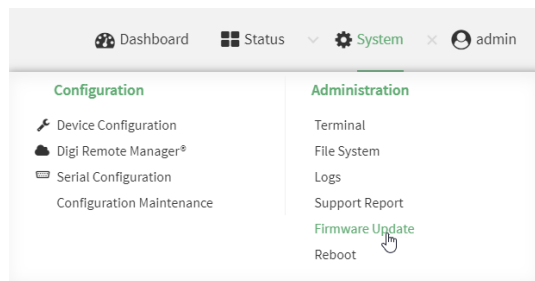
**NEXT STEP:** If you are performing the initial device set-up, proceed to the next step: [Step 6: Connect to the web UI and update the Connect EZ firmware.](#)

---

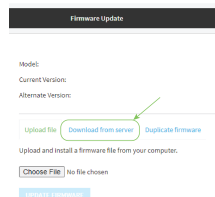
## Step 6: Connect to the web UI and update the Connect EZ firmware

You should update the firmware on the Connect EZ device to ensure that you have the latest features.

1. Make sure that an Ethernet cable is connected to the Connect EZ's **Ethernet** port and to a laptop or PC.
2. Open a browser and enter the [IP address](#) for the device.
3. Log into the device using the default user name and password. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
4. After logging in, the local web admin dashboard is displayed.
5. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



6. Click **Download from server**.



7. For **Version:**, select the version of the device firmware to which you want to update your device.
8. Click **Update Firmware**.

---

**Note** For more detailed information about this process, see [Update system firmware](#).

---

---

**NEXT STEP:** If you are performing the initial device set-up, proceed to the next step: [Step 7: Connect to Digi Remote Manager](#).

---

## Step 7: Connect to Digi Remote Manager

Connect your device to Digi Remote Manager to ensure that you receive automatic notification of firmware updates and security notices. From Remote Manager, you can also easily update firmware, ensure consistent configuration across a large group of devices, and manage and monitor cellular connectivity.

To start Digi Remote Manager

1. If you have not already done so, click [here](#) to sign up for a Digi Remote Manager account.
2. Check your email for Digi Remote Manager login instructions.
3. Go to [remotemanager.digi.com](https://remotemanager.digi.com).
4. Log into your Digi Remote Manager account.

For more information about configuring Remote Manager and managing devices, see [Central management](#).

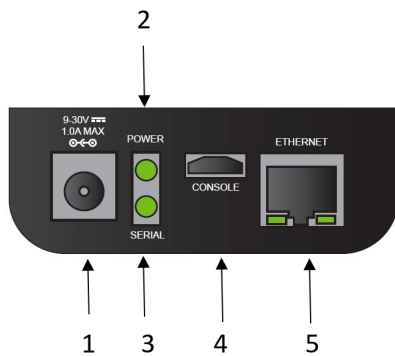
---

**NEXT STEP:** If you are performing the initial device set-up, you have now completed all of the required steps. You can return to [Get started with Connect EZ](#) for information on optional steps.

---

# Hardware

## Top panel and LEDs



Item	Name	Description
1	Power	Connect the power supply. See <a href="#">Step 2: Connect the power supply</a> .
2	Power LED	The LED lights up when the power is supplied to the device and the device powered on. <ul style="list-style-type: none"><li>▪ <b>Solid green:</b> The power source is connected and power is being supplied to the device.</li><li>▪ <b>Flashing green:</b> The <a href="#">Find Me feature</a> has been activated.</li></ul>
3	Serial port LED	Use the serial port to connect to devices and equipment to the Connect EZ. See <a href="#">Connect equipment to the Connect EZ serial port</a> . The serial port LED shows the status of the connection. <ul style="list-style-type: none"><li>▪ <b>Off:</b> The port is not in use.</li><li>▪ <b>Solid Green:</b> A device is connected to the port.</li><li>▪ <b>Blinking Green:</b> The port is in use and there is activity on the port.</li></ul>

Item	Name	Description
4	Console port	Connect a computer to the Connect EZ. This enables you to log into the Connect EZ if a network is not available.
5	Ethernet port	Indicates connection to Ethernet WAN network. The LED lights up when an Ethernet cable is attached. <ul style="list-style-type: none"> <li>▪ Left (yellow): There is activity on the port.</li> <li>▪ Right (green): The port is in use.</li> </ul>

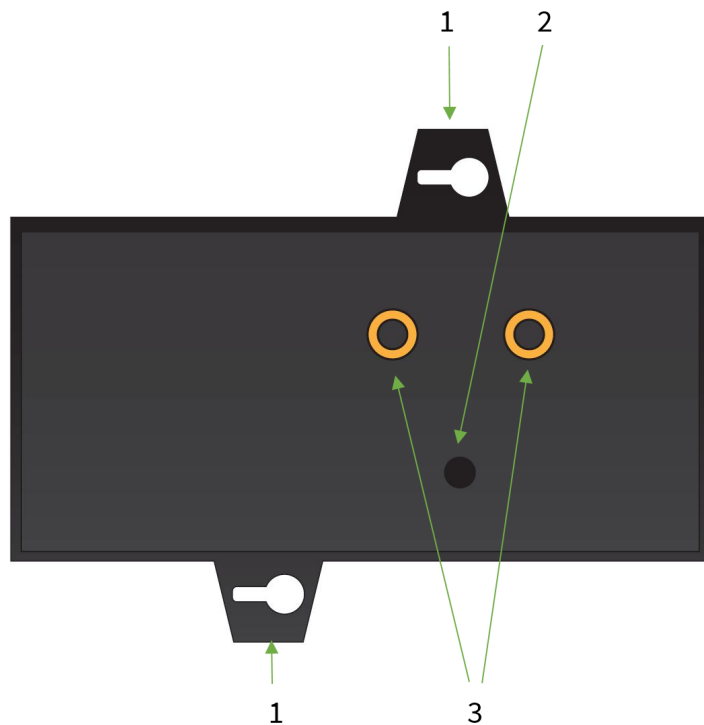
## Bottom panel



Name	Description
Serial port	Connect equipment to a serial port to provide console access to the equipment through a connected Ethernet WAN. See <a href="#">Connect equipment to the Connect EZ serial port</a> .



## Back panel



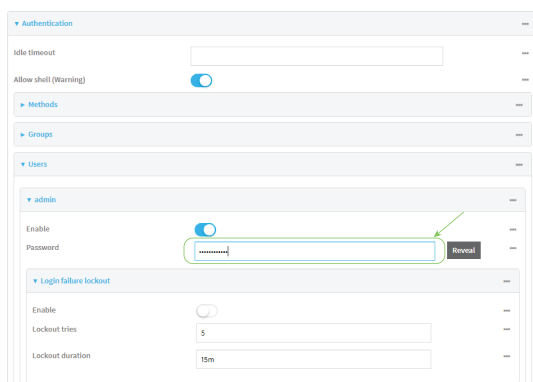
Item	Name	Description
1	Mounting tabs	The <a href="#">mounting tabs on the device</a> are used to mount the device onto a mounting surface. Use round-head M4 size screws. The type and length are dependent on the mounting surface type. Screws are not provided. If you choose not to mount the device, you can permanently remove the mounting tabs with a pliers.
2	Reset button	Use to <a href="#">reset the device</a> to factory defaults.
3	DIN rail clip	You can <a href="#">attach a DIN rail clip to the back</a> of the device and then mount the device to a DIN rail.

## Change the password on the Connect EZ

The unique, factory-assigned password for the default **admin** user account is printed on the bottom label of the device and on the loose label included in the package. For ease of use, you may want to change the password from the default.

If you erase the device configuration or reset the device to factory defaults, the password for the **admin** user will revert to the original, factory-assigned default password.

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System > Device Configuration**. The **Configuration** window appears.
3. Click **Authentication > Users > Admin**.
4. For **Password**, enter the new password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.



5. Click **Apply** to save the configuration and apply the change.

For more detailed information about this process, see [Change the default password for the admin user](#).

## Connect equipment to the Connect EZ serial port

After your device is connected and powered up, you can connect equipment to the device using the serial ports.

The serial port on the Connect EZ provides console access to connected critical equipment through a connected Ethernet LAN. Connect your network device to the Connect EZ serial port. For pinout information, see [Serial connector pinout: Connect EZ Mini](#).

You must use a cable with a DB9 connector to connect to a serial port on the Connect EZ. Consult the user guide for the device you are connecting to the Connect EZ to determine the connector type, cable type, and pinout positions for your specific device.

The serial port is enabled by default. The network devices connected to the serial port may be accessed using RealPort, Digi Remote Manager, the local web user interface, TCP, telnet, or SSH connections. TCP, telnet and SSH connections to serial ports are disabled by default and must be enabled by a device-specific configuration.

## Connect equipment to a serial port

You can connect equipment to a serial port on the Connect EZ, and access it using a terminal emulator program, such as Tera Term or Putty.

---

**Note** Before you begin, make sure a terminal emulator is installed on your laptop and you have a serial cable.

---

1. Connect one end of a serial cable to a serial port on the Connect EZ.
2. Connect the other end of the serial cable to your equipment.
3. Verify the connection between the Connect EZ and the equipment.
  - a. Open your terminal emulator.
  - b. Press **Enter**.
  - c. When the connection has been made, the serial port LED is solid green.

## Serial connector pinout: Connect EZ Mini

The Connect EZ Mini has a DB9 serial connector. The table below contains the pinout information.

DB-9 pin	EIA-232	EIA-422	EIA-485 Half-duplex
1	DCD	CTS-	Not used
2	RxD	RxD+	Data+
3	TxD	TxD+	Not used (Reserved)

DB-9 pin	EIA-232	EIA-422	EIA-485 Half-duplex
4	DTR	RTS-	Not used
5	GND	GND	GND
6	DSR	RxD-	Data-
7	RTS	RTS+	Not used
8	CTS	CTS+	Not used
9	RI	TxD-	Not used (Reserved)
Shell	GND		

## Mount the Connect EZ device

There are two mounting options available:

- [Attach to a mounting surface using the two mounting tabs](#)
- [Attach to DIN rail with DIN rail clip](#)

### Attach to a mounting surface using the two mounting tabs

Attach the device to a surface using the two tabs on the device. The type and length are dependent on the mounting surface type.

**Note** Screws are not provided.

#### Mounting onto soft or thin materials

Examples: Wallboard, sheetrock, wood, thin sheet metal, or plastic.

Use a screw that meets these requirements:

- M4 pan-head Philips screw
- Coarse-thread sheet metal screw
- 12 mm in length. The length should clear the mounting tab thickness and leave at least 1 cm of screw shank to bite into the mounting material.

#### Mounting onto thicker metals

Examples: Aluminum or steel.

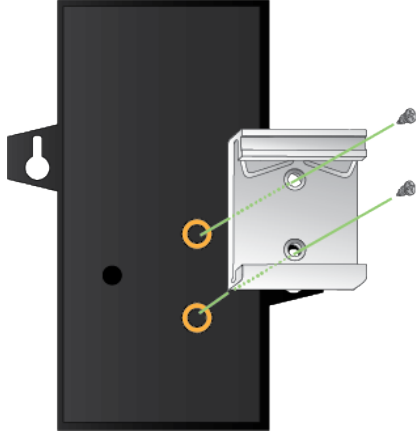
Use a screw that meets these requirements:

- M4 pan-head Philips screw
- Machine-thread screw
- 12 mm in length. The length should clear the mounting tab thickness and leave at least 1 cm of screw shank to bite into the mounting material.

### Attach to DIN rail with clip

The DIN rail clip and two screws are included with the device. You will need an appropriate Phillips-head screwdriver. For details about the hardware, see [DIN rail clip](#) information.

1. Remove required items from DIN rail mounting kit:
  - DIN rail clip
  - Two flat head screws.
2. Place the DIN rail clip on the rear panel of the device. Make sure the screw holes are aligned.



3. In each hole, use a Phillips-head screw driver to screw in a screw.
4. Tighten the screws as needed to securely fasten the DIN rail clip to the device.
5. Set the device onto a DIN rail and gently press until the clip snaps into the rail.

## Power loss and Connect EZ configuration

The Connect EZ retains its configuration if power is lost and then power is restored when the device is plugged into a main power supply, or if the device is commanded to restart automatically or interactively.

## Use the ERASE button to reset your device to the factory defaults

You can reset the Connect EZ to the factory default settings. Resetting the device to factory defaults performs the following actions:

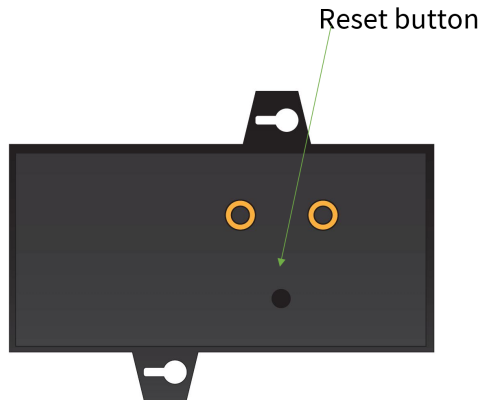
- Clears all configuration settings.
- All firmware updates are deleted.
- Deletes all user files.
- Regenerates SSH keys.
- Clears event and system log files.
- Creates a new event in the event log, indicating a factory reset.

---

**Note** While the settings are reset, the device's firmware version remains the same.

---

1. Make sure that the Connect EZ has been powered on for at least 30 seconds.
2. Locate the **Erase** button on the [back of the device](#).



3. Using a pinhole tool, press and briefly hold the **Erase** button.
4. The device resets to factory defaults and then reboots automatically.

## Discover the IP address using the Digi Navigator

You can use the [Digi Navigator](#) to quickly discover the IP address for the Connect EZ.

**Note** If you don't have access to the **Digi Navigator**, you can use a manual method to discover the IP address. See [Discover the device's IP address: Additional methods](#).

1. To ensure that your computer and device are connected to each other and your local network, make the following connections:
  - Connect the device to your computer with an Ethernet cable.
  - Connect the device to your local network with an Ethernet cable.
  - Connect your computer to your local network with an Ethernet cable.
2. [Download and install](#) the **Digi Navigator**.
3. Launch the **Digi Navigator**.
4. The tool discovers the Connect EZ devices that are powered on and connected to your network. When the process is complete, a list of the devices appears.
  - **Connected to a network:** By default, the HTTPS service is enabled and used to find an IP address for the Connect EZ. Other services can be enabled if needed from the **Filters** section. See [Services used to discover a device when connected to a network](#).
  - **Connected directly to a device or on a network with no DHCP server:** In either of these situations, a default IP address is assigned to the device. You can specify the filters used to assign an IP address. See [Use the autodiscovery protocol to discover a device](#) and [Assign a generic IP address to the device](#).
5. Expand a device to display the IP address.

## Discover the device's IP address: Additional methods

The IP address is used to log in to the Web UI for the device. If you do not have access to the [Digi Navigator](#), you can use either of these methods to discover the IP address.

- [Discover the IP address using a Micro USB cable](#)
- [Manually configure the PC and assign an IP address to the device](#)

## Discover the IP address using a Micro USB cable

You can use a Micro USB cable and a terminal emulation application to determine the device's IP address.

### Prerequisites

- A [power supply](#) must be connected to the device and the device powered on.
- Access to a terminal emulation application.
- A Micro USB cable.

To use the terminal emulation application to discover the device's IP address:

1. Connect one end of a Micro USB cable to your device and the other end to your PC.
2. Use the terminal emulation application to discover the device's IP address.
  - a. Access the terminal emulation application.
  - b. Log in to the Connect EZ.
    - **User name:** admin
    - **Password:** The unique password printed on the device label.
  - c. Type **a** to enter the Admin CLI.
  - d. Type **show network** to show all devices currently connected to the network.
  - e. Scroll down until you discover the Connect EZ.
  - f. Write down the IP address shown for the device.

## Manually configure the PC and assign an IP address to the device

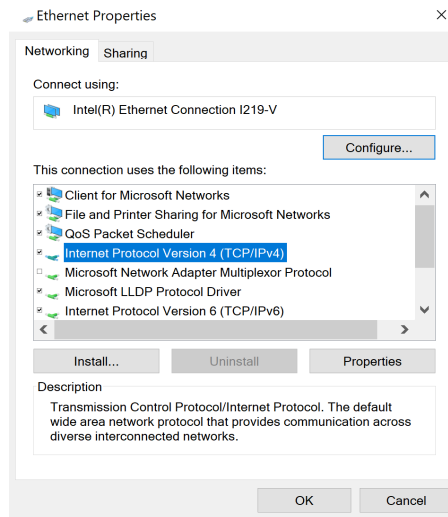
You can manually assign an IP address to the device.

### Prerequisites

- An [Ethernet cable](#) must be connected to the device and your network.
- A [power supply](#) must be connected to the device and the device powered on.
- Determine the IP address that you want to assign to the device.

To configure your laptop and assign an IP address:

1. On your PC, navigate to the Ethernet network settings dialog.
2. Click the **Internet Protocol Version 4 (TCP/IPv4)** parameter.



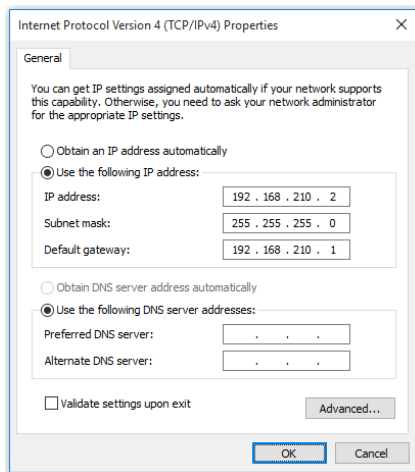
3. Click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog appears.
4. Select **Use the following IP address**.

---

**Note IMPORTANT:** Make note of the current IP address entries for **IP address**, **Subnet mask**, and **Default gateway**. You will need this information to complete the final step of the process.

---

5. Configure with the following details:
  - **IP address** for PC: 192.168.210.2
  - **Subnet**: 255.255.255.0
  - **Gateway**: 192.168.210.1



6. Click **OK**.
7. Open a browser window.
8. Enter the default gateway IP address: 192.168.210.1
9. Log into the device using the default user name and password. The default user name is **admin** and the default password is the unique password printed on the label packaged with your



device. For more detailed instructions, see [Connect to the local Web UI on the Connect EZ](#).

10. Update the IP address for the device.
11. On your PC, revert the IP address information to the original entries.
  - a. Return to the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog.
  - b. Enter the original IP address entries for **IP address**, **Subnet mask**, and **Default gateway**.
  - c. Click **OK**.

## Connect to the local Web UI on the Connect EZ

Once you are connected to the local Web UI, you can configure your device.

**Note** You can also use the **Digi Navigator** to access the web UI and configure the device. See [Access the web UI from the Digi Navigator](#).

1. Make sure that an Ethernet cable is connected to the Connect EZ's **Ethernet** port and to a laptop or PC.
2. Open a browser and enter the [IP address](#) for the device.
3. Log into the device using the default user name and password. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
4. After logging in, the local web admin dashboard is displayed.

The dashboard shows the current state of the device.

Dashboard area	Description
<b>Network activity</b>	Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices.
<b>Digi Remote Manager</b>	Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See <a href="#">Using Digi Remote Manager</a> .
<b>Device</b>	Displays the Connect EZ device's status, statistics, and identifying information.
<b>Network Interfaces</b>	Displays the status of the network interfaces configured on the device.

For more information, see [Using the local web interface](#).

## Device label sticker sample

A device label sticker that includes information about the device is included in the box. You should retain this label sticker with your hardware records.



Item	Description
1	<p>QR code</p> <p>Scan the QR code to display a semicolon separated list of:                      ProductName;DeviceID;Password;SerialNumber;SKUPartNumber                      SKUPartRevision</p> <hr/> <p><b>Note</b> Note the space between SKUPartNumber and SKUPartRevision</p> <hr/> <p>Example: Connect EZ 02;00000000-00000000-112233FF-                      FF445566;PW1234567890;EZ02-123456;EZ02-C000 B</p>
2	Label part number and revision level.
3	Product name, such as Connect EZ Mini, Connect EZ 2, or Connect EZ 8.
4	Device part number (SKU) and revision. For example, EZ02-C000 A
5	The unique default password for the device. This unique default password will be needed if the device is factory reset and you want to access the web UI on the device.
6	The MAC address for the device.
7	The unique serial number assigned to the device. The SN is needed when submitting a Digi support ticket.
8	The part number and revision level of the device kit.

# Firmware configuration

---

This chapter contains the following topics:

Review Connect EZ default settings .....	36
Change the default password for the admin user .....	37
Configuration methods .....	38
Using Digi Remote Manager .....	39
Access Digi Remote Manager .....	39
Using the local web interface .....	40
Use the local REST API to configure the Connect EZ device .....	41
Access the terminal screen from the web UI .....	45
Using the command line .....	46

## Review Connect EZ default settings

You can review the default settings for your Connect EZ device by using the local WebUI or Digi Remote Manager:

### Local WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System > Device Configuration**.

### Digi Remote Manager

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. Locate and select your device as described in [Use Digi Remote Manager to view and manage your device](#).
4. Click **Configure**.

The following tables list important factory default settings for the Connect EZ.

### Default interface configuration

Interface type	Preconfigured interfaces	Devices	Default configuration
<b>Wide Area Networks (WAN)</b>	<ul style="list-style-type: none"> <li>▪ Ethernet</li> </ul>	<ul style="list-style-type: none"> <li>▪ ETH</li> </ul>	<ul style="list-style-type: none"> <li>▪ Firewall zone: Edge</li> <li>▪ WAN priority: Metric=5</li> <li>▪ IP Address: DHCP address</li> <li>▪ Digi SureLink™ disabled for IPv4</li> </ul>
<b>Loopback</b>	<ul style="list-style-type: none"> <li>▪ Loopback</li> </ul>	<ul style="list-style-type: none"> <li>▪ Loopback</li> </ul>	<ul style="list-style-type: none"> <li>▪ Firewall zone: Loopback</li> <li>▪ IP address: 127.0.0.1/8</li> </ul>

### Other default configuration settings

Feature	Configuration
Central management	<ul style="list-style-type: none"> <li>▪ Digi Remote Manager enabled as the central management service.</li> </ul>

Feature	Configuration
Security policies	<ul style="list-style-type: none"> <li>■ Packet filtering allows all outbound traffic.</li> <li>■ SSH and web administration: <ul style="list-style-type: none"> <li>• Enabled for local administration</li> <li>• Firewall zone: Set up</li> </ul> </li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>■ Device health metrics uploaded to Digi Remote Manager at 60 minute interval.</li> <li>■ SNMP: Disabled</li> </ul>

## Change the default password for the admin user

The unique, factory-assigned password for the default **admin** user account is printed on the bottom label of the device and on the loose label included in the package.

If you erase the device configuration or reset the device to factory defaults, the password for the **admin** user will revert to the original, factory-assigned default password.

To change the default password for the admin user:

### ≡ Web

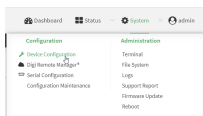
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

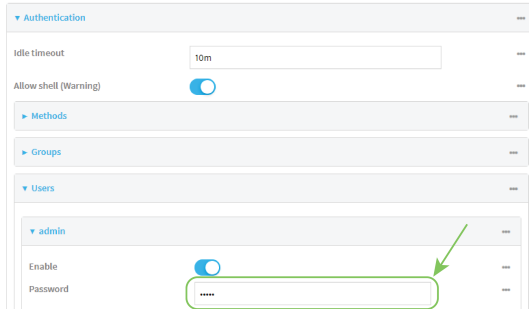
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Users > admin**.
4. Enter a new password for the admin user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.



5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Set a new password for the admin user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

---

```
(config)> auth user admin password new-password
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configuration methods

There are two primary methods for configuring your Connect EZ device:

- Web interface.

The web interface can be accessed in two ways:

- Central management using the Digi Remote Manager, a cloud-based device management and data enablement platform that allows you to connect any device to any application, anywhere. With the Remote Manager, you can configure your Connect EZ device and use the configuration as a basis for a Remote Manager configuration which can be applied to

other similar devices. See [Central management](#) for more information about using the Remote Manager to manage and configure your Connect EZ device.

- The local web interface. See [Using the local web interface](#) for more information about using the local web interface to manage and configure your Connect EZ device.

---

**Note** Changes made to the device's configuration by using the local web interface will not be automatically reflected in Digi Remote Manager. You must manually refresh Remote Manager for the changes to be displayed.

---

Web-based instructions in this guide are applicable to both the Remote Manager and the local web interface.

- **Command line.**

A robust command line allows you to perform all configuration and management tasks from within a command shell. Both the Remote Manager and the local web interface also have the option to open a terminal emulator for executing commands on your Connect EZ device. See [Using the command line](#) for more information about using the command line to manage and configure your Connect EZ device.

In this guide, task topics show how to perform tasks:

 **Web**

Shows how to perform a task by using the local web interface.

 **Command line**

Shows how to perform a task by using the command line interface.

## Using Digi Remote Manager

By default, your Connect EZ device is configured to use Digi Remote Manager as its central management server. Devices must be registered with Remote Manager using one of the following options:

- As part of the getting started process. See the [Quick Start Guide](#) for information.
- If you have not registered the device already, you can do so using the Device ID, MAC address, IMEI, or your Remote Manager login credentials. See [Add a device to Remote Manager](#).

For information about configuring central management for your Connect EZ device, see [Central management](#).

## Access Digi Remote Manager

To access Digi Remote Manager:

1. If you have not already done so, go to <https://myaccount.digi.com/> to sign up for a Digi Remote Manager account.
2. Check your email for Digi Remote Manager login instructions.
3. Go to [remotemanager.digi.com](https://remotemanager.digi.com).
4. Enter your user name and password. The Digi Remote Manager Dashboard appears.

## Using the local web interface

To connect to the Connect EZ local Web UI:

1. Use an Ethernet cable to connect the Connect EZ's **ETH** port to a laptop or PC.
2. Open a browser and go to **192.168.2.1**.
3. Log into the device using a configured user name and password.

The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.

## Review the dashboard

After logging in, the local web admin dashboard is displayed.

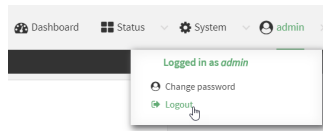
The dashboard shows the current state of the device.

Dashboard area	Description
<b>Network activity</b>	<ul style="list-style-type: none"> <li>▪ Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices.</li> <li>▪ Displays the status of the network interfaces configured on the device.</li> </ul>
<b>Digi Remote Manager</b>	<p>Displays the device connection status for Digi Remote Manager, the amount of time the connection has been up, and the Digi Remote Manager device ID. See <a href="#">Using Digi Remote Manager</a>.</p> <p>The links in this section enable you to do the following:</p> <ul style="list-style-type: none"> <li>▪ <b>Launch Digi Remote Manager:</b> Click <b>Go To Digi Remote Manager</b> to open the Digi Remote Manager login page.</li> <li>▪ <b>Add a device to Remote Manager:</b> Click <b>Register device in new account to add a device</b> to Remote Manager using your Remote Manager login credentials.</li> </ul>
<b>Device</b>	Displays the Connect EZ device's status, statistics, and identifying information.
<b>Serial Ports</b>	<p>Displays information about the serial ports on the Connect EZ. Each serial port is identified by port name or number, followed by the serial port mode configured for the port.</p> <p>The icons next to the port name or number shows the serial port status:</p> <ul style="list-style-type: none"> <li>▪ <b>Empty circle:</b> Port is not connected.</li> <li>▪ <b>Green circle:</b> Active connection on the port.</li> <li>▪ <b>Red X:</b> No signal, which is an error state where the port is not available.</li> <li>▪ <b>Down arrow:</b> One of the control signals is not active. This icon may display For for ports configured in <b>Remote Access serial port mode</b> and that have a signal monitor enabled (CTS or DCD) in the <b>Monitoring Settings</b> section.</li> </ul> <p>You can click the icons at the top of the section to access other pages:</p> <ul style="list-style-type: none"> <li>▪ <b>Blue "i":</b> Click to access the <a href="#">Serial Status</a> page.</li> <li>▪ <b>Blue wrench:</b> Click to access the <a href="#">Serial Configuration</a> page.</li> </ul>



## Log out of the web interface

- On the main menu, click your user name. Click **Log out**.



## Use the local REST API to configure the Connect EZ device

Your Connect EZ device includes a REST API that can be used to return information about the device's configuration and to make modifications to the configuration. You can view the REST API specification from your web browser by opening the URL:

**`https://ip-address/cgi-bin/config.cgi`**

For example:

**`https://192.168.210.1/cgi-bin/config.cgi`**

## Use the GET method to return device configuration information

To return device configuration, issue the **GET** method. For example, using **curl**:

---

```
$ curl -k -u admin https://ip-address/cgi-bin/config.cgi/value/path -X GET
```

---

where:

- ip-address* is the IP address of the Connect EZ device.
- path* is the path location in the configuration for the information being returned.

To determine allowed values for *path* from the Admin CLI:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights. Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

- At the config prompt, type **?(question mark)**:

---

```
(config)> ?
auth                Authentication
cloud               Central management
firewall            Firewall
monitoring          Monitoring
network             Network
serial              Serial
service             Services
```

---

---

```
system          System
vpn             VPN
```

---

```
(config)>
```

---

The allowed values for *path* are listed in the first (left) column.

- To determine further allowed path location values by using the ? (question mark) with the path name:

---

```
(config> service ?
```

```
Services
```

```
Additional Configuration
```

---

```
-----
dns          DNS
iperf       IPerf
location    Location
mdns        Service Discovery (mDNS)
modbus_gateway Modbus Gateway
multicast   Multicast
ntp         NTP
ping        Ping responder
snmp        SNMP
ssh         SSH
telnet      Telnet
web_admin   Web administration
```

```
(config)> service
```

---

For example, to use **curl** to return the ssh configuration:

---

```
$ curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/value/service/ssh -X GET
Enter host password for user 'admin':
{
  "ok": true,
  "result": {
    "type": "object",
    "path": "service.ssh"
  },
  "collapsed": {
    "acl.zone.0": "internal"
  },
  "acl.zone.1": "edge"
},
  "acl.zone.2": "ipsec"
},
  "acl.zone.3": "setup"
},
  "enable": "true"
},
  "key": ""
},
  "mdns.enable": "true"
```

---

---

```

,
"mdns.name": ""
,
"mdns.type": "_ssh._tcp."
,
"port": "22"
,
"protocol.0": "tcp"
    }
}
$

```

---

You can also use the **GET** method to return the configuration parameters associated with an item:

---

```

curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/keys/service/ssh -X GET
Enter host password for user 'admin':
{ "ok": true, "result": [ "acl", "custom", "enable", "key", "mdns", "port", "protocol" ] }
$

```

---

## Use the POST method to modify device configuration parameters and list arrays

### *Use the POST method to modify device configuration parameters*

To modify configuration parameters, use the **POST** method with the **path** and **value** parameters.

---

```

$ curl -k -u admin "https://ip-address/cgi-bin/config.cgi/value?path=path&value=new_value" -X POST

```

---

where:

- *path* is the path to the configuration parameter, in dot notation (for example, **ssh.service.enable**).
- *new\_value* is the new value for the parameter.

For example, to disable the ssh service using **curl**:

---

```

$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=service.ssh.enable&value=false" -X POST
Enter host password for user 'admin':
{ "ok": true }
$

```

---

### *Use the POST method to add items to a list array*

To add items to a list array, use the **POST** method with the **path** and **append** parameters. For example, to add the external firewall zone to the ssh service:

---

```

$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=service.ssh.acl.zone&append=true&value=external" -X POST
Enter host password for user 'admin':

```

---

---

```
{ "ok": true, "result": "service.ssh.acl.zone.4" }
$
```

---

### Use the POST method to add objects to a list array

Objects in an array that require one or more underlying values can be set using the **collapsed** URI parameter. We recommend including the **-g** option as well, to instruct curl to turn off globbing. The below example would add a new static route for the WAN interface for the 1.2.4.0/24 destination network:

---

```
$ curl -g -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=network.route.static&append=true&collapsed[dst]=1.2.4.0/24&collapsed[interface]=/network/interface/wan" -X POST
Enter host password for user 'admin':
{ "ok": true, "result": "network.route.static.1" }
$
```

---

### Use the DELETE method to remove items from a list array

To remove items from a list array, use the **DELETE** method. For example, using **curl**:

---

```
$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=path"
```

---

where *path* is the path to the list item, including the list number, in dot notation (for example, **service.ssh.acl.zone.4**).

For example, to remove the external firewall zone to the ssh service:

1. Use the **GET** method to determine the SSH service's list number for the external zone:

---

```
$ curl -k -u admin "https://192.168.210.1/cgi-bin/config.cgi/value?path=service/ssh/acl/zone" -X GET
{
  "ok": true,
  "result": {
    "type": "array",
    "path": "service.ssh.acl.zone"
  },
  "collapsed": {
    "0": "internal"
  },
  "1": "edge"
  ,
  "2": "ipsec"
  ,
  "3": "setup"
  ,
  "4": "external"
  }
}
$
```

---

2. Use the **DELETE** method to remove the external zone (list item 4).

---

```
$ curl -k -u admin https://192.168.210.1/cgi-bin/config.cgi/value?path=service.ssh.acl.zone.4 -X DELETE
Enter host password for user 'admin':
{ "ok": true }
$
```

---

## Access the terminal screen from the web UI

A user can log into a terminal screen and use CLI commands to access features.

**Note** You can also access the terminal screen from a port listed in the [Serial Status page](#).

1. [Log in to the web UI](#).
2. Click **System** > **Terminal**. The **Terminal** screen displays.
3. When prompted, enter your user name and password.
4. Enter the number of the port that you want to access.
5. Information about the port you are connected to displays, as well as commands.

---

```
Connecting to port5:
Settings: 9600, 8, 1, none, none
Type '~b.' to disconnect from port
Type '~b?' to list commands
```

---

6. Enter **~b?** to display additional commands.

Command	Description
~b.	Disconnect from the port.
~bB	Send a BREAK sequence.
~bc	Clear the history buffer.
~br	Send a DTR reset sequence.
~b?	Display a list of commands.

7. Enter **~b.** to disconnect from the port.

## Using the command line

The Digi Connect EZ device provides a command-line interface that you can use to configure the device, display status and statistics, update firmware, and manage device files.

See [Command line interface](#) for detailed instructions on using the command line interface and see [Command line reference](#) for information on available commands.

### Access the command line interface

You can access the Connect EZ command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

You can also access the command line interface in the WebUI by using the **Terminal**, or the Digi Remote Manager by using the **Console**.

To access the command line, your device must be configured to allow access, and you must log in as a user who has been configured for the appropriate access.

For further information about configuring access to these services, see:

- Serial: [Serial port](#)
- WebUI: [Configure the web administration service](#)
- SSH: [Configure SSH access](#)
- Telnet: [Configure telnet access](#)

### Log in to the command line interface

#### Command line

1. Connect to the Connect EZ device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See [Access the command line interface](#) for more information.
  - For serial connections, the default configuration is:
    - **115200** baud rate
    - **8** data bits
    - **no** parity
    - **1** stop bit
    - **no** flow control
  - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** on the **ETH1** port.
2. At the login prompt, enter the username and password of a user with Admin access:

---

```
login: admin
Password: *****
```

---

The default username is **admin**. The default unique password for your device is printed on the device label.

3. Depending on the device configuration, you may be presented with another menu, for example:

---

Access selection menu:

a: Admin CLI  
q: Quit

Select access or quit [admin] :

---

Type **a** or **admin** to access the Connect EZ command line.

You will now be connected to the Admin CLI:

---

Connecting now...  
Press Tab to autocomplete commands  
Press '?' for a list of commands and details  
Type 'help' for details on navigating the CLI  
Type 'exit' to disconnect from the Admin CLI

>

---

See [Command line interface](#) for detailed instructions on using the command line interface.

## Exit the command line interface

### Command line

1. At the command prompt, type **exit**.

---

> exit

---

2. Depending on the device configuration, you may be presented with another menu, for example:

---

Access selection menu:

a: Admin CLI  
q: Quit

Select access or quit [admin] :

---

Type **q** or **quit** to exit.

# Interfaces

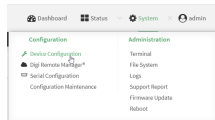
---

Connect EZ devices have a WAN physical communications interface.

## Define a static IP address

You can configure a static IP address for the Connect EZ.

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**. The **Configuration** window is displayed.



3. Click **Network > Interfaces**.
4. Click the desired Ethernet section, and keep the default settings.
  - **Enable:** Selected
  - **Interface type:** Ethernet
  - **Zone:** Edge
  - **Device:** The option matches the selected Ethernet: Device: ETH1, Device: ETH2, or Device ETH.
5. Configure IPv4 settings.
  - a. Click to expand **IPv4** settings.
  - b. Enable IPv4 support, if it is not enabled. This is enabled by default.
  - c. For **Type**, select **Static IP address**.
  - d. For **Address**, type the IP address and subnet of the LAN interface. Use the format *IPv4\_address/netmask*, for example, 192.168.2.1/24. For more information about the netmask, see [IP address and netmask](#).
  - e. For **Default gateway**, type the default gateway associated with this network interface.
6. (Optional) Add DNS servers to use with this static IP address.
  - a. Expand the **DNS Servers** section.
  - b. Click the plus sign icon next to **Add DNS server**.
  - c. In the **DNS server** field, enter the IP address of the DNS server.



- d. Repeat this process if you want to add another DNS server.
- 7. Click **Apply** to save the configuration and apply the change.

### IP address and netmask

The netmask is the length of the subnet mask in bits. For example, for a class C address with a subnet mask of 255.255.255.0, the length in bits would be 24.

NETMASK	255	255	255	255
Netmask length	8	16	24	32

## Wide Area Networks (WANs)

The Connect EZ device is preconfigured with one Wide Area Network (WAN), named **ETH1**.

You can modify configuration settings for the existing WAN, and you can create new WANs.

This section contains the following topics:

Wide Area Networks (WANs) .....	50
Configure WAN priority and default route metrics .....	50
Configure SureLink active recovery to detect WAN failures .....	52
Configure the device to reboot when a failure is detected .....	66
Disable SureLink .....	73
Configure a Wide Area Network (WAN) .....	82
Show WAN status and statistics .....	87
Delete a WAN .....	89

## Wide Area Networks (WANs)

A Wide Area Network (WAN) provides connectivity to the internet or a remote network. A WAN configuration consists of the following:

- A physical device, such as an Ethernet device.
- Several networking parameters for the WAN, such as firewall configuration and IPv4 and IPv6 support.
- Several parameters controlling failover.

## Configure WAN priority and default route metrics

The Connect EZ device is preconfigured with one Wide Area Network (WAN), named **ETH1**. You can also create additional WANs and WWANs.

When a WAN is initialized, the Connect EZ device automatically adds a default IP route for the WAN. The priority of the WAN is based on the metric of the default route, as configured in the WAN's IPv4 and IPv6 metric settings.

### *Assigning priority to WANs*

By default, the Connect EZ device's WAN (**ETH1**) is configured with the lowest metric (**1**), and is therefore the highest priority WAN. By default, the Wireless WAN (**Modem**) is configured with a metric of **3**, which means a lower priority than **ETH1**. You can assign priority to WANs based on the behavior you want to implement for primary and backup WAN interfaces. For example, if you want a cellular connection to be your primary WAN, with an Ethernet interface as backup, configure the metric of the WWAN to be lower than the metric of the WAN.

### *Example: Configure cellular connection as the primary WAN, and the Ethernet connection as backup*

#### Required configuration items

- Configured WAN and WWAN interfaces. This example uses the preconfigured **ETH1** and **Modem** interfaces.
- The metric for each WAN.

### Web

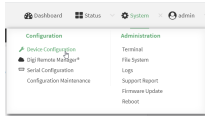
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

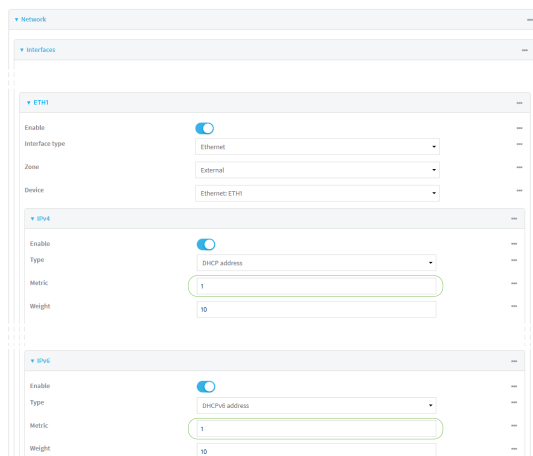
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Set the metrics for **Modem**:
  - a. Click **Network > Interfaces > Modem > IPv4**.
  - b. For **Metric**, type **1**.
  - c. Click **IPv6**.
  - d. For **Metric**, type **1**.
4. Set the metrics for **ETH1**:
  - a. Click **Network > Interfaces > ETH1 > IPv4**.
  - b. For **Metric**, type **2**.
  - c. Click **IPv6**.
  - d. For **Metric**, type **2**.



5. Click **Apply** to save the configuration and apply the change.

The Connect EZ device is now configured to use the cellular modem WWAN, **Modem**, as its highest priority WAN, and its Ethernet WAN, **ETH1**, as its secondary WAN.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set the metrics for **Modem**:

- a. Set the IPv4 metric for **Modem** to **1**. For example:

```
(config)> network interface modem ipv4 metric 1
(config)>
```

- b. Set the IPv6 metric for **Modem** to **1**:

```
(config)> network interface modem ipv6 metric 1
(config)>
```

4. Set the metrics for **ETH1**:

- a. Set the IPv4 metric for **ETH1** to **2**:

```
(config)> network interface eth1 ipv4 metric 2
(config)>
```

- b. Set the IPv6 metric for **ETH1** to **1**:

```
(config)> network interface eth1 ipv6 metric 2
(config)>
```

5. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

The Connect EZ device is now configured to use the cellular modem WWAN, **Modem**, as its highest priority WAN, and its Ethernet WAN, **ETH1**, as its secondary WAN.

## Configure SureLink active recovery to detect WAN failures

Problems can occur beyond the immediate WAN connection that prevent some IP traffic from reaching its destination. Normally this kind of problem does not cause the Connect EZ device to detect that the WAN has failed, because the connection continues to work while the core problem exists somewhere else in the network.

Using Digi SureLink, you can configure the Connect EZ device to regularly probe connections through the WAN to determine if the WAN has failed.

### Required configuration items

- By default, SureLink is enabled for the preconfigured WAN. The default configuration tests the DNS servers configured for the interface.

- The type of tests to be performed:
  - **Ping test:** Uses ICMP to determine connectivity. The default behavior is to ping the interface gateway, which means that an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
  - **DNS test:** Performs a DNS query to the named DNS server.
  - **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.
  - **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
  - **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.
  - **Custom test:** Tests the interface with custom commands.
  - **TCP connection test:** Tests that the interface can reach a destination port on the configured host.
  - **Test another interface's status:** Tests the status of another interface.
- The actions to take to recover connectivity in the event of failed tests:
  - **Change default gateway:** Increases the interface's metric to change the default gateway. This recovery action is enabled by default for the preconfigured WAN interface.
  - **Restart interface** This recovery action is enabled by default for the preconfigured WAN interface.
  - **Reboot device.**
  - Execute custom **Recovery commands.**
  - Two options also apply to every type of action:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

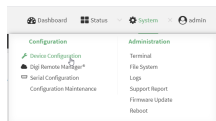
#### Additional configuration items

- The **Test interval** between connectivity tests.
- If more than one tests is configured, determine whether the interface should fail over based on the failure of one of the tests, or all of the tests.
- The number of test that must pass before the interface is considered to be working and its default route and DNS servers are reinstated.
- The amount of time that the device should wait for a response from an individual test before considering it to have failed.
- Advanced configuration items:
  - **Delayed Start:** The amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.
  - **Backoff interval:** The time to add to the test interval when restarting the list of actions.
  - **Test interface gateway by pinging:** Used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway.

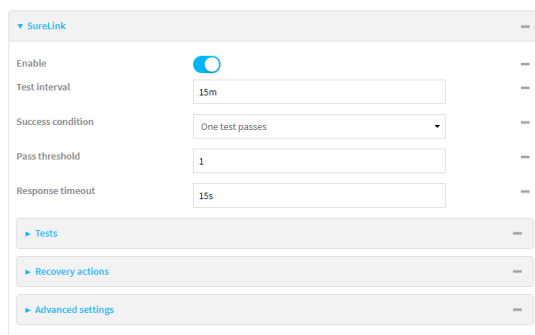
To configure the Connect EZ device to regularly probe connections through the WAN:

## Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. The **Configuration** window is displayed.
4. Click **Network > Interfaces**.
5. Create a new WAN or select an existing one:
  - To create a new WAN, see [Configure a Wide Area Network \(WAN\)](#).
  - To edit an existing WAN, click to expand the appropriate WAN.
6. After creating or selecting the WAN, click **SureLink**.



**Enable** SureLink.

7. (Optional) Change the **Test interval** between connectivity tests.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.  
The default is 15 minutes.
8. (Optional) If more than one test target is configured, for **Success condition**, select either:
  - **One test passes**: Only one test needs to pass for Surelink to consider an interface to be up.
  - **All test pass**: All tests need to pass for SureLink to consider the interface to be up.
9. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
10. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test attempt before considering it to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

The default is 15 seconds.

11. Click to expand **Tests**.

By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

a. Click **+**.



New tests are enabled by default. To disable, click to toggle off **Enable**.

b. Type a **Label** for the test.

c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.

d. Select the **Test type**.

Available test types:

- **Ping test:** Uses ICMP to determine connectivity.

If **Ping test** is selected, complete the following:

- **Ping target:** The type of target for the ping, one of:
  - **Hostname or IP address** of an external server.
    - **Ping host:** hostname or IP address of the server.
    - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - The **Interface address**.
    - The **Interface DNS** server.
  - **Ping payload size:** The number of bytes to send as part of the ping payload.

- **DNS test:** Performs a DNS query to the named DNS server.

If **DNS test** is selected, complete the following:

- **DNS server:** The IP address of the DNS server.

- **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **HTTP test** is selected, complete the following:

- **Web server:** The URL of the web server.

- **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

- **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **Test the interface status** is selected, complete the following:

- **Down time:** The amount of time that the interface is down before the test can be considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number(w|d|h|m|s)**.

For example, to set **Down time** to ten minutes, enter **10m** or **600s**.

- **Initial connection time:** The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number(w|d|h|m|s)**.

For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test:** Tests the interface with custom commands.

If **Custom test** is selected, complete the following:

- The **Commands to run to test**.

- **TCP connection test:** Tests that the interface can reach a destination port on the configured host.

If **TCP connection test** is selected, complete the following:

- **TCP connect host:** The hostname or IP address of the host to create a TCP connection to.
- **TCP connect port:** The TCP port to create a TCP connection to.

- **Test another interface's status:** Tests the status of another interface.

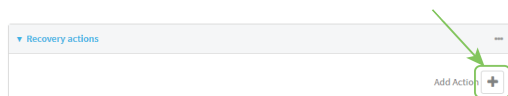
If **Test another interface's status** is selected, complete the following:

- **Test interface:** The interface to test.
- **IP version:** The type of IP connection, one of:
  - **Any:** Either the IPv4 or IPv6 connection must be up.
  - **Both:** Both the IPv4 or IPv6 connection must be up.
  - **IPv4:** The IPv4 connection must be up.
  - **IPv6:** The IPv6 connection must be up.
- **Expected status:** The status required for the test to pass.
  - **Up:** The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
  - **Down:** The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

e. Repeat for each additional test.

12. Add recovery actions:

- Click to expand **Recovery actions**.
- Click **+**.



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

- Type a **Label** for the recovery action.



- d. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.
- **Change default gateway:** Increases the interface's metric to change the default gateway.  
If **Change default gateway** is selected, complete the following:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Increase metric to change active default gateway:** Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Restart interface.**  
If **Restart interface** is selected, complete the following:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Reset modem:** This recovery action is available for WWAN interfaces only.  
If **Reset modem** is selected, complete the following:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Switch to alternate SIM:** Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.  
If **Switch to alternate SIM** is selected, complete the following:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Reboot device.**  
If **Reboot device** is selected, complete the following:
    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- Execute custom **Recovery commands**.

If **Recovery commands** is selected, complete the following:

- **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
- The **Commands to run to recovery connectivity**.
- **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

- **Powercycle the modem.** This recovery action is available for WWAN interfaces only.

If **Powercycle the modem** is selected, complete the following:

- **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
- **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.

e. Repeat for each additional recovery action.

13. (Optional) Configure advanced SureLink parameters:

a. Click to expand **Advanced settings**.

b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

The default is 300 seconds.

c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

The default is 300 seconds.

d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.

14. Click **Apply** to save the configuration and apply the change.



## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Create a new WAN, or edit an existing one:
  - To create a new WAN, see [Configure a LAN](#), [Configure a Wide Area Network \(WAN\)](#), or [Configure a Wide Area Network \(WAN\)](#) or [Configure a Wireless Wide Area Network \(WWAN\)](#).
  - To edit an existing WAN, change to the WAN's node in the configuration schema. For example, for a WAN named **my\_wan**, change to the **my\_wan** node in the configuration schema:

---

```
(config)> network interface my_wan
(config network interface my_wan)>
```

---

4. Enable SureLink.

By default, SureLink is enabled for the preconfigured WAN. The default configuration tests the DNS servers configured for the interface.

---

```
(config network interface my_wan)> surelink enable true
(config network interface my_wan)>
```

---

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

To add additional tests:

- a. Add a test:

---

```
(config network interface my_wan)> add surelink tests end
(config network interface my_wan surelink tests 1)>
```

---

- b. New tests are enabled by default. To disable:

---

```
(config network interface my_wan surelink tests 1)> enable false
(config network interface my_wan surelink tests 1)>
```

---

- c. Create a label for the test:

---

```
(config network interface my_wan surelink tests 1)> label string
(config network interface my_wan surelink tests 1)>
```

---

- d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

---

```
(config network interface my_wan surelink tests 1)> ipv6 true
(config network interface my_wan surelink tests 1)>
```

---

- e. Set the test type:

---

```
(config network interface my_wan surelink tests 1)> test value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **ping:** Uses ICMP to determine connectivity.

If **ping** is selected, complete the following:

- Set the **ping\_method**:

---

```
(config network interface my_wan surelink tests 1)> ping_
method value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **hostname:** The hostname or IP address of an external server.
- Set **ping\_host** to the hostname or IP address of the server:

---

```
(config network interface my_wan surelink tests 1)> ping_
host hostname/IP_address
(config network interface my_wan surelink tests 1)>
```

---

- **interface\_gateway.** If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
- **interface\_address.**
- **interface\_dns:** The interface's DNS server.

- Set the number of bytes to send as part of the ping payload:

---

```
(config network interface my_wan ipsec tunnel ipsec_example
surelink tests 1)> ping_size int
(config network interface my_wan surelink tests 1)>
```

---

- **dns:** Performs a DNS query to the named DNS server.

If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

---

```
(config network interface my_wan surelink tests 1)> dns_server
IP_address
(config network interface my_wan surelink tests 1)>
```

---

- **http:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **http** is set, set the URL of the web server.

---

```
(config network interface my_wan surelink tests 1)> http url
(config network interface my_wan surelink tests 1)>
```

---

- **dns\_configured:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

- **interface\_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **interface\_up** is set, complete the following:

- Set the amount of time that the interface is down before the test can be considered to have failed.

---

```
(config network interface my_wan surelink tests 1)>
interface_down_time value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_down\_time** to ten minutes, enter either **10m** or **600s**:

---

```
(config network interface my_wan surelink tests 1)>
interface_down_time 600s
(config)>
```

---

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

---

```
(config network interface my_wan surelink tests 1)>
interface_timeout value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config network interface my_wan surelink tests 1)>
interface_timeout 600s
(config)>
```

---

- **custom\_test**: Tests the interface with custom commands.

If **custom\_test** is set, set the commands to run to perform the test:

---

```
(config network interface my_wan surelink tests 1)> custom_
test_commands "string"
(config network interface my_wan surelink tests 1)>
```

---

- **tcp\_connection**: Tests that the interface can reach a destination port on the configured host.

If **tcp\_connection** is selected, complete the following:

- Set the hostname or IP address of the host to create a TCP connection to:

---

```
(config network interface my_wan surelink tests 1)> tcp_host
hostname/IP_address
(config network interface my_wan surelink tests 1)>
```

---

- Set the TCP port to create a TCP connection to.

---

```
(config network interface my_wan surelink tests 1)> tcp_port
port
(config network interface my_wan surelink tests 1)>
```

---

- **other**: Tests the status of another interface.

If **other** is selected, complete the following:

- Set the interface to test.
  - Use the ? to determine available interfaces:
  - Set the interface. For example:

---

```
(config network interface my_wan surelink tests 1)> other_
interface /network/interface/eth1
(config network interface my_wan surelink tests 1)>
```

---

- Set the type of IP connection:

---

```
(config network interface my_wan surelink tests 1)> other_ip_
version value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **any**: Either the IPv4 or IPv6 connection must be up.
- **both**: Both the IPv4 or IPv6 connection must be up.
- **ipv4**: The IPv4 connection must be up.
- **ipv6**: The IPv6 connection must be up.
- The status required for the test to pass.

---

```
(config network interface my_wan surelink tests 1)> other_
status value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

- Repeat for each additional test.

## 6. Add recovery actions:

- a. Type ... to return to the root of the configuration:

```
(config network interface my_wan surelink tests 1)> ...
(config)>
```

- b. Add a recovery action:

```
(config)> add network interface my_wan surelink actions end
(config network interface my_wan surelink actions 0)>
```

- c. New actions are enabled by default. To disable:

```
(config network interface my_wan surelink actions 0)> enable false
(config network interface my_wan surelink actions 0)>
```

- d. Create a label for the action:

```
(config network interface my_wan surelink actions 0)> label string
(config network interface my_wan surelink actions 0)>
```

- e. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.

```
(config network interface my_wan surelink actions 0)> action value
(config network interface my_wan surelink actions 0)>
```

where *value* is one of:

- **update\_routing\_table**: Increases the interface's metric to change the default gateway.

If **update\_routing\_table** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config network interface my_wan surelink actions 0)> test_
failures int
(config network interface my_wan surelink actions 0)>
```

The default is **3**.

- Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

```
(config network interface my_wan surelink actions 0)> metric_
adjustment_modem int
(config network interface my_wan surelink actions 0)>
```

The default is **100**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config network interface my_wan surelink actions 0)>
override_interval int
(config network interface my_wan surelink actions 0)>
```

---

- **restart\_interface.**

If **restart\_interface** is selected, complete the following:

(missing or bad snippet)(missing or bad snippet)

- **reboot\_device.**

If **reboot\_device** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config network interface my_wan surelink actions 0)> test_
failures int
(config network interface my_wan surelink actions 0)>
```

---

The default is **3**.

(missing or bad snippet)

- **custom\_action:** Execute custom recovery commands.

If **custom\_action** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config network interface my_wan surelink actions 0)> test_
failures int
(config network interface my_wan surelink actions 0)>
```

---

The default is **3**.

- Set the commands to run to attempt to recovery connectivity.

---

```
(config network interface my_wan surelink actions 0)> custom_
action_commands_modem "string"
(config network interface my_wan surelink actions 0)>
```

---

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config network interface my_wan surelink actions 0)>
override_interval int
(config network interface my_wan surelink actions 0)>
```

---

f. Repeat for each additional recovery action.

7. Optional SureLink configuration parameters:

a. Type ... to return to the root of the configuration:

---

```
(config network interface my_wan surelink actions 0)> ...
(config)>
```

---



- b. Set the test interval between connectivity tests:

```
(config)> network interface my_wan interval value(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink 600s
(config)>
```

The default is **15m**.

- c. If more than one test target is configured, set the success condition:

```
(config)> network interface my_wan success_condition value
(config)>
```

where *value* is either:

- **one**: Only one test needs to pass for Surelink to consider an interface to be up.
- **all**: All tests need to pass for SureLink to consider the interface to be up.

- d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

```
(config)> network interface my_wan pass_threshold int
(config)>
```

The default is **1**.

- e. Set the amount of time that the device should wait for a response to a test attempt before considering it to have failed:

```
(config)> network interface my_wan timeout value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_wan surelink timeout 600s
(config)>
```

The default is **15s**.

- f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

```
(config)> network interface my_wan advanced delayed_start value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **delayed\_start** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> network interface my_wan surelink advanced delayed_start
600s
(config)>
```

---

The default is **300s**.

- g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

---

```
(config)> network interface my_wan advanced backoff_interval value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **backoff\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> network interface my_wan advanced backoff_interval 600s
(config)>
```

---

The default is 300 seconds.

- h. The **interface\_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

---

```
(config)> network interface my_wan advanced interface_gateway
hostname/IP_address
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config network interface my_wan ipv4 surelink)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the device to reboot when a failure is detected

Using SureLink, you can configure the Connect EZ device to reboot when it has determined that an interface has failed.

### Required configuration items

- Enable SureLink.
- Enable device reboot upon interface failure.
- The type of tests to be performed:
  - **Ping test**: Uses ICMP to determine connectivity. The default behavior is to ping the interface gateway, which means that an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route

is used for the ping test.

- **DNS test:** Performs a DNS query to the named DNS server.
- **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.
- **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.
- **Custom test:** Tests the interface with custom commands.
- **TCP connection test:** Tests that the interface can reach a destination port on the configured host.
- **Test another interface's status:** Tests the status of another interface.

#### Additional configuration items

- See for [Configure SureLink active recovery to detect WAN failures](#) optional SureLink configuration parameters.

To configure the Connect EZ device to reboot when an interface has failed:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.
3. The **Configuration** window is displayed.
4. Click **Network > Interfaces**.
5. Create a new WAN or select an existing one:
  - To create a new WAN, see [Configure a Wide Area Network \(WAN\)](#).
  - To edit an existing WAN, click to expand the appropriate WAN.
6. After creating or selecting the WAN, click **SureLink**.
7. **Enable** SureLink.
8. (Optional) Change the **Test interval** between connectivity tests.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Interval** to ten minutes, enter **10m** or **600s**.  
 The default is 15 minutes.
9. (Optional) If more than one test target is configured, for **Success condition**, select either:
  - **One test passes:** Only one test needs to pass for Surelink to consider an interface to be up.
  - **All test pass:** All tests need to pass for SureLink to consider the interface to be up.
10. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
11. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test attempt before considering it to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

The default is 15 seconds.

12. Select the **Test type**.

Available test types:

- **Ping test:** Uses ICMP to determine connectivity.

If **Ping test** is selected, complete the following:

- **Ping target:** The type of target for the ping, one of:
  - **Hostname or IP address** of an external server.
  - **Ping host:** hostname or IP address of the server.
  - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
  - The **Interface address**.
  - The **Interface DNS** server.
- **Ping payload size:** The number of bytes to send as part of the ping payload.

- **DNS test:** Performs a DNS query to the named DNS server.

If **DNS test** is selected, complete the following:

- **DNS server:** The IP address of the DNS server.

- **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **HTTP test** is selected, complete the following:

- **Web server:** The URL of the web server.

- **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

- **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **Test the interface status** is selected, complete the following:

- **Down time:** The amount of time that the interface is down before the test can be considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Down time** to ten minutes, enter **10m** or **600s**.

- **Initial connection time:** The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test:** Tests the interface with custom commands.

If **Custom test** is selected, complete the following:

- The **Commands to run to test**.
- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.

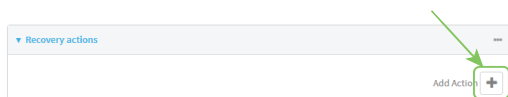
If **TCP connection test** is selected, complete the following:

- **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
- **TCP connect port**: The TCP port to create a TCP connection to.
- **Test another interface's status**: Tests the status of another interface.

If **Test another interface's status** is selected, complete the following:

- **Test interface**: The interface to test.
- **IP version**: The type of IP connection, one of:
  - **Any**: Either the IPv4 or IPv6 connection must be up.
  - **Both**: Both the IPv4 or IPv6 connection must be up.
  - **IPv4**: The IPv4 connection must be up.
  - **IPv6**: The IPv6 connection must be up.
- **Expected status**: The status required for the test to pass.
  - **Up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
  - **Down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

13. Configure the device to reboot when the test fails:
  - a. Click to expand **Recovery actions**.
  - b. Click **+**.



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

- c. Type a **Label** for the recovery action.
  - d. For **Recovery type**, select **Reboot device**.
    - **SureLink test failures**: The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action**: The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
14. (Optional) Configure advanced SureLink parameters:
  - a. Click to expand **Advanced settings**.
  - b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up. (missing or bad snippet)  
The default is 300 seconds.

- c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.(missing or bad snippet)  
The default is 300 seconds.
  - d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.
15. Click **Apply** to save the configuration and apply the change.

### Command line

Active recovery can be configured for both IPv4 and IPv6. These instructions are for IPv4; to configure IPv6 active recovery, replace **ipv4** in the command line with **ipv6**.

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new WAN, or edit an existing one:
  - To create a new WAN, see [Configure a Wide Area Network \(WAN\)](#).
  - To edit an existing WAN, change to the WAN's node in the configuration schema. For example, for a WAN named **my\_wan**, change to the **my\_wan** node in the configuration schema:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Enable SureLink. SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN. It is disabled for IPv6.

```
(config network interface my_wan> ipv4 surelink enable true
(config network interface my_wan)>
```

5. Set the device to reboot when the interface is considered to have failed:

```
(config network interface my_wan ipv4 surelink)> reboot true
(config network interface my_wan ipv4 surelink)>
```

**Note** If both the **restart** and **reboot** parameters are enabled, the **reboot** parameter takes precedence.

6. Add a test target:

```
(config network interface my_wan)> add ipv4 surelink target end
(config network interface my_wan ipv4 surelink target 0)>
```

## 7. Set the test type:

---

```
(config network interface my_wan ipv4 surelink target 0)> test value
(config network interface my_wan ipv4 surelink target 0)>
```

---

where *value* is one of:

- **ping:** Tests connectivity by sending an ICMP echo request to a specified hostname or IP address.

- Specify the hostname or IP address:

---

```
(config network interface my_wan ipv4 surelink target 0)> ping_
host host
(config network interface my_wan ipv4 surelink target 0)>
```

---

- (Optional) Set the size, in bytes, of the ping packet:

---

```
(config network interface my_wan ipv4 surelink target 0)> ping_
size [num]
(config network interface my_wan ipv4 surelink target 0)>
```

---

- **dns:** Tests connectivity by sending a DNS query to the specified DNS server.

- Specify the DNS server. Allowed value is the IP address of the DNS server.

---

```
(config network interface my_wan ipv4 surelink target 0)> dns_
server ip_address
(config network interface my_wan ipv4 surelink target 0)>
```

---

- **dns\_configured:** Tests connectivity by sending a DNS query to the DNS servers configured for this interface.

- **http:** Tests connectivity by sending an HTTP or HTTPS GET request to the specified URL.

- Specify the url:

---

```
(config network interface my_wan ipv4 surelink target 0)> http_
url value
(config network interface my_wan ipv4 surelink target 0)>
```

---

where *value* uses the format **http[s]://hostname[/path]**

- **interface\_up:** The interface is considered to be down based on the interfaces down time, and the amount of time an initial connection to the interface takes before this test is considered to have failed.

- (Optional) Set the amount of time that the interface can be down before this test is considered to have failed:

---

```
(config network interface my_wan ipv4 surelink target 0)>
interface_down_time value
(config network interface my_wan ipv4 surelink target 0)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **parameter name** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> path-param 600s
(config)>
```

---

The default is 60 seconds.

- (Optional) Set the amount of time to wait for an initial connection to the interface before this test is considered to have failed:

---

```
(config network interface my_wan ipv4 surelink target 0)>
interface_timeout value
(config network interface my_wan ipv4 surelink target 0)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **parameter name** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> path-param 600s
(config)>
```

---

The default is 60 seconds.

(Optional) Repeat to add additional test targets.

8. Optional active recovery configuration parameters:

- Move back two levels in the configuration by typing .. ..:

---

```
(config network interface my_wan ipv4 surelink target 0)> .. ..
(config network interface my_wan ipv4 surelink>
```

---

- To configure the device to restart the interface when its connection is considered to have failed:

---

```
(config network interface my_wan ipv4 surelink)> restart enable
(config network interface my_wan ipv4 surelink>
```

---

This is useful for interfaces that may regain connectivity after restarting.

- To configure the device to reboot when the interface is considered to have failed:

---

```
(config network interface my_wan ipv4 surelink)> reboot enable
(config network interface my_wan ipv4 surelink>
```

---

**Note** If both the **restart** and **reboot** parameters are enabled, the **reboot** parameter takes precedence.

- Set the **Interval** between connectivity tests:

---

```
(config network interface my_wan ipv4 surelink)> interval value
(config network interface my_wan ipv4 surelink>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:



---

```
(config network interface my_wan ipv4 surelink)> interval 600s
(config network interface my_wan ipv4 surelink)>
```

---

The default is 15 minutes.

- e. If more than one test target is configured, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

---

```
(config network interface my_wan ipv4 surelink)> success_condition
value
(config network interface my_wan ipv4 surelink)>
```

---

Where *value* is either **one** or **all**.

- f. Set the number of probe attempts before the WAN is considered to have failed:

---

```
(config network interface my_wan ipv4 surelink)> attempts num
(config network interface my_wan ipv4 surelink)>
```

---

The default is **3**.

- g. Set the amount of time that the device should wait for a response to a probe attempt before considering it to have failed:

---

```
(config network interface my_wan ipv4 surelink)> timeout value
(config network interface my_wan ipv4 surelink)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **parameter name** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> path-param 600s
(config)>
```

---

The default is 15 seconds.

9. (Optional) Repeat this procedure for IPv6.
10. Save the configuration and apply the change

---

```
(config network interface my_wan ipv4 surelink)> save
Configuration saved.
>
```

---

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Disable SureLink

If your device uses a private APN with no Internet access or has a restricted WAN connection that doesn't allow DNS resolution, you can disable SureLink connectivity tests. You can also reconfigure SureLink to disable the DNS test and use one or more other tests.



Web

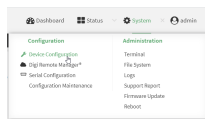
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

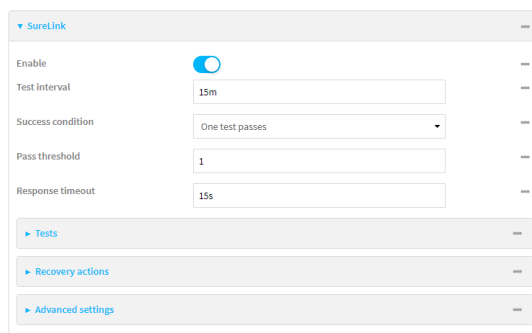
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > Interfaces**.
4. Select the appropriate WAN on which SureLink should be disabled..
5. After selecting the WAN, click **SureLink**.



6. Toggle off **Enable** to disable SureLink.
7. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Change to the WAN's node in the configuration schema. For example, to disable SureLink for the WAN interface:

```
(config)> network interface modem
(config network interface modem)>
```

4. Disable SureLink:

```
(config network interface modem> surelink enable false
(config network interface modem)>
```

5. Save the configuration and apply the change

```
(config network interface my_wwan surelink)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Disable the default DNS test

Alternatively, you can disable the default DNS test for devices that use a private APN with no Internet access, or that have restricted wired WAN connections that do not allow DNS resolution, and configure alternate test.

## Web

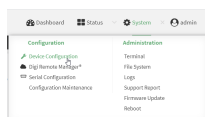
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > Interfaces**.

4. Select the appropriate WAN on which the default DNS test should be disabled..
5. After selecting the WAN, click **SureLink**.

6. Click to expand **Tests**.
7. Click to expand the default **DNS configured** test.
8. Click to toggle off **Enable**.
9. Click **+** to add a new test.

10. Type a **Label** for the test.
11. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.
12. Select the **Test type**.

Available test types:

- **Ping test:** Uses ICMP to determine connectivity.

If **Ping test** is selected, complete the following:

- **Ping target:** The type of target for the ping, one of:
  - **Hostname or IP address** of an external server.
    - **Ping host:** hostname or IP address of the server.
    - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - The **Interface address**.
    - The **Interface DNS** server.
  - **Ping payload size:** The number of bytes to send as part of the ping payload.

- **DNS test:** Performs a DNS query to the named DNS server.

If **DNS test** is selected, complete the following:

- **DNS server:** The IP address of the DNS server.

- **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **HTTP test** is selected, complete the following:

- **Web server:** The URL of the web server.
- **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **Test the interface status** is selected, complete the following:

- **Down time:** The amount of time that the interface is down before the test can be considered to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number{w|d|h|m|s}*.  
For example, to set **Down time** to ten minutes, enter **10m** or **600s**.
- **Initial connection time:** The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number{w|d|h|m|s}*.  
For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test:** Tests the interface with custom commands.

If **Custom test** is selected, complete the following:

- The **Commands to run to test**.
- **TCP connection test:** Tests that the interface can reach a destination port on the configured host.

If **TCP connection test** is selected, complete the following:

- **TCP connect host:** The hostname or IP address of the host to create a TCP connection to.
- **TCP connect port:** The TCP port to create a TCP connection to.
- **Test another interface's status:** Tests the status of another interface.

If **Test another interface's status** is selected, complete the following:

- **Test interface:** The interface to test.
- **IP version:** The type of IP connection, one of:
  - **Any:** Either the IPv4 or IPv6 connection must be up.
  - **Both:** Both the IPv4 or IPv6 connection must be up.
  - **IPv4:** The IPv4 connection must be up.
  - **IPv6:** The IPv6 connection must be up.
- **Expected status:** The status required for the test to pass.
  - **Up:** The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).

- **Down:** The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).
13. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Change to WAN's node in the configuration schema. For example, to disable the default DNS test for an interface named my\_wan:

```
(config)> network interface my_wan
(config network interface my_wan)>
```

4. Disable the default DNS test:

```
(config network interface my_wan)> surelink tests 0 enable false
(config network interface my_wan)>
```

5. Add a new test:

- a. Add a test:

```
(config network interface my_wan)> add surelink tests end
(config network interface my_wan surelink tests 1)>
```

- b. Create a label for the test:

```
(config network interface my_wan surelink tests 1)> label string
(config network interface my_wan surelink tests 1)>
```

- c. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

```
(config network interface my_wan surelink tests 1)> ipv6 true
(config network interface my_wan surelink tests 1)>
```

- d. Set the test type:

```
(config network interface my_wan surelink tests 1)> test value
(config network interface my_wan surelink tests 1)>
```

where *value* is one of:

- **ping:** Uses ICMP to determine connectivity.  
If **ping** is selected, complete the following:

- Set the **ping\_method**:

---

```
(config network interface my_wan surelink tests 1)> ping_
method value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **hostname**: The hostname or IP address of an external server.
  - Set **ping\_host** to the hostname or IP address of the server:

---

```
(config network interface my_wan surelink tests 1)> ping_
host hostname/IP_address
(config network interface my_wan surelink tests 1)>
```

---

- **interface\_gateway**. If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
- **interface\_address**.
- **interface\_dns**: The interface's DNS server.
- Set the number of bytes to send as part of the ping payload:

---

```
(config network interface my_wan ipsec tunnel ipsec_example
surelink tests 1)> ping_size int
(config network interface my_wan surelink tests 1)>
```

---

- **dns**: Performs a DNS query to the named DNS server.

If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

---

```
(config network interface my_wan surelink tests 1)> dns_server
IP_address
(config network interface my_wan surelink tests 1)>
```

---

- **http**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **http** is set, set the URL of the web server.

---

```
(config network interface my_wan surelink tests 1)> http url
(config network interface my_wan surelink tests 1)>
```

---

- **dns\_configured**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface\_up**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **interface\_up** is set, complete the following:

- Set the amount of time that the interface is down before the test can be considered to have failed.

---

```
(config network interface my_wan surelink tests 1)>
interface_down_time value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_down\_time** to ten minutes, enter either **10m** or **600s**:

---

```
(config network interface my_wan surelink tests 1)>
interface_down_time 600s
(config)>
```

---

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

---

```
(config network interface my_wan surelink tests 1)>
interface_timeout value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config network interface my_wan surelink tests 1)>
interface_timeout 600s
(config)>
```

---

- **custom\_test**: Tests the interface with custom commands.

If **custom\_test** is set, set the commands to run to perform the test:

---

```
(config network interface my_wan surelink tests 1)> custom_
test_commands "string"
(config network interface my_wan surelink tests 1)>
```

---

- **tcp\_connection**: Tests that the interface can reach a destination port on the configured host.

If **tcp\_connection** is selected, complete the following:

- Set the hostname or IP address of the host to create a TCP connection to:

---

```
(config network interface my_wan surelink tests 1)> tcp_host
hostname/IP_address
(config network interface my_wan surelink tests 1)>
```

---



- Set the TCP port to create a TCP connection to.

---

```
(config network interface my_wan surelink tests 1)> tcp_port
port
(config network interface my_wan surelink tests 1)>
```

---

- **other**: Tests the status of another interface.

If **other** is selected, complete the following:

- Set the interface to test.
  - i. Use the **?** to determine available interfaces:
  - ii. Set the interface. For example:

---

```
(config network interface my_wan surelink tests 1)> other_
interface /network/interface/eth1
(config network interface my_wan surelink tests 1)>
```

---

- Set the type of IP connection:

---

```
(config network interface my_wan surelink tests 1)> other_ip_
version value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **any**: Either the IPv4 or IPv6 connection must be up.
- **both**: Both the IPv4 or IPv6 connection must be up.
- **ipv4**: The IPv4 connection must be up.
- **ipv6**: The IPv6 connection must be up.
- The status required for the test to pass.

---

```
(config network interface my_wan surelink tests 1)> other_
status value
(config network interface my_wan surelink tests 1)>
```

---

where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

6. Save the configuration and apply the change

---

```
(config network interface my_wan ipv4 surelink)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure a Wide Area Network (WAN)

Configuring a Wide Area Network (WAN) involves configuring the following items:

### **Required configuration items**

- The interface type: **Ethernet**.
- The firewall zone: **External**.
- The network device that is used by the WAN.
- Configure the WAN as a DHCP client.

### **Additional configuration items**

Additional IPv4 configuration:

- The metric for IPv4 routes associated with the WAN.
- The relative weight for IPv4 routes associated with the WAN.
- The IPv4 management priority of the WAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
- The IPv4 Maximum Transmission Unit (MTU) of the WAN.
- When to use DNS servers for this interface.
- Whether to include the Connect EZ device's hostname in DHCP requests.

IPv6 configuration:

- The metric for IPv4 routes associated with the WAN.
- The relative weight for IPv4 routes associated with the WAN.
- The IPv4 management priority of the WAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
- The IPv4 Maximum Transmission Unit (MTU) of the WAN.
  - When to use DNS servers for this interface.
  - Whether to include the Connect EZ device's hostname in DHCP requests.
- MAC address blacklist and whitelist.

SureLink active recovery configuration. See [Configure SureLink active recovery to detect WAN failures](#) for further information.

To create a new WAN or edit an existing WAN:

### **Web**

1. Log into the Connect EZ WebUI as a user with full Admin access rights
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.
3. The **Configuration** window is displayed.
4. Click **Network > Interfaces**.

5. Create the WAN or select an existing WAN:
  - To create a new WAN, for **Add interface**, type a name for the WAN and click **+**.
  - To edit an existing WAN, click to expand the WAN.

The Interface configuration window is displayed.

New WANs are enabled by default. To disable, toggle off **Enable**.
6. For **Interface type**, leave at the default setting of **Ethernet**.
7. For **Zone**, select **External**.
8. For **Device**, select an Ethernet device.
9. Configure IPv4 settings:
  - a. Click to expand **IPv4**.

IPv4 support is enabled by default.
  - b. For **Type**, select **DHCP address**.
  - c. Optional IPv4 configuration items:
    - i. Set the **Metric**.
    - ii. See [Configure WAN priority and default route metrics](#) for further information about metrics.
    - iii. For **Weight**, type the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, **Weight** is used to load balance traffic to the interfaces.
    - iv. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
    - v. Set the **MTU**.
    - vi. For **Use DNS**, select one of the following:
      - **Always**: DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
      - **When primary default route**: Only use the DNS servers provided for this interface when the interface is the primary route.
      - **Never**: Never use DNS servers for this interface.
    - vii. Enable **DHCP Hostname** to instruct the Connect EZ device to include the device's system name with DHCP requests as the Client FQDN option. The DHCP server can then be configured to register the device's hostname and IP address with an associated DNS server.
      - See [RFC4702](#) for further information about DHCP server support for the Client FQDN option.
      - See [Configure system information](#) for information about setting the Connect EZ device's system name.
10. (Optional) Configure IPv6 settings:
  - a. Click to expand **IPv6**.
  - b. **Enable** IPv6 support.
  - c. For **Type**, select **DHCPv6 address**.

- d. For **Prefix length**, type the minimum length of the prefix to assign to this LAN. If the minimum length is not available, then a longer prefix will be used.
  - e. For **Prefix ID**, type the identifier used to extend the prefix to the assigned length. Leave blank to use a random identifier.
  - f. Set the **Metric**.
  - g. See [Configure WAN priority and default route metrics](#) for further information about metrics.
  - h. For **Weight**, type the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, **Weight** is used to load balance traffic to the interfaces.
  - i. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
  - j. Set the **MTU**.
  - k. For **Use DNS**:
    - **Always**: DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
    - **When primary default route**: Only use the DNS servers provided for this interface when the interface is the primary route.
    - **Never**: Never use DNS servers for this interface.
  - l. Enable **DHCP Hostname** to instruct the Connect EZ device to include the device's system name with DHCP requests as the Client FQDN option. The DHCP server can then be configured to register the device's hostname and IP address with an associated DNS server.
    - See [RFC4702](#) for further information about DHCP server support for the Client FQDN option.
    - See [Configure system information](#) for information about setting the Connect EZ device's system name.
11. (Optional) Click to expand **MAC address blacklist**.

Incoming packets will be dropped from any devices whose MAC addresses is included in the **MAC address blacklist**.

    - a. Click to expand **MAC address blacklist**.
    - b. For **Add MAC address**, click **+**.
    - c. Type the **MAC address**.
  12. (Optional) Click to expand **MAC address whitelist**.

If there whitelist entries are specified, incoming packets will only be accepted from the listed MAC addresses.

    - a. Click to expand **MAC address whitelist**.
    - b. For **Add MAC address**, click **+**.
    - c. Type the **MAC address**.
  1. See [Configure SureLink active recovery to detect WAN failures](#) for information about configuring SureLink.
13. Click **Apply** to save the configuration and apply the change.

## Command line

1. Log into the Connect EZ command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Create a new WAN or edit an existing one:

- To create a new WAN named **my\_wan**:

---

```
(config)> add network interface my_wan
(config network interface my_wan)>
```

---

- To edit an existing WAN named **my\_wan**, change to the **my\_wan** node in the configuration schema:

---

```
(config)> network interface my_wan
(config network interface my_wan)>
```

---

4. Set the appropriate firewall zone:

---

```
(config network interface my_wan)> zone zone
(config network interface my_wan)>
```

---

See [Firewall configuration](#) for further information.

5. Select an Ethernet device.
  - a. Enter **device ?** to view available devices and the proper syntax.

---

```
(config network interface my_wan)> device ?
```

Current value:

---

```
(config network interface my_wan)> device
```

---

- b. Set the device for the LAN:

---

```
(config network interface my_wan)> device device
(config network interface my_wan)>
```

---

6. Configure IPv4 settings:

- IPv4 support is enabled by default. To disable:

---

```
(config network interface my_wan)> ipv4 enable false
(config network interface my_wan)>
```

---

- Configure the WAN to be a DHCP client:

---

```
(config network interface my_wan)> ipv4 type dhcp
(config network interface my_wan)>
```

---

- a. Optional IPv4 configuration items:

- i. Set the IP metric:

---

```
(config network interface my_wan)> ipv4 metric num
(config network interface my_wan)>
```

---

See [Configure WAN priority and default route metrics](#) for further information about metrics.

- ii. Set the relative weight for default routes associated with this interface. For multiple active interfaces with the same metric, the weight is used to load balance traffic to the interfaces.

---

```
(config network interface my_wan)> ipv4 weight num
(config network interface my_wan)>
```

---

- iii. Set the management priority. This determines which interface will have priority for central management activity. The interface with the highest number will be used.

---

```
(config network interface my_wan)> ipv4 mgmt num
(config network interface my_wan)>
```

---

- iv. Set the MTU:

---

```
(config network interface my_wan)> ipv4 mtu num
(config network interface my_wan)>
```

---

- v. Configure how to use DNS:

---

```
(config network interface my_wan)> ipv4 use_dns value
(config network interface my_wan)>
```

---

where *value* is one of:

- **always:** DNS will always be used for this WAN; when multiple interfaces have the same DNS server, the interface with the lowest metric will be used for DNS requests.
- **primary:** Only use the DNS servers provided for this interface when the interface is the primary route.
- **never:** Never use DNS servers for this interface.

- b. See [Configure WAN priority and default route metrics](#) for further information about metrics.

7. (Optional) Configure IPv6 settings:

- a. Enable IPv6 support:

---

```
(config network interface my_wan)> ipv6 enable true
(config network interface my_wan)>
```

---

- b. Set the IPv6 type to DHCP:

```
(config network interface my_wan)> ipv6 type dhcpv6
(config network interface my_wan)>
```

- c. Generally, the default settings for IPv6 support are sufficient. You can view the default IPv6 settings by using the question mark (?):

```
(config network interface my_wan)> ipv6 ?
```

IPv6

Parameters	Current Value	
dhcp_hostname	false	DHCP Hostname
enable	true	Enable
metric	0	Metric
mgmt	0	Management priority
mtu	1500	MTU
type	dhcpv6	Type
use_dns	always	Use DNS
weight	10	Weight

Additional Configuration

connection_monitor	Active recovery
--------------------	-----------------

```
(config network interface my_wan)>
```

- d. Modify any of the remaining default settings as appropriate. For example, to change the metric:

```
(config network interface my_wan)> ipv6 metric 1
(config network interface my_wan)>
```

If the minimum length is not available, then a longer prefix will be used.

See [Configure WAN priority and default route metrics](#) for further information about metrics.

8. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show WAN status and statistics



Log into the Connect EZ WebUI as a user with full Admin access rights.

1. From the menu, click **Status**.
2. Under **Networking**, click **Interfaces**.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the **show network** command at the Admin CLI prompt:

```
> show network
```

Interface	Proto	Status	Address
defaultip	IPv4	up	192.168.210.1/24
defaultlinklocal	IPv4	up	169.254.100.100/16
eth2	IPv4	up	192.168.2.1/24
eth2	IPv6	up	fd00:2704::1/48
loopback	IPv4	up	127.0.0.1/8

```
>
```

3. Additional information can be displayed by using the **show network verbose** command:

```
> show network verbose
```

Interface	Proto	Status	Type	Zone	Device	Metric	Weight
defaultip	IPv4	up	static	setup	eth2	10	10
defaultlinklocal	IPv4	up	static	setup	eth2	0	10
eth2	IPv4	up	static	internal	eth2	5	10
eth2	IPv6	up	static	internal	eth2	5	10
loopback	IPv4	up	static	loopback	loopback	0	10

```
>
```

4. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific WAN. For example, to display information about ETH1, enter **show network interface eth1**:

```
> show network interface eth1
```

```
wan1 Interface Status
```

```
Device : eth1
```



---

```

Zone                : external

IPv4 Status         : up
IPv4 Type           : dhcp
IPv4 Address(es)   : 10.10.10.10/24
IPv4 Gateway       : 10.10.10.1
IPv4 MTU           : 1500
IPv4 Metric        : 1
IPv4 Weight        : 10
IPv4 DNS Server(s) : 10.10.10.2, 10.10.10.3

IPv6 Status         : up
IPv6 Type           : dhcpv6
IPv6 Address(es)   : fe00:2404::240:f4ff:fe80:120/64
IPv6 Gateway       : ff80::234:f3ff:ff0e:4320
IPv6 MTU           : 1500
IPv6 Metric        : 1
IPv6 Weight        : 10
IPv6 DNS Server(s) : fd00:244::1, fe80::234:f3f4:fe0e:4320
>

```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a WAN

Follow this procedure to delete any WANs that have been added to the system. You cannot delete the preconfigured WAN, **ETH1**.

### Web

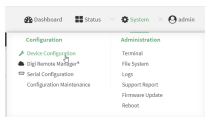
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

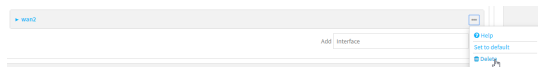
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > Interfaces**.
4. Click the menu icon (...) next to the name of the WAN to be deleted and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **del** command to delete the WAN. For example, to delete a WAN named my\_wan:

```
(config)> del network interface my_wan
```

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status and statistics

You can show SureLink status for all interfaces, or for an individual interface. You can also show Surelink status for ipsec tunnels and OpenVPN clients.

SureLink status is only available from the Admin CLI.

### Command line

## Show SureLink State

To show the current state of SureLink for the Connect EZ device, use the [show surelink state](#) command:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type:

---

```
> show surelink state
```

```
Test on network.interface.eth1.ipv6 with condition: one
dns_configured (n);
```

```
network.interface.eth1.ipv6; -> update_routing_table
ACTION           ATTEMPTS   STATUS
restart_interface 00/01     [FAILED]
update_routing_table 00/01
```

```
Test on network.interface.modem.ipv4 with condition: all
dns_configured (n);
```

```
network.interface.modem.ipv4; -> restart_interface
ACTION           ATTEMPTS   STATUS
update_routing_table 00/03     [ BUSY ]
restart_interface  00/03
reset_modem       00/03
switch_sim        00/03
modem_power_cycle 00/03
restart_interface  00/03
```

```
>
```

---

## Show SureLink status for all interfaces

To show the SureLink status all interfaces, use the [show surelink interface all](#) command:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type :

---

```
> show surelink interface all
```

Interface	Test	Proto	Last Response	Status
eth1	Interface is up	IPv4	32 seconds	Passing
eth1	Interface's DNS servers (DNS)	IPv4	28 seconds	Passing

---

---

eth2	Interface is up	IPv4	21 seconds	Passing
eth2	Interface's DNS servers (DNS)	IPv4	20 seconds	Passing
modem	Interface is up	IPv4	115 seconds	Passing
modem	Interface's DNS servers (DNS)	IPv4	114 seconds	Passing

---

&gt;

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status for a specific interface

To show the SureLink status a specific interface, use the [show surelink interface name name](#) command:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the [show surelink interface name name](#) command to show the Surelink status of a specific interface, for example:

---

```
> show surelink interface name eth1

wan1 Surelink Status
-----
IPv4 Status : Passing
IPv6 Status : Failed

Test                               Proto  Last Response  Status
-----
Interface's DNS servers (DNS)      IPv6   15 seconds     Failed
```

---

&gt;

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status for all IPsec tunnels

To show the SureLink status all IPsec tunnels, use the [show surelink ipsec all](#) command:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the Admin CLI prompt, type :

---

```
> show surelink ipsec all
```

IPsec	Test	Last Response	Status
test	194.43.79.74 (Ping)	29 seconds	Passed
test	194.43.79.75 (Ping)	5 seconds	Passed
test1	194.43.79.74 (Ping)	21 seconds	Failed
test2	194.43.79.75 (Ping)	21 seconds	Waiting for result

```
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status for a specific IPsec tunnel

To show the SureLink status a specific IPsec tunnel, use the [show surelink ipsec tunnel name](#) command:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- Use the [show surelink ipsec tunnel name](#) command to show the Surelink status of a specific tunnel, for example:

---

```
> show surelink ipsec tunnel test
```

IPsec	Test	Last Response	Status
test	194.43.79.74 (Ping)	29 seconds	Passed
test	194.43.79.75 (Ping)	5 seconds	Passed

```
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status for all OpenVPN clients

To show the SureLink status all OpenVPN clients, use the [show surelink openvpn client all](#) command:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the Admin CLI prompt, type :

```
> show surelink openvpn all
```

OpenVPN Client	Test	Last Response	Status
test_client1	194.43.79.74 (Ping)	29 seconds	Passed
test_client1	194.43.79.75 (Ping)	5 seconds	Passed
test_client2	194.43.79.74 (Ping)	21 seconds	Failed
test_client2	194.43.79.75 (Ping)	21 seconds	Waiting for result

```
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SureLink status for a specific OpenVPN client

To show the SureLink status a specific OpenVPN client, use the `show surelink openvpn client name` command:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- Use the `show surelink openvpn client name` command to show the Surelink status of a specific OpenVPN client, for example:

```
> show surelink openvpn client test_client1
```

OpenVPN Client	Test	Last Response	Status
test_client1	194.43.79.74 (Ping)	29 seconds	Passed
test_client1	194.43.79.75 (Ping)	5 seconds	Passed

```
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure a TCP connection timeout

You can configure the number of times an unacknowledged TCP data packet will be retransmitted before the connection is considered lost.

This feature is useful as it allows a backup system to control the serial port if the primary system goes offline, or for the primary system to be able to recover regardless of whether there has been a network disruption.

A low number of retries will end a "stale" connection more quickly than a larger number. The default is 15 retries.

## ≡ Web

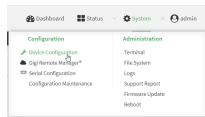
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Set the TCP retry attempts value:
  - a. Click **Network > Advanced**.
  - b. For **TCP retries<sup>2</sup>**, enter the number of times an unacknowledged TCP data packet will be transmitted before the connection is considered lost.
 

**Minimum:** 0

**Maximum:** 255

**Default:** 15
4. Click **Apply** to save the configuration and apply the change.

## Serial port

---

Connect EZ devices have a single serial port that provides access to different features, depending on the serial port mode selection.

### Default serial port configuration

You can review the [default serial port configuration](#) for your device.

### Serial mode options

You can choose a serial mode option for each serial port, depending on the feature that you want to use.

- [Login](#): Allows the port to be used to log into the CLI.
- [Remote Access](#): Provides socket level access to ports.
- [Application](#): Provides access to the serial device from Python applications.
- [PPP dial-in](#): Allows the device to answer Point-to-Point Protocol (PPP) connections over serial ports.
- [RealPort](#): Used in conjunction with the Digi RealPort driver. RealPort can also be configured using the **Digi Navigator**. For more information about configuring RealPort, see [Configure RealPort mode using the Digi Navigator](#).
- [UDP serial](#): Provides access to the serial port using UDP.
- [Modem emulator](#): Allows the device to act as a dial-up modem emulator for handling incoming AT dial-ins.
- [Modbus](#): Allows the device to function as a Modbus protocol gateway.

### View serial port information

- [Show serial port status and statistics](#)
- [Review the serial port message log](#)

### Default serial port configuration

The Connect EZ default serial port configuration is:

- **Enabled**: enabled
- **Serial mode**: Remote access



- **Label:** None
- **Baud rate:** 9600
- **Data bits:** 8
- **Parity:** None
- **Stop bits:** 1
- **Flow control:** None
- **Escape sequence:** None
- **History size:** 0
- **Exclusive access:** disabled
- **Idle timeout:** 0 m

## Baud rate options

The baud rate options are: 50, 75, 110, 134, 150, 200, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400

- **Default baud rate:** 9600
- **Minimum baud rate:** 50
- **Maximum baud rate:** 230400

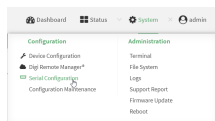
## Configure Login mode for a serial port

**Login** mode allows the user to log into the device through the serial port.

To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

---

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

---

- Click the name of the port that you want to configure.

The screenshot shows a configuration window for a serial port. At the top, there are tabs for 'Port', 'Label', 'Mode', 'Services', and 'Serial Settings'. The 'Port' tab is selected, showing 'Port 1' with a dropdown arrow. The 'Mode' is set to 'Login'. Below this, there is an 'Enable' toggle switch which is turned on, and a 'Label' text input field. There are also expandable sections for 'Serial Settings' and 'Logging Settings'.

The serial port is enabled by default. To disable, toggle off **Enable**.

- For **Mode**, select **Login**.
- Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
- (Optional) For **Label**, enter a label that will be used when referring to this port.
- For **Signalling**, select the electrical signaling interface type used on this serial port:
  - **RS-232**
    - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.
    - For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.
  - **RS-422**
    - Enable **Termination** if you want to enable electrical termination on this serial port.
  - **RS-485**
    - Enable **Termination** if you want to enable electrical termination on this serial port.
    - Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

- Expand **Serial Settings**.

The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

- Baud rate:** For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
  - Max baud rate: **230400**
  - Minimum: **50**

For a complete list, see [Baud rate options](#).
- Data bits:** For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.

- c. **Parity:** For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.
  - d. **Stop bits:** For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.
  - e. **Flow control:** For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
9. Expand **Logging Settings** to configure logging for this serial port.
    - a. To enable logging, click to toggle on **Enable**.
    - b. In the **Log file name** field, enter a descriptive name for the log file.
    - c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
    - d. From the **Type of data to log** list box, specify the type of data that should be saved.
      - **Received**
      - **Transmitted**
      - **Both**
      - **Both with arrows.** This is the default.
    - e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
    - f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

---

**Note** You can review the message log in the **Serial Port Log** page. See [Review the serial port message log](#).

---

10. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode login
(config)>
```

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

6. Set the signaling interface type used on this serial port:

- **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

---

```
(config)> serial port1 rts_toggle true
(config)>
```

---

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 "rts_pre_delay value"
(config)>
```

---

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

- **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

---

```
(config)> serial port1 termination true
(config)>
```

---

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

---

```
(config)> serial port1 full_duplex true
(config)>
```

---

The default is **rs-232**.

7. (Optional) Set a label that will be used when referring to this port.

---

```
(config)> path-paramlabel label
(config)>
```

---

8. Set the baud rate used by the device to which you want to connect:

---

```
(config)> serial port1 baudrate rate
(config)>
```

---

where **rate** is the desired baud rate:

- Default baud rate: **9600**
- Max baud rate: **230400**
- Minimum baud rate: **50**

For a complete list, see [Baud rate options](#).

9. Set the number of data bits used by the device to which you want to connect:

---

```
(config)> serial port1 databits bits
(config)>
```

---

10. Set the type of parity used by the device to which you want to connect:

---

```
(config)> serial port1 parity parity
(config)>
```

---

Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

11. Set the stop bits used by the device to which you want to connect:

---

```
(config)> serial port1 stopbits bits
(config)>
```

---

12. Set the type of flow control used by the device to which you want to connect:

---

```
(config)> serial port1 flow value
(config)>
```

---

where **value** is one of:

- **none**
- **rts/cts**
- **xon/xoff**

13. Configure serial port logging:

- a. Enable serial port logging:

---

```
(config)>serial port1 logging enable true
(config)>
```

---

- b. Set the file name:

---

```
(config)>serial port1 logging filename string
(config)>
```

---

- c. Set the maximum allowed log size for the serial port log when starting the log:

---

```
(config)>serial port1 logging size value
(config)>
```

---

where *value* is the size of the log file in bytes. The default is **65536**.

- d. Specify the data type:

---

```
(config)>serial port1 logging type value
(config)>
```

---

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

- e. Log the time at which data was received or transmitted:

---

```
(config)>serial port1 logging hex true
(config)>
```

---

- f. Log data as hexadecimal values:

---

```
(config)>serial port1 logging timestamp true
(config)>
```

---

14. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

15. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure Remote Access mode for a serial port

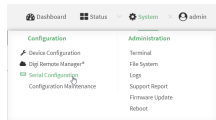
**Remote Access** mode allows for remote access to another device that is connected to the serial port.

To change the configuration to match the serial configuration of the device to which you want to connect:



Web

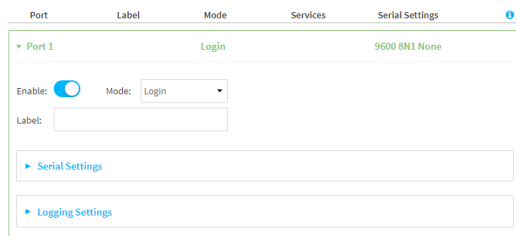
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Serial mode**, select **Remote access**. This is the default.
5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. For **Signalling**, select the electrical signaling interface type used on this serial port:
  - **RS-232**
    - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.
    - For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.
  - **RS-422**
    - Enable **Termination** if you want to enable electrical termination on this serial port.
  - **RS-485**
    - Enable **Termination** if you want to enable electrical termination on this serial port.
    - Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

8. Expand **Serial Settings**.

The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

- a. **Baud rate:** For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
    - Max baud rate: **230400**
    - Minimum: **50**
 For a complete list, see [Baud rate options](#).
  - b. **Data bits:** For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.
  - c. **Parity:** For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.
  - d. **Stop bits:** For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.
  - e. **Flow control:** For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
9. Click to expand **Data Framing**.
- a. Click **Enable** to enable the data framing feature.
  - b. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.
  - c. For **Idle Time**, enter the length of time the device should wait before sending the packet.
  - d. For **End Pattern**, enter the end pattern. The packet is sent when this pattern is received from the serial port.
  - e. Click **Strip End Pattern** if you want to remove the end pattern from the packet before it is sent.
10. Expand **Service Settings**.
- All service settings are disabled by default. Click available options to toggle them to enabled, and set the IP ports as appropriate.

The screenshot shows the 'Service Settings' configuration page. It is organized into three main sections: SSH, TCP, and Telnet. Each section contains a 'Connection Type' dropdown menu and three toggle switches for 'Enable mDNS', 'Enable TCP keepalive', and 'Enable TCP nodelay'. Additionally, there is an 'IP Port' input field for each service. The SSH section has an IP Port of 3001, the TCP section has 4001, and the Telnet section has 2001. All toggle switches are currently turned off.

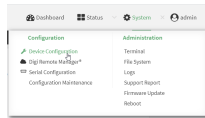
**Note** If the Telnet service is enabled for the serial port, note that the **Telnet Login** option, when enabled, prompts the user to enter Telnet login credentials when accessing the serial port via Telnet. The **Telnet Login** option is enabled by default. To disable this option, navigate to **System > Device Configuration > Authentication > Serial** and disable **Telnet Login**.

For each type of service, you can also configure the access control.

To do this, you need to go to **Device Configuration**:



- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- b. Access the configuration for the appropriate type of service:
- i. Click to expand **Serial**.
  - ii. Click to expand the appropriate serial port.
  - iii. Click to expand the appropriate type of service.
  - iv. Click to expand **Access Control List**.

For example, to set the Access Control List for the SSH connection for serial port 1, click to expand **Serial > Port 1 > SSH connection > Access Control List**:



- To limit access to specified IPv4 addresses and networks:
  - i. Click **IPv4 Addresses**.
  - ii. For **Add Address**, click **+**.
  - iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
    - A single IP address or host name.
    - A network designation in CIDR notation, for example, 192.168.1.0/24.
    - **any**: No limit to IPv4 addresses that can access the service-type.
  - iv. Click **+** again to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:
      - i. Click **IPv6 Addresses**.
      - ii. For **Add Address**, click **+**.
      - iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the service-type.
      - iv. Click **+** again to list additional IP addresses or networks.
    - To limit access to hosts connected through a specified interface on the device:
      - i. Click **Interfaces**.
      - ii. For **Add Interface**, click **+**.
      - iii. For **Interface**, select the appropriate interface from the dropdown.
      - iv. Click **+** again to allow access through additional interfaces.
    - To limit access based on firewall zones:
      - i. Click **Zones**.
      - ii. For **Add Zone**, click **+**.
      - iii. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
      - iv. Click **+** again to allow access through additional firewall zones.
- 11. Expand **Autoconnect Settings**. The autoconnect feature is used to initiate a connection to a remote server to directly access the serial port.
  - a. Click **Enable** to enable the autoconnect feature.
  - b. For **Connection Trigger**, select the option that describes the type of event that should trigger the connection.
 

If you select the **Data received matches a string** option, additional fields display.

    - a. In the **Data Match String** field, enter the received data string that should trigger the connection. The syntax is: *backslash escaped string*
    - b. The **Flush String** option determines whether the match string data sent from the remote server is discarded.
      - **Enable**: Discard the match string data. This is the default.
      - **Disable**: Do not discard the match string data.
  - c. For **Outbound Connection Type**, select the option that describes the method used to initiate the connection.
  - d. For **Destination**, enter the host name or IP address of the remote server. When using SSH, this should be prefixed with the user name and followed by @, for example, **admin@192.168.1.1**.
  - e. For **IP port**, enter the TCP port of the remote server (1-65535).
  - f. Click **Enable TCP keep-alive** to enable TCP keepalive on the connection.
  - g. Click **Enable TCP nodelay** to enable TCP nodelay on the connection.

- h. For **Socket ID string**, type text to be transmitted to the remote server when the socket connects.

12. Expand **Session Settings**.

- a. Enable **Exclusive access** to limit access to the serial port to a single active session. This option is disabled by default. When it is disabled, multiple users can connect using Telnet, TCP, and SSH.
  - b. For **Escape sequence**, type the characters used to start an escape sequence. If no characters are defined, the escape sequence is disabled. The default is **~b**.
  - c. For **History size**, type or select the number of bytes of output from the serial port that are written to buffer. These bytes are redisplayed when a user connects to the serial port. The default is **4000** bytes.
  - d. For **Idle timeout**, type the amount of time to wait before disconnecting due to user inactivity.
13. Expand **Monitor Settings**.
- a. Enable **CTS** to monitor CTS (Clear to Send) changes on this port.
  - b. Enable **DCD** to monitor DCD (Data Carrier Detect) changes on this port.
14. Expand **Logging Settings** to configure logging for this serial port.
- a. To enable logging, click to toggle on **Enable**.
  - b. In the **Log file name** field, enter a descriptive name for the log file.
  - c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
  - d. From the **Type of data to log** list box, specify the type of data that should be saved.
    - **Received**
    - **Transmitted**
    - **Both**
    - **Both with arrows**. This is the default.
  - e. If you want to log the time at which data was received or transmitted, click the **Timestamps** toggle to **Enable**.
  - f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

---

**Note** You can review the message log in the **Serial Port Log** page. See [Review the serial port message log](#).

---

15. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Serial ports is enabled by default. To disable:

---

```
(config)> serial port_number enable false
(config)>
```

---

Command line examples in this section will use port1 for the serial port. However, any port number can be used.

4. Set the mode:

---

```
(config)> serial port1 mode remoteaccess
(config)>
```

---

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

6. Set the signaling interface type used on this serial port:

- **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

---

```
(config)> serial port1 rts_toggle true
(config)>
```

---

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 "rts_pre_delay value"
(config)>
```

---

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

- **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

```
(config)> serial port1 termination true
(config)>
```

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

```
(config)> serial port1 full_duplex true
(config)>
```

The default is **rs-232**.

7. (Optional) Set a label that will be used when referring to this port.

```
(config)>serial port1 label label
(config)>
```

8. Set the baud rate used by the device to which you want to connect:

```
(config)> serial port1 baudrate rate
(config)>
```

where **rate** is the desired baud rate:

- Default baud rate: **9600**
- Max baud rate: **230400**
- Minimum baud rate: **50**

For a complete list, see [Baud rate options](#).

9. Set the number of data bits used by the device to which you want to connect:

```
(config)> serial port1 databits bits
(config)>
```

10. Set the type of parity used by the device to which you want to connect:

```
(config)> serial port1 parity parity
(config)>
```

Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

11. Set the stop bits used by the device to which you want to connect:

```
(config)> serial port1 stopbits bits
(config)>
```

12. Set the type of flow control used by the device to which you want to connect:

---

```
(config)> serial port1 flow value
(config)>
```

---

where *value* is one of:

- **none**
- **rts/cts**
- **xon/xoff**

13. Configure the session settings.

- a. Set the characters used to start an escape sequence:

---

```
(config)>serial port1 escape string
(config)
```

---

If no characters are defined, the escape sequence is disabled. The default is **~b**.

- b. Limit access to the serial port to a single active session:

---

```
(config)>serial port1 exclusive true
(config)
```

---

- c. Set the number of bytes of output from the serial port that are written to buffer. These bytes are redisplayed when a user connects to the serial port.

---

```
(config)>serial port1 history bytes
(config)
```

---

The default is **4000** bytes.

- d. Set the amount of time to wait before disconnecting due to user inactivity:

---

```
(config)>serial port1 idle_timeout value
(config)
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number*{*w*|*d*|*h*|*m*|*s*}**.

For example, to set **idle\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)>serial port1 idle_timeout 600s
(config)
```

---

The default is **15m**.

14. Configure monitor settings.

- a. (Optional) Enable monitoring of CTS (Clear to Send) changes on this port:

---

```
(config)>serial port1 monitor cts true
(config)
```

---

- b. (Optional) Enable monitoring of DCD (Data Carrier Detect) changes on this port:

---

```
(config)>serial port1 monitor dcd true
(config)
```

---

15. (Optional) Configure autoconnect:

- a. Enable autoconnect:

---

```
(config)>serial port1 autoconnect enable true
(config)>
```

---

- b. Set the option that will trigger the connection:

---

```
(config)>serial port1 autoconnect trigger value
(config)>
```

---

where *value* is one of:

- **always**
- **data**
- **dcd**
- **destination**
- **dsr**
- **match**

If **match** is selected:

- i. Set the string that, when received, will trigger the connection:

---

```
(config)>serial port1 autoconnect match_string string
(config)>
```

---

- ii. **flush\_string** is enabled by default, which will discard the matched string from data sent to the server. To disable:

---

```
(config)>serial port1 autoconnect flush_string false
(config)>
```

---

The default is **always**.

- c. Set the option that initiates the connection:

---

```
(config)>serial port1 autoconnect conn_type value
(config)>
```

---

where *value* is one of:

- **ssh**
- **tcp**
- **telnet**
- **tls**
- **tls\_auth**

The default is **tls**.

- d. Set the host name or IP address of the destination server:

```
(config)>serial port1 autoconnect destination hostname/IP_address
(config)>
```

When using SSH, this should be prefixed with the user name and followed by @, for example:

```
(config)>serial port1 autoconnect destination admin@192.168.1.1
(config)>
```

- e. Set the TCP port of the destination server:

```
(config)>serial port1 autoconnect port int
(config)>
```

where *int* is any integer between **1** and **65535**.

- f. To enable TCP keepalive:

```
(config)>serial port1 autoconnect keepalive true
(config)>
```

- g. To enable TCP nodelay:

```
(config)>serial port1 autoconnect nodely true
(config)>
```

- h. Set the text to be transmitted to the remote server when the socket connects:

```
(config)>serial port1 socketid string
(config)>
```

16. (Optional) Configure data framing:

- a. Enable data framing:

```
(config)>serial port1 framing enable true
(config)
```

- b. Set the maximum size of the packet:

```
(config)>serial port1 framing max_count int
(config)
```

The default is **1024**.

- c. Set the length of time the device should wait before sending the packet:

```
(config)>serial port1 framing idle_time value
(config)
```

where *value* is in milliseconds (ms) or seconds (s). The maximum value is **60s**.



- d. Set the end pattern. The packet is sent when this pattern is received from the serial port:

```
(config)>serial port1 framing end_pattern backslash-escaped-string
(config)
```

- e. Set the strip end pattern if you want to remove the end pattern from the packet before it is sent:

```
(config)>serial port1 framing strip_pattern true
(config)
```

17. (Optional) Configure service settings:

- a. Configure SSH settings:

- i. Enable SSH:

```
(config)>serial port1 service ssh enable true
(config)>
```

- ii. Set the port to be used for ssh communications:

```
(config)>serial port1 service ssh port int
(config)>
```

where *int* is any integer between **1** and **65535**. The default is **3001**.

- iii. Enable TCP keep-alive messages:

```
(config)>serial port1 service ssh keepalive true
(config)>
```

- iv. Enable TCP nodelay messages:

```
(config)>serial port1 service ssh nodelay true
(config)>
```

- v. (Optional) Configure access control:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 service ssh acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 service ssh acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add serial port1 service ssh acl interface end
value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add serial port1 service ssh acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

- vi. (Optional) Enable Multicast DNS (mDNS):

---

```
(config)>serial port1 service ssh mdns enable true
(config)>
```

---

b. Configure TCP settings:

i. Enable TCP:

---

```
(config)>serial port1 service tcp enable true
(config)>
```

---

ii. Set the port to be used for ssh communications:

---

```
(config)>serial port1 service tcp port int
(config)>
```

---

where *int* is any integer between **1** and **65535**. The default is **4001**.

iii. Enable TCP keep-alive messages:

---

```
(config)>serial port1 service tcp keepalive true
(config)>
```

---

iv. Set the option that initiates the connection:

---

```
(config)>serial port1 service tcp conn_type value
(config)>
```

---

where *value* is one of:

- **tcp**
- **tls**
- **tls\_auth**

The default is **tls**.

v. Enable TCP nodelay messages:

---

```
(config)>serial port1 service tcp nodelay true
(config)>
```

---

vi. (Optional) Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add serial port1 service tcp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add serial port1 service tcp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add serial port1 service tcp acl interface end
value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add serial port1 service tcp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
```

---

---

```
setup
(config)>
```

---

Repeat this step to include additional firewall zones.

vii. (Optional) Enable Multicast DNS (mDNS):

---

```
(config)>serial port1 service tcp mdns enable true
(config)>
```

---

c. Configure telnet settings:

i. Enable Telnet:

---

```
(config)>serial port1 service telnet enable true
(config)>
```

---

ii. Set the port to be used for Telnet communications:

---

```
(config)>serial port1 service telnet port int
(config)>
```

---

where *int* is any integer between **1** and **65535**. The default is **3001**.

iii. Enable TCP keep-alive messages:

---

```
(config)>serial port1 service telnet keepalive true
(config)>
```

---

iv. Enable TCP nodelay messages:

---

```
(config)>serial port1 service telnet nodelay true
(config)>
```

---

v. (Optional) Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add serial port1 service telnet acl address end
value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add serial port1 service telnet acl address6 end
value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add serial port1 service telnet acl interface end
value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add serial port1 service telnet acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

- vi. (Optional) Enable Multicast DNS (mDNS):

---

```
(config)>serial port1 service telnet mdns enable true
(config)>
```

---

## 18. Configure serial port logging:

## a. Enable serial port logging:

---

```
(config)>serial port1 logging enable true
(config)>
```

---

## b. Set the file name:

---

```
(config)>serial port1 logging filename string
(config)>
```

---

## c. Set the maximum allowed log size for the serial port log when starting the log:

---

```
(config)>serial port1 logging size value
(config)>
```

---

where *value* is the size of the log file in bytes. The default is **65536**.

## d. Specify the data type:

---

```
(config)>serial port1 logging type value
(config)>
```

---

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

## e. Log the time at which date was received or transmitted:

---

```
(config)>serial port1 logging hex true
(config)>
```

---

## f. Log data as hexadecimal values:

---

```
(config)>serial port1 logging timestamp true
(config)>
```

---

## 19. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

20. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

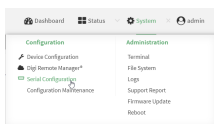
## Configure Application mode for a serial port

**Application** mode provides access to the serial device from Python applications.

To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

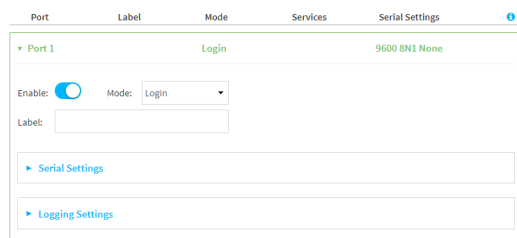
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **Application**. The default is **Login**.
5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. For **Signalling**, select the electrical signaling interface type used on this serial port:
  - **RS-232**
    - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.
    - For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.
  - **RS-422**
    - Enable **Termination** if you want to enable electrical termination on this serial port.



- **RS-485**

- Enable **Termination** if you want to enable electrical termination on this serial port.
- Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

8. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode application
(config)>
```

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

```
(config)> serial port1 altpin true
(config)>
```

6. Set the signaling interface type used on this serial port:

- **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

```
(config)> serial port1 rts_toggle true
(config)>
```

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

```
(config)> serial port1 "rts_pre_delay value
(config)>
```

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

- **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

---

```
(config)> serial port1 termination true
(config)>
```

---

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

---

```
(config)> serial port1 full_duplex true
(config)>
```

---

The default is **rs-232**.

7. (Optional) Set a label that will be used when referring to this port.

---

```
(config)>path-paramlabel label
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure PPP dial-in mode for a serial port

**PPP dial-in** allows the device to answer Point-to-Point Protocol (PPP) connections over serial ports. To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

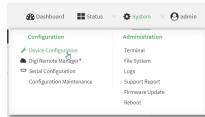
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).

- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

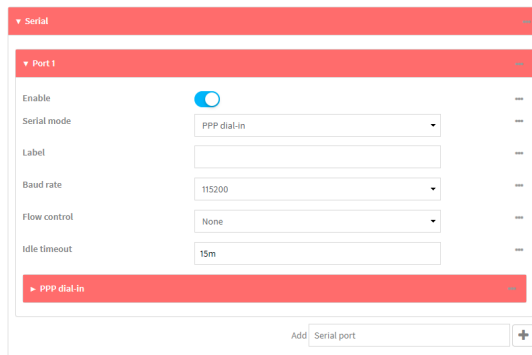
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click to expand the name of the port that you want to configure, for example, **Port 1**.  
The serial port is enabled by default. To disable, toggle off **Enable**.
4. For **Mode**, select **PPP-Dial-in**. The default is **Login**.



5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
  - Max baud rate: **230400**
  - Minimum: **50**

For a complete list, see [Baud rate options](#).
7. For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.
8. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
9. For **Idle timeout**, type the amount of time that the active session can be idle before the session is disconnected.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.
10. Click to expand **PPP dial-in**.

11. For **Local IP address**, type the IP address assigned to this interface.
12. For **Remote IP address**, type the IP address assigned to the remote peer.
13. For **Metric**, set the priority of routes associated with this interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used.
14. For **Default route**, toggle to control whether a default route gets added for the PPP interface. This feature is disabled by default.
15. For **Zone**, select the firewall zone for this interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface.
16. For **Authentication method**, select the method used to authenticate the remote peer. Allowed values are:
  - **None**: No authentication is required.
  - **Automatic**: Attempt to authenticate using CHAP first, and then PAP.
  - **CHAP**: Use Challenge Handshake Authentication Protocol (CHAP) to authenticate.
  - **PAP**: Use Password Authentication Protocol (PAP) to authenticate.

If Automatic, CHAP, or PAP are selected, type the **Username** and **Password** used to authenticate the remote peer.

17. (Optional) Configure the serial port to use a custom PPP configuration file:
  - a. Click to expand **Custom PPP configuration**.
  - b. Click **Enable** to enable the use of a custom PPP configuration file.
  - c. Click **Override** to override the default PPP configuration and only use the custom configuration file.  
If **Override** is not enabled, the custom PPP configuration file is used in addition to the default configuration.
  - d. For **Configuration file**, paste or type the configuration data in the format of a pppd options file. Because the options are passed directly to the pppd command line, they should all be entered on a single line. For example:

---

```
debug lcp-echo-interval 10 lcp-echo-failure 2
```

---

18. (Optional) Configure a script that will be run to prepare the link before PPP negotiations are started:
  - a. Click to expand **Connect script**.
  - b. Click **Enable** to enable the use of a connection script.
  - c. For **Connect script filename**, type the name of the script. Scripts are located in the `/etc/config/serial` directory. An example script, `windows_dun.sh` is provided.  
Example `windows_dun.sh` file:

---

```
#!/bin/sh

# Example connect script for connecting from a PC using a Windows
dial-up
# networking connection with built-in standard 33600 bps modem driver
and phone
# number 123.
```

---

---

```
# The shell's 'read' builtin breaks on newline, so translate incoming
carriage-
# return to newline, and outgoing newline to carriage-return-newline.
stty icrnl onlcr opost

# Read input from the serial port, one line at a time.
while read -r line; do
    case "$line" in
        ATDT123)
            echo "CONNECT" # instruct the peer to start PPP
            exit 0 # start up the local PPP session
            ;;
        AT*)
            echo "OK" # passively accept any other AT command
            ;;
    esac
done
```

---

19. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The serial port is enabled by default. To disable:

---

```
(config)> serial port1 enable false
(config)>
```

---

4. Set the mode:

---

```
(config)> serial port1 mode ppp_dialin
(config)>
```

---

5. (Optional) Set a label that will be used when referring to this port.

---

```
(config)> serial port1 label label
(config)>
```

---

6. Set the baud rate used by the device to which you want to connect:

---

```
(config)> serial port1 baudrate rate
(config)>
```

---

where **rate** is the desired baud rate:

- Default baud rate: **9600**
- Max baud rate: **230400**
- Minimum baud rate: **50**

For a complete list, see [Baud rate options](#).

7. Set the type of flow control used by the device to which you want to connect:

---

```
(config)> serial port1 flow value
(config)>
```

---

where value is one of:

- **none**
- **rts/cts**
- **xon/xoff**

8. Set the amount of time that the active session can be idle before the session is disconnected:

---

```
(config)> serial port1 idle_timeout value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **idle\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> serial port1 idle_timeout 600s
(config)>
```

---

9. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

10. Set the local IP address assigned to this interface:

---

```
(config)> serial port1 ppp_dialin local_address IPv4_address
(config)>
```

---

11. Set the IP address assigned to the remote peer:

---

```
(config)> serial port1 ppp_dialin remote_address IPv4_address
(config)>
```

---

12. The default route is added for the PPP interface is disabled by default. To enable:

---

```
(config)> serial port1 ppp_dialin default_route true
config>
```

---

13. Set the authentication method used to authenticate the remote peer:

---

```
(config)> serial port1 ppp_dialin auth value
(config)>
```

---

where *value* is one of:

- **none**: No authentication is required.
- **auto**: Attempt to authenticate using CHAP first, and then PAP.
- **chap**: Use Challenge Handshake Authentication Protocol (CHAP) to authenticate.
- **pap**: Use Password Authentication Protocol (PAP) to authenticate.

The default is **none**.

If auto, chap, or pap are set, set the username and password used to authenticate the remote peer:

---

```
(config)> serial port1 ppp_dialin username username
(config)> serial port1 ppp_dialin password password
(config)>
```

---

14. Set the priority of routes associated with this interface. If there are multiple active routes that match a destination, then the route with the lowest metric will be used.

---

```
(config)> serial port1 ppp_dialin metric int
(config)>
```

---

The default is **10**.

15. Set the firewall zone for this interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface.
- a. Use the **?** to determine available zones:

---

```
(config)> serial port1 ppp_dialin zone ?
```

Zone: The firewall zone assigned to this interface. This can be used by packet filtering rules and access control lists to restrict network traffic on this interface.

Format:

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

Default value: internal

Current value: internal

```
(config)>
```

---

- b. Set the zone:

---

```
(config)> serial port1 ppp_dialin zone zone
(config)>
```

---

16. (Optional) Configure the serial port to use a custom PPP configuration file:

- a. Enable the use of a custom PPP configuration file:

---

```
(config)> serial port1 ppp_dialin custom enable true
(config)>
```

---

- b. Enable **override** to override the default PPP configuration and only use the custom configuration file:

---

```
(config)> serial port1 ppp_dialin custom override true
(config)>
```

---

If **override** is not enabled, the custom PPP configuration file is used in addition to the default configuration.

- c. Paste or type the configuration data in the format of a pppd options file:

---

```
(config)> serial port1 ppp_dialin custom config_file data
(config)>
```

---

where *data* are one or more pppd command line options. Because the options are passed directly to the pppd command line, they should all be entered on a single line. For example:

---

```
(config)> serial port1 ppp_dialin custom config_file "debug lcp-echo-
interval 10 lcp-echo-failure 2"
(config)>
```

---

17. (Optional) Configure a script that will be run to prepare the link before PPP negotiations are started:

- a. Enable the use of a connection script.

---

```
(config)> serial port1 ppp_dialin connect enable true
(config)>
```

---

- b. Set the name of the script:

---

```
(config)> serial port1 ppp_dialin connect script filename
(config)>
```

---

Scripts are located in the `/etc/config/serial` directory. An example script, `windows_dun.sh` is provided.

Example `windows_dun.sh` file:

---

```
#!/bin/sh

# Example connect script for connecting from a PC using a Windows
```

---



```

dial-up
# networking connection with built-in standard 33600 bps modem driver
and phone
# number 123.

# The shell's 'read' builtin breaks on newline, so translate incoming
carriage-
# return to newline, and outgoing newline to carriage-return-newline.
stty icrnl onlcr opost

# Read input from the serial port, one line at a time.
while read -r line; do
    case "$line" in
        ATDT123)
            echo "CONNECT" # instruct the peer to start PPP
            exit 0 # start up the local PPP session
            ;;
        AT*)
            echo "OK" # passively accept any other AT command
            ;;
    esac
done

```

18. Save the configuration and apply the change

```

(config)> save
Configuration saved.
>

```

19. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

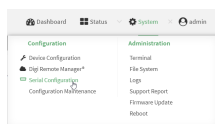
## Configure UDP serial mode for a serial port

The **UDP** serial mode option in the serial port configuration provides access to the serial port using UDP.

To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

- Click to expand the port that you want to configure for UDP serial mode.

The screenshot shows a configuration window for 'Port 1'. At the top, there are tabs for 'Port', 'Label', 'Mode', 'Services', and 'Serial Settings'. The 'Serial Settings' tab is active. Below the tabs, the configuration is as follows:
 

- Port 1** (selected), **Login** (Mode), **9600 8N1 None** (Serial Settings)
- Enable:** A toggle switch is turned on.
- Mode:** A dropdown menu is set to 'Login'.
- Label:** An empty text input field.
- Serial Settings:** A section with a blue arrow pointing right, indicating it is expanded.
- Logging Settings:** A section with a blue arrow pointing right, indicating it is collapsed.

The serial port is enabled by default. To disable, toggle off **Enable**.

- For **Mode**, select **UDP serial**.

The default is **Login**.

- (Optional) For **Label**, enter a label that will be used when referring to this port.
- For **Signalling**, select the electrical signaling interface type used on this serial port:

- **RS-232**

- Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.
    - For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.

- **RS-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **RS-485**

- Enable **Termination** if you want to enable electrical termination on this serial port.
    - Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

- Expand **Serial Settings**.

The screenshot shows the 'Serial Settings' configuration window. It contains the following fields:
 

- Baud Rate:** A dropdown menu set to '115200'.
- Data Bits:** A dropdown menu set to '8'.
- Parity:** A dropdown menu set to 'None'.
- Stop Bits:** A dropdown menu set to '1'.
- Flow Control:** A dropdown menu set to 'None'.

- For **Baud rate**, select the baud rate used by the device to which you want to connect.

- Default baud rate: **9600**
  - Max baud rate: **230400**
  - Minimum: **50**

For a complete list, see [Baud rate options](#).

- b. For **Data bits**, select the number of data bits used by the device to which you want to connect.
  - c. For **Parity**, select the type of parity used by the device to which you want to connect.
  - d. For **Stop bits**, select the number of stop bits used by the device to which you want to connect.
  - e. For **Flow control**, select the type of flow control used by the device to which you want to connect.
8. Expand **Data Framing Settings**.

▼ **Data Framing Settings**

---

Enable:

Maximum Frame Count:  Idle Time:

End Pattern:  Strip End Pattern:

- a. Click to expand **Data Framing**.
    - i. Click **Enable** to enable the data framing feature.
    - ii. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.
    - iii. For **Idle Time**, enter the length of time the device should wait before sending the packet.
    - iv. For **End Pattern**, enter the end pattern. The packet is sent when this pattern is received from the serial port.
    - v. Click **Strip End Pattern** if you want to remove the end pattern from the packet before it is sent.
9. Expand **UDP Serial Settings**.


▼ **UDP Serial Settings**

---

Local Port:

Socket ID String:

**Destinations**

Description	Hostname	Port
 Device1	10.10.xx.xx	1

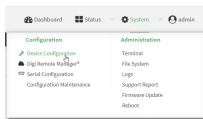
[Add Destination](#)

- a. For **Local port**, enter the UDP port. The default is 4001 or serial port 1, 4002 for serial port 2, etc.

- b. (Optional) For **Socket String ID**, enter a string that should be added at the beginning of each packet.
  - c. For **Destinations**, you can configure the remote sites to which you want to send data. If you do not specify any destinations, the Connect EZ sends new data from the last IP address and port from which data was received. To add a destination:
    - i. Click **Add Destination**. A destination row is added.
    - ii. (Optional) For **Description**, enter a description of the destination.
    - iii. For **Hostname**, enter the host name or IP address of the remote site to which data should be sent.
    - iv. For **Port**, enter the port number of the remote site to which data should be sent.
- You can also configure access control for the serial port.

To do this, you need to go to **Device Configuration**:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- b. Access the configuration for the appropriate type of service:
  - i. Click to expand **Serial**.
  - ii. Click to expand the appropriate serial port.
  - iii. Click to expand **UDP serial**.
  - iv. Click to expand **Access Control List**.

▼ Port 1

Enable

Serial mode UDP serial

Label

Baud rate 115200

Data bits 8

Parity None

Stop bits 1

Flow control None

► Data framing

▼ UDP serial

Local port

▼ Access control list

► IPv4 Addresses

► IPv6 Addresses

► Interfaces

► Zones

- To limit access to specified IPv4 addresses and networks:
  - i. Click **IPv4 Addresses**.
  - ii. For **Add Address**, click **+**.
  - iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
    - A single IP address or host name.
    - A network designation in CIDR notation, for example, 192.168.1.0/24.
    - **any**: No limit to IPv4 addresses that can access the service-type.
  - iv. Click **+** again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
  - i. Click **IPv6 Addresses**.
  - ii. For **Add Address**, click **+**.
  - iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:

- A single IP address or host name.
  - A network designation in CIDR notation, for example, 2001:db8::/48.
  - **any**: No limit to IPv6 addresses that can access the service-type.
- iv. Click **+** again to list additional IP addresses or networks.
- To limit access to hosts connected through a specified interface on the device:
    - i. Click **Interfaces**.
    - ii. For **Add Interface**, click **+**.
    - iii. For **Interface**, select the appropriate interface from the dropdown.
    - iv. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - i. Click **Zones**.
    - ii. For **Add Zone**, click **+**.
    - iii. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - iv. Click **+** again to allow access through additional firewall zones.
10. Expand **Logging Settings** to configure logging for this serial port.
    - a. To enable logging, click to toggle on **Enable**.
    - b. In the **Log file name** field, enter a descriptive name for the log file.
    - c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
    - d. From the **Type of data to log** list box, specify the type of data that should be saved.
      - **Received**
      - **Transmitted**
      - **Both**
      - **Both with arrows**. This is the default.
    - e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
    - f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.
- 
- Note** You can review the message log in the **Serial Port Log** page. See [Review the serial port message log](#).
- 
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The serial port is enabled by default. To disable:

---

```
(config)> serial port1 enable false
(config)>
```

---

4. Set the mode:

---

```
(config)> serial port1 mode udp
(config)>
```

---

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

6. Set the signaling interface type used on this serial port:

- **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

---

```
(config)> serial port1 rts_toggle true
(config)>
```

---

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 "rts_pre_delay value"
(config)>
```

---

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

- **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

---

```
(config)> serial port1 termination true
(config)>
```

---

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

---

```
(config)> serial port1 full_duplex true
(config)>
```

---

The default is **rs-232**.

7. (Optional) Set a label that will be used when referring to this port.

---

```
(config)>serial port1 label label
(config)>
```

---

8. Set the baud rate used by the device to which you want to connect:

---

```
(config)>serial port1 label baudrate rate
(config)>
```

---

where **rate** is the desired baud rate:

- Default baud rate: **9600**
- Max baud rate: **230400**
- Minimum baud rate: **50**

For a complete list, see [Baud rate options](#).

9. Set the number of data bits used by the device to which you want to connect:

---

```
(config)>serial port1 label databits bits
(config)>
```

---

10. Set the type of parity used by the device to which you want to connect:

---

```
(config)>serial port1 label parity parity
(config)>
```

---

Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

11. Set the stop bits used by the device to which you want to connect:

---

```
(config)>serial port1 label stopbits bits
(config)>
```

---

12. Set the type of flow control used by the device to which you want to connect:

---

```
(config)>serial port1 label flow type
(config)
```

---

Allowed values are:



- **none**
- **rts/cts**
- **xon/xoff**

The default is **none**.

13. (Optional) Configure data framing:

a. Enable data framing:

---

```
(config)>serial port1 framing enable true
(config)
```

---

b. Set the maximum size of the packet:

---

```
(config)>serial port1 framing max_count int
(config)
```

---

The default is **1024**.

c. Set the length of time the device should wait before sending the packet:

---

```
(config)>serial port1 framing idle_time value
(config)
```

---

where *value* is in milliseconds (ms) or seconds (s). The maximum value is **60s**.

d. Set the end pattern. The packet is sent when this pattern is received from the serial port:

---

```
(config)>serial port1 framing end_pattern backslash-escaped-string
(config)
```

---

e. Set the strip end pattern if you want to remove the end pattern from the packet before it is sent:

---

```
(config)>serial port1 framing strip_pattern true
(config)
```

---

14. Set the UDP port:

---

```
(config)> serial port1 udp port port
(config)>
```

---

The default is **4001**.

15. (Optional) Enter a string that should be added at the beginning of each packet:

---

```
(config)> serial port1 udp socketid backslash-escaped-string
(config)>
```

---

16. Configure the remote sites to which you want to send data. If you do not specify any destinations, the Connect EZ send new data to the last hostname and port from which data was received. To add a destination:

- i. Add a destination:

```
(config)> add serial port1 udp destination end
(config serial port1 udp destination 0)>
```

- ii. (Optional) Enter a description of the destination:

```
(config serial port1 udp destination 0)> description string
(config serial port1 udp destination 0)>
```

- iii. Set the host name or IP address of the remote site to which data should be sent:

```
(config serial port1 udp destination 0)>hostname hostname-or-IP-
address
(config serial port1 udp destination 0)>
```

- iv. Set the port number of the remote site to which data should be sent:

```
(config serial port1 udp destination 0)> port port
(config serial port1 udp destination 0)>
```

17. (Optional) Configure access control:

- a. Return to the root configuration prompt by typing ...:

```
(config serial port1 udp destination 0)> ...
(config)>
```

- b. Set the Access Control List:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add serial port1 udp acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add serial port1 udp acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add serial port1 udp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add serial port1 udp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

```
Zones: A list of groups of network interfaces that
can be referred to by packet
filtering rules and access control lists.
```

```
Additional Configuration
```

```
-----
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add serial port1 udp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add serial port1 udp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add serial port1 udp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add serial port1 udp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

```
-----
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
-----
```

---

---

```
(config)>
```

---

Repeat this step to include additional firewall zones.

18. Configure serial port logging:

a. Enable serial port logging:

---

```
(config)>serial port1 logging enable true
(config)>
```

---

b. Set the file name:

---

```
(config)>serial port1 logging filename string
(config)>
```

---

c. Set the maximum allowed log size for the serial port log when starting the log:

---

```
(config)>serial port1 logging size value
(config)>
```

---

where *value* is the size of the log file in bytes. The default is **65536**.

d. Specify the data type:

---

```
(config)>serial port1 logging type value
(config)>
```

---

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

e. Log the time at which date was received or transmitted:

---

```
(config)>serial port1 logging hex true
(config)>
```

---

f. Log data as hexadecimal values:

---

```
(config)>serial port1 logging timestamp true
(config)>
```

---

19. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

20. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure Modem emulator mode for a serial port

**Modem emulator** mode allows the device to act as a dial-up modem emulator for handling incoming AT dial-ins.

To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

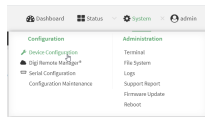
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click to expand the name of the port that you want to configure, for example, **Port 1**.  
The serial port is enabled by default. To disable, toggle off **Enable**.
4. For **Mode**, select **Modem emulator**. The default is **Login**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
  - Max baud rate: **230400**
  - Minimum baud rate: **50**
 For a complete list, see [Baud rate options](#).
7. For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.
8. For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.
9. For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.
10. For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.

11. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
12. For **Idle timeout**, type the amount of time that the active session can be idle before the session is disconnected.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.
13. For **Escape character**, type the character to use in the escape sequence. Enter this character three times, followed by the escape delay and then an AT command to switch from data mode to command mode. The default is the plus sign (+).
14. For **Escape delay**, type the delay between the escape sequence and an AT command to switch from data mode to command mode. The default is **1s**.
15. For **Auto-answer rings**, type the number of rings to wait before auto-answering. Enter **0** (zero) to disable auto-answering.
16. **Command echo** is enabled by default. Commands sent to the port are echoed back to the user. Select to disable this feature.
17. For **Result codes**, select the type of result code that are displayed as responses to commands. Options are:
  - **None**: No result codes are displayed.
  - **Numeric**: Numeric result codes are displayed.
  - **Verbose**: Result codes are displayed in English, for example: OK, ERROR, CONNECT. This is the default.
18. (Optional) Click to expand **Phonebook** and create dial strings that can be used to connect to remote servers.
  - a. Click **+** to add a phone book entry.
  - b. For **Label**, type a descriptive name for the phone book entry.
  - c. (Required) For **Dialstring**, type the string to dial to connect to the remote server.
  - d. (Required) For **Connection destination**, type the hostname or IP address of the remote server.
  - e. (Required) For **Connection port**, type the TCP port of the remote server. Minimum is 1 and maximum is 65535.
19. Expand **TCP connection** to configure TCP connection for this serial port.
  - a. To enable a TCP connection, click to toggle on **Enable**.
  - b. For **Port**, type the TCP port for this service. The default is **4001**.
  - c. Expand **Access control list** to create a list of IP addresses, interfaces, and firewall zones from which this service may be accessed.
    - To limit access to specified IPv4 addresses and networks:
      - i. Click **IPv4 Addresses**.
      - ii. For **Add Address**, click **+**.
      - iii. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:

- A single IP address or host name.
  - A network designation in CIDR notation, for example, 192.168.1.0/24.
  - **any**: No limit to IPv4 addresses that can access the service-type.
- iv. Click **+** again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
    - i. Click **IPv6 Addresses**.
    - ii. For **Add Address**, click **+**.
    - iii. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the service-type.
    - iv. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - i. Click **Interfaces**.
    - ii. For **Add Interface**, click **+**.
    - iii. For **Interface**, select the appropriate interface from the dropdown.
    - iv. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - i. Click **Zones**.
    - ii. For **Add Zone**, click **+**.
    - iii. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - iv. Click **+** again to allow access through additional firewall zones.
- d. Toggle on **Enable mDNS** to enable Multicast DNS (mDNS) reporting for this service. This feature is disabled by default.
20. Expand **Logging Settings** to configure logging for this serial port.
    - a. To enable logging, click to toggle on **Enable**.
    - b. In the **Log file name** field, enter a descriptive name for the log file.
    - c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
    - d. From the **Type of data to log** list box, specify the type of data that should be saved.
      - **Received**
      - **Transmitted**
      - **Both**
      - **Both with arrows**. This is the default.
    - e. If you want to log the time at which date was received or transmitted, click the **Timestamps** toggle to **Enable**.
    - f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.



**Note** You can review the message log in the **Serial Port Log** page. See [Review the serial port message log](#).

21. Click **Apply** to save the configuration and apply the change.

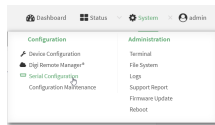
## Configure Modbus mode for a serial port

**Modbus** mode allows you to use the serial port for Modbus. See [Modbus gateway](#).

To change the configuration to match the serial configuration of the device to which you want to connect:

### Web

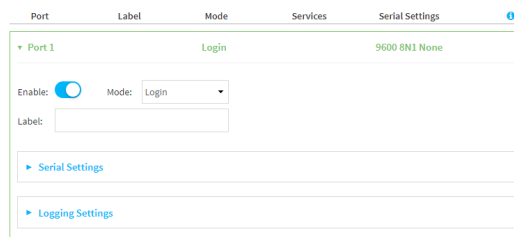
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

3. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **Modbus**.
5. Enable **Alt pin** to use the Alt pin feature. **Alt pin** is disabled by default. If you enable **Alt pin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Alt pin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. For **Signalling**, select the electrical signaling interface type used on this serial port:
  - **RS-232**
    - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.

- For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.
- **RS-422**
  - Enable **Termination** if you want to enable electrical termination on this serial port.
- **RS-485**
  - Enable **Termination** if you want to enable electrical termination on this serial port.
  - Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

#### 8. Expand **Serial Settings**.

The entries in the following fields must match the information for the power controller. Refer to your power controller manual for the correct entries.

- a. **Baud rate:** For **Baud rate**, select the baud rate used by the device to which you want to connect. The default is **9600**.
  - Max baud rate: **230400**
  - Minimum: **50**

For a complete list, see [Baud rate options](#).
- b. **Data bits:** For **Data bits**, select the number of data bits used by the device to which you want to connect. The default is **8**.
- c. **Parity:** For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.
- d. **Stop bits:** For **Stop bits**, select the number of stop bits used by the device to which you want to connect. The default is **1**.
- e. **Flow control:** For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.

#### 9. Click **Apply** to save the configuration and apply the change.

### **Command line**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The serial port is enabled by default. To disable:

---

```
(config)> serial port1 enable false
(config)>
```

---

## 4. Set the mode:

---

```
(config)> serial port1 mode modbus
(config)>
```

---

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

## 6. Set the signaling interface type used on this serial port:

■ **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

---

```
(config)> serial port1 rts_toggle true
(config)>
```

---

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 "rts_pre_delay value"
(config)>
```

---

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

■ **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

■ **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

---

```
(config)> serial port1 termination true
(config)>
```

---

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

---

```
(config)> serial port1 full_duplex true
(config)>
```

---

The default is **rs-232**.

7. (Optional) Set a label that will be used when referring to this port.

---

```
(config)>path-paramlabel label
(config)>
```

---

8. Set the baud rate used by the device to which you want to connect:

---

```
(config)> serial port1 baudrate rate
(config)>
```

---

where **rate** is the desired baud rate:

- Default baud rate: **9600**
- Max baud rate: **230400**
- Minimum baud rate: **50**

For a complete list, see [Baud rate options](#).

9. Set the number of data bits used by the device to which you want to connect:

---

```
(config)> serial port1 databits bits
(config)>
```

---

10. Set the type of parity used by the device to which you want to connect:

---

```
(config)> serial port1 parity parity
(config)>
```

---

Allowed values are:

- **even**
- **odd**
- **none**

The default is **none**.

11. Set the stop bits used by the device to which you want to connect:

---

```
(config)> serial port1 stopbits bits
(config)>
```

---

12. Set the type of flow control used by the device to which you want to connect:

---

```
(config)> serial port1 flow value
(config)>
```

---

where **value** is one of:

- **none**
- **rts/cts**
- **xon/xoff**

13. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

14. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure RealPort mode using the Digi Navigator

You can configure RealPort mode for the Connect EZ using the **Digi Navigator** application. When you install **Digi Navigator** on your computer, the RealPort application is automatically installed as well. Each time the **Digi Navigator** is launched on your computer, any Digi devices that are on the network and support device discovery are discovered by the **Navigator**.

For each of the devices that have been discovered, you can set all serial ports on the device to RealPort mode, and then also enable the RealPort service. The COM ports on your laptop are also configured. These processes ensure that RealPort is configured on the device and on your computer.

### Operating system

The **Digi Navigator** can only be installed on a computer with a Windows OS. If you are using Linux, you can manually install and configure RealPort without **Digi Navigator**. For the Linux installation process, refer to the [Get started: Install RealPort for LINUX](#) in the **RealPort Installation User's Guide**.

## Installation and configuration process

These steps explain how to install and configure the **Digi Navigator**.

Step 1: [Install the Digi Navigator](#)

Step 2: [Configure RealPort on a Digi device from the Digi Navigator](#)

## Digi Navigator features

- [Digi Navigator application features](#)
- [Manage the RealPort configured Digi device list](#)
- [Access the web UI from the Digi Navigator](#)
- [Filter devices for display in the Digi Navigator](#)
- [Access Digi Remote Manager from the Digi Navigator](#)

## Install the Digi Navigator

This section explains how to download and install the **Digi Navigator** application.

---

**Note** Microsoft Visual C++ is required for RealPort and is installed by default during the Digi Navigator install process.

---

1. Navigate to the [Digi Navigator support page](#).

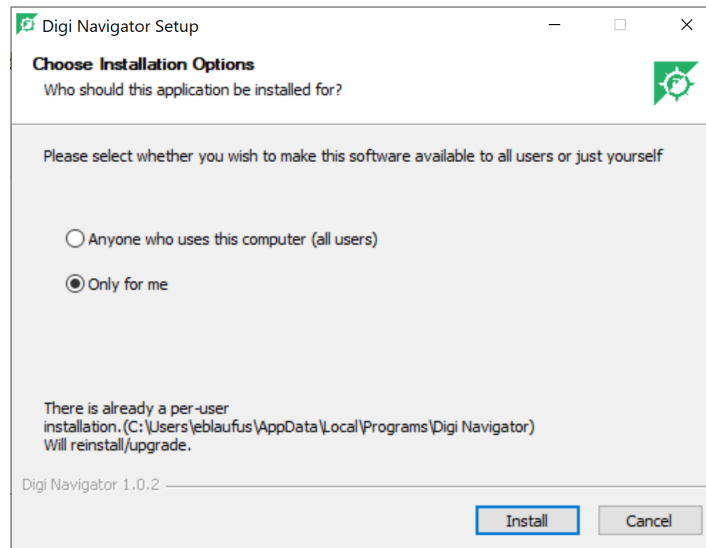
---

**Note** The **Digi Navigator** application can also be downloaded from your device's product support page.

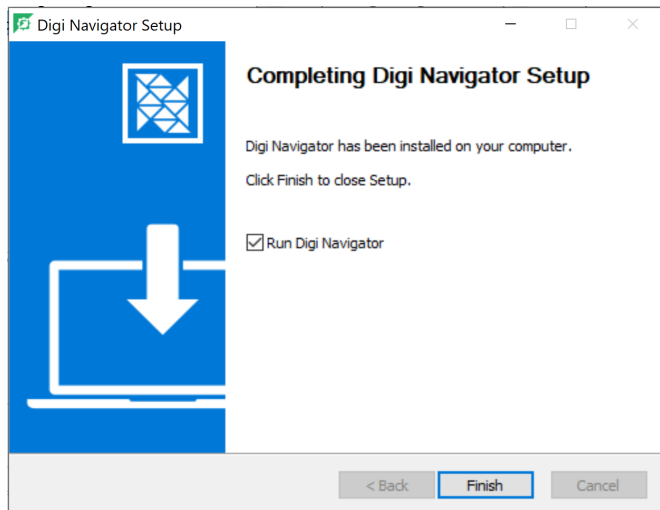
---

2. Scroll down to the **Product Resources** tab, and in the **Drivers & Patches** section, click **Digi Navigator**.

3. From the list box, select the appropriate Microsoft Windows option from the list of driver options.
4. Click the **download** link to download the **Digi Navigator** application.
5. When the download is complete, click on the downloaded .exe file. The **Digi Navigator Setup** wizard displays.
6. Select which user(s) should be able to launch the **Digi Navigator** from this computer after it has been installed:
  - **Anyone who uses this computer (all users):** Any user who logs into this computer can launch the **Digi Navigator**.
  - **Only for me.** Only the user who was logged in to this computer when the **Digi Navigator** was installed can launch the **Digi Navigator**. This is the default.



7. Click **Install**. The **Completing Digi Navigator Setup** screen displays.
8. Choose the **Run Digi Navigator** option if you want to launch the **Navigator** when the installation is complete.



9. Click **Finish** to complete the installation process.

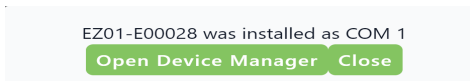
## Configure RealPort on a Digi device from the Digi Navigator

You can configure the Connect EZ to communicate with your computer using RealPort from the **Digi Navigator**. You must enable RealPort on the device and then configure your computer for RealPort. In this step, all serial ports on the device are set to RealPort mode and the RealPort service is enabled. The COM ports on your laptop are also configured.

**Note** You can also manually configure the device for RealPort by logging into the device's web UI. See [Advanced RealPort configuration without using the Digi Navigator](#).

1. [Download and install](#) the **Digi Navigator**.
2. Make sure the Connect EZ is powered connected your local network or computer with an Ethernet cable.
3. Launch the **Digi Navigator**.
4. A list of the devices discovered by the **Digi Navigator** displays. Click on the device that you want to configure. For information about how devices are discovered and how to add a device to the list, see [Digi Navigator device discovery process](#).
5. Configure RealPort on the device.
  - a. Click the **Configure device for RealPort** button. A login screen displays.
  - b. Enter the device's default user name and password in the appropriate fields. The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
  - c. Click **Submit**. A progress message displays.
  - d. When RealPort configuration is complete, the **Success** message displays.
  - e. Click **Close** to close the message.
6. Configure RealPort on your computer. The RealPort service is installed during this process.

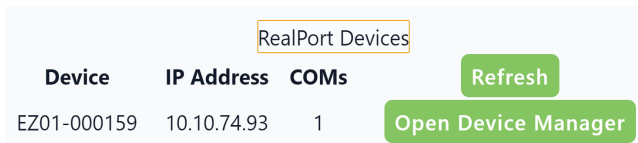
- a. Click **Configure this PC for RealPort**.
- b. From the **Select starting COM** list box, select the COM port that should be configured for RealPort. The first available COM port is selected by default. The number of COM ports configured matches the number of serial ports on the Connect EZ device.
- c. Click **Submit**. A series of progress messages displays.
- d. When the configuration is complete, a message displays.



- e. Determine your final step:
  - **Close**: Click **Close** to close the message. Configuration is complete.
  - **Open Device Manager**: Click **Open Device Manager** if you want to do further configuration to the COM ports. The Windows **Properties** dialog displays.

### Optional activities

- **Verify the RealPort configuration**: If desired, you can verify the RealPort configuration. See [Configure the serial port for RealPort mode](#) and [Configure the RealPort service](#).
- **Review the COM ports that are configured for RealPort**: After RealPort configuration is complete, you can open the Windows **Properties** dialog for the COM ports on your computer that are configured for RealPort from within the **Digi Navigator**.
  1. Launch the **Digi Navigator** if it is not currently open. A list of devices that have RealPort enabled and configured displays in the **RealPort Devices** section at the bottom of the application screen.



2. Click **Open Device Manager** to open the Windows **Properties** dialog and display the COM ports on your computer that are configured for RealPort. For more information, see [Manage the RealPort configured Digi device list](#).

### Digi Navigator device discovery process

When the **Digi Navigator** is installed or launched, it discovers Digi devices that are on your local network and that also support device discovery. A list of the discovered Digi devices are displayed by default in the **Digi Navigator**.

If a Digi device is not on the same network as your computer or the device is undiscoverable, the device is not displayed in the **Digi Navigator**. You can add the device using that device's IP address, and after it has been added, it also displays in the **Digi Navigator**.

The sections below describe different scenarios for discovering devices.



### Device supports Digi Navigator discovery

When the **Digi Navigator** is launched, all discoverable devices are displayed in the application screen. These include devices that are on the same network as your computer and the network has a DHCP server, or devices that have a static IP address.

The **Digi Navigator** uses the HTTPS service by default to discover devices to your network. Other services can be used. See [Services used to discover a device when connected to a network](#).

### Device cannot be discovered by Digi Navigator

If a device is not on the same network as your computer or the device is undiscoverable, you can manually add the device using that device's IP address. See [Specify the IP address to discover a Digi device](#).

### Device supports Digi Navigator discovery, but a DHCP server is not on the network

If the device is directly connected to a computer or connected to a network with no DHCP server, there are two options available to connect to the device:

- **192.168.210.1**: A set up address that is available in the OS. See [Assign a generic IP address to the device](#).
- **169.254.100.100**: An auto-IP address available in the OS. See [Use the autodiscovery protocol to discover a device](#).

---

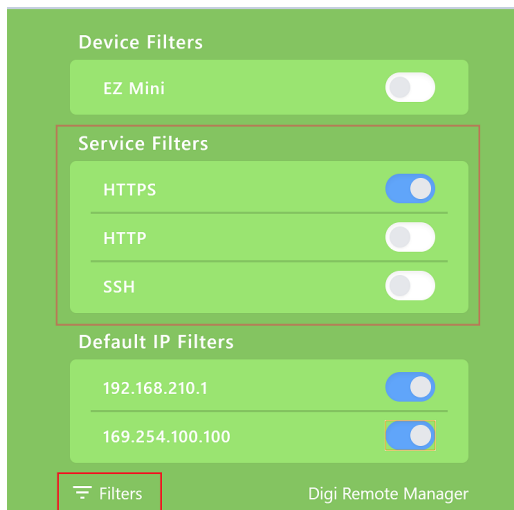
**Note** If you use either of these IP addresses to connect to the device for initial config, you should then set a unique IP address for the device that is appropriate for the network on which it will be deployed.

---

## Services used to discover a device when connected to a network

To discover the IP address for a Digi device connected to your network, the **Digi Navigator** uses the HTTPS service by default. Other services can be used, if needed.

1. Make sure **Digi Navigator** is [installed](#) and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.

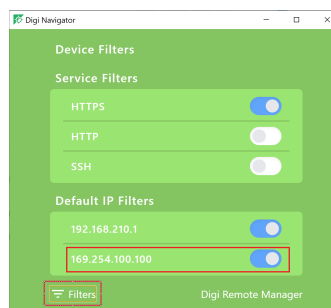


4. In the **Services Filters** section, click the enable button to enable the services that you want to use to find an IP address.
5. Click **Filters** at the bottom of the expanded toolbar to minimize the toolbar and hide the filters.

### ***Use the autodiscovery protocol to discover a device***

If a Digi device is directly connected to a computer or connected to a network with no DHCP server, you can assign an IP address to the Digi device so that the device is automatically discovered.

1. Make sure **Digi Navigator** is [installed](#) and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.



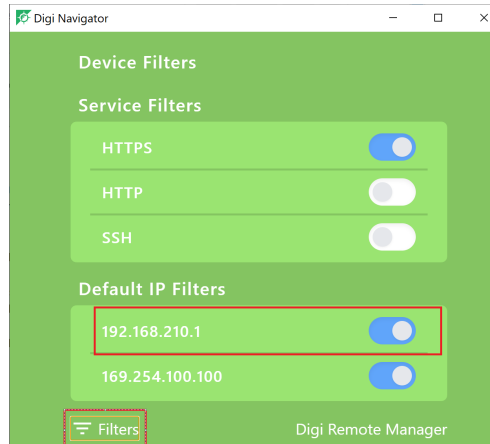
4. In the **Default IP Filters** section, click the enable button for the **169.254.100.100** option.
5. Click **Filters** at the bottom of the expanded toolbar to minimize the toolbar and hide the filters.
6. Log into the device and set a unique IP address for the device that is appropriate for the network on which it will be deployed. See [Define a static IP address](#).

### ***Assign a generic IP address to the device***

If the Connect EZ device is directly connected to a computer or connected to a network with no DHCP server, you can assign a generic IP address to the device. Using this IP address requires you to set this IP address on your computer as well as on the device.

#### **Step 1: Assign a generic IP address to the device**

1. Make sure **Digi Navigator** is [installed](#) and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.

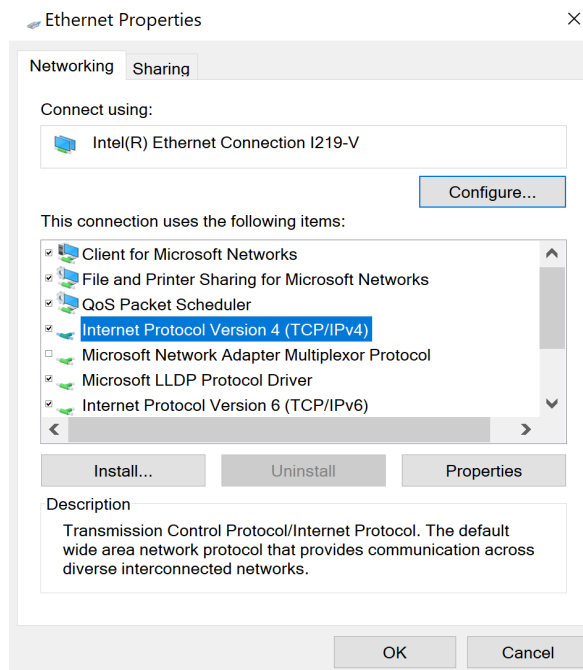


4. In the **Default IP Filters** section, click the enable button for the **192.168.210.1** option.
5. Click **Filters** at the bottom of the expanded toolbar to minimize the toolbar and hide the filters.

### Step 2: Assign the IP address to your computer

You must also manually assign this IP address to your computer to ensure a connection. Both your computer and device must be connected to a private network that does not have a DHCP server.

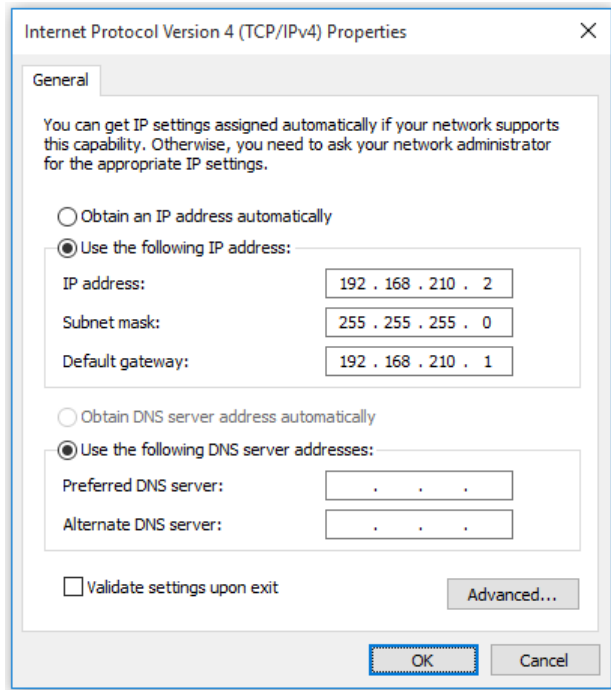
1. Use an Ethernet cable to connect the device and your computer. Both your computer and device must be connected to your private network.
2. On your PC, navigate to the Ethernet network settings dialog.
3. Click the **Internet Protocol Version 4 (TCP/IPv4)** parameter.



4. Click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog appears.
5. Select **Use the following IP address**.

**Note IMPORTANT:** Make note of the current IP address entries for **IP address**, **Subnet mask**, and **Default gateway**. You will need this information to complete the final step of the process.

6. Configure with the following details:
  - **IP address** for PC: 192.168.210.2
  - **Subnet**: 255.255.255.0
  - **Gateway**: 192.168.210.1



7. Click **OK**.
8. Open a browser window.
9. Enter the default gateway IP address to access the device: **192.168.210.1**. The device's login screen displays.
10. Log into the device using the default user name and password. The default user name is **admin** and the default password is printed on the bottom label of the device and on the loose label included in the package. If the defaults do not work, they may have been changed. Confirm this information with your system administrator.
11. Update the IP address for the device.
12. On your PC, revert the IP address information to the original entries.
  - a. Return to the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog.
  - b. Enter the original IP address entries for **IP address**, **Subnet mask**, and **Default gateway**.
  - c. Click **OK**.

### ***Specify the IP address to discover a Digi device***

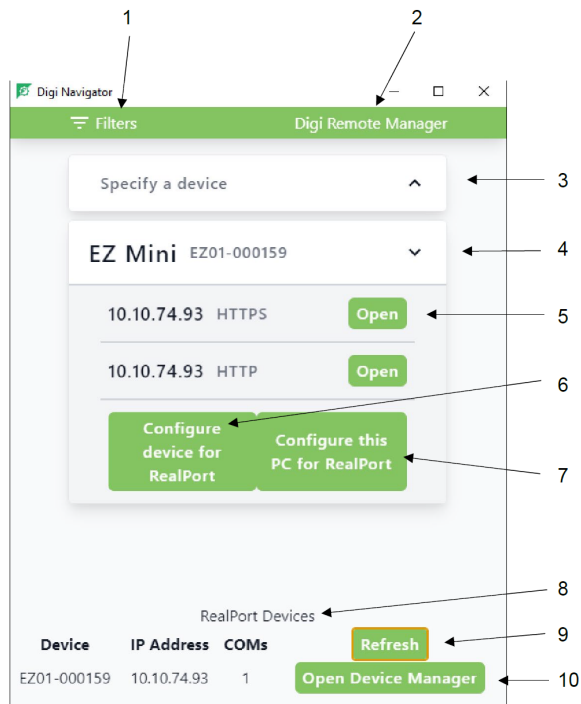
If a Digi device is not on the same network as your computer or the device is undiscoverable, you can manually add the device using that device's IP address.

To add a device, you will need the devices's IP address, and the user name and password for the device.

1. Make sure **Digi Navigator** is **installed** and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Expand the **Specify a device** section.
4. In the **IP Address** field, enter the IP address or host name for the device.
5. Press **Enter**. A dialog displays.
6. Enter the user name and password for the device in the **User name** and **Password** fields.
7. Click **Submit**.
8. The device you just added displays at the bottom of the **Digi Navigator** screen. You can click **Refresh** to update the screen until the device appears.

## Digi Navigator application features

All features of the **Digi Navigator** are available from the main application screen.

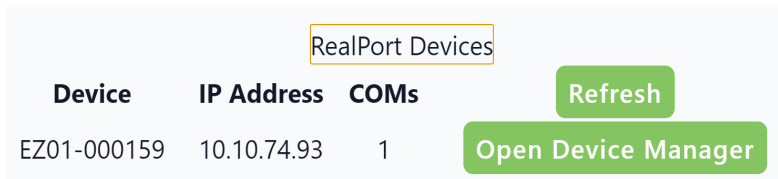


	Item	Description
1	<b>Filters</b>	<p>Click <b>Filters</b> to display the types of filters that can be applied to Digi devices, services, and IP types.</p> <ul style="list-style-type: none"> <li>▪ <b>Device Filters:</b> A list of the Digi device types displays. All types are disabled by default, and when all are disabled, all types are</li> </ul>

	Item	Description
		<p>displayed. To filter the devices by a certain type, click the bar to display only the selected types. See <a href="#">Filter devices for display in the Digi Navigator</a>.</p> <ul style="list-style-type: none"> <li>▪ <b>Services Filters:</b> A list of the services that can be used to discover Digi devices. The <b>HTTPS</b> option is selected by default. Click the enable button to enable the services that you want to use. See <a href="#">Services used to discover a device when connected to a network</a>.</li> <li>▪ <b>Default IP Filters:</b> These specific IP addresses can be used to discover a Digi device that is directly connected to a computer or connected to a network with no DHCP server. <ul style="list-style-type: none"> <li>• <b>192.168.210.1:</b> A set up address that is available in the OS. See <a href="#">Assign a generic IP address to the device</a>.</li> <li>• <b>169.254.100.100:</b> An auto-IP address available in the OS. See <a href="#">Use the autodiscovery protocol to discover a device</a>.</li> </ul> </li> </ul>
2	<b>Digi Remote Manager</b>	Click <b>Digi Remote Manager</b> to launch <b>Digi Remote Manager</b> . See <a href="#">Access Digi Remote Manager from the Digi Navigator</a> .
3	<b>Specify a device</b>	Expand the <b>Specify a device</b> section to enter the IP address of a Digi device. See <a href="#">Specify the IP address to discover a Digi device</a> .
4	<b>List of discovered devices</b>	A list of the Digi devices discovered by the <b>Digi Navigator</b> displays. Expand a device to view additional information. See <a href="#">Digi Navigator device discovery process</a> .
5	<b>Open</b>	Click <b>Open</b> to access the web UI for the Digi device. See <a href="#">Access the web UI from the Digi Navigator</a> .
6	<b>Configure device for Realport</b>	Click <b>Configure device for Realport</b> to configure the Digi device to use RealPort. See <a href="#">Configure RealPort on a Digi device from the Digi Navigator</a> .
7	<b>Configure this PC for RealPort</b>	Click <b>Configure this PC for RealPort</b> to configure your computer to use RealPort. See <a href="#">Configure RealPort on a Digi device from the Digi Navigator</a> .
8	<b>RealPort Devices</b>	Click <b>RealPort Devices</b> at the bottom of the screen to display a list of Digi devices that are configured to use RealPort. See <a href="#">Configure RealPort on a Digi device from the Digi Navigator</a> .
9	<b>Refresh</b>	Click <b>Refresh</b> to update the list of the Digi devices that have RealPort enabled and configured.
10	<b>Open Device Manager</b>	Click <b>Open Device Manager</b> to open the Windows <b>Properties</b> dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device.

### Manage the RealPort configured Digi device list

After you have enabled and configured RealPort on at least one Digi device, a list of configured devices displays at the bottom of the **Digi Navigator**. You can refresh the list and easily access the COM port configuration on your computer.

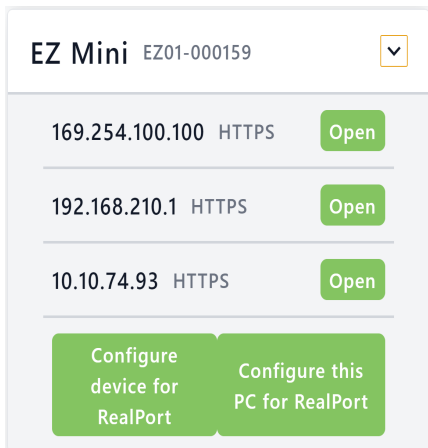


- **Refresh:** Click **Refresh** to update the list of Connect EZ devices that have RealPort enabled and configured.
- **Open Device Manager:** Click **Open Device Manager** to open the Windows **Properties** dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device.

### Access the web UI from the Digi Navigator

You can access the web user interface for a Digi device from the Digi Navigator.

1. Make sure **Digi Navigator** is **installed** and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. From the list of devices shown in the **Digi Navigator**, expand the device you want to access.

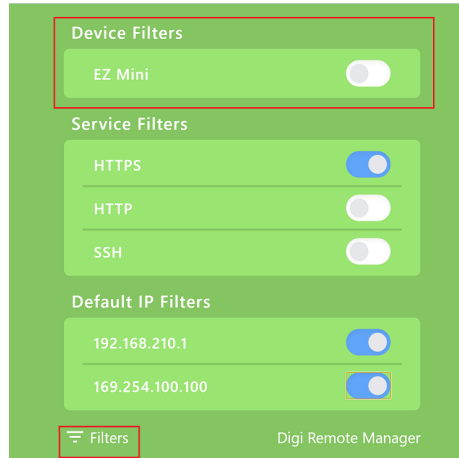


4. Click **Open** next to the IP address you want to use. The login screen for the web UI launches.
  - a. Enter the user name and password for the Connect EZ in the **Username** and **Password** fields.
  - b. Click **Login**.

### Filter devices for display in the Digi Navigator

You can use the **Digi Navigator** filters to determine the types of Digi devices you want to display. Only the devices that are powered on and are discoverable are included.

1. Make sure **Digi Navigator** is [installed](#) and the Connect EZ is powered and connected to your local network or computer with an Ethernet cable.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.



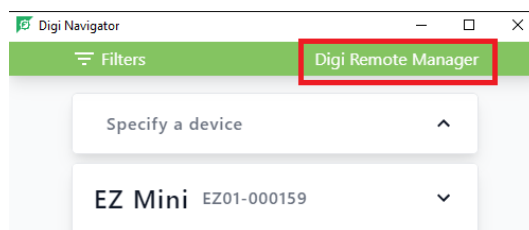
4. In the **Device Filters** section, a list of the Digi device types display. All types are disabled by default, and when all are disabled, all types are displayed.
5. To filter the types that are displayed, click the enable slider for the types you want to display. Only the enabled types will display, and all other types remain disabled and do not display.
6. Click **Filters** at the bottom of the expanded toolbar to minimize the toolbar and hide the filters.

### ***Access Digi Remote Manager from the Digi Navigator***

You can access Digi Remote Manager from the **Digi Navigator**. Within the Remote Manager, you can configure and monitor your Digi devices.

For information about using Digi Remote Manager, refer to the [Digi Remote Manager User Guide](#).

1. Make sure **Digi Navigator** is [installed](#).
2. Launch the **Digi Navigator**.
3. Click the **Digi Remote Manager** link in the toolbar.



4. The **Digi Remote Manager** login screen launches.
  - a. Enter your Remote Manager user name and password.
  - b. Click **Login**.



## Advanced RealPort configuration without using the Digi Navigator

You can configure the Connect EZ to communicate with your computer using RealPort.

### Windows Operating System

This method can be used if your computer has a Windows OS installed and you choose not to use the [Digi Navigator](#) to discover devices and configure RealPort.

To complete the RealPort configuration process for Windows:

**Step 1:** [Download the RealPort driver](#)

**Step 2:** [Configure RealPort on your laptop](#)

**Step 3:** [Configure the serial port for RealPort mode](#)

**Step 4:** [Configure the RealPort service](#)

### Linux Operating System

To complete the RealPort configuration process for Linux OS:

**Step 1:** [Download the RealPort driver](#)

**Step 2:** To complete the RealPort configuration process, refer to the [Get started: Install RealPort for LINUX](#) section in the **RealPort Installation User's Guide**.

### Download the RealPort driver

The first step is to download the RealPort application and save it to a location that you can easily access.

1. Navigate to <https://hub.digi.com/support/products/realport/>.
2. Scroll down to the **Product Resources** tab, and in the **Drivers & Patches** section, click **RealPort Driver**.
3. From the list box, select the appropriate Microsoft Windows option from the list of driver options. The associated RealPort for Windows option displays.
4. Click the **download** link.
5. When the download is complete, navigate to your download folder. The application is in a .zip file.
6. You can leave the .zip file in the download folder, or copy the .zip file and paste it to a location that you can easily access.

### Configure RealPort on your laptop

RealPort must be installed on your laptop, and then RealPort configured for the IP address of each device that should be allowed a RealPort connection.

You will run the RealPort Wizard for each device that you want to configure. RealPort is installed on your laptop the first time that you run the wizard. The installation process is ignored each subsequent time that you run the wizard.

**Before you begin**

- Download RealPort onto your laptop, and make note of the download location. See [Download the RealPort driver](#).
- Have the IP address of the device that you want to configure.

### Step 1: Implement RealPort

1. Navigate to the downloaded Realport .zip file.
2. Open the .zip file.
3. Click on **setup.exe** to launch the RealPort wizard. The **Welcome to the Digi RealPort Setup Wizard** screen displays.
4. If this is not the first time you have run the wizard, select the **Add a New Device** option. If this is the first time running the wizard, no options are available on the screen.
5. Click **Next**. The **Select Device** screen displays.
  - a. From the list of device options, select the **Device not listed** option.
6. Click **Next**. The **Describe the Device** screen displays.
  - a. In the **Device Model Name** field, enter a descriptive name for the device.
  - b. In the **Network Settings** section, select the **IP** option and enter the IP address in the associated field.
  - c. In the **COM Port Settings** section, from the **No. Ports** list box, select the number of physical serial ports that you want to configure. You can specify from 1 to the maximum number of ports available on the device.
  - d. In the **Device Features** section, select both the **Encryption** and **Authentication** options.
7. Click **Finish** to complete the process and close the wizard.

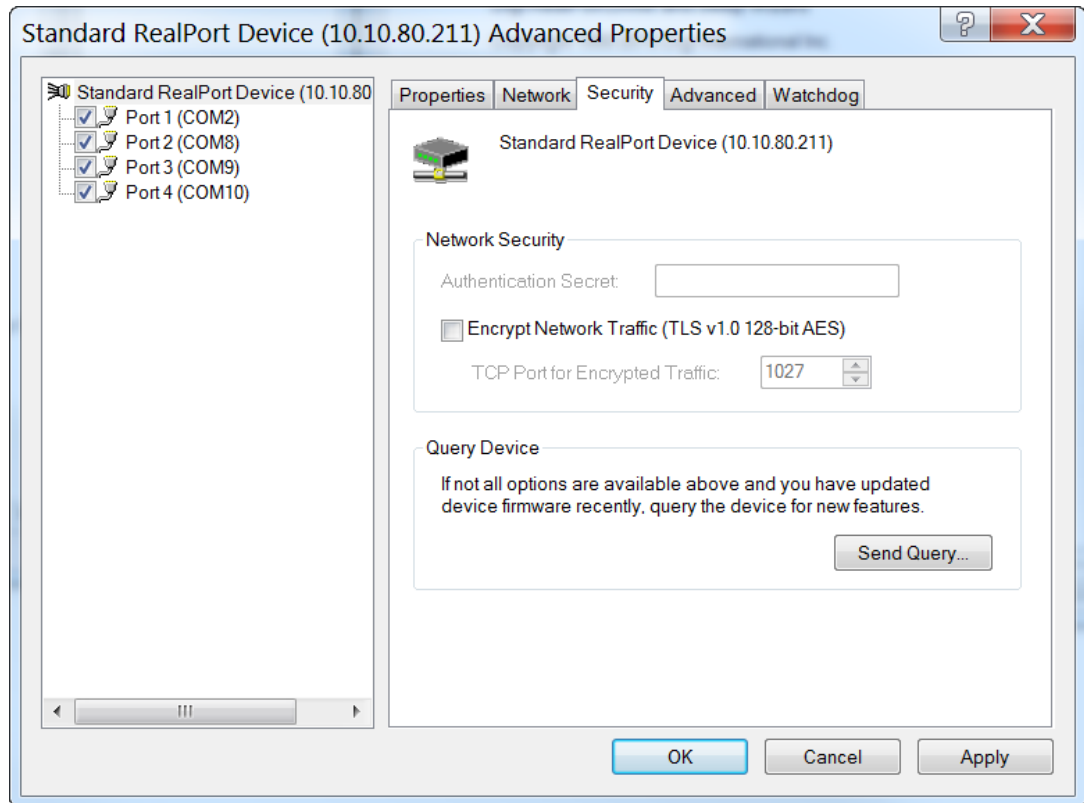
---

**Note** If this is the first time that you have run the RealPort wizard, Realport is installed on your laptop. If it is not the first time or if RealPort is already installed, it is not installed again.

---

### Step 2: Configure a RealPort connection on your laptop for your device

1. Follow the standard Windows process to access the **Device Manager** from your computer's operating system.
2. Select **Multi-port Serial Adapters**.
3. Right-click on your device. Click the **Properties** menu option. The **Properties** dialog appears.
4. Click the **Advanced** tab.
5. Click **Properties**. The **Advanced Properties** dialog appears.
6. Click the **Security** tab.



7. Select the **Encrypt Network Traffic** check box to enable encrypted network traffic. When you select this option, the **TCP Port for Encrypted Traffic** field becomes available.
8. The **TCP Port for Encrypted Traffic** has a default value of **1027**. The entry must match the device's TCP port setting.
9. (Optional) If you want to use authentication, configure the feature.
  - a. From the the **Authentication Method** list box, select the **Shared Secret - SHA256** option.
  - b. Enter the authentication password in the **Shared Secret** field.
10. Click **Apply**.
11. Click **OK** to close the **Advanced Properties** dialog.
12. Click **OK** to close the **Properties** window.

## Configure the serial port for RealPort mode

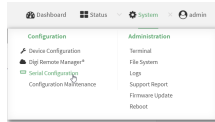
RealPort mode allows you to use Realport.

To change the configuration to match the serial configuration of the device to which you want to connect:

 **Web**

Log into the Connect EZ WebUI as a user with full Admin access rights.

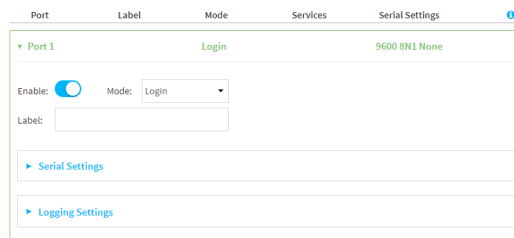
1. On the menu, click **System**. Under **Configuration**, click **Serial Configuration**.



The **Serial Configuration** page is displayed.

**Note** You can also configure the serial port by using **Device Configuration > Serial**. Changes made by using either **Device Configuration** or **Serial Configuration** will be reflected in both.

2. Click the name of the port that you want to configure.



The serial port is enabled by default. To disable, toggle off **Enable**.

3. For **Mode**, select **RealPort**.
4. Select an option from the **Sharing Mode** list box to determine which user(s) can change the port settings, and whether users can receive data from the port.
  - **None**: Only the user that opened the port can change the port settings. All other users are rejected. No other users can receive data from the port. This is the default.
  - **Primary**: Only the user that opened the port can change the port settings. All other users that try to open the port receive all of the data read to the port.
  - **Peer**: Any user that tries to open the port can change the port settings. All users that try to open the port receive all of the data read to the port.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).
7. For **Signalling**, select the electrical signaling interface type used on this serial port:
  - **RS-232**
    - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control.
    - For **RTS Pre-delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**.
    - For **RTS Post-delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**.

- **RS-422**
  - Enable **Termination** if you want to enable electrical termination on this serial port.
- **RS-485**
  - Enable **Termination** if you want to enable electrical termination on this serial port.
  - Enable **Full Duplex** if you want to enable full duplex communication on this serial port.

The default is **RS-232**.

8. Expand **Logging Settings** to configure logging for this serial port.
  - a. To enable logging, click to toggle on **Enable**.
  - b. In the **Log file name** field, enter a descriptive name for the log file.
  - c. For **Log file size**, type the size of the log file. When the log file reaches the size limit, the current file is saved and a new file is created. The default is 65536 bytes.
  - d. From the **Type of data to log** list box, specify the type of data that should be saved.
    - **Received**
    - **Transmitted**
    - **Both**
    - **Both with arrows**. This is the default.
  - e. If you want to log the time at which data was received or transmitted, click the **Timestamps** toggle to **Enable**.
  - f. If you want to log the data as hexadecimal values, click the **Hexadecimal** toggle to **Enable**.

---

**Note** You can review the message log in the **Serial Port Log** page. See [Review the serial port message log](#).

---

9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The serial port is enabled by default. To disable:

---

```
(config)> serial port1 enable false
(config)>
```

---

## 4. Set the mode:

---

```
(config)> serial port1 mode realport
(config)>
```

---

## 5. Set the sharing mode:

---

```
(config)> serial port1 sharing value
(config)>
```

---

where **value** is one of:

- **none**: Only the user that opened the port can change the port settings. All other users are rejected. No other users can receive data from the port. This is the default.
- **peer**: Any user that tries to open the port can change the port settings. All users that try to open the port receive all of the data read to the port.
- **primary**: Only the user that opened the port can change the port settings. All other users that try to open the port receive all of the data read to the port.

## 6. Set the signal mode:

---

```
(config)> serial port1 signal mode value
(config)>
```

---

where **value** is one of:

Set the signaling interface type used on this serial port:

▪ **rs-232**

- Enable **rts\_toggle** if you want to enable RTS toggling during transmission on this serial port. If enabled, this setting overrides RTS\CTS flow control:

---

```
(config)> serial port1 rts_toggle true
(config)>
```

---

- For **rts\_pre\_delay**, enter the amount of time RTS is asserted before starting data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 "rts_pre_delay value
(config)>
```

---

- For **rts\_post\_delay**, enter the amount of time RTS is deasserted before completing data transmission. The time is measured in milliseconds. The default is **0ms**:

---

```
(config)> serial port1 rts_post_delay value
(config)>
```

---

▪ **rs-422**

- Enable **Termination** if you want to enable electrical termination on this serial port.

- **rs-485**

- Enable **termination** if you want to enable electrical termination on this serial port:

---

```
(config)> serial port1 termination true
(config)>
```

---

- Enable **full\_duplex** if you want to enable full duplex communication on this serial port:

---

```
(config)> serial port1 full_duplex true
(config)>
```

---

The default is **rs-232**.

7. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default. If you enable **Altpin** in EIA-232 mode, the DCD and DSR signals are swapped. This allows use of DCD with 8-wire cables. **Altpin** has no impact on 422 or 485 mode. For more information, see [Serial connector pinout](#).

---

```
(config)> serial port1 altpin true
(config)>
```

---

8. Set a label that will be used when referring to this port.

---

```
(config)> serial port1 label label
(config)>
```

---

9. (Optional) Set a label that will be used when referring to this port.

---

```
(config)> serial port1 label label
(config)>
```

---

10. Configure serial port logging:

- a. Enable serial port logging:

---

```
(config)>serial port1 logging enable true
(config)>
```

---

- b. Set the file name:

---

```
(config)>serial port1 logging filename string
(config)>
```

---

- c. Set the maximum allowed log size for the serial port log when starting the log:

---

```
(config)>serial port1 logging size value
(config)>
```

---

where *value* is the size of the log file in bytes. The default is **65536**.

- d. Specify the data type:

---

```
(config)>serial port1 logging type value
(config)>
```

---

where *value* is one of:

- received
- transmitted
- both
- arrows. This is the default.

- e. Log the time at which data was received or transmitted:

---

```
(config)>serial port1 logging hex true
(config)>
```

---

- f. Log data as hexadecimal values:

---

```
(config)>serial port1 logging timestamp true
(config)>
```

---

11. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the RealPort service

After you have configured RealPort mode on the Connect EZ, you must enable and configure the RealPort service. When this step is complete, all of the serial ports on the Connect EZ are configured to use the RealPort service.

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System > Configuration > Device Configuration**.
3. Expand **Services**.
4. Expand **RealPort**.
5. Click **Enable** to enable the RealPort service.
6. For **RealPort Server Port**, enter **1027**. This is the default.
7. For **Minimum TLS version**, select the minimum TLS version that the RealPort service will accept. The default is TLS version 1.0.
8. Enable **Encryption** to enable encryption of data. This is enabled by default.
9. (Optional) Configure the authentication method the RealPort server uses to authenticate clients.
  - a. From the **Authentication Method** list box, select the **Shared Secret - SHA256** option.
  - b. For **Shared Secret**, enter the authentication password to ensure secure communication. Leave this field blank to disable authentication.



10. Enable **Exclusive Mode** to ensure that any connection from an IP address is closed when opening a new connection from the same IP address. This is disabled by default.
11. Enable **RealPort Keepalive** to send RealPort keepalive packets. This is enabled by default.
12. Enable **TCP Port Keepalive** to send TCP keepalive packets. This is disabled by default.
13. Enable **Device Initiated connections** so users can remotely connect to serial devices as if they had a native COM/TTY port on their PC. This is disabled by default.
14. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. RealPort is enabled by default. To disable:

---

```
(config)> service realport enable false
(config)>
```

---

4. Set the RealPort server port.

---

```
(config)> service realport port value
(config)>
```

---

where **value** is the port you want to use for the RealPort service. The default is **1027**.

5. Set the select the minimum TLS version that the RealPort service will accept:

---

```
(config)> service realport minimum_tls_version value
(config)>
```

---

where **value** is one of:

- **TLS-1\_0**. This is the default.
- **TLS-1\_1**
- **TLS-1\_2**
- **TLS-1\_3**

6. Data encryption is enabled by default. To disable:

---

```
(config)> service realport encryption false
(config)>
```

---

7. (Optional) Configure authentication.

---

```
(config)> service realport auth value
(config)>
```

---

where **value** is one of:

- **none**: Do not use authentication. This is the default.
- **shared\_secret\_sha256**: You must also define the authentication password to ensure secure communication. Leave this field blank to disable authentication.

---

```
(config)> service realport auth shared_secret_sha256 value
(config)
```

---

where **value** is the authentication password.

8. Exclusive mode is disabled by default. This mode ensures that any connection from an IP address is closed when opening a new connection from the same IP address. To enable:

---

```
(config)> service realport exclusive true
(config)
```

---

9. Use RealPort keepalive to send RealPort keepalive packets. This is enabled by default. To disable:

---

```
(config)> service realport realport_keepalive false
(config)>
```

---

10. TCP port keepalive to send TCP keepalive packets is disabled by default. To enable:

---

```
(config)> service realport tcp_keepalive true
(config)>
```

---

11. Device initiated connections allow users to remotely connect to serial devices as if they had a native COM/TTY port on their PC. This is disabled by default. To enable:

---

```
(config)> service realport device_initiated_enable true
(config)>
```

---

12. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

13. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Disconnect a user from a serial port

From the **Serial Status** page, you can disconnect any users connected to a serial port configured for one of these modes: [Login](#), [Remote Access](#), [PPP Dial-in](#), or [Modem Emulator](#).

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **Status > Connections > Serial**. The **Serial Status** page displays.

3. Find the port for which you want to disconnect one or more users. Verify that the port is configured for one of the following modes: [Login](#), [Remote Access](#), [PPP Dial-in](#), or [Modem Emulator](#).
4. Click the down arrow next to the user name in the **Users** column to display a pop-up box.
5. A list of the users currently connected to the port display in the pop-up box. Information about each user's connection displays. If more than one user is connected, a check box displays for each user.
  - **User:** The user's log in name or a connection type, such as Telnet, TCP, or SSH.
  - **Remote IP:** The user's IP address.
  - **Connected:** The length of time that the user has been connected to the port. The time is measured in seconds.
  - **Idle:** The length of time that connection has been idle. The time is measured in seconds.
6. Determine the user(s) that you want to disconnect.
  - If only one user is listed, that user will be selected for the disconnect by default.
  - If more than one user is connected to the port, by default the check box for each user is selected. Click on a check box to deselect a user. Click **All** to deselect or select all of of the users.
7. Click **Disconnect**. The single user or set of selected users are disconnected from the serial port.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. (Optional) Review the users currently connected to the port.

---

```
show serial port
>
```

---

Where *port* is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.

3. (Optional) Review information about the disconnect command.

---

```
> system serial disconnect ?
>
```

---

4. Disconnect a specific user from a port.

---

```
>system serial disconnect port remoteip STRING user STRING
>
```

---

Where *port* is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.

Enter one or both of the following:

- *remoteip STRING* The remote IP address to disconnect.
  - *user*: The user name of the user that you want to disconnect.
5. Disconnect all users from a port.

---

```
system serial disconnect port
>
```

---

Where *port*: is the port number you want to review, such as "port2"; a string, such as "console"; or the name of a user-configured serial port, such as USB.

6. Type **exit** to exit the Admin CLI. Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show serial port status and statistics

To show the status and statistics for the serial port:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the main menu, click **Status > Connections > Serial**. The **Serial Status** page displays. See [Serial Status page](#) for information about the features in this page.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **show serial** command:

---

```
> show serial
```

Label	Port	Enable	Mode	Baudrate
Serial 1	port1	true	login	9600

---




```
>
```

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Serial Status page

The **Serial Status** page contains status information about all of the serial ports available on the device.

To navigate to the **Serial Status** page, log into the device's web UI and click **Status > Connection > Serial**.

Item	Description
 configuration icon	Click the  (configuration) icon in the upper right corner of the page to access the <b>Serial Configuration</b> page. See <a href="#">Serial port</a> for more information.
<b>Status</b>	Displays the connection status. <ul style="list-style-type: none"> <li>▪ <b>CONNECTED:</b> A telnet, terminal, SSH, or TCP session is active.</li> <li>▪ <b>DISABLED:</b> The port is not enabled.</li> <li>▪ <b>NO SIGNAL:</b> CTS or DCD is not active on the port.</li> </ul>
<b>Port</b>	A list of the ports on the device. The port number and name displays as a link when the port is configured for remote access. You can click the port number or name to connect to the port in the terminal page. <ol style="list-style-type: none"> <li>1. Click the link to connect to the port in the terminal page.</li> <li>2. In the terminal screen, enter <code>~b?</code> to display additional commands. See <a href="#">Access the terminal screen from the web UI</a> for more information about the commands.</li> </ol> While you are connected to the terminal, the port status displays in the <b>Status</b> column as <b>CONNECTED</b> , and the name of the user logged into the device displays in the <b>User</b> column. <b>Console port</b>
<b>Label</b>	A description for the port. You can change this from the <b>Serial Configuration</b> page. Click the  (configuration) icon in the upper right corner of the page to access that page. The port number and name displays as a link when the port is configured for remote access. You can click the port number or name to connect to the port in the terminal page. See the description for <a href="#">Port</a> (above) for more information.
<b>Log</b>	If configured, you can open the <b>Serial Port Log</b> page for that port. Options are: <ul style="list-style-type: none"> <li>▪ <b>Green Log button:</b> The serial port mode selected for the port supports serial port logging, and logging is enabled. Click the <b>Log</b> button to open the <b>Serial Port Log</b> page for that port. See <a href="#">Review the serial port message log</a> for information about that page.</li> <li>▪ <b>Gray Log button:</b> The serial port mode selected for the port supports serial port logging, but logging is not enabled.</li> <li>▪ <b>No button:</b> The serial port mode selected for the port does not support serial port logging.</li> </ul>
<b>User</b>	When the port is connected to a Telnet, terminal, SSH, or TCP connection the name of the user logged into the device displays. See the description for <a href="#">Port</a> (above) for more information. If a serial port is configured for one of these modes: <a href="#">Login</a> , <a href="#">Remote Access</a> , <a href="#">PPP Dial-in</a> , or <a href="#">Modem Emulator</a> , you can disconnect one or more users from the serial port using the <b>Disconnect</b> feature. See <a href="#">Disconnect a user from a serial port</a> .

Item	Description
<b>TX/RX Bytes</b>	Displays the total number of bytes that have been transmitted and received.
<b>Signals</b>	Indicates the types of communication that the device is ready to send. DCD: Carrier Detected CTS: Clear to Send DTR: Data Terminal Ready RTS: Ready to Dend

## Review the serial port message log

Serial port messages can be reviewed from the **Serial Port Log** page.

A serial port message log is created and saved when serial port logging has been enabled and configured for one of the following serial port modes: [Login](#), [Remote Access](#), [RealPort](#), or [UDP Serial](#). You can view the log file from the **Log** column in the **Serial Status** page.

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the main menu, click **Status**
3. Under **Connections**, click **Serial**. The **Serial Status** page displays.
4. If a green **Log** button is displayed, the serial port mode selected for the port supports serial port logging, and logging is enabled. Click the **Log** button to open the **Serial Port Log** page for that port. The **Serial port log** window displays.

---

**Note** If the **Log** button is gray, the serial port mode selected for the port supports serial port logging, but logging is not enabled. If there is no **Log** button, the serial port mode selected for the port does not support serial port logging.

---

5. Review the messages in the window.
  - Click **Refresh** to refresh the log display.
  - Click **Download** to download the serial port log to your local device. The log file is saved to the /opt/serial directory. Because this is being save to the device's memory, you should use serial logging for diagnostic purposes, rather than having it permanently enabled.
  - Click **Restart** to clear and restart the serial port log.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To show the serial port's contents and logging status:

---

```
> system serial show port-number
Logging is active on port-number
>
```

---

3. To save the log to your local device:

---

```
> system serial save port-number path
>
```

---

If a relative path is provided, `/etc/config/serial` will be used as the root directory for the path and file. (Required)

The log file is saved to the `/opt/serial` directory. Because this is being save to the device's memory, you should use serial logging for diagnostic purposes, rather than having it permanently enabled.

4. To clear and restart the log:

---

```
> system serial clear port-number
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Virtual Private Networks (VPN)

---

Virtual Private Networks (VPNs) are used to securely connect two private networks together so that devices can connect from one network to the other using secure channels.

This chapter contains the following topics:

IPsec .....	177
OpenVPN .....	242
Generic Routing Encapsulation (GRE) .....	283
Dynamic Multipoint VPN (DMVPN) .....	305
L2TP .....	312
L2TPv3 Ethernet .....	324
MACsec .....	330
WireGuard VPN .....	332



## IPsec

IPsec is a suite of protocols for creating a secure communication link—an IPsec tunnel—between a host and a remote IP network or between two IP networks across a public network such as the Internet.

### IPsec data protection

IPsec protects the data being sent across a public network by providing the following:

---

**Data origin authentication**

Authentication of data to validate the origin of data when it is received.

**Data integrity**

Authentication of data to ensure it has not been modified during transmission.

**Data confidentiality**

Encryption of data sent across the IPsec tunnel to ensure that an unauthorized device cannot read the data.

**Anti-Replay**

Authentication of data to ensure an unauthorized device has not injected it into the IPsec tunnel.

---

### IPsec mode

The Connect EZ supports the **Tunnel** mode. With the **Tunnel** mode, the entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet. **Transport** mode is not currently supported.

### IPsec modes

IPsec can run in two different modes: **Tunnel** and **Transport**.

---

**Tunnel**

The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.

**Transport**

Only the payload of the IP packet is encrypted and/or authenticated. The IP header is left untouched. This mode has limitations when using an authentication header, because the IP addresses in the IP header cannot be translated (for example, with Network Address Translation (NAT), as it would invalidate the authentication hash value.

---

### Internet Key Exchange (IKE) settings

IKE is a key management protocol that allows IPsec to negotiate the security associations (SAs) that are used to create the secure IPsec tunnel. Both IKEv1 and IKEv2 are supported.

SA negotiations are performed in two phases, known as **phase 1** and **phase 2**.

#### **Phase 1**

In phase 1, IKE creates a secure authenticated communication channel between the device and the peer (the remote device which is at the other end of the IPsec tunnel) using the configured pre-shared key and the Diffie-Hellman key exchange. This creates the IKE SAs that are used to encrypt further IKE communications.

For IKEv1, there are two modes for the phase 1 negotiation: **Main mode** and **Aggressive mode**. IKEv2 does not use these modes.

---

**Main mode**

Main mode is the default mode. It is slower than aggressive mode, but more secure, in that all sensitive information sent between the device and its peer is encrypted.

**Aggressive mode**

Aggressive mode is faster than main mode, but is not as secure as main mode, because the device and its peer exchange their IDs and hash information in clear text instead of being encrypted.

Aggressive mode is usually used when one or both of the devices have a dynamic external IP address.

---

**Phase 2**

In phase 2, IKE negotiates the SAs for IPsec. This creates two unidirectional SAs, one for each direction. Once the phase 2 negotiation is complete, the IPsec tunnel should be fully functional.

**IPsec and IKE renegotiation**

To reduce the chances of an IPsec tunnel being compromised, the IPsec SAs and IKE SA are renegotiated at a regular interval. This results in different encryption keys being used in the IPsec tunnel.

**Authentication****Client authentication**

XAUTH (extended authentication) pre-shared key authentication mode provides additional security by using client authentication credentials in addition to the standard pre-shared key. The Connect EZ device can be configured to authenticate with the remote peer as an XAUTH client.

**RSA Signatures**

With RSA signatures authentication, the Connect EZ device uses a private RSA key to authenticate with a remote peer that is using a corresponding public key.

**Certificate-based Authentication**

X.509 certificate-based authentication makes use of private keys on both the server and client which are secured and never shared. Both the server and client have a certificate which is generated with their respective private key and signed by a Certificate Authority (CA).

The Connect EZ implementation of IPsec can be configured to use X.509 certificate-based authentication using the private keys and certificates, along with a root CA certificate from the signing authority and, if available, a Certificate Revocation List (CRL).

**Configure an IPsec tunnel**

Configuring an IPsec tunnel with a remote device involves configuring the following items:

### Required configuration items

- **IPsec tunnel configuration items:**

- A name for the tunnel.

---

**Note** If the tunnel name is more than eight characters, the name will be truncated in the underlying network interface to the first six characters followed by three digits, incrementing from 000. This affects any custom scripts or firewall rules that may be trying to adjust the tunnel's interface or routing table entries.

---

- The mode: either tunnel or transport.
- Enable the IPsec tunnel.  
The IPsec tunnel is enabled by default.
- The firewall zone of the IPsec tunnel.
- The routing metric for routes associated with this IPsec tunnel.
- The authentication type and pre-shared key or other applicable keys and certificates.  
If SCEP certificates will be selected as the Authentication type, create the SCEP client prior to configuring the IPsec tunnel. See [Configure a Simple Certificate Enrollment Protocol client](#) for instructions.
- The local endpoint type and ID values, and the remote endpoint host and ID values.

- **IKE configuration items**

- The IKE version, either IKEv1 or IKEv2.
  - Whether to initiate a key exchange or wait for an incoming request.
  - The IKE mode, either main aggressive.
  - The IKE authentication protocol to use for the IPsec tunnel negotiation during phase 1 and phase 2.
  - The IKE encryption protocol to use for the IPsec tunnel negotiation during phase 1 and phase 2.
  - The IKE Diffie-Hellman group to use for the IPsec tunnel negotiation during phase 1 and phase 2.
- Enable dead peer detection and configure the delay and timeout.
  - Destination networks that require source NAT.
  - Active recovery configuration. See [Configure SureLink active recovery for IPsec](#) for information about IPsec active recovery.

### Additional configuration items

The following additional configuration settings are not typically configured to get an IPsec tunnel working, but can be configured as needed:

- Determine whether the device should use UDP encapsulation even when it does not detect that NAT is being used.
- If using IPsec failover, identify the primary tunnel during configuration of the backup tunnel.
- The Network Address Translation (NAT) keep alive time.
- The protocol, either Encapsulating Security Payload (ESP) or Authentication Header (AH).

- The management priority for the IPsec tunnel interface. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
- Enable XAUTH client authentication, and the username and password to be used to authenticate with the remote peer.
- Enable Mode-configuration (MODECFG) to receive configuration information, such as the private IP address, from the remote peer.
- Disable the padding of IKE packets. This should normally not be done except for compatibility purposes.
- Destination networks that require source NAT.
- Depending on your network and firewall configuration, you may need to add a packet filtering rule to allow incoming IPsec traffic.
- **Tunnel and key renegotiating**
  - The lifetime of the IPsec tunnel before it is renegotiated.
  - The amount of time before the IKE phase 1 lifetime expires.
  - The amount of time before the IKE phase 2 lifetime expires
  - The lifetime margin, a randomizing amount of time before the IPsec tunnel is renegotiated.

## ≡ Web

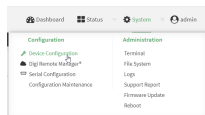
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

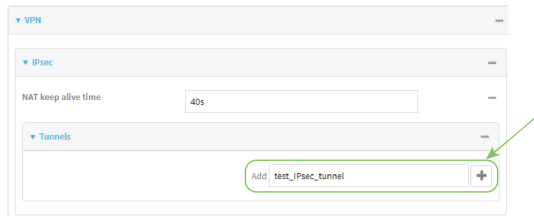
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



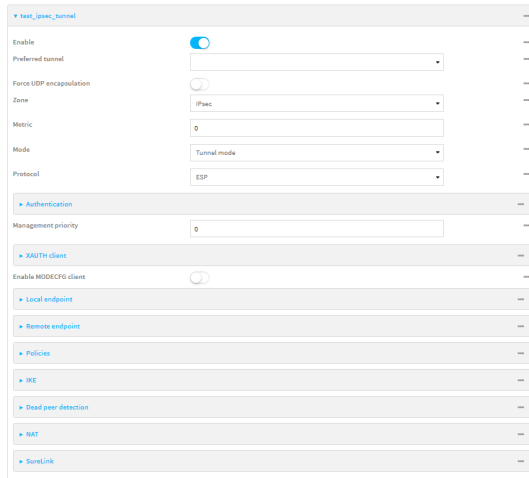
The **Configuration** window is displayed.

3. Click **VPN > IPsec**.
4. Click to expand **Tunnels**.

- For **Add IPsec tunnel**, type a name for the tunnel and click **+**.



The new IPsec tunnel configuration is displayed.



- The IPsec tunnel is enabled by default. To disable, toggle off **Enable**.
- (Optional) **Preferred tunnel** provides an optional mechanism for IPsec failover behavior. See [Configure IPsec failover](#) for more information.
- (Optional) Enable **Force UDP encapsulation** to force the tunnel to use UDP encapsulation even when it does not detect that NAT is being used.
- For **Zone**, select the firewall zone for the IPsec tunnel. Generally this should be left at the default of **IPsec**.

---

**Note** Depending on your network configuration, you may need to add a packet filtering rule to allow incoming traffic. For example, for the **IPsec** zone:

- Click to expand **Firewall > Packet filtering**.
- For **Add packet filter**, click **+**.
- For **Label**, type **Allow incoming IPsec traffic**.
- For **Source zone**, select **IPsec**.

Leave all other fields at their default settings.

---

10. For **Metric**, enter or select the priority of routes associated with this IPsec tunnel. When more than one active route matches a destination, the route with the lowest metric is used.  
The metric can also be used in tandem with SureLink to configure IPsec failover behavior. See [Configure IPsec failover](#) for more information.
11. For **Mode**, select **Tunnel mode**. **Transport mode** is not currently supported.
12. Select the Mode, either:
  - **Tunnel mode**: The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.
  - **Transport mode**: Only the payload of the IP packet is encrypted and/or authenticated. The IP header is unencrypted.
13. Select the **Protocol**, either:
  - **ESP** (Encapsulating Security Payload): Provides encryption as well as authentication and integrity.
  - **AH** (Authentication Header): Provides authentication and integrity only.
14. **Strict routing** is disabled by default. Toggle on to enable.  
Strict routing makes IPsec behave like a policy-based VPN, rather than a route-based VPN.
15. Click to expand **Authentication**.

- a. For **Authentication type**, select one of the following:
  - **Pre-shared key**: Uses a pre-shared key (PSK) to authenticate with the remote peer.
    - i. Type the **Pre-shared key**.
  - **Asymmetric pre-shared keys**: Uses asymmetric pre-shared keys to authenticate with the remote peer.
    - i. For **Local key**, type the local pre-shared key. This must be the same as the remote key on the remote host.
    - ii. For **Remote key**, type the remote pre-shared key. This must be the same as the local key on the remote host.



- b. Click to expand **ID**.
  - i. Select the ID type:
    - **Auto**: The ID will be automatically determined from the value of the tunnels endpoints.
    - **Raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack. For **Raw ID value**, type the ID that will be passed.
    - **Any**: Any ID will be accepted.
    - **IPv4**: The ID will be interpreted as an IP address and sent as an ID\_IPV4\_ADDR IKE identity.  
For **IPv4 ID value**, type an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.
    - **IPv6**: The ID will be interpreted as an IP address and sent as an ID\_IPV6\_ADDR IKE identity.  
For **IPv6 ID value**, type an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.
    - **RFC822/Email**: The ID will be interpreted as an RFC822 (email address).  
For **RFC822 ID value**, type the ID in internet email address format.
    - **FQDN**: The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID\_FQDN IKE identity.  
For **FQDN ID value**, type the ID as an FQDN.
    - **KeyID**: The ID will be interpreted as a Key ID and sent as an ID\_KEY\_ID IKE identity.  
For **KEYID ID value**, type the key ID.
    - **MAC address**: The device's primary MAC address will be used as the ID and sent as a ID\_KEY\_ID IKE identity.
    - **Serial number**: The device's serial number will be used as the ID and sent as a ID\_KEY\_ID IKE identity.
20. Click to expand **Remote endpoint**.
  - a. For **IP version**, select either **IPv4** or **IPv6**.
  - b. For **Hostname list selection**, select one of the following:
    - **Round robin**: Attempts to connect to hostnames sequentially based on the list order.
    - **Random**: Randomly selects an IPsec peer to connect to from the hostname list.
    - **Priority ordered**: Selects the first hostname in the list that is resolvable.
  - c. Click to expand **Hostname**.
    - i. Click **+** next to **Add Hostname**.
    - ii. For **Hostname**, type a hostname or IPv4 address. If your device is not configured to initiate the IPsec connection (see **IKE > Initiate connection**), you can also use the keyword **any**, which means that the hostname is dynamic or unknown.
    - iii. Click **+** again to add additional hostnames.



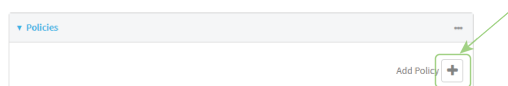
d. Click to expand **ID**.

## i. Select the ID type:

- **Auto:** The ID will be automatically determined from the value of the tunnels endpoints.
- **Raw:** Enter an ID and have it passed unmodified to the underlying IPsec stack. For **Raw ID value**, type the ID that will be passed.
- **Any:** Any ID will be accepted.
- **IPv4:** The ID will be interpreted as an IPv4 address and sent as an ID\_IPV4\_ADDR IKE identity. For **IPv4 ID value**, type an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.
- **IPv6:** The ID will be interpreted as an IPv6 address and sent as an ID\_IPV6\_ADDR IKE identity. For **IPv6 ID value**, type an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.
- **RFC822/Email:** The ID will be interpreted as an RFC822 (email address). For **RFC822 ID value**, type the ID in internet email address format.
- **FQDN:** The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID\_FQDN IKE identity. For **FQDN ID value**, type the ID as an FQDN.
- **KeyID:** The ID will be interpreted as a Key ID and sent as an ID\_KEY\_ID IKE identity. For **KEYID ID value**, type the key ID.
- **MAC address:** The device's primary MAC address will be used as the ID and sent as a ID\_KEY\_ID IKE identity.
- **Serial number:** The device's serial number will be used as the ID and sent as a ID\_KEY\_ID IKE identity.

21. Click to expand **Policies**.

Policies define the network traffic that will be encapsulated by this tunnel.

a. Click **+** to create a new policy.

The new policy configuration is displayed.

- b. Click to expand **Local traffic selector**.

The screenshot shows the 'Local traffic selector' configuration panel. It includes the following fields:

- Type:** A dropdown menu with 'Address' selected.
- Address:** A text input field.
- Protocol:** A dropdown menu with 'Any' selected.
- Port:** A text input field with 'any' entered.

- c. For **Type**, select one of the following:
- **Address:** The address of a local network interface.  
For **Address**, select the appropriate interface.
  - **Network:** The subnet of a local network interface.  
For **Address**, select the appropriate interface.
  - **Custom network:** A user-defined network.  
For **Custom network**, enter the IPv4 address and optional netmask.
  - **Request a network:** Requests a network from the remote peer.
  - **Dynamic:** Uses the address of the local endpoint.
- d. For **Protocol**, select one of the following:
- **Any:** Matches any protocol.
  - **TCP:** Matches TCP protocol only.
  - **UDP:** Matches UDP protocol only.
  - **ICMP:** Matches ICMP requests only.
  - **Other protocol:** Matches an unlisted protocol.  
If **Other protocol** is selected, type the number of the protocol.
- e. For **Port**, type the port matching criteria.  
Allowed values are a port number, a range of port numbers, or **any**.
- f. (Optional) Click to expand **Remote traffic selector**.

The screenshot shows the 'Remote traffic selector' configuration panel. It includes the following fields:

- Remote network:** A text input field.
- Protocol:** A dropdown menu with 'Any' selected.
- Port:** A text input field with 'any' entered.

- g. For **Remote network**, enter the IP address and optional netmask of the remote network.
- h. For **Protocol**, select one of the following:
- **Any:** Matches any protocol.
  - **TCP:** Matches TCP protocol only.
  - **UDP:** Matches UDP protocol only.
  - **ICMP:** Matches ICMP requests only.
  - **Other protocol:** Matches an unlisted protocol.  
If **Other protocol** is selected, type the number of the protocol.

- i. For **Port**, type the port matching criteria.

Allowed values are a port number, a range of port numbers, or **any**.

## 22. Click to expand **IKE**.

The screenshot shows a configuration window for IKE. The 'IKE' section is expanded, revealing several settings:

- IKE version:** A dropdown menu set to 'IKEv1'.
- Initiate connection:** A toggle switch that is turned on (blue).
- Mode:** A dropdown menu set to 'Main mode'.
- Enable padding:** A toggle switch that is turned on (blue).
- Phase 1 lifetime:** A text input field containing '3h'.
- Phase 2 lifetime:** A text input field containing '1h'.
- Lifetime margin:** A text input field containing '9m'.

Below these settings are two expandable sections: 'Phase 1 Proposals' and 'Phase 2 Proposals', each with a right-pointing arrow and a minus sign.

- a. For **IKE version**, select either IKEv1 or IKEv2. This setting must match the peer's IKE version.
- b. **Initiate connection** instructs the device to initiate the key exchange, rather than waiting for an incoming request. This must be disabled if **Remote endpoint** > **Host name** is set to **any**.
- c. For **Mode**, select either **Main mode** or **Aggressive mode**.
- d. For **IKE fragmentation**, select one of the following:
  - **If supported by the peer:** Send oversized IKE messages in fragments, if the peer supports receiving them.
  - **Always:** Always send IKEv1 messages in fragments. For IKEv2, this option is equivalent to **If supported by the peer**.
  - **Never:** Do not send oversized IKE messages in fragments.
  - **Accept:** Do not send oversized IKE messages in fragments, but announce support for fragmentation to the peer.

The default is **Always**.

- e. For **Enable padding**, click to disable the padding of IKE packets. This should normally not be disabled except for compatibility purposes.
- f. For **Phase 1 lifetime**, enter the amount of time that the IKE security association expires after a successful negotiation and must be re-authenticated.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Phase 1 lifetime** to ten minutes, enter **10m** or **600s**.
- g. For **Phase 2 lifetime**, enter the amount of time that the IKE security association expires after a successful negotiation and must be rekeyed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Phase 2 lifetime** to ten minutes, enter **10m** or **600s**.

- h. For **Lifetime margin**, enter a randomizing amount of time before the IPsec tunnel is renegotiated.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Lifetime margin** to ten minutes, enter **10m** or **600s**.
  - i. Click to expand **Phase 1 Proposals**.
    - i. Click **+** to create a new phase 1 proposal.
    - ii. For **Cipher**, select the type of encryption.
    - iii. For **Hash**, select the type of hash to use to verify communication integrity.
    - iv. For **Diffie-Hellman group**, select the type of Diffie-Hellman group to use for key exchange.
    - v. You can add additional Phase 1 proposals by clicking **+** next to **Add Phase 1 Proposal**.
  - j. Click to expand **Phase 2 Proposals**.
    - i. Click **+** to create a new phase 2 proposal.
    - ii. For **Cipher**, select the type of encryption.
    - iii. For **Hash**, select the type of hash to use to verify communication integrity.
    - iv. For **Diffie-Hellman group**, select the type of Diffie-Hellman group to use for key exchange.
    - v. You can add additional Phase 2 proposals by clicking **+** next to **Add Phase 2 Proposal**.
23. (Optional) Click to expand **Dead peer detection**. Dead peer detection is enabled by default. Dead peer detection uses periodic IKE transmissions to the remote endpoint to detect whether tunnel communications have failed, allowing the tunnel to be automatically restarted when failure occurs.
- a. To enable or disable dead peer detection, click **Enable**.
  - b. For **Delay**, type the number of seconds between transmissions of dead peer packets. Dead peer packets are only sent when the tunnel is idle.
  - c. For **Timeout**, type the number of seconds to wait for a response from a dead peer packet before assuming the tunnel has failed.
24. (Optional) Click to expand **NAT** to create a list of destination networks that require source NAT.
- a. Click **+** next to **Add NAT destination**.
  - b. For **Destination network**, type the IPv4 address and optional netmask of a destination network that requires source NAT. You can also use **any**, meaning that any destination network connected to the tunnel will use source NAT.
25. See [Configure SureLink active recovery for IPsec](#) for information about IPsec **Active recovery**.
26. (Optional) Click **Advanced** to set various IPsec-related time out, keep alive, and related values.
27. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add an IPsec tunnel. For example, to add an IPsec tunnel named **ipsec\_example**:

---

```
(config)> add vpn ipsec tunnel ipsec_example
(config vpn ipsec tunnel ipsec_example)>
```

---

The IPsec tunnel is enabled by default. To disable:

---

```
(config vpn ipsec tunnel ipsec_example)> enable false
(config vpn ipsec tunnel ipsec_example)>
```

---

4. (Optional) Set the tunnel to use UDP encapsulation even when it does not detect that NAT is being used:

---

```
(config vpn ipsec tunnel ipsec_example)> force_udp_encap true
(config vpn ipsec tunnel ipsec_example)>
```

---

5. Set the firewall zone for the IPsec tunnel. Generally this should be left at the default of **ipsec**.

---

```
(config vpn ipsec tunnel ipsec_example)> zone zone
(config vpn ipsec tunnel ipsec_example)>
```

---

To view a list of available zones:

---

```
(config vpn ipsec tunnel ipsec_example)> zone ?
```

---

Zone: The firewall zone assigned to this IPsec tunnel. This can be used by packet filtering rules and access control lists to restrict network traffic on this tunnel.

Format:

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

Default value: ipsec

Current value: ipsec

---

```
(config vpn ipsec tunnel ipsec_example)>
```

---

**Note** Depending on your network configuration, you may need to add a packet filtering rule to allow incoming traffic. For example, for the **IPsec** zone:

- a. Type ... to move to the root of the configuration:

```
(config vpn ipsec tunnel ipsec_example)> ...
(config)>
```

- b. Add a packet filter:

```
(config)> add firewall filter end
(config firewall filter 2)>
```

- c. Set the label to **Allow incoming IPsec traffic**:

```
(config config firewall filter 2)> label "Allow incoming IPsec
traffic"
(config firewall filter 2)>
```

- d. Set the source zone to **ipsec**:

```
(config config firewall filter 2)> src_zone ipsec
(config firewall filter 2)>
```

6. Set the metric for the IPsec tunnel. When more than one active route matches a destination, the route with the lowest metric is used. The metric can also be used in tandem with SureLink to configure IPsec failover behavior. See [Configure IPsec failover](#) for more information.

```
(config vpn ipsec tunnel ipsec_example)> metric value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is any integer between **0** and **65535**.

7. Set the mode:

```
(config vpn ipsec tunnel ipsec_example)> mode mode
(config vpn ipsec tunnel ipsec_example)>
```

where *mode* is either:

- **tunnel**: The entire IP packet is encrypted and/or authenticated and then encapsulated as the payload in a new IP packet.
- **transport**: Only the payload of the IP packet is encrypted and/or authenticated. The IP header is unencrypted.

The default is **tunnel**.

8. Set the protocol:

```
(config vpn ipsec tunnel ipsec_example)> type protocol
(config vpn ipsec tunnel ipsec_example)>
```

where *protocol* is either:

- **esp** (Encapsulating Security Payload): Provides encryption as well as authentication and integrity.
- **ah** (Authentication Header): Provides authentication and integrity only.

The default is **esp**.

9. (Optional) Set the management priority for this IPsec tunnel:

---

```
(config vpn ipsec tunnel ipsec_example)> mgmt value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is any interger between **0** and **1000**.

10. Set the authentication type:

---

```
(config vpn ipsec tunnel ipsec_example)> auth type value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is one of:

- **secret**: Uses a pre-shared key (PSK) to authenticate with the remote peer.
  - a. Set the pre-shared key:

---

```
(config vpn ipsec tunnel ipsec_example)> auth secret key
(config vpn ipsec tunnel ipsec_example)>
```

---

- **asymmetric-secrets**: Uses asymmetric pre-shared keys to authenticate with the remote peer.

- a. Set the local pre-shared key. This must be the same as the remote key on the remote host.:

---

```
(config vpn ipsec tunnel ipsec_example)> auth local_secret key
(config vpn ipsec tunnel ipsec_example)>
```

---

- b. Set the remote pre-shared key. This must be the same as the local key on the remote host.:

---

```
(config vpn ipsec tunnel ipsec_example)> auth remote_secret key
(config vpn ipsec tunnel ipsec_example)>
```

---

- **rsasig**: Uses a private RSA key to authenticate with the remote peer.

- a. For the **private\_key** parameter, paste the device's private RSA key in PEM format:

---

```
(config vpn ipsec tunnel ipsec_example)> auth private_key key
(config vpn ipsec tunnel ipsec_example)>
```

---

- b. Set the private key passphrase that is used to decrypt the private key. Leave blank if the private key is not encrypted.

---

```
(config vpn ipsec tunnel ipsec_example)> auth private_key_
passphrase passphrase
(config vpn ipsec tunnel ipsec_example)>
```

---

- c. For the **peer\_public\_key** parameter, paste the peer's public RSA key in PEM format:

---

```
(config vpn ipsec tunnel ipsec_example)> auth peer_public_key
key
(config vpn ipsec tunnel ipsec_example)>
```

---

- **x509:** Uses private key and X.509 certificates to authenticate with the remote peer.
  - a. For the **private\_key** parameter, paste the device's private RSA key in PEM format:

---

```
(config vpn ipsec tunnel ipsec_example)> auth private_key key
(config vpn ipsec tunnel ipsec_example)>
```

---

- b. Set the private key passphrase that is used to decrypt the private key. Leave blank if the private key is not encrypted.

---

```
(config vpn ipsec tunnel ipsec_example)> auth private_key_
passphrase passphrase
(config vpn ipsec tunnel ipsec_example)>
```

---

- c. For the **cert** parameter, paste the local X.509 certificate in PEM format:

---

```
(config vpn ipsec tunnel ipsec_example)> auth cert certificate
(config vpn ipsec tunnel ipsec_example)>
```

---

- d. Set the method for verifying the peer's X.509 certificate:

---

```
(config vpn ipsec tunnel ipsec_example)> auth peer_verify value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is either:

- **cert:** Uses the peer's X.509 certificate in PEM format for verification.
  - For the **peer\_cert** parameter, paste the peer's X.509 certificate in PEM format:

---

```
(config vpn ipsec tunnel ipsec_example)> auth peer_cert
certificate
(config vpn ipsec tunnel ipsec_example)>
```

---

- **ca:** Uses the Certificate Authority chain for verification.
  - For the **ca\_cert** parameter, paste the Certificate Authority (CA) certificates. These must include all peer certificates in the chain up to the root CA certificate, in PEM format.

---

```
(config vpn ipsec tunnel ipsec_example)> auth ca_cert cert_
chain
(config vpn ipsec tunnel ipsec_example)>
```

---

11. (Optional) Configure the device to connect to its remote peer as an XAUTH client:

- a. Enable XAUTH client functionality:

---

```
(config vpn ipsec tunnel ipsec_example)> xauth_client enable true
(config vpn ipsec tunnel ipsec_example)>
```

---



- b. Set the XAUTH client username:

```
(config vpn ipsec tunnel ipsec_example)> xauth_client username name
(config vpn ipsec tunnel ipsec_example)>
```

- c. Set the XAUTH client password:

```
(config vpn ipsec tunnel ipsec_example)> xauth_client password pwd
(config vpn ipsec tunnel ipsec_example)>
```

12. (Optional) Enable MODECFG client functionality:

MODECFG client functionality configures the device to receive configuration information, such as the private IP address, from the remote peer.

- a. Enable MODECFG client functionality:

```
(config vpn ipsec tunnel ipsec_example)> modecfg_client enable true
(config vpn ipsec tunnel ipsec_example)>
```

13. Configure the local endpoint:

- a. Set the method for determining the local network interface:

```
(config vpn ipsec tunnel ipsec_example)> local type value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is either:

- **defaultroute**: Uses the same network interface as the default route.
- **interface**: Select the **Interface** to be used as the local endpoint.

- b. Set the ID type:

```
(config vpn ipsec tunnel ipsec_example)> local id type value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is one of:

- **auto**: The ID will be automatically determined from the value of the tunnels endpoints.
- **raw**: Enter an ID and have it passed unmodified to the underlying IPsec stack.  
Set the unmodified ID that will be passed:

```
(config vpn ipsec tunnel ipsec_example)> local id type raw_id id
(config vpn ipsec tunnel ipsec_example)>
```

- **any**: Any ID will be accepted.
- **ipv4**: The ID will be interpreted as an IPv4 address and sent as an ID\_IPV4\_ADDR IKE identity.  
Set an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.

---

```
(config vpn ipsec tunnel ipsec_example)> local id type ipv4_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **ipv6:** The ID will be interpreted as an IPv6 address and sent as an ID\_IPV6\_ADDR IKE identity.

Set an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.

---

```
(config vpn ipsec tunnel ipsec_example)> local id type ipv6_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **rfc822:** The ID will be interpreted as an RFC822 (email address).

Set the ID in internet email address format:

---

```
(config vpn ipsec tunnel ipsec_example)> local id type rfc822_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **fqdn:** The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID\_FQDN IKE identity.

- **keyid:** The ID will be interpreted as a Key ID and sent as an ID\_KEY\_ID IKE identity.

Set the key ID:

---

```
(config vpn ipsec tunnel ipsec_example)> local id type keyid_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **mac\_address:** The device's MAC address will be used for the Key ID and sent as an ID\_KEY\_ID IKE identity.

- **serial\_number:** The ID device's serial number will be used for the Key ID and sent as an ID\_KEY\_ID IKE identity.

#### 14. Configure the remote endpoint:

- Add a remote hostname:

---

```
(config vpn ipsec tunnel ipsec_example)> add remote hostname end value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is the hostname or IPv4 address of the IPsec peer. If your device is not configured to initiate the IPsec connection (see [ike initiate](#)), you can also use the keyword **any**, which means that the hostname is dynamic or unknown.

Repeat for additional hostnames.

- Set the hostname selection type:

---

```
(config vpn ipsec tunnel ipsec_example)> remote hostname_selection
value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is one of:

- **round\_robin:** Attempts to connect to hostnames sequentially based on the list order.
  - **random:** Randomly selects an IPsec peer to connect to from the hostname list.
  - **priority:** Selects the first hostname in the list that is resolvable.
- c. Set the ID type:

---

```
(config vpn ipsec tunnel ipsec_example)> remote id type value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is one of:

- **auto:** The ID will be automatically determined from the value of the tunnels endpoints.
- **raw:** Enter an ID and have it passed unmodified to the underlying IPsec stack.  
Set the unmodified ID that will be passed:

---

```
(config vpn ipsec tunnel ipsec_example)> remote id type raw_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **any:** Any ID will be accepted.
- **ipv4:** The ID will be interpreted as an IPv4 address and sent as an ID\_IPV4\_ADDR IKE identity.  
Set an IPv4 formatted ID. This can be a fully-qualified domain name or an IPv4 address.

---

```
(config vpn ipsec tunnel ipsec_example)> remote id type ipv4_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **ipv6:** The ID will be interpreted as an IPv6 address and sent as an ID\_IPV6\_ADDR IKE identity.  
Set an IPv6 formatted ID. This can be a fully-qualified domain name or an IPv6 address.

---

```
(config vpn ipsec tunnel ipsec_example)> remote id type ipv6_id
id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **rfc822:** The ID will be interpreted as an RFC822 (email address).  
Set the ID in internet email address format:

---

```
(config vpn ipsec tunnel ipsec_example)> remote id type rfc822_
id id
(config vpn ipsec tunnel ipsec_example)>
```

---

- **fqdn:** The ID will be interpreted as FQDN (Fully Qualified Domain Name) and sent as an ID\_FQDN IKE identity.

- **keyid:** The ID will be interpreted as a Key ID and sent as an ID\_KEY\_ID IKE identity. Set the key ID:

```
(config vpn ipsec tunnel ipsec_example)> remote id type keyid_id
id
(config vpn ipsec tunnel ipsec_example)>
```

- **mac\_address:** The device's MAC address will be used for the Key ID and sent as an ID\_KEY\_ID IKE identity.
- **serial\_number:** The ID device's serial number will be used for the Key ID and sent as an ID\_KEY\_ID IKE identity.

15. Configure IKE settings:

- a. Set the IKE version:

```
(config vpn ipsec tunnel ipsec_example)> ike version value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is either **ikev1** or **ikev2**. This setting must match the peer's IKE version.

- b. Determine whether the device should initiate the key exchange, rather than waiting for an incoming request. By default, the device will initiate the key exchange. This must be disabled if [remote hostname](#) is set to **any**. To disable:

```
(config vpn ipsec tunnel ipsec_example)> ike initiate false
(config vpn ipsec tunnel ipsec_example)>
```

- c. Set the IKE phase 1 mode:

```
(config vpn ipsec tunnel ipsec_example)> ike mode value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is either **aggressive** or **main**.

- d. Set the IKE fragmentation:

```
(config vpn ipsec tunnel ipsec_example)> ike fragmentation value
(config vpn ipsec tunnel ipsec_example)>
```

where *value* is one of:

- **if\_supported:** Send oversized IKE messages in fragments, if the peer supports receiving them.
- **always:** Always send IKEv1 messages in fragments. For IKEv2, this option is equivalent to **if supported**.
- **never:** Do not send oversized IKE messages in fragments.
- **accept:** Do not send oversized IKE messages in fragments, but announce support for fragmentation to the peer.

The default is **always**.

- e. Padding of IKE packets is enabled by default and should normally not be disabled except for compatibility purposes. To disable:

---

```
(config vpn ipsec tunnel ipsec_example)> ike pad false
(config vpn ipsec tunnel ipsec_example)>
```

---

- f. Set the amount of time that the IKE security association expires after a successful negotiation and must be re-authenticated:

---

```
(config vpn ipsec tunnel ipsec_example)> ike phase1_lifetime value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **phase1\_lifetime** to ten minutes, enter either **10m** or **600s**:

---

```
(config vpn ipsec tunnel ipsec_example)> ike phase1_lifetime 600s
(config vpn ipsec tunnel ipsec_example)>
```

---

The default is three hours.

- g. Set the amount of time that the IKE security association expires after a successful negotiation and must be rekeyed.

---

```
(config vpn ipsec tunnel ipsec_example)> ike phase2_lifetime value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **phase2\_lifetime** to ten minutes, enter either **10m** or **600s**:

---

```
(config vpn ipsec tunnel ipsec_example)> ike phase2_lifetime 600s
(config vpn ipsec tunnel ipsec_example)>
```

---

The default is one hour.

- h. Set a randomizing amount of time before the IPsec tunnel is renegotiated:

---

```
(config vpn ipsec tunnel ipsec_example)> ike lifetime_margin value
(config vpn ipsec tunnel ipsec_example)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **lifetime\_margin** to ten minutes, enter either **10m** or **600s**:

---

```
(config vpn ipsec tunnel ipsec_example)> ike lifetime_margin 600s
(config vpn ipsec tunnel ipsec_example)>
```

---

The default is nine minutes.

- i. Configure the types of encryption, hash, and Diffie-Hellman group to use during phase 1:
- i. Add a phase 1 proposal:

---

```
(config vpn ipsec tunnel ipsec_example)> add ike phase1_proposal
end
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

---

- ii. Set the type of encryption to use during phase 1:

---

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
cipher value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

---

where *value* is one of:

- **3des**
- **aes128**
- **aes128gcm128**
- **aes128gcm64**
- **aes128gcm96**
- **aes192**
- **aes192gcm128**
- **aes192gcm64**
- **aes192gcm96**
- **aes256**
- **aes256gcm128**
- **aes256gcm64**
- **aes256gcm96**
- **null**

The default is **3des**.

- iii. Set the type of hash to use during phase 1 to verify communication integrity:

---

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
hash value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
```

---

where *value* is one of:

- **md5**
- **sha1**
- **sha256**
- **sha384**
- **sha512**

The default is **sha1**.

- iv. Set the type of Diffie-Hellman group to use for key exchange during phase 1:

- i. Use the ? to determine available Diffie-Hellman group types:

---

```
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
dh_group ?
curve25519
curve448
ecp192
```

---

---

```

ecp224
...
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>

```

---

- ii. Set the Diffie-Hellman group type:

---

```

(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
dh_group value
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>

```

---

The default is **modp2048**.

- v. (Optional) Add additional phase 1 proposals:

- i. Move back one level in the schema:

---

```

(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)>
..
(config vpn ipsec tunnel ipsec_example ike phase1_proposal)>

```

---

- ii. Add an additional proposal:

---

```

(config vpn ipsec tunnel ipsec_example ike phase1_proposal)>
add end
(config vpn ipsec tunnel ipsec_example ike phase1_proposal 1)>

```

---

Repeat the above steps to set the type of encryption, hash, and Diffie-Hellman group for the additional proposal.

- iii. Repeat to add more phase 1 proposals.

- j. Configure the types of encryption, hash, and Diffie-Hellman group to use during phase 2:

- i. Move back two levels in the schema:

---

```

(config vpn ipsec tunnel ipsec_example ike phase1_proposal 0)> ..
..
(config vpn ipsec tunnel ipsec_example ike)>

```

---

- ii. Add a phase 2 proposal:

---

```

(config vpn ipsec tunnel ipsec_example ike)> add ike phase2_
proposal end
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>

```

---

- iii. Set the type of encryption to use during phase 2:

---

```

(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
cipher value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>

```

---

where *value* is one of:

- **3des**
- **aes128**
- **aes128gcm128**

- **aes128gcm64**
- **aes128gcm96**
- **aes192**
- **aes192gcm128**
- **aes192gcm64**
- **aes192gcm96**
- **aes256**
- **aes256gcm128**
- **aes256gcm64**
- **aes256gcm96**
- **null**

The default is **3des**.

- iv. Set the type of hash to use during phase 2 to verify communication integrity:

---

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
hash value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

---

where *value* is one of:

- **md5**
- **sha1**
- **sha256**
- **sha384**
- **sha512**

The default is **sha1**.

- v. Set the type of Diffie-Hellman group to use for key exchange during phase 2:
- i. Use the ? to determine available Diffie-Hellman group types:

---

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
dh_group ?
curve25519
curve448
ecp192
ecp224
...
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

---

- ii. Set the Diffie-Hellman group type:

---

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
dh_group value
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
```

---

The default is **modp2048**.

- vi. (Optional) Add additional phase 2 proposals:



- i. Move back one level in the schema:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)>
..
(config vpn ipsec tunnel ipsec_example ike phase2_proposal)>
```

- ii. Add an additional proposal:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal)>
add end
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 1)>
```

Repeat the above steps to set the type of encryption, hash, and Diffie-Hellman group for the additional proposal.

- iii. Repeat to add more phase 2 proposals.

16. (Optional) Configure dead peer detection:

Dead peer detection is enabled by default. Dead peer detection uses periodic IKE transmissions to the remote endpoint to detect whether tunnel communications have failed, allowing the tunnel to be automatically restarted when failure occurs.

- a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example ike phase2_proposal 0)> ...
(config)>
```

- b. To disable dead peer detection:

```
(config)> vpn ipsec tunnel ipsec_example dpd enable false
(config)>
```

- c. Set the number of seconds between transmissions of dead peer packets. Dead peer packets are only sent when the tunnel is idle. The default is **60**.

```
(config)> vpn ipsec tunnel ipsec_example dpd delay value
(config)>
```

- d. Set the number of seconds to wait for a response from a dead peer packet before assuming the tunnel has failed. The default is **90**.

```
(config)> vpn ipsec tunnel ipsec_example dpd timeout value
(config)>
```

17. (Optional) Create a list of destination networks that require source NAT:

- a. Add a destination network:

```
(config)> add vpn ipsec tunnel ipsec_example nat end
(config vpn ipsec tunnel ipsec_example nat 0)>
```

- b. Set the IPv4 address and optional netmask of a destination network that requires source NAT. You can also use **any**, meaning that any destination network connected to the tunnel will use source NAT.

---

```
(config vpn ipsec tunnel ipsec_example nat 0)> dst value
(config vpn ipsec tunnel ipsec_example nat 0)>
```

---

18. Configure policies that define the network traffic that will be encapsulated by this tunnel:

- a. Change to the root of the configuration schema:

---

```
(config vpn ipsec tunnel ipsec_example nat 0)> ...
(config)>
```

---

- b. Add a policy:

---

```
(config)> add vpn ipsec tunnel ipsec_example policy end
(config vpn ipsec tunnel ipsec_example policy 0)>
```

---

- c. Set the type of local traffic selector:

---

```
(config vpn ipsec tunnel ipsec_example policy 0)> local type value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

---

where *value* is one of:

- **address:** The address of a local network interface.

Set the address:

- i. Use the **?** to determine available interfaces:
- ii. Set the interface. For example:

---

```
(config vpn ipsec tunnel ipsec_example policy 0)> local
address eth1
(config vpn ipsec tunnel ipsec_example policy 0)>
```

---

- **network:** The subnet of a local network interface.

Set the network:

- i. Use the **?** to determine available interfaces:
- ii. Set the interface. For example:

---

```
(config vpn ipsec tunnel ipsec_example policy 0)> local
network eth1
(config vpn ipsec tunnel ipsec_example policy 0)>
```

---

- **custom:** A user-defined network.

Set the custom network:

---

```
(config vpn ipsec tunnel ipsec_example policy 0)> local custom
value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

---

where *value* is the IPv4 address and optional netmask. The keyword **any** can also be used.

- **request:** Requests a network from the remote peer.
- **dynamic:** Uses the address of the local endpoint.

- d. Set the port matching criteria for the local traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local port value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is the port number, a range of port numbers, or the keyword **any**.

- e. Set the protocol matching criteria for the local traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local protocol value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is one of:

- **any**: Matches any protocol.
- **tcp**: Matches TCP protocol only.
- **udp**: Matches UDP protocol only.
- **icmp**: Matches ICMP requests only.
- **other**: Matches an unlisted protocol.

If **other** is used, set the number of the protocol:

```
(config vpn ipsec tunnel ipsec_example policy 0)> local
protocol_other int
(config vpn ipsec tunnel ipsec_example policy 0)>
```

Allowed values are an integer between **1** and **255**.

- f. Set the IP address and optional netmask of the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote network value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

- g. Set the port matching criteria for the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote port value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is the port number, a range of port numbers, or the keyword **any**.

- h. Set the protocol matching criteria for the remote traffic selector:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote protocol
value
(config vpn ipsec tunnel ipsec_example policy 0)>
```

where *value* is one of:

- **any**: Matches any protocol.
- **tcp**: Matches TCP protocol only.
- **udp**: Matches UDP protocol only.
- **icmp**: Matches ICMP requests only.

- **other**: Matches an unlisted protocol.

If **other** is used, set the number of the protocol:

```
(config vpn ipsec tunnel ipsec_example policy 0)> remote
protocol_other int
(config vpn ipsec tunnel ipsec_example policy 0)>
```

Allowed values are an integer between **1** and **255**.

19. (Optional) You can also configure various IPsec related time out, keep alive, and related values:
- a. Change to the root of the configuration schema:

```
(config vpn ipsec tunnel ipsec_example policy 0)> ...
(config)>
```

- b. Use the **?** to determine available options:

```
(config)> vpn ipsec advanced ?
```

Advanced: Advanced configuration that applies to all IPsec tunnels.

Parameters	Current Value	
debug	none	Debug level
ike_fragment_size	1280	Maximum IKE fragment size
ike_retransmit_tries	5	IKE retransmit tries
keep_alive	40s	NAT keep alive time

Additional Configuration

connection_retry_timeout	Connection retry timeout
connection_try_interval	Connection try interval
ike_timeout	IKE timeout

```
(config)>
```

Generally, the default settings for these should be sufficient.

- c. You can also enable debugging for IPsec:

```
(config)> vpn ipsec advanced debug value
(config)>
```

where *value* is one of:

- **none**
- **basic\_auditing**
- **detailed\_control**
- **generic\_control**
- **raw\_data**
- **sensitive\_data**

20. Save the configuration and apply the change

---

```
(config)> save  
Configuration saved.  
>
```

---

21. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure IPsec failover

There are two methods to configure the Connect EZ device to fail over from a primary IPsec tunnel to a backup tunnel:

- **SureLink** active recovery—You can use SureLink along with the IPsec tunnel's metric to configure two or more tunnels so that when the primary tunnel is determined to be inactive by SureLink, a secondary tunnel can begin serving traffic that the primary tunnel was serving.
- **Preferred tunnel**—When multiple IPsec tunnels are configured, one tunnel can be configured as a backup to another tunnel by defining a preferred tunnel for the backup device.

### Required configuration items

- Two or more configured IPsec tunnels: The primary tunnel, and one or more backup tunnels.
- Either:
  - SureLink configured on the primary tunnel with **Restart Interface** enabled, and the metric for all tunnels set appropriately to determine which IPsec tunnel has priority. With this failover configuration, both tunnels are active simultaneously, and there is minimal downtime due to failover.
  - Identify the preferred tunnel during configuration of the backup tunnel. In this scenario, the backup tunnel is not active until the preferred tunnel fails.

### IPsec failover using SureLink

With this configuration, when two IPsec tunnels are configured with the same local and remote endpoints but different metrics, traffic addressed to the remote endpoint will be routed through the IPsec tunnel with the lower metric.

If **SureLink > Restart Interface** is enabled for the tunnel with the lower metric, and SureLink determines that the tunnel is not functioning properly (for example, pings to a host at the other end of the tunnel are failing), then:

1. SureLink will shut down the tunnel and renegotiate its IPsec connection.
2. While the tunnel with the lower metric is down, traffic addressed to the remote endpoint will be routed through the tunnel with the higher metric.

For example:

- Tunnel\_1:
  - **Metric:** 10
  - **Local endpoint > Interface:** ETH2
  - **Remote endpoint > Hostname:** 192.168.10.1
  - **SureLink** configuration:
    - **Restart Interface** enabled
    - **Test target:**
      - **Test type:** Ping test
      - **Ping host:** 192.168.10.2
- Tunnel\_2:

- **Metric:** 20
- **Local endpoint > Interface:** ETH2
- **Remote endpoint > Hostname:** 192.168.10.1

In this configuration:

1. Tunnel\_1 will normally be used for traffic destined for the 192.168.10.1 endpoint.
2. If pings to 192.168.10.2 fail, SureLink will shut down the tunnel and renegotiate its IPsec connection.
3. While Tunnel\_1 is down, Tunnel\_2 will be used for traffic destined for the 192.168.10.1 endpoint.

## Web

1. Configure the primary IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
  - During configuration of the IPsec tunnel, set the metric to a low value (for example, **10**).

The screenshot shows the configuration page for an IPsec tunnel. The 'Metric' field is highlighted with a green box and contains the value '10'. Other visible fields include 'Enable' (checked), 'Preferred tunnel', 'Force UDP encapsulation' (unchecked), 'Zone' (IPsec), 'Mode' (Tunnel mode), and 'Protocol' (ESP).

- Configure SureLink for the primary IPsec tunnel and enable **Restart interface**. See [Configure SureLink active recovery for IPsec](#) for instructions.

The screenshot shows the SureLink configuration page. The 'Restart interface' checkbox is checked. Other visible fields include 'Interval' (15m), 'Success condition' (One test target passes), 'Attempts' (3), and 'Response timeout' (15s).

2. Create a backup IPsec tunnel. Configure this tunnel to use the same local and remote endpoints as the primary tunnel. See [Configure an IPsec tunnel](#) for instructions.
  - During configuration of the IPsec tunnel, set the metric to a value that is higher than the metric of the primary tunnel (for example, **20**).

The screenshot shows the configuration page for a backup IPsec tunnel. The 'Metric' field is highlighted with a green box and contains the value '20'. Other visible fields include 'Enable' (checked), 'Preferred tunnel', 'Force UDP encapsulation' (unchecked), 'Zone' (IPsec), 'Mode' (Tunnel mode), and 'Protocol' (ESP).

## Command line

1. Configure the primary IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
  - During configuration of the IPsec tunnel, set the metric to a low value (for example, **10**):

```
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)> metric 10
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)>
```

- Configure SureLink for the primary IPsec tunnel and enable **Restart interface**. See [Configure SureLink active recovery for IPsec](#) for instructions.

```
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)> surelink
restart true
(config vpn ipsec tunnel IPsecFailoverPrimaryTunnel)>
```

2. Create a backup IPsec tunnel. Configure this tunnel to use the same local and remote endpoints as the primary tunnel. See [Configure an IPsec tunnel](#) for instructions.
  - During configuration of the IPsec tunnel, set the metric to a value that is higher than the metric of the primary tunnel (for example, **20**):

```
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)> metric 20
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)>
```

## IPsec failover using Preferred tunnel

### Web

1. Configure the primary IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
2. Create a backup IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
3. During configuration of the backup IPsec tunnel, identify the primary IPsec tunnel in the **Preferred tunnel** parameter:

The screenshot shows the configuration page for an IPsec Failover Backup Tunnel. The 'Preferred tunnel' field is a dropdown menu that has been set to 'IPsecFailoverPrimaryTunnel'. Other fields include 'Enable' (checked), 'Force UDP encapsulation' (unchecked), 'Zone' (set to 'IPsec'), 'Metric' (set to '0'), 'Mode' (set to 'Tunnel mode'), and 'Protocol' (set to 'ESP').

### Command line

1. Configure the primary IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
2. Create a backup IPsec tunnel. See [Configure an IPsec tunnel](#) for instructions.
3. During configuration of the backup IPsec tunnel, identify the primary IPsec tunnel:
  - a. Use the **?** to view a list of available tunnels:

```
(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover ?
```

```
Preferred tunnel: This tunnel will not start until the preferred
tunnel has failed. It will continue
to operate until the preferred tunnel returns to full operation
```



---

```

status.
Format:
  primary_ipsec_tunnel
  backup_ipsec_tunnel
Optional: yes
Current value:

(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover

```

---

- b. Set the primary IPsec tunnel:

---

```

(config vpn ipsec tunnel backup_ipsec_tunnel)> ipsec_failover primary_
ipsec_tunnel
(config vpn ipsec tunnel backup_ipsec_tunnel)>

```

---

## Configure SureLink active recovery for IPsec

You can configure the Connect EZ device to regularly probe IPsec tunnels to determine if the connection has failed and take remedial action.

You can also configure the IPsec tunnel to fail over to a backup tunnel. See [Configure IPsec failover](#) for further information.

### Required configuration items

- A valid IPsec configuration. See [Configure an IPsec tunnel](#) for configuration instructions.
- Enable IPsec SureLink.
- The behavior of the Connect EZ device upon IPsec failure: either
  - Restart the IPsec interface
  - Reboot the device.

### Additional configuration items

- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.
- The number of probe failures before the IPsec connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe failures before considering it to have failed.

To configure the Connect EZ device to regularly probe the IPsec connection:

### Web

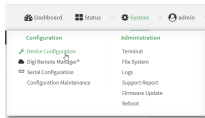
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > IPsec**.
4. Create a new IPsec tunnel or select an existing one:
  - To create a new IPsec tunnel, see [Configure an IPsec tunnel](#).
  - To edit an existing IPsec tunnel, click to expand the appropriate tunnel.
5. After creating or selecting the IPsec tunnel, click **SureLink**.

▼ SureLink	
Enable	<input type="checkbox"/>
Test interval	15m
Success condition	One test passes
Pass threshold	1
Response timeout	15s
▶ Tests	
▶ Recovery actions	
▶ Advanced settings	

6. **Enable** SureLink.
7. (Optional) Change the **Test interval** between connectivity tests.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Interval** to ten minutes, enter **10m** or **600s**.  
 The default is 15 minutes.
8. (Optional) If more than one test target is configured, for **Success condition**, select either:

- **One test passes:** Only one test needs to pass for Surelink to consider an interface to be up.
  - **All test pass:** All tests need to pass for SureLink to consider the interface to be up.
9. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
  10. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

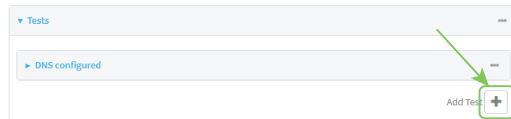
For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.

The default is 15 seconds.

11. Click to expand **Tests**.

By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

- a. Click **+**.



New tests are enabled by default. To disable, click to toggle off **Enable**.

- b. Type a **Label** for the test.
- c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.
- d. Select the **Test type**.

Available test types:

- **Ping test:** Uses ICMP to determine connectivity.

If **Ping test** is selected, complete the following:

- **Ping target:** The type of target for the ping, one of:
  - **Hostname or IP address** of an external server.
    - **Ping host:** hostname or IP address of the server.
    - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
    - The **Interface address**.
    - The **Interface DNS** server.
  - **Ping payload size:** The number of bytes to send as part of the ping payload.

- **DNS test:** Performs a DNS query to the named DNS server.

If **DNS test** is selected, complete the following:

- **DNS server:** The IP address of the DNS server.

- **HTTP test:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **HTTP test** is selected, complete the following:

- **Web server:** The URL of the web server.
- **Test DNS servers configured for this interface:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **Test the interface status** is selected, complete the following:

- **Down time:** The amount of time that the interface is down before the test can be considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number(w|d|h|m|s)*.

For example, to set **Down time** to ten minutes, enter **10m** or **600s**.

- **Initial connection time:** The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number(w|d|h|m|s)*.

For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.

- **Custom test:** Tests the interface with custom commands.

If **Custom test** is selected, complete the following:

- The **Commands to run to test**.

- **TCP connection test:** Tests that the interface can reach a destination port on the configured host.

If **TCP connection test** is selected, complete the following:

- **TCP connect host:** The hostname or IP address of the host to create a TCP connection to.
- **TCP connect port:** The TCP port to create a TCP connection to.

- **Test another interface's status:** Tests the status of another interface.

If **Test another interface's status** is selected, complete the following:

- **Test interface:** The interface to test.
- **IP version:** The type of IP connection, one of:
  - **Any:** Either the IPv4 or IPv6 connection must be up.
  - **Both:** Both the IPv4 or IPv6 connection must be up.
  - **IPv4:** The IPv4 connection must be up.
  - **IPv6:** The IPv6 connection must be up.
- **Expected status:** The status required for the test to pass.
  - **Up:** The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).

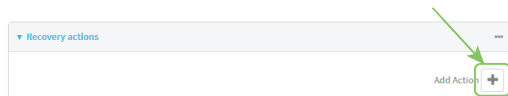
- **Down:** The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).
  - e. Repeat for each additional test.
12. Add recovery actions:

- a. Click to expand **Recovery actions**.

By default, there are two preconfigured recovery actions:

- **Update routing:** Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
- **Restart interface.**

- b. Click **+**.



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

- c. Type a **Label** for the recovery action.
- d. For **Recovery type**, select **Reboot device**.
- e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.
- **Change default gateway:** Increases the interface's metric to change the default gateway.
 

If **Change default gateway** is selected, complete the following:

    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Increase metric to change active default gateway:** Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Restart interface.**

If **Restart interface** is selected, complete the following:

    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Reset modem:** This recovery action is available for WWAN interfaces only.
 

If **Reset modem** is selected, complete the following:

    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.

- **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
    - **Switch to alternate SIM:** Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.
      - If **Switch to alternate SIM** is selected, complete the following:
        - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
        - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
    - **Reboot device.**
      - If **Reboot device** is selected, complete the following:
        - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
        - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
    - **Execute custom Recovery commands.**
      - If **Recovery commands** is selected, complete the following:
        - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
        - The **Commands to run to recovery connectivity.**
        - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
    - **Powercycle the modem.** This recovery action is available for WWAN interfaces only.
      - If **Powercycle the modem** is selected, complete the following:
        - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
        - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - f. Repeat for each additional recovery action.
13. (Optional) Configure advanced SureLink parameters:
  - a. Click to expand **Advanced settings**.
  - b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.
 

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number(w|d|h|m|s)**.

For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.

The default is 300 seconds.

- c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.

The default is 300 seconds.

- d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.

14. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create a new IPsec tunnel, or edit an existing one:

- To create a new IPsec tunnel, see [Configure an IPsec tunnel](#).
- To edit an existing IPsec tunnel, change to the IPsec tunnel's node in the configuration schema. For example, for an IPsec tunnel named **ipsec\_example**, change to the **ipsec\_example** node in the configuration schema:

```
(config)> vpn ipsec tunnel ipsec_example
(config vpn ipsec tunnel ipsec_example)>
```

4. Enable SureLink:

```
(config vpn ipsec tunnel ipsec_example)> surelink enable true
(config vpn ipsec tunnel ipsec_example)>
```

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

To add additional tests:

- a. Add a test:

```
(config vpn ipsec tunnel ipsec_example)> add surelink tests end
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

- b. New tests are enabled by default. To disable:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> enable false
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- c. Create a label for the test:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> label string
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> ipv6 true
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- e. Set the test type:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> test value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is one of:

- **ping:** Uses ICMP to determine connectivity.

If **ping** is selected, complete the following:

- Set the **ping\_method**:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
ping_method value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is one of:

- **hostname:** The hostname or IP address of an external server.
  - Set **ping\_host** to the hostname or IP address of the server:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
ping_host hostname/IP_address
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **interface\_gateway.** If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
- **interface\_address.**
- **interface\_dns:** The interface's DNS server.

- Set the number of bytes to send as part of the ping payload:

---

```
(config vpn ipsec tunnel ipsec_example ipsec tunnel ipsec_
example surelink tests 1)> ping_size int
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **dns:** Performs a DNS query to the named DNS server.

If **dns** is set, set the IPv4 or IPv6 address of the DNS server:



---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> dns_
server IP_address
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **http:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **http** is set, set the URL of the web server.

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> http
url
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **dns\_configured:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface\_up:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **interface\_up** is set, complete the following:

- Set the amount of time that the interface is down before the test can be considered to have failed.

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
interface_down_time value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_down\_time** to ten minutes, enter either **10m** or **600s**:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
interface_down_time 600s
(config)>
```

---

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
interface_timeout value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
interface_timeout 600s
(config)>
```

---

- **custom\_test:** Tests the interface with custom commands.

If **custom\_test** is set, set the commands to run to perform the test:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
custom_test_commands "string"
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **tcp\_connection:** Tests that the interface can reach a destination port on the configured host.

If **tcp\_connection** is selected, complete the following:

- Set the hostname or IP address of the host to create a TCP connection to:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
tcp_host hostname/IP_address
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- Set the TCP port to create a TCP connection to.

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
tcp_port port
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- **other:** Tests the status of another interface.

If **other** is selected, complete the following:

- Set the interface to test.
  - Use the **?** to determine available interfaces:
  - Set the interface. For example:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
other_interface /network/interface/eth1
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

- Set the type of IP connection:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
other_ip_version value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is one of:

- **any:** Either the IPv4 or IPv6 connection must be up.
- **both:** Both the IPv4 or IPv6 connection must be up.
- **ipv4:** The IPv4 connection must be up.
- **ipv6:** The IPv6 connection must be up.

- The status required for the test to pass.

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
other_status value
(config vpn ipsec tunnel ipsec_example surelink tests 1)>
```

---

where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

6. Add recovery actions:

a. Type ... to return to the root of the configuration:

---

```
(config vpn ipsec tunnel ipsec_example surelink tests 1)> ...
(config)>
```

---

b. Add a recovery action:

---

```
(config)> add vpn ipsec tunnel ipsec_example surelink actions end
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

c. New actions are enabled by default. To disable:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> enable
false
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

d. Create a label for the action:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> label
string
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

e. Set the type of recovery action to **reboot\_device**:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> action
reboot_device
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

- f. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed. The command varies depending on whether the interface is a WAN or WWAN:

- WAN interfaces:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
action value
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

- WWAN interfaces:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
modem_action value
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

where *value* is one of:

- **update\_routing\_table**: Increases the interface's metric to change the default gateway.

If **update\_routing\_table** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

The default is **3**.

- Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
metric_adjustment_modem int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

The default is **100**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

- **restart\_interface**.

If **restart\_interface** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **reset\_modem**: This recovery action is available for WWAN interfaces only.

If **reset\_modem** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **switch\_sim**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

If **switch\_sim** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **modem\_power\_cycle:** This recovery action is available for WWAN interfaces only.

If **modem\_power\_cycle** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **reboot\_device.**

If **reboot\_device** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

- **custom\_action:** Execute custom recovery commands.

If **custom\_action** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
test_failures int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

The default is **3**.

- Set the commands to run to attempt to recovery connectivity.

---

```
(config network interface my_wan surelink actions 0)> custom_
action_commands_modem "string"
(config network interface my_wan surelink actions 0)>
```

---

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
override_interval int
(config vpn ipsec tunnel ipsec_example surelink actions 0)>
```

---

g. Repeat for each additional recovery action.

7. Optional SureLink configuration parameters:

a. Type ... to return to the root of the configuration:

---

```
(config vpn ipsec tunnel ipsec_example surelink actions 0)> ...
(config)>
```

---

b. Set the test interval between connectivity tests:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink interval value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink interval 600s
(config)>
```

---

The default is **15m**.

c. If more than one test target is configured, set the success condition:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink success_condition
value
(config)>
```

---

where *value* is either:

- **one**: Only one test needs to pass for Surelink to consider an interface to be up.
- **all**: All tests need to pass for SureLink to consider the interface to be up.

d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

---

```
(config)> vpn ipsec tunnel ipsec_example surelink pass_threshold int
(config)>
```

---

The default is **1**.

e. Set the amount of time that the device should wait for a response to a test attempt before considering it to have failed:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink timeout value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink timeout 600s
(config)>
```

---

The default is **15s**.

- f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

---

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced delayed_
start value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **delayed\_start** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced delayed_
start 600s
(config)>
```

---

The default is **300s**.

- g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

---

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced backoff_
interval value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **backoff\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced backoff_
interval 600s
(config)>
```

---

The default is 300 seconds.

- h. The **interface\_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:



---

```
(config)> vpn ipsec tunnel ipsec_example surelink advanced interface_
gateway hostname/IP_address
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.


## Show IPsec status and statistics

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status > IPsec**.

The **IPsec** page appears.

2. To view configuration details about an IPsec tunnel, click the  (configuration) icon in the upper right of the tunnel's status pane.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To display details about all configured IPsec tunnels, type the following at the prompt:

---

```
> show ipsec all
```

Name	Enable	Status	Hostname
ipsec1	true	up	192.168.2.1
vpn1	false	pending	192.168.3.1

```
>
```

---

3. To display details about a specific tunnel:

---

```
> show ipsec tunnel ipsec1
```

Tunnel	: ipsec1
Enable	: true
Status	: pending
Hostname	: 192.168.2.1

---

---

```

Zone           : ipsec
Mode           : tunnel
Type          : esp

```

---

>

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Debug an IPsec configuration

If you experience issues with an IPsec tunnel not being successfully negotiated with the remote end of the tunnel, you can enable IPsec debug messages to be written to the system log. See [View system and event logs](#) for more information about viewing the system log.

### Web

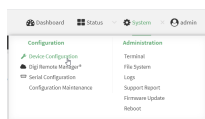
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > IPsec**.
4. Click to expand **Advanced**.
5. For **Debug level**, select one of the following:
  - **Disable debug messages**.
  - **Basic auditing debug**: Logs basic auditing information, (for example, SA up/SA down).
  - **Generic control flow** : Select this for basic debugging information.
  - **Detailed control flow** : More detailed debugging control flow.
  - **Raw data**: Includes raw data dumps in hexadecimal format.

- **Sensitive material:** Also includes sensitive material in dumps (for example, encryption keys).
6. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Set the IPsec debug value:

---

```
config> vpn ipsec advanced debug value
config>
```

---

where *value* is one of:

- **none.** (Default) No debug messages are written.
  - **basic\_auditing:** Logs basic auditing information, (for example, SA up/SA down).
  - **generic\_control:** Select this for basic debugging information.
  - **detailed\_control:** More detailed debugging control flow.
  - **raw\_data:** Includes raw data dumps in hexadecimal format.
  - **sensitive\_data:** Also includes sensitive material in dumps (for example, encryption keys).
4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure a Simple Certificate Enrollment Protocol client

Simple Certificate Enrollment Protocol (SCEP) is a mechanism that allows for large-scale X.509 certificate deployment. You can configure Connect EZ device to function as a SCEP client that will connect to a SCEP server that is used to sign Certificate Signing Requests (CSRs), provide Certificate Revocation Lists (CRLs), and distribute valid certificates from a Certificate Authority (CA).

### Required configuration

- Enable the SCEP client.
- The fully-qualified domain name of the SCEP server to be used for certificate requests.
- The challenge password provided by the SCEP server that the SCEP client will use when making SCEP requests.
- The distinguished name to be used for the CSR.

### Additional configuration

- The number of days that the certificate enrollment can be renewed, prior to the request expiring.

## Web

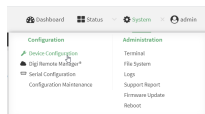
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

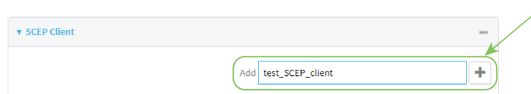
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > SCEP Client**.
4. For **Add clients**, enter a name for the SCEP client and click **+**.



The new SCEP client configuration is displayed.

5. Click **Enable** to enable the SCEP client.
6. For **Maximum Polling Time**, type the maximum time that the device will poll the SCEP server, when operating in manual mode.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Maximum Polling Time** to ten minutes, enter **10m** or **600s**.  
 The default is **1d**.
7. For **Polling Interval**, type the amount of time that the device should wait between polling attempts, when operating in manual mode.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Polling Interval** to ten minutes, enter **10m** or **600s**.  
 The default is **5s**.
8. For **Key Length**, type the bit size of the private key. The default is **2048**.
9. For **Renewable Time**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value is configured on the SCEP server, and is used by the Connect EZ device to determine when to start attempting to auto-renew an existing certificate. The default is **7**.
10. (Optional) Click **Debug** to enable verbose logging in `/var/log/scep_client`.
11. Click to expand **SCEP server**.

12. For **FQDN**, type the fully qualified domain name or IP address of the SCEP server.
13. (Optional) For **CA identity**, type a string that will be understood by the certificate authority. For example, it could be a domain name or a user name. If the certificate authority has multiple CA certificates, this field can be used to distinguish which is required.

14. For **Path**, Type the HTTP URL path required for accessing the certificate authority. You should leave this option at the default of **/cgi-bin/pkiclient.exe** unless directed by the CA to use another path.
15. For **Password**, type the challenge password as configured on the SCEP server.
16. For **Encryption Algorithm**, select the PKCS#7 encryption algorithm. The default is **Auto**, which automatically selects the best algorithm.
17. For **Signature Algorithm**, select the PKCS#7 signature algorithm. The default is **Auto**, which automatically selects the best algorithm.
18. Click to expand **Distinguished Name**.

19. Type the value for each appropriate Distinguished Name attribute.
20. (Optional) Configure the certificate revocation list (CRL):
  - a. Click to expand **CRL**.
  - b. Click **Enable** to enable the CRL.
  - c. For **Type**, select the type of CRL:
    - **URL**: The URL to the file name used to access the certificate revocation list from the CA.
    - **CRLDP**: The CRL distribution point.
    - **getCRL**: A CRL query using the issuer name and serial number from the certificate whose revocation status is being queried.

The default is **URL**.
  - d. If **Type** is set to **URL**, for **URL**, type the URL to be used.
21. Configure certificate renewal:
  - a. Click to expand **Renewal**.
  - b. Click **Use New Private Key** to enable the creation of a new private key for renewal requests.
  - c. **Use Client Certificate** is enabled by default. Click to disable the use of a client certificate for renewal requests.
22. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a new SCEP client:

---

```
(config)> add network scep_client scep_client_name
(config network scep_client scep_client_name
)>
```

---

4. Enable the SCEP client:

---

```
(config network scep_client scep_client_name)> enable true
(config network scep_client scep_client_name)>
```

---

5. Set the url parameter to the fully qualified domain name or IP address of the SCEP server:

---

```
(config network scep_client scep_client_name)> server url
https://scep.example.com
(config network scep_client scep_client_name)>
```

---

6. (Optional) Set a CA identity string that will be understood by the certificate authority. For example, it could be a domain name or a user name. If the certificate authority has multiple CA certificates, this field can be used to distinguish which is required.

---

```
(config network scep_client scep_client_name)> server ca_ident string
(config network scep_client scep_client_name)>
```

---

7. Set the HTTP URL path required for accessing the certificate authority. You should leave this option at the default of **/cgi-bin/pkiclient.exe** unless directed by the CA to use another path.

---

```
(config network scep_client scep_client_name)> server path path
(config network scep_client scep_client_name)>
```

---

8. Set the challenge password as configured on the SCEP server:

---

```
(config network scep_client scep_client_name)> server password challenge_
password
(config network scep_client scep_client_name)>
```

---

9. Set Distinguished Name attributes:

- a. Set the Domain Component:

---

```
(config network scep_client scep_client_name)> distinguished_name dc
value
(config network scep_client scep_client_name)>
```

---

- b. Set the two letter Country Code:

---

```
(config network scep_client scep_client_name)> distinguished_name c
value
(config network scep_client scep_client_name)>
```

---

c. Set the State or Province:

---

```
(config network scep_client scep_client_name)> distinguished_name st
value
(config network scep_clientscep_client_name )>
```

---

d. Set the Locality:

---

```
(config network scep_client scep_client_name)> distinguished_name l
value
(config network scep_client scep_client_name)>
```

---

e. Set the Organization:

---

```
(config network scep_client scep_client_name)> distinguished_name o
value
(config network scep_client scep_client_name)>
```

---

f. Set the Organizational Unit:

---

```
(config network scep_client scep_client_name)> distinguished_name ou
value
(config network scep_client scep_client_name)>
```

---

g. Set the Common Name:

---

```
(config network scep_client scep_client_name)> distinguished_name cn
value
(config network scep_client scep_client_name)>
```

---

10. (Optional) Configure the certificate revocation list (CRL):

a. Enable the CRL:

---

```
(config network scep_client scep_client_name)> crl enable true
(config network scep_client scep_client_name)>
```

---

b. Set the type of CRL:

---

```
(config network scep_client scep_client_name)> crl type value
(config network scep_client scep_client_name)>
```

---

where *value* is one of:

- **url**: The URL to the file name used to access the certificate revocation list from the CA.
- **crldp**: The CRL distribution point.
- **getCRL**: A CRL query using the issuer name and serial number from the certificate whose revocation status is being queried.

The default is **url**.



- c. If **type** is set to **url**, set the URL that should be used:

```
(config network scep_client scep_client_name)> crl url value
(config network scep_client scep_client_name)>
```

11. Configure certificate renewal:

- a. To enable the creation of a new private key for renewal requests:

```
(config network scep_client scep_client_name)> renewal new_key true
(config network scep_client scep_client_name)>
```

- b. The use of a client certificate for renewal requests is enabled by default. To disable:

```
(config network scep_client scep_client_name)> renewal use_client_cert
false
(config network scep_client scep_client_name)>
```

12. Set the maximum time that the device will poll the SCEP server, when operating in manual mode:

```
(config network scep_client scep_client_name)> max_poll_time value
(config network scep_client scep_client_name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **max\_poll\_time** to ten minutes, enter either **10m** or **600s**:

```
(config network scep_client scep_client_name)> max_poll_time 600s
(config network scep_client scep_client_name)>
```

The default is **1d**.

13. Set the amount of time that the device should wait between polling attempts, when operating in manual mode:

```
(config network scep_client scep_client_name)> polling_interval value
(config network scep_client scep_client_name)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **polling\_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network scep_client scep_client_name)> polling_interval 600s
(config network scep_client scep_client_name)>
```

The default is **5s**.

14. Set the bit size of the private key:

```
(config network scep_client scep_client_name)> key_length int
(config network scep_client scep_client_name)>
```

The default is **2048**.

15. Set the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value is configured on the SCEP server, and is used by the Connect EZ device to determine when to start attempting to auto-renew an existing certificate. The default is 7.

---

```
(config network scep_client scep_client_name)> renewable_time integer
(config network scep_client scep_client_name)>
```

---

16. (Optional) Enable verbose logging in /var/log/scep\_client:

---

```
(config network scep_client scep_client_name)> debug true
(config network scep_client scep_client_name)>
```

---

17. Save the configuration and apply the change

---

```
(config network scep_client scep_client_name)> save
Configuration saved.
>
```

---

18. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example: SCEP client configuration with Fortinet SCEP server

In this example configuration, we will configure the Connect EZ device as a SCEP client that will connect to a Fortinet SCEP server.

### **Fortinet configuration**

On the Fortinet server:

1. Enable ports for SCEP services:
  - a. From the menu, select **Network > Interfaces**.
  - b. Select the appropriate port and click **Edit**.
  - c. For **Access Rights > Services**, enable the following services:
    - **HTTPS > SCEP**
    - **HTTPS > CRL Downloads**
    - **HTTP > SCEP**
    - **HTTP > CRL Downloads**
  - d. The remaining fields can be left at their defaults or changed as appropriate.
  - e. Click **OK**.
2. Create a Certificate Authority (CA):
  - a. From the menu, click **Certificate Authorities > Local CAs**.
  - b. Click **Create New**.
  - c. Type a **Certificate ID** for the CA, for example, **fortinet\_example\_ca**.
  - d. Complete the **Subject Information** fields.
  - e. The remaining fields can be left at their defaults or changed as appropriate.
  - f. Click **OK**.

3. Edit SCEP settings:
  - a. From the menu, click **SCEP > General**.
  - b. Click **Enable SCEP** if it is not enabled.
  - c. For **Default enrollment password**, enter a password. The password entered here must correspond to the challenge password configured for the SCEP client on the Connect EZ device.
  - d. The remaining fields can be left at their defaults or changed as appropriate.
  - e. Click **OK**.
4. Create an **Enrollment Request**:
  - a. From the menu, click **SCEP > Enrollment Requests**.
  - b. Click **Create New**.
  - c. For **Automatic request type**, select **Wildcard**.
  - d. For **Certificate authority**, select the CA created in step 1, above.
  - e. Complete the **Subject Information** fields. The Distinguished Name (DN) attributes entered here must correspond to the Distinguished Name attributes configured for the SCEP client on the Connect EZ device.
  - f. For **Renewal > Allow renewal x days before the certified is expired**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. The **Renewable Time** setting on the Connect EZ device must match the setting of this parameter.
  - g. The remaining fields can be left at their defaults or changed as appropriate.
  - h. Click **OK**.

### **Connect EZ configuration**

On the Connect EZ device:

#### **Web**

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

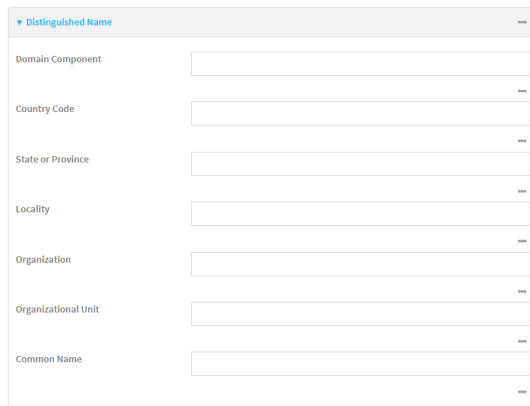
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:



11. Click to expand **Distinguished Name**.



The screenshot shows a web form titled "Distinguished Name" with a dropdown arrow on the right. The form contains eight input fields, each with a label and a corresponding text box:

- Domain Component
- Country Code
- State or Province
- Locality
- Organization
- Organizational Unit
- Common Name

Each input field has a small dropdown arrow on its right side, indicating that these fields are expandable.

12. Type the value for each appropriate Distinguished Name attribute. The values entered here must correspond to the DN attributes in the **Enrollment Request** on the Fortinet server.
13. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a new SCEP client, for example, **Fortinet\_SCEP\_client**:

```
(config)> add network scep_client Fortinet_SCEP_client
(config network scep_client Fortinet_SCEP_client
)>
```

4. Enable the SCEP client:

```
(config network scep_client Fortinet_SCEP_client)> enable true
(config network scep_client Fortinet_SCEP_client)>
```

5. Set the url parameter to the fully qualified domain name or IP address of the SCEP server:

```
(config network scep_client Fortinet_SCEP_client)> server url
https://fortinet.example.com
(config network scep_client Fortinet_SCEP_client)>
```

6. Set the challenge password as configured on the SCEP server. This corresponds to the **Default enrollment password** on the Fortinet server.

```
(config network scep_client Fortinet_SCEP_client)> server password
challenge_password
(config network scep_client Fortinet_SCEP_client)>
```

7. Set Distinguished Name attributes. The values entered here must correspond to the DN attributes in the **Enrollment Request** on the Fortinet server.

- a. Set the Domain Component:

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
dc value
(config network scep_client Fortinet_SCEP_client)>
```

- b. Set the two letter Country Code:

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
c value
(config network scep_client Fortinet_SCEP_client)>
```

- c. Set the State or Province:

---

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
st value
(config network scep_client Fortinet_SCEP_client)>
```

---

- d. Set the Locality:

---

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
l value
(config network scep_client Fortinet_SCEP_client)>
```

---

- e. Set the Organization:

---

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
o value
(config network scep_client Fortinet_SCEP_client)>
```

---

- f. Set the Organizational Unit:

---

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
ou value
(config network scep_client Fortinet_SCEP_client)>
```

---

- g. Set the Common Name:

---

```
(config network scep_client Fortinet_SCEP_client)> distinguished_name
cn value
(config network scep_client Fortinet_SCEP_client)>
```

---

8. Set the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value must match the setting of the **Allow renewal x days before the certified is expired** option on the Fortinet server.

---

```
(config network scep_client Fortinet_SCEP_client)> renewable_time integer
(config network scep_client Fortinet_SCEP_client)>
```

---

9. (Optional) Enable verbose logging in /var/log/scep\_client:

---

```
(config network scep_client Fortinet_SCEP_client)> debug true
(config network scep_client Fortinet_SCEP_client)>
```

---

10. Save the configuration and apply the change

---

```
(config network scep_client Fortinet_SCEP_client)> save
Configuration saved.
>
```

---

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show SCEP client status and information

You can show general SCEP client information for all SCEP clients, and specific information for an individual SCEP client.

This procedure is only available from the Admin CLI.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured SCEP clients, type the following at the prompt:

---

```
> show scep-client

SCEP   Enabled  Expiry
-----
test   true     Jun  4 19:05:25 2022 GMT
test1  false
```

---

```
>
```

3. To display details about a specific SCEP client:

---

```
> show scep-client name name
```

---

For example:

---

```
> show scep-client name test

test SCEP Status
-----
Enabled      : true

Client Certificate
-----
Subject      : C=US,ST=MA,L=BOS,O=Digi,OU=IT1,CN=dummy
Issuer       : CN=TA-SCEP-1-CA
Serial       : 1100000017A30C8EDD3805EB52000000000017
Expiry       : Jun  4 19:05:25 2022 GMT

Certificate Authority Certificate {1}
-----
Subject      : C=US,CN=TA-SCEP-1-MSCEP-RA
Issuer       : CN=TA-SCEP-1-CA
Serial       : 1100000002A1E755981C0C3F34000000000002
Expiry       : Apr 25 13:42:47 2023 GMT

Certificate Authority Certificate {2}
-----
Subject      : C=US,CN=TA-SCEP-1-MSCEP-RA
Issuer       : CN=TA-SCEP-1-CA
Serial       : 1100000003268AFB5E98BFCA73000000000003
Expiry       : Apr 25 13:42:48 2023 GMT
```

---



---

```
Certificate Authority Certificate {3}
-----
Subject      : CN=TA-SCEP-1-CA
Issuer       : CN=TA-SCEP-1-CA
Serial       : 681670E9EFB7FCB74E79C33DD9D54847
Expiry       : Apr 25 13:36:42 2027 GMT
```

```
Certificate Revocation List
-----
Issuer       : CN=TA-SCEP-1-CA
Last Update  : May 23 13:27:21 2022 GMT
```

>

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## OpenVPN

OpenVPN is an open-source Virtual Private Network (VPN) technology that creates secure point-to-point or site-to-site connections in routed or bridged configurations. OpenVPN uses a custom security protocol that is Secure Socket Layer (SSL) / Transport Layer Security (TLS) for key exchange. It uses standard encryption and authentication algorithms for data privacy and authentication over TCP or UDP.

The OpenVPN server can push the network configuration, such as the topology and IP routes, to OpenVPN clients. This makes OpenVPN simpler to configure as it reduces the chances of a configuration mismatch between the client and server. OpenVPN also supports cipher negotiation between the client and server. This means you can configure the OpenVPN server and clients with a range of different cipher options and the server will negotiate with the client on the cipher to use for the connection.

For more information on OpenVPN, see [www.openvpn.net](http://www.openvpn.net).

### **OpenVPN modes:**

There are two modes for running OpenVPN:

- Routing mode, also known as TUN.
- Bridging mode, also known as TAP.

### **Routing (TUN) mode**

In routing mode, each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.

The manner in which the IP subnets are defined depends on the OpenVPN topology in use. The Connect EZ device supports two types of OpenVPN topology:

OpenVPN Topology	Subnet definition method
net30	Each OpenVPN client is assigned a /30 subnet within the IP subnet specified in the OpenVPN server configuration. With net30 topology, pushed routes are used, with the exception of the default route. Automatic route pushing (exec) is not allowed, because this would not inform the firewall and would be blocked.
subnet	Each OpenVPN client connected to the OpenVPN server is assigned an IP address within the IP subnet specified in the OpenVPN server configuration. For the Connect EZ device, pushed routes are not allowed; you will need to manually configure routes on the device.

For more information on OpenVPN topologies, see [OpenVPN topology](#).

### **Bridging (TAP) mode**

In bridging mode, a LAN interface on the OpenVPN server is assigned to OpenVPN. The LAN interfaces of the OpenVPN clients are on the same IP subnet as the OpenVPN server's LAN interface. This means that devices connected to the OpenVPN client's LAN interface are on the same IP subnet as devices. The Connect EZ device supports two mechanisms for configuring an OpenVPN server in TAP mode:

- OpenVPN managed—The Connect EZ device creates the interface and then uses its standard configuration to set up the connection (for example, its standard DHCP server configuration).
- Device only—IP addressing is controlled by the system, not by OpenVPN.

### ***Additional OpenVPN information***

For more information on OpenVPN, see these resources:

[Bridging vs. routing](#)

[OpenVPN/Routing](#)

## **Configure an OpenVPN server**

### **Required configuration items**

- Enable the OpenVPN server.  
The OpenVPN server is enabled by default.
- The mode used by the OpenVPN server, one of:
  - **TUN (OpenVPN managed)**—Also known as routing mode. Each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.
  - **TAP - OpenVPN managed**—Also know as bridging mode. A more advanced implementation of OpenVPN. The Connect EZ device creates an OpenVPN interface and uses standard interface configuration (for example, a standard DHCP server configuration).
  - **TAP - Device only**—An alternate form of OpenVPN bridging mode, in which the device, rather than OpenVPN, controls the interface configuration. If this method is is, the OpenVPN server must be included as a device in either an interface or a bridge.
- The firewall zone to be used by the OpenVPN server.
- The IP network and subnet mask of the OpenVPN server.
- The server's Certificate authority (CA) certificate, and public, private and Diffie-Hellman (DH) keys.
- An OpenVPN authentication group and an OpenVPN user.
- Determine the method of certificate management:
  - Certificates managed by the server.
  - Certificates created externally and added to the server.
- If certificates are created and added to the server, determine the level of authentication:
  - Certificate authentication only.
  - Username and password authentication only.
  - Certificate and username and password authentication.

If username and password authentication is used, you must create an OpenVPN authentication group and user. See [Configure an OpenVPN Authentication Group and User](#) for instructions.
- Certificates and keys:
  - The **CA certificate** (usually in a ca.crt file).
  - The **Public key** (for example, server.crt)

- The **Private key** (for example, server.key).
- The **Diffie Hellman key** (usually in dh2048.pem).
- Active recovery configuration. See [Configure SureLink active recovery for OpenVPN](#) for information about OpenVPN active recovery.

### Additional configuration items

- The route metric for the OpenVPN server.
- The range of IP addresses that the OpenVPN server will provide to clients.
- The TCP/UDP port to use. By default, the Connect EZ device uses port **1194**.
- Access control list configuration to restrict access to the OpenVPN server through the firewall.
- Additional OpenVPN parameters.

## Web

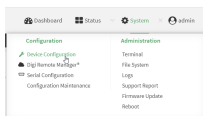
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

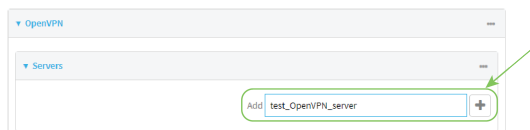
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > OpenVPN > Servers**.
4. For **Add**, type a name for the OpenVPN server and click **+**.



The new OpenVPN server configuration is displayed.

The OpenVPN server is enabled by default. To disable, toggle off **Enable**.

5. For **Device type**, select the mode used by the OpenVPN server, either:
  - **TUN (OpenVPN managed)**
  - **TAP - OpenVPN managed**
  - **TAP - Device only**
- See [OpenVPN](#) for information about OpenVPN server modes.
6. If **TUN (OpenVPN managed)** or **TAP - OpenVPN managed** is selected for **Device type**:
  - a. For **Zone**, select the firewall zone for the OpenVPN server. For TUN device types, this should be set to **Internal** to treat clients as LAN devices.
  - b. (Optional) Select the **Metric** for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used. The default setting is **0**.
  - c. For **Address**, type the IP address and subnet mask of the OpenVPN server.
  - d. (Optional) For **First IP address** and **Last IP address**, set the range of IP addresses that the OpenVPN server will use when providing IP addresses to clients. The default is from **80** to **99**.
7. (Optional) Set the **VPN port** that the OpenVPN server will use. The default is **1194**.
8. For **Server managed certificates**, determine the method of certificate management. If enabled, the server will manage certificates. If not enabled, certificates must be created externally and added to the server.
9. If **Server managed certificates** is not enabled:
  - a. Select the **Authentication** type:
    - **Certificate only**: Uses only certificates for client authentication. Each client requires a public and private key.
    - **Username/password only**: Uses a username and password for client authentication. You must create an OpenVPN authentication group and user. See [Configure an OpenVPN Authentication Group and User](#) for instructions.
    - **Certificate and username/password**: Uses both certificates and a username and password for client authentication. Each client requires a public and private key, and you must create an OpenVPN authentication group and user. See [Configure an OpenVPN Authentication Group and User](#) for instructions.

- b. Paste the contents of the **CA certificate** (usually in a ca.crt file), the **Public key** (for example, server.crt), the **Private key** (for example, server.key), and the **Diffie Hellman key** (usually in dh2048.pem) into their respective fields. The contents will be hidden when the configuration is saved.
10. (Optional) Click to expand **Access control list** to restrict access to the OpenVPN server:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the service-type.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the service-type.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
11. (Optional) Click to expand **Advanced Options** to manually set additional OpenVPN parameters.
  - a. Click **Enable** to enable the use of additional OpenVPN parameters.
  - b. Click **Override** if the additional OpenVPN parameters should override default options.
  - c. For **OpenVPN parameters**, type the additional OpenVPN parameters.
12. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> add vpn openvpn server name
(config vpn openvpn server name)>
```

---

where *name* is the name of the OpenVPN server.

The OpenVPN server is enabled by default. To disable the server, type:

---

```
(config vpn openvpn server name)> enable false
(config vpn openvpn server name)>
```

---

4. Set the mode used by the OpenVPN server:

---

```
(config vpn openvpn server name)> device_type value
(config vpn openvpn server name)>
```

---

where *value* is one of:

- **TUN (OpenVPN managed)**—Also known as routing mode. Each OpenVPN client is assigned a different IP subnet from the OpenVPN server and other OpenVPN clients. OpenVPN clients use Network Address Translation (NAT) to route traffic from devices connected on its LAN interfaces to the OpenVPN server.
- **TAP - OpenVPN managed**—Also know as bridging mode. A more advanced implementation of OpenVPN. The Connect EZ device creates an OpenVPN interface and uses standard interface configuration (for example, a standard DHCP server configuration).
- **TAP - Device only**—An alternate form of OpenVPN bridging mode, in which the device, rather than OpenVPN, controls the interface configuration. If this method is is, the OpenVPN server must be included as a device in either an interface or a bridge.

See [OpenVPN](#) for information about OpenVPN modes. The default is **tun**.

5. If **tap** or **tun** are set for **device\_type**:

- a. Set the IP address and subnet mask of the OpenVPN server.

---

```
(config vpn openvpn server name)> address ip_address/netmask
(config vpn openvpn server name)>
```

---

- b. Set the firewall zone for the OpenVPN server. For TUN device types, this should be set to **internal** to treat clients as LAN devices.

---

```
(config vpn openvpn server name)> zone value
(config vpn openvpn server name)>
```

---

To view a list of available zones:

---

```
(config vpn openvpn server name)> firewall zone ?
```

Zone: The zone for the local TUN interface. To treat clients as LAN devices this would usually be set to internal.

Format:

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

Current value:

---

```
(config vpn openvpn server name)>
```

---

- c. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

---

```
(config vpn openvpn server name)> metric value
(config vpn openvpn server name)>
```

---

where *value* is an interger between **0** and **65535**. The default is **0**.

- d. (Optional) Set the range of IP addresses that the OpenVPN server will use when providing IP addresses to clients:
- i. Set the first address in the range limit:

---

```
(config vpn openvpn server name)> server_first_ip value
(config vpn openvpn server name)>
```

---

where *value* is a number between **1** and **255**. The number entered here will represent the first client IP address. For example, if **address** is set to **192.168.1.1/24** and **server\_first\_ip** is set to **80**, the first client IP address will be 192.168.1.80.

The default is from **80**.

- ii. Set the last address in the range limit:

---

```
(config vpn openvpn server name)> server_last_ip value
(config vpn openvpn server name)>
```

---

where *value* is a number between **1** and **255**. The number entered here will represent the last client IP address. For example, if **address** is set to **192.168.1.1/24** and **server\_last\_ip** is set to **99**, the last client IP address will be 192.168.1.80.

The default is from **80**.



6. (Optional) Set the port that the OpenVPN server will use:

---

```
(config vpn openvpn server name)> port port
(config vpn openvpn server name)>
```

---

The default is **1194**.

7. Determine the method of certificate management:
- a. To allow the server to manage certificates:

---

```
(config vpn openvpn server name)> autogenerate true
(config vpn openvpn server name)>
```

---

- b. To create certificates externally and add them to the server

---

```
(config vpn openvpn server name)> autogenerate false
(config vpn openvpn server name)>
```

---

The default setting is **false**.

- c. If **autogenerate** is set to false:
  - i. Set the authentication type:

---

```
(config vpn openvpn server name)> authentication value
(config vpn openvpn server name)>
```

---

where *value* is one of:

- **cert**: Uses only certificates for client authentication. Each client requires a public and private key.
  - **passwd**: Uses a username and password for client authentication. You must create an OpenVPN authentication group and user. See [Configure an OpenVPN Authentication Group and User](#) for instructions.
  - **cert\_passwd**: Uses both certificates and a username and password for client authentication. Each client requires a public and private key, and you must create an OpenVPN authentication group and user. See [Configure an OpenVPN Authentication Group and User](#) for instructions.
- ii. Paste the contents of the CA certificate (usually in a ca.crt file) into the value of the **cacert** parameter:
 

---

```
(config vpn openvpn server name)> cacert value
(config vpn openvpn server name)>
```

---
  - iii. Paste the contents of the public key (for example, server.crt) into the value of the **server\_cert** parameter:
 

---

```
(config vpn openvpn server name)> server_cert value
(config vpn openvpn server name)>
```

---
  - iv. Paste the contents of the private key (for example, server.key) into the value of the **server\_key** parameter:

---

```
(config vpn openvpn server name)> server_key value
(config vpn openvpn server name)>
```

---

- v. Paste the contents of the Diffie Hellman key (usually in dh2048.pem) into the value of the **diffie** parameter:

---

```
(config vpn openvpn server name)> diffie value
(config vpn openvpn server name)>
```

---

8. (Optional) Set the access control list to restrict access to the OpenVPN server:

- To limit access to specified IPv4 addresses and networks:

---

```
(config vpn openvpn server name)> add acl address end value
(config vpn openvpn server name)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config vpn openvpn server name)> add acl address6 end value
(config vpn openvpn server name)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config vpn openvpn server name)> add acl interface end value
(config vpn openvpn server name)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config vpn openvpn server name)> add acl zone end value
(config vpn openvpn server name)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

```
(config vpn openvpn server name)> ... firewall zone ?

Zones: A list of groups of network interfaces that can be
referred to by packet
filtering rules and access control lists.

Additional Configuration
-----
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup

(config vpn openvpn server name)>
```

Repeat this step to include additional firewall zones.

9. (Optional) Set additional OpenVPN parameters.

a. Enable the use of additional OpenVPN parameters:

```
(config vpn openvpn server name)> advanced_options enable true
(config vpn openvpn server name)>
```

b. Configure whether the additional OpenVPN parameters should override default options:

```
(config vpn openvpn server name)> advanced_options override true
(config vpn openvpn server name)>
```

c. Set the additional OpenVPN parameters:

```
(config vpn openvpn server name)> extra parameters
(config vpn openvpn server name)>
```

10. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure an OpenVPN Authentication Group and User

If username and password authentication is used for the OpenVPN server, you must create an OpenVPN authentication group and user.

See [Configure an OpenVPN server](#) for information about configuring an OpenVPN server to use username and password authentication. See [Connect EZ user authentication](#) for more information about creating authentication groups and users.

### Web

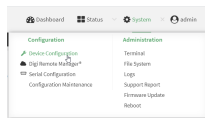
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

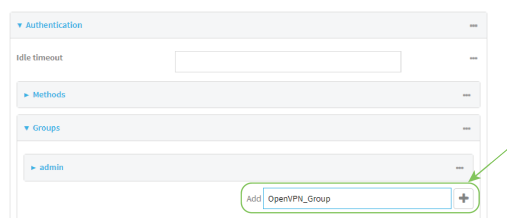
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

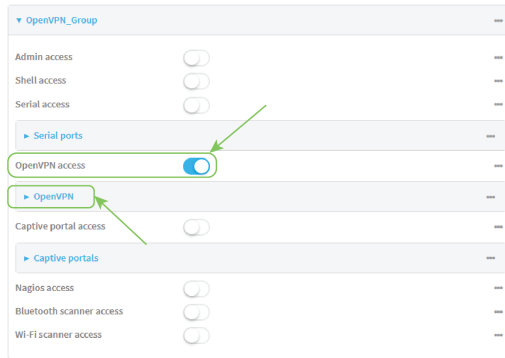


The **Configuration** window is displayed.

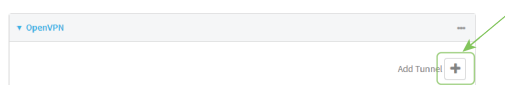
3. Add an OpenVPN authentication group:
  - a. Click **Authentication > Groups**.
  - b. For **Add Group**, type a name for the group (for example, **OpenVPN\_Group**) and click **+**.



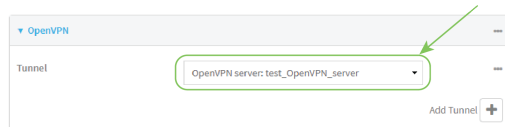
The new authentication group configuration is displayed.



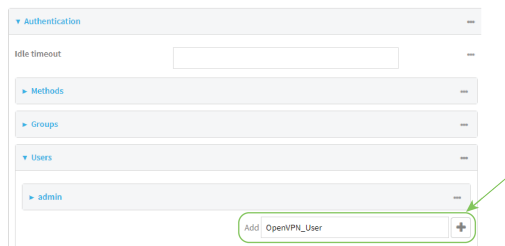
- c. Click **OpenVPN access** to enable OpenVPN access rights for users of this group.
- d. Click to expand the **OpenVPN** node.
- e. Click **+** to add a tunnel.



- f. For **Tunnel**, select an OpenVPN tunnel to which users of this group will have access.

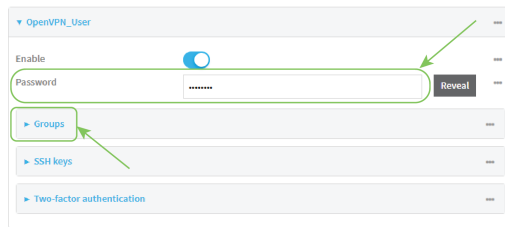


- g. Repeat to add additional OpenVPN tunnels.
- 4. Add an OpenVPN authentication user:
  - a. Click **Authentication > Users**.
  - b. For **Add**, type a name for the user (for example, **OpenVPN\_User**) and click **+**.



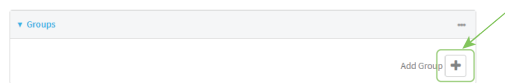
- c. Type a password for the user.  
 This password is used for local authentication of the user. You can also configure the user to use RADIUS or TACACS+ authentication by configuring authentication methods. See [User authentication methods](#) for information.

- d. Click to expand the **Groups** node.



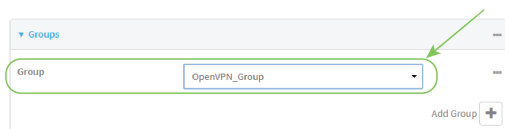
The screenshot shows the configuration page for an OpenVPN user. The 'Groups' node is expanded and highlighted with a green box and a green arrow. The 'Enable' toggle is turned on, and the 'Password' field is visible with a 'Reveal' button. Other nodes like 'SSH keys' and 'Two-factor authentication' are also visible.

- e. Click **+** to add a group to the user.



The screenshot shows the configuration page for groups. The 'Add Group +' button is highlighted with a green box and a green arrow.

- f. Select a **Group** with **OpenVPN access** enabled.



The screenshot shows the configuration page for groups. The 'Group' dropdown menu is highlighted with a green box and a green arrow, showing 'OpenVPN\_Group' selected. The 'Add Group +' button is also visible.

5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **add auth group** command to add a new authentication. For example, to add a group named **OpenVPN\_Group**:

```
(config)> add auth group OpenVPN_Group
(config auth group OpenVPN_Group)>
```

4. Enable OpenVPN access rights for users of this group:

```
(config auth group OpenVPN_Group)> acl openvpn enable true
```

5. Add an OpenVPN tunnel to which users of this group will have access:
  - a. Determine available tunnels:

```
(config auth group OpenVPN_Group)> .. .. .. vpn openvpn server ?
```

Servers: A list of openvpn servers

Additional Configuration

-----  
-----

OpenVPN_server1	OpenVPN server
-----------------	----------------

```
(config auth group OpenVPN_Group)>
```

- b. Add a tunnel:

```
(config auth group OpenVPN_Group)> add auth group test acl openvpn
tunnels end /vpn/openvpn/server/OpenVPN_server1
(config auth group OpenVPN_Group)>
```

6. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure an OpenVPN client by using an .ovpn file

### Required configuration items

- Enable the OpenVPN client.  
The OpenVPN client is enabled by default.
- The firewall zone to be used by the OpenVPN client.

### Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.

See [Configure SureLink active recovery for OpenVPN](#) for information about OpenVPN active recovery.

### ≡ Web

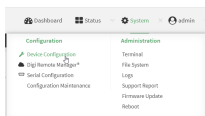
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > OpenVPN > Clients**.
4. For **Add**, type a name for the OpenVPN client and click **+**.



The new OpenVPN client configuration is displayed.



5. The OpenVPN client is enabled by default. To disable, toggle off **Enable**.
6. The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually, click **Use .ovpn file** to disable. If **Use .ovpn file** is disabled, see [Configure an OpenVPN client without using an .ovpn file](#) for configuration information.
7. For **Zone**, select the firewall zone for the OpenVPN client.
8. (Optional) Select the **Metric** for the OpenVPN client. If multiple active routes match a destination, the route with the lowest metric will be used.
9. (Optional) For **Username** and **Password**, type the login credentials as configured on the OpenVPN server.
10. For **OVPN file**, paste the content of the client.ovpn file.
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> add vpn openvpn client name
(config vpn openvpn client name)>
```

where *name* is the name of the OpenVPN server.

The OpenVPN client is enabled by default. To disable the client, type:

```
(config vpn openvpn client name)> enable false
(config vpn openvpn client name)>
```

4. Set the firewall zone for the OpenVPN client:

---

```
(config vpn openvpn client name)> zone value
(config vpn openvpn client name)>
```

---

To view a list of available zones:

---

```
(config vpn openvpn client name)> zone ?
```

Zone: The zone for the openvpn client interface.

Format:

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

Current value:

---

```
(config vpn openvpn client name)>
```

---

5. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

---

```
(config vpn openvpn client name)> metric value
(config vpn openvpn client name)>
```

---

where *value* is an interger between **0** and **65535**. The default is **0**.

6. (Optional) Set the login credentials as configured on the OpenVPN server:

---

```
(config vpn openvpn client name)> username value
(config vpn openvpn client name)> password value
(config vpn openvpn client name)>
```

---

7. Paste the content of the client.ovpn file into the value of the **config\_file** parameter:

---

```
(config vpn openvpn client name)> config_file value
(config vpn openvpn client name)>
```

---

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure an OpenVPN client without using an .ovpn file

### Required configuration items

- Enable the OpenVPN client.  
The OpenVPN client is enabled by default.
- The mode used by the OpenVPN server, either routing (TUN), or bridging (TAP).
- The firewall zone to be used by the OpenVPN client.
- The IP address of the OpenVPN server.
- Certificates and keys:
  - The **CA certificate** (usually in a ca.crt file).
  - The **Public key** (for example, client.crt)
  - The **Private key** (for example, client.key).

### Additional configuration items

- The route metric for the OpenVPN client.
- The login credentials for the OpenVPN client, if configured on the OpenVPN server.
- Additional OpenVPN parameters.

See [Configure SureLink active recovery for OpenVPN](#) for information about OpenVPN active recovery.

## ≡ Web

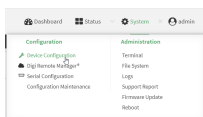
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

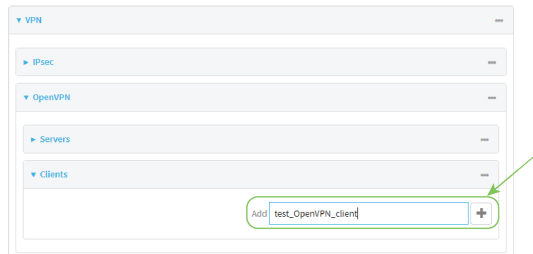
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



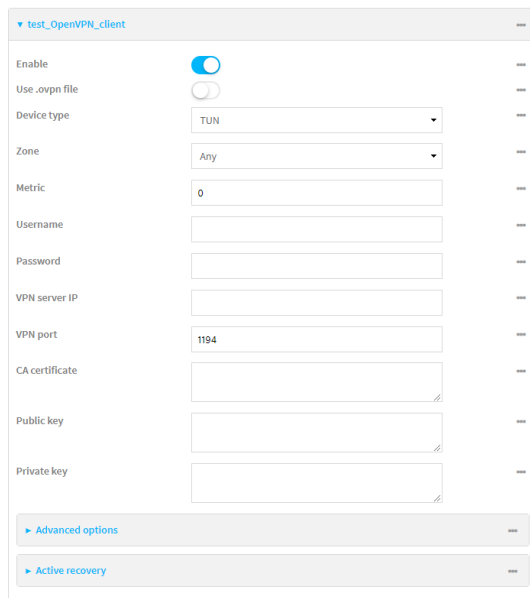
The **Configuration** window is displayed.

3. Click **VPN > OpenVPN > Clients**.

- For **Add**, type a name for the OpenVPN client and click **+**.



The new OpenVPN client configuration is displayed.



- The OpenVPN client is enabled by default. To disable, toggle off **Enable**.
- The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually, click **Use .ovpn file** to disable.
- For **Device type**, select the mode used by the OpenVPN server, either **TUN** or **TAP**.
- For **Zone**, select the firewall zone for the OpenVPN client.
- (Optional) Select the **Metric** for the OpenVPN client. If multiple active routes match a destination, the route with the lowest metric will be used.
- (Optional) For **Username** and **Password**, type the login credentials as configured on the OpenVPN server.
- For **VPN server IP**, type the IP address of the OpenVPN server.
- (Optional) Set the **VPN port** used by the OpenVPN server. The default is **1194**.
- Paste the contents of the **CA certificate** (usually in a ca.crt file), the **Public key** (for example, client.crt), and the **Private key** (for example, client.key) into their respective fields. The contents will be hidden when the configuration is saved.
- (Optional) Click to expand **Advanced Options** to manually set additional OpenVPN parameters.

- a. Click **Enable** to enable the use of additional OpenVPN parameters.
  - b. Click **Override** if the additional OpenVPN parameters should override default options.
  - c. For **OpenVPN parameters**, type the additional OpenVPN parameters. For example, to override the configuration by using a configuration file, enter **--config filename**, for example, **--config /etc/config/openvpn\_config**.
15. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> add vpn openvpn client name
(config vpn openvpn client name)>
```

---

where *name* is the name of the OpenVPN server.

The OpenVPN client is enabled by default. To disable the client, type:

---

```
(config vpn openvpn client name)> enable false
(config vpn openvpn client name)>
```

---

4. The default behavior is to use an OVPN file for client configuration. To disable this behavior and configure the client manually:

---

```
(config vpn openvpn client name)> use_file false
(config vpn openvpn client name)>
```

---

5. Set the mode used by the OpenVPN server:

---

```
(config vpn openvpn client name)> device_type value
(config vpn openvpn client name)>
```

---

where *value* is either **tun** or **tap**. The default is **tun**.

6. Set the firewall zone for the OpenVPN client:

---

```
(config vpn openvpn client name)> zone value
(config vpn openvpn client name)>
```

---

To view a list of available zones:

---

```
(config vpn openvpn client name)> zone ?
```

---

Zone: The zone for the openvpn client interface.

---

---

```
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup
Current value:
```

```
(config vpn openvpn client name)>
```

---

7. (Optional) Set the route metric for the OpenVPN server. If multiple active routes match a destination, the route with the lowest metric will be used.

```
(config vpn openvpn client name)> metric value
(config vpn openvpn client name)>
```

---

where *value* is an interger between **0** and **65535**. The default is **0**.

8. (Optional) Set the login credentials as configured on the OpenVPN server:

```
(config vpn openvpn client name)> username value
(config vpn openvpn client name)> password value
(config vpn openvpn client name)>
```

---

9. Set the IP address of the OpenVPN server:

```
(config vpn openvpn client name)> server ip_address
(config vpn openvpn client name)>
```

---

10. (Optional) Set the port used by the OpenVPN server:

```
(config vpn openvpn client name)> port port
(config vpn openvpn client name)>
```

---

The default is **1194**.

11. Paste the contents of the CA certificate (usually in a ca.crt file) into the value of the **cacert** parameter:

```
(config vpn openvpn client name)> cacert value
(config vpn openvpn client name)>
```

---

12. Paste the contents of the public key (for example, client.crt) into the value of the **public\_cert** parameter:

```
(config vpn openvpn client name)> public_cert value
(config vpn openvpn client name)>
```

---

13. Paste the contents of the private key (for example, client.key) into the value of the **private\_key** parameter:

---

```
(config vpn openvpn client name)> private_key value
(config vpn openvpn client name)>
```

---

14. (Optional) Set additional OpenVPN parameters.

- a. Enable the use of additional OpenVPN parameters:

---

```
(config vpn openvpn client name)> advanced_options enable true
(config vpn openvpn client name)>
```

---

- b. Configure whether the additional OpenVPN parameters should override default options:

---

```
(config vpn openvpn client name)> advanced_options override true
(config vpn openvpn client name)>
```

---

- c. Set the additional OpenVPN parameters:

---

```
(config vpn openvpn client name)> advanced_options extra parameters
(config vpn openvpn client name)>
```

---

15. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

16. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure SureLink active recovery for OpenVPN

You can configure the Connect EZ device to regularly probe OpenVPN client connections to determine if the connection has failed and take remedial action.

### Required configuration items

- A valid OpenVPN client configuration. See [Configure an OpenVPN client by using an .ovpn file](#) or [Configure an OpenVPN client without using an .ovpn file](#) for configuration instructions.
- Enable OpenVPN SureLink.
- The behavior of the Connect EZ device upon OpenVPN failure: either
  - Restart the OpenVPN interface
  - Reboot the device.

### Additional configuration items

- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.
- The number of probe failures before the OpenVPN connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe failures before considering it to have failed.

To configure the Connect EZ device to regularly probe the OpenVPN connection:

## Web

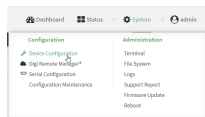
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > OpenVPN > Clients**.
4. Create a new OpenVPN client or select an existing one:
  - To create a new OpenVPN client, see [Configure an OpenVPN client by using an .ovpn file](#) or [Configure an OpenVPN client without using an .ovpn file](#).
  - To edit an existing OpenVPN client, click to expand the appropriate client.
5. After creating or selecting the OpenVPN client, click **SureLink**.

▼ SureLink ⋮

Enable	<input type="checkbox"/>	<span>⋮</span>
Test interval	<input type="text" value="15m"/>	<span>⋮</span>
Success condition	<input type="text" value="One test passes"/>	<span>⋮</span>
Pass threshold	<input type="text" value="1"/>	<span>⋮</span>
Response timeout	<input type="text" value="15s"/>	<span>⋮</span>

▶ Tests ⋮

▶ Recovery actions ⋮

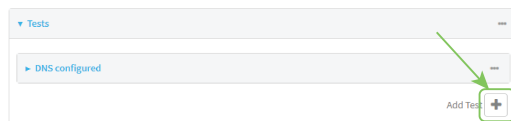
▶ Advanced settings ⋮



6. **Enable** SureLink.
7. (Optional) Change the **Test interval** between connectivity tests.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.  
The default is 15 minutes.
8. (Optional) If more than one test target is configured, for **Success condition**, select either:
  - **One test passes:** Only one test needs to pass for Surelink to consider an interface to be up.
  - **All test pass:** All tests need to pass for SureLink to consider the interface to be up.
9. (Optional) For **Pass threshold**, type or select the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.
10. (Optional) For **Response timeout**, type the amount of time that the device should wait for a response to a test failure before considering it to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Response timeout** to ten minutes, enter **10m** or **600s**.  
The default is 15 seconds.
11. Click to expand **Tests**.

By default, **Test DNS servers configured for this interface** is automatically configured and enabled. This test communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

- a. Click **+**.



New tests are enabled by default. To disable, click to toggle off **Enable**.

- b. Type a **Label** for the test.
- c. Click to toggle on **IPv6** if the test should apply to both IPv6 rather than IPv4.
- d. Select the **Test type**.

Available test types:

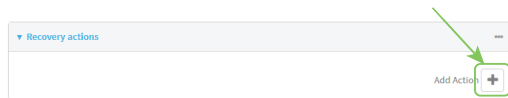
- **Ping test:** Uses ICMP to determine connectivity.

If **Ping test** is selected, complete the following:

- **Ping target:** The type of target for the ping, one of:
  - **Hostname or IP address** of an external server.
  - **Ping host:** hostname or IP address of the server.
  - The **Interface gateway**. If **Interface gateway** is selected, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.

- The **Interface address**.
- The **Interface DNS** server.
- **Ping payload size**: The number of bytes to send as part of the ping payload.
- **DNS test**: Performs a DNS query to the named DNS server.  
If **DNS test** is selected, complete the following:
  - **DNS server**: The IP address of the DNS server.
- **HTTP test**: Uses HTTP(s) GET requests to determine connectivity to the configured web server.  
If **HTTP test** is selected, complete the following:
  - **Web server**: The URL of the web server.
- **Test DNS servers configured for this interface**: Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **Test the interface status**: Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.  
If **Test the interface status** is selected, complete the following:
  - **Down time**: The amount of time that the interface is down before the test can be considered to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number(w|d|h|m|s)*.  
For example, to set **Down time** to ten minutes, enter **10m** or **600s**.
  - **Initial connection time**: The amount of time to wait for the interface to connect for the first time before the test is considered to have failed.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format *number(w|d|h|m|s)*.  
For example, to set **Initial connection time** to ten minutes, enter **10m** or **600s**.
- **Custom test**: Tests the interface with custom commands.  
If **Custom test** is selected, complete the following:
  - The **Commands to run to test**.
- **TCP connection test**: Tests that the interface can reach a destination port on the configured host.  
If **TCP connection test** is selected, complete the following:
  - **TCP connect host**: The hostname or IP address of the host to create a TCP connection to.
  - **TCP connect port**: The TCP port to create a TCP connection to.
- **Test another interface's status**: Tests the status of another interface.  
If **Test another interface's status** is selected, complete the following:

- **Test interface:** The interface to test.
  - **IP version:** The type of IP connection, one of:
    - **Any:** Either the IPv4 or IPv6 connection must be up.
    - **Both:** Both the IPv4 or IPv6 connection must be up.
    - **IPv4:** The IPv4 connection must be up.
    - **IPv6:** The IPv6 connection must be up.
  - **Expected status:** The status required for the test to pass.
    - **Up:** The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
    - **Down:** The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).
- e. Repeat for each additional test.
12. Add recovery actions:
- a. Click to expand **Recovery actions**.
- By default, there are two preconfigured recovery actions:
- **Update routing:** Uses the **Change default gateway** action, which increases the interface's metric by 100 to change the default gateway.
  - **Restart interface.**
- b. Click **+**.



New recovery actions are enabled by default. To disable, click to toggle off **Enable**.

- c. Type a **Label** for the recovery action.
- d. For **Recovery type**, select **Reboot device**.
- e. For **Recovery type**, select the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed.
- **Change default gateway:** Increases the interface's metric to change the default gateway.
 

If **Change default gateway** is selected, complete the following:

    - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
    - **Increase metric to change active default gateway:** Increase the interface's metric by this amount. This should be set to a number large enough to change the routing table to use another default gateway. The default is **100**.
    - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
  - **Restart interface.**

If **Restart interface** is selected, complete the following:

- **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
- **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Reset modem:** This recovery action is available for WWAN interfaces only.  
If **Reset modem** is selected, complete the following:
  - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Switch to alternate SIM:** Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.  
If **Switch to alternate SIM** is selected, complete the following:
  - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Reboot device.**  
If **Reboot device** is selected, complete the following:
  - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
  - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Execute custom Recovery commands.**  
If **Recovery commands** is selected, complete the following:
  - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.
  - The **Commands to run to recovery connectivity.**
  - **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- **Powercycle the modem.** This recovery action is available for WWAN interfaces only.  
If **Powercycle the modem** is selected, complete the following:
  - **SureLink test failures:** The number of failures for this recovery action to perform, before moving to the next recovery action.

- **Override wait interval before performing the next recovery action:** The time to wait before the next test is run. If set to the default value of **0s**, the **Test interval** is used.
- f. Repeat for each additional recovery action.
13. (Optional) Configure advanced SureLink parameters:
    - a. Click to expand **Advanced settings**.
    - b. For **Delayed Start**, type the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Delayed start** to ten minutes, enter **10m** or **600s**.  
 The default is 300 seconds.
    - c. For **Backoff interval**, type the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.  
 Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
 For example, to set **Backoff interval** to ten minutes, enter **10m** or **600s**.  
 The default is 300 seconds.
    - d. **Test interface gateway by pinging** is used by the **Interface gateway Ping test** as the endpoint for traceroute to use to determine the interface gateway. The default is 8.8.8.8, and should only be changed if this IP address is not accessible due to networking issues.
  14. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
 Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:
 

```
> config
(config)>
```
3. Create a new OpenVPN client, or edit an existing one:
  - To create a new OpenVPN client, see [Configure an OpenVPN client by using an .ovpn file](#) or [Configure an OpenVPN client without using an .ovpn file](#).
  - To edit an existing OpenVPN client, change to the OpenVPN client's node in the configuration schema. For example, for an OpenVPN client named **openvpn\_client1**, change to the **openvpn\_client1** node in the configuration schema:

```
(config)> vpn openvpn client openvpn_client1
(config vpn openvpn client openvpn_client1)>
```

## 4. Enable SureLink:

---

```
(config vpn openvpn client openvpn_client1)> surelink enable true
(config vpn openvpn client openvpn_client1)>
```

---

5. By default, the **Test DNS servers configured for this interface** test is automatically configured and enabled. This tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.

To add additional tests:

## a. Add a test:

---

```
(config vpn openvpn client openvpn_client1)> add surelink tests end
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

## b. New tests are enabled by default. To disable:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> enable
false
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

## c. Create a label for the test:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> label
string
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

## d. if the test should apply to both IPv6 rather than IPv4, enable IPv6:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ipv6
true
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

## e. Set the test type:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> test
value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

where *value* is one of:

- **ping:** Uses ICMP to determine connectivity.

If **ping** is selected, complete the following:

- Set the **ping\_method**:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
ping_method value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

where *value* is one of:

- **hostname:** The hostname or IP address of an external server.
- Set **ping\_host** to the hostname or IP address of the server:

---

```
(config vpn openvpn client openvpn_client1 surelink tests
1)> ping_host hostname/IP_address
(config vpn openvpn client openvpn_client1 surelink tests
1)>
```

---

- **interface\_gateway.** If set, an initial traceroute is sent to the hostname or IP address configured in the SureLink advanced settings, and then the first hop in that route is used for the ping test.
- **interface\_address.**
- **interface\_dns:** The interface's DNS server.
- Set the number of bytes to send as part of the ping payload:

---

```
(config vpn openvpn client openvpn_client1 openvpn client
openvpn_client1 surelink tests 1)> ping_size int
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

- **dns:** Performs a DNS query to the named DNS server.

If **dns** is set, set the IPv4 or IPv6 address of the DNS server:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
dns_server IP_address
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

- **http:** Uses HTTP(s) GET requests to determine connectivity to the configured web server.

If **http** is set, set the URL of the web server.

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
http url
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

- **dns\_configured:** Tests communication with DNS servers that are either provided by DHCP, or statically configured for this interface.
- **interface\_up:** Tests the current status of the interface. The test fails if the interface is down. Failing this test infers that all other tests fail.

If **interface\_up** is set, complete the following:

- Set the amount of time that the interface is down before the test can be considered to have failed.

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
interface_down_time value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format ***number*{w|d|h|m|s}**.

For example, to set **interface\_down\_time** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
interface_down_time 600s
(config)>
```

- Set the amount of time to wait for the interface to connect for the first time before the test is considered to have failed.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
interface_timeout value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interface\_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
interface_timeout 600s
(config)>
```

- **custom\_test**: Tests the interface with custom commands.

If **custom\_test** is set, set the commands to run to perform the test:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
custom_test_commands "string"
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **tcp\_connection**: Tests that the interface can reach a destination port on the configured host.

If **tcp\_connection** is selected, complete the following:

- Set the hostname or IP address of the host to create a TCP connection to:

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
tcp_host hostname/IP_address
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- Set the TCP port to create a TCP connection to.

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
tcp_port port
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

- **other**: Tests the status of another interface.

If **other** is selected, complete the following:



- Set the interface to test.
  - i. Use the ? to determine available interfaces:
  - ii. Set the interface. For example:

---

```
(config vpn openvpn client openvpn_client1 surelink tests
1)> other_interface /network/interface/eth1
(config vpn openvpn client openvpn_client1 surelink tests
1)>
```

---

- Set the type of IP connection:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
other_ip_version value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

where *value* is one of:

- **any**: Either the IPv4 or IPv6 connection must be up.
  - **both**: Both the IPv4 or IPv6 connection must be up.
  - **ipv4**: The IPv4 connection must be up.
  - **ipv6**: The IPv6 connection must be up.
- The status required for the test to pass.

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)>
other_status value
(config vpn openvpn client openvpn_client1 surelink tests 1)>
```

---

where *value* is one of:

- **up**: The test will pass only if the referenced interface is up and passing its own SureLink tests (if applicable).
- **down**: The test will pass only if the referenced interface is down or failing its own SureLink tests (if applicable).

f. Repeat for each additional test.

## 6. Add recovery actions:

- a. Type ... to return to the root of the configuration:

---

```
(config vpn openvpn client openvpn_client1 surelink tests 1)> ...
(config)>
```

---

- b. Add a recovery action:

---

```
(config)> add vpn openvpn client openvpn_client1 surelink actions end
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

---

- c. New actions are enabled by default. To disable:

---

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> enable
false
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

---

- d. Create a label for the action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> label
string
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- e. Set the type of recovery action to **reboot\_device**:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> action
reboot_device
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)>
test_failures int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

```
(config vpn openvpn client openvpn_client1 surelink actions 0)>
override_interval int
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- f. Set the type of recovery action. If multiple recovery actions are configured, they are performed in the order that they are listed. The command varies depending on whether the interface is a WAN or WWAN:

- WAN interfaces:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)>
action value
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

- WWAN interfaces:

```
(config vpn openvpn client openvpn_client1 surelink actions 0)>
modem_action value
(config vpn openvpn client openvpn_client1 surelink actions 0)>
```

where *value* is one of:

- **update\_routing\_table**: Increases the interface's metric to change the default gateway.

If **update\_routing\_table** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the amount that the interface's metric should be increased. This should be set to a number large enough to change the routing table to use another default gateway.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> metric_adjustment_modem int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **100**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

#### ■ **restart\_interface.**

If **restart\_interface** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

#### ■ **reset\_modem:** This recovery action is available for WWAN interfaces only.

If **reset\_modem** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

- **switch\_sim**: Switches to an alternate SIM. This recovery action is available for WWAN interfaces only.

If **switch\_sim** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

- **modem\_power\_cycle**: This recovery action is available for WWAN interfaces only.

If **modem\_power\_cycle** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

- **reboot\_device.**

If **reboot\_device** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

- **custom\_action:** Execute custom recovery commands.

If **custom\_action** is selected, complete the following:

- Set the number of failures for this recovery action to perform, before moving to the next recovery action:

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> test_failures int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

The default is **3**.

- Set the commands to run to attempt to recovery connectivity.

---

```
(config network interface my_wan surelink actions 0)> custom_
action_commands_modem "string"
(config network interface my_wan surelink actions 0)>
```

---

- Set the time to wait before the next test is run. If set to the default value of **0s**, the test interval is used.

---

```
(config vpn openvpn client openvpn_client1 surelink actions
0)> override_interval int
(config vpn openvpn client openvpn_client1 surelink actions
0)>
```

---

- g. Repeat for each additional recovery action.

## 7. Optional SureLink configuration parameters:

- a. Type ... to return to the root of the configuration:

---

```
(config vpn openvpn client openvpn_client1 surelink actions 0)> ...
(config)>
```

---

- b. Set the test interval between connectivity tests:

---

```
(config)> vpn openvpn client openvpn_client1 surelink interval value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn openvpn client openvpn_client1 surelink interval 600s
(config)>
```

---

The default is **15m**.

- c. If more than one test target is configured, set the success condition:

---

```
(config)> vpn openvpn client openvpn_client1 surelink success_
condition value
(config)>
```

---

where *value* is either:

- **one**: Only one test needs to pass for Surelink to consider an interface to be up.
- **all**: All tests need to pass for SureLink to consider the interface to be up.

- d. Set the number of times that the test must pass after failure, before the interface is determined to be working and is reinstated.

---

```
(config)> vpn openvpn client openvpn_client1 surelink pass_threshold
int
(config)>
```

---

The default is **1**.

- e. Set the amount of time that the device should wait for a response to a test attempt before considering it to have failed:

---

```
(config)> vpn openvpn client openvpn_client1 surelink timeout value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn openvpn client openvpn_client1 surelink timeout 600s
(config)>
```

---

The default is **15s**.

- f. Set the amount of time to wait while the device is starting before SureLink testing begins. This setting is bypassed when the interface is determined to be up.

---

```
(config)> vpn openvpn client openvpn_client1 surelink advanced
delayed_start value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **delayed\_start** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn openvpn client openvpn_client1 surelink advanced
delayed_start 600s
(config)>
```

---

The default is **300s**.

- g. Set the time to add to the test interval when restarting the list of actions. This option is capped at 15 minutes.

---

```
(config)> vpn openvpn client openvpn_client1 surelink advanced
backoff_interval value
(config)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **backoff\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> vpn openvpn client openvpn_client1 surelink advanced
backoff_interval 600s
(config)>
```

---

The default is 300 seconds.

- h. The **interface\_gateway** parameter is used by the Interface gateway Ping test as the endpoint for traceroute to use to determine the interface gateway. The default is **8.8.8.8**, and should only be changed if this IP address is not accessible due to networking issues. To set to an alternate host:

---

```
(config)> vpn openvpn client openvpn_client1 surelink advanced
interface_gateway hostname/IP_address
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config vpn openvpn client openvpn_client1 connection_monitor target 0)>
save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.


See [Show SureLink status and statistics](#) for information about showing Surelink status for OpenVPN clients.

## Show OpenVPN server status and statistics

You can view status and statistics for OpenVPN servers from either the web interface or the command line:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status > OpenVPN > Servers**.  
The **OpenVPN Servers** page appears.
2. To view configuration details about an OpenVPN server, click the  (configuration) icon in the upper right of the OpenVPN server's status pane.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured OpenVPN servers, type the following at the prompt:

---

```
> show openvpn server all
```

Server	Enable	Type	Zone	IP Address	Port
OpenVPN_server1	true	tun	internal	192.168.30.1/24	1194
OpenVPN_server2	false	tun	internal	192.168.40.1/24	1194

```
>
```

---

3. To display details about a specific server:

---

```
> show openvpn server name OpenVPN_server1
```

```
Server           : OpenVPN_server1
Enable           : true
Type             : tun
Zone             : internal
IP Address       : 192.168.30.1/24
Port             : 1194
Use File         : true
Metric           : 0
Protocol         : udp
First IP         : 80
Last IP          : 99
```

```
>
```

---



4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show OpenVPN client status and statistics


You can view status and statistics for OpenVPN clients from either web interface or the command line:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status > OpenVPN > Clients**.

The **OpenVPN Clients** page appears.

2. To view configuration details about an OpenVPN client, click the  (configuration) icon in the upper right of the OpenVPN client's status pane.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. To display details about all configured OpenVPN clients, type the following at the prompt:

---

```
> show openvpn client all
```

Client	Enable	Status	Username	Use File	Zone
OpenVPN_Client1	true	connected		true	internal
OpenVPN_Client2	true	pending		true	internal

```
>
```

---

3. To display details about a specific client:

---

```
> show openvpn client name OpenVPN_client1
```

```
Client           : OpenVPN_client1
Enable           : true
Status           : up
Username         : user1
IP address       : 123.122.121.120
Remote           : 120.121.122.123
MTU              : 1492
Zone             : internal
IP Address       : 192.168.30.1/24
Port             : 1194
Use File         : true
Metric           : 0
```

---

---

```
Protocol      : udp
Port         : 1194
Type        : tun
```

```
>
```

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## **Generic Routing Encapsulation (GRE)**

Generic Routing Encapsulation (GRE) is an IP packet encapsulation protocol that allow for networks and routes to be advertized from one network device to another. You can use GRE to encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an IP network.

## Configuring a GRE tunnel

Configuring a GRE tunnel involves the following items:

### Required configuration items

- A GRE loopback endpoint interface.
- GRE tunnel configuration:
  - Enable the GRE tunnel.
    - The GRE tunnels are enabled by default.
  - The local endpoint interface.
  - The IP address of the remote device/peer.

### Additional configuration items

- A GRE key.
- Enable the device to respond to keepalive packets.

### Task One: Create a GRE loopback endpoint interface

#### ≡ Web

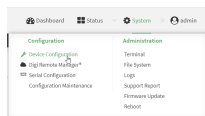
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > Interfaces**.
4. For **Add Interface**, type a name for the GRE loopback endpoint interface and click **+**.

5. **Enable** the interface.  
New interfaces are enabled by default. To disable, toggle off **Enable**.
6. For **Interface type**, select **Ethernet**.
7. For **Zone**, select **Internal**.
8. For **Device**, select **Ethernet: Loopback**.
9. Click to expand **IPv4**.
10. For **Address**, enter the IP address and subnet mask of the local GRE endpoint, for example **10.10.1.1/24**.
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the GRE endpoint interface. For example, to add an interface named **gre\_endpoint**:

```
(config)> add network interface gre_interface
(config network interface gre_interface)>
```

4. Set the interface zone to **internal**:

```
(config network interface gre_interface)> zone internal
(config network interface gre_interface)>
```

5. Set the interface device to **loopback**:

```
(config network interface gre_interface)> device /network/device/loopback
(config network interface gre_interface)>
```

6. Set the IP address and subnet mask of the local GRE endpoint. For example, to set the local GRE endpoint's IP address and subnet mask to **10.10.1.1/24**:

```
(config network interface gre_interface)> ipv4 address 10.10.1.1/24
(config network interface gre_interface)>
```

7. Save the configuration and apply the change

```
(config network interface gre_interface)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Task Two: Configure the GRE tunnel

### Web

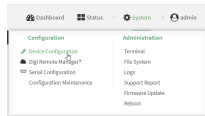
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- Click **VPN > IP Tunnels**.
- For **Add IP tunnel**, type a name for the GRE tunnel and click **+**.
- Enable** the tunnel.  
New tunnels are enabled by default. To disable, toggle off **Enable**.
- For **Mode**, select one of the following options:
  - **GRE**: Standard GRE point-to-point protocol.
  - **mGRE**: multipoint GRE protocol.
  - **GRETAP**: Ethernet over GRE.
- For **Local endpoint**, select the GRE endpoint interface created in [Task One](#).
- If **GRE** is selected for the **Mode**, for **Remote endpoint**, type the IP address of the GRE endpoint on the remote peer.
- If **GRETAP** is selected for **Mode**, for **Local endpoint**, select the interface.
- (Optional) For **Key**, enter a key that will be inserted in GRE packets created by this tunnel. It must match the key set by the remote endpoint. Allowed value is an integer between 0 and 4294967295, or an IP address.

11. (Optional) **Enable keepalive reply** to enable the device to reply to Cisco GRE keepalive packets.
12. (Optional) **Enable open routing** to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel.
13. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the GRE endpoint tunnel. For example, to add a tunnel named **gre\_example**:

```
(config)> add vpn iptunnel gre_example
(config vpn iptunnel gre_example)>
```

GRE tunnels are enabled by default. To disable:

```
(config vpn iptunnel gre_example)> enable false
(config vpn iptunnel gre_example)>
```

4. Set the mode:

```
(config vpn iptunnel gre_example)> type value
(config vpn iptunnel gre_example)>
```

where *value* is either:

- **gre**: Standard GRE point-to-point protocol.
- **mgre**: multipoint GRE protocol.
- **GRETAP**: Ethernet over GRE

5. Set the local endpoint to the GRE endpoint interface created in [Task One](#), for example:

```
(config vpn iptunnel gre_example)> local /network/interface/gre_endpoint
(config vpn iptunnel gre_example)>
```

6. If **type** is set to **gre**, set the IP address of the GRE endpoint on the remote peer:

```
(config vpn iptunnel gre_example)> remote ip_address
(config vpn iptunnel gre_example)>
```

7. (Optional) Set a key that will be inserted in GRE packets created by this tunnel.  
The key must match the key set by the remote endpoint.

---

```
(config vpn iptunnel gre_example)> key value
(config vpn iptunnel gre_example)>
```

---

where value is an integer between 0 and 4294967295, or an IP address.

8. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

---

```
(config vpn iptunnel gre_example)> keepalive true
(config vpn iptunnel gre_example)>
```

---

9. (Optional) Enable the device to allow packets destined for an address which is not explicitly in the routing table to exit the IP tunnel:

---

```
(config vpn iptunnel gre_example)> open_routing true
(config vpn iptunnel gre_example)>
```

---

10. Save the configuration and apply the change

---

```
(config vpn iptunnel gre_example)> save
Configuration saved.
>
```

---

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.



## Show GRE tunnels


To view information about currently configured GRE tunnels:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **Status > IP tunnels**.

The **IP Tunnels** page appears.

2. To view configuration details about a GRE tunnel, click the  (configuration) icon in the upper right of the tunnel's status pane.

## Example: GRE tunnel over an IPsec tunnel

The Connect EZ device can be configured as an advertised set of routes through an IPsec tunnel. This allows you to leverage the dynamic route advertisement of GRE tunnels through a secured IPsec tunnel.

The example configuration provides instructions for configuring the Connect EZ device with a GRE tunnel through IPsec.

### Connect EZ-1 configuration tasks

1. Create an IPsec tunnel named **ipsec\_gre1** with:
  - A pre-shared key.
  - **Remote endpoint** set to the public IP address of the Connect EZ-2 device.
  - A policy with:
    - **Local network** set to the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**.
    - **Remote network** set to the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**.
2. Create an IPsec endpoint interface named **ipsec\_endpoint1**:
  - a. **Zone** set to **Internal**.
  - b. **Device** set to **Ethernet: Loopback**.
  - c. IPv4 Address set to the IP address of the local GRE tunnel, **172.30.0.1/32**.
3. Create a GRE tunnel named **gre\_tunnel1**:
  - a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec\_endpoint1**.
  - b. **Remote endpoint** set to the IP address of the GRE tunnel on Connect EZ-2, **172.30.0.2**.
4. Create an interface named **gre\_interface1** and add it to the GRE tunnel:
  - a. **Zone** set to **Internal**.
  - b. **Device** set to **IP tunnel: gre\_tunnel1**.
  - c. IPv4 Address set to a virtual IP address on the GRE tunnel, **172.31.0.1/30**.

### Connect EZ-2 configuration tasks

1. Create an IPsec tunnel named **ipsec\_gre2** with:
  - The same pre-shared key as the **ipsec\_gre1** tunnel on Connect EZ-1.
  - **Remote endpoint** set to the public IP address of Connect EZ-1.
  - A policy with:
    - **Local network** set to the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**.
    - **Remote network** set to the IP address of the remote GRE tunnel, **172.30.0.1/32**.
2. Create an IPsec endpoint interface named **ipsec\_endpoint2**:
  - a. **Zone** set to **Internal**.
  - b. **Device** set to **Ethernet: Loopback**.
  - c. IPv4 Address set to the IP address of the local GRE tunnel, **172.30.0.2/32**.

3. Create a GRE tunnel named **gre\_tunnel2**:
  - a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec\_endpoint2**.
  - b. Remote endpoint set to the IP address of the GRE tunnel on Connect EZ-1, **172.30.0.1**.
4. Create an interface named **gre\_interface2** and add it to the GRE tunnel:
  - a. **Zone** set to **Internal**.
  - b. **Device** set to **IP tunnel: gre\_tunnel2**.
  - c. IPv4 Address set to a virtual IP address on the GRE tunnel, **172.31.0.2/30**.

## Configuration procedures

### Configure the Connect EZ-1 device

#### Task one: Create an IPsec tunnel

#### Web

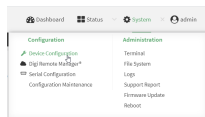
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > IPsec > Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec\_gre1** and click **+**.



5. Click to expand **Authentication**.

- For **Pre-shared key**, type **testkey**.

The screenshot shows the 'Authentication' configuration page. The 'Pre-shared key' field is highlighted with a green box and a green arrow pointing to it.

- Click to expand **Remote endpoint**.
- For **Hostname**, type public IP address of the Connect EZ-2 device.

The screenshot shows the 'Remote endpoint' configuration page. The 'Hostname' field is highlighted with a green box.

- Click to expand **Policies**.
- For **Add Policy**, click **+** to add a new policy.

The screenshot shows the 'Policies' configuration page. The 'Add Policy' button is highlighted with a green box and a green arrow pointing to it.

- Click to expand **Local network**.
- For **Type**, select **Custom network**.
- For **Address**, type the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**.
- For **Remote network**, type the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**.

The screenshot shows the 'Policy' configuration page. The 'Local network' section is expanded, showing 'Type' set to 'Custom network', 'Custom network' set to '172.30.0.1/32', and 'Remote network' set to '172.30.0.2/32'.

- Click **Apply** to save the configuration and apply the change.

## Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Add an IPsec tunnel named **ipsec\_gre1**:

```
(config)> add vpn ipsec tunnel ipsec_gre1
(config vpn ipsec tunnel ipsec_gre1)>
```

4. Set the pre-shared key to **testkey**:

---

```
(config vpn ipsec tunnel ipsec_gre1)> auth secret testkey  
(config vpn ipsec tunnel ipsec_gre1)>
```

---

5. Set the remote endpoint to public IP address of the Connect EZ-2 device:

---

```
(config vpn ipsec tunnel ipsec_gre1)> remote hostname 192.168.101.1  
(config vpn ipsec tunnel ipsec_gre1)>
```

---

6. Add a policy:

---

```
(config vpn ipsec tunnel ipsec_gre1)> add policy end  
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

---

7. Set the local network policy type to **custom**:

---

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> local type custom  
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

---

8. Set the local network address to the IP address and subnet of the local GRE tunnel, **172.30.0.1/32**:

---

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> local custom 172.30.0.1/32  
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

---

9. Set the remote network address to the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**:

---

```
(config vpn ipsec tunnel ipsec_gre1 policy 0)> remote network  
172.30.0.2/32  
(config vpn ipsec tunnel ipsec_gre1 policy 0)>
```

---

10. Save the configuration and apply the change

---

```
(config ipsec tunnel ipsec_gre1 policy 0)> save  
Configuration saved.  
>
```

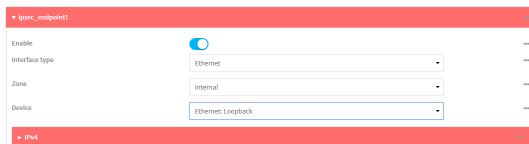
---

**Task two: Create an IPsec endpoint interface****Web**

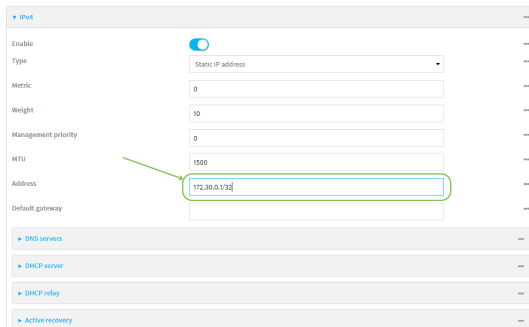
1. Click **Network > Interface**.
2. For **Add Interface**, type **ipsec\_endpoint1** and click **+**.



3. For **Zone**, select **Internal**.
4. For **Device**, select **Ethernet: loopback**.



5. Click to expand **IPv4**.
6. For **Address**, type the IP address of the local GRE tunnel, **172.30.0.1/32**.



7. Click **Apply** to save the configuration and apply the change.

## Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **ipsec\_endpoint1**:

```
(config)> add network interface ipsec_endpoint1
(config network interface ipsec_endpoint1)>
```

3. Set the zone to **internal**:

```
(config network interface ipsec_endpoint1)> zone internal
(config network interface ipsec_endpoint1)>
```

4. Set the device to **/network/device/loopback**:

```
(config network interface ipsec_endpoint1)> device
/network/device/loopback
(config network interface ipsec_endpoint1)>
```

5. Set the IPv4 address to the IP address of the local GRE tunnel, **172.30.0.1/32**:

```
(config network interface ipsec_endpoint1)> ipv4 address 172.30.0.1/32
(config network interface ipsec_endpoint1)>
```

6. Save the configuration and apply the change

```
(config vpn ipsec tunnel ipsec_endpoint1 policy 0)> save
Configuration saved.
>
```

### Task three: Create a GRE tunnel

#### Web

1. Click **VPN > IP Tunnels**.
2. For **Add IP Tunnel**, type **gre\_tunnel1** and click **+**.



3. For **Local endpoint**, select the IPsec endpoint interface created in [Task two](#) (Interface: **ipsec\_endpoint1**).

4. For **Remote endpoint**, type the IP address of the GRE tunnel on Connect EZ-2, **172.30.0.2**.

The screenshot shows a configuration window for a GRE tunnel. The 'Remote endpoint' field is highlighted with a blue border and contains the IP address '172.30.0.2'. Other fields include 'Local endpoint' set to 'interface: ipsec\_endpoint', 'Mode' set to 'GRE', and 'Enable keepalive reply' set to 'off'.

5. Click **Apply** to save the configuration and apply the change.

## Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add a GRE tunnel named **gre\_tunnel1**:

```
(config)> add vpn iptunnel gre_tunnel1
(config vpn iptunnel gre_tunnel1)>
```

3. Set the local endpoint to the IPsec endpoint interface created in [Task two \(/network/interface/ipsec\\_endpoint1\)](#):

```
(config vpn iptunnel gre_tunnel1)> local /network/interface/ipsec_
endpoint1
(config vpn iptunnel gre_tunnel1)>
```

4. Set the remote endpoint to the IP address of the GRE tunnel on Connect EZ-2, **172.30.0.2**:

```
(config vpn iptunnel gre_tunnel1)> remote 172.30.0.2
(config vpn iptunnel gre_tunnel1)>
```

5. Save the configuration and apply the change

```
(config vpn iptunnel gre_tunnel1)> save
Configuration saved.
>
```



**Task four: Create an interface for the GRE tunnel device****Web**

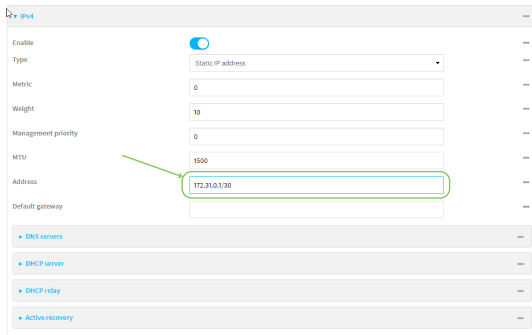
1. Click **Network > Interfaces**.
2. For **Add Interface**, type **gre\_interface1** and click **+**.



3. For **Zone**, select **Internal**.
4. For **Device**, select the GRE tunnel created in [Task three](#) (IP tunnel: **gre\_tunnel1**).



5. Click to expand **IPv4**.
6. For **Address**, type **172.31.0.1/30** for a virtual IP address on the GRE tunnel.



7. Click **Apply** to save the configuration and apply the change.

## Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **gre\_interface1**:

```
(config)> add network interface gre_interface1
(config network interface gre_interface1)>
```

3. Set the zone to **internal**:

```
(config network interface gre_interface1)> zone internal
(config network interface gre_interface1)>
```

4. Set the device to the GRE tunnel created in [Task three \(/vpn/iptunnel/gre\\_tunnel1\)](#):

```
(config network interface gre_interface1)> device /vpn/iptunnel/gre_
tunnel1
(config network interface gre_interface1)>
```

5. Set **172.31.0.1/30** as the virtual IP address on the GRE tunnel:

```
(config network interface gre_interface1)> ipv4 address 172.31.0.1/30
(config network interface gre_interface1)>
```

6. Save the configuration and apply the change

```
(config network interface gre_interface1)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the Connect EZ-2 device

### Task one: Create an IPsec tunnel

#### Web

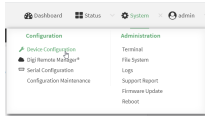
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

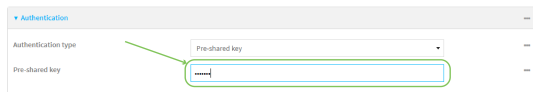


The **Configuration** window is displayed.

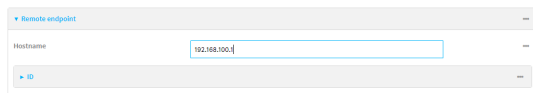
3. Click **VPN > IPsec > Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec\_gre2** and click **+**.



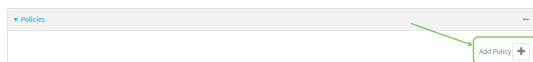
5. Click to expand **Authentication**.
6. For **Pre-shared key**, type the same pre-shared key that was configured for the Connect EZ-1 (**testkey**).



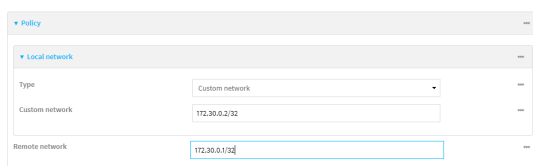
7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the Connect EZ-1 device.



9. Click to expand **Policies**.
10. For **Add Policy**, click **+** to add a new policy.



11. Click to expand **Local network**.
12. For **Type**, select **Custom network**.
13. For **Address**, type the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**.
14. For **Remote network**, type the IP address and subnet of the remote GRE tunnel, **172.30.0.1/32**.



- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

- Add an IPsec tunnel named **ipsec\_gre2**:

---

```
(config)> add vpn ipsec tunnel ipsec_gre2
(config vpn ipsec tunnel ipsec_gre2)>
```

---

- Set the pre-shared key to the same pre-shared key that was configured for the Connect EZ-1 (**testkey**):

---

```
(config vpn ipsec tunnel ipsec_gre2)> auth secret testkey
(config vpn ipsec tunnel ipsec_gre2)>
```

---

- Set the remote endpoint to public IP address of the Connect EZ-1 device:

---

```
(config vpn ipsec tunnel ipsec_gre2)> remote hostname 192.168.100.1
(config vpn ipsec tunnel ipsec_gre2)>
```

---

- Add a policy:

---

```
(config vpn ipsec tunnel ipsec_gre2)> add policy end
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

---

- Set the local network policy type to **custom**:

---

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> local type custom
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

---

- Set the local network address to the IP address and subnet of the local GRE tunnel, **172.30.0.2/32**:

---

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> local custom 172.30.0.2/32
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

---

- Set the remote network address to the IP address and subnet of the remote GRE tunnel, **172.30.0.1/32**:

---

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> remote network
172.30.0.1/32
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

---

10. Save the configuration and apply the change

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> save
Configuration saved.
>
```

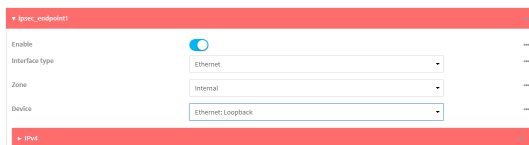
## Task two: Create an IPsec endpoint interface

### Web

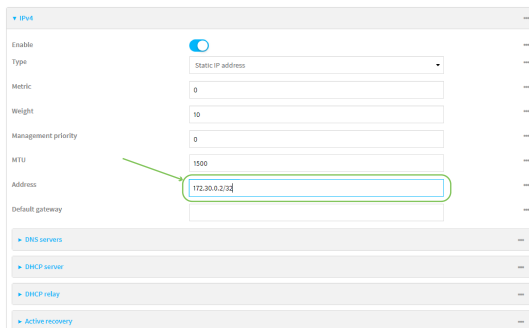
1. Click **Network > Interfaces**.
2. For **Add Interface**, type **ipsec\_endpoint2** and click **+**.



3. For **Zone**, select **Internal**.
4. For **Device**, select **Ethernet: loopback**.



5. Click to expand **IPv4**.
6. For **Address**, type the IP address of the local GRE tunnel, **172.30.0.2/32**.



7. Click **Apply** to save the configuration and apply the change.

### Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **ipsec\_endpoint2**:

```
(config)> add network interface ipsec_endpoint2
(config network interface ipsec_endpoint2)>
```

3. Set the zone to **internal**:

```
(config network interface ipsec_endpoint2)> zone internal
(config network interface ipsec_endpoint2)>
```

4. Set the device to **/network/device/loopback**:

```
(config network interface ipsec_endpoint2)> device
/network/device/loopback
(config network interface ipsec_endpoint2)>
```

5. Set the IPv4 address to the IP address of the local GRE tunnel, **172.30.0.2/32**:

```
(config network interface ipsec_endpoint2)> ipv4 address 172.30.0.2/32
(config network interface ipsec_endpoint2)>
```

6. Save the configuration and apply the change

```
(config vpn ipsec tunnel ipsec_endpoint2)> save
Configuration saved.
>
```

### Task three: Create a GRE tunnel

#### Web

1. Click **VPN > IP Tunnels**.
2. For **Add IP Tunnel**, type **gre\_tunnel2** and click **+**.



3. For **Local endpoint**, select the IPsec endpoint interface created in [Task two](#) (Interface: **ipsec\_endpoint2**).

4. For **Remote endpoint**, type the IP address of the GRE tunnel on Connect EZ-1, **172.30.0.1**.

5. Click **Apply** to save the configuration and apply the change.

## Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add a GRE tunnel named **gre\_tunnel2**:

```
(config)> add vpn iptunnel gre_tunnel2
(config vpn iptunnel gre_tunnel2)>
```

3. Set the local endpoint to the IPsec endpoint interface created in [Task two](#) (**/network/interface/ipsec\_endpoint2**):

```
(config vpn iptunnel gre_tunnel2)> local /network/interface/ipsec_
endpoint2
(config vpn iptunnel gre_tunnel2)>
```

4. Set the remote endpoint to the IP address of the GRE tunnel on Connect EZ-1, **172.30.0.1**:

```
(config vpn iptunnel gre_tunnel2)> remote 172.30.0.1
(config vpn iptunnel gre_tunnel2)>
```

5. Save the configuration and apply the change

```
(config vpn iptunnel gre_tunnel2)> save
Configuration saved.
>
```

### Task four: Create an interface for the GRE tunnel device

## Web

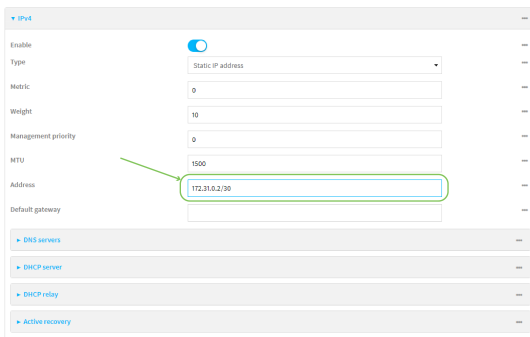
1. Click **Network > Interfaces**.
2. For **Add Interface**, type **gre\_interface2** and click **+**.



3. For **Zone**, select **Internal**.
4. For **Device**, select the GRE tunnel created in [Task three](#) (IP tunnel: **gre\_tunnel2**).



5. Click to expand **IPv4**.
6. For **Address**, type **172.31.0.2/30** for a virtual IP address on the GRE tunnel.



7. Click **Apply** to save the configuration and apply the change.

## Command line

1. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

2. Add an interface named **gre\_interface2**:

```
(config)> add network interface gre_interface2
(config network interface gre_interface2)>
```



3. Set the zone to **internal**:

---

```
(config network interface gre_interface2)> zone internal
(config network interface gre_interface2)>
```

---

4. Set the device to the GRE tunnel created in [Task three \(/vpn/iptunnel/gre\\_tunnel2\)](#):

---

```
(config network interface gre_interface2)> device /vpn/iptunnel/gre_
tunnel2
(config network interface gre_interface2)>
```

---

5. Set **172.31.0.2/30** as the virtual IP address on the GRE tunnel:

---

```
(config network interface gre_interface2)> ipv4 address 172.31.0.2/30
(config network interface gre_interface2)>
```

---

6. Save the configuration and apply the change

---

```
(config network interface gre_interface2)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Dynamic Multipoint VPN (DMVPN)

Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of a virtual private network (VPN), using a multi spoke-to-hub network in which the network addresses of the spoke routers do not need to be known, and therefore do not need to be configured in the hub router.

One advantage to this form of VPN is a scalable network in which the size of the hub configuration is minimized. When one spoke of the network needs to send traffic to another spoke, a direct transfer is possible without having to add any load onto the hub. This is achieved by the creation of a dynamic GRE tunnel directly to the other spoke. The network address of the target spoke is resolved with the use of Next Hop Resolution Protocol (NHRP).

This section contains the following topics:

Configure a DMVPN spoke .....306

## Configure a DMVPN spoke

To configure a DMVPN spoke:

### Web

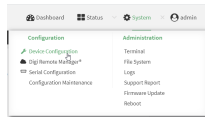
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

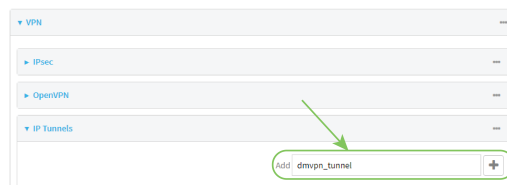
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

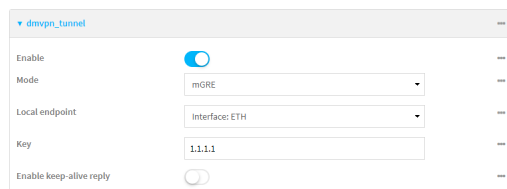


The **Configuration** window is displayed.

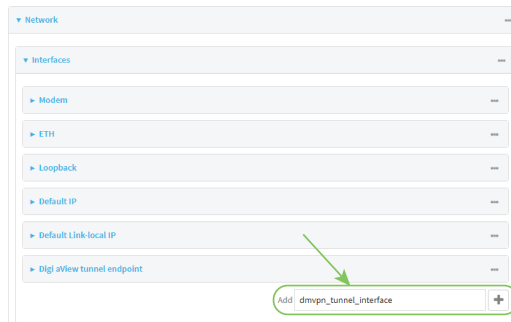
3. Create an IP tunnel.
  - a. Click **VPN > IP Tunnels**.
  - b. In **Add IP tunnel**, type the name of the tunnel and click **+**.



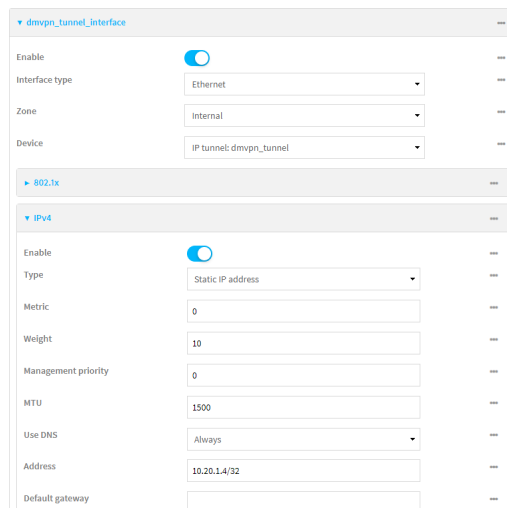
- c. For **Mode**, select **mGRE**.
- d. For **Local endpoint**, select the interface that will serve as the local endpoint of the tunnel.
- e. For **Key**, type a four-octet value that matches the key on the remote endpoint.



- f. (Optional) **Enable keep-alive reply** to enable the device to reply to Cisco GRE keep-alive packets.
  - g. (Optional) **Enable open routing** to enable packets destined for an address which is not explicitly in the routing table to exit the IP tunnel.
4. Assign an IP address to the IP tunnel:
    - a. Click **Network > Interfaces**.
    - b. For **Add Interface**, type a name for the interface and click **+**.

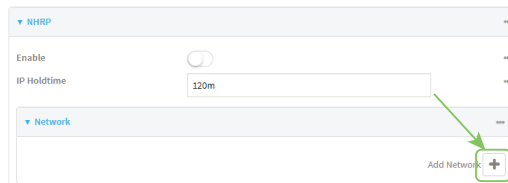


- c. For **Zone**, select **Internal**.
- d. For **Device**, select the IP tunnel created above.
- e. Click to expand **IPv4**.
- f. For **Address**, type the IP address and netmask of the tunnel. The netmask must be set to **/32**.

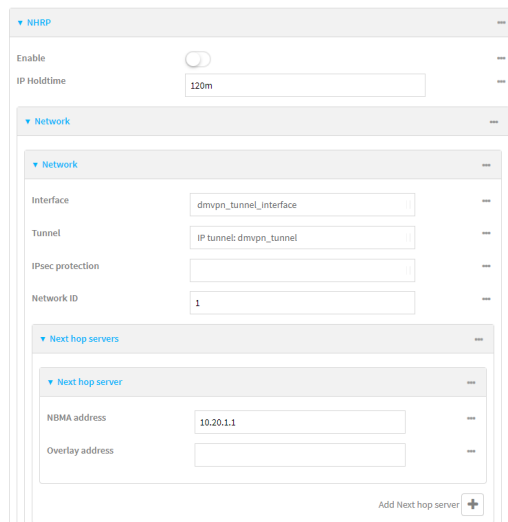


5. Configure **NHRP**:
  - a. Click **Network > Routing Services**.
  - b. **Enable** routing services.
  - c. Click to expand **NHRP**.
  - d. **Enable** NHRP.
  - e. Click to expand **Network**.

- f. Click **+** to add a network.

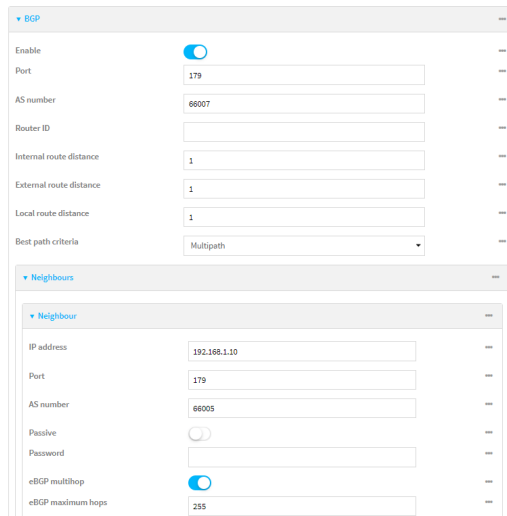


- g. For **Interface**, select the interface created above.  
 h. For **Tunnel**, select the IP tunnel created above.  
 i. Click to expand **Next hop servers**.  
 j. Click **+** to add a server.  
 k. For **NBMA address**, type the hostname or IP address of the node that will be the next hop server.



6. To enable redirection of packets between spokes, configure OSPF routing:
- Click **Network > Routes > Routing services > OSPF**.
  - Enable** OSPF.
  - For **ABR behavior**, choose the Area Border Router for the network.
  - For **Reference bandwidth**, type the link bandwidth.
  - Enable** the Opaque-LSA standard.
  - Enable** the RFC1583 standard.
7. Configure the overlay connection:
- Click **Network > Routing services > BGP**.
  - Enable** BGP.
  - For **AS number**, type the autonomous system number for this device.
  - For **Best path criteria**, select **Multipath**.
  - Click to expand **Neighbours**.
  - Click **+** to add a neighbour.

- g. For **IP address**, type the IP address of the hub.
- h. Click to toggle on **eBGP multihop**.



8. Repeat to add additional spokes.
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Create an IP tunnel.
  - a. Add an IP tunnel. For example, to add a tunnel named **dmvpn\_tunnel**:

```
(config)> add vpn iptunnel dmvpn_tunnel
(config vpn iptunnel dmvpn_tunnel)>
```

- b. Set the type to multipoint:

```
(config vpn iptunnel dmvpn_tunnel)> type multipoint
(config vpn iptunnel dmvpn_tunnel)>
```

- c. Set the local interface:
    - i. Use the **?** to determine available interfaces:
    - ii. Set the interface. For example:

```
(config vpn iptunnel dmvpn_tunnel)> local /network/interface/eth1
(config vpn iptunnel dmvpn_tunnel)>
```

- d. Set the key to a four-octet value that matches the key on the remote endpoint. For example:

```
(config vpn iptunnel dmvpn_tunnel)> key 1.1.1.1
(config vpn iptunnel dmvpn_tunnel)>
```

- e. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

```
(config vpn iptunnel dmvpn_tunnel)> keepalive true
(config vpn iptunnel dmvpn_tunnel)>
```

- f. (Optional) Enable the device to allow packets destined for an address which is not explicitly in the routing table to exit the IP tunnel:

```
(config vpn iptunnel dmvpn_tunnel)> open_routing true
(config vpn iptunnel dmvpn_tunnel)>
```

4. Assign an IP address to the IP tunnel:

- a. Type ... to return to the top level of the configuration schema:

```
(config vpn iptunnel dmvpn_tunnel)> ...
(config)>
```

- b. Add a network interface. For example, to add an interface named `dmvpn_tunnel_interface`:

```
(config)> add network interface dmvpn_tunnel_interface
(config network interface dmvpn_tunnel_interface)>
```

- c. Set the zone to **internal**:

```
(config network interface dmvpn_tunnel_interface)> zone internal
(config network interface dmvpn_tunnel_interface)>
```

- d. Set the device to the IP tunnel created above:

```
(config network interface dmvpn_tunnel_interface)> device
/vpn/iptunnel/dmvpn_tunnel
(config network interface dmvpn_tunnel_interface)>
```

- e. Set the IP address and netmask of the tunnel. The netmask must be set to **/32**. For example, to set the IP address to **10.20.1.4/32**:

```
(config network interface dmvpn_tunnel_interface)> ipv4 address
10.20.1.4/32
(config network interface dmvpn_tunnel_interface)>
```

5. Configure NHRP:

- a. Type ... to return to the top level of the configuration schema:

```
(config network interface dmvpn_tunnel_interface)> ...
(config)>
```

- b. Enable routing services:

```
(config)> network route service enable true  
(config)>
```

- c. Enable NHRP:

```
(config)> network route service nhrp enable true  
(config)>
```

- d. Add an NHRP network:

```
(config)> add network route service nhrp network end  
(config network route service nhrp network 0)>
```

- e. Set the interface to the interface that was created above:

```
(config network route service nhrp network 0)> interface dmvpn_tunnel_  
interface  
(config network route service nhrp network 0)>
```

- f. Set the tunnel to the IP tunnel created above:

```
(config network route service nhrp network 0)> tunnel  
/vpn/iptunnel/dmvpn_tunnel  
(config network route service nhrp network 0)>
```

- g. Add a net hop server:

```
(config network route service nhrp network 0)> add nhs end  
(config network route service nhrp network 0 nhs 0)>-
```

6. Set the hostname or IP address of the node that will be the next hop server:

```
(config network route service nhrp network 0 nhs 0)> nbma hostname/IP_  
address  
(config network route service nhrp network 0 nhs 0)>
```

7. Configure OSPF routing:

```
(config network route service ospf)  
(config)>
```

8. Configure the overlay connection using BGP:

- a. Type ... to return to the top level of the configuration schema:

```
(config network interface dmvpn_tunnel_interface)> ...  
(config)>
```

- b. Enable BGP:

```
(config)> network route service bgp enable true  
(config)>
```

- c. Set the autonomous system number for this device. For example, to set the autonomous system number to 66007:

```
(config)> network route service bgp asn 66007
(config)>
```

- d. Set the best path criteria to multipath:

```
(config)> network route service bgp as_path multipath-relax
(config)>
```

- e. Add a neighbour:

```
(config)> add network route service bgp neighbour end
(config network route service bgp neighbour 0)>
```

- f. Set **ip** to the IP address of the hub. For example:

```
(config network route service bgp neighbour 0)> ip 10.20.1.1
(config network route service bgp neighbour 0)>
```

- g. Enable eBGP multihop:

```
(config network route service bgp neighbour 0)> ebgp_multihop true
(config network route service bgp neighbour 0)>
```

9. Repeat to add additional spokes.  
10. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## L2TP

Your Connect EZ device supports PPP-over-L2TP (Layer 2 Tunneling Protocol).

### Configure a PPP-over-L2TP tunnel

Your Connect EZ device supports PPP-over-L2TP (Layer 2 Tunneling Protocol). The tunnel endpoints are known as L2TP Access Concentrators (LAC) and L2TP Network Servers (LNS). Each endpoint terminates the PPP session.

#### Required configuration items

- For L2TP access concentrators:
  - The hostname or IP address of the L2TP network server.
  - The firewall zone for the tunnel.



- For L2TP network servers:
  - The IP address of the L2TP access concentrator.
  - The local IP address assigned to the L2TP virtual network interface.
  - The IP address assigned to the remote peer.
  - The firewall zone for the tunnel.

### Additional configuration items

- The UDP port that L2TP servers will listen on, if other than the default of **1701**.
- Access control for the L2TP tunnel.
- For L2TP access concentrators:
  - L2TP network server port.
  - The username and password of the L2TP server.
  - The metric for the tunnel.
  - Enable custom PPP configuration options for the tunnel.
    - Whether to override the default configuration and only use the custom options.
    - Optional configuration data in the format of a pppd options file.
- For L2TP network servers:
  - The Authentication method.
  - The metric for the tunnel.
  - Enable custom PPP configuration options for the tunnel.
    - Whether to override the default configuration and only use the custom options.
    - Optional configuration data in the format of a pppd options file.

## ≡ Web

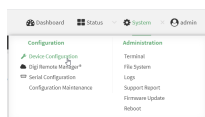
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > L2TP**.
4. (Optional) Type the **UDP listening port** that L2TP servers will listen on, if other than the default of **1701**.
5. Set the access control for L2TP tunnels:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's service-type. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the service-type.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's service-type. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the service-type.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
6. To add an L2TP access concentrator:
  - a. Click to expand **L2TP access concentrators**.
  - b. For **Add L2TP access concentrator**, type a name for the LAC and click **+**.
  - c. LACs are enabled by default. To disable, toggle off **Enable**.
  - d. For **L2TP network server**, type the hostname or IP address of the L2TP network server.

- e. (Optional) Type the **L2TP network server port** to use to connect to the server, if other than the default of **1701**.
  - f. (Optional) Type the **Username** to use to log into the server.
  - g. (Optional) Type the **Password** to use to log into the server.
  - h. (Optional) Type the **Metric** for the tunnel, if other than the default of **1**.
  - i. Select a firewall **Zone** for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.
  - j. (Optional): Custom PPP configuration:
    - i. **Enable** custom PPP configuration.
    - ii. Enable **Override** if the custom configuration should override the default configuration and only use the custom options.
    - iii. For **Configuration file**, paste or type the configuration data in the format of a pppd options file.
7. To add an L2TP network server:
- a. Click to expand **L2TP network servers**.
  - b. For **Add L2TP network server**, type a name for the LNS and click **+**.
  - c. LNSs are enabled by default. To disable, toggle off **Enable**.
  - d. For **L2TP access concentrator**, type the IP address of the L2TP access concentrator that this server will allow connections from. This can also be:
    - A range of IP addresses, using the format x.x.x.x-y.y.y.y, for example **192.168.188.1-192.168.188.254**.
    - The keyword **any**, which means that the server will accept connections from any IP address.
  - e. For **Local IP address**, type the IP address of the L2TP virtual network interface.
  - f. For **Remote IP address**, type the IP address to assign to the remote peer.
  - g. (Optional) For **Authentication method**, select one of the following:
    - **None**: No authentication is required.
    - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
    - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
    - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

If **Automatic**, **CHAP**, or **PAP** is selected, enter the **Username** and **Password** required to authenticate.

The default is **None**.
  - h. (Optional) For **Authentication method**, select the authentication method, one of:
    - **None**: No authentication is required.
    - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
    - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
    - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.

- **MS-CHAPv2**: Uses the Microsoft version of the Challenge Handshake Authentication Profile (CHAP) to authenticate.
  - If **Automatic**, **CHAP**, **PAP**, or **MS-CHAPv2** is selected, enter the **Username** and **Password** required to authenticate.
  - The default is **None**.
- i. (Optional) Type the **Metric** for the tunnel, if other than the default of **1**.
  - j. Select a firewall **Zone** for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.
  - k. (Optional): Custom PPP configuration:
    - i. **Enable** custom PPP configuration.
    - ii. Enable **Override** if the custom configuration should override the default configuration and only use the custom options.
    - iii. For **Configuration file**, paste or type the configuration data in the format of a pppd options file.
8. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Set the UDP listening port that L2TP servers will listen on:

```
(config)> vpn l2tp port value
(config)>
```

where *value* is an integer between **1** and **65535**. The default is **1701**.

4. Set the access control for L2TP tunnels:
  - To limit access to specified IPv4 addresses and networks:

```
(config)> add vpn l2tp acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add vpn l2tp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add vpn l2tp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add vpn l2tp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

---

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

---

---

```
(config)>
```

---

Repeat this step to include additional firewall zones.

5. To add an L2TP access concentrator:

a. Add an LAC:

---

```
(config)> add vpn l2tp lac name
(config add vpn l2tp lac name)>
```

---

where *name* is the name of the LAC. For example, to add an LAC named `lac_tunnel`:

---

```
(config)> add vpn l2tp lac lac_tunnel
(config vpn l2tp lac lac_tunnel)>
```

---

LACs are enabled by default. To disable:

---

```
(config vpn l2tp lac lac_tunnel)> enable false
(config vpn l2tp lac lac_tunnel)>
```

---

b. Set the hostname or IP address of the L2TP network server:

---

```
(config vpn l2tp lac lac_tunnel)> lns hostname
(config vpn l2tp lac lac_tunnel)>
```

---

c. (Optional) Set the UDP port to use to connect to the L2TP network server:

---

```
(config vpn l2tp lac lac_tunnel)> port int
(config vpn l2tp lac lac_tunnel)>
```

---

where *int* is an integer between **1** and **65535**. The default is **1701**.

d. (Optional) Set the username to use to log into the server:

---

```
(config vpn l2tp lac lac_tunnel)> username username
(config vpn l2tp lac lac_tunnel)>
```

---

e. (Optional) Set the password to use to log into the server:

---

```
(config vpn l2tp lac lac_tunnel)> password password
(config vpn l2tp lac lac_tunnel)>
```

---

f. (Optional) Set the metric for the tunnel:

---

```
(config vpn l2tp lac lac_tunnel)> metric int
(config vpn l2tp lac lac_tunnel)>
```

---

where *int* is an integer between **0** and **65535**. The default is **1**.

g. Set the firewall zone for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.

- i. Use the ? to determine available zones:

---

```
(config vpn l2tp lac lac_tunnel)> zone ?
```

```
Zone: The firewall zone assigned to this tunnel. This can be used
by packet
filtering rules and access control lists to restrict network
traffic on this
tunnel.
```

```
Format:
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
Current value:
```

---

```
(config vpn l2tp lac lac_tunnel)>
```

---

- ii. Set the zone:

---

```
(config vpn l2tp lac lac_tunnel)> zone zone
(config vpn l2tp lac lac_tunnel)>
```

---

- h. (Optional): Custom PPP configuration:

- i. Enable custom PPP configuration:

---

```
(config vpn l2tp lac lac_tunnel)> custom enable true
(config vpn l2tp lac lac_tunnel)>
```

---

- ii. Enable overriding, if the custom configuration should override the default configuration and only use the custom options:

---

```
(config vpn l2tp lac lac_tunnel)> custom override true
(config vpn l2tp lac lac_tunnel)>
```

---

- iii. Paste or type the configuration data in the format of a pppd options file:

---

```
(config vpn l2tp lac lac_tunnel)> custom config_file data
(config vpn l2tp lac lac_tunnel)>
```

---

6. To add an L2TP network server:

- a. Add an LNS:

---

```
(config)> add vpn l2tp lns name
(config add vpn l2tp lac name)>
```

---

where *name* is the name of the LNS. For example, to add an LNS named *lns\_server*:

---

```
(config)> add vpn l2tp lns lns_server
(config vpn l2tp lns lns_server)>
```

---

LACs are enabled by default. To disable:

---

```
(config vpn l2tp lns lns_server)> enable false
(config vpn l2tp lns lns_server)>
```

---

- b. Set the IP address of the L2TP access concentrator that this server will allow connections from:

---

```
(config vpn l2tp lns lns_server)> lac IP_address
(config vpn l2tp lns lns_server)>
```

---

This can also be:

- A range of IP addresses, using the format *x.x.x-y.y.y*, for example **192.168.188.1-192.168.188.254**.
- The keyword **any**, which means that the server will accept connections from any IP address.

- c. Set the IP address of the L2TP virtual network interface:

---

```
(config vpn l2tp lns lns_server)> local_address IP_address
(config vpn l2tp lns lns_server)>
```

---

- d. Set the IP address to assign to the remote peer:

---

```
(config vpn l2tp lns lns_server)> remote_address IP_address
(config vpn l2tp lns lns_server)>
```

---

- e. (Optional) Set the authentication method:

---

```
(config vpn l2tp lns lns_server)> auth method
(config)>
```

---

where *method* is one of the following:

- **none**: No authentication is required.
- **auto**: The device will attempt to connect using CHAP first, and then PAP.
- **chap**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
- **pap**: Uses the Password Authentication Profile (PAP) to authenticate.
- **mschapv2**: Uses the Microsoft version of the Challenge Handshake Authentication Profile (CHAP) to authenticate.

If **auto**, **chap**, **pap** or **mschapv2** is selected, enter the **Username** and **Password** required to authenticate:

---

```
(config vpn l2tp lns lns_server)> username username
(config vpn l2tp lns lns_server)> password password
(config vpn l2tp lns lns_server)>
```

---

The default is **none**.



- f. (Optional) Set the metric for the tunnel:

---

```
(config vpn l2tp lns lns_server)> metric int
(config vpn l2tp lns lns_server)>
```

---

where *int* is an integer between **0** and **65535**. The default is **1**.

- g. Set the firewall zone for the tunnel. This is used by packet filtering rules and access control lists to restrict network traffic on the tunnel.
- i. Use the **?** to determine available zones:

---

```
(config vpn l2tp lns lns_server)> zone ?
```

```
Zone: The firewall zone assigned to this tunnel. This can be used
by packet
filtering rules and access control lists to restrict network
traffic on this
tunnel.
```

```
Format:
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
Current value:
```

```
(config vpn l2tp lns lns_server)>
```

---

- ii. Set the zone:

---

```
(config vpn l2tp lns lns_server)> zone zone
(config vpn l2tp lns lns_server)>
```

---

- h. (Optional): Custom PPP configuration:

- i. Enable custom PPP configuration:

---

```
(config vpn l2tp lac lns lns_server)> custom enable true
(config vpn l2tp lns lns_server)>
```

---

- ii. Enable overriding, if the custom configuration should override the default configuration and only use the custom options:

---

```
(config vpn l2tp lns lns_server)> custom override true
(config vpn l2tp lns lns_server)>
```

---

- iii. Paste or type the configuration data in the format of a pppd options file:

---

```
(config vpn l2tp lns lns_server)> custom config_file data
(config vpn l2tp lns lns_server)>
```

---

7. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## L2TP with IPsec

L2TP is commonly used in conjunction with IPsec in transport mode (to provide security).

Your Connect EZ supports L2TP with IPsec by configuring a transport-mode IPsec tunnel between the two endpoints, and then an L2TP tunnel with its LNS and LAC configured the same as the IPsec tunnel's endpoints. See [Configure an IPsec tunnel](#) for information about configuring an IPsec tunnel.

**Note** The Connect EZ does not currently support the configuration of IPsec protocol/port traffic selectors. This means that you cannot restrict traffic on the IPsec tunnel to L2TP traffic (typically UDP port 1701).


While multiple L2TP clients are supported on the Connect EZ by configuring a separate LNS for each client, multiple clients behind a Network Address Translation (NAT) device are not supported, because they will all appear to have the same IP address.

## Show L2TP tunnel status

### Web


#### *Show the status of L2TP access connectors from the WebUI*

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TP > Access Connectors**.  
The **L2TP Access Connectors** page appears.
2. To view configuration details about an L2TP access connector, click the  (configuration) icon in the upper right of the tunnel's status pane.

#### *Show the status of L2TP network servers from the WebUI*

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TP > Network Servers**.  
The **L2TP Network Servers** page appears.
2. To view configuration details about an L2TP network server, click the  (configuration) icon in the upper right of the tunnel's status pane.

### Command line

**Show the status of L2TP access connectors from the Admin CLI**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured L2TP access connectors, type the following at the prompt:

---

```
> show l2tp lac

Name          Enabled  Status  Device
-----
lac_test1    true     up      test_device0
lac_test2    true     pending
>
```

---

3. To display details about a specific tunnel:

---

```
> show l2tp lac name lac_test2

lac_test2 L2TP Access Concentrator Status
-----
Enabled           : true
Status            : pending
>
```

---

4. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

**Show the status of L2TP network servers from the Admin CLI**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To display details about all configured L2TP access connectors, type the following at the prompt:

---

```
> show l2tp lns

Name          Enabled  Status  Device
-----
lns_test1    true     up      test_device0
lns_test2    true     pending
>
```

---

- To display details about a specific tunnel:

---

```
> show l2tp lns name lns_test2

lns_test2 L2TP Access Concentrator Status
-----
Enabled           : true
Status            : pending

>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## L2TPv3 Ethernet

Your Connect EZ device supports Layer 2 Tunneling Protocol Version 3 (L2TPv3) static unmanaged Ethernet tunnels.

### Configure an L2TPv3 tunnel

Your Connect EZ device supports Layer 2 Tunneling Protocol Version 3 (L2TPv3) static unmanaged Ethernet tunnels.

#### Required configuration items

- A name for the L2TPv3 tunnel.
- Enable the tunnel.
- The remote endpoint IP address.
- The local endpoint IP address.
- The session ID.
- The peer session ID.

#### Additional configuration items

- Encapsulation type. If UDP is selected:
  - The ID for the tunnel.
  - The ID of the peer's tunnel.
  - Determine whether to enable UDP checksum.
- The session cookie.
- The peer session cookie.
- The Layer2SpecificHeader type.
- The Sequence numbering control.



Web

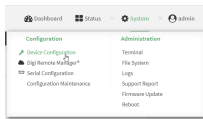
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > L2TPv3 ethernet**.
4. For **Add L2TPv3 ethernet tunnel**, type a name for the tunnel and click **+**.
5. For **Remote endpoint**, type the IPv4 address of the remote endpoint.
6. For **Local endpoint**, select the interface that will be the local endpoint.
7. For **Tunnel ID**, type the tunnel identifier for this tunnel. This must match the value for **Peer tunnel ID** on the remote peer. Allowed value is any integer between 1 and 4294967295.
8. For **Peer tunnel ID**, type the **Tunnel ID** of the remote peer.
9. (Optional) For **Encapsulation type**, select either **UDP** or **IP**. If **UDP** is selected:
  - a. For **UDP source port**, type the number of the source UDP port to be used for the tunnel.
  - b. For **UDP destination port**, type the number of the destination UDP port to be used for the tunnel.
  - c. (Optional) Click to enable **UDP checksum** to calculate and check the UDP checksum.
10. Click to expand **Sessions**.
  - a. For **Add Sesssion**, type a name for a session carried by the parent tunnel and click **+**.
  - b. For **Session ID**, type the session identifier for this session. This must match the value for **Peer session ID** on the remote peer. Allowed value is any integer between 1 and 4294967295.
  - c. For **Peer session ID**, type the **Session ID** of the remote peer.
  - d. (Optional) For **Cookie**, type the cookie value to be assigned to the session. Allowed value is 8 or 16 hex digits.
  - e. (Optional) For **Peer cookie**, type the **Cookie** value of the remote peer.
  - f. For **Layer2SpecificHeader type**, select the Layer2Specific header type. This must match what is configured on the remote peer.

- g. For **Sequence numbering control**, determine the sequence number control to prevent or detect out of order packets. Allowed values are:
- **None**: No sequence numbering.
  - **Send**: Add a sequence number to each outgoing packet.
  - **Receive**: Reorder packets if they are received out of order.
  - **Both**: Add a sequence number to each outgoing packet, and reorder packets if they are received out of order.

The default is **None**.

- h. Repeat for additional sessions.
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a L2TPv3 Ethernet tunnel. For example, to add a tunnel named **L2TPv3\_example**:

```
(config)> add vpn l2tpv3 L2TPv3_example
(config vpn l2tpeth L2TPv3_example)>
```

The tunnel is enabled by default. To disable:

```
(config vpn l2tpeth L2TPv3_example)> enable false
(config vpn l2tpeth L2TPv3_example)>
```

4. Set the IPv4 address of the remote endpoint:

```
(config vpn l2tpeth L2TPv3_example)> remote IP_address
(config vpn l2tpeth L2TPv3_example)>
```

5. Set the interface of the local endpoint:

- i. Use the **?** to determine available interfaces:
- ii. Set the interface. For example:

```
(config vpn l2tpeth L2TPv3_example)> local /network/interface/eth1
(config vpn l2tpeth L2TPv3_example)>
```

6. Set the tunnel identifier for this tunnel. This must match the value for peer tunnel ID on the remote peer.

```
(config vpn l2tpeth L2TPv3_example)> tunnel_id value
(config vpn l2tpeth L2TPv3_example)>
```

where *value* is any integer between 1 and 4294967295.

7. Set the tunnel ID of the remote peer:

```
(config vpn l2tpeth L2TPv3_example)> peer_tunnel_id value
(config vpn l2tpeth L2TPv3_example)>
```

where *value* is any integer between 1 and 4294967295.

8. (Optional) Set the encapsulation type:

```
(config vpn l2tpeth L2TPv3_example)> encapsulation value
(config vpn l2tpeth L2TPv3_example)>
```

where *value* is either **udp** or **ip**. The default is **udp**.

If **udp** is set:

- a. Set the source UDP port to be used for the tunnel:

```
(config vpn l2tpeth L2TPv3_example)> udp_source_port port
(config vpn l2tpeth L2TPv3_example)>
```

- b. Set the destination UDP port to be used for the tunnel.

```
(config vpn l2tpeth L2TPv3_example)> udp_destination_port port
(config vpn l2tpeth L2TPv3_example)>
```

- c. (Optional) To calculate and check the UDP checksum:

```
(config vpn l2tpeth L2TPv3_example)> udp_checksum true
(config vpn l2tpeth L2TPv3_example)>
```

9. Add a session carried by the parent tunnel:

```
(config vpn l2tpeth L2TPv3_example)> add session session_example
(config vpn l2tpeth L2TPv3_example session_example)>
```

10. Set the session identifier for this session. This must match the value for peer session ID on the remote peer.

```
(config vpn l2tpeth L2TPv3_example session_example)> session_id value
(config vpn l2tpeth L2TPv3_example session_example)>
```

where *value* is any integer between 1 and 4294967295.

11. Set the session ID of the remote peer:

```
(config vpn l2tpeth L2TPv3_example session_example)> peer_session_id
value
(config vpn l2tpeth L2TPv3_example session_example)>
```

where *value* is any integer between 1 and 4294967295.

12. (Optional) Set the cookie value to be assigned to the session.

---

```
(config vpn l2tpeth L2TPv3_example session_example)> cookie value
(config vpn l2tpeth L2TPv3_example session_example)>
```

---

Allowed *value* is 8 or 16 hex digits.

13. (Optional) Set the cookie value of the remote peer:

---

```
(config vpn l2tpeth L2TPv3_example session_example)> peer cookie value
(config vpn l2tpeth L2TPv3_example session_example)>
```

---

Allowed *value* is 8 or 16 hex digits.

14. Set the Layer2Specific header type. This must match what is configured on the remote peer.

---

```
(config vpn l2tpeth L2TPv3_example session_example)> l2spec_type value
(config vpn l2tpeth L2TPv3_example session_example)>
```

---

where *value* is either **none** or **default**. The default is **default**.

15. Set the sequence number control to prevent or detect out of order packets.

---

```
(config vpn l2tpeth L2TPv3_example session_example)> seq value
(config vpn l2tpeth L2TPv3_example session_example)>
```

---

where *value* is one of:

- **none**: No sequence numbering.
- **send**: Add a sequence number to each outgoing packet.
- **recv**: Reorder packets if they are received out of order.
- **both**: Add a sequence number to each outgoing packet, and reorder packets if they are received out of order.

The default is **none**.

16. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

17. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show L2TPV3 tunnel status


### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status**. Under VPN, select **L2TPv3 Ethernet**.

The **L2TPv3 Ethernet** page appears.



- To view configuration details about an L2TPv3 tunnel, click the  (configuration) icon in the upper right of the tunnel's status pane.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- To display details about all configured L2TPv3 Ethernet tunnels, type the following at the prompt:

---

```
> show l2tpeth

Tunnel Session      Enabled  Device      Status
-----
test/session/test   true    le_test_test up

>
```

---

- To display details about a specific tunnel:

---

```
> show l2tpeth name /vpn/l2tpeth/test/session/test

test/session/test Tunnel Session Status
-----
Enabled                : true
Status                 : up

Local IP                : 4.3.2.1
Remote IP              : 10.10.10.1
Tunnel ID              : modem
Peer Tunnel ID        : 10.10.10.1 === 4.3.2.1
Session ID             : 255
Peer Session ID       : 1476
Lifetime (Actual)     : 600

Device                 : le_test_test
RX Packets             : 2,102
RX Bytes               : 462
TX Packets             : 2,787
TX Bytes               : 3,120

>
```

---

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## MACsec

MACsec (Media Access Control Security) is a 802.1ae (Layer2) VPN protocol that can be used to create a secure MACsec tunnel over a wired Ethernet LAN. The MACsec uses keys to provide multiple authentications between hosts in a network.

A MACsec tunnel must be tied to a physical interface. You cannot create a MACsec tunnel for a bridge.

### Security modes

Two security modes are available for a MACsec tunnel.

- **Automatic:** Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
- **Manual:** Uses connectivity association key information that is manually entered in the **CAK** and **CKN** fields.

## Configure a MACsec tunnel

Your Connect EZ device supports MACsec (Layer 2 Tunneling Protocol).

### Required configuration items

- The local network device to connect to the peer device.
- When using **Manual** mode, the connectivity association key and key name.

### Web

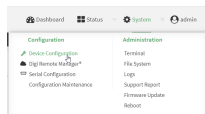
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device.](#)
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **VPN > MACsec**.
4. For **Add MACsec tunnel**, click **+**.

5. Click **Enable**.
6. For **Local endpoint**, select the local network device you want to use to connect to the peer device.
7. For **Security mode**, select your desired mode.
  - **Automatic**: Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
  - **Manual**: Uses connectivity association key information that is manually entered in the **CAK** and **CKN** fields.
8. If you selected **Manual**, additional required fields display.
  - a. For **CAK**, enter the connectivity associated key. The key format is 16 hex digits.
  - b. For **CKN**, enter the connectivity associated key name. The key format is 32 hex digits.
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Name the tunnel. At the config prompt, type:

```
(config)> add vpn macsec name
(config)>
```

where *name* is a string.

4. Enable the tunnel:

```
(config vpn macsec tunnel1) enable true
(config vpn macsec tunnel1)>
```

5. Specify the local endpoint:

```
(config vpn macsec tunnel1) local value
(config vpn macsec tunnel1)>
```

where *value* is one of the available options.

6. Specify the security mode:

```
(config vpn macsec tunnel1) type value
(config vpn macsec tunnel1)>
```

where *value* is one of the following:

- **automatic:** Uses a pre-shared key to generate association key information, which is periodically rotated through using 802.1x.
  - **manual:** Uses connectivity association key information that is manually entered.
- 7. If you specified the **manual** security mode, enter the connectivity association key and key name.
  - a. Specify the connectivity association key:

---

```
(config vpn macsec tunnel1) association cak value
(config vpn macsec tunnel1)>
```

---

where *value* is the association key. The key format is 16 hex digits.

- b. Specify the connectivity association key name:

---

```
(config vpn macsec tunnel1) association ckn value
(config vpn macsec tunnel1)>
```

---

where *value* is the association key name. The key format is 32 hex digits.

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## WireGuard VPN

WireGuard is a [VPN<sup>1</sup>](#) is a protocol that operates at the network layer to provide communication between devices over a public network. It encrypts and encapsulates traffic to protect information. WireGuard supports full networking capabilities including standard, policy-based, and static routes, as well as firewalls. In addition to having IPs inside the tunnel, like IPsec and OpenVPN, you can use this WireGuard tunnel for policy-based routing: send only certain traffic through the tunnel or use it for static routes to send routing and networking through regardless of the source IP. You can also have multiple tunnels.

There are two modes available when [configuring a WireGuard VPN](#):

- **Client mode:** Configure the Connect EZ device to act as a client, so it establishes an outbound WireGuard VPN tunnel to a remote server.
- **Server mode:** Configure the Connect EZ device to act as a server, so one or more remote devices can establish an inbound WireGuard VPN tunnel to the device.

## Configure the WireGuard VPN

Your Connect EZ device supports using WireGuard VPN. You can configure the device for either client or server mode. For client mode, your Connect EZ is establishing an outbound WireGuard VPN

---

<sup>1</sup>virtual private network

connection to the WireGuard server. For server mode, your Connect EZ is acting as a WireGuard server and accepts incoming WireGuard VPN connections from one or more client devices.

### Required configuration items

<p><b>For client mode</b> You need the following information from the WireGuard server:</p> <ul style="list-style-type: none"> <li>■ Private key</li> <li>■ Remote endpoint address or hostname</li> <li>■ Remote endpoint port</li> <li>■ Remote endpoint public key</li> <li>■ Preshared key (optional)</li> <li>■ Local and remote IP addresses</li> </ul>	<p><b>For server mode</b> You need the following information:</p> <ul style="list-style-type: none"> <li>■ Client public key (can come from the client device or generated from the Digi device's shell console using the wg command if needed)</li> <li>■ Pre-shared key (optional)</li> <li>■ Local and remote IP addresses</li> </ul>
---	--

## Web

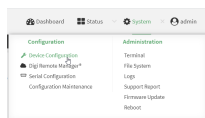
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

1. Navigate to **VPN > WireGuard > WireGuard tunnel**.
2. Click **+** to add a new WireGuard tunnel.

3. Type a name for the tunnel.
4. Click **OK**.  
The settings for your new tunnel appear.
5. Modify the settings.

Tunnel setting	UI Configuration
<b>Enable</b>	The new tunnel is enabled by default. It can be disabled if the tunnel is being set up for future use or if you want to stop the tunnel while testing other configuration changes.
<b>Peers</b>	<ol style="list-style-type: none"> <li>a. Click <b>+</b> to add a new peer. <ul style="list-style-type: none"> <li>▪ If this Connect EZ is the WireGuard client, then only add one peer. The peer is the remote Wireguard server to which it connects.</li> <li>▪ If this Connect EZ is the WireGuard server, add one or more peers. The peer(s) are the remote WireGuard clients that will connect to this device.</li> </ul> </li> <li>b. Configure the settings for the new peer(s). If the new peer is to act as the WireGuard server, make sure to configure the following settings: <ul style="list-style-type: none"> <li>▪ [Remote] Public key</li> <li>▪ [Remote] Pre-shared key (optional)</li> <li>▪ [Remote] Allowed addresses: Only traffic destined for an IP address added here is sent to this peer.</li> <li>▪ [Remote] Endpoint address</li> <li>▪ [Remote] Endpoint port</li> </ul>           If the new peer is to act as a remote WireGuard client, make sure to configure the following settings: <ul style="list-style-type: none"> <li>▪ [Client] Public key</li> <li>▪ [Client] Pre-shared key (optional)</li> <li>▪ [Local and Remote] Allowed addresses</li> </ul> </li> </ol>
<b>Device managed private key</b>	Enable to allow the Connect EZ to generate its own public and private keys. If this setting is enabled, it triggers the Connect EZ to automatically generate a private key and corresponding public key. This private and public key is used to establish the encrypted communication between the client and peer via the Wireguard tunnel. To see the public key, navigate to <b>Status &gt; VPN &gt; WireGuard</b> .
<b>Private key</b>	Type the private key for the Wireguard tunnel, if the <b>Device managed private key</b> setting is disabled.
<b>Endpoint port</b>	The WireGuard connection value of <b>51820</b> is populated by default.

- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Save the configuration and apply the change

```
(config vpn iptunnel gre_example)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.
- At the command line, type **VPN** to enter configuration mode for VPN:

```
> config vpn
(config vpn)>
```

- Type **wireguard** to enter configuration mode for WireGuard.

```
> config vpn wireguard
(config vpn wireguard)>
```

- The table below lists the required settings for creating and configuring a client WireGuard tunnel.

Configuration	Description
<b>add</b>	<p>Add a new WireGuard tunnel.</p> <pre>&gt; config vpn wireguard add name (config)&gt;</pre> <p>Where <i>name</i> is the name of the new WireGuard tunnel.</p>
<b>enable</b>	<p>The WireGuard tunnel is enabled by default. You may want to temporarily disable the tunnel while it is being set up, for future use, or if you want to stop the tunnel while testing other configuration changes. To disable:</p> <pre>(config)&gt; vpn wireguard name enable false</pre>

	<pre>(config)&gt;</pre> <hr/> <p>To enable:</p> <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> enable true (config)&gt;</pre> <hr/>
<b>peer</b>	<p>a. Determine if the Connect EZ will act as a client or server.</p> <ul style="list-style-type: none"> <li>▪ If this Connect EZ is the WireGuard client, then only add one peer. The peer is the remote Wireguard server to which it connects.</li> <li>▪ If this Connect EZ is the WireGuard server, add one or more peers. The peer(s) are the remote WireGuard clients that will connect to this device.</li> </ul> <p>b. Create the peer(s).</p> <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> add peer (config)&gt;</pre> <hr/> <p>For a peer that acts as the remote Wireguard server, configure the following settings:</p> <ul style="list-style-type: none"> <li>▪ [Remote] Public key <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> peer public_key (config)&gt;</pre> <hr/> </li> <li>▪ [Remote] Pre-shared key (optional) <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> peer psk (config)&gt;</pre> <hr/> </li> <li>▪ [Remote] Allowed addresses: Only traffic destined for an IP address added here will be sent to this peer. <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> peer overlay (config)&gt;</pre> <hr/> </li> <li>▪ [Remote] Endpoint address <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> peer endpoint (config)&gt;</pre> <hr/> </li> <li>▪ [Remote] Endpoint port <hr/> <pre>(config)&gt; vpn wireguard <i>name</i> peer port (config)&gt;</pre> <hr/> </li> </ul> <p>For the a peer(s) that acts as the remote WireGuard client, configure the following settings:</p> <ul style="list-style-type: none"> <li>▪ [Client] Public key</li> </ul>



	<pre>(config)&gt; vpn wireguard name peer public_key (config)&gt;</pre> <hr/> <ul style="list-style-type: none"> <li>▪ [Client] Pre-shared key (optional)</li> </ul> <pre>(config)&gt; vpn wireguard name peer psk (config)&gt;</pre> <hr/> <ul style="list-style-type: none"> <li>▪ [Local and Remote] Allowed addresses</li> </ul>
<b>autogenerate</b>	<p>Enable to allow the Connect EZ to generate its own public and private keys. If this setting is enabled, it triggers the Connect EZ to automatically generate a private key and corresponding public key. To enable:</p> <pre>&gt; config vpn wireguard add name autogenerate true (config)&gt;</pre> <p>To disable:</p> <pre>&gt; config vpn wireguard add name autogenerate true (config)&gt;</pre>
<b>port</b>	<p>The WireGuard connection value of <b>51820</b> is populated by default.</p> <pre>(config)&gt; vpn wireguard name port (config)&gt;</pre>
<b>private-key</b>	<p>Type the private key for the Wireguard tunnel, if the <b>Device managed private key</b> setting is disabled.</p> <pre>&gt; config vpn wireguard add name private key value (config)&gt;</pre> <p>With <i>value</i> being a 32-byte string encoded in base 64.</p>

## Services

---

This chapter contains the following topics:

Allow remote access for web administration and SSH .....	339
Configure the web administration service .....	342
Configure SSH access .....	351
Use SSH with key authentication .....	358
Configure telnet access .....	361
Configure DNS .....	366
Simple Network Management Protocol (SNMP) .....	373
Location information .....	380
Modbus gateway .....	409
System time .....	426
Network Time Protocol .....	430
Configure a multicast route .....	437
Enable service discovery (mDNS) .....	440
Use the iPerf service .....	443
Configure the ping responder service .....	447

## Allow remote access for web administration and SSH

By default, only devices connected to the Connect EZ's LAN have access to the device via web administration and SSH. To enable these services for access from remote devices:

- The Connect EZ device must have a publicly reachable IP address.
- The **External** firewall zone must be added to the web administration or SSH service. See [Firewall configuration](#) for information on zones.
- See [Set the idle timeout for Connect EZ users](#) for information about setting the inactivity timeout for the web administration and SSH services.

To allow web administration or SSH for the External firewall zone:

### Add the External firewall zone to the web administration service

#### ≡ Web

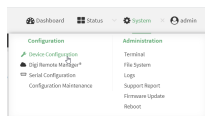
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

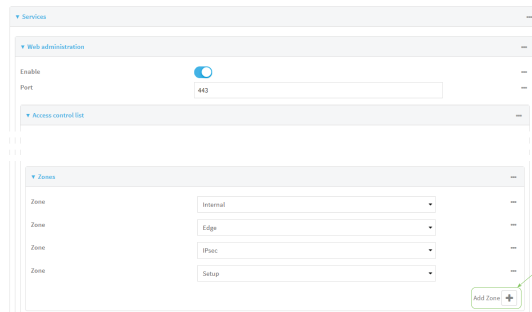
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



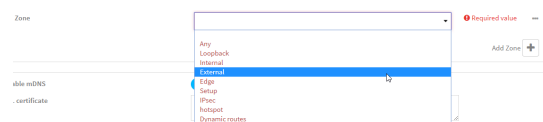
The **Configuration** window is displayed.

3. Click **Services > Web administration > Access Control List > Zones**.

- For **Add Zone**, click **+**.



- Select **External**.



- Click **Apply** to save the configuration and apply the change.

## Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Add the external zone to the web administration service:

```
(config)> add service web_admin acl zone end external
(config)>
```

- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Add the External firewall zone to the SSH service

## Web

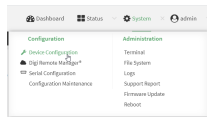
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

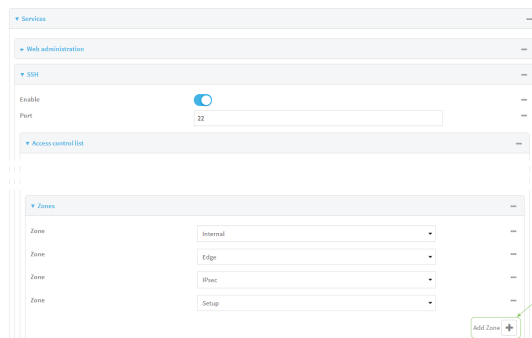
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

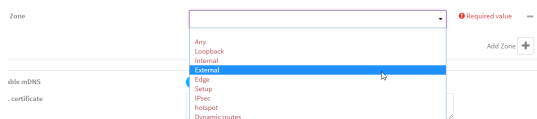


The **Configuration** window is displayed.

3. Click **Configuration > Services > SSH > Access Control List > Zones**.
4. For **Add Zone**, click **+**.



5. Select **External**.



6. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the **External** zone to the SSH service:

```
(config)> add service ssh acl zone end external
(config)>
```

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the web administration service

The web administration service allows you to monitor and configure the Connect EZ device by using the WebUI, a browser-based interface.

By default, the web administration service is enabled and uses the standard HTTPS port, 443. The default access control for the service uses the **Internal** firewall zone, which means that only devices connected to the Connect EZ's LAN can access the WebUI. If this configuration is sufficient for your needs, no further configuration is required. See [Allow remote access for web administration and SSH](#) for information about configuring the web administration service to allow access from remote devices.

### **Required configuration items**

- The web administration service is enabled by default.
- Configure access control for the service.

### **Additional configuration items**

- Port to use for web administration service communication.
- Multicast DNS (mDNS) support.
- An SSL certificate to use for communications with the service.
- Support for legacy encryption protocols.

See [Set the idle timeout for Connect EZ users](#) for information about setting the inactivity timeout for the web administration services.

## Enable or disable the web administration service

The web administration service is enabled by default. To disable the service, or enable it if it has been disabled:

### ≡ Web

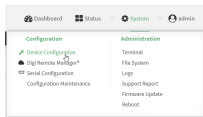
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Web administration**.
4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

### ⌨ Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable or disable the web administration service:
  - To enable the service:

```
(config)> service web_admin enable true
(config)>
```

- To disable the service:

```
(config)> service web_admin enable false
(config)>
```

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the service

### Web

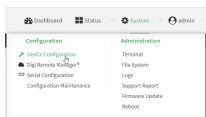
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Web administration**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:



- A single IP address or host name.
  - A network designation in CIDR notation, for example, 192.168.1.0/24.
  - **any**: No limit to IPv4 addresses that can access the web administration service.
- d. Click **+** again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the web administration service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
7. For **SSL certificate**, if you have your own signed SSL certificate, paste the certificate and private key. If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
- The SSL certificate and private key must be in PEM format.
  - The private key can use one of the following algorithms:
    - RSA
    - DSA
    - ECDSA
    - ECDH

---

**Note** Password-protected certificate keys are not supported.

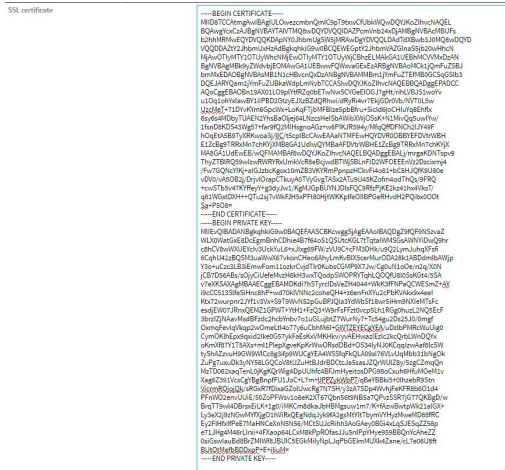
---

Example:

- a. Generate the SSL certificate and private key, for example:

```
# openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365
-out certificate.pem
```

- b. Paste the contents of **certificate.pem** and **key.pem** into the **SSL certificate** field. The contents of the **certificate.pem** must be first. For example:



8. **View** is set to **Auto** by default and normally should not be changed.
9. **Legacy port redirection** is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed. To disable legacy port redirection, click to expand **Legacy port redirection** and deselect **Enable**.
10. For **Minimum TLS version**, select the minimum TLS version that can be used by client to negotiate the HTTPS session.
11. Click **Apply** to save the configuration and apply the change.

 **Command line**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
  - To limit access to specified IPv4 addresses and networks:

```
(config)> add service web_admin acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the web administration service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service web_admin acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the web administration service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service web_admin acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service web_admin acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

```
-----
-----
any
dynamic_routes
edge
```

---

---

```
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

4. (Optional) If you have your own signed SSL certificate, if you have your own signed SSL certificate, set the certificate and private key by pasting their contents into the **service web\_admin cert** command. Enclose the certificate and private key contents in quotes (").

---

```
(config)> service web_admin cert "ssl-cert-and-private-key"
(config)>
```

---

- If **SSL certificate** is blank, the device will use an automatically-generated, self-signed certificate.
- The SSL certificate and private key must be in PEM format.
- The private key can use one of the following algorithms:
  - RSA
  - DSA
  - ECDSA
  - ECDH

---

**Note** Password-protected certificate keys are not supported.

---

### Example

- a. Generate the SSL certificate and private key, for example:

---

```
# openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365
-out certificate.pem
```

---

- b. Paste the contents of **certificate.pem** and **key.pem** into the **service web\_admin cert** command. Enclose the contents of **certificate.pem** and **key.pem** in quotes. For example:

---

```
(config)> service web_admin cert "-----BEGIN CERTIFICATE-----
MIID8TCCAAtmgAwIBAgIULOwezcmBnQmIC9pT9txwCfUbkWQwDQYJKoZIhvcNAQEL
BQAwgYcx CzA JBgNVBAYTALVTMQ8wDQYDVQQIDAZPcmVnb24xDjAMBgNVBACMBUFs
b2hhMRMwEQYDVQKDApNY0JhbmUgSW5jMRAwDgYDVQLDAdTdBWb3J0M08wDQYD
VQQDDAztY2JhbmUxHzAdBgkqhkiG9w0BCQEWEgptY2JhbmVAZGlnaS5jb20wHhcN
MjAwOTIyMTY1OTUyWhcNMjEwOTIyMTY1OTUyWjCBhzELMAkGA1UEBhMCMVVMxZAN
BgNVBAGMBk9yZWdvbjEOMAwGA1UEBwwFQWxvaGEzEzARBgNVBAoMCK1jQmFuZSBj
bmMxEDA0BgNVBAsMB1N1cHBvcnQxDzANBgNVBAMMBm1jYmFuZTEfMB0GCSqGSIb3
DQEJARYQam1jYmFuZUBkaWdpLmNvbTCCASIdQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBA0Bn19AX01L09pLYtFRZq0bETwNwSCYGeEIOGJ7gHt/rihLVBJS1woYv
u10q1ohYxIawBY1iIPBD2GtzyEJXzBZdQRhwi/dRyRi4vr7EkjGDr0Vb/NVT0L5w
UzcMeT+71DYvKYm6GpcWx+LoKqFTjbMFBIZE5pbBfru+SicId6jochIuYq8Ehflx
6sy6s4MDbyTUAEN2YhsBa0ljeje64LNzcsHeISbAWibXWj0SsK+N1MivQq5uwIYw/
```

---

```

1fsnD8KDS43Wg57+far9fQ2MIHsgnoAGz+w6PIKJR594y/MfqQffDFNCh2LJY49F
h0qEtA5B9TyXRKwoa3j/LIC/t5cpIBcCAwEAAaNTMFewHQYDVR00BbYEFDVtrWBH
E1ZcBg9TRRxMn7chKYjXMB8GA1UdIwQYMBaAFDVtrWBHE1ZcBg9TRRxMn7chKYjX
MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBALj/mrgaKDNTspv9
ThyZTBLRQ59wIzwrWRYRxxUmkVcR8eBcjwdBTWjSBLnFLD2WFOEEEnVz2Dzcixmj4
/Fw7GQNCyIKj+aIGJzbcKgox10mZB3VKYRmPpnpzHCkvFi4o81+bC8HJQfK9U80e
vDV0/vA50B2j/DrjvlOrapCTkuyA0TVyGvgTASx2ATu9U45KZoFm4odThQs/9FRQ
+cwStb5v47KYffeyY+g3dyJw1/KgMJGpBUYNJDI5FQC9RfzPjKE2kz41hx4VksT/
q81WGstDXH++QTu2sj7vWkFJH5xPFt80HjtWKKpIfeOILBPGerHvdH2PQibx000t
Sa+P508=
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIEVQIBADANBgkqhkiG9w0BAQEFAASCBAwEAAoIBAQDgZ9fQF9NSzvaZ
WLX0WatGxE8DcEgmBnhCDhie4B7f64oS1QSutckGL7tTqtaIWMSSGSAWNYiDwQ9hr
c8hCV8wWUXUEYcIv3UckYuL6+xJIxg69FW/zVU9C+cFM3DHk/u9Q2LymJuhqXFfi
6CqhU42zBQSM3uaWwX67vkonCHeo6AhyLmKvBIX5cerMurODA28k1ABDdmIbAWjp
Y3o+uCzc3LB3iEmwFom1lozkrCvjdTir0KubsCGMP9X7Jw/Cg0uN1o0e/n2q/X0N
jCB7D56ABs/s0jyCiUefeMvzH6kH3wxTQodpSWOPRYTqhLQOQfU8l0SsKgt4/5SA
v7eXKSAXAgMBAECCgEBAMDKdi7hSTyrclDsVeZH4044+WkK3fFNPaQCWESmZ+AY
i9cCC513SlfeSiHnc8hP+wd70klVNNc2coheQH4+z6enFnXYu2cPbKVAKx9x4eeI
Ktx72wurpnr2JYf1v3Vx+S9T9WvN52pGuBPJQla3YdWbSf18wr5iHm9NXIEMTsfC
esdjEW07JRnxQEMZ1GPWT+YtH1+FzQ3+W9rFsFFzt0vcp5Lh1RGg0huzL2NQ5EcF
3brzIZjNAavMsdBFzdc2hcbYnbnv7o1uGLujbtZ7WurNy7+Tc54gu2Ds25J0/0mgf
OxmQFevIqVkp2w0meLTI4o77y6uCbhfA6I+GWTZEYECgYEA/uDzlbPMRcWuUig0
Cym0KlhEpx9qxid2Ike0G57ykFaEsKxVMKHkv/yvAEHwazIEzlc2kcQrbLWnDQYx
oKmf87Y1T5AXs+mL1PlepXgveKpKrWwORsdDBd+OS34lyNJ0KCqQIzwaaf8lcSW
tyShAZzvuH9Gw9WlCc8g3ifp9WUCgYEA4WSSfqFkQLA09sI76VLvUqMbb31bNgOk
ZuPg7uxuDk3yNY58LGQCov8tUZuHtBjdrBDCtcJa5sasJZQRWUJLZ8y/5zgcZmqQn
MzTD062xaqTenL0jKgKQRWig4DpUUhfc4BFJmHyeitosDPG98oCxuh6HfUM0eM1v
Xag6Z391VcsCgYBgnPffU1JoC+L7m+LIPPZykWbPT/qBeYBBki5+0lhzebR9Stn
VicrmR0joJq/sRGxR7fdixaGZolUwcRg7N7SH/y3zA7SDp4WvhjFeKFR8b601d4
PFnW02envUUie/50ZoPFwsv1o8eK2XT67Qbn56t9NB5a7QPvzSSR7jG77QKBGD/w
BrqTT9wL4DBrsxEiLK+1g0/iMKCm8dkaJbHBMgsuw1m7/K+fAzwbwtpWk21aLgX+
Ly3eX2j9zNGwMYfXjg01hViRxQEgNdqJyk9fA2gsMtYlTbymVYHyzMweMD88fRC
Ey2FLHfxIFeE7MaHNceXnN5N56/MctSUJcrihh3AoGAey0BGi4xLqSJESqZZ58p
e71JHg4M46rLlrx+i4FXaop64LCxM8kPpR0fasJJu5nLpPYHye959BBQnYcAheZZ
0siGswIauBd8BrZMIWf8JBUIc5EGkMiIyNpLJqPbGEImMUXk4Zane/cL7e06U8ft
BUt0tMefbBDDxp+E+iIiuM=
-----END PRIVATE KEY-----"
(config)>

```

5. (Optional) Configure Multicast DNS (mDNS):

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

- To enable the mDNS protocol:

```

(config)> service web_admin mdns enable true
(config)>

```

- To disable the mDNS protocol:

---

```
(config)> service web_admin mdns enable false
(config)>
```

---

6. (Optional) Set the port number for this service.

The default setting of 443 normally should not be changed.

---

```
(config)> service web_admin port 444
(config)>
```

---

7. (Optional) Set the minimum TLS version that can be used by client to negotiate the HTTPS session:

---

```
(config)> service web_admin legacy_encryption value
(config)>
```

---

where *value* is one of:

- **TLS-1\_1**
- **TLS-1\_2**
- **TLS-1\_3**

The default is **TLS-1\_2**.

8. (Optional) Disable legacy port redirection.

Legacy port redirection is used to redirect client HTTP requests to the HTTPS service. Legacy port redirection is enabled by default, and normally these settings should not be changed.

To disable legacy port redirection:

---

```
(config)> service web_admin legacy enable false
(config)>
```

---

9. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

10. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure SSH access

The Connect EZ's default configuration has SSH access enabled, and allows SSH access to the device from authorized users within the **Internal** firewall zone. If this configuration is sufficient for your needs, no further configuration is required. See [Allow remote access for web administration and SSH](#) for information about configuring the SSH service to allow access from remote devices.

### Required configuration items

- Enable SSH access.
- Configure access control for the SSH service.

### Additional configuration items

- Port to use for communications with the SSH service.
- Multicast DNS (mDNS) support.
- A private key to use for communications with the SSH service.
- Create custom SSH configuration settings.

See [Set the idle timeout for Connect EZ users](#) for information about setting the inactivity timeout for the SSH service.

### Enable or disable the SSH service

The SSH service is enabled by default. To disable the service, or enable it if it has been disabled:

#### ≡ Web

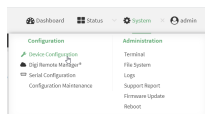
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > SSH**.
4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable or disable the SSH service:

- To enable the service:

---

```
(config)> service ssh enable true
(config)>
```

---

- To disable the service:

---

```
(config)> service ssh enable false
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Configure the service

#### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

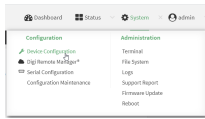
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.



Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > SSH**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's SSH service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the SSH service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's SSH service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the SSH service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.

6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
7. For **Private key**, type the private key in PEM format. If **Private key** is blank, the device will use an automatically-generated key.
8. To create custom SSH configuration settings:
  - a. Click to expand **Custom configuration**.
  - b. Click **Enable**.
  - c. For **Override**:
    - If **Override** is enabled, entries in **Configuration file** will be used in place of the standard SSH configuration.
    - If **Override** is not enabled, entries in **Configuration file** will be added to the standard SSH configuration.
  - d. For **Configuration file**, type configuration settings in the form of an OpenSSH sshd\_config file.  
For example, to enable the diffie-hellman-group-sha-14 key exchange algorithm:
    - i. Click **Enable** to enable SSH custom configuration.
    - ii. Leave **Override** disabled.
    - iii. For **Configuration file**, type the following:
 

```
KexAlgorithms +diffie-hellman-group14-sha1
```
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Configure access control:
  - To limit access to specified IPv4 addresses and networks:

```
(config)> add service ssh acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the SSH service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service ssh acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the SSH service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service ssh acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service ssh acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

```
-----
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
-----
```

---

---

```
(config)>
```

---

Repeat this step to include additional firewall zones.

4. (Optional) Set the private key in PEM format. If not set, the device will use an automatically-generated key.

---

```
(config)> service ssh key key.pem
(config)>
```

---

5. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is enabled by default. To disable mDNS, or enable it if it has been disabled:

- To enable the mDNS protocol:

---

```
(config)> service ssh mdns enable true
(config)>
```

---

- To disable the mDNS protocol:

---

```
(config)> service ssh mdns enable false
(config)>
```

---

6. (Optional) Set the port number for this service.

The default setting of 22 normally should not be changed.

---

```
(config)> service ssh port 24
(config)>
```

---

7. To create custom SSH configuration settings:

- a. Enable custom configurations:

---

```
(config)> service ssh custom enable true
(config)>
```

---

- b. To override the standard SSH configuration and only use the **config\_file** parameter:

---

```
(config)> service ssh custom override true
(config)>
```

---

- If **override** is set to **true**, entries in **Configuration file** will be used in place of the standard SSH configuration.
- If **override** is set to **false**, entries in **Configuration file** will be added to the standard SSH configuration.

The default is **false**.

- c. Set the configuration settings:

---

```
(config)> service ssh custom config_file value
(config)>
```

---

where *value* is one or more entries in the form of an OpenSSH `sshd_config` file. For example, to enable the `diffie-hellman-group-sha-14` key exchange algorithm:

---

```
(config)> service ssh custom config_file "KexAlgorithms +diffie-  
hellman-group14-sha1"  
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config)> save  
Configuration saved.  
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Use SSH with key authentication

Rather than using passwords, you can use SSH keys to authenticate users connecting via SSH, SFTP, or SCP. SSH keys provide security and scalability:

- **Security:** Using SSH keys for authentication is more secure than using passwords. Unlike a password that can be guessed by an unauthorized user, SSH key pairs provide more sophisticated security. A public key configured on the Connect EZ device is paired with a private key on the user's PC. The private key, once generated, remains on the user's PC.
- **Scalability:** SSH keys can be used on more than one Connect EZ device.

### Generating SSH key pairs

On a Microsoft Windows PC, you can generate SSH key pairs using a terminal emulator application, such as **Putty** or **Tera Term**.

On a Linux host, an SSH key pair is usually created automatically in the user's **.ssh** directory. The private and public keys are named **id\_rsa** and **id\_rsa.pub**. If you need to generate an SSH key pair, you can use the **ssh-keygen** application.

For example, the following entry generates an RSA key pair in the user's **.ssh** directory:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa
```

The private key file is named **id\_rsa** and the public key file is named **id\_rsa.pub**. (The **.pub** extension is automatically appended to the name specified for the private key output file.)

### Required configuration items

- Name for the user
- SSH public key for the user

### Additional configuration items

- If you want to access the Connect EZ device using SSH over a WAN interface, configure the access control list for the SSH service to allow SSH access for the **External** firewall zone.

### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Users**.
4. Select an existing user or create a new user. See [User authentication](#) for information about creating a new user.
5. Click **SSH keys**.
6. In **Add SSH key**, enter a name for the SSH key and click **+**.
7. Enter the public SSH key by pasting or typing a public encryption key that this user can use for passwordless SSH login.
8. Click **Apply** to save the configuration and apply the change.

### Command line

You can add configure passwordless SSH login for an existing user or include the support when creating a new user. See [User authentication](#) for information about creating a new user. These instructions assume an existing user named **temp\_user**.

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add an SSH key for the user by using the `ssh_key` command and pasting or typing a public encryption key:

```
(config)> add auth user maria ssh_key key_name key
(config)>
```

where:

- `key_name` is a name for the key.
  - `key` is a public SSH key, which you can enter by pasting or typing a public encryption key that this user can use for passwordless SSH login
4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.



## Configure telnet access

By default, the telnet service is disabled.

**Note** Telnet is an insecure protocol and should only be used for backward-compatibility reasons, and only if the network connection is otherwise secured.

### Required configuration items

- Enable telnet access.
- Configure access control for the telnet service.

### Additional configuration items

- Port to use for communications with the telnet service.
- Multicast DNS (mDNS) support.

See [Set the idle timeout for Connect EZ users](#) for information about setting the inactivity timeout for the telnet service.

### Enable the telnet service

The telnet service is disabled by default. To enable the service:

#### ≡ Web

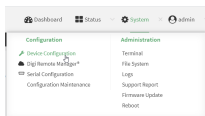
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > telnet**.

4. Click **Enable**.
5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable the telnet service:

---

```
(config)> service telnet enable true
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Configure the service

#### Web

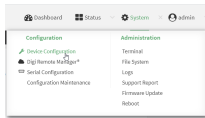
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > telnet**.
4. (Optional) For **Port**, enter the port number for the service. Normally this should not be changed.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's telnet service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the telnet service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's telnet service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the telnet service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.

6. Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
7. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service telnet acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the telnet service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service telnet acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the telnet service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service telnet acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service telnet acl zone end value
(config)>
```

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

```
-----
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

Repeat this step to include additional firewall zones.

4. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. mDNS is disabled by default. To enable:

```
(config)> service telnet mdns enable true
(config)>
```

5. (Optional) Set the port number for this service.

The default setting of 23 normally should not be changed.

```
(config)> service telnet port 25
(config)>
```

6. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure DNS

The Connect EZ device includes a caching DNS server which forwards queries to the DNS servers that are associated with the network interfaces, and caches the results. This server is used within the device, and cannot be disabled. Use the access control list to restrict external access to this server.

### Required configuration items

- Configure access control for the DNS service.

### Additional configuration items

- Whether the device should cache negative responses.
- Whether the device should always perform DNS queries to all available DNS servers.
- Whether to prevent upstream DNS servers from returning private IP addresses.
- Additional DNS servers, in addition to the ones associated with the device's network interfaces.
- Specific host names and their IP addresses.

The device is configured by default with the hostname **digi.device**, which corresponds to the **192.168.210.1** IP address.

To configure the DNS server:

### Web

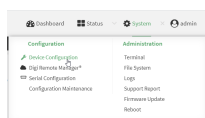
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > DNS**.
4. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's DNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the DNS service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's DNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the DNS service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
5. (Optional) **Cache negative responses** is enabled by default. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable, click to toggle off **Cache negative responses**.
6. (Optional) **Query all servers** is enabled by default. This option is useful when only some DNS servers will be able to resolve hostnames. To disable, click to toggle off **Query all servers**.
7. (Optional) **Rebind protection**, if enabled, prevents upstream DNS servers from returning private IP addresses. To enable, click **Rebind protection**.
8. (Optional) **Allow localhost rebinding** is enabled by default if **Rebind protection** is enabled. This is useful for Real-time Black List (RBL) servers.

9. (Optional) Type the IP address of the **Fallback server**. This is a DNS server to be used in the absence of any other server. The default is **8.8.8.8**.
10. (Optional) To add additional DNS servers:
  - a. Click **DNS servers**.
  - b. For **Add Server**, click **+**.
  - c. (Optional) Enter a label for the DNS server.
  - d. For **DNS server**, enter the IP address of the DNS server.
  - e. **Domain** restricts the device's use of this DNS server based on the domain. If no domain are listed, then all queries may be sent to this server.
11. (Optional) To add host names and their IP addresses that the device's DNS server will resolve:
  - a. Click **Additional DNS hostnames**.
  - b. For **Add Host**, click **+**.
  - c. Type the **IP address** of the host.
  - d. For **Name**, type the hostname.
12. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Configure access control:
  - To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service dns acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service dns acl address6 end value
(config)>
```

---

Where *value* can be:



- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the DNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service dns acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service dns acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

#### 4. (Optional) Cache negative responses

By default, the device's DNS server caches negative responses. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers

may have positive results. To disable:

---

```
(config)> service dns cache_negative_responses false
(config)>
```

---

5. (Optional) Query all servers

By default, the device's DNS server queries all available DNS servers. Disabling this option may improve performance on networks with transient DNS results, when one or more DNS servers may have positive results. To disable:

---

```
(config)> service dns query_all_servers false
(config)>
```

---

6. (Optional) Rebind protection

By default, rebind protection is disabled. If enabled, this prevents upstream DNS servers from returning private IP addresses. To enable:

---

```
(config)> service dns stop_dns_rebind false
(config)>
```

---

7. (Optional) Allow localhost rebinding

By default, localhost rebinding is enabled by default if rebind protection is enabled. This is useful for Real-time Black List (RBL) servers. To disable:

---

```
(config)> service dns rebind_localhost_ok false
(config)>
```

---

8. (Optional) Fallback server

Configure the IP address of the DNS server to be used in the absence of any other server. The default is **8.8.8.8**.

---

```
(config)> service dns fallback_server value
(config)>
```

---

9. (Optional) Add additional DNS servers

a. Add a DNS server:

---

```
(config)> add service dns server end
(config service dns server 0)>
```

---

b. Set the IP address of the DNS server:

---

```
(config service dns server 0)> address ip-addr
(config service dns server 0)>
```

---

c. To restrict the device's use of this DNS server based on the domain, use the **domain** command. If no domain are listed, then all queries may be sent to this server.

---

```
(config service dns server 0)> domain domain
(config service dns server 0)>
```

---

- d. (Optional) Set a label for this DNS server:

```
(config service dns server 0)> label label
(config service dns server 0)>
```

10. (Optional) Add host names and their IP addresses that the device's DNS server will resolve
- a. Add a host:

```
(config)> add service dns host end
(config service dns host 0)>
```

- b. Set the IP address of the host:

```
(config service dns host 0)> address ip-addr
(config service dns host 0)>
```

- c. Set the host name:

```
(config service dns host 0)> name host-name
(config service dns host 0)>
```

11. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show DNS server

You can display status for DNS servers. This command is available only at the Admin CLI.

### Command line

#### Show DNS information

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the [show dns](#) command at the system prompt:

```
> show dns
```

Interface	Label	Server	Domain
eth1		192.168.3.1	
eth1		fd00:2704::1	

---

```
eth1          fe80::227:4ff:fe2b:ae12
eth1          fe80::227:4ff:fe44:105b
eth1          fe80::240:ffff:fe80:23b0
```

>

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a protocol for remotely managing and monitoring network devices. Network administrators can use the SNMP architecture to manage nodes, including servers, workstations, routers, switches, hubs, and other equipment on an IP network, manage network performance, find and solve network problems, and plan for network growth.

The Connect EZ device supports both SNMPv3 and SNMPv2c in read-only mode. Both are disabled by default. SNMPv1 is not supported.

### SNMP Security

By default, the Connect EZ device automatically blocks SNMP packets from being received over WAN and LAN interfaces. As a result, if you want a Connect EZ device to receive SNMP packets, you must configure the SNMP access control list to allow the device to receive the packets. See [Configure Simple Network Management Protocol \(SNMP\)](#).

### Standard and custom Management Information Bases (MIB)

The standard MIB defines the properties and access permissions for various managed objects so that you can query standard information about a device, like *system contact* or *system location* via SNMP monitoring. The custom MIB defines the unique properties and access permissions not found in the standard MIB. To view the MIB list, see [Download MIBs](#).

### Dynamic SNMP

To expose a specific device property for SNMP monitoring that is not included in the standard MIB - properties like *serial number*, *system firmware version*, *hardware model name*, and *dynamic properties* - you can query the runtime database for the property value and then add a Dynamic SNMP. The device property is added to the custom MIB.

## Configure Simple Network Management Protocol (SNMP)

### Required configuration items

- Enable SNMP.
- Firewall configuration using access control to allow remote connections to the SNMP agent.
- The user name and password used to connect to the SNMP agent.

### Additional configuration items

- The port used by the SNMP agent.
- Authentication type (either MD5 or SHA).
- Privacy protocol (either DES or AES).
- Privacy passphrase, if different than the SNMP user password.
- Enable Multicast DNS (mDNS) support.

To configure the SNMP agent on your Connect EZ device:



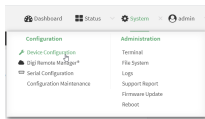
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > SNMP**.
4. Click **Enable**.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's SNMP agent. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the SNMP agent.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's SNMP agent. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the SNMP agent.
    - d. Click **+** again to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
- 6. Type the **Username** used to connect to the SNMP agent.
- 7. Type the **Password** used to connect to the SNMP agent.
- 8. (Optional) For **Port**, type the port number. The default is **161**.
- 9. (Optional) Multicast DNS (mDNS) is disabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To enable mDNS, click **Enable mDNS**.
- 10. (Optional) Select the **Authentication type**, either **MD5** or **SHA**. The default is **MD5**.
- 11. (Optional) Type the **Privacy passphrase**. If not set, the password, entered above, is used.
- 12. (Optional) Select the **Privacy protocol**, either **DES** or **AES**. The default is **DES**.
- 13. (Optional) Add **Dynamic SNMP Properties** to expose specific details about your device for SNMP monitoring that are not included in the standard MIB. To query the runtime database to find the device property you want to expose to SNMP, see [Use digidevice runtime to access the runtime database](#).
  - a. Click **+**.
  - b. For **Property**, type the device property (e.g., "system.cpu\_temp" or "system.name").
  - c. Click **+** again to add another dynamic SNMP property.
- 14. (Optional) Click **Enable version 2c access** to enable read-only access to SNMP version 2c.
- 15. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

## 3. Enable the SNMP agent:

---

```
(config)> service snmp enable true
(config)>
```

---

## 4. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service snmp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the SNMP service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service snmp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the SNMP service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service snmp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service snmp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:



Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

---



---

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

---

```
(config)>
```

---

Repeat this step to include additional firewall zones.

5. Set the name of the user that will be used to connect to the SNMP agent.

---

```
(config)> service snmp username name
(config)>
```

---

6. Set the password for the user that will be used to connect to the SNMP agent:

---

```
(config)> service snmp password pwd
(config)>
```

---

7. (Optional) Set the port number for the SNMP agent. The default is **161**.

---

```
(config)> service snmp port port
(config)>
```

---

8. (Optional) Configure Multicast DNS (mDNS)

mDNS is a protocol that resolves host names in small networks that do not have a DNS server. For the SNMP agent, mDNS is disabled by default. To enable:

---

```
(config)> service snmp mdns enable true
(config)>
```

---

9. (Optional) Set the authentication type. Allowed values are **MD5** or **SHA**. The default is **MD5**.

---

```
(config)> service snmp auth_type SHA
(config)>
```

---

10. (Optional) Set the privacy passphrase. If not set, the password, entered above, is used.

---

```
(config)> service snmp privacy pwd
(config)>
```

---

11. (Optional) Set the privacy protocol, either **DES** or **AES**. The default is **DES**.

---

```
(config)> service snmp privacy_protocol AES
(config)>
```

---

12. (Optional) Add **Dynamic SNMP Properties** to expose specific details about your device for SNMP monitoring that are not included in the standard MIB.

---

```
(config) service snmp runt> add end value
(config)>
```

---

Where *value* can be any element in the runtime table you want to expose to SNMP monitoring (for example, "system.cpu\_temp" or "system.name").

13. (Optional) Enable read-only access to to SNMP version 2c.

---

```
(config)> service snmp enable 2c true
(config)>
```

---

14. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

15. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Download MIBs

This procedure is available from the WebUI only.

### Required configuration items

- Enable SNMP.

To download a .zip archive of the SNMP MIBs supported by this device:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. Enable SNMP.

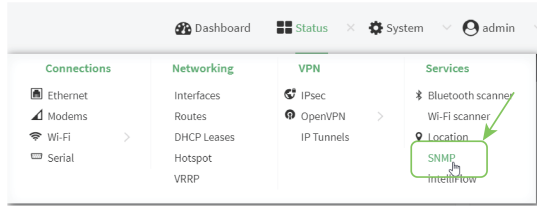
See [Configure Simple Network Management Protocol \(SNMP\)](#) for information about enabling and configuring SNMP support on the Connect EZ device.

2. On the main menu, click **Status**. Under **Services**, click **SNMP**.

---

**Note** If you have recently enabled SNMP and the SNMP option is not visible, refresh your browser.

---



The **SNMP** page is displayed.



3. Click **Download**.

## Location information

Your Connect EZ device can be configured to use the following location sources:

- User-defined static location.
- Location messages forwarded to the device from other location-enabled devices.

You can also configure your Connect EZ device to forward location messages, either from the Connect EZ device or from external sources, to a remote host. Additionally, the device can be configured to use a geofence, to allow you to determine actions that will be taken based on the physical location of the device.

This section contains the following topics:

Configure the location service .....	381
Configure the device to use a user-defined static location .....	383
Configure the device to accept location messages from external sources .....	385
Forward location information to a remote host .....	389
Configure geofencing .....	396
Show location information .....	408

## Configure the location service

Use the location service feature to identify and track the location of your Connect EZ router. This feature is enabled by default.

### Web

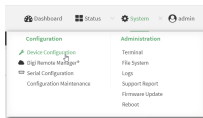
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

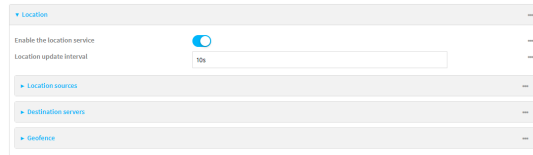
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Location**.



4. The location service is enabled by default. To disable, toggle off **Enable**.
5. For **Location update interval**, type the amount of time to wait between polling location sources for new location data. The default is ten seconds.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Location update interval** to ten minutes, enter **10m** or **600s**.

6. For information about configuring **Location sources**, see the following:
  - a. To accept location information from an external location-enabled server, see [Configure the device to accept location messages from external sources](#).
  - b. To set a static location for the device, see [Configure the device to use a user-defined static location](#).

If multiple location sources are enabled at the same time, the device's location will be determined based on the order that the location sources are listed here.

7. See [Forward location information to a remote host](#) for information about configuring **Destination servers**.
8. See [Configure geofencing](#) for information about configuring **Geofence**.
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable or disable the GNSS module:

- To enable the module:

---

```
(config)> service location gnss true
(config)>
```

---

- To disable the module:

---

```
(config)> service location gnss false
(config)>
```

---

4. Set the amount of time that the Connect EZ device will wait before polling location sources for updated location data:

---

```
(config)> service location interval value
(config)>
```

---

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> service location interval 600s
(config)>
```

---

The default is 10 seconds.

5. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the device to use a user-defined static location

You can configure your Connect EZ device to use a user-defined static location.

### Web

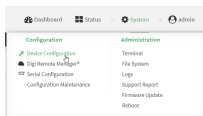
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- Click **Services > Location > Location sources**.
- Click **+** to add a location source.
- (Optional) Type a **Label** for this location source.
- For **Type of location source**, select **User-defined location**.
- The location source is enabled by default. Click **Enable the location source** to disable the location source, or to enable it if it has been disabled.
- For **Latitude**, type the latitude of the device. Allowed values are **-90** and **90**, with up to six decimal places.
- For **Longitude**, type the longitude of the device. Allowed values are **-180** and **180**, with up to six decimal places.
- For **Altitude**, type the altitude of the device. Allowed values are an integer followed by **m** or **km**, for example, **100m** or **1km**.
- Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a location source:

---

```
(config)> add service location source end
(config service location source 0)>
```

---

The location source is enabled by default. To disable:

---

```
(config service location source 0)> enable false
(config service location source 0)>
```

---

4. (Optional) Set a label for this location source:

---

```
(config service location source 0)> label "label"
(config)>
```

---

5. Set the **type** of location source to **user\_defined**:

---

```
(config service location source 0)> type user_defined
(config service location source 0)>
```

---

6. Set the latitude of the device:

---

```
(config service location source 0 coordinates latitude int
(config service location source 0)>
```

---

where *int* is any integer between **-90** and **90**, with up to six decimal places.

7. Set the longitude of the device:

---

```
(config service location source 0 coordinates longitude int
(config service location source 0)>
```

---

where *int* is any integer between **-180** and **180**, with up to six decimal places.

8. Set the altitude of the device:

---

```
(config service location source 0 coordinates altitude alt
(config service location source 0)>
```

---

Where *alt* is an integer followed by **m** or **km**, for example, **100m** or **1km**.

9. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---



10. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the device to accept location messages from external sources

You can configure the Connect EZ device to accept NMEA and TAIP messages from external sources. For example, location-enabled devices connected to the Connect EZ device can forward their location information to the device, and then the Connect EZ device can serve as a central repository for this location information and forward it to a remote host. See [Forward location information to a remote host](#) for information about configuring the Connect EZ device to forward location messages.

This procedure configures a UDP port on the Connect EZ device that will be used to listen for incoming messages.

### Required configuration items

- The location server must be enabled.
- UDP port that the Connect EZ device will listen to for incoming location messages.
- Access control list configuration to provide access to the port through the firewall.

To configure the device to accept location messages from external sources:

### Web

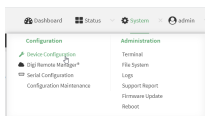
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Location > Location sources**.
4. Click **+** to add a location source.
5. (Optional) Type a **Label** for this location source.
6. For **Type of location source**, select **Server**.

7. For **Location server port**, type the number of the UDP port that will receive incoming location messages.
8. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's location server UDP port. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the location server UDP port.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's location server UDP port. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the location server UDP port.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
9. Click **Apply** to save the configuration and apply the change.

### **Command line**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a location source:

---

```
(config)> add service location source end
(config service location source 0)>
```

---

4. (Optional) Set a label for this location source:

---

```
(config service location source 0)> label "label"
(config service location source 0)>
```

---

5. Set the **type** of location source to **server**:

---

```
(config service location source 0)> type server
(config service location source 0)>
```

---

6. Set the UDP port that will receive incoming location messages.

---

```
(config service location source 0)> server port port
(config service location source 0)>
```

---

7. Click **Access control list** to configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service location source 1 acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the location server UDP port.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service location source 1 acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the location server UDP port.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service location source 1 acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service location source 1 acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

2. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Forward location information to a remote host

You can configure location clients on the Connect EZ device that forward location messages in either NMEA or TAIP format to a remote host.

### Required configuration items

- Enable the location service.
- The hostname or IP address of the remote host to which the location messages will be forwarded.
- The communication protocol, either TCP or UDP.
- The destination port on the remote host to which the messages will be forwarded.
- Message protocol type of the messages being forwarded, either NMEA or TAIP.

### Additional configuration items

- Additional remote hosts to which the location messages will be forwarded.
- Location update interval, which determines how often the device will forward location information to the remote hosts.
- A description of the remote hosts.
- Specific types of NMEA or TAIP messages that should be forwarded.
- If the message protocol is NMEA, configure a talker ID to be used for all messages.
- Text that will be prepended to the forwarded message.
- A vehicle ID that is used in the TAIP ID message and can also be prepended to the forwarded message.

Configure the Connect EZ device to forward location information:

### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Location > Destination servers**.
4. For **Add destination server**, click **+**.
5. (Optional) For **Label**, type a description of the location destination server.
6. For **Destination server**, enter the hostname or IP address of the remote host to which location messages will be sent.
7. For **Destination server port**, enter the UDP or TCP port on the remote host to which location messages will be sent.
8. For **Communication protocol**, select either **UDP** or **TCP**.
9. For **Forward interval multiplier**, select the number of **Location update intervals** to wait before forwarding location data to this server. See [Configure the location service](#) for more information about setting the **Location update interval**.
10. For **NMEA filters**, select the filters that represent the types of messages that will be forwarded. By default, all message types are forwarded.
  - To remove a filter:
    - a. Click the down arrow (▼) next to the appropriate message type.
    - b. Click **Delete**.
  - To add a message type:
    - a. For **Add NMEA filter** or **Add TAIP filter**, click **+**.
    - b. Select the filter type. Allowed values are:
      - **GGA**: Reports time, position, and fix related data.
      - **GLL**: Reports position data: position fix, time of position fix, and status.
      - **GSA**: Reports GPS DOP and active satellites.
      - **GSV**: Reports the number of SVs in view, PRN, elevation, azimuth, and SNR.
      - **RMC**: Reports position, velocity, and time.
      - **VTG**: Reports direction and speed over ground.
11. For **TAIP filters**, select the filters that represent the types of messages that will be forwarded. By default, all message types are forwarded.
  - To remove a filter:
    - a. Click the down arrow (▼) next to the appropriate message type.
    - b. Click **Delete**.
  - To add a message type:
    - a. For **Add NMEA filter** or **Add TAIP filter**, click **+**.
    - b. Select the filter type. Allowed values are:
      - **AL**: Reports altitude and vertical velocity.
      - **CP**: Compact position: reports time, latitude, and longitude.

- **ID:** Reports the vehicle ID.
  - **LN:** Long navigation: reports the latitude, longitude, and altitude, the horizontal and vertical speed, and heading.
  - **PV:** Position/velocity: reports the latitude, longitude, and heading.
12. For **Outgoing message type**, select either **NMEA** or **TAIP** for the type of message that the device will forward to a remote host.
- (Optional) If **NMEA** is selected:
- a. Select a **Talker ID**.  
The talker ID is a two-character prefix in the NMEA message that identifies the source type. The talker ID set here will override the talker ID from all sources, and all forwarded sentences will use the configured ID. The default setting is **Default**, which means that the talker ID provided by the source will be used.
  - b. Determine the **Behavior when fix is invalid**:
    - **None:** No messages are sent.
    - **Empty:** Send messages with empty fields.
    - **Last fix:** Send messages with information from the last valid fix.
13. (Optional) For **Prepend text**, enter text to prepend to the forwarded message. Two variables can be included in the prepended text:
- **%s:** Includes the Connect EZ device's serial number in the prepended text.
  - **%v:** Includes the vehicle ID in the prepended text.
- For example, to include both the device's serial number and vehicle ID in the prepend message, you can enter the following in the **Prepend** field:
- 
- ```
__|%s|__|%v|__
```
- 
14. Type a four-digit alphanumeric **Vehicle ID** that will be included with to location messages. If no vehicle ID is configured, this setting defaults to 0000.
15. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a remote host to which location messages will be sent:

---

```
(config)> add service location forward end
(config service location forward 0)>
```

---

4. Set the hostname or IP address of the remote host to which location messages will be sent:

---

```
(config service location forward 0)> server host
(config service location forward 0)>
```

---

5. Set the communication protocol to either **udp** or **tcp**:

---

```
(config service location forward 0)> protocol protocol
(config service location forward 0)>
```

---

6. Set the TCP or UDP port on the remote host to which location messages will be sent:

---

```
(config service location forward 0)> server_port 8000
(config service location forward 0)>
```

---

7. Set the number of **Location update intervals** to wait before forwarding location data to this server. See [Configure the location service](#) for more information about setting the **Location update interval**.

---

```
(config service location forward 0)> interval_multiplier int
(config service location forward 0)>
```

---

8. Set the protocol type for the messages. Allowed values are **taip** or **nmea**; the default is **taip**:

---

```
(config service location forward 0)> type nmea
(config service location forward 0)>
```

---

(Optional) If the protocol type is set to **nmea**:

- a. Configure a **Talker ID**.

The talker ID is a two-character prefix in the NMEA message that identifies the source type. The talker ID set here will override the talker ID from all sources, and all forwarded sentences will use the configured ID.

- i. Use the **?** to determine available talker IDs:

---

```
(config service location forward 0)> talker_id ?
```

```
Talker ID: Setting a talker ID will override the talker ID from
all remote
sources, and all forwarded sentences from remote sources will use
the configured
ID.
```

```
Format:
```

```
Default
```

```
GA
```

```
GB
```

```
GI
```

```
GL
```

```
GN
```

```
GP
```

```
GQ
```

```
Default value: Default
```

---



---

```
Current value: Default
```

```
(config service location forward 0)>
```

---

ii. Set the talker ID:

```
(config service location forward 0)> talker_id value
(config service location forward 0)>
```

---

The default setting is **Default**, which means that the talker ID provided by the source will be used.

b. Determine the behavior when fix is invalid:

```
(config service location forward 0)> no_fix value
(config service location forward 0)>
```

---

where *value* is one of:

- **none**: No messages are sent.
- **empty**: Send messages with empty fields.
- **last\_fix**: Send messages with information from the last valid fix.

The default is **empty**.

9. (Optional) Set the text to prepend to the forwarded message. Two variables can be included in the prepended text:

- **%s**: Includes the Connect EZ device's serial number in the prepended text.
- **%v**: Includes the vehicle ID in the prepended text.

```
(config service location forward 0)> prepend __|s|__|v|__
(config service location forward 0)>
```

---

10. (Optional) Set the vehicle ID.

Allowed value is a four digit alphanumeric string (for example, 01A3 or 1234). If no vehicle ID is configured, this setting defaults to 0000.

```
(config service location forward 0)> vehicle-id 1234
(config service location forward 0)>
```

---

11. (Optional) Provide a description of the remote host:

```
(config service location forward 0)> label "Remote host 1"
(config service location forward 0)>
```

---

12. (Optional) Specify types of messages that will be forwarded. Allowed values vary depending on the message protocol type. By default, all message types are forwarded.

- If the message protocol type is NMEA:

Allowed values are:

- **gga**: Reports time, position, and fix related data.
- **gll**: Reports position data: position fix, time of position fix, and status.
- **gsa**: Reports GPS DOP and active satellites.
- **gsv**: Reports the number of SVs in view, PRN, elevation, azimuth, and SNR.

- **rmc**: Reports position, velocity, and time.
- **vtg**: Reports direction and speed over ground.

To remove a message type:

- Use the **show** command to determine the index number of the message type to be deleted:

---

```
(config service location forward 0)> show filter_nmea
0 gga
1 gll
2 gsa
3 gsv
4 rmc
5 vtg
(config service location forward 0)>
```

---

- Use the index number to delete the message type. For example, to delete the **gsa** (index number 2) message type:

---

```
(config service location forward 0)> del filter_nmea 2
(config service location forward 0)>
```

---

To add a message type:

- Change to the **filter\_nmea** node:

---

```
(config service location forward 0)> filter_nmea
(config service location forward 0 filter_nmea)>
```

---

- Use the **add** command to add the message type. For example, to add the **gsa** message type:

---

```
(config service location forward 0 filter_nmea)> add gsa end
(config service location forward 0 filter_nmea)>
```

---

- If the message protocol type is TAIP:

Allowed values are:

- **al**: Reports altitude and vertical velocity.
- **cp**: Compact position: reports time, latitude, and longitude.
- **id**: Reports the vehicle ID.
- **ln**: Long navigation: reports the latitude, longitude, and altitude, the horizontal and vertical speed, and heading.
- **pv**: Position/velocity: reports the latitude, longitude, and heading.

To remove a message type:

- Use the **show** command to determine the index number of the message type to be deleted:

---

```
(config service location forward 0)> show filter_taip
0 al
1 cp
```

---

---

```
2 id
3 ln
4 pv
(config service location forward 0)>
```

---

- b. Use the index number to delete the message type. For example, to delete the **id** (index number 2) message type:

---

```
(config service location forward 0)> del filter_taip 2
(config service location forward 0)>
```

---

To add a message type:

- a. Change to the **filter\_taip** node:

---

```
(config service location forward 0)> filter_taip
(config service location forward 0 filter_taip)>
```

---

- b. Use the **add** command to add the message type. For example, to add the **id** message type:

---

```
(config service location forward 0 filter_taip)> add id end
(config service location forward 0 filter_taip)>
```

---

13. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

14. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure geofencing

Geofencing is a mechanism to create a virtual perimeter that allows you configure your Connect EZ device to perform actions when entering or exiting the perimeter. For example, you can configure a device to factory default if its location service indicates that it has been moved outside of the geofence.

Multiple geofences can be defined for one device, allowing for a complex configuration in which different actions are taken depending on the physical location of the device.

### Required configuration items

- Location services must be enabled.
- The geofence must be enabled.
- The boundary type of the geofence, either circular or polygonal.
  - If boundary type is circular, the latitude and longitude of the center point of the circle, and the radius.
  - If boundary type is polygonal, the latitude and longitude of the polygon's vertices (a vertex is the point at which two sides of a polygon meet). Three vertices will create a triangular polygon; four will create a square, etc. Complex polygons can be defined.
- Actions that will be taken when the device's location triggers a geofence event. You can define actions for two types of events:
  - Actions taken when the device enters the boundary of the geofence, or is inside the boundary when the device boots.
  - Actions taken when the device exits the boundary of the geofence, or is outside the boundary when the device boots.

For each event type:

- Determine if the action(s) associated with the event type should be performed when the device boots inside or outside of the geofence boundary.
- The number of update intervals that should take place before the action(s) are taken.

Multiple actions can be configured for each type of event. For each action:

- The type of action, either a factory erase or executing a custom script.
- If a custom script is used:
  - The script that will be executed.
  - Whether to log output and errors from the script.
  - The maximum memory that the script will have available.
  - Whether the script should be executed within a sandbox that will prevent the script from affecting the system itself.

### Additional configuration items

- Update interval, which determines the amount of time that the geofence should wait between polling for updated location data.



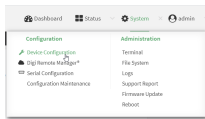
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

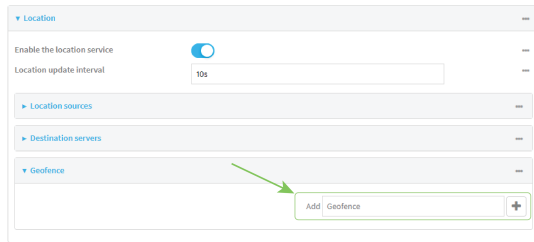
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Location > Geofence**.
4. For **Add Geofence**, type a name for the geofence and click **+**.



The geofence is enabled by default. To disable, toggle off **Enable**.

5. For **Update interval**, type the amount of time that the geofence should wait between polling for updated location data. The default is one minute.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Update interval** to ten minutes, enter **10m** or **600s**.

6. For **Boundary type**, select the type of boundary that the geofence will have.
  - If **Circular** is selected:
    - a. Click to expand **Center**.
    - b. Type the **Latitude** and **Longitude** of the center point of the circle. Allowed values are:
      - For **Latitude**, any integer between **-90** and **90**, with up to six decimal places.
      - For **Longitude**, any integer between **-180** and **180**, with up to six decimal places.

- c. For **Radius**, type the radius of the circle. Allowed values are an integer followed by **m** or **km**, for example, **100m** or **1km**.
- If **Polygonal** is selected:
  - a. Click to expand **Coordinates**.
  - b. Click **+** to add a point that represents a vertex of the polygon. A vertex is the point at which two sides of a polygon meet.
  - c. Type the **Latitude** and **Longitude** of one of the vertices of the polygon. Allowed values are:
    - For **Latitude**, any integer between **-90** and **90**, with up to six decimal places.
    - For **Longitude**, any integer between **-180** and **180**, with up to six decimal places.
  - d. Click **+** again to add an additional point, and continue adding points to create the desired polygon.

For example, to configure a square polygon around the Digi headquarters, configure a polygon with four points:

This defines a square-shaped polygon equivalent to the following:



- 7. Define actions to be taken when the device's location triggers a geofence event:
  - To define actions that will be taken when the device enters the geofence, or is inside the geofence when it boots:

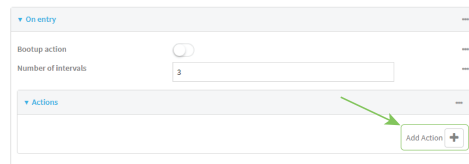
- a. Click to expand **On entry**.



- b. (Optional) Enable **Bootup action** to configure the device to perform the **On entry** actions if the device is inside the geofence when it boots.
- c. For **Number of intervals**, type or select the number of **Update Intervals** that must take place prior to performing the **On entry** actions.

For example, if the **Update interval** is **1m** (one minute) and the **Number of intervals** is **3**, the **On entry** actions will not be performed until the device has been inside the geofence for three minutes.

- d. Click to expand **Actions**.
- e. Click **+** to create a new action.



- f. For Action type, select either:
- **Factory erase** to erase the device configuration when the action is triggered.
  - **Custom script** to execute a custom script when the action is triggered.

If **Custom script** is selected:

- i. Click to expand **Custom script**.
  - ii. For **Commands**, type the script that will be executed when the action is triggered. If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.
  - iii. Enable **Log script output** to log the output of the script to the **system log**.
  - iv. Enable **Log script errors** to log errors from the script to the **system log**.
  - v. (Optional) For **Maximum memory**, type the maximum amount of system memory that will be available for the script and its spawned processes.  
Allowed values are any integer followed by one of the following:  
**b|bytes|KB|k|MB|M|GB|G|TB|T**.  
For example. the allocate one megabyte of memory to the script and its spawned processes, type **1MB** or **1M**.
  - vi. **Sandbox** is enabled by default. This prevents the script from adversely affecting the system. If you disable **Sandbox**, the script may render the system unusable.
  - vii. Repeat for any additional actions.
- To define actions that will be taken when the device exits the geofence, or is outside the geofence when it boots:

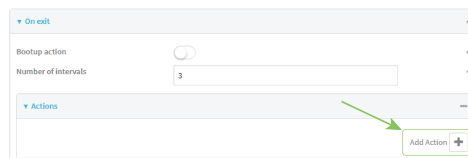
- a. Click to expand **On exit**.



- b. (Optional) Enable **Bootup action** to configure the device to perform the **On exit** actions if the device is inside the geofence when it boots.
- c. For **Number of intervals**, type or select the number of **Update Intervals** that must take place prior to performing the **On exit** actions.

For example, if the **Update interval** is **1m** (one minute) and the **Number of intervals** is **3**, the **On entry** actions will not be performed until the device has been inside the geofence for three minutes.

- d. Click to expand **Actions**.
- e. Click **+** to create a new action.



- f. For Action type, select either:
- **Factory erase** to erase the device configuration when the action is triggered.
  - **Custom script** to execute a custom script when the action is triggered.

If **Custom script** is selected:

- i. Click to expand **Custom script**.
  - ii. For **Commands**, type the script that will be executed when the action is triggered. If the script begins with **#!**, then the preceding file path will be used to invoke the script interpreter. If not, then the default shell will be used.
  - iii. Enable **Log script output** to log the output of the script to the **system log**.
  - iv. Enable **Log script errors** to log errors from the script to the **system log**.
  - v. (Optional) For **Maximum memory**, type the maximum amount of system memory that will be available for the script and its spawned processes.  
Allowed values are any integer followed by one of the following:  
**b|bytes|KB|k|MB|M|GB|G|TB|T**.  
For example. the allocate one megabyte of memory to the script and its spawned processes, type **1MB** or **1M**.
  - vi. **Sandbox** is enabled by default. This prevents the script from adversely affecting the system. If you disable **Sandbox**, the script may render the system unusable.
  - vii. Repeat for any additional actions.
8. Click **Apply** to save the configuration and apply the change.

## Command line



1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a geofence:

---

```
(config)> add service location geofence name
(config service location geofence name)>
```

---

where *name* is a name for the geofence. For example:

---

```
(config)> add service location geofence test_geofence
(config service location geofence test_geofence)>
```

---

The geofence is enabled by default. To disable:

---

```
(config service location geofence test_geofence)> enable false
(config service location geofence test_geofence)>
```

---

4. Set the amount of time that the geofence should wait between polling for updated location data:

---

```
(config service location geofence test_geofence)> update_interval value
(config service location geofence test_geofence)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **update\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config service location geofence test_geofence)> update_interval 600s
(config service location geofence test_geofence)>
```

---

The default is **1m** (one minute).

5. Set the boundary type for the geofence:

---

```
(config service location geofence test_geofence)> boundary value
(config service location geofence test_geofence)>
```

---

where *value* is either **circular** or **polygonal**.

- If **boundary** is set to **circular** :

- a. Set the latitude and longitude of the center point of the circle:

---

```
(config service location geofence test_geofence)> center
latitude int
(config service location geofence test_geofence)> center
```

---

---

```
longitude int
(config service location geofence test_geofence)>
```

---

where *int* is:

- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

- b. Set the radius of the circle:

---

```
(config service location geofence test_geofence)> radius radius
(config service location geofence test_geofence)>
```

---

where *radius* is an integer followed by **m** or **km**, for example, **100m** or **1km**.

- If **boundary** is set to **polygonal**:

- a. Set the coordinates of one vertex of the polygon. A vertex is the point at which two sides of a polygon meet.

- i. Add a vertex:

---

```
(config service location geofence test_geofence)> add
coordinates end
(config service location geofence test_geofence coordinates
0)>
```

---

- ii. Set the latitude and longitude of the vertex:

---

```
(config service location geofence test_geofence coordinates
0)> latitude int
(config service location geofence test_geofence coordinates
0)> longitude int
(config service location geofence test_geofence coordinates
0)>
```

---

where *int* is:

- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

- iii. Configure additional vertices:

---

```
(config service location geofence test_geofence coordinates
0)> ..
(config service location geofence test_geofence coordinates)>
add end
(config service location geofence test_geofence coordinates
1)> latitude int
(config service location geofence test_geofence coordinates
1)> longitude int
```

---

---

```
(config service location geofence test_geofence coordinates
1)>
```

---

where *int* is:

- For **latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **longitude**, any integer between **-180** and **180**, with up to six decimal places.

Repeat for each vortex of the polygon.

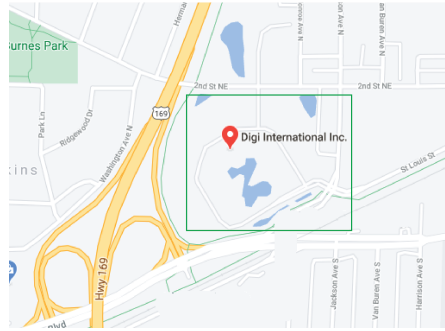
For example, to configure a square polygon around the Digi headquarters, configure a polygon with four points:

---

```
(config service location geofence test_geofence)> add
coordinates end
(config service location geofence test_geofence coordinates
0)> latitude 44.927220
(config service location geofence test_geofence coordinates
0)> longitude -93.399200
(config service location geofence test_geofence coordinates
0)> ..
(config service location geofence test_geofence coordinates)>
add end
(config service location geofence test_geofence coordinates
1)> latitude 44.927220
(config service location geofence test_geofence coordinates
1)> longitude -93.39589
(config service location geofence test_geofence coordinates
1)> ..
(config service location geofence test_geofence coordinates)>
add end
(config service location geofence test_geofence coordinates
2)> latitude 44.925161
(config service location geofence test_geofence coordinates
2)> longitude -93.39589
(config service location geofence test_geofence coordinates
2)> ..
(config service location geofence test_geofence coordinates)>
add end
(config service location geofence test_geofence coordinates
3)> latitude 44.925161
(config service location geofence test_geofence coordinates
3)> longitude -93.399200
(config service location geofence test_geofence coordinates
3)>
```

---

This defines a square-shaped polygon equivalent to the following:



6. Define actions to be taken when the device's location triggers a geofence event:
- To define actions that will be taken when the device enters the geofence, or is inside the geofence when it boots:
    - a. (Optional) Configure the device to preform the actions if the device is inside the geofence when it boots:

---

```
(config)> service location geofence test_geofence on_entry
bootup true
(config)>
```

---

- b. Set the number of [update\\_intervals](#) that must take place prior to performing the actions:

---

```
(config)> service location geofence test_geofence on_entry num_
intervals int
(config)>
```

---

For example, if the update interval is **1m** (one minute) and the **num\_intervals** is set to **3**, the actions will not be performed until the device has been inside the geofence for three minutes.

- c. Add an action:
  - i. Type ... to return to the root of the configuration:

---

```
(config service location geofence test_geofence coordinates
3)> ...
(config)>
```

---

- ii. Add the action:

---

```
(config)> add service location geofence test_geofence on_
entry action end
(config service location geofence test_geofence on_entry
action 0)>
```

---

- d. Set the type of action:

---

```
(config service location geofence test_geofence on_entry action
0)> type value
```

---

---

```
(config service location geofence test_geofence on_entry action
0)>
```

---

where *value* is either:

- **factory\_erase**—Erases the device configuration when the action is triggered.
- **script**—Executes a custom script when the action is triggered.

**factory\_erase** or **script**.

If **type** is set to **script**:

- Type or paste the script, closed in quote marks:

---

```
(config service location geofence test_geofence on_entry
action 0)> commands "script"
(config service location geofence test_geofence on_entry
action 0)>
```

---

If the script begins with **#!**, then the preceding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

- To log the output of the script to the [system log](#):

---

```
(config service location geofence test_geofence on_entry
action 0)> syslog_stdout true
(config service location geofence test_geofence on_entry
action 0)>
```

---

- To log the errors from the script to the [system log](#):

---

```
(config service location geofence test_geofence on_entry
action 0)> syslog_stderr true
(config service location geofence test_geofence on_entry
action 0)>
```

---

- (Optional) Set the maximum amount of system memory that will be available for the script and its spawned processes:

---

```
(config service location geofence test_geofence on_entry
action 0)> max_memory value
(config service location geofence test_geofence on_entry
action 0)>
```

---

where *value* is any integer followed by one of the following:

**b|bytes|KB|k|MB|M|GB|G|TB|T.**

For example, to allocate one megabyte of memory to the script and its spawned processes:

---

```
(config service location geofence test_geofence on_entry
action 0)> max_memory 1MB
(config service location geofence test_geofence on_entry
action 0)>
```

---

- v. A sandbox is enabled by default to prevent the script from adversely affecting the system. To disable the sandbox:

---

```
(config service location geofence test_geofence on_entry
action 0)> sandbox false
(config service location geofence test_geofence on_entry
action 0)>
```

---

If you disable the sandbox, the script may render the system unusable.

- vi. Repeat for any additional actions.
- To define actions that will be taken when the device exits the geofence, or is outside the geofence when it boots:
  - a. (Optional) Configure the device to preform the actions if the device is outside the geofence when it boots:

---

```
(config)> service location geofence test_geofence on_exit bootup
true
(config)>
```

---

- b. Set the number of [update\\_intervals](#) that must take place prior to performing the actions:

---

```
(config)> service location geofence test_geofence on_exit num_
intervals int
(config)>
```

---

For example, if the update interval is **1m** (one minute) and the **num\_intervals** is set to **3**, the actions will not be performed until the device has been outside the geofence for three minutes.

- c. Add an action:
  - i. Type ... to return to the root of the configuration:

---

```
(config service location geofence test_geofence coordinates
3)> ...
(config)>
```

---

- ii. Add the action:

---

```
(config)> add service location geofence test_geofence on_exit
action end
(config service location geofence test_geofence on_exit
action 0)>
```

---

- d. Set the type of action:

---

```
(config service location geofence test_geofence on_exit action
0)> type value
(config service location geofence test_geofence on_exit action
0)>
```

---

where *value* is either:

- **factory\_erase**—Erases the device configuration when the action is triggered.
- **script**—Executes a custom script when the action is triggered.

**factory\_erase** or **script**.

If **type** is set to **script**:

- Type or paste the script, closed in quote marks:

---

```
(config service location geofence test_geofence on_exit
action 0)> commands "script"
(config service location geofence test_geofence on_exit
action 0)>
```

---

If the script begins with **#!**, then the proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

- To log the output of the script to the [system log](#):

---

```
(config service location geofence test_geofence on_exit
action 0)> syslog_stdout true
(config service location geofence test_geofence on_exit
action 0)>
```

---

- To log the errors from the script to the [system log](#):

---

```
(config service location geofence test_geofence on_exit
action 0)> syslog_stderr true
(config service location geofence test_geofence on_exit
action 0)>
```

---

- (Optional) Set the maximum amount of system memory that will be available for the script and its spawned processes:

---

```
(config service location geofence test_geofence on_exit
action 0)> max_memory value
(config service location geofence test_geofence on_exit
action 0)>
```

---

where *value* is any integer followed by one of the following:

**b|bytes|KB|k|MB|M|GB|G|TB|T.**

For example, to allocate one megabyte of memory to the script and its spawned processes:

---

```
(config service location geofence test_geofence on_exit
action 0)> max_memory 1MB
(config service location geofence test_geofence on_exit
action 0)>
```

---

- A sandbox is enabled by default to prevent the script from adversely affecting the system. To disable the sandbox:

---

```
(config service location geofence test_geofence on_exit
action 0)> sandbox false
(config service location geofence test_geofence on_exit
action 0)>
```

---

If you disable the sandbox, the script may render the system unusable.

vi. Repeat for any additional actions.

7. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show location information

You can view status and statistics about location information from either the WebUI or the command line.

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.
2. Under **Services**, click **Location**.

The device's current location is displayed, along with the status of any configured geofences.

### Command line

#### Show location information

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the `show location` command at the system prompt:

---

```
> show location

Location Status
-----
State           : enabled
Source          : 192.168.2.3
Latitude        : 44* 55' 14.809" N (44.92078)
Longitude       : 93* 24' 47.262" w (-93.413128)
Altitude        : 279 meters
```

---



---

```

Velocity          : 0 meters per second
Direction        : None
Quality          : Standard GNSS (2D/3D)
UTC Date and Time : Fri, Jan 12, 2024 12:10:00 03
No. of Satellites : 7
    
```

>

---

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Show geofence information

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **show location geofence** command at the system prompt:

---

```
> show location geofence
```

| Geofence      | Status | State  | Transitions | Last Transition |
|---------------|--------|--------|-------------|-----------------|
| test_geofence | Up     | Inside | 0           |                 |

>

---

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Modbus gateway

The Connect EZ supports the ability to function as a Modbus gateway, to provide serial-to-Ethernet connectivity to Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and other industrial devices. MODBUS provides client/server communication between devices connected on different types of buses and networks, and the Modbus gateway allows for communication between buses and networks that use the Modbus protocol.

This section contains the following topics:

|                                                 |     |
|-------------------------------------------------|-----|
| Configure the Modbus gateway .....              | 410 |
| Show Modbus gateway status and statistics ..... | 423 |

## Configure the Modbus gateway

### Required configuration items

- Server configuration:
  - Enable the server.
  - Connection type, either socket or serial.
    - If the connection type is socket, the IP protocol to be used.
    - If the connection type is serial, the serial port to be used.
- Client configuration:
  - Enable the client.
  - Connection type, either socket or serial.
    - If the connection type is socket:
      - The IP protocol to be used.
      - The hostname or IPv4 address of the remote host on which the Modbus server is running.
    - If the connection type is serial:
      - The serial port to be used.
  - Modbus address or addresses to determine if messages should be forwarded to a destination device.

### Additional configuration items

- Server configuration:
  - The packet mode.
  - The maximum time between bytes in a packet.
  - If the connection type is set to socket:
    - The port to use.
    - The inactivity timeout.
    - Access control list.
  - If the connection type is set to serial:
    - Whether to use half duplex (two wire) mode.
- Client configuration:
  - The packet mode.
  - The maximum time between bytes in a packets.
  - Whether to send broadcast messages.
  - Response timeout
  - If connection type is set to socket:
    - The port to use.
    - The inactivity timeout.
  - If connection type is set to serial:
    - Whether to use half duplex (two wire) mode.

- Whether packets should be delivered to a fixed Modbus address.
- Whether packets should have their Modbus address adjusted downward before to delivery.

## Web

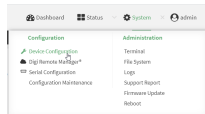
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

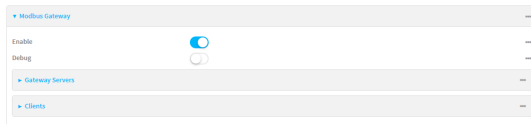
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

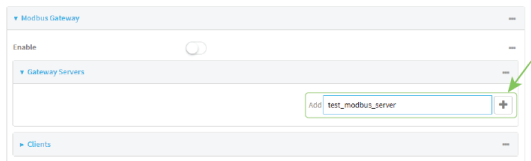
3. Click **Services > Modbus Gateway**.



4. Click **Enable** to enable the gateway.
5. Click **Debug** to allow verbose logging in the system log.

### Configure gateway servers

1. Click to expand **Gateway Servers**.
2. For **Add Modbus server**, type a name for the server and click **+**.



The new Modbus gateway server configuration is displayed.

test\_modbus\_server

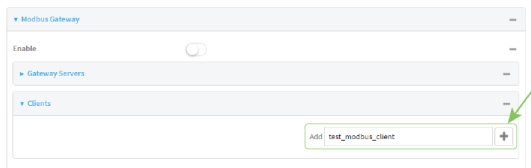
- Enable the server:
- Connection type: Socket
- IP Protocol: TCP
- Port: 502
- Packet mode: RTU
- Packet idle gap: 200ms
- Inactivity timeout: 60s
- Access control list: [+](#)

3. The new Modbus gateway server is enabled by default. Toggle off **Enable the server** to disable.
4. For **Connection type**, select **Socket** or **Serial**. Available options in the gateway server configuration vary depending on this setting.
  - If **Socket** is selected for **Connection type**:
    - a. For **IP Protocol**, select **TCP** or **UDP**. The default is **TCP**.
    - b. For **Port**, enter or select an appropriate port. The default is port **502**.
  - If **Serial** is selected for **Connection type**:
    - a. For **Serial port**, select the appropriate serial port on the Connect EZ device.
5. For **Packet mode**, select **RTU** or **RAW** (if **Connection type** is set to **Socket**) or **ASCII** (if **Connection type** is set to **Serial**) for the type of packet that will be used by this connection. The default is **RTU**.
6. For **Packet idle gap**, type the maximum allowable time between bytes in a packet. Allowed values are between 10 milliseconds and one second, and take the format **number {m|s}**.  
For example, to set **Packet idle gap** to 20 milliseconds, enter **20ms**.
7. If **Connection type** is set to **Socket**, for **Inactivity timeout**, type the amount of time to wait before disconnecting the socket when it has become inactive. Allowed values are any number of minutes or seconds up to a maximum of 15 minutes, and take the format **number{m|s}**.  
For example, to set **Inactivity timeout** to ten minutes, enter **10m** or **600s**.
8. (Optional) If **Connection type** is set to **Serial**, click **Half duplex** to enable half duplex (two wire) mode.
9. (Optional) If **Connection type** is set to **Socket**, click to expand **Access control list**:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the web administration service.
    - d. Click **+** again to list additional IP addresses or networks.

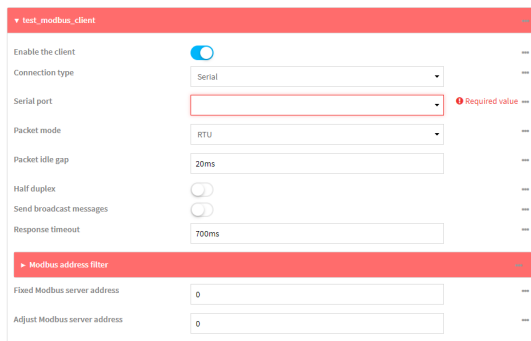
- a. Click **IPv6 Addresses**.
      - b. For **Add Address**, click **+**.
      - c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
        - A single IP address or host name.
        - A network designation in CIDR notation, for example, 2001:db8::/48.
        - **any**: No limit to IPv6 addresses that can access the web administration service.
      - d. Click **+** again to list additional IP addresses or networks.
    - a. Click **Interfaces**.
      - b. For **Add Interface**, click **+**.
      - c. For **Interface**, select the appropriate interface from the dropdown.
      - d. Click **+** again to allow access through additional interfaces.
    - a. Click **Zones**.
      - b. For **Add Zone**, click **+**.
      - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
      - d. Click **+** again to allow access through additional firewall zones.
10. Repeat these steps to configure additional servers.

## Configure clients

1. Click to expand **Clients**.
2. For **Add Modbus client**, type a name for the client and click **+**.



The new Modbus gateway client configuration is displayed.



3. The new Modbus gateway client is enabled by default. Toggle off **Enable the client** to disable.
4. For **Connection type**, select **Socket** or **Serial**. Available options in the gateway server configuration vary depending on this setting.
  - If **Socket** is selected for **Connection type**:
    - a. For **IP Protocol**, select **TCP** or **UDP**. The default is **TCP**.
    - b. For **Port**, enter or select an appropriate port. The default is port **502**.
    - c. For **Remote host**, type the hostname or IP address of the remote host on which the Modbus server is running.
  - If **Serial** is selected for **Connection type**:
    - a. For **Serial port**, select the appropriate serial port on the Connect EZ device.
5. For **Packet mode**, select **RTU** or **RAW** (if **Connection type** is set to **Socket**) or **ASCII** (if **Connection type** is set to **Serial**) for the type of packet that will be used by this connection. The default is **RTU**.
6. For **Packet idle gap**, type the maximum allowable time between bytes in a packet. Allowed values are between 10 milliseconds and one second, and take the format **number {m|s}**.

For example, to set **Packet idle gap** to 20 milliseconds, enter **20ms**.
7. If **Connection type** is set to **Socket**, for **Inactivity timeout**, type the amount of time to wait before disconnecting the socket when it has become inactive. Allowed values are any number of minutes or seconds up to a maximum of 15 minutes, and take the format **number{m|s}**.

For example, to set **Inactivity timeout** to ten minutes, enter **10m** or **600s**.
8. (Optional) If **Connection type** is set to **Serial**, click **Half duplex** to enable half duplex (two wire) mode.
9. (Optional) If **Connection type** is set to **Socket**, click to expand **Access control list**:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the web administration service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's web administration service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.

- **any**: No limit to IPv6 addresses that can access the web administration service.
- d. Click **+** again to list additional IP addresses or networks.
    - To limit access to hosts connected through a specified interface on the device:
      - a. Click **Interfaces**.
      - b. For **Add Interface**, click **+**.
      - c. For **Interface**, select the appropriate interface from the dropdown.
      - d. Click **+** again to allow access through additional interfaces.
    - To limit access based on firewall zones:
      - a. Click **Zones**.
      - b. For **Add Zone**, click **+**.
      - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
      - d. Click **+** again to allow access through additional firewall zones.
  10. (Optional) Enable **Send broadcast messages** to configure the gateway to send broadcast messages to this client.
  11. For **Response timeout**, type the maximum time to wait for a response to a message. Allowed values are between 1 millisecond and 700 milliseconds, and take the format **numbers**.  
For example, to set **Response timeout** to 100 milliseconds, enter **100ms**. The default is **700ms**.
  12. Click to expand **Modbus address filter**.  
This filter is used by the gateway to determine if a message should be forwarded to a destination device. If the Modbus address in the message matches one or more of the filters, the message is forwarded. If it does not match the filters, the message is not forwarded.
  13. For **Address or address range**, type a Modbus address or range of addresses. Allowed values are 1 through 255 or a hyphen-separated range.  
For example, to have this client filter for incoming messages that contain the Modbus address of 10, type **10**. To filter for all messages with addresses in the range of 20 to 30, type **20-30**.  
To add additional address filters for this client, click **+**.

The screenshot shows a configuration window for 'Modbus address filter'. It contains two text input fields. The first field has the value '10' and the second field has the value '20-30'. Below these fields is a button with a plus sign icon and the text 'Add Address or address range'. A green arrow points to this button.

14. For **Fixed Modbus server address**, if request messages handled by this client should always be forwarded to a specific device, type the device's Modbus address. Leave at the default setting of **0** to allow messages that match the **Modbus address filter** to be forwarded to devices based on the Modbus address in the message.
15. For **Adjust Modbus server address**, type a value to adjust the Modbus server address downward by the specified value prior to delivering the message. Allowed values are **0** through **255**. Leave at the default setting of **0** to not adjust the server address.  
If a packet contains a Modbus server address above the amount entered here, the address will be adjusted downward by this amount before the packet is delivered. This allows you to

configure clients on the gateway that will forward messages to remote devices with the same Modbus address on different buses. For example, if there are two devices on two different buses that have the same Modbus address of 10, you can create two clients on the gateway:

- Client one:

- **Modbus address filter** set to **10**.

This will configure the gateway to deliver all messages that have the Modbus server address of 10 to this device.

- Client two:

- **Modbus address filter** set to **20**.
- **Adjust Modbus server address** set to **10**.

This will configure the gateway to deliver all messages that have the Modbus server address address of 20 to the device with address 10.

16. Repeat these steps to configure additional clients.
17. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable the Modbus gateway:

---

```
(config)> service modbus_gateway enable true
(config)>
```

---

4. Configure servers:
  - a. Add a server:

---

```
(config)> add service modbus_gateway server name
(config service modbus_gateway server name)>
```

---

where *name* is a name for the server, for example:

---

```
(config)> add service modbus_gateway server test_modbus_server
(config service modbus_gateway server test_modbus_server)>
```

---

The Modbus server is enabled by default. To disable:

---

```
(config service modbus_gateway server test_modbus_server)> enable
false
(config service modbus_gateway server test_modbus_server)>
```

---



- b. Set the connection type:

```
(config service modbus_gateway server test_modbus_server)> connection_
type type
(config service modbus_gateway server test_modbus_server)>
```

where *type* is either **socket** or **serial**. The default is **socket**.

- If **connection\_type** is set to **socket**:

- i. Set the IP protocol:

```
(config service modbus_gateway server test_modbus_server)>
socket protocol value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is either **tcp** or **udp**.

- ii. Set the port:

```
(config service modbus_gateway server test_modbus_server)>
socket port
(config service modbus_gateway server test_modbus_server)>
```

where *port* is an integer between **1** and **65535**. The default is **502**.

- iii. Set the packet mode:

```
(config service modbus_gateway server test_modbus_server)>
socket packet_mode value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is either **rtu** or **raw**. The default is **rtu**.

- iv. Set the maximum allowable time between bytes in a packet:

```
(config service modbus_gateway server test_modbus_server)>
socket idle_gap value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is any number between 10 milliseconds and one second, and take the format **number{ms|s}**.

For example, to set *idle\_gap* to 20 milliseconds, enter **20ms**.

- v. Set the amount of time to wait before disconnecting the socket when it has become inactive:

```
(config service modbus_gateway server test_modbus_server)>
inactivity_timeout value
(config service modbus_gateway server test_modbus_server)>
```

where *value* is any number of minutes or seconds up to a maximum of 15 minutes, and takes the format **number{m|s}**.

For example, to set **inactivity\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config service modbus_gateway server test_modbus_server)>
inactivity_timeout 600s
(config service modbus_gateway server test_modbus_server)>
```

---

- If **connection\_type** is set to **serial**:

- i. Set the serial port:

- i. Use the ? to determine available serial ports:

---

```
(config service modbus_gateway server test_modbus_
server)> ... serial port ?
```

```
Serial
```

```
Additional Configuration
```

```
-----
```

```
port1                Port 1
```

---

```
(config service modbus_gateway server test_modbus_
server)>
```

---

- ii. Set the port:

---

```
(config service modbus_gateway server test_modbus_
server)> serial port
(config service modbus_gateway server test_modbus_
server)>
```

---

- ii. Set the packet mode:

---

```
(config service modbus_gateway server test_modbus_server)>
serial packet_mode value
(config service modbus_gateway server test_modbus_server)>
```

---

where *value* is either **rtu** or **ascii**. The default is **rtu**.

- iii. Set the maximum allowable time between bytes in a packet:

---

```
(config service modbus_gateway server test_modbus_server)>
serial idle_gap value
(config service modbus_gateway server test_modbus_server)>
```

---

where *value* is any number between 10 milliseconds and one second, and take the format **number{ms|s}**.

For example, to set `idle_gap` to one second, enter **1000ms** or **1s**.

- iv. (Optional) Enable half-duplex (two wire) mode:

---

```
(config service modbus_gateway server test_modbus_server)>
serial half_duplex true
(config service modbus_gateway server test_modbus_server)>
```

---

- c. Repeat the above instructions for additional servers.

## 5. Configure clients:

- a. Type ... to return to the root of the configuration:

```
(config)> add service modbus_gateway server test_modbus_server)> ...
(config)>
```

- b. Add a client:

```
(config)> add service modbus_gateway client name
(config service modbus_gateway client name)>
```

where *name* is a name for the client, for example:

```
(config)> add service modbus_gateway client test_modbus_client
(config service modbus_gateway client test_modbus_client)>
```

The Modbus client is enabled by default. To disable:

```
(config service modbus_gateway client test_modbus_client)> enable
false
(config service modbus_gateway client test_modbus_client)>
```

- c. Set the connection type:

```
(config service modbus_gateway client test_modbus_client)> connection_
type type
(config service modbus_gateway client test_modbus_client)>
```

where *type* is either **socket** or **serial**. The default is **socket**.

- If **connection\_type** is set to **socket**:

- i. Set the IP protocol:

```
(config service modbus_gateway client test_modbus_client)>
socket protocol value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is either **tcp** or **udp**.

- ii. Set the port:

```
(config service modbus_gateway client test_modbus_client)>
socket port
(config service modbus_gateway client test_modbus_client)>
```

where *port* is an integer between **1** and **65535**. The default is **502**.

- iii. Set the packet mode:

```
(config service modbus_gateway client test_modbus_client)>
socket packet_mode value
(config service modbus_gateway client test_modbus_client)>
```

where *value* is either **rtu** or **ascii**. The default is **rtu**.

- iv. Set the maximum allowable time between bytes in a packet:

---

```
(config service modbus_gateway client test_modbus_client)>
socket idle_gap value
(config service modbus_gateway client test_modbus_client)>
```

---

where *value* is any number between 10 milliseconds and one second, and take the format **number{m|s}**.

For example, to set `idle_gap` to 20 milliseconds, enter **20ms**.

- v. Set the amount of time to wait before disconnecting the socket when it has become inactive:

---

```
(config service modbus_gateway client test_modbus_client)>
inactivity_timeout value
(config service modbus_gateway client test_modbus_client)>
```

---

where *value* is any number of minutes or seconds up to a maximum of 15 minutes, and takes the format **number{m|s}**.

For example, to set `inactivity_timeout` to ten minutes, enter either **10m** or **600s**:

---

```
(config service modbus_gateway client test_modbus_client)>
inactivity_timeout 600s
(config service modbus_gateway client test_modbus_client)>
```

---

- vi. Set the hostname or IP address of the remote host on which the Modbus server is running:

---

```
(config service modbus_gateway client test_modbus_client)>
remote_host ip_address|hostname
(config service modbus_gateway client test_modbus_client)>
```

---

- If `connection_type` is set to **serial**:

- i. Set the serial port:

- i. Use the `?` to determine available serial ports:

---

```
(config service modbus_gateway client test_modbus_
client)> ... serial port ?
```

Serial

Additional Configuration

-----

port1

Port 1

```
(config service modbus_gateway client test_modbus_
client)>
```

---

## ii. Set the port:

---

```
(config service modbus_gateway client test_modbus_
client)> serial port
(config service modbus_gateway client test_modbus_
client)>
```

---

## ii. Set the packet mode:

---

```
(config service modbus_gateway client test_modbus_client)>
serial packet_mode value
(config service modbus_gateway client test_modbus_client)>
```

---

where *value* is either **rtu** or **ascii**. The default is **rtu**.

## iii. Set the maximum allowable time between bytes in a packet:

---

```
(config service modbus_gateway client test_modbus_client)>
serial idle_gap value
(config service modbus_gateway client test_modbus_client)>
```

---

where *value* is any number between 10 milliseconds and one second, and take the format **number{ms|s}**.

For example, to set `idle_gap` to one second, enter **1000ms** or **1s**.

## iv. (Optional) Enable half-duplex (two wire) mode:

---

```
(config service modbus_gateway client test_modbus_client)>
serial half_duplex true
(config service modbus_gateway client test_modbus_client)>
```

---

## d. (Optional) Enable the gateway to send broadcast messages to this client:

---

```
(config service modbus_gateway client test_modbus_client)> broadcast
true
(config service modbus_gateway client test_modbus_client)>
```

---

## e. Set the maximum time to wait for a response to a message:

---

```
(config service modbus_gateway client test_modbus_client)> response_
timeout value
(config service modbus_gateway client test_modbus_client)>
```

---

Allowed values are between 1 millisecond and 700 milliseconds, and take the format **numbersms**.

For example, to set `response_timeout` to 100 milliseconds:

---

```
(config service modbus_gateway client test_modbus_client)> response_
timeout 100ms
(config service modbus_gateway client test_modbus_client)>
```

---

The default is **700ms**.

## f. Configure the address filter:

This filter is used by the gateway to determine if a message should be forwarded to a destination device. If the Modbus address in the message matches one or more of the filters, the message is forwarded. If it does not match the filters, the message is not forwarded. Allowed values are **1** through **255** or a hyphen-separated range.

For example:

- To have this client filter for incoming messages that contain the Modbus address of 10, set the index **0** entry to **10**:

---

```
(config service modbus_gateway client test_modbus_client)>
filter 0 10
(config service modbus_gateway client test_modbus_client)>
```

---

- To filter for all messages with addresses in the range of 20 to 30, set the index **0** entry to **20-30**:

---

```
(config service modbus_gateway client test_modbus_client)>
filter 0 20-30
(config service modbus_gateway client test_modbus_client)>
```

---

To add additional filters, increment the index number. For example, to add an additional filter for addresses in the range of 50-100:

---

```
(config service modbus_gateway client test_modbus_client)> filter 1
50-100
(config service modbus_gateway client test_modbus_client)>
```

---

g. If request messages handled by this client should always be forwarded to a specific device, use **fixed\_server\_address** to set the device's Modbus address:

---

```
(config service modbus_gateway client test_modbus_client)> fixed_
server_address value
(config service modbus_gateway client test_modbus_client)>
```

---

Leave at the default setting of **0** to allow messages that match the Modbus address filter to be forwarded to devices based on the Modbus address in the message.

h. To adjust the Modbus server address downward by the specified value prior to delivering the message, use **adjust\_server\_address**:

---

```
(config service modbus_gateway client test_modbus_client)> adjust_
server_address value
(config service modbus_gateway client test_modbus_client)>
```

---

where *value* is an integer from **0** to **255**. Leave at the default setting of **0** to not adjust the server address.

If a packet contains a Modbus server address above the amount entered here, the address will be adjusted downward by this amount before the packet is delivered. This allows you to configure clients on the gateway that will forward messages to remote devices with the same Modbus address on different buses. For example, if there are two devices on two

different buses that have the same Modbus address of 10, you can create two clients on the gateway:

- Client one:

- **filter** set to **10**.

This will configure the gateway to deliver all messages that have the Modbus server address of 10 to this device.

- Client two:

- **filter** set to **20**.
- **adjust\_server\_address** set to **10**.

This will configure the gateway to deliver all messages that have the Modbus server address address of 20 to the device with address 10.

i. Repeat the above instructions for additional clients.

6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show Modbus gateway status and statistics

You can view status and statistics about location information from either the WebUI or the command line.


### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, select **Status > Modbus Gateway**.

The **Modbus Gateway** page appears.

Statistics related to the Modbus gateway server are displayed. If the message **Server connections not available** is displayed, this indicates that there are no connected clients.

- To view information about Modbus gateway clients, click **Clients**.
- To view statistics that are common to both the clients and server, click **Common Statistics**.
- To view configuration details about the gateway, click the  (configuration) icon in the upper right of the gateway's status pane.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the `show modbus-gateway` command at the system prompt:

---

```
> show modbus-gateway

Server Connection  IP Address  Port  Uptime
-----
modbus_socket     10.45.1.139 49570  6
modbus_socket     10.45.1.139 49568  13

Client            Uptime
-----
modbus_socket_41  0
modbus_socket_21  0
modbus_serial_client 428

>
```

---

If the message **Server connections not available** is displayed, this indicates that there are no connected clients.

3. Use the `show modbus-gateway verbose` command at the system prompt to display more information:

---

```
> show modbus-gateway verbose

Client            Uptime
-----
modbus_socket_41  0
modbus_socket_21  0
modbus_serial_client 506

Common Statistics
-----
Configuration Updates           : 1
Client Configuration Failure    : 0
Server Configuration Failure    : 0
Configuration Load Failure     : 0
Incoming Connections            : 4
Internal Error                   : 0
Resource Shortages               : 0

Servers
-----

modbus_socket
-----
Client Lookup Errors            : 0
Incoming Connections            : 4
Packet Errors                   : 0
RX Broadcasts                   : 0
RX Requests                     : 12
TX Exceptions                    : 0
```

---



---

```
TX Responses           : 12
```

```
Clients
```

```
-----
```

```
modbus_socket_41
```

```
-----
```

```
Address Translation Errors : 0
Connection Errors         : 0
Packet Errors             : 0
RX Responses              : 4
RX Timeouts               : 0
TX Broadcasts             : 0
TX Requests               : 4
```

```
modbus_socket_21
```

```
-----
```

```
Address Translation Errors : 0
Connection Errors         : 0
Packet Errors             : 0
RX Responses              : 4
RX Timeouts               : 0
TX Broadcasts             : 0
TX Requests               : 4
```

```
modbus_serial_client
```

```
-----
```

```
Address Translation Errors : 0
Connection Errors         : 0
Packet Errors             : 0
RX Responses              : 4
RX Timeouts               : 0
TX Broadcasts             : 0
TX Requests               : 4
```

```
>
```

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## System time

By default, the Connect EZ device synchronizes the system time by periodically connecting to the Digi NTP server, [time.devicecloud.com](http://time.devicecloud.com). In this mode, the device queries the time server based on following events and schedule:

- At boot time.
- Once a day.

The default configuration has the system time zone set to UTC. No additional configuration is required for the system time if the default configuration is sufficient. However, you can change the default time zone and the default NTP server, as well as configuring additional NTP servers. If multiple servers are configured, a number of time samples are obtained from each of the servers and a subset of the NTP clock filter and selection algorithms are applied to select the best of these. See [Configure the system time](#) for details about changing the default configuration.

The Connect EZ device can also be configured to serve as an NTP server, providing NTP services to downstream devices. See [Network Time Protocol](#) for more information about NTP server support.

You can also set the local date and time manually, if there is no access to NTP servers. See [Manually set the system date and time](#) for information

### Configure the system time

This procedure is optional.

The Connect EZ device's default system time configuration uses the Digi NTP server, [time.devicecloud.com](http://time.devicecloud.com), and has the time zone set to **UTC**. You can change the default NTP server and the default time zone. You can also set the local date and time without using an upstream NTP server, as well as configuring additional NTP servers.

#### Required Configuration Items

- The time zone for the Connect EZ device.
- If t least one upstream NTP server for synchronization.

#### Additional Configuration Options

- Additional upstream NTP servers.

#### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

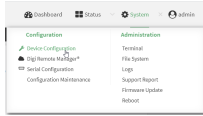
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.

- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System > Time**
4. (Optional) For **Timezone**, select either **UTC** or select the location nearest to your current location to set the timezone for your Connect EZ device. The default is **UTC**.
5. (Optional) Add upstream NTP servers that the device will use to synchronize its time. The default setting is **time.devicecloud.com**.
  - To change the default value of the NTP server:
    - a. Click **NTP servers**.
    - b. For **Server**, type a new server name.
  - To add an NTP server:
    - a. Click **NTP servers**.
    - b. For **Add Server**, click **+**.
    - c. For **Server**, enter the hostname of the upstream NTP server that the device will use to synchronize its time.
    - d. Click **+** to add additional NTP servers. If multiple servers are included, servers are tried in the order listed until one succeeds.

---

**Note** This list is synchronized with the list of servers included with NTP server configuration, and changes made to one will be reflected in the other. See [Configure the device as an NTP server](#) for more information about NTP server configuration.

---

6. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. (Optional) Set the timezone for the location of your Connect EZ device. The default is **UTC**.

---

```
(config)> system time timezone value
(config)>
```

---

Where *value* is the timezone using the format specified with the following command:

---

```
(config)> system time timezone ?
```

Timezone: The timezone for the location of this device. This is used to adjust the time for log messages. It also affects actions that occur at a specific time of day.

Format:

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
```

---

```
(config)>
```

---

4. (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.

- To delete the default NTP server, **time.devicecloud.com**:

---

```
(config)> del service ntp server 0
(config)>
```

---

- To add the NTP server to the beginning of the list, use the index value of **0** to indicate that it should be added as the first server:

---

```
(config)> add service ntp server 0 time.server.com
(config)>
```

---

- To add the NTP server to the end of the list, use the index keyword **end**:

---

```
(config)> add service ntp server end time.server.com
(config)>
```

---

- To add the NTP server in another location in the list, use an index value to indicate the appropriate position. For example:

---

```
(config)> add service ntp server 1 time.server.com
(config)>
```

---

**Note** This list is synchronized with the list of servers included with NTP server configuration, and changes made to one will be reflected in the other. See [Configure the device as an NTP server](#) for more information about NTP server configuration.

---

5. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

6. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Test the connection to the NTP servers

The following procedure tests the configured NTP servers for connectivity. This test does not affect the device's current local date and time.

#### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Test the configured NTP servers for connectivity:

---

```
> system time test
Testing NTP server time.devicecloud.com on UDP port 123...
server 52.2.40.158, stratum 2, offset -0.000216, delay 0.05800
server 35.164.164.69, stratum 2, offset -0.000991, delay 0.07188
24 Aug 22:01:20 ntpdate[28496]: adjust time server 52.2.40.158 offset -
0.000216 sec
NTP test sync successful

Testing NTP server time.accns.com on UDP port 123...
server 128.136.167.120, stratum 3, offset -0.001671, delay 0.08455
24 Aug 22:01:20 ntpdate[28497]: adjust time server 128.136.167.120 offset -
-0.001671 sec
NTP test sync successful
>
```

---

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Manually synchronize with the NTP server

The following procedure perform a NTP query to the configured servers and set the local time to the first server that responds.

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Synchronize the device's local date and time:

---

```
> system time synch
24 Aug 22:03:55 ntpdate[2520]: step time server 52.2.40.158 offset -
```

---

---

```
0.000487 sec
NTP sync to time.devicecloud.com successful
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Manually set the system date and time

If your network restricts access to NTP servers, use this procedure to set the local date and time. This procedure is available at the Admin CLI only.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Set the device's local date and time:

---

```
> system time set value
>
```

---

where *value* is the The date in year-month-day hour:minute:second format. For example:

---

```
> system time set 2024-01-12 12:10:00
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Network Time Protocol

Network Time Protocol (NTP) enables devices connected on local and worldwide networks to synchronize their internal software and hardware clocks to the same time source. The Connect EZ device can be configured as an NTP server, allowing downstream hosts that are attached to the device's Local Area Networks to synchronize with the device.

When the device is configured as an NTP server, it also functions as an NTP client. The NTP client will be consistently synchronized with one or more upstream NTP servers, which means that NTP packets are transferred every few seconds. A minimum of one upstream NTP server is required. Additional NTP servers can be configured. If multiple servers are configured, a number of time samples are obtained from each of the servers and a subset of the NTP clock filter and selection algorithms are applied to select the best of these.

See [Configure the device as an NTP server](#) for information about configuring your device as an NTP server.

## Configure the device as an NTP server

### Required Configuration Items

- Enable the NTP service.
- At least one upstream NTP server for synchronization. The default setting is the Digi NTP server, time.devicecloud.com.

### Additional Configuration Options

- Additional upstream NTP servers.
- Access control list to limit downstream access to the Connect EZ device's NTP service.
- The time zone setting, if the default setting of UTC is not appropriate.

To configure the Connect EZ device's NTP service:

### ≡ Web

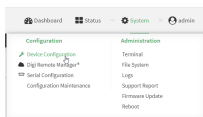
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > NTP**.
4. Enable the Connect EZ device's NTP service by clicking **Enable**.
5. (Optional) Configure the access control list to limit downstream access to the Connect EZ device's NTP service.
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's NTP service. Allowed values are:

- A single IP address or host name.
  - A network designation in CIDR notation, for example, 192.168.1.0/24.
  - **any**: No limit to IPv4 addresses that can access the NTP service.
- d. Click **+** again to list additional IP addresses or networks.
- To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's NTP service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the NTP service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.

---

**Note** By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the Connect EZ device can use the NTP service.

---

6. Enable **Fall back to local clock** to allow the device's local system clock to be used as backup time source.
7. (Optional) Add upstream NTP servers that the device will use to synchronize its time. The default setting is **time.devicecloud.com**.
  - To change the default value of the NTP server:
    - a. Click **NTP servers**.
    - b. For **Server**, type a new server name.
  - To add an NTP server:
    - a. Click **NTP servers**.
    - b. For **Add Server**, click **+**.
    - c. For **Server**, enter the hostname of the upstream NTP server that the device will use to synchronize its time.
    - d. Click **+** to add additional NTP servers. If multiple servers are included, servers are tried in the order listed until one succeeds.



---

**Note** This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See [Configure the system time](#) for more information about NTP client configuration.

---

8. (Optional) Configure the system time zone. The default is **UTC**.
  - a. Click **System > Time**
  - b. Select the **Timezone** for the location of your Connect EZ device.
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

---

3. Enable the ntp service:

```
(config)> service ntp enable true
(config)>
```

---

4. (Optional) Add an upstream NTP server that the device will use to synchronize its time to the appropriate location in the list of NTP servers. The default setting is **time.devicecloud.com**.
  - To delete the default NTP server, **time.devicecloud.com**:

```
(config)> del service ntp server 0
(config)>
```

---

- To add the NTP server to the beginning of the list, use the index value of **0** to indicate that it should be added as the first server:

```
(config)> add service ntp server 0 time.server.com
(config)>
```

---

- To add the NTP server to the end of the list, use the index keyword **end**:

```
(config)> add service ntp server end time.server.com
(config)>
```

---

- To add the NTP server in another location in the list, use an index value to indicate the appropriate position. For example:

```
(config)> add service ntp server 1 time.server.com
(config)>
```

---

---

**Note** This list is synchronized with the list of servers included with NTP client configuration, and changes made to one will be reflected in the other. See [Configure the system time](#) for more information about NTP client configuration.

---

5. Allow the device's local system clock to be used as backup time source:

```
(config)> service ntp local true
(config)>
```

---

6. (Optional) Configure the access control list to limit downstream access to the Connect EZ device's NTP service.

- To limit access to specified IPv4 addresses and networks:

```
(config)> add service ntp acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the NTP server agent.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service ntp acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the NTP server agent.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

```
(config)> add service ntp acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

```
(config)> add service ntp acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:  
Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

```
Zones: A list of groups of network interfaces that can be
referred to by packet
filtering rules and access control lists.
```

```
Additional Configuration
```

```
-----
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

---

**Note** By default, the access control list for the NTP service is empty, which means that all downstream hosts connected to the Connect EZ device can use the NTP service.

---

7. (Optional) Set the timezone for the location of your Connect EZ device. The default is **UTC**.

---

```
(config)> system time timezone value
(config)>
```

---

Where *value* is the timezone using the format specified with the following command:

---

```
(config)> system time timezone ?
```

```
Timezone: The timezone for the location of this device. This is used to
adjust the time for log
messages. It also affects actions that occur at a specific time of day.
```

```
Format:
```

```
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
...
```

```
(config)>
```

---

- Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show status and statistics of the NTP server

You can display status and statistics for active NTP servers

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

- On the main menu, click **Status**.
- Under **Services**, click **NTP**.

The NTP server status page is displayed.

### Command line

#### Show NTP information

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- Use the `show ntp` command at the system prompt:

---

```
> show ntp

NTP Status Status
-----
Status      : Up
Sync Status : Up

Remote      Refid      ST  T  When  Poll  Reach  Delay
Offset  Jitter
-----  -----  --  -  ----  ----  ----  -----
-  -----
*ec2-52-2-40-158  129.6.15.32  2  u  191  1024  377  33.570
+1.561  0.991
128.136.167.120  128.227.205.3  3  u  153  1024  1  43.583 -
1.895  0.382

>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure a multicast route

Multicast routing allows a device to transmit data to a single multicast address, which is then distributed to a group of devices that are configured to be members of that group.

To configure a multicast route:

### ≡ Web

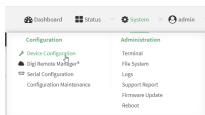
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Multicast**.
4. For **Add Multicast route**, type a name for the route and click **+**.
5. The new route is enabled by default. To disable, toggle off **Enable**.
6. Type the **Source address** for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.
7. Select a **Source interface** where multicast packets will arrive.
8. To add one or more destination interface that the Connect EZ device will send multicast packets to:
  - a. Click to expand **Destination interfaces**.
  - b. Click **+**.
  - c. For **Destination interface**, select the interface.
  - d. Repeat for additional destination interfaces.
9. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the multicast route. For example, to add a route named **test**:

```
(config)> add service multicast test
(config service multicast test)>
```

4. The multicast route is enabled by default. If it has been disabled, enable the route:

```
(config service multicast test)> enable true
(config service multicast test)>
```

5. Set the source address for the route. This must be a multicast IP address between 224.0.0.1 and 239.255.255.255.

```
(config service multicast test)> dst ip-address
(config service multicast test)>
```

6. Set the source interface for the route where multicast packets will arrive:

- a. Use the **?** to determine available interfaces:
- b. Set the interface. For example:

```
(config service multicast test)> src_interface /network/interface/eth1
(config service multicast test)>
```

7. Set a destination interface that the Connect EZ device will send multicast packets to:

- a. Use the **?** to determine available interfaces:
- b. Set the interface. For example:

```
(config service multicast test)> add interface end
/network/interface/eth1
(config service multicast test)>
```

- c. Repeat for each additional destination interface.

8. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Enable service discovery (mDNS)

Multicast DNS mDNS is a protocol that resolves host names in small networks that do not have a DNS server. You can enable the Connect EZ device to use mDNS.

---

**Note** This feature is enabled by default.

---

### ≡ Web

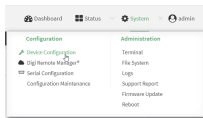
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Service Discovery (mDNS)**.
4. The mDNS service is enabled by default. To disable, click to toggle off **Enable**.
5. Click **Access control list** to configure access control:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's mDNS service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the mDNS service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.



- c. For **Address**, enter the IPv6 address or network that can access the device's mDNS service. Allowed values are:
    - A single IP address or host name.
    - A network designation in CIDR notation, for example, 2001:db8::/48.
    - **any**: No limit to IPv6 addresses that can access the mDNS service.
  - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
6. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The mDNS service is enabled by default. To disable:

---

```
(config)> service mdns enable false
(config)>
```

---

4. Configure access control:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service mdns acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service mdns acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the mDNS service.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service mdns acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service mdns acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

---

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

---

---

```
(config)>
```

---

Repeat this step to include additional firewall zones.

5. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Use the iPerf service

Your Connect EZ device includes an iPerf3 server that you can use to test the performance of your network.

iPerf3 is a command-line tool that measures the maximum network throughput an interface can handle. This is useful when diagnosing network speed issues.

The Connect EZ implementation of iPerf3 supports testing with both TCP and UDP.

---

**Note** Using iPerf clients that are at a version earlier than iPerf3 to connect to the Connect EZ device's iPerf3 server may result in unpredictable results. As a result, Digi recommends using an iPerf client at version 3 or newer to connect to the Connect EZ device's iPerf3 server.

---

### Required configuration items

- Enable the iPerf server on the Connect EZ device.
- An iPerf3 client installed on a remote host. iPerf3 software can be downloaded at <https://iperf.fr/iperf-download.php>.

### Additional configuration Items

- The port that the Connect EZ device's iPerf server will use to listen for incoming connections.
- The access control list for the iPerf server.

When the iPerf server is enabled, the Connect EZ device will automatically configure its firewall rules to allow incoming connections on the configured listening port. You can restrict access by configuring the access control list for the iPerf server.

To enable the iPerf3 server:

### Web

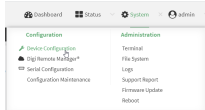
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

## Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device.](#)
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

## Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > iPerf**.
4. Click **Enable**.
5. (Optional) For **iPerf Server Port**, type the appropriate port number for the iPerf server listening port.
6. (Optional) Click to expand **Access control list** to restrict access to the iPerf server:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's iPerf service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the iPerf service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's iPerf service. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the iPerf service.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.

- c. For **Interface**, select the appropriate interface from the dropdown.
- d. Click **+** again to allow access through additional interfaces.
  - To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
7. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable the iPerf server:

```
(config)> service iperf enable true
(config)>
```

4. (Optional) Set the port number for the iPerf server listening port. The default is 5201.

```
(config)> service iperf port port_number
(config)>
```

5. (Optional) Set the access control list to restrict access to the iPerf server:

- To limit access to specified IPv4 addresses and networks:

```
(config)> add service iperf acl address end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

```
(config)> add service iperf acl address6 end value
(config)>
```

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service iperf acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service iperf acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

-----

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example performance test using iPerf3

On a remote host with iPerf3 installed, enter the following command:

```
$ iperf3 -c device_ip
```

where *device\_ip* is the IP address of the Connect EZ device. For example:

```
$ iperf3 -c 192.168.2.1
Connecting to host 192.168.2.1, port 5201
[ 4] local 192.168.3.100 port 54934 connected to 192.168.1.1 port 5201
[ ID] Interval      Transfer    Bandwidth   Retr  Cwnd
[ 4]  0.00-1.00    sec  26.7 MBytes  224 Mbits/sec    8  2.68 MBytes
[ 4]  1.00-2.00    sec  28.4 MBytes  238 Mbits/sec   29  1.39 MBytes
[ 4]  2.00-3.00    sec  29.8 MBytes  250 Mbits/sec    0  1.46 MBytes
[ 4]  3.00-4.00    sec  31.2 MBytes  262 Mbits/sec    0  1.52 MBytes
[ 4]  4.00-5.00    sec  32.1 MBytes  269 Mbits/sec    0  1.56 MBytes
[ 4]  5.00-6.00    sec  32.5 MBytes  273 Mbits/sec    0  1.58 MBytes
[ 4]  6.00-7.00    sec  33.9 MBytes  284 Mbits/sec    0  1.60 MBytes
[ 4]  7.00-8.00    sec  33.7 MBytes  282 Mbits/sec    0  1.60 MBytes
[ 4]  8.00-9.00    sec  33.5 MBytes  281 Mbits/sec    0  1.60 MBytes
[ 4]  9.00-10.00   sec  33.2 MBytes  279 Mbits/sec    0  1.60 MBytes
-----
[ ID] Interval      Transfer    Bandwidth   Retr
[ 4]  0.00-10.00   sec  315 MBytes  264 Mbits/sec   37
[ 4]  0.00-10.00   sec  313 MBytes  262 Mbits/sec
sender
receiver

iperf Done.
$
```

## Configure the ping responder service

Your Connect EZ device's ping responder service replies to ICMP and ICMPv6 echo requests. The service is enabled by default. You can disable the service, or you can configure the service to use an access control list to limit the service to specified IP address, interfaces, and/or zones.

To enable the iPerf3 server:

### Web

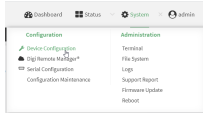
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Services > Ping responder**.

The ping responder service is enabled by default. Click **Enable** to disable all ping responses.

4. Click to expand **Access control list** to restrict ping responses to specified IP address, interfaces, and/or zones:
  - To limit access to specified IPv4 addresses and networks:
    - a. Click **IPv4 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv4 address or network that can access the device's ping responder. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 192.168.1.0/24.
      - **any**: No limit to IPv4 addresses that can access the ping responder.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to specified IPv6 addresses and networks:
    - a. Click **IPv6 Addresses**.
    - b. For **Add Address**, click **+**.
    - c. For **Address**, enter the IPv6 address or network that can access the device's ping responder. Allowed values are:
      - A single IP address or host name.
      - A network designation in CIDR notation, for example, 2001:db8::/48.
      - **any**: No limit to IPv6 addresses that can access the ping responder.
    - d. Click **+** again to list additional IP addresses or networks.
  - To limit access to hosts connected through a specified interface on the device:
    - a. Click **Interfaces**.
    - b. For **Add Interface**, click **+**.
    - c. For **Interface**, select the appropriate interface from the dropdown.
    - d. Click **+** again to allow access through additional interfaces.



- To limit access based on firewall zones:
    - a. Click **Zones**.
    - b. For **Add Zone**, click **+**.
    - c. For **Zone**, select the appropriate firewall zone from the dropdown.  
See [Firewall configuration](#) for information about firewall zones.
    - d. Click **+** again to allow access through additional firewall zones.
- 5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable the iPerf server:

---

```
(config)> service iperf enable true
(config)>
```

---

4. (Optional) Set the port number for the iPerf server listening port. The default is 5201.

---

```
(config)> service iperf port port_number
(config)>
```

---

5. (Optional) Set the access control list to restrict access to the iPerf server:

- To limit access to specified IPv4 addresses and networks:

---

```
(config)> add service iperf acl address end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 192.168.1.0/24.
- **any**: No limit to IPv4 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to specified IPv6 addresses and networks:

---

```
(config)> add service iperf acl address6 end value
(config)>
```

---

Where *value* can be:

- A single IP address or host name.
- A network designation in CIDR notation, for example, 2001:db8::/48.
- **any**: No limit to IPv6 addresses that can access the service-type.

Repeat this step to list additional IP addresses or networks.

- To limit access to hosts connected through a specified interface on the Connect EZ device:

---

```
(config)> add service iperf acl interface end value
(config)>
```

---

Where *value* is an interface defined on your device.

Display a list of available interfaces:

Use ... **network interface ?** to display interface information:

Repeat this step to list additional interfaces.

- To limit access based on firewall zones:

---

```
(config)> add service iperf acl zone end value
(config)>
```

---

Where *value* is a firewall zone defined on your device, or the **any** keyword.

Display a list of available firewall zones:

Type ... **firewall zone ?** at the config prompt:

---

```
(config)> ... firewall zone ?
```

```
Zones: A list of groups of network interfaces that can be
referred to by packet
filtering rules and access control lists.
```

```
Additional Configuration
```

```
-----
```

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

```
(config)>
```

---

Repeat this step to include additional firewall zones.

## 6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example performance test using iPerf3

On a remote host with Iperf3 installed, enter the following command:

---

```
$ iperf3 -c device_ip
```

---

where *device\_ip* is the IP address of the Connect EZ device. For example:

---

```
$ iperf3 -c 192.168.2.1
Connecting to host 192.168.2.1, port 5201
[ 4] local 192.168.3.100 port 54934 connected to 192.168.1.1 port 5201
[ ID] Interval          Transfer      Bandwidth      Retr  Cwnd
[ 4]  0.00-1.00      sec  26.7 MBytes  224 Mbits/sec    8   2.68 MBytes
[ 4]  1.00-2.00      sec  28.4 MBytes  238 Mbits/sec   29   1.39 MBytes
[ 4]  2.00-3.00      sec  29.8 MBytes  250 Mbits/sec    0   1.46 MBytes
[ 4]  3.00-4.00      sec  31.2 MBytes  262 Mbits/sec    0   1.52 MBytes
[ 4]  4.00-5.00      sec  32.1 MBytes  269 Mbits/sec    0   1.56 MBytes
[ 4]  5.00-6.00      sec  32.5 MBytes  273 Mbits/sec    0   1.58 MBytes
[ 4]  6.00-7.00      sec  33.9 MBytes  284 Mbits/sec    0   1.60 MBytes
[ 4]  7.00-8.00      sec  33.7 MBytes  282 Mbits/sec    0   1.60 MBytes
[ 4]  8.00-9.00      sec  33.5 MBytes  281 Mbits/sec    0   1.60 MBytes
[ 4]  9.00-10.00     sec  33.2 MBytes  279 Mbits/sec    0   1.60 MBytes
- - - - -
[ ID] Interval          Transfer      Bandwidth      Retr
[ 4]  0.00-10.00     sec  315 MBytes  264 Mbits/sec   37
[ 4]  0.00-10.00     sec  313 MBytes  262 Mbits/sec
iperf Done.
$
```

---

# Applications

---

The Connect EZ supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. You can also specify Python applications and other scripts to be run each time the device system restarts, at specific intervals, or at a specified time.

This chapter contains the following topics:

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| Develop Python applications .....                                  | 453 |
| Set up the Connect EZ to automatically run your applications ..... | 489 |
| Start an interactive Python session .....                          | 498 |
| Run a Python application at the shell prompt .....                 | 499 |
| Configure scripts to run manually .....                            | 500 |
| Start a manual script .....                                        | 506 |

## Develop Python applications

The Connect EZ features a standard Python 3.6 distribution. Python is a dynamic, object-oriented language for developing software applications, from simple programs to complex embedded applications. Digi offers the Digi IoT PyCharm Plugin to help you while writing, building, and testing your application. See [Create and test a Python application](#).

In addition to the standard Python library, the Connect EZ includes a set of extensions to access its configuration and interfaces. See [Python modules](#).

The Connect EZ provides you with the ability to:

- Run Python applications on the device interactively or from a file.
- Specify Python applications and other scripts to be run each time the device system restarts, at specific intervals, or at a specified time. See [Configure scripts to run automatically](#).
- Use pip to install Python packages.

---

**Note** Although pip is provided to help facilitate the installation of Python packages, there are limitations in Python package support due to package dependencies, storage limitations, and other issues.

---

This section contains the following topics:

|                                                    |     |
|----------------------------------------------------|-----|
| Set up the Connect EZ for Python development ..... | 454 |
| Create and test a Python application .....         | 454 |
| Python modules .....                               | 458 |

## Set up the Connect EZ for Python development

1. Access the Connect EZ local web interface
  - a. Use an Ethernet cable to connect the Connect EZ to your local laptop or PC.  
The factory default IP address is **192.168.2.1**
  - b. Log into the Connect EZ WebUI as a user with full admin access rights.  
The default user name is **admin** and the default password is the unique password printed on the label packaged with your device.
2. Go to the Configuration window
  - a. On the menu, click **System**.
  - b. Under **Configuration**, click **Device Configuration**. The Configuration window displays.
3. Enable service discovery (mDNS)
  - a. Click **Services > Service Discovery (mDNS)**.
  - b. **Enable** the mDNS service.

---

**Note** For more information, see [Enable service discovery \(mDNS\)](#).

---

4. Configure SSH access
  - a. Click **Services > SSH**.
  - b. Click **Enable**.

---

**Note** For more information, see the following topics: [Configure SSH access](#), [Use SSH with key authentication](#), and [Allow remote access for web administration and SSH](#).

---

5. Enable shell access
  - a. Click **Authentication > Groups > admin**.
  - b. Click the **Interactive shell access** option.
  - c. If this option is not displayed, see [Disable shell access](#).
6. Click **Apply** to save the configuration and apply the changes.  
The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

## Create and test a Python application

To develop a Python application for the Connect EZ:

1. [Set up the Connect EZ for Python development](#).
2. Create and test your application with:
  - [PyCharm](#). You can create, build, and remotely launch your application in the Connect EZ.
  - Your preferred editor and [manually transfer the application, install dependencies, and launch](#) in the Connect EZ.

### **Develop an application in PyCharm**

The Digi IoT PyCharm Plugin allows you to write, build and run Python applications for Digi devices in a quick and easy way. See the [Digi XBee PyCharm IDE Plugin User Guide](#) for details.

This is what you can do with it:

- Create Python projects from scratch or import one of the available examples.
- Get help while you write your code thanks to the syntax highlight, quick documentation, and code completion features.
- Build and upload Python applications to your Digi device with just one click.
- Add libraries that facilitate the usage of external peripherals or non-standard APIs.
- Communicate with your Digi device through the integrated SSH console to see the application output or execute quick tests.

### **Manually install and launch an application**

To create, build, and launch your application:

1. Write your Python application code. Code can include:
  - Any Python 3.6 standard feature.
  - Access to the Connect EZ configuration and hardware with the [Python modules](#).
  - Third-party modules included in the Connect EZ, for example:
    - pySerial 3.4
    - Eclipse Paho MQTT Python Client
  - Any other third-party module implemented in Python.
2. Install the application in `/etc/config/scripts` directory.
3. Launch your application:
  - [Run your application at the shell prompt](#).
  - [Configure your application to run automatically](#).

### **PyCharm FAQ: My Connect EZ is not listed in Digi Device Selector**

If an Connect EZ does not appear on the list of the Digi Device Selector:

- Ensure that your device has the mDNS service enabled and is on the same network as the computer. See [Set up the Connect EZ for Python development](#).
- Or click the link **Click here to add it manually** to specify the IP address, port, username, and password.



### **Example: Configure a custom port to listen for incoming socket connections**

The following example Python script configures a custom port, port 9999, to accept incoming socket connections.

You will also need to add a custom firewall rule to accept the incoming traffic on this port.

#### **Example script**

---

```
import socket
import socketserver

class MyTCPHandler(socketserver.BaseRequestHandler):
    """
    The request handler class for our server.

    It is instantiated once per connection to the server, and must
    override the handle() method to implement communication to the
    client.
    """

    def handle(self):
        # self.request is the TCP socket connected to the client
        self.data = self.request.recv(1024).strip()
        print("{} wrote:".format(self.client_address[0]))
        print(self.data)
        # just send back the same data, but upper-cased
        self.request.sendall(self.data.upper())
```

---



```
if __name__ == "__main__":
    HOST, PORT = '', 9999

    # Create the server, binding to localhost on port 9999
    with socketserver.TCPServer((HOST, PORT), MyTCPHandler) as server:
        # Activate the server; this will keep running until you
        # interrupt the program with Ctrl-C
        print("Waiting for data...")
        server.serve_forever()
```

**Create a custom firewall rule**

**Web**

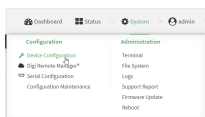
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

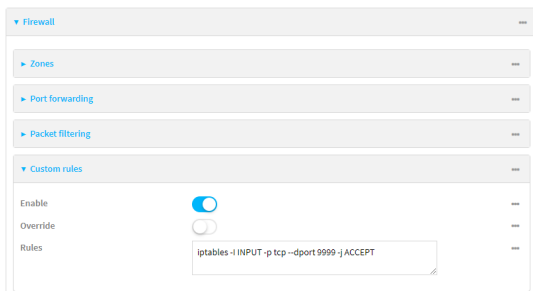
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Custom rules**.
4. **Enable** the custom rules.
5. For **Rules**, type the following:

```
iptables -I INPUT -p tcp --dport 9999 -j ACCEPT
```



6. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable custom firewall rules:

```
(config)> firewall custom enable true(config)>
```

4. Set the shell command that will execute the custom firewall rules script:

```
(config)> firewall custom rules "iptables -I INPUT -p tcp --dport 9999 -j
ACCEPT"
(config)>
```

5. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Python modules

The Connect EZ supports Python 3.6 and provides you with the ability to run Python applications on the device interactively or from a file. It also offers extensions to manage your Connect EZ:

- The **digidevice** module provides platform-specific extensions that allow you to interact with the device's configuration and interfaces.

The following submodules are included with the **digidevice** module:

- LEDs: **digidevice.led**
- SMS: **digidevice.sms**
- GPS: **digidevice.location**
- Digi Remote Manager:
  - **digidevice.datapoint**
  - **digidevice.device\_request**
  - **digidevice.name**
- Device configuration: **digidevice.config**
- Command line interface: **digidevice.cli**

- Access runtime database: **digidevice.runt**
- Set the maintenance window: **digidevice.maintenance**
- Use the Python **serial** module—[pySerial](#)—to access the serial ports.
- [Eclipse Paho MQTT Python client](#) enables applications to connect to an [MQTT](#) broker to publish messages, and to subscribe to topics and receive published messages.

---

**Note** Module-related documentation is in the [Digidevice module](#) section.

---

### ***Digidevice module***

The Python **digidevice** module provides platform-specific extensions that allow you to interact with the device's configuration and interfaces. The following submodules are included with the **digidevice** module:

This section contains the following topics:

### Use digidevice.cli to execute CLI commands

Use the **digidevice.cli** Python module to issue CLI commands from Python to retrieve status and statistical information about the device.

For example, to display the system status and statistics by using an interactive Python session, use the [show system](#) command with the **cli** module:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **cli** submodule:

---

```
>>> from digidevice import cli
>>>
```

---

4. Execute a CLI command using the **cli.execute(command)** function. For example, to print the system status and statistics to stdout using the **show system** command:

---

```
>>> response = cli.execute("show system")
>>>
>>> print (response)
```

```

Model                : Digi Connect EZ
Serial Number         : Connect EZxxxxxxxxxyyyxx
SKU                   : Connect EZ
Hostname              : Connect EZ
MAC Address           : DF:DD:E2:AE:21:18

Hardware Version      : 50001947-01 1P
Firmware Version      : 24.3
Alt. Firmware Version : 24.3
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version    : 19.7.23.0-15f936e0ed

Current Time          : Thu, Jan 11, 2024 12:10:00 +0000
CPU                   : 1.4%
Uptime                : 6 days, 6 hours, 21 minutes, 57 seconds
(541317s)
Temperature           : 40C
Location              :
Contact               :

>>>
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### Help for using Python to execute Connect EZ CLI commands

Get help executing a CLI command from Python by accessing help for **cli.execute**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **cli** submodule:

---

```
>>> from digidevice import cli
>>>
```

---

4. Use the help command with **cli.execute**:

---

```
>>> help(cli.execute)
Help on function execute in module digidevice.cli:

execute(command, timeout=5)
Execute a CLI command with the timeout specified returning the results.
...
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### Use digidevice.datapoint to upload custom datapoints to Digi Remote Manager

Use the **datapoint** Python module to upload custom datapoints to Digi Remote Manager.

The following characteristics can be defined for a datapoint:

- Stream ID
- Value
- (Optional) Data type
  - integer
  - long
  - float
  - double
  - string
  - binary
- Units (optional)
- Timestamp (optional)
- Location (optional)

- Tuple of latitude, longitude and altitude
- Description (optional)
- Quality (optional)
  - An integer describing the quality of the data point

For example, to use an interactive Python session to upload datapoints related to velocity, temperature, and the state of the emergency door:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **datapoint** submodule and other necessary modules:

---

```
>>> from digidevice import datapoint
>>> import time
>>>
```

---

4. Upload the datapoints to Remote Manager:

---

```
>>> datapoint.upload("Velocity", 69, units="mph")
>>> datapoint.upload("Temperature", 24, geo_location=(54.409469, -
1.718836, 129))
>>> datapoint.upload("Emergency_Door", "closed", timestamp=time.time())
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

You can also upload multiple datapoints:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **datapoint** submodule and other necessary modules:

---

```
>>> from digidevice import datapoint
>>> import time
>>>
```

---

4. Create datapoint objects:

---

```
>>> p1 = datapoint.DataPoint("Velocity", 69, units="mph")
>>> p2 = datapoint.DataPoint("Temperature", 24, geo_location=(54.409469,
-1.718836, 129))
>>> p3 = datapoint.DataPoint("Emergency_Door", "closed",
timestamp=time.time())
>>>
```

---

5. Upload the datapoints to Remote Manager:

---

```
>>> datapoint.upload_multiple([p1, p2, p3])
>>>
```

---

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Once the datapoints have been uploaded to Remote Manager, they can be viewed via Remote Manager or accessed using Web Services calls. See the [Digi Remote Manager Programmers Guide](#) for more information on web services and datapoints.

#### ***Help for using Python to upload custom datapoints to Remote Manager***

Get help for uploading datapoints to your Digi Remote Manager account by accessing help for **datapoint.upload** and **datapoint.upload\_multiple**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **datapoint** submodule and other necessary modules:

---

```
>>> from digidevice import datapoint
>>>
```

---

4. Use the help command with **datapoint.upload**:

---

```
>>> help(datapoint.upload)
Help on function upload in module digidevice.datapoint:
```

---

---

```
upload(stream_id:str, data, *, description:str=None,
timestamp:float=None, units:str=None,
geo_location:Tuple[float, float, float]=None, quality:int=None,
data_type:digidevice.datapoint.DataType=None, timeout:float=None)
...
```

---

5. Use the help command with **datapoint.upload\_multiple**:

---

```
>>> help(datapoint.upload_multiple)
Help on function upload_multiple in module digidevice.datapoint:

upload_multiple(datapoints:List[digidevice.datapoint.DataPoint],
timeout:float=None)
...
```

---

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### Use digidevice.config for device configuration

Use the **config** Python module to access and modify the device configuration.

#### Read the device configuration

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

4. Use **config.load()** and the **get()** method to return the device's configuration:

- a. Return the entire configuration:

---

```
>>> from pprint import pprint # use pprint vs. print to make the
output easier to read
>>> cfg = config.load()
>>> pprint(cfg.dump().splitlines())
```

---

This returns the device configuration:

---

```
...
network.interface.lan1.device=/network/bridge/lan1
```

---



---

```
network.interface.lan1.enable=true
network.interface.lan1.ipv4.address=192.168.2.1/24
network.interface.lan1.ipv4.connection_monitor.attempts=3
...
```

---

- b. Print a list of available interfaces:

---

```
>>> cfg = config.load()
>>> interfaces = cfg.get("network.interface")
>>> print(interfaces.keys())
```

---

This returns the following:

---

```
['defaultip', 'defaultlinklocal', 'lan1', 'loopback', 'wan1']
```

---

- c. Print the IPv4 address of the LAN interface:

---

```
>>> cfg = config.load()
>>> interfaces = cfg.get("network.interfaces")
>>> print(interfaces.get("lan.ipv4.address"))
```

---

Which returns:

---

```
192.168.2.1/24
```

---

### **Modify the device configuration**

Use the **set()** and **commit()** methods to modify the device configuration:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

4. Use **config.load(writable=True)** to enable write mode for the configuration:

---

```
>>> cfg = config.load(writable=True)
>>>
```

---

- Use the **set()** method to make changes to the configuration:

---

```
>>> cfg.set("system.name", "New-Name")
>>>
```

---

- Use the **commit()** method to save the changes:

---

```
>>> cfg.commit()
True
>>>
```

---

- Use the **get()** method to verify the change:

---

```
>>> print(cfg.get("system.name"))
New-Name
>>>
```

---

### **Help for using Python to read and modify device configuration**

Get help for reading and modifying the device configuration by accessing help for **digidevice.config**:

- Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **config** submodule:

---

```
>>> from digidevice import config
>>>
```

---

- Use the help command with **config**:

---

```
>>> help(config)
Help on module acl.config in acl:

NAME
acl.config - Python interface to ACL configuration (libconfig).
...
```

---

- Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### **Use Python to respond to Digi Remote Manager SCI requests**

The **device\_request** Python module allows you to interact with Digi Remote Manager by using Remote Manager's Server Command Interface (SCI), a web service that allows users to access information and perform commands that relate to their devices.

Use Remote Manager's SCI interface to create SCI requests that are sent to your Connect EZ device, and use the `device_request` module to send responses to those requests to Remote Manager.

See the [Digi Remote Manager Programmers Guide](#) for more information on SCI.

**Task one: Use the `device_request` module on your Connect EZ device to create a response**

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type `shell` to access the device shell.

2. At the shell prompt, use the `python` command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the `device_request` module:

---

```
>>> from digidevice import device_request
>>>
```

---

4. Create a function to handle the request from Remote Manager:

---

```
>>> def handler(target, request):
    print ("received request %s for target %s" % (request, target))
    return "OK"
>>>
```

---

5. Register a callback function that will be called when the device receives a SCI request from Remote Manager:

---

```
>>> device_request.register("myTarget", handler)
>>>
```

---

**Note** Leave the interactive Python session active while completing task two, below. Once you have completed task two, exit the interactive session by using **Ctrl-D**. You can also exit the session using `exit()` or `quit()`.

**Task two: Create and send an SCI request from Digi Remote Manager**

The second step in using the `device_request` module is to create an SCI request that Remote Manager will forward to the device. For example, you can create in SCI request a the Remote Manager API explorer:

1. In Remote Manager, click **Documentation > API Explorer**.
2. Select the device to use as the SCI target:
  - a. Click **SCI Targets**.
  - b. Click **Add Targets**.
  - c. Enter or select the device ID of the device.

- d. Click **Add**.
- e. Click **OK**.
3. Click **Examples > SCI > Data Service > Send Request**.

Code similar to the following will be displayed in the HTTP message body text box:

---

```
<sci_request version="1.0">
  <data_service>
    <targets>
      <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

---

**Note** The value of the **target\_name** parameter in the **device\_request** element must correspond to the **target** parameter of the **device\_request.register** function in the Python script. In this example, the two are the same.

---

4. Click **Send**.

Once that the request has been sent to the device, the handler on the device is executed.

- On the device, you will receive the following output:

---

```
>>> received request
      my payload string
      for target myTarget
>>>
```

---

- In Remote Manager, you will receive a response similar to the following:

---

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    <requests>
      <device_request target_name="myTarget"
status="0">OK</device_request>
    </requests>
  </device>
</data_service>
</sci_request>
```

---

### Example: Use `digidevice.cli` with `digidevice.device_request`

In this example, we will use the `digidevice.cli` module in conjunction with the `digidevice.device_request` module to return information about multiple devices to Remote Manager.

1. Create a Python application, called `showsystem.py`, that uses the `digidevice.cli` module to create a response containing information about device and the `device_request` module to respond with this information to a request from Remote Manager:

```

from digidevice import device_request
from digidevice import cli
import time

def handler(target, request):
    return cli.execute("show system verbose")

def status_cb(error_code, error_description):
    if error_code != 0:
        print("error handling showSystem device request: %s" % error_
description)

device_request.register("showSystem", handler, status_callback = status_
cb)

# Do not let the process finish so that it handles device requests
while True:
    time.sleep(10)
    
```

2. Upload the showsystem.py application to the /etc/config/scripts directory on two or more Digi devices. In this example, we will upload it to two devices, and use the same request in Remote Manager to query both devices.  
 See [Configure scripts to run automatically](#) for information about uploading Python applications to your device. You can also create the script on the device by using the vi command when logged in with shell access.
3. For both devices:
  - a. Configure the device to automatically run the showsystem.py application on reboot, and to restart the application if it crashes. This can be done from either the WebUI or the command line:

**Web**

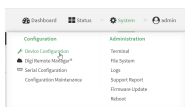
- i. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- ii. Access the device configuration:

Remote Manager:

- i. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- ii. Click the **Device ID**.
- iii. Click **Settings**.
- iv. Click to expand **Config**.

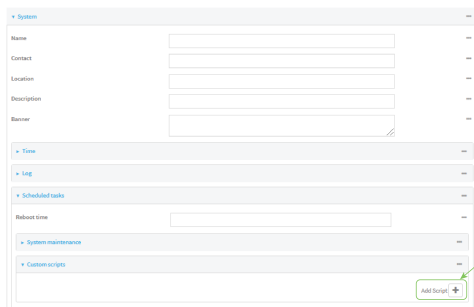
Local Web UI:

- i. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

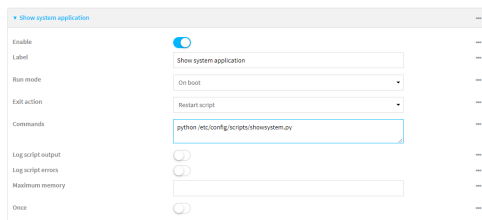


The **Configuration** window is displayed.

- iii. Click **System > Scheduled tasks > Custom scripts**.
- iv. Click **+** to add a custom script.



- v. For **Label**, type **Show system application**.
- vi. For **Run mode**, select **On boot**.
- vii. For **Exit action**, select **Restart script**.
- viii. For **Commands**, type **python /etc/config/scripts/showsystem.py**.



- ix. Click **Apply** to save the configuration and apply the change.

## Command line

- i. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- ii. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- iii. Add an application entry:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

Scheduled scripts are enabled by default. To disable:

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

- iv. Provide a label for the script:

---

```
(config system schedule script 0)> label "Show system application"
```

---

- v. Configure the application to run automatically when the device reboots:

---

```
(config system schedule script 0)> when boot
(config system schedule script 0)>
```

---

- vi. Configure the application to restart if it crashes:

---

```
(config system schedule script 0)> exit_action restart
(config system schedule script 0)>
```

---

- vii. Set the command that will execute the application:

---

```
(config system schedule script 0)> commands "python
/etc/config/scripts/showsystem.py"
(config system schedule script 0)>
```

---

- viii. Save the configuration and apply the change:

---

```
(config)> save
Configuration saved.
>
```

---

- b. Run the showsystem.py application. You can run the application by either rebooting the device, or by running it from the shell prompt.

- To reboot the device:

- i. From the WebUI:

- i. From the main menu, click **System**.
- ii. Click **Reboot**.

- i. From the command line, at the Admin CLI prompt, type:

---

```
> reboot
```

---

- To run the application from the shell prompt:

- i. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- ii. Type the following at the shell prompt:

---

```
# python /etc/config/scripts/showsystem.py &
#
```

---

- iii. Exit the shell:

---

```
# exit
```

---

4. In Remote Manager, click **Documentation > API Explorer**.
5. Select the devices to use as the SCI target:
  - a. Click **SCI Targets**.
  - b. Click **Add Targets**.
  - c. Enter or select the device ID of one of the devices.
  - d. Click **Add**.
  - e. Enter or select the device ID of the second device and click **Add**.
  - f. Click **OK**.
6. Click **Examples > SCI > Data Service > Send Request**.

Code similar to the following will be displayed in the HTTP message body text box:

---

```
<sci_request version="1.0">
  <data_service>
    <targets>
      <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
      <device id="00000000-00000000-0000FFFF-485740BC"/>
    </targets>
    <requests>
      <device_request target_name="myTarget">
        my payload string
      </device_request>
    </requests>
  </data_service>
</sci_request>
```

---

7. For the **device\_request** element, replace the value of **target\_name** with **showSystem**. This matches the **target** parameter of the **device\_request.register** function in the **showsystem.py** application.

---

```
<device_request target_name="showSystem">
```

---

8. Click **Send**.

You should receive a response similar to the following:

---

```
<sci_reply version="1.0">
  <data_service>
    <device id="00000000-00000000-0000FFFF-A83CF6A3"/>
    <requests>
      <device_request target_name="showSystem" status="0">Model
        : Digi Connect EZ
        Serial Number           : Connect EZ-000068
        Hostname                 : Connect EZ
        MAC                      : 00:40:D0:13:35:36

        Hardware Version        : 50001959-01 A
        Firmware Version         : 24.3
        Bootloader Version       : 1
```

---



---

```

        Firmware Build Date      : Fri, Jan 12, 2024 12:10:00
        Schema Version           : 461

        Timezone                  : UTC
        Current Time              : Thu, Jan 11, 2024 12:10:00
        CPU                       : 1.1
        Uptime                    : 1 day, 21 hours, 49 minutes, 47
seconds (164987s)
        Temperature              : 39C

        Contact                   : Jane Smith

        Disk
        ----
        Load Average              : 0.10, 0.05, 0.00
        RAM Usage                 : 85.176MB/250.484MB(34%)
        Disk /etc/config Usage    : 0.068MB/13.416MB(1%)
        Disk /opt Usage           : 47.724MB/5309.752MB(1%)
        Disk /overlay Usage       : MB/MB(%)
        Disk /tmp Usage           : 0.004MB/40.96MB(0%)
        Disk /var Usage           : 0.820MB/32.768MB(3%)</device_
request>
</requests>
</device>
<device id="00000000-00000000-0000FFFF-485740BC"/>
<requests>
  <device_request target_name="showSystem" status="0">Model
    : Digi Connect EZ
    Serial Number                : Connect EZ-000023
    Hostname                     : Connect EZ
    MAC                          : 00:40:D0:26:79:1C

    Hardware Version             : 50001959-01 A
    Firmware Version             : 24.3
    Bootloader Version           : 1
    Firmware Build Date          : Fri, Jan 12, 2024 12:10:00
    Schema Version               : 461

    Timezone                     : UTC
    Current Time                 : Thu, Jan 11, 2024 12:10:00
    CPU                          : 1.1
    Uptime                      : 4 day, 13 hours, 43 minutes, 22
seconds (395002s)
    Temperature                  : 37C

    Contact                      : Omar Ahmad

    Disk
    ----
    Load Average                : 0.10, 0.05, 0.00
    RAM Usage                    : 85.176MB/250.484MB(34%)
    Disk /etc/config Usage       : 0.068MB/13.416MB(1%)
    Disk /opt Usage              : 47.724MB/5309.752MB(1%)
    Disk /overlay Usage          : MB/MB(%)
    Disk /tmp Usage              : 0.004MB/40.96MB(0%)
    Disk /var Usage              : 0.820MB/32.768MB(3%)</device_
request>
</requests>

```

---

---

```

    </device>
  </data_service>
</sci_request>

```

---

### Help for using Python to respond to Digi Remote Manager SCI requests

Get help for respond to Digi Remote Manager Server Command Interface (SCI) requests by accessing help for **digidevice.device\_request**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```

# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>

```

---

3. Import the **device\_request** submodule:

---

```

>>> from digidevice import device_request
>>>

```

---

4. Use the help command with **device\_request**:

---

```

>>> help(device_request)
Help on module digidevice.device_request in digidevice:

NAME
digidevice.device_request - APIs for registering device request handlers
...

```

---

You can also use the help command with available **device\_request** functions:

- Use the help command with **device\_request.register**:

---

```

>>> help(device_request.register)
Help on function register in module digidevice.device_request:

register(target:str, response_callback:Callable[[str, str], str],
status_callback:Callable[[int, str], NoneType]=None, xml_
encoding:str='UTF-8')
...

```

---

- Use the help command with **device\_request.unregister**:

---

```

>>> help(device_request.unregister)
Help on function unregister in module digidevice.device_request:

```

---

---

```
unregister(target:str) -> bool
...
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### Use digidevice runtime to access the runtime database

Use the **runt** submodule to access and modify the device runtime database.

#### Read from the runtime database

Use the **keys()** and **get()** methods to read the device configuration:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

4. Use the **start()** method to open the runtime database:

---

```
>>> runt.start()
>>>
```

---

5. Use the **keys()** method to display available keys in the runtime database, and use the **get()** method to print information from the runtime database:

- a. Print available keys:

---

```
>>> print(runt.keys(""))
```

---

This returns available keys:

---

```
['advanced', 'drm', 'firmware', 'location', 'manufacture', 'metrics',
 'mm', 'network', 'pam', 'serial', 'system']
```

---

- b. Print available keys for the system key:

---

```
>>> print(runt.keys("system"))
```

---

This will return the following:

---

```
['boot_count', 'chassis', 'cpu_temp', 'cpu_usage', 'disk', 'load_avg',
'local_time', 'mac', 'mcu', 'model', 'ram', 'serial', 'uptime']
```

---

- c. Use the **get()** method to print the device's MAC address:

---

```
>>> print(runt.get("system.mac"))
```

---

This will return the MAC address of the device.

6. Use the **stop()** method to close the runtime database:
7. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### **Modify the runtime database**

Use the **set()** method to modify the runtime database:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

4. Use **start()** method to open the runtime database:

---

```
>>> runt.start()
>>>
```

---

5. Use the **set()** method to make changes to the runtime database:

---

```
>>> runt.set("my-variable", "my-value")
>>>
```

---

6. Use the **get()** method to verify the change:

---

```
>>> print(runt.get("my-variable"))
my-variable
>>>
```

---

7. Close the runtime database:

---

```
>>> runt.stop()
>>>
```

---

- Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

#### **Help for using Python to access the runtime database**

Get help for reading and modifying the device runtime database by accessing help for **digidevice.runt**:

- Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **runt** submodule:

---

```
>>> from digidevice import runt
>>>
```

---

- Use the help command with **runt**:

---

```
>>> help(runt)

Help on module acl.runt in digidevice:

NAME
acl.runt - Python interface to ACL runtime database (runt).
...
```

---

- Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

#### **Use Python to upload the device name to Digi Remote Manager**

The **name** submodule can be used to upload a custom name for your device to Digi Remote Manager.

When you use the **name** submodule to upload a custom device name to Remote Manager, the following issues apply:

- If the name is being used by to another device in your Remote Manager account, the name will be removed from the previous device and added to the new device.
- If Remote Manager is configured to apply a profile to a device based on the device name, changing the name of the device may cause Remote Manager to automatically push a profile onto the device.

Together, these two features allow you to swap one device for another by using the **name** submodule to change the device name, while guaranteeing that the new device will have the same configuration as the previous one.

---

**Note** Because causing a profile to be automatically pushed from Remote Manager may change the behavior of the device, including overwriting existing usernames and passwords, the **name** submodule should be used with caution. As a result, support for this functionality is disabled by default on Remote Manager.

---

### **Enable support on Digi Remote Manager for uploading custom device names**

1. In Remote Manager, click **API Explorer**.
2. For the HTTP method, select **PUT**.
3. For **Enter and API or select an example**, type **/ws/v1/settings/inventory/AllowDeviceToSetOwnNameEnabled**.
4. In the HTTP message body text box, type the following:

---

```
{
  "name" : "AllowDeviceToSetOwnNameEnabled",
  "value" : "true"
}
```

---

5. Click **Send**.

### **Upload a custom name**

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Import the **name** submodule:

---

```
>>> from digidevice import name
```

---

4. Upload the name to Remote Manager:

---

```
>>> name.upload("my_name")
```

---

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### **Help for uploading the device name to Digi Remote Manager**

Get help for uploading the device name to Digi Remote Manager by accessing help for **digidevice.name**:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line

as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **name** submodule:

---

```
>>> from digidevice import name
>>>
```

---

- Use the help command with **name**:

---

```
>>> help(name)

Help on module digidevice.name in digidevice:

NAME
digidevice.name - API for uploading name from the device
...
```

---

- Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### Use Python to set the maintenance window

The **maintenance** Python module allows you to set the service state of a device. When the module sets the device to out of service, this can be used as trigger to begin maintenance activity. See [Schedule system maintenance tasks](#) for more details.

- Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **maintenance** module:

---

```
>>> from digidevice import maintenance
>>>
```

---

- To determine the current service state of the device:

---

```
>>> maintenance.state()
'IN_SERVICE'
>>>
```

---

- To set the device to out of service:

---

```
>>> maintenance.out_of_service()
>>> maintenance.state()
'OUT_OF_SERVICE'
>>>
```

---

- To set the device to in service:

---

```
>>> maintenance.in_service()
>>> maintenance.state()
'IN_SERVICE'
>>>
```

---

**Note** Leave the interactive Python session active while completing task two, below. Once you have completed task two, exit the interactive session by using **Ctrl-D**. You can also exit the session using **exit()** or **quit()**.

---

### **Help for the digidevice maintenance module**

Get help for the digidevice maintenance module:

- Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **maintenance** submodule:

---

```
>>> from digidevice import maintenance
>>>
```

---

- Use the help command with **maintenance** :

---

```
>>> help(maintenance )
Help on module digidevice.maintenance in digidevice:

NAME
    digidevice.maintenance
```

---



DESCRIPTION

API for setting the device's service state. The service state is stored in runt.  
...

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

**Use Python to send and receive SMS messages**

You can create Python scripts that send and receive SMS message in tandem with the Digi Remote Manager by using the digidevice.sms module. To use a script to send or receive SMS messages, you must also enable the ability to schedule SMS scripting.

**Enable the ability to schedule SMS scripting**

**Web**

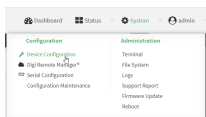
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device.](#)
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

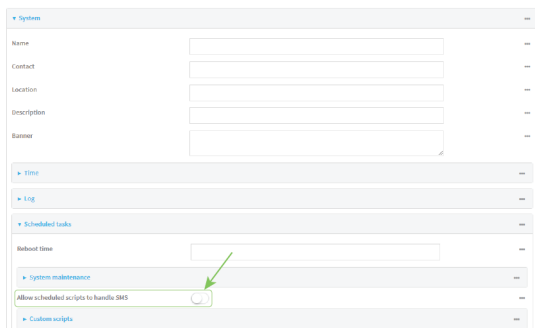
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System > Scheduled tasks**.

- Click to enable **Allow scheduled scripts to handle SMS**.



- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- At the config prompt, type:

```
(config)> system schedule sms_script_handling true
(config)>
```

- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See [Configure scripts to run automatically](#) for more information about scheduling scripts.

#### **Example digidevice.sms script**

The following example script receives an SMS message and sends a response:

```
#!/usr/bin/python3.10.1

import os
import threading
import sys
from digidevice.sms import Callback, send
COND = threading.Condition()
```

---

```

def sms_test_callback(sms, info):
    print(f"SMS message from {info['content.number']} received")
    print(sms)
    print(info)
    COND.acquire()
    COND.notify()
    COND.release()

def send_sms(destination, msg):
    print("sending SMS message", msg)
    if len(destination) == 10:
        destination = "+1" + destination
    send(destination, msg)

if __name__ == '__main__':
    if len(sys.argv) > 1:
        dest = sys.argv[1]
    else:
        dest = '+15005550006'
    my_callback = Callback(sms_test_callback, metadata=True)
    send_sms(dest, 'Hello World!')
    print("Please send an SMS message now.")
    print("Execution halted until a message is received or 60 seconds have
passed.")
    # acquire the semaphore and wait until a callback occurs
    COND.acquire()
    try:
        COND.wait(60.0)
    except Exception as err:
        print("exception occurred while waiting")
        print(err)
    COND.release()
    my_callback.unregister_callback()

```

---

### **Example script using digidevice.sms to send CLI commands**

The following example script listens for an incoming SMS message from a specific phone number (2223334444) and then executes the SMS message as a CLI command. If the CLI command being run has output, it will send that output as a response SMS message. If the CLI command being run has no output but ran successfully, the script will instead send an OK response SMS message. Errors in running the CLI will have those error messages sent as a SMS response.

---

```

#!/usr/bin/python

# Take an incoming SMS message from a specified phone number and run it as
# a CLI command. Send a reponse SMS to the sender before running the command

import os
import threading
import sys
from digidevice import cli
from digidevice.sms import Callback, send
COND = threading.Condition()
allowed_incoming_phone_number = '2223334444'

def sms_test_callback(sms, info):
    if info['content.number'] == allowed_incoming_phone_number:
        print(f"SMS message from {info['content.number']} received")

```

---

---

```

        print(sms)
        print(info)
        #if sms == "Reboot":
        # send_sms(dest, 'Reboot message received, rebooting device...')
        # response = cli.execute("reboot")
        # print (response)
        send_sms(dest, 'Message received (' + sms + '). Performing as CLI
command...')
        response = cli.execute(sms)
        if not response:
            response = 'OK'
        send_sms(dest, 'CLI results: ' + response)
        print (response)
    COND.acquire()
    COND.notify()
    COND.release()

def send_sms(destination, msg):
    print("sending SMS message", msg)
    if len(destination) == 10:
        destination = "+1" + destination
    send(destination, msg)

if __name__ == '__main__':
    if len(sys.argv) > 1:
        dest = sys.argv[1]
    else:
        dest = allowed_incoming_phone_number
    my_callback = Callback(sms_test_callback, metadata=True)
    #send_sms(dest, 'Ready to receive incoming SMS message')
    print("Waiting up to 60 seconds for incoming SMS message")
    # acquire the semaphore and wait until a callback occurs
    COND.acquire()
    try:
        COND.wait(60.0)
    except Exception as err:
        print("exception occurred while waiting")
        print(err)
    COND.release()
    my_callback.unregister_callback()
    os.system('rm -f /var/run/sms/scripts/*') # remove all stored SMS messages,
since we've processed them
    print("SMS script finished. Please re-run if you want to check for more
incoming SMS messages")
    os._exit(0)

```

---

### Use Python to access serial ports

You can use the Python **serial** module to access serial ports on your Connect EZ device that are configured to be in Application mode. See [Configure Application mode for a serial port](#) for information about configuring a serial port in Application mode.

To use Python to access serial ports:

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

- Determine the path to the serial port:

---

```
# ls /dev/serial/
by-id  by-path  port1
#
```

---

- At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

- Import the **serial** module:

---

```
>>> import serial
>>>
```

---

- You can now perform operations on the serial port. For example, to write a message to the serial port:

---

```
>>> s = serial.Serial("/dev/serial/port1", 115200)
>>> s.write(b"Hello from serial port")
26
>>>
```

---

- Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

### ***Use the Paho MQTT python library***

Your Connect EZ device includes support for the Paho MQTT python library. MQTT is a lightweight messaging protocol used to communicate with various applications including cloud-based applications such as Amazon Web Services and Microsoft Azure. The following is example code that reads CPU and RAM usage on the device, updates the device firmware, then publishes information about DHCP clients and system information to the MQTT server at 192.168.1.100. The MQTT server IP is configurable.

```
"""
MQTT client example:
- Reporting some device metrics from runt
- Reporting DHCP clients
- Firmware update feature (simple implementation, read TODO in cmd_fwupdate)
"""

import sys
import time
import paho.mqtt.client as mqtt
import json
from acl import runt, config
from http import HTTPStatus
import urllib.request
import tempfile
```

---

```

import os
from digidevice import cli

POLL_TIME = 60

def cmd_reboot(params):
    print("Rebooting unit...")
    try:
        cli.execute("reboot", 10)
    except:
        print("Failed to run 'reboot' command")
        return HTTPStatus.INTERNAL_SERVER_ERROR

return HTTPStatus.OK

def cmd_fwupdate(params):
    try:
        fw_uri = params["uri"]
    except:
        print("Firmware file URI not passed")
        return HTTPStatus.BAD_REQUEST

    print("Request to update firmware with URI: {}".format(fw_uri))

    try:
        fd, fname = tempfile.mkstemp()
        os.close(fd)
        try:
            urllib.request.urlretrieve(fw_uri, fname)
        except:
            print("Failed to download FW file from URI {}".format(fw_uri))
            return HTTPStatus.NOT_FOUND

        try:
            ret = cli.execute("system firmware update file " + fname, 60)
        except:
            print("Failed to run firmware update command")
            return HTTPStatus.INTERNAL_SERVER_ERROR

        if not "Firmware update completed" in ret:
            print("Failed to update firmware")
            return HTTPStatus.INTERNAL_SERVER_ERROR
    finally:
        os.remove(fname)

    print("Firmware update finished")

    return HTTPStatus.OK

CMD_HANDLERS = {
    "reboot": cmd_reboot,
    "fw-update": cmd_fwupdate
}

def send_cmd_reply(client, cmd_path, cid, cmd, status):
    if not status or not cid:
        return

    if cmd_path.startswith(PREFIX_CMD):

```

---

```

        path = cmd_path[len(PREFIX_CMD):]
    else:
        print("Invalid command path ({}), cannot send reply".format(cmd_path))
        return

    reply = {
        "cmd": cmd,
        "status": status
    }

    client.publish(PREFIX_RSP + path + "/" + cid, json.dumps(reply, separators=
(' ',':')))

def on_connect(client, userdata, flags, rc):
    print("Connected to MQTT server")
    client.subscribe(PREFIX_CMD + "/system")

def on_message(client, userdata, msg):
    """ Supporting only a single topic for now, no need for filters
    Expects the following message format:
    {
        "cid": "<client-id>",
        "cmd": "<command>",
        "params": {
            <optional_parameters>
        }
    }

    Supported commands:
    - "fw-update"
      params:
        - "uri": "<firmware_file_URL>"
    - "reboot"
      params:
    """

    try:
        m = json.loads(msg.payload)
        cid = m["cid"]
        cmd = m["cmd"]
        try:
            payload = m["params"]
        except:
            payload = None
    except:
        print("Invalid command format: {}".format(msg.payload))
        if not cid:
            # Return if client-ID not passed
            return None
        send_cmd_reply(client, msg.topic, cid, cmd, HTTPStatus.BAD_REQUEST)

    try:
        status = CMD_HANDLERS[cmd](payload)
    except:
        print("Invalid command: {}".format(cmd))
        status = HTTPStatus.NOT_IMPLEMENTED

    send_cmd_reply(client, msg.topic, cid, cmd, status)

```

---

```

def publish_dhcp_leases():
    leases = []
    try:
        with open('/etc/config/dhcp.leases', 'r') as f:
            for line in f:
                elems = line.split()
                if len(elems) != 5:
                    continue
                leases.append({"mac": elems[1], "ip": elems[2], "host": elems
[3]})
    if leases:
        client.publish(PREFIX_EVENT + "/leases", json.dumps(leases,
separators=(',', ':')))
    except:
        print("Failed to open DHCP leases file")

def publish_system():
    avg1, avg5, avg15 = runt.get("system.load_avg").split(' ', ')
    ram_used = runt.get("system.ram.per")
    disk_opt = runt.get("system.disk./opt.per")
    disk_config = runt.get("system.disk./etc/config.per")

    msg = json.dumps({
        "load_avg": {
            "1min": avg1,
            "5min": avg5,
            "15min": avg15
        },
        "disk_usage": {
            "/opt": disk_opt,
            "/etc/config": disk_config,
            "ram": ram_used
        }
    })

    client.publish(PREFIX_EVENT + "/system", json.dumps(msg))

runt.start()
serial = runt.get("system.serial")

PREFIX = "router/" + serial
PREFIX_EVENT = "event/" + PREFIX
PREFIX_CMD = "cmd/" + PREFIX
PREFIX_RSP = "rsp/" + PREFIX

client = mqtt.Client()
client.on_connect = on_connect
client.on_message = on_message

try:
    client.connect("192.168.1.100", 1883, 60)
    client.loop_start()
except:
    print("Failed to connect to MQTT server")
    sys.exit(1)

while True:
    publish_dhcp_leases()
    publish_system()
    time.sleep(POLL_TIME)

```

---



## Set up the Connect EZ to automatically run your applications

This section contains the following topics:

- [Configure scripts to run automatically](#)
- [Show script information](#)
- [Stop a script that is currently running](#)

### Configure scripts to run automatically

You can configure a script or a python application to run automatically when the system restarts, at specific intervals, or at a specified time. By default, scripts execute in a "sandbox," which restricts access to the file system and available commands that can be used by the script.

#### Required configuration items

- Upload or create the script. The script must be uploaded to /etc/config/scripts or a subdirectory.
- Enable the script.
- Select whether the script should run:
  - When the device boots.
  - At a specified time.
  - At a specified interval.
  - During system maintenance.

#### Additional configuration items

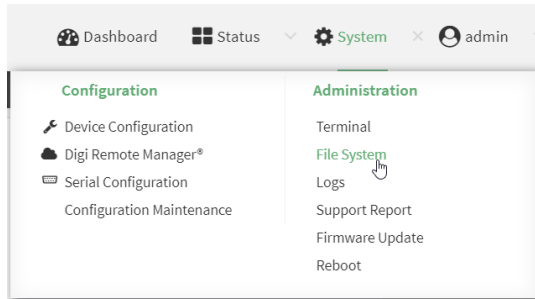
- If the script is a Python application, include the full path to the script.
- A label used to identify the script.
- The action to take if the script finishes. The actions that can be taken are:
  - None.
  - Restart the script.
  - Reboot the device.
- Whether to write the script output and errors to the system log.
- If the script is set to run at a specified interval, whether another instance of the script should be run at the specified interval if the previous instance is still running.
- The memory available to be used by the script .
- Whether the script should run one time only.

#### ***Task one: Upload the application***



Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight the **scripts** directory and click to open the directory.
3. Click (upload).
4. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, use the **scp** command to upload the Python application script to the Connect EZ device:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the **/etc/config/scripts** directory on the Connect EZ device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local
/etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                               100%   36MB   11.1MB/s   00:03
>
```

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

**Note** You can also create scripts by using the **vi** command when logged in with shell access.

### Task two: Configure the application to run automatically

**Note** This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

## Web

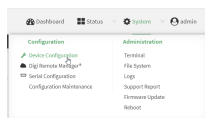
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

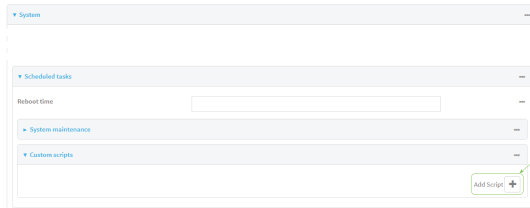
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



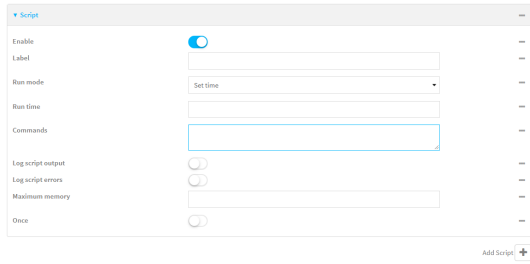
The **Configuration** window is displayed.

3. Click **System > Scheduled tasks > Custom scripts**.

4. For **Add Script**, click **+**.



The script configuration window is displayed.



Custom scripts are enabled by default. To disable, toggle off **Enable** to toggle off.

5. (Optional) For **Label**, provide a label for the script.
6. For **Run mode**, select the mode that will be used to run the script. Available options are:
- **On boot**: The script will run once each time the device boots.
    - If **On boot** is selected, select the action that will be taken when the script completes in **Exit action**. Available options are:
      - **None**: Action taken when the script exits.
      - **Restart script**: Runs the script repeatedly.
      - **Reboot**: The device will reboot when the script completes.
  - **Interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved.
    - If **Interval** is selected, in **Interval**, type the interval.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
    - Click to enable **Run single** to run only a single instance of the script at a time.  
If **Run single** is not enabled, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.
  - **Set time**: Runs the script at a specified time of the day.
    - If **Set Time** is selected, specify the time that the script should run in **Run time**, using the format **HH:MM**.
  - **During system maintenance**: The script will run during the system maintenance time window.
7. For **Commands**, type the commands that will execute the script.

- If a Python script is being used, include the full path to the Python script. For example:

---

```
python /etc/config/scripts/test.py
```

---

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).
8. Script logging options:
    - a. Click to enable **Log script output** to log the script's output to the system log.
    - b. Click to enable **Log script errors** to log script errors to the system log.

If neither option is selected, only the script's exit code is written to the system log.
  9. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{**b**|**bytes**|**KB**|**k**|**MB**|**MB**|**M**|**GB**|**G**|**TB**|**T**}.
  10. **Sandbox** is enabled by default, which restricts access to the file system and available commands that can be used by the script. This option protects the script from accidentally destroying the system it is running on.
  11. Click to enable **Once** to configure the script to run only once at the specified time.  
If **Once** is enabled, rebooting the device will cause the script to not run again. The only way to re-run the script is to:
    - Remove the script from the device and add it again.
    - Make a change to the script.
    - Uncheck **Once**.
  12. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a script:

---

```
(config)> add system schedule script end
(config system schedule script 0)>
```

---

Scheduled scripts are enabled by default. To disable:

---

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

---

4. (Optional) Provide a label for the script.

---

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

---

where *value* is any string. If spaces are used, enclose *value* within double quotes.

5. Set the mode that will be used to run the script:

---

```
(config system schedule script 0)> when mode
(config system schedule script 0)>
```

---

where *mode* is one of the following:

- **boot**: The script will run once each time the device boots.
  - If **boot** is selected, set the action that will be taken when the script completes:

---

```
(config system schedule script 0)> exit_action action
(config system schedule script 0)>
```

---

where *action* is one of the following:

- **none**: Action taken when the script exits.
  - **restart**: Runs the script repeatedly.
  - **reboot**: The device will reboot when the script completes.
- **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected:
    - Set the interval:

---

```
(config system schedule script 0)> on_interval value
(config system schedule script 0)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number**{w|d|h|m|s}.

For example, to set **on\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config system schedule script 0)> on_interval 600s
(config system schedule script 0)>
```

---

- (Optional) Configure the script to run only a single instance at a time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is set to **false**, a new instance of the script will be started at every interval, regardless of whether the script is still running from a previous interval.

- **set\_time**: Runs the script at a specified time of the day.
  - If **set\_time** is set, set the time that the script should run, using the format **HH:MM**

---

```
(config system schedule script 0)> run_time HH:MM
(config system schedule script 0)>
```

---

- **maintenance\_time**: The script will run during the system maintenance time window.

## 6. Set the commands that will execute the script:

---

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

---

where *filename* is the path and filename of the script, and any related command line information.

- If a Python script is being used, include the full path to the Python script and enclose in quotation marks. For example:

---

```
(config system schedule script 0)> commands python
"/etc/config/scripts/test.py"
(config system schedule script 0)>
```

---

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

## 7. Script logging options:

- To log the script's output to the system log:

---

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

---

- To log script errors to the system log:

---

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

---

If **syslog\_stdout** and **syslog\_stderr** are not enabled, only the script's exit code is written to the system log.

## 8. Set the maximum amount of memory available to be used by the script and its subprocesses:

---

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

---

where *value* uses the syntax **number{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}**.

## 9. To run the script only once at the specified time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:

- Remove the script from the device and add it again.
- Make a change to the script.
- Disable **once**.

10. **Sandbox** is enabled by default. This option protects the script from accidentally destroying the system it is running on.

---

```
(config system schedule script 0)> sandbox true
(config system schedule script 0)>
```

---

11. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Show script information

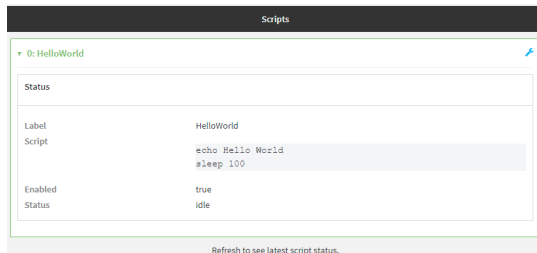
You can view status and statistics about location information from either the WebUI or the command line.

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. At the **Status** page, click **Scripts**.

The **Scripts** page displays:



### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the `show scripts` command at the system prompt:

---

```
> show scripts
```

```

Index  Label           Enabled  Status  Run time
-----  -
0      script1         true    active
1      script2         true    idle    01:00
>
```

---



3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Stop a script that is currently running

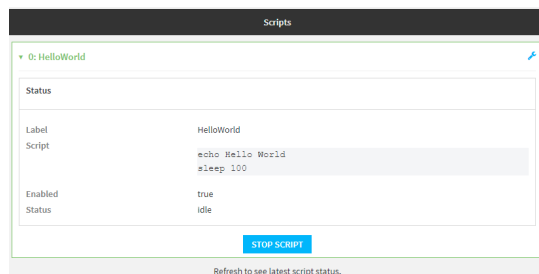
You can stop a script that is currently running.

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. At the **Status** page, click **Scripts**.

The **Scripts** page displays:



2. For scripts that are currently running, click **Stop Script** to stop the script.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Determine the name of scripts that are currently running:

```
> show scripts
```

```

Index  Label          Enabled  Status  Run time
-----  -
0      script1       true    active
1      script2       true    idle    01:00
>
```

Scripts that are currently running have the status of **active**.

3. Stop the appropriate script:

```
)> system script stop script1
>
```

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Start an interactive Python session

Use the **python** command without specifying any parameters to start an interactive Python session. The Python session operates interactively using REPL (Read Evaluate Print Loop) to allow you to write Python code on the command line.

**Note** The Python interactive session is not available from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See [Authentication groups](#) for information about configuring authentication groups that include shell access.

1. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

2. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

---

```
# python
Python 3.10.1 (main, Mar 30 2023, 23:47:13) [GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

---

3. Type Python commands at the Python prompt. For example, to view help for the digidevice module, type:

---

```
>>> help("digidevice")
Help on package digidevice:

NAME
    digidevice - Digi device python extensions

DESCRIPTION
    This module includes various extensions that allow Python
    to interact with additional features offered by the device.
    ...
```

---

4. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

## Run a Python application at the shell prompt

Python applications can be run from a file at the shell prompt. The Python application will run until it completes, displaying output and prompting for additional user input if needed. To interrupt the application, enter **CTRL-C**.

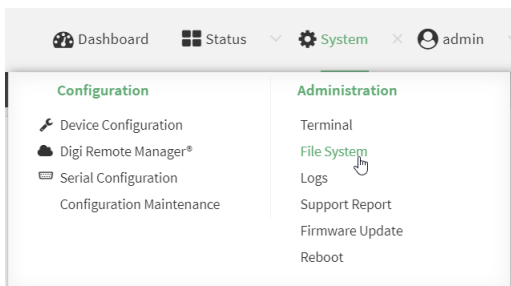
**Note** Python applications cannot be run from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See [Authentication groups](#) for information about configuring authentication groups that include shell access.

1. Upload the Python application to the Connect EZ device:

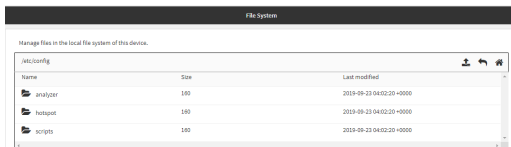
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

- a. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



- b. Highlight the **scripts** directory and click to open the directory.
- c. Click (upload).
- d. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

### Command line

- a. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- b. At the command line, use the **scp** command to upload the Python application script to the Connect EZ device:

---

```
> scp host hostname-or-ip user username remote remote-path local
local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the /etc/config/scripts directory on the Connect EZ device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local
/etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                               100%   36MB   11.1MB/s   00:03
>
```

---

c. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

---

**Note** You can also create scripts by using the **vi** command when logged in with shell access.

---

2. Select a device in Remote Manager that is configured to allow shell access to the admin user, and click **Actions > Open Console**. Alternatively, log into the Connect EZ local command line as a user with shell access.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **shell** to access the device shell.

3. Use the **python** command to run the Python application. In the following example, the Python application, **test.py**, takes 3 parameters: **120**, **ports** and **storage**:

---

```
# python /etc/config/scripts/test.py 120 ports storage
```

---

## Configure scripts to run manually

You can configure an scripts to be manually run.

### **Required configuration items**

- Upload or create the script.
- Enable the script.
- Set the script to run manually.

### Additional configuration items

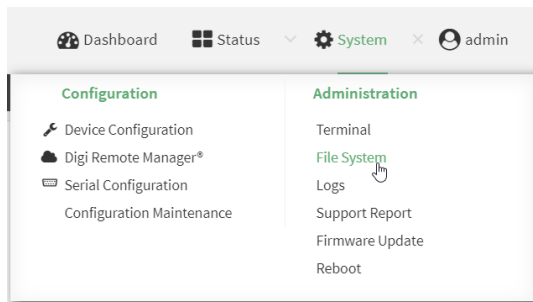
- A label used to identify the script.
- The arguments for the script.
- Whether to write the script output and errors to the system log.
- The memory available to be used by the script.
- Whether the script should run one time only.

## Task one: Upload the application

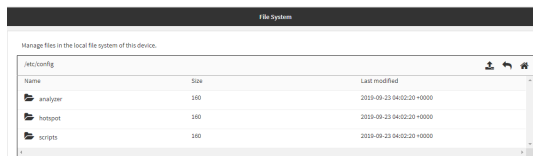
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight the **scripts** directory and click to open the directory.
3. Click (upload).
4. Browse to the location of the script on your local machine. Select the file and click **Open** to upload the file.

The uploaded file is uploaded to the **/etc/config/scripts** directory.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, use the **scp** command to upload the Python application script to the Connect EZ device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

To upload a script from a remote host with an IP address of 192.168.4.1 to the `/etc/config/scripts` directory on the Connect EZ device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/test.py local
/etc/config/scripts/ to local
admin@192.168.4.1's password: adminpwd
test.py                100%   36MB   11.1MB/s   00:03
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

---

**Note** You can also create scripts by using the **vi** command when logged in with shell access.

---

## Task two: Configure the application to run automatically

**Note** This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

---

### Web

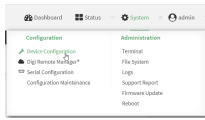
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

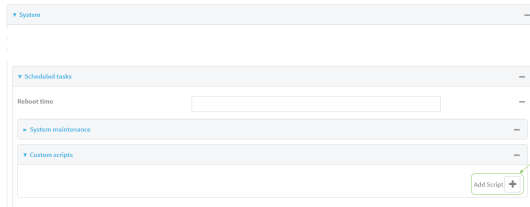
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

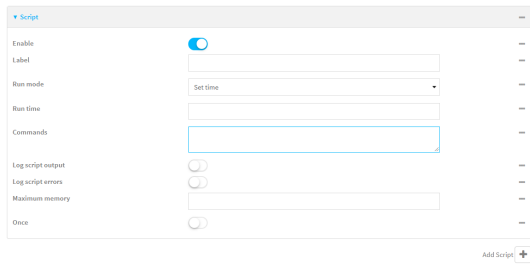


The **Configuration** window is displayed.

3. Click **System > Scheduled tasks > Custom scripts**.
4. For **Add Script**, click **+**.



The script configuration window is displayed.



Custom scripts are enabled by default. To disable, toggle off **Enable** to toggle off.

5. (Optional) For **Label**, provide a label for the script.
6. For **Run mode**, select **Manual**.
7. For **Commands**, type the commands that will execute the script.
  - If a Python script is being used, include the full path to the Python script. For example:
 

```
python /etc/config/scripts/test.py
```
  - If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).
8. Script logging options:
  - a. Click to enable **Log script output** to log the script's output to the system log.
  - b. Click to enable **Log script errors** to log script errors to the system log.

If neither option is selected, only the script's exit code is written to the system log.
9. For **Maximum memory**, enter the maximum amount of memory available to be used by the script and its subprocesses, using the format *number*{**b**|**bytes**|**KB**|**k**|**MB**|**M**|**GB**|**G**|**TB**|**T**}.
10. **Sandbox** is enabled by default, which restricts access to the file system and available commands that can be used by the script. This option protects the script from accidentally destroying the system it is running on.

11. Click to enable **Once** to configure the script to run only once at the specified time.  
If **Once** is enabled, rebooting the device will cause the script to not run again. The only way to re-run the script is to:
  - Remove the script from the device and add it again.
  - Make a change to the script.
  - Uncheck **Once**.
12. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a script:

```
(config)> add system schedule script end
(config system schedule script 0)>
```

Scheduled scripts are enabled by default. To disable:

```
(config system schedule script 0)> enable false
(config system schedule script 0)>
```

4. (Optional) Provide a label for the script.

```
(config system schedule script 0)> label value
(config system schedule script 0)>
```

where *value* is any string. if spaces are used, enclose *value* within double quotes.

5. Set the run mode to manual:

```
(config system schedule script 0)> when manual
(config system schedule script 0)>
```

6. Set the commands that will execute the script:

```
(config system schedule script 0)> commands filename
(config system schedule script 0)>
```

where *filename* is the path and filename of the script, and any related command line information.

- If a Python script is being used, include the full path to the Python script and enclose in quotation marks. For example:



---

```
(config system schedule script 0)> commands python
"/etc/config/scripts/test.py"
(config system schedule script 0)>
```

---

- If the script begins with **#!**, then the script will be invoked in the location specified by the path for the script command. Otherwise, the default shell will be used (equivalent to **#!/bin/sh**).

7. Script logging options:

- To log the script's output to the system log:

---

```
(config system schedule script 0)> syslog_stdout true
(config system schedule script 0)>
```

---

- To log script errors to the system log:

---

```
(config system schedule script 0)> syslog_stderr true
(config system schedule script 0)>
```

---

If **syslog\_stdout** and **syslog\_stderr** are not enabled, only the script's exit code is written to the system log.

8. Set the maximum amount of memory available to be used by the script and its subprocesses:

---

```
(config system schedule script 0)> max_memory value
(config system schedule script 0)>
```

---

where *value* uses the syntax **number**{b|bytes|KB|k|MB|MB|M|GB|G|TB|T}.

9. To run the script only once at the specified time:

---

```
(config system schedule script 0)> once true
(config system schedule script 0)>
```

---

If **once** is enabled, rebooting the device will cause the script to run again. The only way to re-run the script is to:

- Remove the script from the device and add it again.
- Make a change to the script.
- Disable **once**.

10. **Sandbox** is enabled by default. This option protects the script from accidentally destroying the system it is running on.

---

```
(config system schedule script 0)> sandbox true
(config system schedule script 0)>
```

---

11. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- 12. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Start a manual script

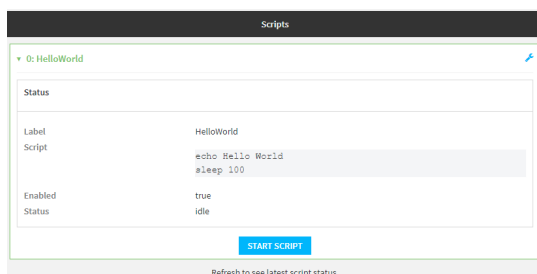
You can start a script that is enabled and configured to have a run mode of **Manual**.

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

- 1. At the **Status** page, click **Scripts**.

The **Scripts** page displays:



- 2. For scripts that are enabled and configured to have a run mode of **Manual**, click **Start Script** to start the script.

### Command line

- 1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- 2. Determine the name of scripts that are currently running:

```
> show scripts
```

| Index | Label   | Enabled | Status | Run time |
|-------|---------|---------|--------|----------|
| 0     | script1 | true    | active |          |
| 1     | script2 | true    | idle   | 01:00    |

```
>
```

- 3. Start the script:

```
)> system script start script1
>
```

4. Save the configuration and apply the change

---

```
(config)> save  
Configuration saved.  
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## User authentication

---

This chapter contains the following topics:

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| Connect EZ user authentication .....                                  | 509 |
| User authentication methods .....                                     | 509 |
| Authentication groups .....                                           | 516 |
| Local users .....                                                     | 526 |
| Terminal Access Controller Access-Control System Plus (TACACS+) ..... | 540 |
| Remote Authentication Dial-In User Service (RADIUS) .....             | 547 |
| LDAP .....                                                            | 552 |
| Disable shell access .....                                            | 560 |
| Set the idle timeout for Connect EZ users .....                       | 562 |
| Example user configuration .....                                      | 564 |

## Connect EZ user authentication

User authentication on the Connect EZ has the following features and default configuration:

| Feature             | Description                                                                                                                                                                                                                                                                                                      | Default configuration                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Idle timeout</b> | Determines how long a user session can be idle before the system automatically disconnects.                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>10 minutes</li> </ul>                                                                                                                                                       |
| <b>Allow shell</b>  | <p>If disabled, prevents all authentication prohibits access to the shell prompt for all authentication groups. This does not prevent access to the Admin CLI.</p> <hr/> <p><b>Note</b> If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.</p> <hr/> | <ul style="list-style-type: none"> <li>Enabled</li> </ul>                                                                                                                                                          |
| <b>Methods</b>      | Determines how users are authenticated for access: <b>local users</b> , <b>TACACS+</b> , or <b>RADIUS</b> .                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li><b>local users</b></li> </ul>                                                                                                                                               |
| <b>Groups</b>       | Associates access permissions for a group. . You can modify the released groups and create additional groups as needed for your site. A user can be assigned to more than one group.                                                                                                                             | <ul style="list-style-type: none"> <li><b>admin:</b> Provides the logged-in user with administrative and shell access.</li> <li><b>serial:</b> Provides the logged-in user with access to serial ports.</li> </ul> |
| <b>Users</b>        | Defines local users for the Connect EZ.                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li><b>admin:</b> Belongs to both the <b>admin</b> and <b>serial</b> groups.</li> </ul>                                                                                         |
| <b>TACACS+</b>      | Configures support for TACACS+ (Terminal Access Controller Access-Control System Plus) servers and users.                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>Not configured</li> </ul>                                                                                                                                                   |
| <b>RADIUS</b>       | Configures support for RADIUS (Remote Authentication Dial-In User Service) servers and users.                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>Not configured</li> </ul>                                                                                                                                                   |
| <b>LDAP</b>         | Configures support for LDAP (Lightweight Directory Access Protocol) servers and users.                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>Not configured</li> </ul>                                                                                                                                                   |
| <b>Serial</b>       | Configures authentication for serial TCP and autoconnect services.                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>Not configured</li> </ul>                                                                                                                                                   |

## User authentication methods

Authentication methods determine how users of the Connect EZ device are authenticated. Available authentication methods are:

- **Local users:** User are authenticated on the local device.
- **RADIUS:** Users authenticated by using a remote RADIUS server for authentication.  
See [Remote Authentication Dial-In User Service \(RADIUS\)](#) for information about configuring RADIUS authentication.
- **TACACS+:** Users authenticated by using a remote TACACS+ server for authentication.  
See [Terminal Access Controller Access-Control System Plus \(TACACS+\)](#) for information about configuring TACACS+ authentication.
- **LDAP:** Users authenticated by using a remote LDAP server for authentication.  
See [LDAP](#) for information about configuring LDAP authentication.

## Add a new authentication method

### Required configuration items

- The types of authentication method to be used:

To add an authentication method:

### Web

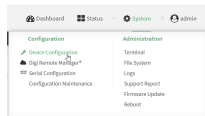
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

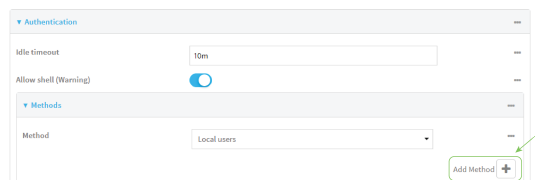
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

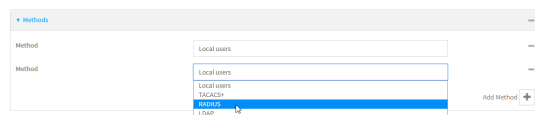


The **Configuration** window is displayed.

3. Click **Authentication > Methods**.
4. For **Add Method**, click **+**.



5. Select the appropriate authentication type for the new method from the **Method** drop-down.



---

**Note** Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. See [Rearrange the position of authentication methods](#) for information about how to reorder the authentication methods.

---

6. Repeat these steps to add additional methods.
7. Click **Apply** to save the configuration and apply the change.

### **Command line**

Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This procedure describes how to add methods to various places in the list.

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add the new authentication method to the appropriate location in the list:

- To determine the current list of authentication methods:

- a. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- b. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

- c. Use the **show auth method** command to display the current authentication methods configuration:

---

```
(config)> show auth method
0 local
(config)>
```

---

- To add the new authentication method to the beginning of the list, use the index value of **0** to indicate that it should be added as the first method:

---

```
(config)> add auth method 0 auth_type
(config)>
```

---

where *auth\_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.

- To add the new authentication method to the end of the list, use the index keyword **end**:



```
(config)> add auth method end auth_type
(config)>
```

where *auth\_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.

- To add the new authentication in another location in the list, use an index value to indicate the appropriate position. For example:

```
(config)> add auth method 1 auth_type
(config)>
```

where *auth\_type* is one of **local**, **radius**, **tacacs+**, or **ldap**.

- You can also use the **move** command to rearrange existing methods. See [Rearrange the position of authentication methods](#) for information about how to reorder the authentication methods.

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete an authentication method

### Web

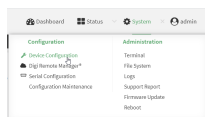
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

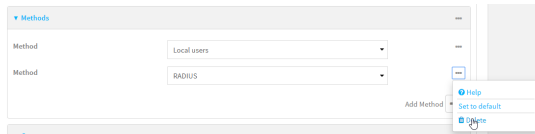
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Methods**.
4. Click the menu icon (...) next to the method and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **show auth method** command to determine the index number of the authentication method to be deleted:

```
(config)> show auth method
0 local
1 radius
2 tacacs+
(config)>
```

4. Delete the appropriate authentication method:

```
(config)> del auth method n
```

Where *n* is index number of the authentication method to be deleted. For example, to delete the TACACS+ authentication method as displayed by the example **show** command, above:

```
(config)> del auth method 2
```

5. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

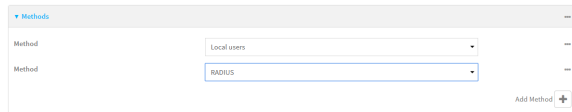
6. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Rearrange the position of authentication methods

## Web

Authentication methods are reordered by changing the method type in the **Method** drop-down for each authentication method to match the appropriate order.

For example, the following configuration has **Local users** as the first method, and **RADIUS** as the second.



To reorder these so that **RADIUS** is first and **Local users** is second:

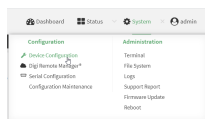
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

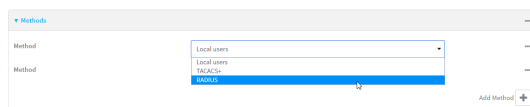
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

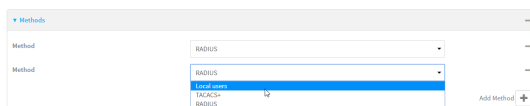


The **Configuration** window is displayed.

3. Click to expand the first **Method**.
4. In the **Method** drop-down, select **RADIUS**.



5. Click to expand the second **Method**.
6. In the **Method** drop-down, select **Local users**.



7. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Use the **show** command to display current configuration:

---

```
(config)> show auth method
0 local
1 radius
(config)>
```

---

4. Use the **move** command to rearrange the methods:

---

```
(config)> move auth method 1 0
(config)>
```

---

5. Use the **show** command again to verify the change:

---

```
(config)> show auth method
0 radius
1 local
(config)>
```

---

6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Authentication groups

Authentication groups are used to assign access rights to Connect EZ users. Three types of access rights can be assigned:

- **Admin access:** Users with Admin access can be configured to have either:
  - The ability to manage the Connect EZ device by using the WebUI or the Admin CLI.
  - Read-only access to the WebUI and Admin CLI.
- **Shell access:** Users with Shell access have the ability to access the shell when logging into the Connect EZ via ssh, telnet, or the serial console.  
Shell access is not available if the **Allow shell** parameter has been disabled. See [Disable shell access](#) for more information about the **Allow shell** parameter.

- **Serial access:** Users with Serial access have the ability to log into the Connect EZ device by using the serial console.

### ***Preconfigured authentication groups***

The Connect EZ device has two preconfigured authentication groups:

- The **admin** group is configured by default to have full **Admin access**.
- The **serial** group is configured by default to have **Serial access**.

The preconfigured authentication groups cannot be deleted, but the access rights defined for the group are configurable.

This section contains the following topics:

|                                                       |     |
|-------------------------------------------------------|-----|
| Change the access rights for a predefined group ..... | 518 |
| Add an authentication group .....                     | 520 |
| Delete an authentication group .....                  | 524 |

## Change the access rights for a predefined group

By default, two authentication groups are predefined: **admin** and **serial**. To change the access rights of the predefined groups:

### Web

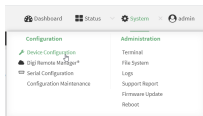
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Groups**.
4. Click the authentication group to be changed, either **admin** or **serial**, to expand its configuration node.
5. Click the box next to the following options, as appropriate, to enable or disable access rights for each:

- **Admin access**

For groups assigned Admin access, you can also determine whether the **Access level** should be **Full access** or **Read-only access**.

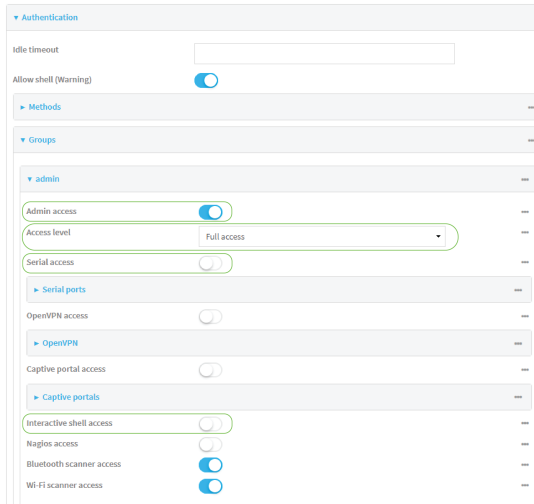
- **Full access** provides users of this group with the ability to manage the Connect EZ device by using the WebUI or the Admin CLI.
- **Read-only access** provides users of this group with read-only access to the WebUI and Admin CLI.

The default is **Full access**.

- **Serial access**

- **Interactive shell access**

Shell access is not available if the **Allow shell** parameter has been disabled. See [Disable shell access](#) for more information about the **Allow shell** parameter.



6. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable or disable access rights for the group. For example:

- Admin access:

- To set the access level for Admin access of the **admin** group:

---

```
(config)> auth group admin acl admin level value
(config)>
```

---

where *value* is either:

- **full**: provides users of this group with the ability to manage the Connect EZ device by using the WebUI or the Admin CLI.
- **read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

The default is **full**.

- To disable Admin access for the **admin** group:

---

```
(config)> auth group admin acl admin enable false
(config)>
```

---

- Shell access:

- To enable Shell access for the **serial** group:

---

```
(config)> auth group serial acl shell enable true
(config)>
```

---

Shell access is not available if the **Allow shell** parameter has been disabled. See [Disable shell access](#) for more information about the **Allow shell** parameter.

- Serial access:
  - To enable Serial access for the **admin** group:

---

```
(config)> auth group admin acl serial enable true
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Add an authentication group

### Required configuration items

- The access rights to be assigned to users that are assigned to this group.

### Additional configuration items

- Access rights to OpenVPN tunnels, and the tunnels to which they have access.
- Access rights to captive portals, and the portals to which they have access.
- Access rights to query the device for Nagios monitoring.

To add an authentication group:

### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

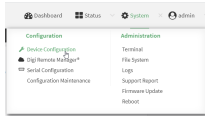
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.



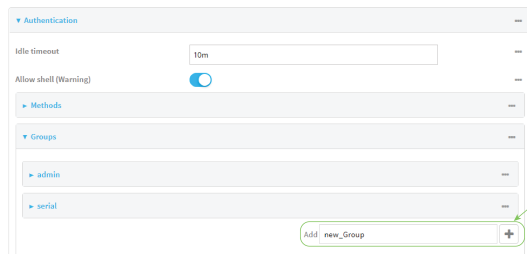
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

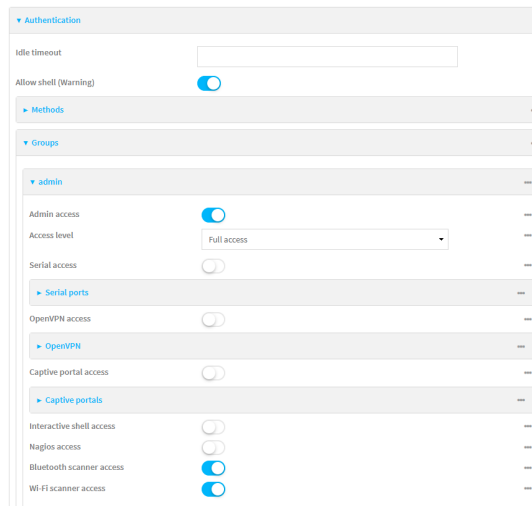


The **Configuration** window is displayed.

3. Click **Authentication > Groups**.
4. For **Add**, type a name for the group and click **+**.



The group configuration window is displayed.



5. Click the following options, as appropriate, to enable or disable access rights for each:

- **Admin access**

For groups assigned **Admin access**, you can also determine whether the **Access level** should be **Full access** or **Read-only access**.

where *value* is either:

- **Full access full**: provides users of this group with the ability to manage the Connect EZ device by using the WebUI or the Admin CLI.
- **Read-only access read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

The default is **Full access full**.

- **Serial access**
- 6. (Optional) Configure OpenVPN access. See for further information.
- 7. (Optional) Configure captive portal access:
  - a. Enable captive portal access rights for users of this group by checking the box next to **Captive portal access**.
  - b. Click **Captive portals** to expand the **Captive portal** node.
  - c. For **Add Captive portal**, click **+**.
  - d. In the **Captive portal** dropdown, select a captive portal to which users of this group will have access.
  - e. Click **+** again to add additional captive portals.
- 8. **Interactive shell access**  
Shell access is not available if the **Allow shell** parameter has been disabled. See [Disable shell access](#) for more information about the **Allow shell** parameter.
- 9. (Optional) Enable users that belong to this group to query the device for Nagios monitoring by checking the box next to **Nagios access**.
- 10. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Use the **add auth group** command to add a new authentication. For example, to add a group named **test**:

---

```
(config)> add auth group test
(config auth group test)>
```

---

4. Enable access rights for the group:

- Admin access:

---

```
(config auth group test)> acl admin enable true
(config)>
```

---

- Set the access level for Admin access:

---

```
(config)> auth group admin acl admin level value
(config)>
```

---

where *value* is either:

- **full**: provides users of this group with the ability to manage the Connect EZ device by using the WebUI or the Admin CLI.

- **read-only**: provides users of this group with read-only access to the WebUI and Admin CLI.

The default is **full**.

■ Shell access:

---

```
(config auth group test)> acl shell enable true
(config)>
```

---

Shell access is not available if the **Allow shell** parameter has been disabled. See [Disable shell access](#) for more information about the **Allow shell** parameter.

■ Serial access:

---

```
(config auth group test)> acl serial enable true
(config)>
```

---

5. (Optional) Configure captive portal access:

a. Return to the config prompt by typing three periods (...):

---

```
(config auth group test)> ...
(config)>
```

---

b. Enable captive portal access rights for users of this group:

---

```
(config)> auth group test acl portal enable true
(config)>
```

---

c. Add a captive portal to which users of this group will have access:

i. Determine available portals:

---

```
(config)> show firewall portal
portal1
    auth none
    enable true
    http redirect
    no interface
    no message
    no redirect_url
    no terms
    timeout 24h
    no title
(config)>
```

---

ii. Add a captive portal:

---

```
(config)> add auth group test acl portal portals end portal1
(config)>
```

---

6. (Optional) Configure Nagios monitoring:

---

```
(config)> auth group test acl nagios enable true
(config)>
```

---

7. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete an authentication group

By default, the Connect EZ device has two preconfigured authentication groups: **admin** and **serial**. These groups cannot be deleted.

To delete an authentication group that you have created:

### Web

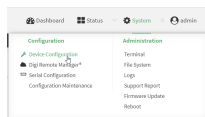
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Groups**.
4. Click the menu icon (...) next to the group to be deleted and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> del auth group groupname
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Local users

Local users are authenticated on the device without using an external authentication mechanism such as TACACS+ or RADIUS. Local user authentication is enabled by default, with one preconfigured default user.

### **Default user**

At manufacturing time, each Connect EZ device comes with a default user configured as follows:

- Username: **admin**.
- Password: The default password is displayed on the label on the bottom of the device.

---

**Note** The default password is a unique password for the device, and is the most critical security feature for the device. If you reset the device to factory defaults, you must log in using the default user and password, and you should immediately [change the password](#) to a custom password. Before deploying or mounting the Connect EZ device, record the default password, so you have the information available when you need it even if you cannot physically access the label on the bottom of the device.

---

The default **admin** user is preconfigured with both Admin and Serial access. You can configure the **admin** user account to fit with the needs of your environment.

This section contains the following topics:

|                                      |     |
|--------------------------------------|-----|
| Change a local user's password ..... | 527 |
| Configure a local user .....         | 529 |
| Delete a local user .....            | 537 |

## Change a local user's password

To change a user's password:

### Web

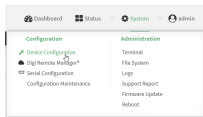
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

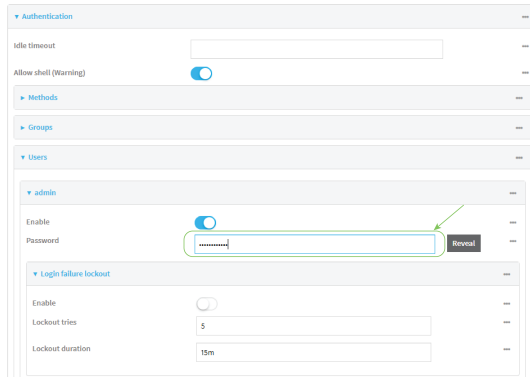


The **Configuration** window is displayed.

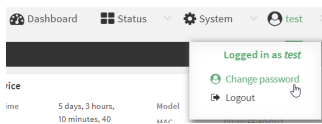
3. Click **Authentication > Users**.
4. Click the username to expand the user's configuration node.
5. For **Password**, enter the new password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

For the **admin** user, the password field can be left blank:

- If the password field for the **admin** user is left blank, the **admin** user's password will be the default password printed on the device's label.
- If the **admin** user's password has been changed from the default and the configuration saved, if you then clear the password field for the **admin** user, this will result in the device's configuration being erased and reset to the default configuration.



You can also change the password for the active user by clicking the user name in the menu bar:



The active user must have full Admin access rights to be able to change the password.

6. Click **Apply** to save the configuration and apply the change.



## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> auth user username password pwd
```

---

Where:

- *username* is the name of the user.
  - *pwd* is the new password for the user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.
4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure a local user

### Required configuration items

- A username.
- A password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character. For security reasons, passwords are stored in hash form. There is no way to get or display passwords in clear-text form, although prior to saving the configuration, the password can be shown by clicking **Reveal**.
- The authentication group or groups from which the user will inherit access rights. See [Authentication groups](#) for information about configuring groups.

### Additional configuration items

- An alias for the user. Because the username cannot contain any special characters, such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters.
- The number of unsuccessful login attempts before the user is locked out of the system.

- The amount of time that the user is locked out of the system after the specified number of unsuccessful login attempts.
- An optional public ssh key, to authenticate the user when using passwordless SSH login.
- Two-factor authentication information for user login over SSH, telnet, and the serial console:
  - The verification type for two-factor authentication: Either time-based or counter-based.
  - The security key.
  - Whether to allow passcode reuse (time based verification only).
  - The passcode refresh interval (time based verification only).
  - The valid code window size.
  - The login limit.
  - The login limit period.
  - One-time use eight-digit emergency scratch codes.

To configure a local user:

## ≡ Web

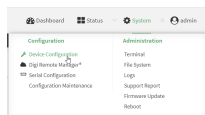
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

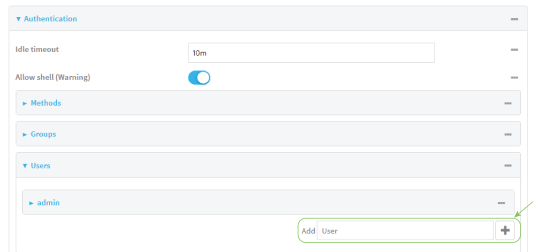
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



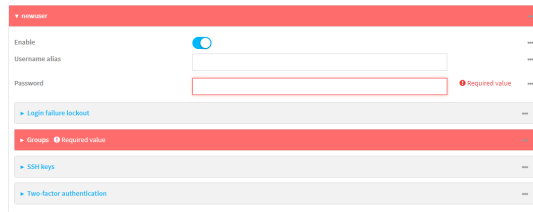
The **Configuration** window is displayed.

3. Click **Authentication > Users**.

- In **Add User**, type a name for the user and click **+**.



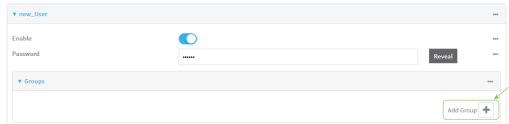
The user configuration window is displayed.



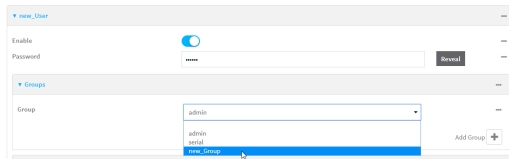
The user is enabled by default. To disable, toggle off **Enable**.

- (Optional) For **Username alias**, type an alias for the user.  
Because the name used to create the user and cannot contain special characters such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters. For security purposes, if two users have the same alias, the alias will be disabled.
- Enter a password for the user. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.
- Click to expand **Login failure lockout**.  
The login failure lockout feature is enabled by default. To disable, toggle off **Enable**.
  - For **Lockout tries**, type the number of unsuccessful login attempts before the user is locked out of the device. The default is **5**.
  - For **Lockout duration**, type the amount of time that the user is locked out after the number of unsuccessful login attempts defined in **Lockout tries**.  
Allowed values are any number of minutes, or seconds, and take the format **number{m|s}**.  
For example, to set **Lockout duration** to ten minutes, enter **10m** or **600s**.  
The minimum value is 1 second, and the maximum is 15 minutes. The default is 15 minutes.
- Add groups for the user.  
Groups define user access rights. See [Authentication groups](#) for information about configuring groups.

- a. Click to expand **Groups**.
- b. For **Add Group**, click **+**.



- c. For **Group**, select an appropriate group.

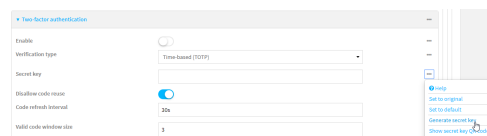



---

**Note** Every user must be configured with at least one group. You can add multiple groups to a user by clicking **Add** again and selecting the next group.

---

9. (Optional) Add SSH keys for the user to use passwordless SSH login:
  - a. Click **SSH keys**.
  - b. In **Add SSH key**, paste or type a public encryption key that this user can use for passwordless SSH login and click **+**.
10. (Optional) Configure two-factor authentication for SSH, telnet, and serial console login:
  - a. Click **Two-factor authentication**.
  - b. Check **Enable** to enable two-factor authentication for this user.
  - c. Select the **Verification type**:
    - **Time-based (TOTP)**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
    - **Counter-based (HOTP)**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.
  - d. Generate a **Secret key**:
    - i. Click ... next to the field label and select **Generate secret key**.



- ii. Copy the secret key for use with an application or mobile device to generate passcodes.
  - e. For time-based verification only, select **Disallow code reuse** to prevent a code from being used more than once during the time that it is valid.
  - f. For time-based verification only, in **Code refresh interval**, type the amount of time that a code will remain valid.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**. For example, to set **Code refresh interval** to ten minutes, enter **10m** or **600s**.

- g. In **Valid code window size**, type the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the **Valid code window size** may be necessary when the clocks used by the server and client are not synchronized.
  - h. For **Login limit**, type the number of times that the user is allowed to attempt to log in during the **Login limit period**. Set **Login limit** to **0** to allow an unlimited number of login attempts during the **Login limit period**.
  - i. For **Login limit period**, type the amount of time that the user is allowed to attempt to log in.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**. For example, to set **Login limit period** to ten minutes, enter **10m** or **600s**.
  - j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:
    - i. Click **Scratch codes**.
    - ii. For **Add Code**, click **+**.
    - iii. For **Code**, enter the scratch code. The code must be eight digits, with a minimum of 10000000.
    - iv. Click **+** again to add additional scratch codes.
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a user. For example, to create a user named **new\_user**:

```
(config)> add auth user new_user
(config auth user new_user)>
```

The user is enabled by default. To disable the user, type:

```
(config auth user new_user)> enable false
(config auth user new_user)>
```

4. (Optional) Create a username alias for the user.

Because the name to create the user cannot contain special characters such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters. For security purposes, if two users have the same alias, the alias will be disabled.

```
(config auth user new_user> username username_alias
(config auth user new_user)>
```

5. Set the user's password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

---

```
(config auth user new_user> password pwd
(config auth user new_user)>
```

---

6. Configure login failure lockout settings:

The login failure lockout feature is enabled by default. To disable:

---

```
(config auth user new_user> lockout enable false
(config auth user new_user)>
```

---

- a. Set the number of unsuccessful login attempts before the user is locked out of the device. where *value* is any integer. The minimum value is **1**, and the default value is **5**.
- b. Set the amount of time that the user is locked out after the number of unsuccessful login attempts defined in **lockout tries**:

---

```
(config auth user new_user> lockout duration value
(config auth user new_user)>
```

---

where *value* is any number of minutes, or seconds, and takes the format **number{m|s}**.

For example, to set **duration** to ten minutes, enter either **10m** or **600s**:

---

```
(config auth user new_user)> lockout duration 600s
(config auth user new_user)>
```

---

The minimum value is 1 second, and the maximum is 15 minutes. The default is 15 minutes.

7. Add groups for the user.

Groups define user access rights. See [Authentication groups](#) for information about configuring groups.

- a. Add a group to the user. For example, to add the admin group to the user:

---

```
(config auth user new_user> add group end admin
(config auth user new_user)>
```

---

**Note** Every user must be configured with at least one group.

---

- b. (Optional) Add additional groups by repeating the add group command:

---

```
(config auth user new_user> add group end serial
(config auth user new_user)>
```

---

To remove a group from a user:

- a. Use the **show** command to determine the index number of the group to be deleted:

---

```
(config auth user new_user> show group
0 admin
1 serial
(config auth user new_user>
```

---

- b. Type the following:

---

```
(config auth user new_user)> del group n
(config auth user new_user)>
```

---

Where *n* is index number of the authentication method to be deleted. For example, to delete the serial group as displayed by the example **show** command, above:

---

```
(config auth user new_user)> del group 1
(config auth user new_user)>
```

---

8. (Optional) Add SSH keys for the user to use passwordless SSH login:

- a. Change to the user's `ssh_key` node:

---

```
(config auth user new_user)> ssh_key
(config auth user new_user ssh_key)>
```

---

- b. Add the key by using the `ssh_key` command and pasting or typing a public encryption key that this user can use for passwordless SSH login:

---

```
(config auth user new_user ssh_key)> ssh_key key
(config auth user new_user ssh_key)>
```

---

9. (Optional) Configure two-factor authentication for SSH, telnet, and serial console login:

- a. Change to the user's two-factor authentication node:

---

```
(config auth user new_user)> 2fa
(config auth user new_user 2fa)>
```

---

- b. Enable two-factor authentication for this user:

---

```
(config auth user new_user 2fa)> enable true
(config auth user new_user 2fa)>
```

---

- c. Configure the verification type. Allowed values are:

- **totp**: Time-based One-Time Password (TOTP) authentication uses the current time to generate a one-time password.
- **hotp**: HMAC-based One-Time Password (HOTP) uses a counter to validate a one-time password.

The default value is **totp**.

---

```
(config auth user new_user 2fa)> type totp
(config auth user new_user 2fa)>
```

---

- d. Add a secret key:

---

```
(config auth user new_user 2fa)> secret key
(config auth user new_user 2fa)>
```

---

This key should be used by an application or mobile device to generate passcodes.

- e. For time-based verification only, enable **disallow\_reuse** to prevent a code from being used more than once during the time that it is valid.

---

```
(config auth user new_user 2fa)> disallow_reuse true
(config auth user new_user 2fa)>
```

---

- f. For time-based verification only, configure the code refresh interval. This is the amount of time that a code will remain valid.

---

```
(config auth user new_user 2fa)> refresh_interval value
(config auth user new_user 2fa)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **refresh\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config auth user name 2fa)> refresh_interval 600s
(config auth user name 2fa)>
```

---

The default is **30s**.

- g. Configure the valid code window size. This represents the allowed number of concurrently valid codes. In cases where TOTP is being used, increasing the valid code window size may be necessary when the clocks used by the server and client are not synchronized.

---

```
(config auth user new_user 2fa)> window_size 3
(config auth user new_user 2fa)>
```

---

- h. Configure the login limit. This represents the number of times that the user is allowed to attempt to log in during the Login limit period. Set to 0 to allow an unlimited number of login attempts during the Login limit period

---

```
(config auth user new_user 2fa)> login_limit 3
(config auth user new_user 2fa)>
```

---

- i. Configure the login limit period. This is the amount of time that the user is allowed to attempt to log in.

---

```
(config auth user new_user 2fa)> login_limit_period value
(config auth user new_user 2fa)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **login\_limit\_period** to ten minutes, enter either **10m** or **600s**:

---

```
(config auth user name 2fa)> login_limit_period 600s
(config auth user name 2fa)>
```

---

The default is **30s**.

- j. Scratch codes are emergency codes that may be used once, at any time. To add a scratch code:



- i. Change to the user's scratch code node:

```
(config auth user new_user 2fa)> scratch_code
(config auth user new_user 2fa scratch_code)>
```

- ii. Add a scratch code:

```
(config auth user new_user 2fa scratch_code)> add end code
(config auth user new_user 2fa scratch_code)>
```

Where code is an digit number, with a minimum of 10000000.

- iii. To add additional scratch codes, use the **add end code** command again.

10. Save the configuration and apply the change

```
(config auth user new 2fa scratch_code)> save
Configuration saved.
>
```

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a local user

To delete a user from your Connect EZ:

### Web

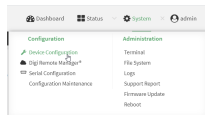
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Users**.

4. Click the menu icon (...) next to the name of the user to be deleted and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

 **Command line**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:  

---

```
> config
(config)>
```

---
3. At the config prompt, type:  

---

```
(config)> del auth user username
```

---
4. Save the configuration and apply the change  

---

```
(config)> save
Configuration saved.
>
```

---
5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Terminal Access Controller Access-Control System Plus (TACACS+)

Your Connect EZ device supports Terminal Access Controller Access-Control System Plus (TACACS+), a networking protocol that provides centralized authentication and authorization management for users who connect to the device. With TACACS+ support, the Connect EZ device acts as a TACACS+ client, which sends user credentials and connection parameters to a TACACS+ server over TCP. The TACACS+ server then authenticates the TACACS+ client requests and sends back a response message to the device.

When you are using TACACS+ authentication, you can have both local users and TACACS+ users able to log in to the device. To use TACACS+ authentication, you must set up a TACACS+ server that is accessible by the Connect EZ device prior to configuration. The process of setting up a TACACS+ server varies by the server environment.

This section contains the following topics:

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| TACACS+ user configuration .....                                   | 541 |
| TACACS+ server failover and fallback to local authentication ..... | 542 |
| Configure your Connect EZ device to use a TACACS+ server .....     | 542 |

## TACACS+ user configuration

When configured to use TACACS+ support, the Connect EZ device uses a remote TACACS+ server for user authentication (password verification) and authorization (assigning the access level of the user). Additional TACACS+ servers can be configured as backup servers for user authentication.

This section outlines how to configure a TACACS+ server to be used for user authentication on your Connect EZ device.

### Example TACACS+ configuration

With TACACS+, users are defined in the server configuration file. On Ubuntu, the default location and filename for the server configuration file is `/etc/tacacs+/tac_plus.conf`.

**Note** TACACS+ configuration, including filenames and locations, may vary depending on your platform and installation. This example assumes a Ubuntu installation.

To define users:

1. Open the TACACS+ server configuration file in a text editor. For example:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

2. Add users to the file using the following format. This example will create two users, one with admin and serial access, and one with only serial access.

```
user = user1 {
    name = "User1 for Connect EZ"
    pap = cleartext password1
    service = system {
        groupname = admin,serial
    }
}
user = user2 {
    name = "User2 for Connect EZ"
    pap = cleartext password2
    service = system {
        groupname = serial
    }
}
```

The **groupname** attribute is optional. If used, the value must correspond to authentication groups configured on your Connect EZ. Alternatively, if the user is also configured as a local user on the Connect EZ device and the LDAP server authenticates the user but does not return any groups, the local configuration determines the list of groups. See [Authentication groups](#) for more information about authentication groups. The **groupname** attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

```
$ sudo tac_plus -C /etc/tacacs+/tac_plus.conf -P
```

If successful, this command will echo the configuration file to standard out. If the command encounters any syntax errors, a message similar to this will display:

---

```
Error: Unrecognised token on line 1
```

---

5. Restart the TACACS+ server:

---

```
$ sudo /etc/init.d/tacacs_plus restart
```

---

## TACACS+ server failover and fallback to local authentication

In addition to the primary TACACS+ server, you can also configure your Connect EZ device to use backup TACACS+ servers. Backup TACACS+ servers are used for authentication requests when the primary TACACS+ server is unavailable.

### *Falling back to local authentication*

With user authentication methods, you can configure your Connect EZ device to use multiple types of authentication. For example, you can configure both TACACS+ authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup TACACS+ servers are unavailable. Additionally, users who are configured locally but are not configured on the TACACS+ server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the TACACS+ server, and only authenticated locally if the TACACS+ server is unavailable or if the user is not defined on the TACACS+ server, then you should list the TACACS+ authentication method prior to the Local users authentication method.

See [User authentication methods](#) for more information about authentication methods.

If the TACACS+ servers are unavailable and the Connect EZ device falls back to local authentication, only users defined locally on the device are able to log in. TACACS+ users cannot log in until the TACACS+ servers are brought back online.

## Configure your Connect EZ device to use a TACACS+ server

This section describes how to configure a Connect EZ device to use a TACACS+ server for authentication and authorization.

### Required configuration items

- Define the TACACS+ server IP address or domain name.
- Define the TACACS+ server shared secret.
- The group attribute configured in the TACACS+ server configuration.
- The service field configured in the TACACS+ server configuration.
- Add TACACS+ as an authentication method for your Connect EZ device.

### Additional configuration items

- Whether other user authentication methods should be used in addition to the TACACS+ server, or if the TACACS+ server should be considered the authoritative login method.
- Enable command authorization, so that the device will communicate with the TACACS+ server to determine if the user is authorized to execute a specific command.
- Enable command accounting, so that the device will communicate with the TACACS+ server to log commands that the user executes.

- The TACACS+ server port. It is configured to 49 by default.
- Add additional TACACS+ servers in case the first TACACS+ server is unavailable.

## Web

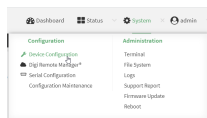
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

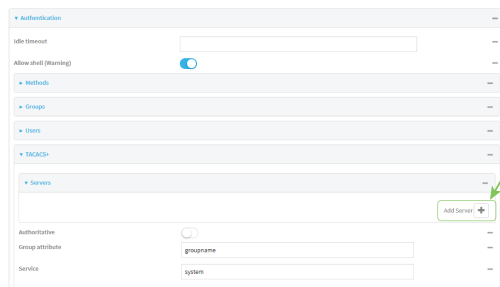
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > TACACS+ > Servers**.
4. Add TACACS+ servers:
  - a. For **Add server**, click **+**.

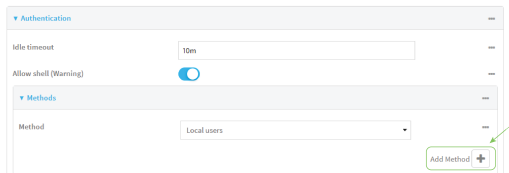


- b. For **Hostname**, type the hostname or IP address of the TACACS+ server.
- c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 49.
- d. For **Secret**, type the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's `tac_plus.conf` file, for example:

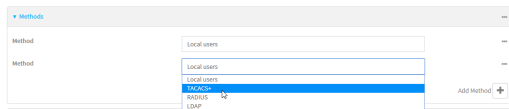
```
key = testing123
```

**Note** DAL authentication does not support the use of the # character in the key (e.g., DAL#123;&). If included, the server will be unable to decipher the request.

- e. (Optional) Click **+** again to add additional TACACS+ servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if TACACS+ login fails.
6. (Optional) For **Group attribute**, type the name of the attribute used in the TACACS+ server's configuration to identify the Connect EZ authentication group or groups that the user is a member of. For example, in [TACACS+ user configuration](#), the group attribute in the sample tac\_plus.conf file is **groupname**, which is also the default setting in the Connect EZ configuration.
7. (Optional) For **Service**, type the value of the **service** attribute in the the TACACS+ server's configuration. For example, in [TACACS+ user configuration](#), the value of the **service** attribute in the sample tac\_plus.conf file is **system**, which is also the default setting in the Connect EZ configuration.
8. (Optional) Enable **Command authorization**, which instructs the device to communicate with the TACACS+ server to determine if the user is authorized to execute a specific command. Only the first configured TACACS+ server will be used for command authorization.
9. (Optional) Enable **Command accounting**, which instructs the device to communicate with the TACACS+ server to log commands that the user executes. Only the first configured TACACS+ server will be used for command accounting.
10. Add TACACS+ to the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. For **Add method**, click **+**.



- c. Select **TACACS+** for the new method from the **Method** drop-down.



Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See [Rearrange the position of authentication methods](#) for information about rearranging the position of the methods in the list.

11. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.



2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. (Optional) Prevent other authentication methods from being used if TACACS+ authentication fails. Other authentication methods will only be used if the TACACS+ server is unavailable.

---

```
(config)> auth tacacs+ authoritative true
(config)>
```

---

4. (Optional) Configure the `group_attribute`. This is the name of the attribute used in the TACACS+ server's configuration to identify the Connect EZ authentication group or groups that the user is a member of. For example, in [TACACS+ user configuration](#), the group attribute in the sample `tac_plus.conf` file is **groupname**, which is also the default setting for the `group_attribute` in the Connect EZ configuration.

---

```
(config)> auth tacacs+ group_attribute attribute-name
(config)>
```

---

5. (Optional) Configure the type of service. This is the value of the **service** attribute in the the TACACS+ server's configuration. For example, in [TACACS+ user configuration](#), the value of the **service** attribute in the sample `tac_plus.conf` file is **system**, which is also the default setting in the Connect EZ configuration.

---

```
(config)> auth tacacs+ service service-name
(config)>
```

---

6. (Optional) Enable command authorization, which instructs the device to communicate with the TACACS+ server to determine if the user is authorized to execute a specific command. Only the first configured TACACS+ server will be used for command authorization.

---

```
(config)> auth tacacs+ command_authorization true
(config)>
```

---

7. (Optional) Enable command accounting, which instructs the device to communicate with the TACACS+ server to log commands that the user executes. Only the first configured TACACS+ server will be used for command accounting.

---

```
(config)> auth tacacs+ command_accounting true
(config)>
```

---

8. Add a TACACS+ server:

- a. Add the server:

---

```
(config)> add auth tacacs+ server end
(config auth tacacs+ server 0)>
```

---

- b. Enter the TACACS+ server's IP address or hostname:

---

```
(config auth tacacs+ server 0)> hostname hostname|ip-address
(config auth tacacs+ server 0)>
```

---

- c. (Optional) Change the default port setting to the appropriate port:

---

```
(config auth tacacs+ server 0)> port port
(config auth tacacs+ server 0)>
```

---

- d. (Optional) Repeat the above steps to add additional TACACS+ servers.
9. Add TACACS+ to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add TACACS+ to the end of the list. See [User authentication methods](#) for information about adding methods to the beginning or middle of the list.

---

```
(config)> add auth method end tacacs+
(config)>
```

---

10. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Remote Authentication Dial-In User Service (RADIUS)

Your Connect EZ device supports Remote Authentication Dial-In User Service (RADIUS), a networking protocol that provides centralized authentication and authorization management for users who connect to the device. With RADIUS support, the Connect EZ device acts as a RADIUS client, which sends user credentials and connection parameters to a RADIUS server over UDP. The RADIUS server then authenticates the RADIUS client requests and sends back a response message to the device.

When you are using RADIUS authentication, you can have both local users and RADIUS users able to log in to the device. To use RADIUS authentication, you must set up a RADIUS server that is accessible by the Connect EZ device prior to configuration. The process of setting up a RADIUS server varies by the server environment. An example of a RADIUS server is FreeRADIUS.

This section contains the following topics:

|                                                                  |     |
|------------------------------------------------------------------|-----|
| RADIUS user configuration .....                                  | 548 |
| RADIUS server failover and fallback to local configuration ..... | 548 |
| Configure your Connect EZ device to use a RADIUS server .....    | 549 |

## RADIUS user configuration

When configured to use RADIUS support, the Connect EZ device uses a remote RADIUS server for user authentication (password verification) and authorization (assigning the access level of the user). Additional RADIUS servers can be configured as backup servers for user authentication.

This section outlines how to configure a RADIUS server to be used for user authentication on your Connect EZ device.

### Example FreeRADIUS configuration

With FreeRADIUS, users are defined in the **users** file in your FreeRADIUS installation. To define users:

1. Open the FreeRadius user file in a text editor. For example:

---

```
$ sudo gedit /etc/freeradius/3.0/users
```

---

2. Add users to the file using the following format:

---

```
user1 Cleartext-Password := "user1"
      Unix-FTP-Group-Names := "admin"

user2 Cleartext-Password := "user2"
      Unix-FTP-Group-Names := "serial"
```

---

The **Unix-FTP-Group-Names** attribute is optional. If used, the value must correspond to authentication groups configured on your Connect EZ. Alternatively, if the user is also configured as a local user on the Connect EZ device and the RADIUS server authenticates the user but does not return any groups, the local configuration determines the list of groups. See [Authentication groups](#) for more information about authentication groups. The **Unix-FTP-Group-Names** attribute can contain one group or multiple groups in a comma-separated list.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

---

```
$ sudo freeradius -CX
```

---

This should return a message that completes similar to:

---

```
...
Configuration appears to be OK
```

---

5. Restart the FreeRADIUS server:

---

```
$ sudo /etc/init.d/freeradius restart
```

---

## RADIUS server failover and fallback to local configuration

In addition to the primary RADIUS server, you can also configure your Connect EZ device to use backup RADIUS servers. Backup RADIUS servers are used for authentication requests when the primary RADIUS server is unavailable.

### Falling back to local authentication

With user authentication methods, you can configure your Connect EZ device to use multiple types of authentication. For example, you can configure both RADIUS authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup RADIUS

servers are unavailable. Additionally, users who are configured locally but are not configured on the RADIUS server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the RADIUS server, and only authenticated locally if the RADIUS server is unavailable or if the user is not defined on the RADIUS server, then you should list the RADIUS authentication method prior to the Local users authentication method.

See [User authentication methods](#) for more information about authentication methods.

If the RADIUS servers are unavailable and the Connect EZ device falls back to local authentication, only users defined locally on the device are able to log in. RADIUS users cannot log in until the RADIUS servers are brought back online.

## Configure your Connect EZ device to use a RADIUS server

This section describes how to configure a Connect EZ device to use a RADIUS server for authentication and authorization.

### Required configuration items

- Define the RADIUS server IP address or domain name.
- Define the RADIUS server shared secret.
- Add RADIUS as an authentication method for your Connect EZ device.

### Additional configuration items

- Whether other user authentication methods should be used in addition to the RADIUS server, or if the RADIUS server should be considered the authoritative login method.
- The RADIUS server port. It is configured to 1812 by default.
- Add additional RADIUS servers in case the first RADIUS server is unavailable.
- The server NAS ID. If left blank, the default value is used:
  - If you are access the Connect EZ device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are access the Connect EZ device by using ssh, the default value is **sshd**.
- Time in seconds before the request to the server times out. The default is 3 seconds and the maximum possible value is 60 seconds.
- Enable additional debug messages from the RADIUS client.

## Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

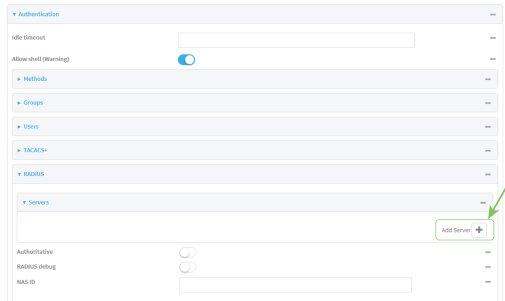
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

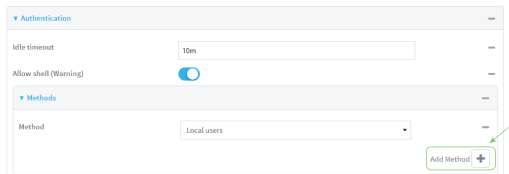
3. Click **Authentication > RADIUS > Servers**.
4. Add RADIUS servers:
  - a. For **Add server**, click **+**.



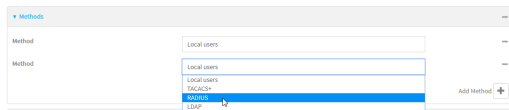
- b. For **Hostname**, type the hostname or IP address of the RADIUS server.
  - c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 1812.
  - d. For **Secret**, type the RADIUS server's shared secret. This is configured in the secret parameter of the RADIUS server's client.conf file, for example:
 

```
secret=testing123
```
  - e. For **Timeout**, type or select the amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.
  - f. (Optional) Click **+** again to add additional RADIUS servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if RADIUS login fails.
6. (Optional) Click **RADIUS debug** to enable additional debug messages from the RADIUS client.
7. (Optional) For **NAS ID**, type the unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:
  - If you are accessing the Connect EZ device by using the WebUI, the default value is for NAS ID is **httpd**.
  - If you are accessing the Connect EZ device by using ssh, the default value is **sshd**.

8. Add RADIUS to the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. For **Add method**, click **+**.



- c. Select **RADIUS** for the new method from the **Method** drop-down.



Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See [Rearrange the position of authentication methods](#) for information about rearranging the position of the methods in the list.

9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) Prevent other authentication methods from being used if RADIUS authentication fails. Other authentication methods will only be used if the RADIUS server is unavailable.

```
(config)> auth radius authoritative true
(config)>
```

4. (Optional) Enable debug messages from the RADIUS client:

```
(config)> auth radius debug true
(config)>
```

5. (Optional) Configure the NAS ID. This is a unique identifier for this network access server (NAS). You can use the fully-qualified domain name of the NAS or any arbitrary string. If not set, the default value is used:

- If you are accessing the Connect EZ device by using the WebUI, the default value is for NAS ID is **httpd**.
- If you are accessing the Connect EZ device by using ssh, the default value is **sshd**.

---

```
(config)> auth radius nas_id id
(config)>
```

---

6. Add a RADIUS server:

a. Add the server:

---

```
(config)> add auth radius server end
(config auth radius server 0)>
```

---

b. Enter the RADIUS server's IP address or hostname:

---

```
(config auth radius server 0)> hostname hostname|ip-address
(config auth radius server 0)>
```

---

c. (Optional) Change the default port setting to the appropriate port:

---

```
(config auth radius server 0)> port port
(config auth radius server 0)>
```

---

d. Configure the amount of time in seconds to wait for the RADIUS server to respond. Allowed value is any integer from **3** to **60**. The default value is **3**.

---

```
(config auth radius server 0)> timeout value
(config auth radius server 0)>
```

---

e. (Optional) Repeat the above steps to add additional RADIUS servers.

7. Add RADIUS to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add RADIUS to the end of the list. See [User authentication methods](#) for information about adding methods to the beginning or middle of the list.

---

```
(config)> add auth method end radius
(config)>
```

---

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## LDAP

Your Connect EZ device supports LDAP (Lightweight Directory Access Protocol), a protocol used for directory information services over an IP network. LDAP can be used with your Connect EZ device for centralized authentication and authorization management for users who connect to the device. With LDAP support, the Connect EZ device acts as an LDAP client, which sends user credentials and connection parameters to an LDAP server. The LDAP server then authenticates the LDAP client requests and sends back a response message to the device.



When you are using LDAP authentication, you can have both local users and LDAP users able to log in to the device. To use LDAP authentication, you must set up a LDAP server that is accessible by the Connect EZ device prior to configuration. The process of setting up a LDAP server varies by the server environment.

This section contains the following topics:

|                                                                |     |
|----------------------------------------------------------------|-----|
| LDAP user configuration .....                                  | 554 |
| LDAP server failover and fallback to local configuration ..... | 555 |
| Configure your Connect EZ device to use an LDAP server .....   | 555 |

## LDAP user configuration

When configured to use LDAP support, the Connect EZ device uses a remote LDAP server for user authentication (password verification) and authorization (assigning the access level of the user). Additional LDAP servers can be configured as backup servers for user authentication.

This section outlines how to configure a LDAP server to be used for user authentication on your Connect EZ device.

There are several different implementations of LDAP, including Microsoft Active Directory. This section uses OpenLDAP as an example configuration. Other implementations of LDAP will have different configuration methods.

### Example OpenLDAP configuration

With OpenLDAP, users can be configured in a text file using the LDAP Data Interchange Format (LDIF). In this case, we will be using a file called **add\_user.ldif**.

1. Create the **add\_user.ldif** file in a text editor. For example:

---

```
$ gedit ./add_user.ldif
```

---

2. Add users to the file using the following format:

---

```
dn: uid=john,dc=example,dc=com
objectClass: inetOrgPerson
cn: John Smith
sn: Smith
uid: john
userPassword: password
ou: admin serial
```

---

- The value of **uid** and **userPassword** must correspond to the username and password used to log into the Connect EZ device.
- The **ou** attribute is optional. If used, the value must correspond to authentication groups configured on your Connect EZ. Alternatively, if the user is also configured as a local user on the Connect EZ device and the LDAP server authenticates the user but does not return any groups, the local configuration determines the list of groups. See [Authentication groups](#) for more information about authentication groups.

Other attributes may be required by the user's objectClass. Any objectClass may be used as long it allows the **uid**, **userPassword**, and **ou** attributes.

3. Save and close the file.
4. Add the user to the OpenLDAP server:

---

```
$ ldapadd -x -H 'ldap:/// ' -D 'cn=admin,dc=example,dc=com' -W -f add_
user.ldif
adding new entry "uid=john,dc=example,dc=com"
```

---

5. Verify that the user has been added by performing an LDAP search:

---

```
$ ldapsearch -x -LLL -H 'ldap:/// ' -b 'dc=example,dc=com'
uid=john
dn: uid=john,dc=example,dc=com
objectClass: inetOrgPerson
```

---

---

```
cn: John Smith
sn: Smith
uid: john
ou: admin serial
```

---

## LDAP server failover and fallback to local configuration

In addition to the primary LDAP server, you can also configure your Connect EZ device to use backup LDAP servers. Backup LDAP servers are used for authentication requests when the primary LDAP server is unavailable.

### *Falling back to local authentication*

With user authentication methods, you can configure your Connect EZ device to use multiple types of authentication. For example, you can configure both LDAP authentication and local authentication, so that local authentication can be used as a fallback mechanism if the primary and backup LDAP servers are unavailable. Additionally, users who are configured locally but are not configured on the LDAP server are still able to log into the device. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned; therefore if you want to ensure that users are authenticated first through the LDAP server, and only authenticated locally if the LDAP server is unavailable or if the user is not defined on the LDAP server, then you should list the LDAP authentication method prior to the Local users authentication method.

See [User authentication methods](#) for more information about authentication methods.

If the LDAP servers are unavailable and the Connect EZ device falls back to local authentication, only users defined locally on the device are able to log in. LDAP users cannot log in until the LDAP servers are brought back online.

## Configure your Connect EZ device to use an LDAP server

This section describes how to configure a Connect EZ device to use an LDAP server for authentication and authorization.

### Required configuration items

- Define the LDAP server IP address or domain name.
- Add LDAP as an authentication method for your Connect EZ device.

### Additional configuration items

- Whether other user authentication methods should be used in addition to the LDAP server, or if the LDAP server should be considered the authoritative login method.
- The LDAP server port. It is configured to 389 by default.
- Whether to use Transport Layer Security (TLS) when communicating with the LDAP server.
- The distinguished name (DN) and password used to communicate with the server.
- The distinguished name used to search to user base.
- The group attribute.
- The number of seconds to wait to receive a message from the server.
- Add additional LDAP servers in case the first LDAP server is unavailable.



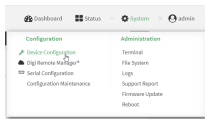
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

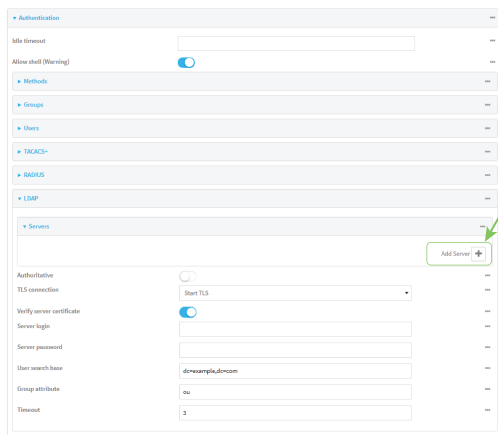
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



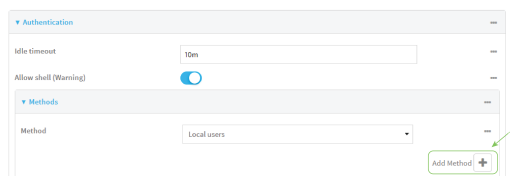
The **Configuration** window is displayed.

3. Click **Authentication > LDAP > Servers**.
4. Add LDAP servers:
  - a. For **Add server**, click **+**.

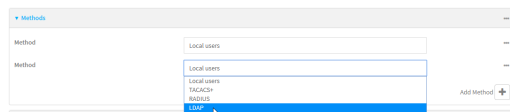


- b. For **Hostname**, type the hostname or IP address of the LDAP server.
  - c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 389 for non-TLS and 636 for TLS.
  - d. (Optional) Click **+** again to add additional LDAP servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being attempted if LDAP login fails.
  6. For **TLS connection**, select the type of TLS connection used by the server:
    - **Disable TLS:** Uses a non-secure TCP connection on the LDAP standard port, 389.
    - **Enable TLS:** Uses an SSL/TLS encrypted connection on port 636.

- **Start TLS:** Makes a non-secure TCP connection to the LDAP server on port 389, then sends a request to upgrade the connection to a secure TLS connection. This is the preferred method for LDAP.
- 7. If **Enable TLS** or **Start TLS** are selected for **TLS connection**:
  - Leave **Verify server certificate** at the default setting of enabled to verify the server certificate with a known Certificate Authority.
  - Disable **Verify server certificate** if the server is using a self-signed certificate.
- 8. (Optional) For **Server login**, type a distinguished name (DN) that is used to bind to the LDAP server and search for users, for example **cn=user,dc=example,dc=com**. Leave this field blank if the server allows anonymous connections.
- 9. (Optional) For **Server password**, type the password used to log into the LDAP server. Leave this field blank if the server allows anonymous connections.
- 10. For **User search base**, type the distinguished name (DN) on the server to search for users. This can be the root of the directory tree (for example, **dc=example,dc=com**) or a sub-tree (for example, **ou=People,dc=example,dc=com**).
- 11. For **Login attribute**, enter the user attribute containing the login of the authenticated user. For example, in the [LDAP user configuration](#), the login attribute is **uid**. If this attribute is not set, the user will be denied access.
- 12. (Optional) For **Group attribute**, type the name of the user attribute that contains the list of Connect EZ authentication groups that the authenticated user has access to. See [LDAP user configuration](#) for further information about the group attribute.
- 13. For **Timeout**, type or select the amount of time in seconds to wait for the LDAP server to respond. Allowed value is between **3** and **60** seconds.
- 14. Add LDAP to the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. For **Add method**, click **+**.



- c. Select **LDAP** for the new method from the **Method** drop-down.



Authentication methods are attempted in the order they are listed until an authentication response, either pass or fail, is received. If **Authoritative** is enabled (see above), non-authoritative methods are not attempted. See [Rearrange the position of authentication methods](#) for information about rearranging the position of the methods in the list.

15. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. (Optional) Prevent other authentication methods from being used if LDAP authentication fails. Other authentication methods will only be used if the LDAP server is unavailable.

---

```
(config)> auth ldap authoritative true
(config)>
```

---

4. Set the type of TLS connection used by the LDAP server:

---

```
(config)> auth ldap tls value
(config)>
```

---

where *value* is one of:

- **off**: Uses a non-secure TCP connection on the LDAP standard port, 389.
- **on**: Uses an SSL/TLS encrypted connection on port 636.
- **start\_tls**: Makes a non-secure TCP connection to the LDAP server on port 389, then sends a request to upgrade the connection to a secure TLS connection. This is the preferred method for LDAP.

The default is **off**.

5. If **tls** is set to **on** or **start\_tls**, configure whether to verify the server certificate:

---

```
(config)> auth ldap verify_server_cert value
(config)>
```

---

where *value* is either:

- **true**: Verifies the server certificate with a known Certificate Authority.
- **false**: Does not verify the certificate. Use this option if the server is using a self-signed certificate.

The default is **true**.

6. Set the distinguished name (DN) that is used to bind to the LDAP server and search for users. Leave this option unset if the server allows anonymous connections.

---

```
(config)> auth ldap bind_dn dn_value
(config)>
```

---

For example:

---

```
(config)> auth ldap bind_dn cn=user,dc=example,dc=com
(config)>
```

---

7. Set the password used to log into the LDAP server. Leave this option unset if the server allows anonymous connections.

---

```
(config)> auth ldap bind_password password
(config)>
```

---

8. Set the distinguished name (DN) on the server to search for users. This can be the root of the directory tree (for example, **dc=example,dc=com**) or a sub-tree (for example, **ou=People,dc=example,dc=com**).

---

```
(config)> auth ldap base_dn value
(config)>
```

---

9. Set the login attribute:

---

```
(config)> auth ldap login_attribute value
(config)>
```

---

where *value* is the user attribute containing the login of the authenticated user. For example, in the [LDAP user configuration](#), the login attribute is **uid**. . If this attribute is not set, the user will be denied access.

10. (Optional) Set the name of the user attribute that contains the list of Connect EZ authentication groups that the authenticated user has access to. See [LDAP user configuration](#) for further information about the group attribute.

---

```
(config)> auth ldap group_attribute value
(config)>
```

---

For example:

---

```
(config)> auth ldap group_attribute ou
(config)>
```

---

11. Configure the amount of time in seconds to wait for the LDAP server to respond.

---

```
(config)> auth ldap timeout value
(config)>
```

---

where *value* is any integer from **3** to **60**. The default value is **3**.

12. Add an LDAP server:

- a. Add the server:

---

```
(config)> add auth ldap server end
(config auth ldap server 0)>
```

---

- b. Enter the LDAP server's IP address or hostname:

---

```
(config auth ldap server 0)> hostname hostname|ip-address
(config auth ldap server 0)>
```

---

- c. (Optional) Change the default port setting to the appropriate port:

---

```
(config auth ldap server 0)> port port
(config auth ldap server 0)>
```

---

- d. (Optional) Repeat the above steps to add additional LDAP servers.

13. Add LDAP to the authentication methods. Authentication methods are attempted in the order they are listed until the first successful authentication result is returned. This example will add LDAP to the end of the list. See [User authentication methods](#) for information about adding methods to the beginning or middle of the list.

---

```
(config)> add auth method end ldap
(config)>
```

---

14. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

15. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Disable shell access

To prohibit access to the shell prompt for all authentication groups, disable the **Allow shell** parameter.. This does not prevent access to the Admin CLI.

---

**Note** If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

---

### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

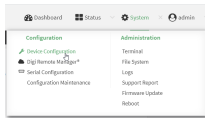
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

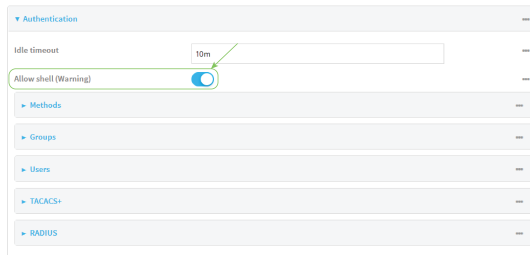


- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication**.
4. Click to disable **Allow shell**.




---

**Note** If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

---

5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set the **allow\_shell** parameter to **false**:

```
(config)> auth allow_shell false
```

---

**Note** If shell access is disabled, re-enabling it will erase the device's configuration and perform a factory reset.

---

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Set the idle timeout for Connect EZ users

To configure the amount of time that the user's active session can be inactive before it is automatically disconnected, set the **Idle timeout** parameter.

By default, the Idle timeout is set to 10 minutes.

### Web

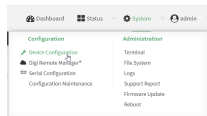
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

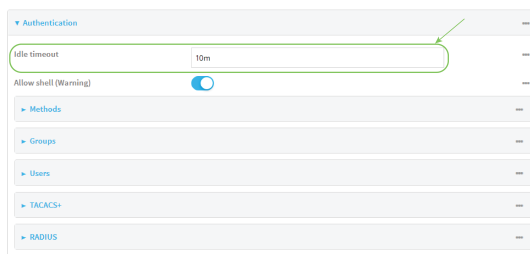


The **Configuration** window is displayed.

3. Click **Authentication**.
4. For **Idle timeout**, enter the amount of time that the active session can be idle before the user is automatically logged out.

Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.

For example, to set **Idle timeout** to ten minutes, enter **10m** or **600s**.



5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> auth idle_timeout value
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **idle\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> auth idle_timeout 600s
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example user configuration

### Example 1: Administrator user with local authentication

Goal: To create a user with administrator rights who is authenticated locally on the device.

#### Web

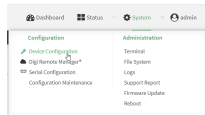
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

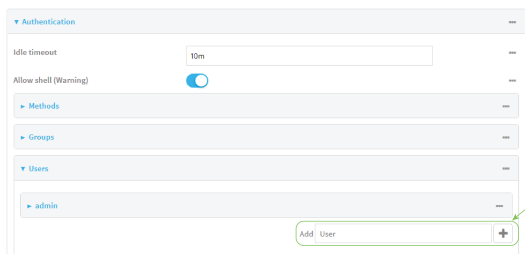
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Authentication > Users**.
4. In **Add User**: enter a name for the user and click **+**.



The user configuration window is displayed.

The screenshot shows a configuration form for a user. It includes a toggle for 'Enable', a text field for 'Username alias', a password field with a 'required value' indicator, and expandable sections for 'Login failure lockout', 'Groups', 'SSH keys', and 'Two-factor authentication'.

5. Enter a **Password** for the user.
6. Assign the user to the **admin** group:
  - a. Click **Groups**.
  - b. For **Add Group**, click **+**.
  - c. For **Group**, select the **admin** group.
  - d. Verify that the **admin** group has full administrator rights:
    - i. Click **Authentication > Groups**.
    - ii. Click **admin**.
    - iii. Verify that the admin group has **Admin access** enabled. If not, click **Admin access** to enable.
    - iv. Verify that **Access level** is set to **Full access**. If not, select **Full access**.
  - e. Verify that **Local users** is one of the configured authentication methods:
    - i. Click **Authentication > Methods**.
    - ii. Verify that **Local users** is one of the methods listed in the list. If not:
      - i. For **Add Method**, click **+**.
      - ii. For **Method**, select **Local users**.
7. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Verify that the **admin** group has full administrator rights:

```
(config)> show auth group admin acl
admin
    enable true
    level full
...
(config)>
```

If **admin > enable** is set to false:

```
(config)> auth group admin acl admin enable true
(config)>
```

If **admin > level** is set to read-only:

```
(config)> auth group admin acl admin level full
(config)>
```

4. Verify that **local** is one of the configured authentication methods:

```
(config)> show auth method
0 local
(config)>
```

If **local** is not listed:

```
(config)> add auth method end local
(config)>
```

5. Create the user. In this example, the user is being created with the username **adminuser**:

```
(config)> add auth user adminuser
(config auth user adminuser)>
```

6. Assign a password to the user:

```
(config auth user adminuser)> password pwd
(config auth user adminuser)>
```

7. Assign the user to the **admin** group:

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

8. Save the configuration and apply the change

```
(config auth user adminuser)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example 2: RADIUS, TACACS+, and local authentication for one user

Goal: To create a user with administrator rights who is authenticated by using all three authentication methods.

In this example, when the user attempts to log in to the Connect EZ device, user authentication will occur in the following order:

1. The user is authenticated by the RADIUS server. If the RADIUS server is unavailable,
2. The user is authenticated by the TACACS+ server. If both the RADIUS and TACACS+ servers are unavailable,
3. The user is authenticated by the Connect EZ device using local authentication.

This example uses a FreeRadius 3.0 server running on ubuntu, and a TACACS+ server running on ubuntu. Server configuration may vary depending on the platforms or type of servers used in your environment.

## ≡ Web

1. Configure a user on the RADIUS server:
  - a. On the ubuntu machine hosting the FreeRadius server, open the `/etc/freeradius/3.0/users` file:

---

```
$ sudo gedit /etc/freeradius/3.0/users
```

---

- b. Add a RADIUS user to the `users` file:

---

```
admin1 Cleartext-Password := "password1"
      Unix-FTP-Group-Names := "admin"
```

---

In this example:

- The user's username is **admin1**.
- The user's password is **password1**.
- The authentication group on the Connect EZ device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.

- c. Save and close the `users` file.
2. Configure a user on the TACACS+ server:
  - a. On the ubuntu machine hosting the TACACS+ server, open the `/etc/tacacs+/tac_plus.conf` file:

---

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

---

- b. Add a TACACS+ user to the `tac_plus.conf` file:

---

```
user = admin1 {
    name = "Admin1 for TX64"
    pap = cleartext password1
    service = system {
        groupname = admin
    }
}
```

---

In this example:

- The user's username is **admin1**.
- The user's password is **password1**.
- The authentication group on the Connect EZ device, **admin**, is identified in the **groupname** parameter.

- c. Save and close the `tac_plus.conf` file.
3. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
4. Access the device configuration:

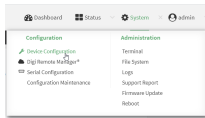
Remote Manager:



- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

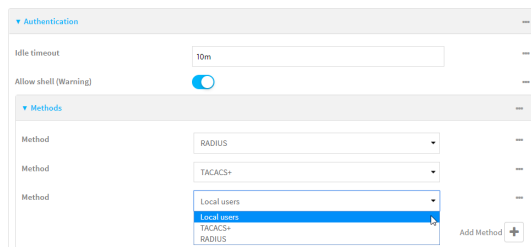
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

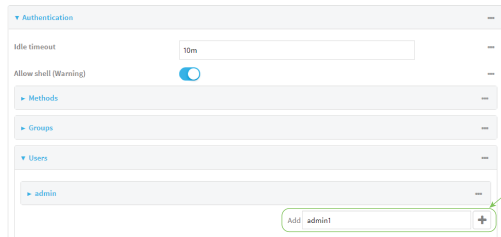


The **Configuration** window is displayed.

5. Configure the authentication methods:
  - a. Click **Authentication > Methods**.
  - b. For **Method**, select **RADIUS**.
  - c. For **Add Method**, click **+** to add a new method.
  - d. For the new method, select **TACACS+**.
  - e. Click **+** to add another new method.
  - f. For the new method, select **Local users**.

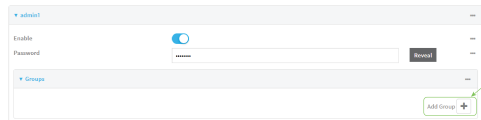


6. Create the local user:
  - a. Click **Authentication > Users**.
  - b. In **Add User:**, type **admin1** and click **+**.

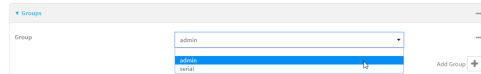


- c. For **password**, type **password1**.

- d. Assign the user to the **admin** group:
  - i. Click **Groups**.
  - ii. For **Add Group**, click **+**.



- iii. For **Group**, select the **admin** group.



- a. Verify that the **admin** group has full administrator rights:
  - i. Click **Authentication > Groups**.
  - ii. Click **admin**.
  - iii. Verify that the admin group has **Admin access** enabled. If not, click **Admin access** to enable.
  - iv. Verify that **Access level** is set to **Full access**. If not, select **Full access**.
7. Click **Apply** to save the configuration and apply the change.

## Command line

1. Configure a user on the RADIUS server:
  - a. On the ubuntu machine hosting the FreeRadius server, open the `/etc/freeradius/3.0/users` file:

```
$ sudo gedit /etc/freeradius/3.0/users
```

- b. Add a RADIUS user to the **users** file:

```
admin1 Cleartext-Password := "password1"
      Unix-FTP-Group-Names := "admin"
```

In this example:

- The user's username is **admin1**.
  - The user's password is **password1**.
  - The authentication group on the Connect EZ device, **admin**, is identified in the **Unix-FTP-Group-Names** parameter.
- c. Save and close the **users** file.
  2. Configure a user on the TACACS+ server:
    - a. On the ubuntu machine hosting the TACACS+ server, open the `/etc/tacacs+/tac_plus.conf` file:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

- b. Add a TACACS+ user to the **tac\_plus.conf** file:

---

```

user = admin1 {
    name = "Admin1 for TX64"
    pap = cleartext password1
    service = system {
        groupname = admin
    }
}

```

---

In this example:

- The user's username is **admin1**.
  - The user's password is **password1**.
  - The authentication group on the Connect EZ device, **admin**, is identified in the **groupname** parameter.
- c. Save and close the **tac\_plus.conf** file.
3. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
4. At the command line, type **config** to enter configuration mode:

---

```

> config
(config)>

```

---

5. Configure the authentication methods:

- a. Determine the current authentication method configuration:

---

```

(config)> show auth method
0 local
(config)>

```

---

This output indicates that on this example system, only local authentication is configured.

- b. Add RADIUS authentication to the beginning of the list:

---

```

(config)> add auth method 0 radius
(config)>

```

---

- c. Add TACACS+ authentication second place in the list:

---

```

(config)> add auth method 1 tacacs+(config)>

```

---

- d. Verify that authentication will occur in the correct order:

---

```

(config)> show auth method
0 radius
1 tacacs+

```

---

---

```
2 local
(config)>
```

---

6. Verify that the **admin** group has full administrator rights:

---

```
(config)> show auth group admin acl
admin
    enable true
    level full
...
(config)>
```

---

If **admin > enable** is set to false:

---

```
(config)> auth group admin acl admin enable true
(config)>
```

---

If **admin > level** is set to read-only:

---

```
(config)> auth group admin acl admin level full
(config)>
```

---

7. Configure the local user:

- a. Create a local user with the username **admin1**:

---

```
(config)> add auth user admin1
(config auth user admin1)>
```

---

- b. Assign a password to the user:

---

```
(config auth user adminuser)> password password1
(config auth user adminuser)>
```

---

- c. Assign the user to the **admin** group:

---

```
(config auth user adminuser)> add group end admin
(config auth user adminuser)>
```

---

8. Save the configuration and apply the change

---

```
(config auth user adminuser)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

# Firewall

---

This chapter contains the following topics:

|                                            |     |
|--------------------------------------------|-----|
| Firewall configuration .....               | 574 |
| Port forwarding rules .....                | 579 |
| Packet filtering .....                     | 586 |
| Configure custom firewall rules .....      | 593 |
| Configure Quality of Service options ..... | 595 |
| Web filtering .....                        | 604 |

## Firewall configuration

Firewall configuration includes the following configuration options:

- **Zones:** A zone is a firewall access group to which network interfaces can be added. You then use zones to configure packet filtering and access control lists for interfaces that are included in the zone. Preconfigured zones include:
  - **Any:** Matches any network interface, even if they are not assigned to this zone.
  - **Loopback:** Zone for interfaces that are used for communication between processes running on the device.
  - **Internal:** Used for interfaces connected to trusted networks. By default, the firewall will allow most access from this zone.
  - **External:** Used for interfaces to connect to untrusted zones, such as the internet. This zone has Network Address Translation (NAT) enabled by default. By default, the firewall will block most access from this zone.
  - **Edge:** Used for interfaces connected to trusted networks, where the device is a client on the edge of the network rather than a router or gateway.
  - **Setup:** Used for interfaces involved in the initial setup of the device. By default, the firewall will only allow this zone to access administration services.
  - **IPsec:** The default zone for IPsec tunnels.
  - **Dynamic routes:** Used for routes learned using routing services.
- **Port forwarding:** A list of rules that allow network connections to the Connect EZ to be forwarded to other servers by translating the destination address.
- **Packet filtering:** A list of packet filtering rules that determine whether to accept or reject network connections that are forwarded through the Connect EZ.
- **Custom rules:** A script that is run to install advanced firewall rules beyond the scope/capabilities of the standard device configuration.
- **Quality Of Service:** Quality of Service (QoS) options for bandwidth allocation and policy-based traffic shaping and prioritizing.

### Create a custom firewall zone

In addition to the preconfigured zones, you can create your custom zones that can be used to configure packet filtering and access control lists for network interfaces.

To create a zone:

#### Web

1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

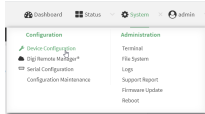
Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.

- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

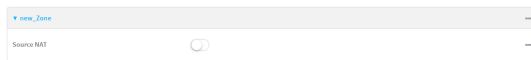


The **Configuration** window is displayed.

3. Click **Firewall > Zones**.
4. In **Add Zone**, enter a name for the zone and click **+**.



The firewall configuration window is displayed.



5. (Optional) If traffic on this zone will be forwarded from a private network to the internet, enable Network Address Translation (NAT).
6. Click **Apply** to save the configuration and apply the change.

See [Configure the firewall zone for a network interface](#) for information about how to configure network interfaces to use a zone.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add the new zone. For example, to add a zone named **my\_zone**:

```
(config)> add firewall zone my_zone
(config firewall zone my_zone)>
```

- (Optional) Enable Network Address Translation (NAT):

```
(config firewall zone my_zone)> src_nat true
(config firewall zone my_zone)>
```

- Save the configuration and apply the change

```
(config firewall zone my_zone)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See [Configure the firewall zone for a network interface](#) for information about how to configure network interfaces to use a zone.

## Configure the firewall zone for a network interface

Firewall zones allow you to group network interfaces for the purpose of packet filtering and access control. There are several preconfigured firewall zones, and you can create custom zones as well. The firewall zone that a network interfaces uses is selected during interface configuration.

This example procedure uses an existing network interface named **ETH2** and changes the firewall zone from the default zone, **Internal**, to **External**.

### Web

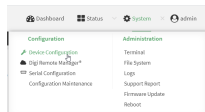
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- Click **Network > Interfaces > ETH2**.



4. For **Zone**, select **External**.
5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> network interface eth2 zone my_zone
(config)>
```

---

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a custom firewall zone

You cannot delete preconfigured firewall zones. To delete a custom firewall zone:

### Web

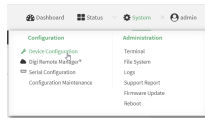
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

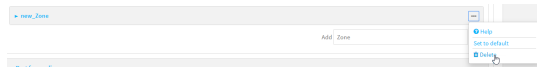
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Zones**.
4. Click the menu icon (...) next to the appropriate custom firewall zone and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Use the **del** command to delete a custom firewall rule. For example:

```
(config)> del firewall zone my_zone
```

4. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Port forwarding rules

Most computers are protected by a firewall that prevents users on a public network from accessing servers on the private network. To allow a computer on the Internet to connect to a specific server on a private network, set up one or more port forwarding rules. Port forwarding rules provide mapping instructions that direct incoming traffic to the proper device on a LAN.

### Configure port forwarding

#### *Required configuration items*

- The network interface for the rule.  
Network connections will only be forwarded if their destination address matches the IP address of the selected network interface.
- The public-facing port number that network connections must use for their traffic to be forwarded.
- The IP address of the server to which traffic should be forwarded.
- The port or range of ports to which traffic should be forwarded.

#### *Additional configuration items*

- A label for the port forwarding rule.
- The IP version (either IPv4 or IPv6) that incoming network connections must match.
- The protocols that incoming network connections must match.

- A white list of devices, based on either IP address or firewall zone, that are authorized to leverage this forwarding rule.

To configure a port forwarding rule:

## Web

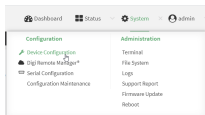
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

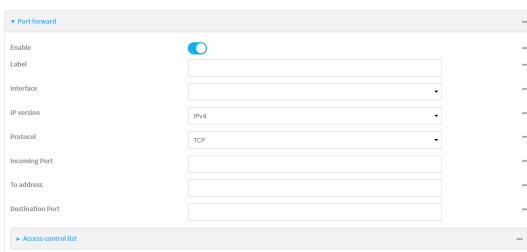


The **Configuration** window is displayed.

3. Click **Firewall > Port forwarding**.
4. For **Add port forward**, click **+**.



The port forwarding rule configuration window is displayed.



Port forwarding rules are enabled by default. To disable, toggle off **Enable**.

5. (Optional) Type a **Label** that will be used to identify the rule.

6. For **Interface**, select the network interface for the rule.  
Network connections will only be forwarded if their destination address matches the IP address of the selected network interface.
7. For **IP version**, select either **IPv4** or **IPv6**.  
Network connections will only be forwarded if they match the selected IP version.
8. For **Protocol**, select the type of internet protocol.  
Network connections will only be forwarded if they match the selected protocol.
9. For **Incoming port(s)**, type the public-facing port number that network connections must use for their traffic to be forwarded.
10. For **To Address**, type the IP address of the server to which traffic should be forwarded.
11. For **Destination Port(s)**, type the port number, comma-separated list of port numbers, or range of port numbers on the server to which traffic should be forwarded. For example, to forward traffic to ports one, three, and five through ten, enter: **1, 3, 5-10**.
12. (Optional) Click **Access control list** to create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone:
  - To white list IP addresses:
    - a. Click **Addresses**.
    - b. For **Add Address**, enter an IP address and click **+**.
    - c. Repeat for each additional IP address that should be white listed.
  - To specify firewall zones for white listing:
    - a. Click **Zones**.
    - b. For **Add zone**, click **+**.
    - c. For **Zone**, select the appropriate zone.
    - d. Repeat for each additional zone.
13. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. At the config prompt, type:

---

```
(config)> add firewall dnat end
(config firewall dnat 0)>
```

---

Port forwarding rules are enabled by default. To disable the rule:

---

```
(config firewall dnat 0)> enable false
(config firewall dnat 0)>
```

---

4. Set the network interface for the rule.

---

```
(config firewall dnat 0)> interface
(config firewall dnat 0)>
```

---

Network connections will only be forwarded if their destination address matches the IP address of this network interface.

- a. Use the `?` to determine available interfaces:
- b. Set the interface. For example:

---

```
(config firewall dnat 0)> interface eth1
(config firewall dnat 0)>
```

---

5. Set the IP version. Allowed values are **ipv4** and **ipv6**. The default is **ipv4**.

---

```
(config firewall dnat 0)> ip_version ipv6
(config firewall dnat 0)>
```

---

6. Set the public-facing port number that network connections must use for their traffic to be forwarded.

---

```
(config firewall dnat 0)> port port
(config firewall dnat 0)>
```

---

7. Set the type of internet protocol .

---

```
(config firewall dnat 0)> protocol value
(config firewall dnat 0)>
```

---

Network connections will only be forwarded if they match the selected protocol. Allowed values are **custom**, **tcp**, **tcpudp**, or **udp**. The default is **tcp**.

8. Set the IP address of the server to which traffic should be forwarded:
- For IPv4 addresses:

---

```
(config firewall dnat 0)> to_address ip-address
(config firewall dnat 0)>
```

---

- For IPv6 addresses:

---

```
(config firewall dnat 0)> to_address6 ip-address
(config firewall dnat 0)>
```

---

9. Set the public-facing port number(s) that network connections must use for their traffic to be forwarded.

---

```
(config firewall dnat 0)> to_port value
(config firewall dnat 0)>
```

---

where *value* is the port number, comma-separated list of port numbers, or range of port numbers on the server to which traffic should be forwarded. For example, to forward traffic to ports one, three, and five through ten, enter **1, 3, 5-10**.

10. (Optional) To create a white list of devices that are authorized to leverage this forwarding rule, based on either the IP address or firewall zone, change to the `acl` node:

---

```
(config firewall dnat 0)> acl
(config firewall dnat 0 acl)>
```

---

- To white list an IP address:

- For IPv4 addresses:

---

```
(config firewall dnat 0 acl> add address end ip-address
(config firewall dnat 0 acl)>
```

---

- For IPv6 addresses:

---

```
(config firewall dnat 0 acl> add address6 end ip-address
(config firewall dnat 0 acl)>
```

---

Repeat for each appropriate IP address.

- To specify the firewall zone for white listing:

---

```
(config firewall dnat 0 acl)> add zone end zone
```

---

Repeat for each appropriate zone.

To view a list of available zones:

---

```
(config firewall dnat 0 acl)> .. .. .. zone ?
```

Zones: A list of groups of network interfaces that can be referred to by packet filtering rules and access control lists.

Additional Configuration

```
-----
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup

(config firewall dnat 0 acl)>
```

---

11. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

12. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a port forwarding rule

To delete a port forwarding rule:

### Web

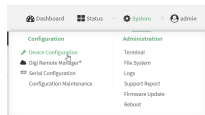
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Port forwarding**.
4. Click the menu icon (...) next to the appropriate port forwarding rule and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.



Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Determine the index number of the port forwarding rule you want to delete:

---

```
(config)> show firewall dnat
0
    acl
        no address
        no zone
    enable true
    interface
    ip_version ipv4
    label IPv4 port forwarding rule
    port 10000
    protocol tcp
    to_address6 10.10.10.10
    to_port 10001

1
    acl
        no address6
        no zone
    enable false
    interface
    ip_version ipv6
    label IPv6 port forwarding rule
    port 10002
    protocol tcp
    to_address6 c097:4533:bd63:bb12:9a6f:5569:4b53:c29a
    to_port 10003
(config)>
```

---

4. To delete the rule, use the index number with the **del** command. For example:

---

```
(config)> del firewall dnat 1
```

---

5. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Packet filtering

By default, one preconfigured packet filtering rule, **Allow all outgoing traffic**, is enabled and monitors traffic going to and from the Connect EZ device. The predefined settings are intended to block unauthorized inbound traffic while providing an unrestricted flow of outgoing data. You can modify the default packet filtering rule and create additional rules to define how the device accepts or rejects traffic that is forwarded through the device.

### Configure packet filtering

#### *Required configuration items*

- The action that the packet filtering rule will perform, either **Accept**, **Reject**, or **Drop**.
- The source firewall zone: Packets originating from interfaces on this zone will be monitored by this rule.
- The destination firewall zone: Packets destined for interfaces on this zone will be accepted, rejected, or dropped by this rule.

#### *Additional configuration requirements*

- A label for the rule.
- The IP version to be matched, either **IPv4**, **IPv6**, or **Any**.
- The protocol to be matched, one of:
  - **TCP**
  - **UDP**
  - **ICMP**
  - **ICMP6**
  - **Any**

To configure a packet filtering rule:

#### Web

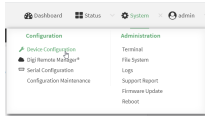
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

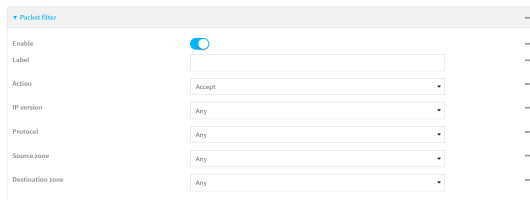
3. Click **Firewall > Packet filtering**.

- To create a new packet filtering rule, for **Add packet filter**, click **+**.



- To edit the default packet filtering rule or another existing packet filtering rule, click to expand the rule.

The packet filtering rule configuration window is displayed.



Packet filters are enabled by default. To disable, toggle off **Enable**.

4. (Optional) Type a **Label** that will be used to identify the rule.
5. For **Action**, select one of:
  - **Accept**: Allows matching network connections.
  - **Reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
  - **Drop**: Blocks matching network connections, and does not send a reply.
6. Select the **IP version**.
7. Select the **Protocol**.
8. For **Source zone**, select the firewall zone that will be monitored by this rule for incoming connections from network interfaces that are a member of this zone.  
See [Firewall configuration](#) for more information about firewall zones.
9. For **Destination zone**, select the firewall zone. Packets destined for network interfaces that are members of this zone will either be accepted, rejected or dropped by this rule.  
See [Firewall configuration](#) for more information about firewall zones.
10. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

To edit the default packet filtering rule or another existing packet filtering rule:

- a. Determine the index number of the appropriate packet filtering rule:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
  dst_zone internal
  enable true
  ip_version any
  label myfilter
  protocol any
  src_zone external
(config)>
```

---

- b. Select the appropriate rule by using its index number:

---

```
(config)> firewall filter 1
(config firewall filter 1)>
```

---

To create a new packet filtering rule:

---

```
(config)> add firewall filter end
(config firewall filter 1)>
```

---

Packet filtering rules are enabled by default. To disable the rule:

---

```
(config firewall filter 1)> enable false
(config firewall filter 1)>
```

---

3. (Optional) Set the label for the rule.

---

```
(config firewall filter 1)> label "My filter rule"
(config firewall filter 1)>
```

---

4. Set the action to be performed by the filter rule.

---

```
(config firewall filter 1)> action value
(config firewall filter 1)>
```

---

where *value* is one of:

- **accept**: Allows matching network connections.
  - **reject**: Blocks matching network connections, and sends an ICMP error if appropriate.
  - **drop**: Blocks matching network connections, and does not send a reply.
5. Set the firewall zone that will be monitored by this rule for incoming connections from network interfaces that are a member of this zone:

See [Firewall configuration](#) for more information about firewall zones.

---

```
(config firewall filter 1)> src_zone my_zone
(config firewall filter 1)>
```

---

6. Set the destination firewall zone. Packets destined for network interfaces that are members of this zone will either be accepted, rejected or dropped by this rule.

See [Firewall configuration](#) for more information about firewall zones.

---

```
(config firewall filter 1)> dst_zone my_zone
(config firewall filter 1)>
```

---

7. Set the IP version.

---

```
(config firewall filter 1)> ip_version value
(config firewall filter 1)>
```

---

where *value* is one of:

- **any**
  - **ipv4**
  - **ipv6**
  - The default is **any**.
8. Set the protocol.

---

```
(config firewall filter 1)> protocol value
(config firewall filter 1)>
```

---

where *value* is one of:

- **any**
  - **icmp**
  - **icmpv6**
  - **tcp**
  - **udp**
- The default is **any**.

- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Enable or disable a packet filtering rule

To enable or disable a packet filtering rule:

### Web

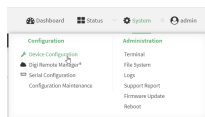
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

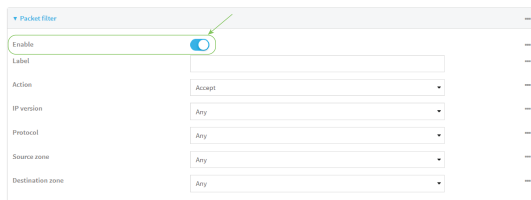
Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- Click **Firewall > Packet filtering**.
- Click the appropriate packet filtering rule.
- Click **Enable** to toggle the rule between enabled and disabled.



- Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Determine the index number of the appropriate port forwarding rule:

---

```
(config)> show firewall filter
0
  action accept
  dst_zone any
  enable true
  ip_version any
  label Allow all outgoing traffic
  protocol any
  src_zone internal
1
  action drop
  dst_zone internal
  enable true
  ip_version any
  label My packet filter
  protocol any
  src_zone external
(config)>
```

---

4. To enable a packet filtering rule, use the index number with the **enable true** command. For example:

---

```
(config)> firewall filter 1 enable true
```

---

5. To disable a packet filtering rule, use the index number with the **enable false** command. For example:

---

```
(config)> firewall filter 1 enable false
```

---

6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Delete a packet filtering rule

To delete a packet filtering rule:

## Web

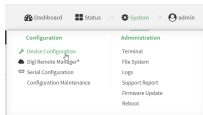
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Packet filtering**.
4. Click the menu icon (...) next to the appropriate packet filtering rule and select **Delete**.



5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Determine the index number of the packet filtering rule you want to delete:

```
(config)> show firewall filter
0
    action accept
```



---

```

dst_zone any
enable true
ip_version any
label Allow all outgoing traffic
protocol any
src_zone internal
1
action drop
dst_zone internal
enable true
ip_version any
label My packet filter
protocol any
src_zone external
(config)>

```

---

- To delete the rule, use the index number with the **del** command. For example:

---

```
(config)> del firewall filter 1
```

---

- Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure custom firewall rules

Custom firewall rules consist of a script of shell commands that can be used to install firewall rules, ipsets, and other system configuration. These commands are run whenever system configuration changes occur that might cause changes to the firewall.

To configure custom firewall rules:

### Web

- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

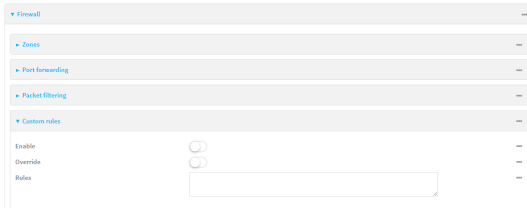
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Custom rules**.



4. **Enable** the custom rules.
5. (Optional) Enable **Override** to override all preconfigured firewall behavior and rely solely on the custom firewall rules.
6. For **Rules**, type the shell command that will execute the custom firewall rules script.
7. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable custom firewall rules:

```
(config)> firewall custom enable true
(config)>
```

4. (Optional) Instruct the device to override all preconfigured firewall behavior and rely solely on the custom firewall rules:

```
(config)> firewall custom override true
(config)>
```

5. Set the shell command that will execute the custom firewall rules script:

```
(config)> firewall custom rules "shell-command"
(config)>
```

- Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure Quality of Service options

Quality of Service (QoS) options allow you to manage the traffic performance of various services, such as Voice over IP (VoIP), cloud computing, traffic shaping, traffic prioritizing, and bandwidth allocation. When configuring QoS, you can only control the queue for outgoing packets on each interface (egress packets), not what is received on the interface (packet ingress).

A QoS *binding* contains the policies and rules that apply to packets exiting the Connect EZ device on the binding's interface. By default, the Connect EZ device has two preconfigured QoS bindings, **Outbound** and **Inbound**. These bindings are an example configuration designed for a typical VoIP site:

- **Outbound** provides an example of matching packets as they are routed from the device onto the WAN interface.
- **Inbound** provides an example of matching packets as they are routed from the device onto a LAN interface.

These example bindings are disabled by default.

### Enable the preconfigured bindings

#### ≡ Web

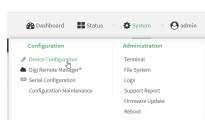
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Quality of Service**.
4. Click to expand either **Outbound** or **Inbound**.
5. **Enable** the binding.
6. Select an **Interface**.
7. Examine the remaining default settings and modify as appropriate for your network.
8. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Enable one of the preconfigured bindings:

- To enable the Outbound binding:

---

```
(config)> firewall qos 0 enable true
(config)>
```

---

- To enable the Inbound binding:

---

```
(config)> firewall qos 1 enable true
(config)>
```

---

4. Set the interface for the binding. Use the index number of the binding; for example, to set the interface for the Outbound binding:
  - a. Use the **?** to determine available interfaces:
  - b. Set the interface. For example:

---

```
(config)> firewall qos 0 interface /network/interface/eth1
(config)>
```

---

5. Examine the remaining default settings and modify as appropriate for your network.
6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Create a new binding

### Web

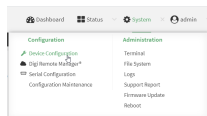
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

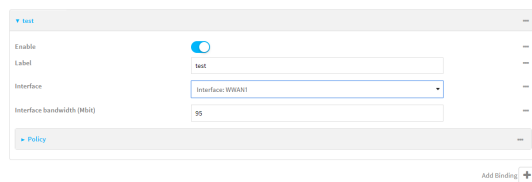


The **Configuration** window is displayed.

3. Click **Firewall > Quality of Service**.
4. For **Add Binding**, click **+**.



The quality of service binding configuration window is displayed.

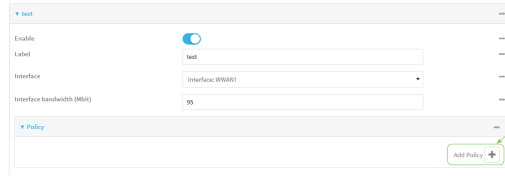


5. **Enable** the binding.
6. (Optional) Type a **Label** for the binding.
7. Select an **Interface** to queue egress packets on. The binding will only match traffic that is being sent out on this interface.
8. (Optional) For **Interface bandwidth (Mbit)**, set the maximum egress bandwidth of the interface, in megabits, allocated to this binding. Typically, this should be 95% of the available bandwidth. Allowed value is any integer between **1** and **1000**.

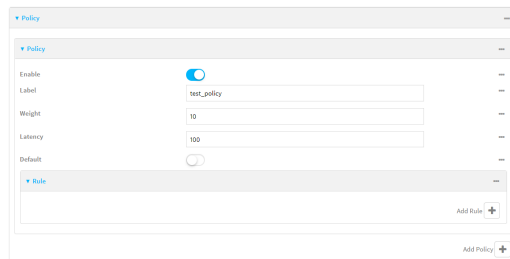
## 9. Create a policy for the binding:

At least one policy is required for each binding. Each policy can contain up to 30 rules.

- a. Click to expand **Policy**.
- b. For **Add Policy**, click **+**.

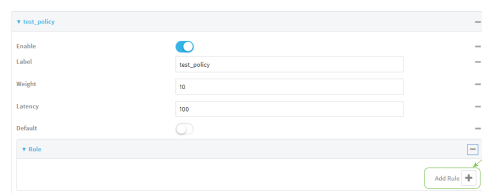


The QoS binding policy configuration window is displayed.



New QoS binding policies are enabled by default. To disable, toggle off **Enable**.

- c. (Optional) Type a **Label** for the binding policy.
- d. For **Weight**, type a value for the amount of available bandwidth allocated to the policy, relative to other policies for this binding.  
The larger the weight, with respect to the other policy weights, the larger portion of the maximum bandwidth is available for this policy. For example, if a binding contains three policies, and each policy contains a weight of 10, each policy will be allocated one third of the total interface bandwidth.
- e. For **Latency**, type the maximum delay before the transmission of packets. A lower latency means that the packets will be scheduled more quickly for transmission.
- f. Select **Default** to identify this policy as a fall-back policy. The fall-back policy will be used for traffic that is not matched by any other policy. If there is no default policy associated with this binding, packets that do not match any policy rules will be dropped.
- g. If **Default** is disabled, you must configure at least one rule:
  - i. Click to expand **Rule**.
  - ii. For **Add Rule**, click **+**.



The QoS binding policy rule configuration window is displayed.

The screenshot shows a configuration window for a rule named 'test\_rule'. At the top, there is a toggle switch for 'Enable' which is turned on. Below it, the 'Label' field contains 'test\_rule'. The 'Type Of Service' field is empty. The 'Protocol' field is a dropdown menu set to 'any'. The 'Source port' and 'Destination port' fields are both set to 'any'. At the bottom, there are two expandable sections: 'Source address' and 'Destination address', both currently collapsed.

New QoS binding policy rules are enabled by default. To disable, toggle off **Enable**.

- iii. (Optional) Type a **Label** for the binding policy rule.
- iv. For **Type Of Service**, type the value of the Type of Service (ToS) packet header that defines packet priority. If unspecified, this field is ignored.  
See <https://www.tucny.com/Home/dscp-tos> for a list of common TOS values.
- v. For **Protocol**, select the IP protocol matching criteria for this rule.
- vi. For **Source port**, type the port, or **any**, as a source traffic matching criteria.
- vii. For **Destination port**, type the port, or **any**, as a destination traffic matching criteria.
- viii. Click to expand **Source address** and select the **Type**:
  - **Any**: Source traffic from any address will be matched.
  - **Interface**: Only traffic from the selected **Interface** will be matched.
  - **IPv4 address**: Only traffic from the IP address typed in **IPv4 address** will be matched. Use the format **IPv4\_address[/netmask]**, or use **any** to match any IPv4 address.
  - **IPv6 address**: Only traffic from the IP address typed in **IPv6 address** will be matched. Use the format **IPv6\_address[/prefix\_length]**, or use **any** to match any IPv6 address.
  - **MAC address**: Only traffic from the MAC address typed in **MAC address** will be matched.
- ix. Click to expand **Destination address** and select the **Type**:
  - **Any**: Traffic destined for anywhere will be matched.
  - **Interface**: Only traffic destined for the selected **Interface** will be matched.
  - **IPv4 address**: Only traffic destined for the IP address typed in **IPv4 address** will be matched. Use the format **IPv4\_address[/netmask]**, or use **any** to match any IPv4 address.
  - **IPv6 address**: Only traffic destined for the IP address typed in **IPv6 address** will be matched. Use the format **IPv6\_address[/prefix\_length]**, or use **any** to match any IPv6 address.

Repeat to add a new rule. Up to 30 rules can be configured.

10. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a binding:

---

```
(config)> add firewall qos end
(config firewall qos 2)>
```

---

New binding are enabled by default. To disable:

---

```
(config firewall qos 2)> enable false
(config firewall qos 2)>
```

---

4. (Optional) Set a label for the new binding:

---

```
(config firewall qos 2)> label my_binding
(config firewall qos 2)>
```

---

5. Set the interface to queue egress packets on. The binding will only match traffic that is being sent out on this interface:
  - a. Use the **?** to determine available interfaces:
  - b. Set the interface. For example:

---

```
(config firewall qos 2)> interface /network/interface/eth1
(config firewall qos 2)>
```

---

6. (Optional) Set the maximum egress bandwidth of the interface, in megabits, allocated to this binding.

---

```
(config firewall qos 2)> bandwidth int
(config firewall qos 2)>
```

---

where *int* is an integer between **1** and **1000**. Typically, this should be 95% of the available bandwidth. The default is **95**.

7. Create a policy for the binding:

At least one policy is required for each binding. Each policy can contain up to 30 rules.

- a. Change to the policy node of the configuration:

---

```
(config firewall qos 2)> policy
(config firewall qos 2 policy)>
```

---



- b. Add a policy:

---

```
(config firewall qos 2 policy)> add end
(config firewall qos 2 policy 0)>
```

---

New QoS binding policies are enabled by default. To disable:

---

```
(config firewall qos 2 policy 0)> enable false
(config firewall qos 2 policy 0)>
```

---

- c. (Optional) Set a label for the new binding policy:

---

```
(config firewall qos 2 policy 0)> label my_binding_policy
(config firewall qos 2 policy 0)>
```

---

- d. Set a value for the amount of available bandwidth allocated to the policy, relative to other policies for this binding.

The larger the weight, with respect to the other policy weights, the larger portion of the maximum bandwidth is available for this policy. For example, if a binding contains three policies, and each policy contains a weight of 10, each policy will be allocated one third of the total interface bandwidth.

---

```
(config firewall qos 2 policy 0)> weight int
(config firewall qos 2 policy 0)>
```

---

where *int* is any integer between **1** and **65535**. The default is **10**.

- e. Set the maximum delay before the transmission of packets. A lower number means that the packets will be scheduled more quickly for transmission.

---

```
(config firewall qos 2 policy 0)> latency int
(config firewall qos 2 policy 0)>
```

---

where *int* is any integer, **1** or greater. The default is **100**.

- f. To identify this policy as a fall-back policy:

---

```
(config firewall qos 2 policy 0)> default true
(config firewall qos 2 policy 0)>
```

---

The fall-back policy will be used for traffic that is not matched by any other policy. If there is no default policy associated with this binding, packets that do not match any policy rules will be dropped. If the policy is not a fall-back policy, you must configure at least one rule:

- i. Change to the rule node of the configuration:

---

```
(config firewall qos 2 policy 0)> rule
(config firewall qos 2 policy 0 rule)>
```

---

- ii. Add a rule:

---

```
(config firewall qos 2 policy 0 rule)> add end
(config firewall qos 2 policy 0 rule 0)>
```

---

New QoS binding policy rules are enabled by default. To disable:

---

```
(config firewall qos 2 policy 0 rule 0)> enable false
(config firewall qos 2 policy 0 rule 0)>
```

---

- iii. (Optional) Set a label for the new binding policy rule:

---

```
(config firewall qos 2 policy 0 rule 0)> label my_binding_policy_
rule
(config firewall qos 2 policy 0 rule 0)>
```

---

- iv. Set the value of the Type of Service (ToS) packet header that defines packet priority. If unspecified, this field is ignored.

---

```
(config firewall qos 2 policy 0 rule 0)> tos value
(config firewall qos 2 policy 0 rule 0)>
```

---

where *value* is a hexadecimal number. See <https://www.tucny.com/Home/dscp-tos> for a list of common TOS values.

- v. Set the IP protocol matching criteria for this rule:

---

```
(config firewall qos 2 policy 0 rule 0)> protocol value
(config firewall qos 2 policy 0 rule 0)>
```

---

where *value* is one of **tcp**, **udp**, or **any**.

- vi. Set the source port to define a source traffic matching criteria:

---

```
(config firewall qos 2 policy 0 rule 0)> srcport value
(config firewall qos 2 policy 0 rule 0)>
```

---

where *value* is the IP port number, a range of port numbers using the format *IP\_port-IP\_port*, or **any**.

- vii. Set the destination port to define a destination matching criteria:

---

```
(config firewall qos 2 policy 0 rule 0)> dstport value
(config firewall qos 2 policy 0 rule 0)>
```

---

where *value* is the IP port number, a range of port numbers using the format *IP\_port-IP\_port*, or **any**.

- viii. Set the source address type:

---

```
(config network qos 2 policy 0 rule 0)> src type value
(config network qos 2 policy 0 rule 0)>
```

---

where *value* is one of:

- **any**: Source traffic from any address will be matched.  
See [Firewall configuration](#) for more information about firewall zones.
- **interface**: Only traffic from the selected interface will be matched. Set the interface:

- i. Use the ? to determine available interfaces:
- ii. Set the interface. For example:

---

```
(config network qos 2 policy 0 rule 0)> src interface
/network/interface/eth1
(config network qos 2 policy 0 rule 0)>
```

---

- **address:** Only traffic from the IP address typed in **IPv4 address** will be matched. Set the address that will be matched:

---

```
(config network qos 2 policy 0 rule 0)> src address value
(config network qos 2 policy 0 rule 0)>
```

---

where value uses the format **IPv4\_address[/netmask]**, or **any** to match any IPv4 address.

- **address6:** Only traffic from the IP address typed in **IPv6 address** will be matched. Set the address that will be matched:

---

```
(config network qos 2 policy 0 rule 0)> src address6 value
(config network qos 2 policy 0 rule 0)>
```

---

where value uses the format **IPv6\_address[/prefix\_length]**, or **any** to match any IPv6 address.

- **mac:** Only traffic from the MAC address typed in **MAC address** will be matched. Set the MAC address to be matched:

---

```
(config network qos 2 policy 0 rule 0)> src mac MAC_address
(config network qos 2 policy 0 rule 0)>
```

---

- ix. Set the destination address type:

---

```
(config network qos 2 policy 0 rule 0)> dst type value
(config network qos 2 policy 0 rule 0)>
```

---

where *value* is one of:

- **any:** Traffic destined for anywhere will be matched.  
See [Firewall configuration](#) for more information about firewall zones.
- **interface:** Only traffic destined for the selected **Interface** will be matched. Set the interface:
  - i. Use the ? to determine available interfaces:
  - ii. Set the interface. For example:

---

```
(config network qos 2 policy 0 rule 0)> dst interface
/network/interface/eth1
(config network qos 2 policy 0 rule 0)>
```

---

- **address:** Only traffic destined for the IP address typed in **IPv4 address** will be matched. Set the address that will be matched:

---

```
(config network qos 2 policy 0 rule 0)> src address value
(config network qos 2 policy 0 rule 0)>
```

---

where value uses the format **IPv4\_address[/netmask]**, or **any** to match any IPv4 address.

- **address6**: Only traffic destined for the IP address typed in **IPv6 address** will be matched. Set the address that will be matched:

---

```
(config network qos 2 policy 0 rule 0)> src address6 value
(config network qos 2 policy 0 rule 0)>
```

---

where value uses the format **IPv6\_address[/prefix\_length]**, or **any** to match any IPv6 address.

Repeat to add a new rule. Up to 30 rules can be configured.

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Web filtering

Web filtering allows you to control access to services that can be accessed through the Connect EZ device by forwarding all Domain Name System (DNS) traffic to a web filtering service. This allows the network security administrator to configure a set of policies with the web filtering service that are applied to all routing devices with web filtering enabled. For example, a policy may allow or deny access to a specific service or type of service such as social media, gaming, and so on.

Your Connect EZ device supports two methods for configuring web filtering:

- Cisco Umbrella (formally known as OpenDNS).
- Manual DNS server entry.

### Configure web filtering with Cisco Umbrella

#### Required configuration items

- Enable web filtering.
- A Cisco Umbrella account.  
See <https://umbrella.cisco.com> for information about how to create a Cisco Umbrella account. A 14 day trial account is available.
- A customer-specific API token.

### Task one: Generate a Cisco Umbrella API token

1. Log into the Cisco Umbrella Dashboard (<https://dashboard.umbrella.com>).
2. On the menu, select **Admin > API Keys**.  
The **API Keys** page displays.
3. Click **+** (**Create**).
4. Select **Legacy Network Devices**.
5. Click **Create**.
6. Copy the token.

### Task two: Configure web filtering

#### Web

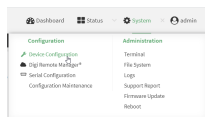
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

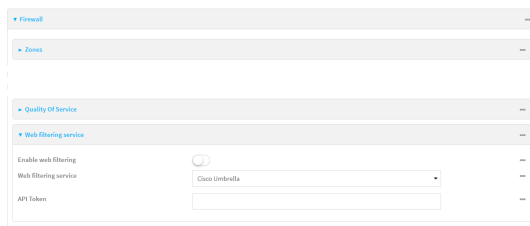
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Firewall > Web filtering service**.



4. Click **Enable web filtering** to enable.
5. For **Web filtering service**, select **Cisco Umbrella**.
6. Paste the **API token** that was generated in [Task one: Generate a Cisco Umbrella API token](#).

- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Enable web filtering:

```
(config)> firewall web-filter enable true
(config)>
```

- Set the web filter service type to **umbrella**:

```
(config)> firewall web-filter service umbrella
(config)>
```

- Set `umbrella_token` to the API token generated in [Task one: Generate a Cisco Umbrella API token](#):

```
(config)> firewall web-filter umbrella_token token
(config)>
```

- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### **Clear the Cisco Umbrella device ID**

If the Cisco Umbrella device ID being used by your Connect EZ is invalid, you can clear the device ID.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the Admin CLI prompt, use the `rm` command to delete the **web-filter-id** file, and confirm the deletion:

```
> rm /etc/config/web-filter-id
rm: remove '/etc/config/web-filter-id'? yes
>
```

### 3. Restart the web filtering service:

```
> config firewall web-filter enable false
> config firewall web-filter enable true
>
```

## Configure web filtering with manual DNS servers

### Required configuration items

- Enable web filtering.
- The IP address of one or more DNS servers. Cisco provides two open DNS servers for web filtering:
  - 208.67.222.220
  - 208.67.220.222

See <https://www.opendns.com/setupguide/> for more information about using Cisco DNS servers for web filtering.

To configure web filtering with manual DNS servers:

### ≡ Web

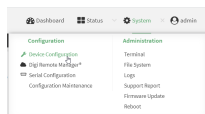
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device.](#)
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

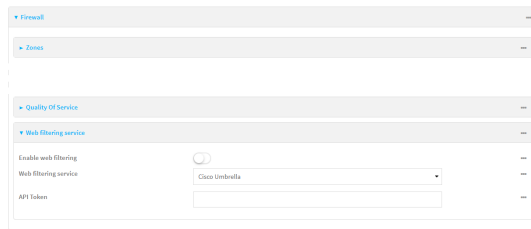
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

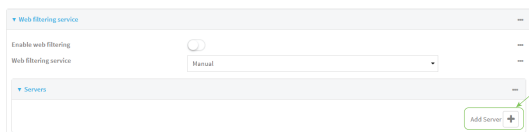


The **Configuration** window is displayed.

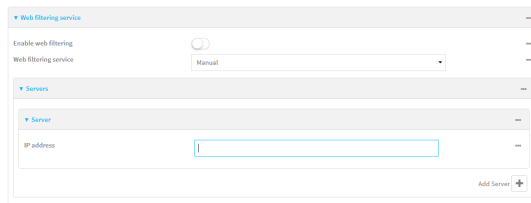
3. Click **Firewall > Web filtering service**.



4. Click **Enable web filtering** to enable.
5. For **Web filtering service**, select **Manual**.
6. Click to expand **Servers**.
7. Click **+** to add a server.



8. For **IP address**, enter the IP address of the DNS server.



9. (Optional) Repeat for additional DNS servers.
10. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable web filtering:

```
(config)> firewall web-filter enable true
(config)>
```



4. Set the web filter service type to **manual**:

```
(config)> firewall web-filter service manual
(config)>
```

5. Add a DNS server:

```
(config)> add firewall web-filter server end
(config firewall web-filter server 0)>
```

6. Set the DNS server's IP address:

```
(config firewall web-filter server 0)> ip ip_address
(config firewall web-filter server 0)>
```

7. (Optional) Repeat for additional DNS servers.

For example, to configure manual web-filtering using Cisco's open DNS servers:

- a. Enable web filtering:

```
(config)> firewall web-filter enable true
(config)>
```

- b. Set the web filter service type to **manual**:

```
(config)> firewall web-filter service manual
(config)>
```

- c. Add the first DNS server:

- i. Add the server:

```
(config)> add firewall web-filter server end
(config firewall web-filter server 0)>
```

- ii. Set the server's IP address:

```
(config firewall web-filter server 0)> ip 208.67.222.220
(config firewall web-filter server 0)>
```

- d. Add the second DNS server:

- i. Move back one node in the configuration tree:

```
(config firewall web-filter server 0)> ..
(config firewall web-filter server)>
```

- ii. Add the server:

```
(config firewall web-filter server)> add end
(config firewall web-filter server 1)>
```

- iii. Set the server's IP address:

```
(config firewall web-filter server 1)> ip 208.67.222.222
(config firewall web-filter server 0)>
```

8. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Verify your web filtering configuration

If your web filtering implementation has the service set to Cisco Umbrella, or if it is configured to use manual DNS servers and uses the Cisco open DNS servers, you can verify the web filtering implementation by using the Cisco test site [www.internetbadguys.com](http://www.internetbadguys.com).

To verify the implementation:

### Web

This procedure assumes you have already configured web filtering to use either Cisco Umbrella or the Cisco open DNS servers.

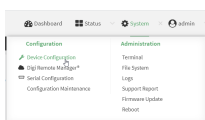
- See [Configure web filtering with Cisco Umbrella](#) for information about configuring web filtering with Cisco Umbrella.
  - See [Configure web filtering with manual DNS servers](#) for information about configuring web filtering to use Cisco open DNS servers.
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
  2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

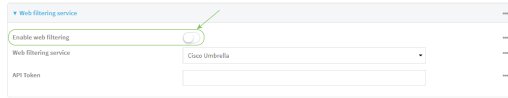
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Disable web filtering:
  - a. Click **Firewall > Web filtering service**.
  - b. Click **Enable web filtering** to disable.



- c. Click **Apply** to save the configuration and apply the change.
4. From a new tab in your browser, attempt to connect to the Cisco test URL <http://www.internetbadguys.com>.  
The connection should be successful.
5. Return to the Connect EZ WebUI and enable web filtering:
  - a. Click **Firewall > Web filtering service**.
  - b. Click **Enable web filtering** to enable.
  - c. Click **Apply** to save the configuration and apply the change.
6. From your browser, attempt to connect to <http://www.internetbadguys.com> again.  
The connection attempt should fail with the message, "This site is blocked due to a phishing threat."

### Command line

This procedure assumes you have already configured web filtering to use either Cisco Umbrella or the Cisco open DNS servers.

- See [Configure web filtering with Cisco Umbrella](#) for information about configuring web filtering with Cisco Umbrella.
  - See [Configure web filtering with manual DNS servers](#) for information about configuring web filtering to use Cisco open DNS servers.
1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
  2. Disable web filtering:

---

```
> config firewall web-filter enable false
>
```

---

3. Attempt to connect to the Cisco test URL <http://www.internetbadguys.com> by using either a web browser or the **curl** command from a Linux shell:

---

```
$ curl -I http://www.internetbadguys.com
HTTP/1.1 200 OK
Server: Apache
Content-Type: text/html; charset=UTF-8
Accept-Ranges: bytes
Date: Thu, Jan 11, 2024 12:10:00
```

---

---

```
X-Varnish: 4201397492
Age: 0
Via: 1.1 varnish
Connection: keep-alive
```

```
$
```

---

You should receive an "HTTP/1.1 200 OK" message, as highlighted above.

- Return to the Admin CLI and enable web filtering:

---

```
> config firewall web-filter enable true
>
```

---

- Attempt to connect to <http://www.internetbadguys.com> again:

---

```
$ curl -I www.internetbadguys.com
HTTP/1.1 403 Forbidden
Server: openresty/1.9.7.3
Date: Thu, Jan 11, 2024 12:10:00
Content-Type: text/html
Connection: keep-alive
```

```
$
```

---

You should receive an "HTTP/1.1 403 Forbidden" message, as highlighted above.

## Show web filter service information

To view information about the web filter service:

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the Admin CLI prompt, use the [show web-filter](#) command to view information about the web-filter service:

---

```
> show web-filter

Enabled      : true
Service     : umbrella
Device ID   : 0004b5s63f5e2de7aa
```

```
>
```

---

If the device is configured to use Cisco Umbrella for web filtering, a device ID is displayed. The device ID is a unique ID assigned to the device by Cisco Umbrella. If there is a problem with the device ID, you can clear the ID. See [Clear the Cisco Umbrella device ID](#) for instructions.

## System administration

---

This chapter contains the following topics:

|                                                                |     |
|----------------------------------------------------------------|-----|
| Review device status .....                                     | 614 |
| Configure system information .....                             | 615 |
| Update system firmware .....                                   | 617 |
| Reboot your Connect EZ device .....                            | 623 |
| Erase device configuration and reset to factory defaults ..... | 625 |
| Locate the device by using the Find Me feature .....           | 631 |
| Enable FIPS mode .....                                         | 632 |
| Configuration files .....                                      | 634 |
| Schedule system maintenance tasks .....                        | 639 |
| Disable device encryption .....                                | 644 |
| Configure the speed of your Ethernet port .....                | 646 |
| Configure the system watchdog .....                            | 648 |

## Review device status

You can review the system of your device from either the **Status** page of the Web interface, or from the command line:

### Web

To display system information:

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **Status**.  
A secondary menu appears, along with a status panel.
2. On the secondary menu, click to display the details panel for the status you want to view.

### Command line

To display system information, use the `show system` command.

- Show basic system information:
  1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type `admin` to access the Admin CLI.
  2. Enter `show system` at the prompt:

---

```
> show system

Model                : Digi Connect EZ
Serial Number        : Connect EZxxxxxxxxxyyyxx
SKU                  : Connect EZ
Hostname              : Connect EZ
MAC Address           : DF:DD:E2:AE:21:18

Hardware Version     : 50001947-01 1P
Firmware Version     : 24.3
Alt. Firmware Version : 24.3
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version   : 19.7.23.0-15f936e0ed

Current Time         : Thu, Jan 11, 2024 12:10:00 +0000
CPU                  : 1.4%
Uptime               : 6 days, 6 hours, 21 minutes, 57 seconds
(541317s)
Temperature          : 40C
Location             :
```

---

---

```
Contact :
```

```
>
```

---

- Show more detailed system information:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Enter **show system verbose** at the prompt:

---

```
> show system verbose
```

```

Model                : Digi Connect EZ
Serial Number        : Connect EZxxxxxxxxxyyyxx
SKU                  : Connect EZ
Hostname              : Connect EZ
MAC Address          : DF:DD:E2:AE:21:18

Hardware Version     : 50001947-01 1P
Firmware Version     : 24.3
Alt. Firmware Version : 24.3
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version   : 19.7.23.0-15f936e0ed
Schema Version       : 715

Timezone              : UTC
Current Time          : Thu, Jan 11, 2024 12:10:00 +0000
CPU                   : 1.4%
Uptime                : 6 days, 6 hours, 21 minutes, 57 seconds
(541317s)
Load Average          : 0.01, 0.03, 0.02
RAM Usage              : 119.554MB/1878.984MB(6%)
Temperature           : 40C
Location              :
Contact               :
Disk
----
Disk /etc/config Usage : 18.421MB/4546.371MB(0%)
Disk /var/log_mnt Usage : 0.104MB/14.868MB(1%)
Disk /opt Usage        : 215.739MB/458.328MB(50%)
Disk /tmp Usage        : 0.003MB/120.0MB(0%)
Disk /var Usage        : 0.816MB/32.0MB(3%)

```

```
>
```

---

## Configure system information

You can configure information related to your Connect EZ device, such as providing a name and location for the device.

## Configuration items

- A name for the device.
- The name of a contact for the device.
- The location of the device.
- A description of the device.
- A banner that will be displayed when users access terminal services on the device.

To enter system information:

### Web

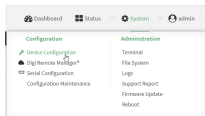
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System**.
4. For **Name**, type a name for the device. This name will appear in log messages and at the command prompt.
5. For **Contact**, type the name of a contact for the device.
6. For **Location**, type the location of the device.
7. For **Banner**, type a banner message that will be displayed when users log into terminal services on the device.
8. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.



Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Set a name for the device. This name will appear in log messages and at the command prompt.

```
(config)> system name 192.168.3.1
192.168.3.1(config)>
```

4. Set the contact for the device:

```
192.168.3.1(config)> system contact "Jane User"
192.168.3.1(config)>
```

5. Set the location for the device:

```
192.168.3.1(config)> system location "9350 Excelsior Blvd., Suite 700,
Hopkins, MN"
192.168.3.1(config)>
```

6. Set the banner for the device. This is displayed when users access terminal services on the device.

```
192.168.3.1(config)> system banner "Welcome to the Digi Connect EZ."
192.168.3.1(config)>
```

7. Save the configuration and apply the change

```
192.168.3.1(config)> save
Configuration saved.
192.168.3.1>
```

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Update system firmware

The Connect EZ operating system firmware images consist of a single file with the following naming convention:

***platform-version.bin***

For example, **Connect EZ-24.3.bin**.

## Manage firmware updates using Digi Remote Manager

If you have a network of many devices, you can use Digi Remote Manager **Profiles** to manage firmware updates. Profiles ensure all your devices are running the correct firmware version and that all newly installed devices are updated to that same version. For more information, see the **Profiles** section of the [Digi Remote Manager User Guide](#).

## Certificate management for firmware images

The system firmware files are signed to ensure that only Digi-approved firmware load onto the device. The Connect EZ device validates the system firmware image as part of the update process and only successfully updates if the system firmware image can be authenticated.

## Downgrading

Downgrading to an earlier release of the firmware may result in the device configuration being erased.

### Downgrading from firmware version 22.2.9.x

Beginning with firmware version 22.2.9.x, the Connect EZ device uses certificate-based communication for enhanced security when connecting to Digi Remote Manager. If you downgrade your firmware from version 22.2.9.x to version 21.11.x or previous, your device will no longer be able to communicate with Remote Manager.

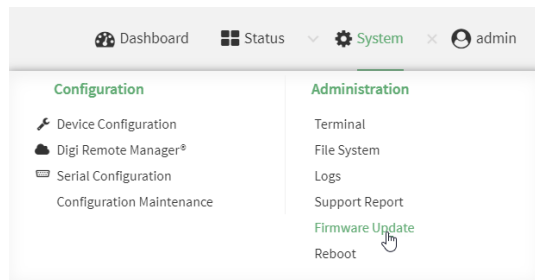
To remedy this issue, select the device in Remote Manager and select **Actions > Reset Device Certificate**.

## Update firmware over the air (OTA) from the Digi firmware server

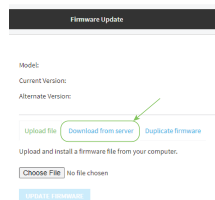
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



2. Click **Download from server**.



3. For **Version:**, select the appropriate version of the device firmware.
4. Click **Update Firmware**.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. >Use the **system firmware ota check** command to determine if new modem firmware is available on the Digi firmware repository.

---

```
> system firmware ota check
Current firmware version is 23.9.74.0
Checking for latest Connect EZ firmware...
Newest firmware version available to download is '24.3'
Device firmware update from '23.9.74.0' to '24.3' is needed
>
```

---

3. Use the **modem firmware ota list** command to list available firmware on the Digi firmware repository.

---

```
> system firmware ota list
23.9.74.0
24.3
>
```

---

4. Perform an OTA firmware update:

- To perform an OTA firmware update by using the most recent available firmware from the Digi firmware repository:

- a. Update the firmware:

---

```
> system firmware ota update
Downloading firmware version '24.3'...
Downloaded firmware /tmp/cli_firmware.bin remaining
Applying firmware version '24.3'...
41388K
netflash: got "/tmp/cli_firmware.bin", length=42381373
netflash: authentication successful
netflash: vendor and product names are verified.
netflash: programming FLASH device /dev/flash/image1
41408K 100%
Firmware update completed, reboot device
>
```

---

- b. Reboot the device:

---

```
> reboot
>
```

---

- To perform an OTA firmware update by using a specific version from the Digi firmware repository, use the **version** parameter to identify the appropriate firmware version as determined by using **system firmware ota list** command. For example:

- a. Update the firmware:

---

```
> system firmware ota update version 24.3
Downloading firmware version '24.3'...
Downloaded firmware /tmp/cli_firmware.bin remaining
```

---

```

Applying firmware version '24.3'...
41388K
netflash: got "/tmp/cli_firmware.bin", length=42381373
netflash: authentication successful
netflash: vendor and product names are verified.
netflash: programming FLASH device /dev/flash/image1
41408K 100%
Firmware update completed, reboot device
>

```

- b. Reboot the device:

```

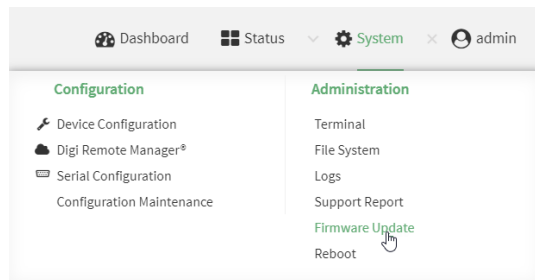
> reboot
>

```

## Update firmware from a local file

### Web

1. Download the Connect EZ operating system firmware from the Digi Support FTP site to your local machine.  
Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Choose file**.
4. Browse to the location of the firmware on your local file system and select the file.
5. Click **Update Firmware**.

### Command line

1. Download the Connect EZ operating system firmware from the Digi Support FTP site to your local machine.
2. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
3. Load the firmware image onto the device. We recommend using the /tmp directory.

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect EZ-24.3.bin local /tmp/ to local
admin@192.168.4.1's password: adminpwd
Connect EZ-24.3.bin          100%   36MB   11.1MB/s   00:03
>
```

---

4. Verify that the firmware file has been successfully uploaded to the device:

---

```
> ls /tmp
-rw-r--r--  1 root   root   37511229 May 16 20:10 Connect EZ-24.3.bin
-rw-r--r--  1 root   root    2580 May 16 16:44 blank.json
...
>
```

---

5. Update the firmware by entering the [system firmware update](#) command, specifying the path and file name to the firmware file:

---

```
> system firmware update file /tmp/Connect EZ-24.3.bin
36632K
netflash: got "/tmp/Connect EZ-24.3.bin", length=37511229
netflash: authentication successful
netflash: programming FLASH device /dev/flash/image
36633K 100%
Firmware update completed, reboot device
>
```

---

6. Reboot the device to run the new firmware image using the [reboot](#) command.

---

```
> reboot
Rebooting system
>
```

---

7. Once the device has rebooted, log into the Connect EZ's command line as a user with Admin access and verify the running firmware version by entering the [show system](#) command.

---

```
> show system

Hostname           : Connect EZ
FW Version         : 24.3
MAC                : 0040FF800120
```

---

---

```

Model           : Digi Connect EZ
Current Time    : Thu, Jan 11, 2024 12:10:00 +0000
Uptime         : 42 seconds (42s)

```

---

&gt;

## Dual boot behavior

By default, the Connect EZ device stores two copies of firmware in two flash memory banks:

- The current firmware version that is used to boot the device.
- A copy of the firmware that was in use prior to your most recent firmware update.

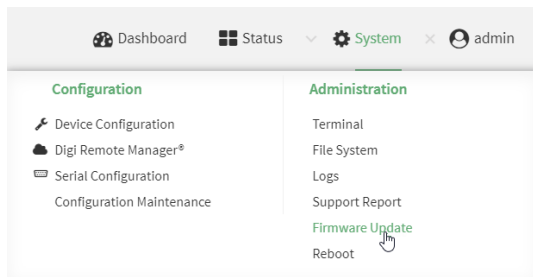
When the device reboots, it will attempt to use the current firmware version. If the current firmware version fails to load after three consecutive attempts, it is marked as invalid and the device will use the previous firmware version stored in the alternate memory bank.

If the device consistently loses power during the boot process, this may result in the current firmware being marked as invalid and the device downgrading to a previous version of the firmware. As a result of this behavior, you can use the following procedure to guarantee that the same firmware is stored in both memory banks:

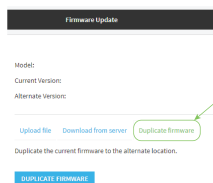
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



2. Click **Duplicate firmware**.



3. Click **Duplicate Firmware**.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Duplicate the firmware:

---

```
> system duplicate-firmware
>
```

---

## Reboot your Connect EZ device

You can reboot the Connect EZ device immediately or schedule a reboot for a specific time every day.

**Note** You may want to save your configuration settings to a file before rebooting. See [Save configuration to a file](#).

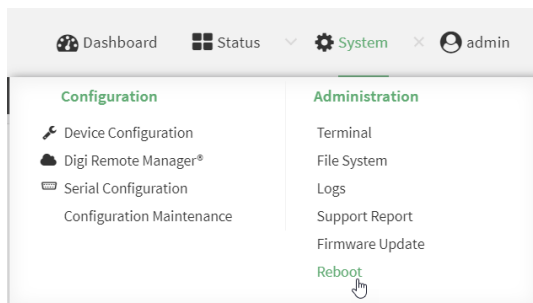
---

### Reboot your device immediately

#### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. From the main menu, click **System**.
2. Click **Reboot**.



3. Click **Reboot** to confirm that you want to reboot the device.

#### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

---

```
> reboot
```

---

### Schedule reboots of your device

## Web

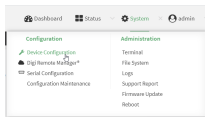
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Select **System > Scheduled tasks**.
4. For **Reboot time**, enter the time of the day that the device should reboot, using the format *HH:MM*. The device will reboot at this time every day.  
If **Reboot time** is set, but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See [System time](#) for information about configuring NTP servers. If **Reboot window** is set, the reboot will occur during a random time within the reboot window.
5. For **Reboot window**, enter the maximum random delay that will be added to **Reboot Time**. Allowed values are any number of hours, minutes, or seconds, and take the format *number {h|m|s}*.  
For example, to set **parameter name** to ten minutes, enter **10m** or **600s**. The default is **10m**, and the maximum allowed time is **24h**.
6. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```



3. Set the reboot time:

---

```
(config>> system schedule reboot_time time
(config)>
```

---

where *time* is the time of the day that the device should reboot, using the format *HH:MM*. For example, to set the device to reboot at two in the morning every day:

---

```
(config>> system schedule reboot_time 02:00
(config)>
```

---

If **reboot\_time** is set, but the device is unable to synchronize its time with an NTP server, the device will reboot after it has been up for 24 hours. See [System time](#) for information about configuring NTP servers. If **reboot\_window** is set, the reboot will occur during a random time within the reboot window.

4. Set the maximum random delay that will be added to **reboot\_time**:

---

```
(config>> system schedule reboot_window value
(config)>
```

---

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **reboot\_window** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> system schedule reboot_window 600s
(config)>
```

---

5. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Erase device configuration and reset to factory defaults

You can erase the device configuration in the WebUI, at the command line, or by using the **RESET** button on the device. Erasing the device configuration performs the following actions:

- Clears all configuration settings. When the device restarts, it uses the factory default configuration.
- Deletes all user files including Python scripts.
- Clears event and system log files.

Additionally, if the **RESET** button is used to erase the configuration, pressing the **RESET** button a second time immediately after the device has rebooted:

- Erases all automatically generated certificates and keys.
- With firmware release 22.2.9.x and newer, erases the client-side certificate used for communication with Digi Remote Manager.

If you are using Digi Remote Manager with firmware release 22.2.9.x and newer, by default the device uses a client-side certificate for communication with Remote Manager. If the client-side certificate is erased, you must use the Remote Manager interface to reset the certificate.

- If your device uses a [custom factory default](#), the custom factory default will be removed and the device will reboot using standard factory default settings.

You can also reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command.

### Reset the device by using the RESET button

1. Locate the **RESET** button on your device.
2. Press the **RESET** button perform a device reset. The **RESET** button has the following modes:
  - **Configuration reset:**
    - Press and release the **RESET** button .
    - The device reboots automatically and resets to factory defaults. This does not remove any automatically generated certificates and keys.
  - **Full device reset:**
    - After the device reboots from the first button press, immediately press and release the **RESET** button again.
    - The device reboots again and resets to factory defaults, as well as also removing generated certificates and keys.
3. After resetting the device:
  - a. Connect to the Connect EZ by using the serial port or by using an Ethernet cable to connect the Connect EZ **ETH2** port to your PC.
  - b. Log into the Connect EZ:
 

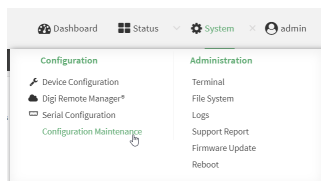
**User name:** Use the default user name: **admin**.

**Password:** Use the unique password printed on the bottom label of the device (or the printed label included in the package).
  - c. (Optional) Reset the default password for the admin account. See [Change the default password for the admin user](#) for further information.

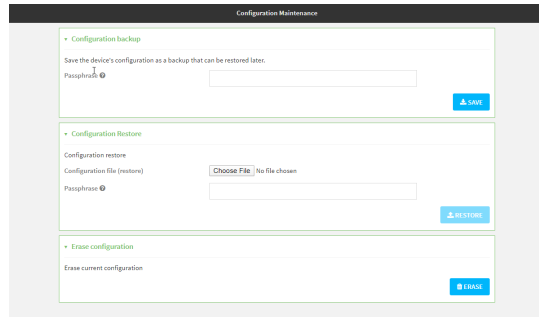
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

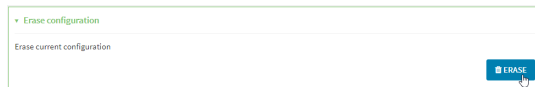
1. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



2. In the **Erase configuration** section, click **ERASE**.



3. Click **CONFIRM**.
4. After resetting the device:
  - a. Connect to the Connect EZ by using the serial port or by using an Ethernet cable to connect the Connect EZ **ETH2** port to your PC.
  - b. Log into the Connect EZ:
 

**User name:** Use the default user name: **admin**.

**Password:** Use the unique password printed on the bottom label of the device (or the printed label included in the package).
  - c. (Optional) Reset the default password for the admin account. See [Change the default password for the admin user](#) for further information.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights. Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

```
> system factory-erase
```

3. After resetting the device:
  - a. Connect to the Connect EZ by using the serial port or by using an Ethernet cable to connect the Connect EZ **ETH2** port to your PC.
  - b. Log into the Connect EZ:
 

**User name:** Use the default user name: **admin**.

**Password:** Use the unique password printed on the bottom label of the device (or the printed label included in the package).
  - c. (Optional) Reset the default password for the admin account. See [Change the default password for the admin user](#) for further information.

### Reset the device with the revert command

You can reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, enter **revert**:

```
(config)> revert
(config)>
```

4. Set the password for the admin user prior to saving the changes:

```
(config)> auth user admin password pwd
(config)>
```

5. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Custom factory default settings

You can configure your Connect EZ device to use custom factory default settings. This way, when you erase the device's configuration, the device will reset to your custom configuration rather than to the original factory defaults.

### Required configuration items

- Custom factory default file.

### Configure the Connect EZ device to use custom factory default settings

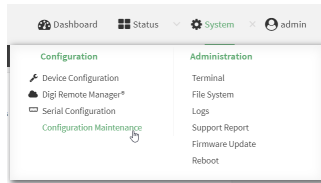
#### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

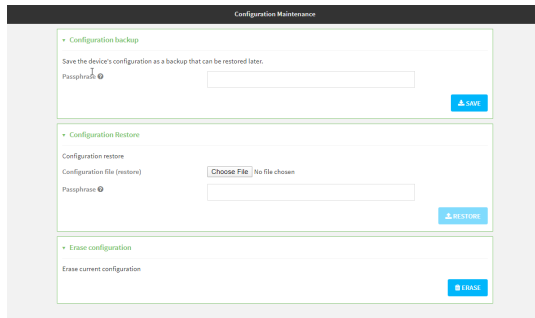
1. Configure your Connect EZ device to match the desired custom factory default configuration.

For example, you may want to configure the device to use a custom APN or a particular network configuration, so that when you reset the device to factory defaults, it will automatically have your required network configuration.

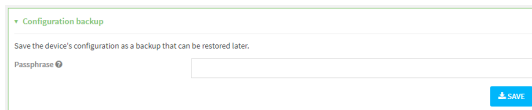
- On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.

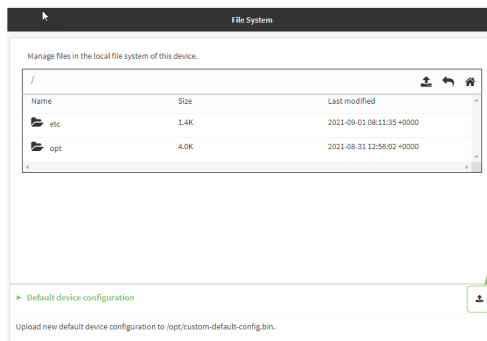


- In the **Configuration backup** section, click **SAVE**.



Do not set a **Passphrase** for the configuration backup. The file will be downloaded using your browser's standard download process.

- After the configuration backup file has been downloaded, rename the file to:
  - custom-default-config.bin**
- Upload the file to the device:
  - From the main menu, select **System > Filesystem**.
  - Under **Default device configuration**, click **⬆️**.



- Select the file from your local file system.
- Reboot** the device.

---

**Note** After configuring a device to use custom factory default settings, wait five minutes after restoring to defaults before:

- Powering off the device.
- Performing any additional [configuration restoration activities](#).

If you do not wait five minutes after restoring to custom factory defaults before performing these activities, the device will clear the custom factory defaults and reboot to standard factory defaults.

---

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Enter the following:

---

```
> system backup / type custom-defaults
Backup saved as /opt/custom-default-config.bin
>
```

---

3. Reboot the device:

---

```
> reboot
>
```

---

4. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.
- 

**Note** After configuring a device to use custom factory default settings, wait five minutes after restoring to defaults before:

- Powering off the device.
- Performing any additional [configuration restoration activities](#).

If you do not wait five minutes after restoring to custom factory defaults before performing these activities, the device will clear the custom factory defaults and reboot to standard factory defaults.

---

### Clear the custom factory default settings

After configuring the device to use custom factory default settings, to clear the custom default configuration and reset the device to standard factory defaults:

1. Press the device's [RESET button](#).
2. Wait for the device to reboot.
3. Press the RESET button a second time.

You must press the RESET the second time within five minutes of the first in order to clear the custom default configuration.

## Locate the device by using the Find Me feature

Use the **Find Me** feature to cause LEDs on the device to blink, which can help you to identify the specific device. For the Connect EZ, the Power LED blinks when the Find Me feature is in use.

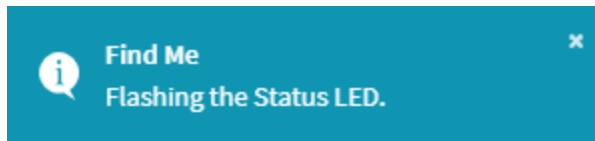
To use this feature:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **Find Me**.

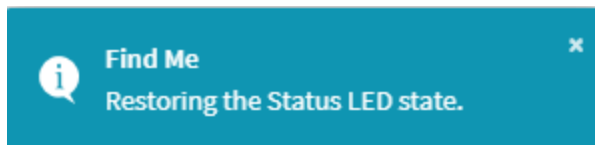
A notification message appears, noting that the LED is flashing on the device. Click the **x** in the message to close it.



2. On the menu, click **System** again. A blue circle next to **Find Me** is blinking, indicating that the **Find Me** feature is active.

3. To deactivate the **Find Me** feature, click **System** and click **Find Me** again.

A notification message appears, noting that the LED is no longer flashing on the device. Click the **x** in the message to close it.



### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. To activate the **Find Me** feature, at the prompt, type the following at the command prompt:

```
> system find-me on
>
```

3. To deactivate the **Find Me** feature, type the following at the command prompt:

```
> system find-me off
>
```

4. To determine the status of the **Find Me** feature, type the following at the command prompt:

```
> system find-me status
off
>
```

## Enable FIPS mode

You can enable your device to be Federal Information Processing Standard (FIPS) 140-2 compliant. With FIPS 140-2 compliance, only FIPS 140-2 cipher and MAC algorithms are available. As a result, features like stunnel, ssh, and openvpn are limited in what they can use. For example, in FIPS mode ssh will only offer and negotiate AES based ciphers.

When the FIPS setting is changed, the device will reboot automatically. Disabling FIPS after it has been enabled will cause the current configuration to be erased.

### ≡ Web

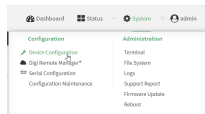
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.



3. Expand **System**.

The screenshot shows a configuration page for a system. At the top, there is a 'System' header with a dropdown arrow and three dots. Below it, the 'FIPS' section is visible with a toggle switch that is currently turned off. Underneath, there are several input fields: 'Name' (containing 'Techpubs'), 'Contact', 'Location', 'Description', and 'Banner'. At the bottom of the page, there are several expandable sections, each with a right-pointing arrow and three dots: 'Time', 'Log', 'Scheduled tasks', 'Power', 'Containers', and 'Advanced watchdog'.

4. Click to enable **FIPs**.
5. Click **Apply** to save the configuration and apply the change.
6. Click **System > Reboot** to reboot the device.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Enable FIPS:

```
(config)> system fips true
>
```

3. Save the change:

```
(config)> save
>
```

4. Reboot the device:

```
> reboot
>
```

## Configuration files

The Connect EZ configuration file, `/etc/config/accns.json`, contains all configuration changes that have been made to the device. It does not contain the complete device configuration; it only contains changes to the default configuration. Both the default configuration and the changes contained in the `accns.json` file are applied when the device reboots.

## Save configuration changes

When you make changes to the Connect EZ configuration, the changes are not automatically saved. You must explicitly save configuration changes, which also applies the changes. If you do not save configuration changes, the system discards the changes.

### Web

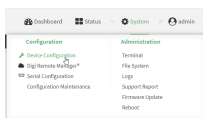
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Make any necessary configuration changes.
4. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Make any necessary configuration changes.
- Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Save configuration to a file

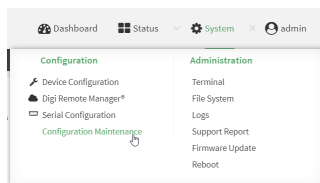
You can save your Connect EZ device's configuration to a file and use this file to restore the configuration, either to the same device or to similar devices.

### Web

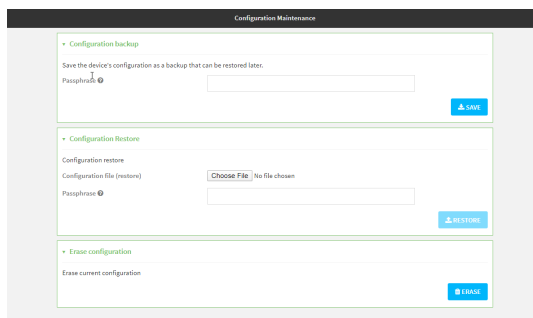
This procedure creates a binary archive file containing the device's configuration, certificates and keys, and other information.

Log into the Connect EZ WebUI as a user with full Admin access rights.

- On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** windows is displayed.



- In the **Configuration backup** section:
  - (Optional) To encrypt the configuration using a passphrase, for **Passphrase (save/restore)**, enter the passphrase.
  - Click **SAVE**.

The file will be downloaded using your browser's standard download process.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Enter the following:

---

```
> system backup path [passphrase passphrase] type type
```

---

where

- *path* is the location on the Connect EZ's filesystem where the configuration backup file should be saved.
- *passphrase* (optional) is a passphrase used to encrypt the configuration backup.
- *type* is the type of backup, either:
  - **archive**: Creates a binary archive file containing the device's configuration, certificates and keys, and other information.
  - **cli-config**: Creates a text file containing only the configuration changes.

For example:

---

```
> system backup /etc/config/scripts/ type archive
```

---

3. (Optional) Use **scp** to copy the file from your device to another host:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the Connect EZ device.

For example:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/ local /etc/config/backup-archive-0040FF800120-19.05.17-19.01.17.bin to remote
```

---

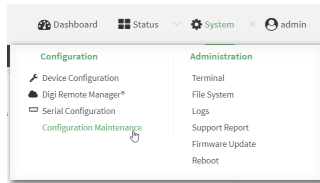
## Restore the device configuration

You can restore a configuration file to your Connect EZ device by using a backup from the device, or a backup from a similar device.

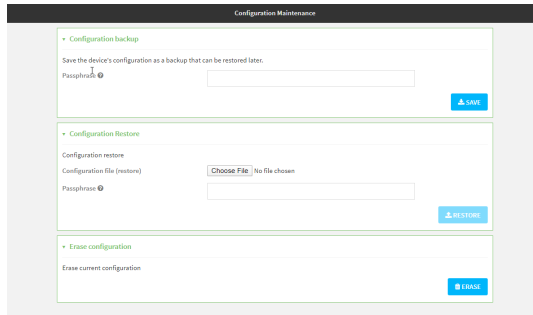
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



The **Configuration Maintenance** window is displayed.



2. In the **Configuration Restore** section:
  - a. If a passphrase was used to create the configuration backup, for **Passphrase (save/restore)**, enter the passphrase.
  - b. Under **Configuration Restore**, click **Choose File**.
  - c. Browse to the system firmware file location on your local computer and select the file.
  - d. Click **RESTORE**.
3. Click **CONFIRM**.  
The configuration will be restored and the device will be rebooted.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. If the configuration backup is on a remote host, use **scp** to copy the file from the host to your device:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied

to the Connect EZ device.

- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/backup-archive-0040FF800120-24.3-19.23.42.bin local /opt to local
```

---

3. Enter the following:

---

```
> system restore filepath [passphrase passphrase]
```

---

where

- *filepath* is the the path and filename of the configuration backup file on the Connect EZ's filesystem (*local-path* in the previous step).
- *passphrase* (optional) is the passphrase to restore the configuration backup, if a passphrase was used when the backup was created.

For example:

---

```
> system restore /opt/backup-archive-0040FF800120-24.3-19.23.42.bin
```

---

## Schedule system maintenance tasks

You can configure tasks to be run during a specified maintenance window. When the device is within its maintenance window, firmware updates and Digi Remote Manager configuration checks will be performed.

You can also schedule custom scripts to run during the maintenance window. See [Configure scripts to run automatically](#) for more information.

### Required configuration items

- Events that trigger the maintenance window to begin.
- Whether all configured triggers, or only one of the triggers, must be met.
- The tasks to be performed. Options are:
  - Firmware updates.
  - Digi Remote Manager configuration check.
- Whether the device will check for updates to the device firmware.
- The frequency (daily, weekly, or monthly) that checks for firmware updates will run.

### ≡ Web

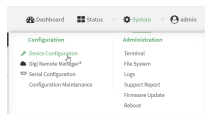
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

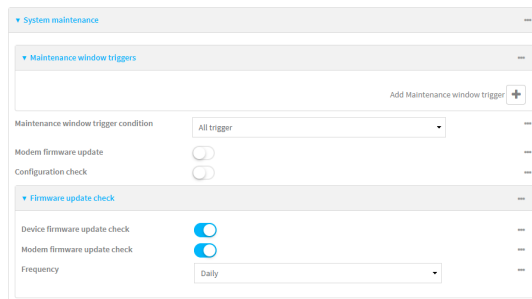
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System > Scheduled tasks > System maintenance**.



4. Click to expand **Maintenance window triggers**.  
 5. Click **+** to add a maintenance window trigger.



6. For **Maintenance window trigger type**, select one of the following:
- **Check if interface is up**, for **Test Interface**, select the interface.
  - **Time period for maintenance window:**

- a. Click to expand **Maintenance window**.
- b. For **Start time**, type the time of day that the maintenance window should start, using the syntax *HH:MM*. If **Start time** is not set, maintenance tasks are not scheduled and will not be run.

The behavior of **Start time** varies depending on the setting of **Duration window**, which is configured in the next step.

- If **Duration window** is set to **Immediately**, all scheduled tasks will begin at the exact time specified in **Start time**.
  - If **Duration window** is set to **24 hours**, **Start time** is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting **Duration window** to **24 hours** can potentially overstress the device and should be used with caution.
  - If **Duration window** is set to any value other than to **Immediately** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
  - If **Duration window** is set to one or more hours, the minutes field in **Start time** is ignored and the duration window will begin at the beginning of the specified hour.
- c. For **Duration window**, select the amount of time that the maintenance tasks will be run. If **Immediately** is selected, all scheduled tasks will begin at the exact time specified in **Start time**.
  - d. For **Frequency**, select whether the maintenance window will be started every day, or once per week.



- If **Check if Python Out-of-Service** is set, the maintenance window will only start if the Python Out-of-Service is set. See [Use Python to set the maintenance window](#) for further information.
- 7. If **Central Management** is disabled, click **Device firmware update** to instruct the system to look for any updated device firmware during the maintenance window. If updated firmware is found, it will then be installed. This options is only available if **Central Management** is disabled; see [Central management](#) for more information.
- 8. The **Modem firmware update** option, which is only available if **Central Management** is disabled, is not used with the Connect EZ.
- 9. (Optional) Configure automated checking for device firmware updates:
  - a. Click to expand **Firmware update check**.
  - b. **Device firmware update check** is enabled by default. This enables the automated checking for device firmware updates.
  - c. **Modem firmware update check** is enabled by default. This enables the automated checking for modem firmware updates.

---

**Note** The **Modem firmware update** option is not used with theConnect EZ. Any selection is ignored.

---

  - d. For **Frequency**, select how often automated checking for device and modem firmware should take place. Allowed values are **Daily**, **Weekly**, and **Monthly**. The default is **Daily**.
- 10. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Configure a system maintenance trigger:
  - a. Add a trigger:

---

```
(config)> add system schedule maintenance trigger end
(config)>
```

---

- b. Set the type of trigger:

---

```
(config add system schedule maintenance trigger)> type value
(config)>
```

---

where *value* is one of:

- **interface\_up:** If **interface\_up** is set:

- i. Set the interface:

---

```
(config add system schedule maintenance trigger)> interface
value
(config)>
```

---

- i. Use the **?** to determine available interfaces:

- ii. Set the interface. For example:

---

```
(config system schedule maintenance trigger 0)> interface
/network/interface/eth1
(config system schedule maintenance trigger 0)>
```

---

- **out\_of\_service:** The maintenance window will only start if the Python Out-of-Service is set. See [Use Python to set the maintenance window](#) for further information.

- **time:** Configure a time period for the maintenance window:

- i. Configure the time of day that the maintenance window should start, using the syntax *HH:MM*. If the start time is not set, maintenance tasks are not scheduled and will not be run.

---

```
(config system schedule maintenance trigger 0)> time from
HH:MM
(config system schedule maintenance trigger 0)>
```

---

The behavior of the start time varies depending on the setting of the duration length, which is configured in the next step.

- If the duration length is set to **0**, all scheduled tasks will begin at the exact time specified in the start time.
  - If the duration length is set to **24 hours**, the start time is effectively obsolete and the maintenance tasks will be scheduled to run at any time. Setting the duration length to **24 hours** can potentially overstress the device and should be used with caution.
  - If the duration length is set to any value other than to **0** or **24 hours**, the maintenance tasks will run at a random time during the time allotted for the duration window.
  - If the duration length is set to one or more hours, the minutes field in the start time is ignored and the duration window will begin at the beginning of the specified hour.
- ii. Configure the duration length (the amount of time that the maintenance tasks will be run). If **0** is used, all scheduled tasks will begin at the start time, defined in the previous step.

---

```
(config system schedule maintenance trigger 0)> length num
(config system schedule maintenance trigger 0)>
```

---

where *num* is any whole number between **0** and **24**.

- iii. Configure the frequency that the maintenance tasks should be run:

---

```
(config system schedule maintenance trigger 0)> frequency
value
(config system schedule maintenance trigger 0)>
```

---

where *value* is either **daily** or **weekly**. **Daily** is the default.

4. If **Central Management** is disabled, configure the device to look for any updated device firmware during the maintenance window. If updated firmware is found, it will then be installed. The device will look for updated firmware both on the local device and over the network, using a WAN connection.

This options is only available if **Central Management** is disabled; see [Central management](#) for more information.

---

```
(config)> system schedule maintenance device_fw_update true
(config)>
```

---

5. (Optional) Configure automated checking for device and modem firmware updates:
  - a. **Device firmware update check** is enabled by default. This enables to automated checking for device firmware updates. To disable:

---

```
(config)> system schedule maintenance firmware_update_check device
false
(config)>
```

---

- b. **Modem firmware update check** is enabled by default. This enables to automated checking for modem firmware updates.

---

```
(config)> system schedule maintenance firmware_update_check modem
false
(config)>
```

---

- c. Set how often automated checking for device and modem firmware should take place:

---

```
(config)> system schedule maintenance frequency value
(config)>
```

---

where *value* is either **daily**, **weekly**, or **monthly**. **daily** is the default.

6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

7. (Optional) Configure automated checking for device and modem firmware updates:
  - a. **Device firmware update check** is enabled by default. This enables to automated checking for device firmware updates. To disable:

---

```
(config)> system schedule maintenance firmware_update_check device
false
(config)>
```

---

- b. **Modem firmware update check** is enabled by default. This enables to automated checking for modem firmware updates.

---

```
(config)> system schedule maintenance firmware_update_check modem
false
(config)>
```

---

- c. Set how often automated checking for device and modem firmware should take place:

---

```
(config)> system schedule maintenance frequency value
(config)>
```

---

where *value* is either **daily**, **weekly**, or **monthly**. **daily** is the default.

8. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

9. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Disable device encryption

You can disable the cryptography on your Connect EZ device. This can be used to ship unused devices from overseas without needing export licenses from the country from which the device is being shipped.

When device encryption is disabled, the following occurs:

- The device is reset to the default configuration and rebooted.
- After the reboot:
  - Access to the device via the WebUI and SSH are disabled.
  - All internet connectivity is disabled, including WAN. Connectivity to central management software is also disabled.
  - All IP networks and addresses are disabled except for the default 192.168.210.1/24 network on the local LAN Ethernet port. DHCP server is also disabled.

The device can only be accessed by using telnet from a local machine connecting to the 192.168.210.1/24 network.

Disabling device encryption is not available in the WebUI. It can only be performed from the Admin CLI.

### Command line

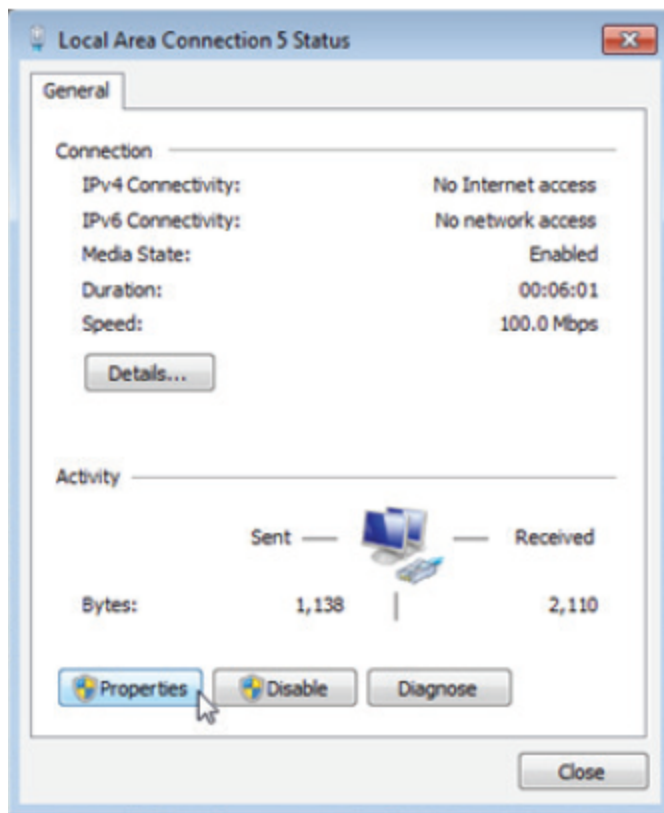
1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Disable encryption with the following command:
 

```
> system disable-cryptography
>
```
3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Re-enable cryptography after it has been disabled.

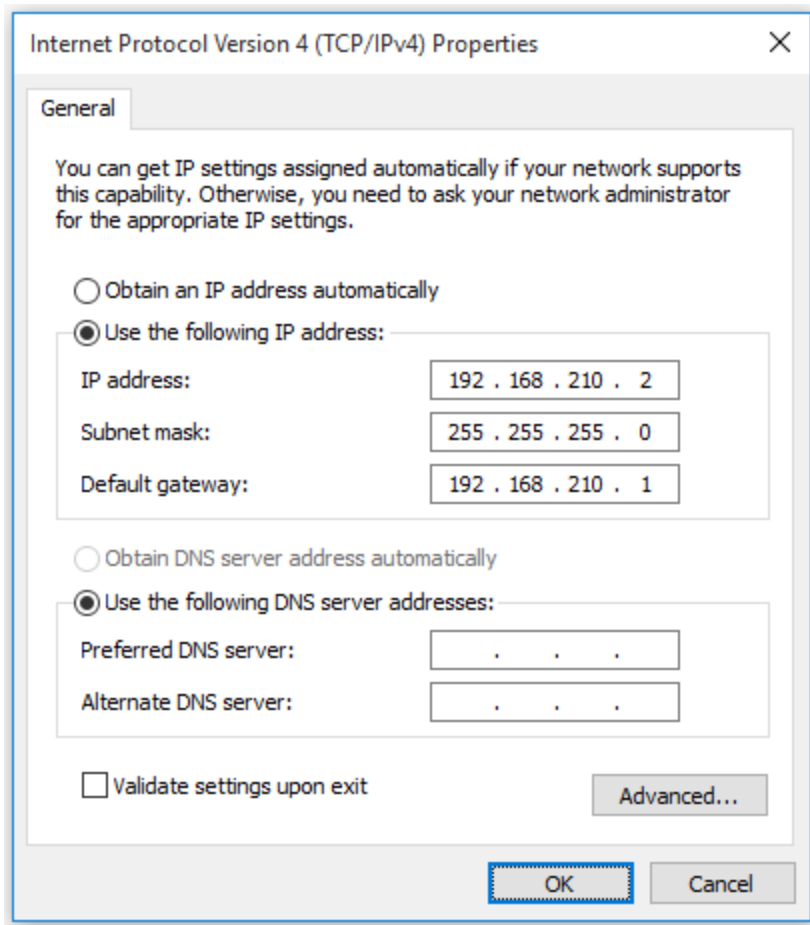
To re-enable cryptography:

1. Configure your PC network to connect to the 192.168.210 subnet. For example, on a Windows PC:
  - a. Select the **Properties** of the relevant network connection on the Windows PC.



- b. Click the **Internet Protocol Version 4 (TCP/IPv4)** parameter.
- c. Click **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog appears.
- d. Configure with the following details:

- **IP address** for PC: 192.168.210.2
- **Subnet**: 255.255.255.0
- **Gateway**: 192.168.210.1



2. Connect the PC's Ethernet port to the Ethernet port on your Connect EZ device.
3. Open a telnet session and connect to the Connect EZ device at the IP address of 192.168.210.1.
4. Log into the device:
  - Username: **admin**
  - Password: The default unique password for your device is printed on the device label.
5. At the shell prompt, type:

---

```
# rm /etc/config/.nocrypt
# flatfsd -i
```

---

This will re-enable encryption and leave the device at its factory default setting.

## Configure the speed of your Ethernet port

You can configure the speed of your Connect EZ device's Ethernet port.



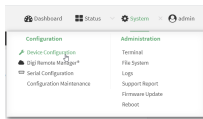
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network > Device**.
4. For **Speed**, select the appropriate speed for the Ethernet port, or select **Auto** to automatically detect the speed. The default is **Auto**.
5. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, type:

```
(config)> network device eth_port value
```

where:

- *eth\_port* is the name of the Ethernet port (for example, **eth**)
- *value* is one of:
  - **10**—Sets the speed to 10 Mbps.
  - **100**—Sets the speed to 100 Mbps.
  - **1000**—Sets the speed to 1 Gbps. Available only for devices with Gigabit Ethernet ports.

**auto**—Configures the device to automatically determine the best speed for the Ethernet port.

The default is **auto**.

4. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

5. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure the system watchdog

You can configure your Connect EZ device's advanced watchdog to test the system for problems, and to reboot the device when problems are encountered.

### Web

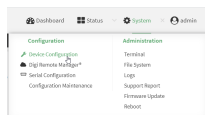
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System > Advanced Watchdog**.
4. The watchdog is disabled by default. To enable, click to toggle off **Disable**.
5. For **Watchdog test interval**, type the amount of time between running system tests. Allowed values are any number of days, hours, minutes, or seconds, and take the format **number{d|h|m|s}**. For example, to set **Watchdog test interval** to ten minutes, enter **10m** or **600s**. The maximum is two days (**2d**), and the default is five minutes (**5m**).
6. Type or select the **Number of test failures before a reboot**.



7. Configure the tests that the watchdog will perform:
  - a. Click to expand **Fault detection tests**.
  - b. Click to expand **Memory usage**.
    - i. The memory check is enabled by default. To disable, click the **Enable memory check** toggle.
    - ii. For **RAM usage threshold to trigger a warning**, type or select the percentage of RAM usage that will trigger a warning. The minimum value is **60** percent, the maximum is **100** percent. The default is **90** percent.
    - iii. Type or select the **Percentage of system memory used before triggering a reboot**. The minimum value is **60** percent, the maximum is **100** percent. The default is **95** percent.
    - iv. To log memory usage with every watchdog memory usage test, click to enable **Log memory usage every interval**.
  - c. Click to expand **Interface tests**.
    - i. Click the **Enable interface(s) down check** toggle to enable. The system periodically checks the interfaces you configure here and, after the specified amount of time, reboots them.
    - ii. Click to expand **Check interface(s)**.
    - iii. Click **+** to add a new interface.
    - iv. For **Interface**, choose the interface you want to test.
  - d. Click to expand **Modem down**. This configuration is enabled by default.
    - i. Click the **Enable modem check** toggle to disable.
    - ii. Click the **Enable modem power cycle** toggle if you want the modem to be power cycled after an initial timeout instead of this timeout being reported as a failure.
    - iii. For **Downtime**, type the amount of time the modem is down before it is reported.
8. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. The watchdog is enabled by default. To disable:

---

```
(config)> system watchdog enable false
(config)>
```

---

4. Set the amount of time between running system tests:

---

```
(config)> system watchdog interval value
(config)>
```

---

where *value* is any number of days, hours, minutes, or seconds, and takes the format ***number {d|h|m|s}***.

For example, to set **interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> system watchdog interval 600s
(config)>
```

---

The maximum is two days (**2d**), and the default is five minutes (**5m**).

5. Set the number of test failures before the system reboots:

---

```
(config)> system watchdog num_failures int
(config)>
```

---

6. Configure the tests that the watchdog will perform:

- a. The memory check is enabled by default. To disable:

---

```
(config)> system watchdog tests memory enable false
(config)>
```

---

- b. Set the percentage of RAM usage that will trigger a warning:

---

```
(config)> system watchdog tests memory max_memory_warning int
(config)>
```

---

The minimum value is **60** percent, the maximum is **100** percent. The default is **90** percent.

- c. Set the percentage of RAM usage that will trigger a reboot of the device:

---

```
(config)> system watchdog tests memory max_memory_critical int
(config)>
```

---

The minimum value is **60** percent, the maximum is **100** percent. The default is **95** percent.

- d. To log memory usage with every watchdog memory usage test, enable **log\_memory**:

---

```
(config)> system watchdog tests memory log_memory true
(config)>
```

---

- e. To have the interface(s) checked and rebooted after the specified amount of time:

---

```
(config)> system watchdog tests interfaces interfaces add [value]
(config)>
```

---

with *value* being the name of the interface.

- f. To have the modem power cycled after an initial timeout instead of this timeout being reported as a failure:

---

```
(config)> system watchdog tests modem
(config)>
```

---

7. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

# Monitoring

---

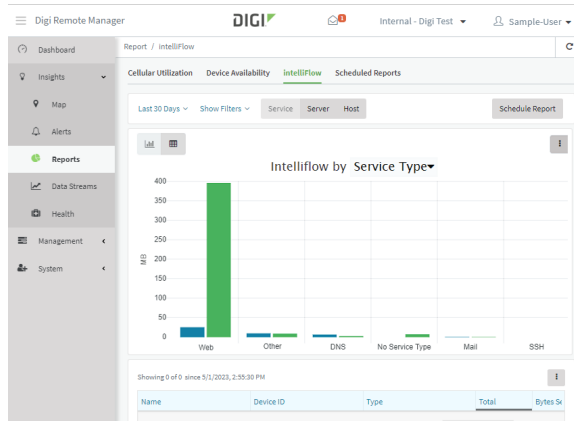
This chapter contains the following topics:

|                               |     |
|-------------------------------|-----|
| intelliFlow .....             | 653 |
| Configure NetFlow Probe ..... | 665 |

## intelliFlow

Digi intelliFlow is a reporting and graphical presentation tool for visualizing your network’s data usage and network traffic information.

intelliFlow can be enabled on Digi Remote Manager to provide a full analysis of all Digi devices on your network. Contact your Digi sales representative for information about enabling intelliFlow on Remote Manager.



IntelliFlow is also available on the local device for device-specific visualization of network use. To use intelliFlow on the local device, you must have access to the local WebUI. Once you enable intelliFlow, the **Status > intelliFlow** option is available in the main menu. By default, intelliFlow is disabled on the local device.

On the local device, intelliFlow provides charts on the following information:

- System utilisation
- Top data usage by host
- Top data usage by server
- Top data usage by service
- Host data usage over time

intelliFlow charts are dynamic; at any point, you can click inside the chart to drill down to view more granular information, and menu options allow you to change various aspects of the information being displayed.

This section contains the following topics:

|                                                               |     |
|---------------------------------------------------------------|-----|
| Enable intelliFlow .....                                      | 654 |
| Configure service types .....                                 | 656 |
| Configure domain name groups .....                            | 658 |
| Use intelliFlow to display average CPU and RAM usage .....    | 661 |
| Use intelliFlow to display top data usage information .....   | 662 |
| Use intelliFlow to display data usage by host over time ..... | 664 |

## Enable intelliFlow

### Required configuration items

- Enable intelliFlow.

### Additional configuration items

- The firewall zone for internal clients being monitored by intelliFlow.

To enable intelliFlow:

### Web

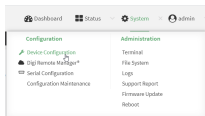
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

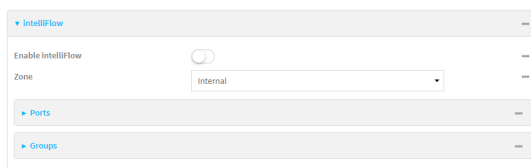
- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring > intelliFlow**.

The intelliFlow configuration window is displayed.



4. Click **Enable intelliFlow**.
5. For **Zone**, select the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone.
6. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable IntelliFlow:

```
(config)> monitoring intelliflow enable true
```

4. Set the firewall zone. Internal clients that are being monitored by IntelliFlow should be present on the specified zone:

- a. Determine available zones:

```
(config)> monitoring intelliflow zone ?
```

```
Zone: The firewall zone which is assigned to the network interface(s)
that
intelliFlow will see as internal clients. intelliFlow relies on an
internal to
external relationship, where the internal clients are present on the
zone specified.
```

Format:

```
any
dynamic_routes
edge
external
internal
ipsec
loopback
setup
```

Default value: internal

Current value: internal

```
(config)>
```

- b. Set the zone to be used by IntelliFlow:

```
(config)> monitoring intelliflow zone my_zone
```

5. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure service types

The service type is used to categorize several ports under one service. For example, port numbers 80, 443, and 8080 are included in the **Web** service type.

There are several predefined service types:

- **Web:** Ports 80, 443, and 8080.
- **FTP:** Ports 20, 21, 989, and 990.
- **SSH:** Port 22.
- **Telnet:** Ports 23 and 992.
- **Mail:** Ports 25, 110, 143, 220, 993 and 995.
- **DNS:** Port 53.
- **IRC:** Ports 194 and 994.
- **RSYNC:** Ports 873.

You can add and remove ports from the predefined service port types, and you can also define your own service types. For example, to define a service type called "MyService" using ports 9000 and 9001:

### ≡ Web

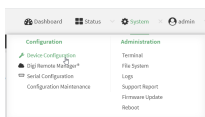
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring > intelliFlow**.
4. Click to expand **Ports**.



- At the bottom of the list of ports, click **+** to add a port.



- Label** is optional.
- For **Port number**, type **9000**.
- For **Service name**, type **MyService**.

- Click **+** to add a another port.
- For **Port number**, type **9001**.
- For **Service name**, type **MyService**.
- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

- Add a port:

```
(config)> add monitoring intelliflow ports end
(config monitoring intelliflow ports 20)>
```

- Set the port number:

```
(config monitoring intelliflow ports 20)> port 9000
(config monitoring intelliflow ports 20)>
```

- Set the service type:

```
(config monitoring intelliflow ports 20)> service MyService
(config monitoring intelliflow ports 20)>
```

6. Add another port:

```
(config monitoring intelliflow ports 20)> add .. end
(config monitoring intelliflow ports 21)>
```

7. Set the port number:

```
(config monitoring intelliflow ports 21)> port 9001
(config monitoring intelliflow ports 21)>
```

8. Set the service type:

```
(config monitoring intelliflow ports 21)> service MyService
(config monitoring intelliflow ports 21)>
```

9. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

10. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure domain name groups

Domain name groups are used to categorize several domains names in one group. For example, digi.com and devicecloud.com could be grouped together in an intelliFlow group called Digi.

### Web

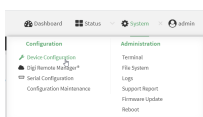
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

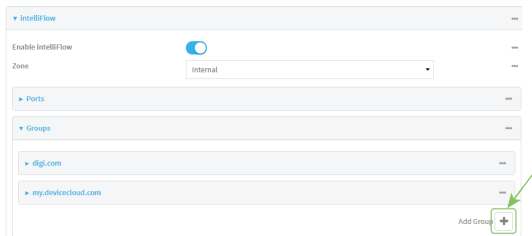
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring > intelliFlow > Groups**.
4. Click **+** to add a domain.



5. **Label** is optional.
6. For **Domain name**, type **digi.com**.
7. For **Group**, type **Digi**.
8. Click **+** to add a another port.
9. For **Domain name**, type **devicecloud.com**.
10. For **Group**, type **Digi**.
11. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Add a group:

```
(config)> add monitoring intelliflow groups end
(config monitoring intelliflow groups 1)>
```

4. Set the domain name:

```
(config monitoring intelliflow groups 1)> domain digi.com
(config monitoring intelliflow groups 1)>
```

5. Set the group name:

```
(config monitoring intelliflow groups 1)> group Digi
(config monitoring intelliflow groups 1)>
```

6. Add another port:

---

```
(config monitoring intelliflow groups 1)> add .. end  
(config monitoring intelliflow groups 2)>
```

---

7. Set the port number:

---

```
(config monitoring intelliflow groups 2)> domain devicecloud.com  
(config monitoring intelliflow groups 2)>
```

---

8. Set the service type:

---

```
(config monitoring intelliflow groups 2)> group Digi  
(config monitoring intelliflow groups 2)>
```

---

9. Save the configuration and apply the change

---

```
(config)> save  
Configuration saved.  
>
```

---

10. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Use intelliFlow to display average CPU and RAM usage

This procedure is only available from the WebUI.

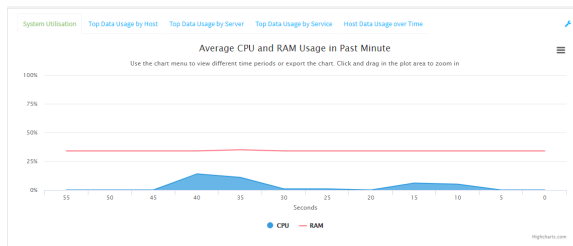
To display average CPU and RAM usage:

### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

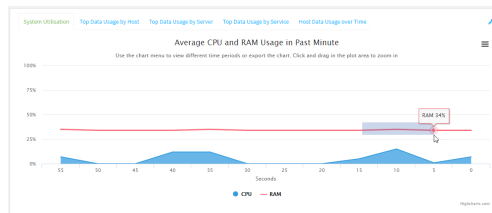
1. If you have not already done so, enable intelliFlow. See [Enable intelliFlow](#).
2. From the menu, click **Status > intelliFlow**.

The System Utilisation chart is displayed:

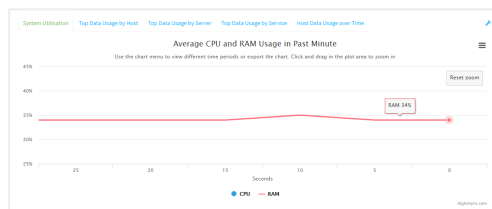


#### ■ Display more granular information:

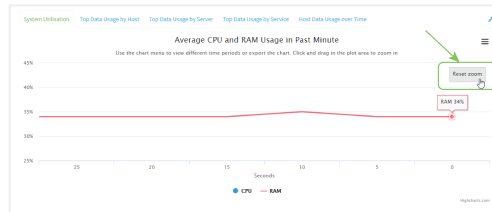
1. Click and drag over an area in the chart to zoom into that area and provide more granular information.



2. Release to display the selected portion of the chart:



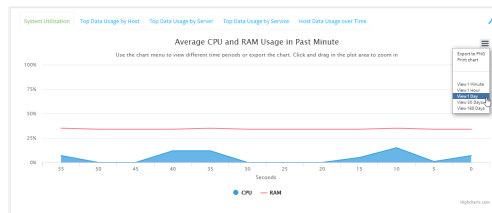
3. Click **Reset zoom** to return to the original display:



- Change the time period displayed by the chart.

By default, the **System utilisation** chart displays the average CPU and RAM usage over the last minute. You can change this to display the average CPU and RAM usage:

- Over the last hour.
  - Over the last day.
  - Over the last 30 days.
  - Over the last 180 days.
1. Click the menu icon (☰).
  2. Select the time period to be displayed.



- Save or print the chart.
  1. Click the menu icon (☰).
  2. To save the chart to your local filesystem, select **Export to PNG**.
  3. To print the chart, select **Print chart**.

## Use intelliFlow to display top data usage information

With intelliFlow, you can display top data usage information based on the following:

- Top data usage by host
- Top data usage by server
- Top data usage by service

To generate a top data usage chart:

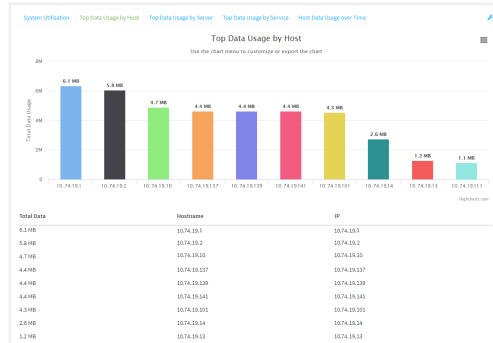
### ☰ Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

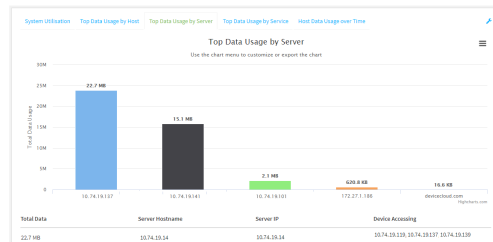
1. If you have not already done so, enable intelliFlow. See [Enable intelliFlow](#).
2. From the menu, click **Status > intelliFlow**.

3. Display a data usage chart:

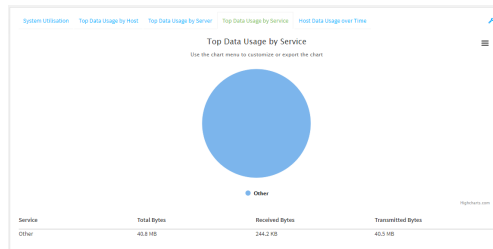
- To display the **Top Data Usage by Host** chart, click **Top Data Usage by Host**.



- To display the **Top Data Usage by Server** chart, click **Top Data Usage by Server**.

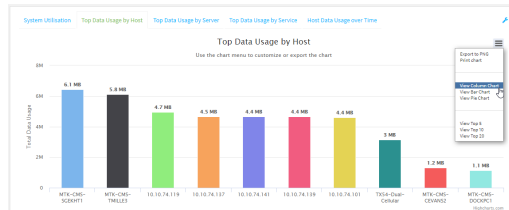


- To display the **Top Data Usage by Service** chart, click **Top Data Usage by Service**.



4. Change the type of chart that is used to display the data:

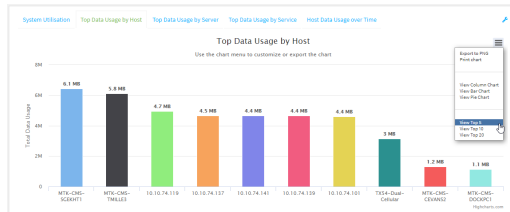
- Click the menu icon (☰).
- Select the type of chart.



5. Change the number of top users displayed.

You can display the top five, top ten, or top twenty data users.

- a. Click the menu icon (☰).
- b. Select the number of top users to displayed.



6. Save or print the chart.
  - a. Click the menu icon (☰).
  - b. To save the chart to your local filesystem, select **Export to PNG**.
  - c. To print the chart, select **Print chart**.

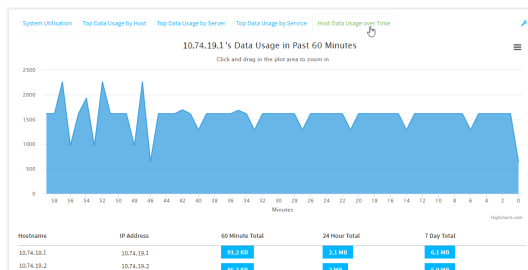
## Use intelliFlow to display data usage by host over time

To generate a chart displaying a host's data usage over time:

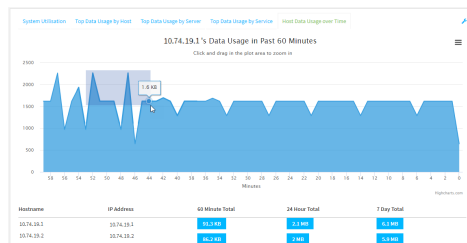
### ☰ Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. If you have not already done so, enable intelliFlow. See [Enable intelliFlow](#).
2. From the menu, click **Status > intelliFlow**.
3. Click **Host Data Usage Over Time**.

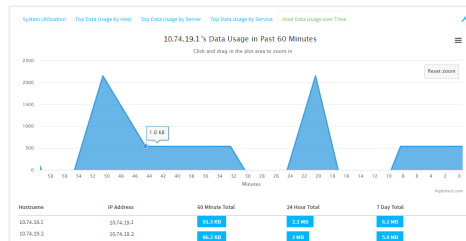


- Display more granular information:
  - a. Click and drag over an area in the chart to zoom into that area and provide more granular information.

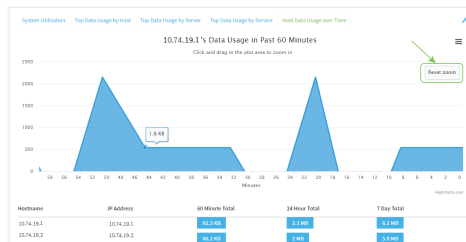




- b. Release to display the selected portion of the chart:



- c. Click **Reset zoom** to return to the original display:



- Save or print the chart.
  - a. Click the menu icon (☰).
  - b. To save the chart to your local filesystem, select **Export to PNG**.
  - c. To print the chart, select **Print chart**.

## Configure NetFlow Probe

NetFlow probe is used to probe network traffic on the Connect EZ device and export statistics to NetFlow collectors.

### Required configuration items

- Enable NetFlow.
- The IP address of a NetFlow collector.

### Additional configuration items

- The NetFlow version.
- Enable flow sampling and select the flow sampling technique.
- The number of flows from which the flow sampler can sample.
- The number of seconds that a flow is inactive before it is exported to the NetFlow collectors.
- The number of seconds that a flow is active before it is exported to the NetFlow collectors.
- The maximum number of simultaneous flows.
- A label for the NetFlow collector.
- The port of the NetFlow collector.
- Additional NetFlow collectors.

To probe network traffic and export statistics to NetFlow collectors:

## Web

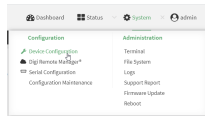
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

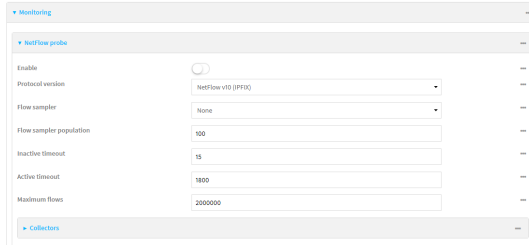
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring > NetFlow probe**.



4. **Enable** NetFlow probe.
5. **Protocol version:** Select the **Protocol version**. Available options are:
  - **NetFlow v5**—Supports IPv4 only.
  - **NetFlow v9**—Supports IPv4 and IPv6.
  - **NetFlow v10 (IPFIX)**—Supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

The default is **NetFlow v10 (IPFIX)**.

6. Enable **Flow sampler** by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows. Available options are:
  - **None**—No flow sampling method is used. Each flow is accounted.
  - **Deterministic**—Selects every  $n$ th flow, where  $n$  is the value of **Flow sampler population**.

- **Random**—Randomly selects one out of every  $n$  flows, where  $n$  is the value of **Flow sampler population**.
  - **Hash**—Randomly selects one out of every  $n$  flows using the hash of the flow key, where  $n$  is the value of **Flow sampler population**.
7. For **Flow sampler population**, if you selected a flow sampler, enter the number of flows for the sampler. Allowed value is any number between **2** and **16383**. The default is **100**.
  8. For **Inactive timeout**, type the the number of seconds that a flow can be inactive before sent to a collector. Allowed value is any number between **1** and **15**. The default is **15**.
  9. For **Active timeout**, type the number of seconds that a flow can be active before sent to a collector. Allowed value is any number between **1** and **1800**. The default is **1800**.
  10. For **Maximum flows**, type the maximum number of flows to probe simultaneously. Allowed value is any number between **0** and **2000000**. The default is **2000000**.
  11. Add collectors:
    - a. Click to expand **Collectors**.
    - b. For **Add Collector**, click **+**.
    - c. (Optional) Type a **Label** for the collector.
    - d. For **Address**, type the IP address of the collector.
    - e. (Optional) For **Port**, enter the port number used by the collector. The default is 2055.
 Repeat to add additional collectors.
  12. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Enable NetFlow:

```
(config)> monitoring netflow enable true
(config)>
```

4. Set the protocol version:

```
(config)> monitoring netflow protocol version
  (config)>
```

where *version* is one of:

- **v5**—NetFlow v5 supports IPv4 only.
- **v9**—NetFlow v9 supports IPv4 and IPv6.
- **v10**—NetFlow v10 (IPFIX) supports both IPv4 and IPv6 and includes IP Flow Information Export (IPFIX).

The default is **v10**.

1. Enable flow sampling by selecting a sampling technique. Flow sampling can reduce flow processing and transmission overhead by providing a representative subset of all flows.

---

```
(config)> monitoring netflow sampler type
(config)>
```

---

where *type* is one of:

- **none**—No flow sampling method is used. Each flow is accounted.
- **deterministic**—Selects every *n*th flow, where *n* is the value of the flow sample population.
- **random**—Randomly selects one out of every *n* flows, where *n* is the value of the flow sample population.
- **hash**—Randomly selects one out of every *n* flows using the hash of the flow key, where *n* is the value of the flow sample population.

5. If you are using a flow sampler, set the number of flows for the sampler:

---

```
(config)> monitoring netflow sampler_population value
(config)>
```

---

where *value* is any number between **2** and **16383**. The default is **100**.

6. Set the number of seconds that a flow can be inactive before sent to a collector:

---

```
(config)> monitoring netflow inactive_timeout value
(config)>
```

---

where *value* is any is any number between **1** and **15**. The default is **15**.

7. Set the number of seconds that a flow can be active before sent to a collector:

---

```
(config)> monitoring netflow active_timeout value
(config)>
```

---

where *value* is any is any number between **1** and **1800**. The default is **1800**.

8. Set the maximum number of flows to probe simultaneously:

---

```
(config)> monitoring netflow max_flows value
(config)>
```

---

where *value* is any is any number between **0** and **2000000**. The default is **2000000**.

9. Add collectors:

- a. Add a collector:

---

```
(config)> add monitoring netflow collector end
(config monitoring netflow collector 0)>
```

---

- b. Set the IP address of the collector:

---

```
(config monitoring netflow collector 0)> address ip_address
(config monitoring netflow collector 0)>
```

---

- c. (Optional) Set the port used by the collector:

---

```
(config monitoring netflow collector 0)> port port
(config monitoring netflow collector 0)>
```

---

- d. (Optional) Set a label for the collector:

---

```
(config monitoring netflow collector 0)> label "This is a collector."
(config monitoring netflow collector 0)>
```

---

Repeat to add additional collectors.

10. Save the configuration and apply the change

---

```
(config monitoring netflow collector 0)> save
Configuration saved.
>
```

---

11. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Central management

---

This chapter contains the following topics:

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Digi Remote Manager support .....                                                       | 671 |
| Certificate-based enhanced security .....                                               | 671 |
| Configure your device for Digi Remote Manager support .....                             | 671 |
| Reach Digi Remote Manager on a private network .....                                    | 682 |
| Log into Digi Remote Manager .....                                                      | 683 |
| Use Digi Remote Manager to view and manage your device .....                            | 684 |
| Add a device to Remote Manager .....                                                    | 684 |
| Configure multiple Connect EZ devices by using Digi Remote Manager configurations ..... | 686 |
| View Digi Remote Manager connection status .....                                        | 687 |
| Learn more .....                                                                        | 688 |

## Digi Remote Manager support

Digi Remote Manager is a hosted remote configuration and management system that allows you to remotely manage a large number of devices. Remote Manager includes a web-based interface that you can use to perform device operations, such as viewing and changing device configurations and performing firmware updates. Remote Manager servers also provide a data storage facility. The Digi Remote Manager is the default cloud-based management system, and is enabled by default.

To use Remote Manager, you must set up a Remote Manager account. To set up a Remote Manager account and learn more about Digi Remote Manager, go to <http://www.digi.com/products/cloud/digi-remote-manager>.

To learn more about Remote Manager features and functions, see the [Digi Remote Manager User Guide](#).

## Certificate-based enhanced security

Beginning with firmware version 22.2.9.x, the default URL for the device's Remote Manager connection is edp12.devicecloud.com. This URL is required to utilize the client-side certificate support. Prior to release 22.2.9.x, the default URL was my.devicecloud.com.

- If your Digi device is configured to use a non-default URL to connect to Remote Manager, updating the firmware will not change your configuration. However, if you erase the device's configuration, the Remote Manager URL will change to the default of edp12.devicecloud.com.
- If you perform a factory reset by pressing the **RESET** twice, the client-side certificate will be erased and you must use the Remote Manager interface to reset the certificate. Select the device in Remote Manager and select **Actions > Reset Device Certificate**.
- The certificate that is provided to the client by Remote Manager is signed by a specific certificate authority, and the device is expecting that same certificate authority. If your IT infrastructure uses its own certificate-based authentication, this might cause the device to interpret the certificate provided by Remote Manager as being from an incorrect certificate authority. If this is the case, you need to include an exception to allow edp12.devicecloud.com to authenticate using its own certificate.

The new URL of edp12.devicecloud.com is for device communication only. Use <https://remotemanager.digi.com> for user interaction with remote manager.

### ***Firewall issues***

To utilize the certificate-based security, you may need to open a port through your firewall for egress connectivity to edp12.devicecloud.com. TCP port 3199 is used for communication with Remote Manager.

## Configure your device for Digi Remote Manager support

By default, your Connect EZ device is configured to use for central management.

### ***Additional configuration options***

These additional configuration settings are not typically configured, but you can set them as needed:

- Disable the Digi Remote Manager connection if it is not required. You can also configure an alternate cloud-based central management application.

- Change the reconnection timer.
- The non-cellular keepalive timeout.
- The keepalive count before the Remote Manager connection is dropped.
- SMS support.
- HTTP proxy server support.

To configure your device's Digi Remote Manager support:

## ≡ Web

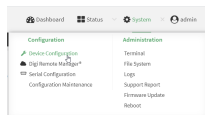
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.



### 3. Click **Central management**.

The Central management configuration window is displayed.

Digi Remote Manager support is enabled by default. To disable, toggle off **Enable central management**.

### 4. For **Service**, select **Digi Remote Manager**.

### 5. (Optional) For **Management server**, type the URL for the central management server.

The default varies depending on firmware versions:

- Firmware version 22.2.9.x and newer, the default is the edp12.devicecloud.com. This server is for device-connectivity only, and uses enhanced security through certificate-based communication. See [Digi Remote Manager support](#) for further information.
- Firmware prior to version 22.2.9.x, the default is the Digi Remote Manager server, <https://remotemanager.digi.com>.

### 6. (Optional) For **Management port**, type the destination port for the remote cloud services connection. The default is **3199**.

### 7. **Firmware server** should normally be left at the default location.

### 8. (Optional) For **Speedtest server**, type the name or IP address of the server to use to test the speed of the device's internet connection(s).

### 9. (Optional) For **Retry interval**, type the amount of time that the Connect EZ device should wait before reattempting to connect to remote cloud services after being disconnected. The default is 30 seconds.

Allowed values are any number of hours, minutes, or seconds, and take the format **number {h|m|s}**.

For example, to set **Retry interval** to ten minutes, enter **10m** or **600s**.

### 10. (Optional) For **Keep-alive interval**, type the amount of time that the Connect EZ device should wait between sending keep-alive messages to remote cloud services when using a non-cellular interface. The default is 60 seconds.

Allowed values are any number of hours, minutes, or seconds, and take the format **number {h|m|s}**.

For example, to set **Keep-alive interval** to ten minutes, enter **10m** or **600s**.

---

**Note** The **Cellular keep-alive interval** is not used by the Connect EZ. Any entry is ignored.

---

11. (Optional) For **Allowed keep-alive misses**, type the number of allowed keep-alive misses. The default is **3**.
12. **Enable watchdog** is used to monitor the connection to remote cloud services. If the connection is down, you can configure the device to restart the connection, or to reboot. The watchdog is enabled by default.
13. If **Enable watchdog** is enabled:
  - a. (Optional) For **Restart Timeout**, type the amount of time to wait before restarting the connection to the remote cloud services, once the connection is down.  
Allowed values are any number of hours, minutes, or seconds, and take the format **number{h|m|s}**.  
For example, to set **Restart Timeout** to ten minutes, enter **10m** or **600s**.  
The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is 30 minutes.
  - b. (Optional) For **Reboot Timeout**, type the amount of time to wait before rebooting the device, once the connection to the remote cloud services is down. By default, this option is not set, which means that the option is disabled.  
Allowed values are any number of hours, minutes, or seconds, and take the format **number{h|m|s}**.  
For example, to set **Reboot Timeout** to ten minutes, enter **10m** or **600s**.  
The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is disabled.
14. (Optional) Enable **Locally authenticate CLI** to require a login and password to authenticate the user from the remote cloud services CLI. If disabled, no login prompt will be presented and the user will be logged in as **admin**. The default is disabled.
15. (Optional) Configure the Connect EZ device to communicate with remote cloud services by using SMS:
  - a. Click to expand **Short message service**.
  - b. **Enable** SMS messaging.
  - c. For **Destination phone number**, type the phone number for the remote cloud services:
    - Within the US: **12029823370**
    - International: **447537431797**
  - d. (Optional) Type the **Service identifier**.
16. (Optional) Configure the Connect EZ device to communicate with remote cloud services via one of two methods: Pinhole or Proxy server.  
If using the Pinhole method, refer to the following  
If using the Proxy server method:
  - a. Click to expand **HTTP Proxy**.
  - b. **Enable** the use of an HTTP proxy server.
  - c. For **Server**, type the hostname of the HTTP proxy server.
  - d. For **Port**, type or select the port number on the HTTP proxy server that the device should connect to. The default is **2138**.
17. Click **Apply** to save the configuration and apply the change.

 **Command line**

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Digi Remote Manager support is enabled by default. To disable Remote Manager support:

---

```
(config)> cloud enable false
(config)>
```

---

4. (Optional) Set the URL for the central management server.

---

```
(config)> cloud drm drm_url url
(config)>
```

---

The default varies depending on firmware versions:

- Firmware version 22.2.9.x and newer, the default is the edp12.devicecloud.com. This server is for device-connectivity only, and uses enhanced security through certificate-based communication. See [Digi Remote Manager support](#) for further information.
  - Firmware prior to version 22.2.9.x, the default is the Digi Remote Manager server, <https://remotemanager.digi.com>.
5. (Optional) Set the amount of time that the Connect EZ device should wait before reattempting to connect to the remote cloud services after being disconnected. The minimum value is ten seconds. The default is 30 seconds.

---

```
(config)> cloud drm retry_interval value
```

---

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **the retry interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> cloud drm retry_interval 600s
(config)>
```

---

6. (Optional) Set the amount of time that the Connect EZ device should wait between sending keep-alive messages to the Digi Remote Manager when using a non-cellular interface. Allowed values are from 30 seconds to two hours. The default is 60 seconds.

---

```
(config)> cloud drm keep_alive value
(config)>
```

---

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **the keep-alive interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> cloud drm keep_alive 600s
(config)>
```

---

**Note** The **Cellular keep-alive interval** is not used by the Connect EZ. Any entry is ignored.

---

7. Set the number of allowed keep-alive misses. Allowed values are any integer between **2** and **64**. The default is **3**.

---

```
(config)> cloud drm keep_alive_misses integer
(config)>
```

---

8. The **watchdog** is used to monitor the connection to remote cloud services. If the connection is down, you can configure the device to restart the connection, or to reboot. The watchdog is enabled by default. To disable:

---

```
(config)> cloud drm watchdog false
(config)>
```

---

9. If **watchdog** is enabled:
  - a. (Optional) Set the amount of time to wait before restarting the connection to the remote cloud services, once the connection is down.

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **restart\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> cloud drm restart_timeout 600s
(config)>
```

---

The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is 30 minutes.

- b. (Optional) Set the amount of time to wait before rebooting the device, once the connection to the remote cloud services is down. By default, this option is not set, which means that the option is disabled.

where *value* is any number of hours, minutes, or seconds, and takes the format **number {h|m|s}**.

For example, to set **reboot\_timeout** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> cloud drm reboot_timeout 600s
(config)>
```

---

The minimum value is 30 minutes and the maximum is 48 hours. If not set, this option is disabled. The default is disabled.

10. **firmware\_url** should normally be left at the default location. To change:

---

```
(config)> cloud drm firmware_url url
(config)>
```

---

11. (Optional) Set the hostname or IP address of the speedtest server. The default is speedtest.accns.com.

---

```
(config)> cloud drm speedtest_server name
(config)>
```

---

12. (Optional) Determine whether to require a login and password to authenticate the user from the remote cloud services CLI:

---

```
(config)> cloud drm cli_local_auth true
(config)>
```

---

If set to **false**, no login prompt will be presented and the user will be logged in as **admin**. The default is **false**.

13. (Optional) Configure the Connect EZ device to communicate with remote cloud services by using SMS:

- a. **Enable** SMS messaging:

---

```
(config)> cloud drm sms enable true
(config)>
```

---

- b. Set the phone number for Digi Remote Manager:

---

```
(config)> cloud drm sms destination value
(config)>
```

---

where *value* is either:

- Within the US: **12029823370**
- International: **447537431797**

- c. (Optional) Set the service identifier:

---

```
(config)> cloud drm sms service_id id
(config)>
```

---

14. (Optional) Configure the Connect EZ device to communicate with remote cloud services by using an HTTP proxy server:

- a. **Enable** the use of an HTTP proxy server:

---

```
(config)> cloud drm proxy enable true
(config)>
```

---

- b. Set the hostname of the proxy server:

---

```
(config)> cloud drm proxy host hostname
(config)>
```

---

- c. (Optional) Set the port number on the proxy server that the device should connect to. The default is 2138.

---

```
(config)> cloud drm proxy port integer
(config)>
```

---

15. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

16. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Collect device health data and set the sample interval

You can enable or disable the collection of device health data to upload to Digi Remote Manager, and configure the interval between health sample uploads. By default, device health data upload is enabled, and the health sample interval is set to 60 minutes. Each time a device connects to Digi Remote Manager after the device boots (or re-boots), the device immediately uploads all health metrics.

To avoid a situation where several devices are uploading health metrics information to Remote Manager at the same time, the Connect EZ device includes a preconfigured randomization of two minutes for uploading metrics. For example, if **Health sample interval** is set to five minutes, the metrics will be uploaded to Remote Manager at a random time between five and seven minutes.

To disable the collection of device health data or enable it if it has been disabled, or to change the health sample interval:

### Web

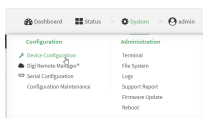
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

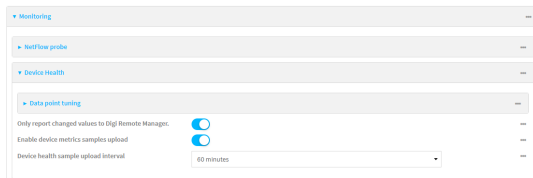
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Monitoring > Device Health**.



4. (Optional) Click to expand **Data point tuning**.

Data point tuning options allow you to configure what data are uploaded to the Digi Remote Manager. All options are enabled by default.

5. **Only report changed values to Digi Remote Manager** is enabled by default.

When enabled:

- The device only reports device health metrics that have changed health metrics were last uploaded. This is useful to reduce the bandwidth used to report health metrics.
- All metrics are uploaded once every hour.

When disabled, all metrics are uploaded every **Health sample interval**.

6. Device health data upload is enabled by default. To disable, toggle off **Enable Device Health samples upload**.
7. For **Health sample interval**, select the interval between health sample uploads.
8. Click **Apply** to save the configuration and apply the change.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. Device health data upload is enabled by default. To enable or disable:

- To enable:

```
(config)> monitoring devicehealth enable true
(config)>
```

- To disable:

```
(config)> monitoring devicehealth enable false
(config)>
```

4. The interval between health sample uploads is set to 60 minutes by default. To change:

```
(config)> monitoring devicehealth interval value
(config)>
```

where *value* is one of **1**, **5**, **15**, **30**, or **60**, and represents the number of minutes between uploads of health sample data.

- By default, the device will only report health metrics values to Digi Remote Manager that have changed health metrics were last uploaded. This is useful to reduce the bandwidth used to report health metrics. This is useful to reduce the bandwidth used to report health metrics. Even if enabled, all metrics are uploaded once every hour.

To disable:

---

```
(config)> monitoring devicehealth only_send_deltas false
(config)>
```

---

When disabled, all metrics are uploaded every **Health sample interval**.

- (Optional) Tuning parameters allow to you configure what data are uploaded to the Digi Remote Manager. By default, all tuning parameters are enabled.

To view a list of all available tuning parameters, use the **show** command:

---

```
(config)> show monitoring devicehealth tuning
all

      eth
        rx
          bytes
            enable true
        tx
          bytes
            enable true
      serial
        rx
          bytes
            enable true
        tx
          bytes
            enable true
      ...
   (config)>
```

---

To disable a tuning parameter, set its value to false. For example, to turn off all reporting for the serial port:

---

```
(config)> monitoring devicehealth tuning all serial rx bytes enabled
false
(config)> monitoring devicehealth tuning all serial tx bytes enabled
false
(config)>
```

---

- Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---



- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Enable event log upload to Digi Remote Manager

You can configure your device to upload the event log to Digi Remote Manager, and configure the interval between event log uploads.

To enable the event log upload, or disable it if it has been disabled, and to change the upload interval:

### Web

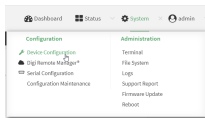
- Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
- Access the device configuration:

Remote Manager:

- Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- Click the **Device ID**.
- Click **Settings**.
- Click to expand **Config**.

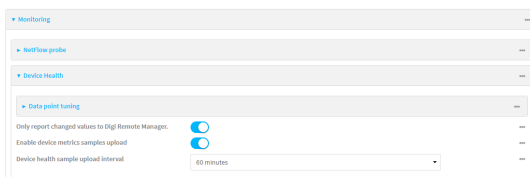
Local Web UI:

- On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

- Click **Monitoring > Device event logs**.



- Click **Enable event log uploads**.
- For **Device event log upload interval**, select the interval between health sample uploads.
- Click **Apply** to save the configuration and apply the change.

### Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

- Device health data upload is enabled by default. To enable or disable:

- To enable:

---

```
(config)> monitoring events enable true
(config)>
```

---

- To disable:

---

```
(config)> monitoring events enable false
(config)>
```

---

- The interval between event log uploads is set to 60 minutes by default. To change:

---

```
(config)> monitoring events interval value
(config)>
```

---

where *value* is one of **1, 5, 15, 30**, or **60**, and represents the number of minutes between uploads of health sample data.

- Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Reach Digi Remote Manager on a private network

If your company has a private network and you have devices that need to reach Digi Remote Manager, there are several methods available:

- Pinhole:** a communication port on your network not protected by the firewall which allows the application on the device to reach Digi Remote Manager.
- Proxy server:** a dedicated software system equipped with its own IP address that runs on your network and acts as an intermediary between the device and Digi Remote Manager.
- VPN Tunnel:** a virtual private network that offers a secure, encrypted connection between a device and the internet.

### Pinhole method

Using the pinhole method requires your network administrator to remove the firewall connection on a communication port. For more information, see [Firewall concerns for outbound EDP connections to Digi Remote Manager](#).

## Proxy server method

The device is capable of connecting through an HTTP proxy, such as Squid, but it is up to the network administrator to decide which HTTP proxy type to use.

To enable a proxy server and enter the server and port in Digi Remote Manager, see step 17 in [Configure your device for Digi Remote Manager support](#).

---

**Tip** To see instructions for setting up Squid and then configuring a device (not DAL) to reach Digi Remote Manager, see the Digi Quick Note, [Connecting to Digi Remote Manager Through Web Proxy](#). Though this Quick Note references older technology and device types, it may provide a network administrator with concrete examples from which they can draw correlations to newer technology and devices.

---

## VPN Tunnel method

Configuring a VPN tunnel to communicate with Digi Remote Manager is a two-step process. One step is done by your organization's network administrator and the other by Digi Support.

### Step 1: Set up the VPN tunnel

Your organization's network administrator needs to set up a VPN tunnel on your network, which will be used to communicate with Digi Remote Manager through the Digi cloud service.

### Step 2. Contact Digi Support.

Digi Support configures the Digi cloud service to allow your VPN to communicate with Digi Remote Manager. Contact Digi Support at <https://www.digi.com/contactus>.


## Log into Digi Remote Manager

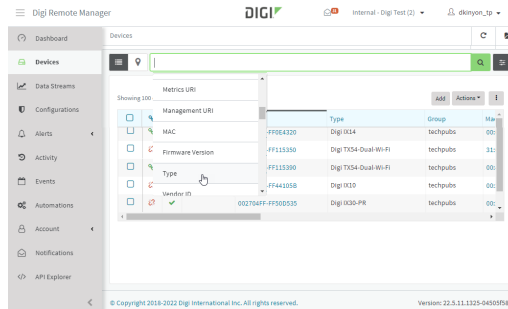
To start Digi Remote Manager

1. If you have not already done so, click [here](#) to sign up for a Digi Remote Manager account.
2. Check your email for Digi Remote Manager login instructions.
3. Go to [remotemanager.digi.com](https://remotemanager.digi.com).
4. Log into your Digi Remote Manager account.

## Use Digi Remote Manager to view and manage your device

To view and manage your device:

1. If you have not already done so, connect to your Digi Remote Manager account.
2. From the menu, click **Devices** to display a list of your devices.
3. Use the Filter bar to locate the device you want to manage. For example, to search by type of device:
  - a. Click the Advanced Search button (  )
  - b. Click in the filter bar.



- c. Type the type of device (for example, Connect EZ).

## Add a device to Remote Manager

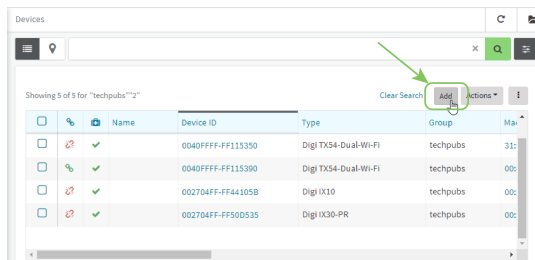
There are several options for adding a device to Remote Manager.

- **Quick Start process.** Use this process to both install a device and then add it to Remote Manager. See the [Connect EZ Quick Start Guide](#).
- **Device label information.** Use the information on the device label (e.g., Device ID, MAC address, Password) to add a new device to Remote Manager. See [Add a device to Remote Manager using information from the label](#).
- **Digi Remote Manager credentials.** Use your Remote Manager credentials to add a device to Remote Manager when you do not have the device password. See [Add a device to Remote Manager using your Remote Manager login credentials](#).

### Add a device to Remote Manager using information from the label

**Tip** If you do not have access to the device label, you can add the device using your Remote Manager login credentials. See [Add a device to Remote Manager using your Remote Manager login credentials](#).

1. If you have not already done so, connect to your Digi Remote Manager account.
2. From the menu, click **Devices** to display a list of your devices.

3. Click **Add**.

4. Type the Device ID, MAC Address, or IMEI.
5. For **Device Default Password**, enter the default password on the printed label packaged with your device. The same default password is also shown on the label affixed to the bottom of the device.
6. (Optional) Complete the other fields.
1. Click **Add Device**.  
Remote Manager adds the Connect EZ device to your account and it appears in the **Device Management** view.

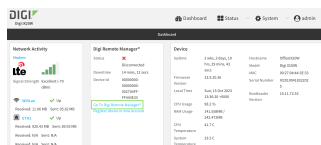
## Add a device to Remote Manager using your Remote Manager login credentials

If you want to add a device to Remote Manager, and you do not have its password, you can add it using your Remote Manager login credentials.

To add a device using your Remote Manager credentials:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the dashboard, in **Digi Remote Manager** status pane, click **Register device in new account**.



3. The **Register Device in New Account** page displays.

**REGISTER DEVICE IN A NEW ACCOUNT**

Digi Remote Manager Username:

Digi Remote Manager Password:

Digi Remote Manager Group (optional):

**REGISTER**

4. For **Digi Remote Manager Username**, type your Remote Manager username.
5. For **Digi Remote Manager Password**, type your Remote Manager password.
6. For **Digi Remote Manager Group (optional)**, type the group to which the device will be added, if needed.

7. Click **Register**.

The device is added to Remote Manager.

### Command line

1. Log into the Connect EZ local command line as a user with full Admin access rights.
2. Register a device.

---

```
(register) [group STRING] password STRING username STRING
```

---

where:

- group: group to add device in Digi Remote Manager.
- password: Digi Remote Manager password (required).
- username: Digi Remote Manager username (required).

1. Click **Apply** to save the configuration and apply the change.
2. Save the configuration and apply the change

---

```
(config)> save  
Configuration saved.  
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

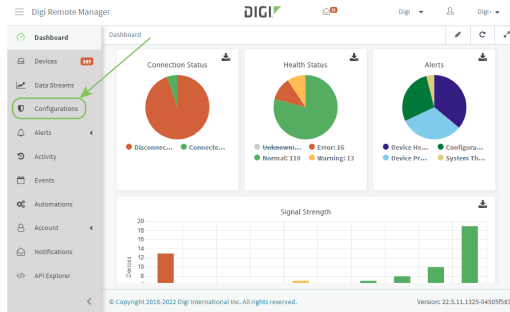
## Configure multiple Connect EZ devices by using Digi Remote Manager configurations

Digi recommends you take advantage of Remote Manager configurations to manage multiple Connect EZ devices. A Remote Manager configuration is a named set of device firmware, settings, and file system options. You use the configuration to automatically update multiple devices and to periodically scan devices to check for compliance with the configuration. See the [Digi Remote Manager User Guide](#) for more information about Remote Manager configurations.

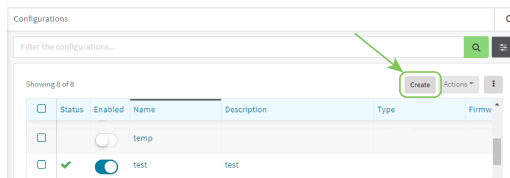
Typically, if you want to provision multiple Connect EZ routers:

1. Using the Connect EZ local WebUI, configure one Connect EZ router to use as the model configuration for all subsequent Connect EZs you need to manage.
2. Register the configured Connect EZ device in your Remote Manager account.

3. In Remote Manager, create a configuration:
  - a. From the Dashboard, select Configurations.



- b. Click **Create**.



- c. Enter a **Name** and an optional **Description** for the configuration, and select the **Groups**, **Device Type**, and **Firmware Version**.
  - d. Click **Save and continue**.
  - e. Click **Import from device** and select the device configured above.
  - f. Click **Import**.
  - g. At the **Settings** page, configure any desired configuration overrides and click **Continue**.
  - h. At the **File System** page, make any desired changes to the files that were imported from the device and click **Continue**.
  - i. At the Automations page, click **Enable Scanning**, make any other desired changes, and click **Save**.

Digi Remote Manager provides multiple methods for applying configurations to registered devices. You can also include site-specific settings with a profile to override settings on a device-by-device basis.

## View Digi Remote Manager connection status

To view the current Digi Remote Manager connection status from the local device:

### Web

1. Log into the Connect EZ WebUI as a user with full Admin access rights.  
The dashboard includes a Digi Remote Manager status pane:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the [show cloud](#) command to view the status of your device's connection to Remote Manager:

---

```
> show cloud

Device Cloud Status
-----

Status      : Connected
Server      : edp12.devicecloud.com Device ID : 00000000-00000000-89E1FE-
7550D7>
```

---

1. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Learn more

To learn more about Digi Remote Manager features and functions, see the [Digi Remote Manager User Guide](#).



## File system

---

This chapter contains the following topics:

|                                          |     |
|------------------------------------------|-----|
| The Connect EZ local file system .....   | 690 |
| Display directory contents .....         | 690 |
| Create a directory .....                 | 691 |
| Display file contents .....              | 692 |
| Copy a file or directory .....           | 692 |
| Move or rename a file or directory ..... | 693 |
| Delete a file or directory .....         | 694 |
| Upload and download files .....          | 695 |

## The Connect EZ local file system

The Connect EZ local file system has approximately 150 MB of space available for storing files, such as Python programs, alternative configuration files and firmware versions, and release files. The writable directories within the filesystem are:

- /tmp
- /opt
- /etc/config

Files stored in the /tmp directory do not persist across reboots. Therefore, /tmp is a good location to upload temporary files, such as files used for firmware updates. Files stored in /opt and /etc/config do persist across reboots, but are deleted if a factory reset of the system is performed. See [Erase device configuration and reset to factory defaults](#) for more information.

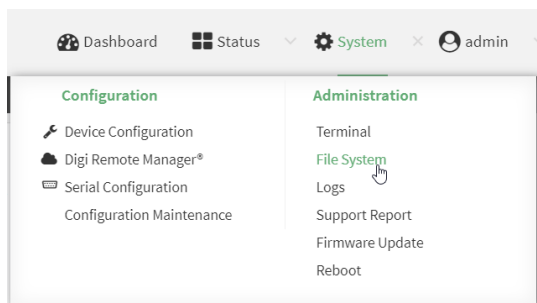
## Display directory contents

To display directory contents by using the WebUI or the Admin CLI:

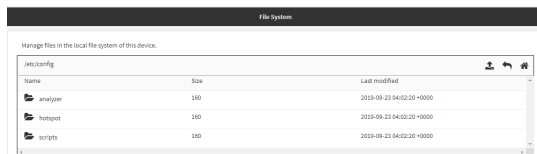
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight a directory and click to open the directory and view the files in the directory.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the Admin CLI prompt, type **ls /path/dir\_name**. For example, to display the contents of the **/etc/config** directory:

---

```
> ls /etc/config
-rw-r--r--    1 root    root           856 Nov 20 20:12 accns.json
drw-----    2 root    root           160 Sep 23 04:02 analyzer
drwxr-xr-x    3 root    root           224 Sep 23 04:02 cc_acl
-rw-r--r--    1 root    root            47 Sep 23 04:02 dhcp.leases
...
>
```

---

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Create a directory

### Command line

This procedure is not available through the WebUI. To make a new directory, use the **mkdir** command, specifying the name of the directory.

For example:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the Admin CLI prompt, type **mkdir /path/dir\_name**. For example, to create a directory named **temp** in **/etc/config**:

---

```
> mkdir /etc/config/temp
>
```

---

- Verify that the directory was created:

---

```
> ls /etc/config
...
-rw-r--r--    1 root    root          1436 Aug 12 21:36 ssl.crt
-rw-----    1 root    root          3895 Aug 12 21:36 ssl.pem
-rw-r--r--    1 root    root            10 Aug  5 06:41 start
drwxr-xr-x    2 root    root           160 Aug 25 17:49 temp
>
```

---

- Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Display file contents

This procedure is not available through the WebUI. To display the contents of a file by using the Admin CLI, use the [more](#) command, specifying the name of the directory.

For example:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type **more /path/filename**. For example, to view the content of the file **accns.json** in **/etc/config**:

---

```
> more /etc/config/accns.json
{
  "auth":
    "user": {
      "admin": {
        "password":
"$2a$05$W1s1s1oxsadf/n4J0XT.Rgr6ewr1yerHtXQdbafsatGswKg0YUm"
      }
    },
  "schema": {
    "version": "461"
  }
}
>
```

---

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Copy a file or directory

This procedure is not available through the WebUI. To copy a file or directory by using the Admin CLI, use the [cp](#) command, specifying the existing path and filename followed by the path and filename of the new file, or specifying the existing path and directory name followed by the path and directory name of the new directory.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- At the Admin CLI prompt, type **cp /path/filename|dir\_name/path[filename]|dir\_name**. For example:

- To copy the file **/etc/config/accns.json** to a file named **backup\_cfg.json** in a directory named **/etc/config/test**, enter the following:

---

```
> cp /etc/config/accns.json /etc/config/test/backup_cfg.json
>
```

---

- To copy a directory named **/etc/config/test** to **/opt**:

---

```
> cp /etc/config/test/ /opt/
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Move or rename a file or directory

This procedure is not available through the WebUI. To move or rename a file or directory by using the Admin CLI, use the [mv](#) command.

### Command line

To rename a file named **test.py** in **/etc/config/scripts** to **final.py**:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the Admin CLI prompt, type:

---

```
> mv /etc/config/scripts/test.py /etc/config/scripts/final.py
>
```

---

- Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

To move **test.py** from **/etc/config/scripts** to **/opt**:

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- At the Admin CLI prompt, type:

---

```
> mv /etc/config/scripts/test.py /opt/
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

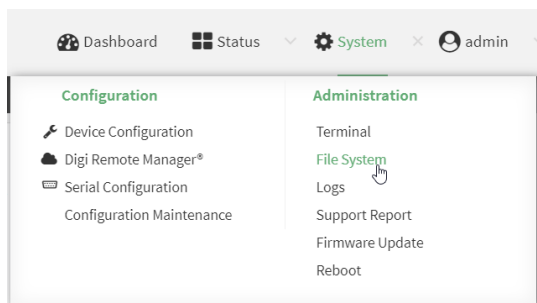
## Delete a file or directory

To delete a file or directory by using the WebUI or the Admin CLI:

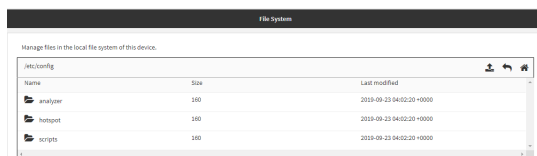
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight the directory containing the file to be deleted and click to open the directory.
3. Highlight the file to be deleted and click .
4. Click **OK** to confirm.

### Command line

To delete a file named **test.py** in **/etc/config/scripts**:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type:

```
> rm /etc/config/scripts/test.py
rm: remove '/etc/config/scripts/test.py'? yes
>
```

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

To delete a directory named **temp** from **/opt**:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. At the Admin CLI prompt, type:

```
> rm /opt/temp/
rm: descend into directory '/opt/temp'? yes
rm: remove directory '/opt/temp'? yes
>
```

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Upload and download files

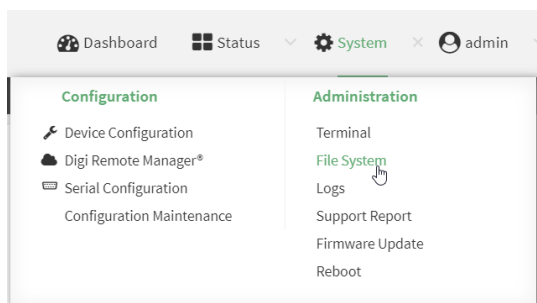
You can download and upload files by using the WebUI or from the command line by using the [scp](#) Secure Copy command, or by using a utility such as SSH File Transfer Protocol (SFTP) or an SFTP application like FileZilla.

### Upload and download files by using the WebUI

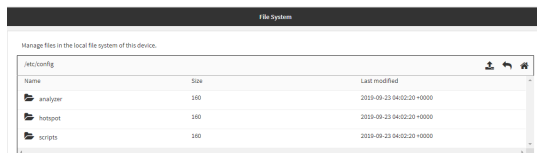
#### Upload files

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



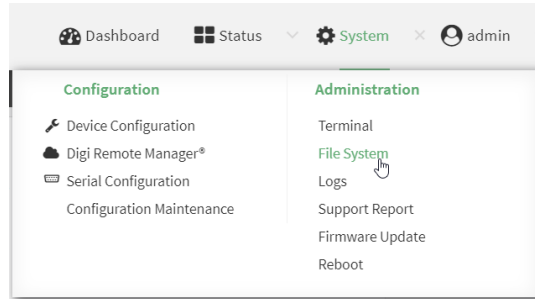
2. Highlight the directory to which the file will be uploaded and click to open the directory.
3. Click (upload).

4. Browse to the location of the file on your local machine. Select the file and click **Open** to upload the file.

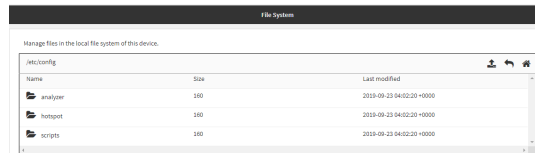
## Download files

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



2. Highlight the directory to which the file will be uploaded and click to open the directory.
3. Highlight the appropriate file and click (download).

## Upload and download files by using the Secure Copy command

### Copy a file from a remote host to the Connect EZ device

To copy a file from a remote host to the Connect EZ device, use the `scp` command as follows:

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the `/etc/config` directory on the Connect EZ device, issue the following command:

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect EZ-24.3.bin local /etc/config/scripts to local
```



---

```
admin@192.168.4.1's password: adminpwd
Connect EZ-24.3.bin          100%   36MB   11.1MB/s   00:03
>
```

---

### **Transfer a file from the Connect EZ device to a remote host**

To copy a file from the Connect EZ device to a remote host, use the `scp` command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
remote
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the Connect EZ device.

For example:

To copy a support report from the Connect EZ device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

---

```
> system support-report path /var/log/
Saving support report to /var/log/support-report-0040D0133536-24-01-12-
12:10:00.bin
Support report saved.
>
```

---

2. Use the **scp** command to transfer the report to a remote host:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/var/log/support-report-00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-24-01-12-12:10:00.bin
>
```

---

## **Upload and download files using SFTP**

### **Transfer a file from a remote host to the Connect EZ device**

This example uploads firmware from a remote host to the Connect EZ device with an IP address of **192.168.2.1**, using the username **ahmed**:

---

```
$ sftp ahmed@192.168.2.1
Password:
Connected to 192.168.2.1
sftp> put Connect EZ-24.3
Uploading Connect EZ-24.3 to Connect EZ-24.3
Connect EZ-24.3
      100% 24M 830.4KB/s   00:00
sftp> exit
$
```

---

**Transfer a file from the Connect EZ device to a remote host**

This example downloads a file named **test.py** from the Connect EZ device at the IP address of **192.168.2.1** with a username of **ahmed** to the local directory on the remote host:

---

```
$ sftp ahmed@192.168.2.1
Password:
Connected to 192.168.2.1
sftp> get test.py
Fetching test.py to test.py
test.py
  100% 254   0.3KB/s   00:00
sftp> exit
$
```

---

## Diagnostics

---

This chapter contains the following topics:

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Perform a speedtest .....                                        | 700 |
| Generate a support report .....                                  | 700 |
| View system and event logs .....                                 | 705 |
| Configure syslog servers .....                                   | 710 |
| Configure options for the event and system logs .....            | 712 |
| Configure an email notification for a system event .....         | 716 |
| Configure an SNMP trap for a system event .....                  | 717 |
| Analyze network traffic .....                                    | 719 |
| Use the ping command to troubleshoot network connections .....   | 737 |
| Use the traceroute command to diagnose IP routing problems ..... | 737 |

## Perform a speedtest

To perform a speedtest:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the **speedtest** command to generate the report:

```
> speedtest host
```

where *host* is the hostname or IP address of a speedtest host. For example:

```
> speedtest speedtest.accns.com
Tx (upload) average: 50.1110 Mbps
Tx latency: 31.45 ms
Rx (download) average: 44.7588 Mbps
Rx latency: 30.05 ms
>
```

3. To output the result in json format, use the **output** parameter:

```
> speedtest host output json
{"tx_avg": "51.8510", "tx_avg_units": "Mbps", "tx_latency": "31.07",
"tx_latency_units": "ms", "rx_avg": "39.5770", "rx_avg_units": "Mbps",
"rx_latency": "34.19", "rx_latency_units": "ms" }
>
```

4. To change the size of the speedtest packet, use the **size** parameter:

```
> speedtest host size int
```

5. By default, the speedtest uses nuttcp for the mode. You can change this to iperf with the **mode** parameter:

```
> speedtest host mode iperf
```

6. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

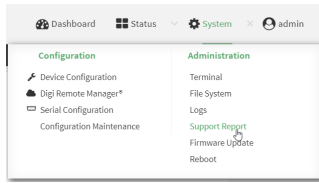
## Generate a support report


To generate and download a support report:

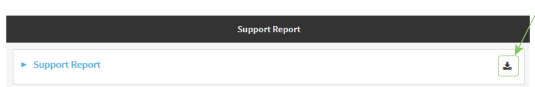
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. On the main menu, click **System**. Under **Administration**, click **Support Report**.



2. Click  to generate and download the support report.



Attach the support report to any support requests.

## Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the **system support-report** command to generate the report:

---

```
> system support-report path /var/log/
Saving support report to /var/log/support-report-0040D0133536-24-01-12-
12:10:00.bin
Support report saved.
>
```

---

3. Use the **scp** command to transfer the report to a remote host:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/var/log/support-report-00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-24-01-12-12:10:00.bin
>
```

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

See [Support report overview](#) for an overview of what is contained in the support report.

## Support report overview

### Generating a Support Report

Support reports provide a snapshot of a device's current settings and connection status at the time of the report's generation. The relevant log files are packaged into a **.bin** file that can be downloaded from the local (web) UI. For more information about generating support reports, see [Generate a support report](#).

**Note** Information logged on the device will be erased when the device is powered off or rebooted to avoid unnecessary wear to the flash memory. See [Configure options for the event and system logs](#) for more information on how to enable persistent system logs.

Use 7-Zip or any other file-archiving utility to extract a support report. Its contents are organized into the following directories:

### **/etc**

This folder most notably contains a running list of the cellular connections that have been registered by the device's radio.

| Directory   | Filename | Notes                                                                                                  |
|-------------|----------|--------------------------------------------------------------------------------------------------------|
| /etc        | version  | Active firmware version                                                                                |
| /etc/config | mn.json  | Cellular connections logged as having been engaged by the radio; establishes previous APN associations |

### **/opt**

Information stored here persists between reboots and system resets.

| Directory     | Filename | Notes                                                                                                                                   |
|---------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------|
| /opt/log_last | messages | With persistent system logs enabled, syslog info will be stored in the /opt directory which isn't erased after reboots or system resets |

### **/tmp**

Output from a series of diagnostic queries is stored in a randomly generated sub-directory within /tmp. When combing through these logs, pay particular attention to config\_dump-public (to verify local device settings) and mmcli-dump (to validate the cellular connection status).

| Directory | Filename           | Notes                                                                                             |
|-----------|--------------------|---------------------------------------------------------------------------------------------------|
| /tmp/#*   |                    | *# is generated at random                                                                         |
|           | arp_nv             | The table of IP-address to MAC-address translations used by the address resolution protocol (ARP) |
|           | arptables_nv-L     | The tables of ARP packet filter rules in the Linux kernel                                         |
|           | cat_procmeminfo    | A breakdown of memory utilization at the time when the support report was generated               |
|           | config_dump-public | The device's current settings, scrubbed of passwords and preshared keys                           |
|           | conntrack-L        | A list of all currently tracked connections through the system                                    |

| Directory | Filename                   | Notes                                                                                                                                                                                                                          |
|-----------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | conntrack_-S               | A summary of currently tracked connections                                                                                                                                                                                     |
|           | date                       | Local system time. If the device isn't online when the support report is generated, the date will be based on the date/month/year that the firmware running on the device was created (e.g. 18.4.54.41 was created 2018-07-05) |
|           | df_-h                      | A report of the file system disk space usage                                                                                                                                                                                   |
|           | event_list                 | A list of events leveraged for syslog messages                                                                                                                                                                                 |
|           | fw_printenv                | The entire environment for the bootloader U-Boot                                                                                                                                                                               |
|           | ip_addr_list               | IP addresses listed per interface                                                                                                                                                                                              |
|           | ip_route_list              | Default routing information per interface                                                                                                                                                                                      |
|           | ip6tables_-nv_-L           | A list of IPv6 routing tables                                                                                                                                                                                                  |
|           | ip6tables_-nv_-L_-t_mangle | Firewall table used when handling mangled/fragmented IPv6 packets                                                                                                                                                              |
|           | ip6tables_-nv_-L_-t_nat    | Firewall table used to direct NAT'd traffic                                                                                                                                                                                    |
|           | iptables_-nv_-L            | A list of IPv4 firewall tables                                                                                                                                                                                                 |
|           | iptables_-nv_-L_-t_mangle  | Firewall table used when handling mangled/fragmented IPv4 packets                                                                                                                                                              |
|           | iptables_-nv_-L_-t_nat     | Firewall table used to direct NAT'd traffic                                                                                                                                                                                    |
|           | s_-RlhA_etccconfig         | An index of items in /etc/config (and its sub-directories)                                                                                                                                                                     |
|           | ls_-RlhA_opt               | An index of items in /opt (and its sub-directories)                                                                                                                                                                            |
|           | ls_-RlhA_tmp               | An index of items in /tmp (and its sub-directories)                                                                                                                                                                            |
|           | ls_-RlhA_var               | An index of items in /var (and its sub-directories)                                                                                                                                                                            |
|           | mmcli-dump                 | A repository of critical information about the cellular radio based off of the cited modem-manager output and defined set of AT commands                                                                                       |
|           | netstat_-i                 | Interface statistics for transmitted/ received packets                                                                                                                                                                         |
|           | netstat_-na                | List of both listening and non-listening network sockets on the device                                                                                                                                                         |
|           | ps_l                       | A snapshot of the current processes running at the time of generating the report                                                                                                                                               |

| Directory | Filename           | Notes                                                                                                                    |
|-----------|--------------------|--------------------------------------------------------------------------------------------------------------------------|
|           | runt_json          | Storage for active/ engaged system variables                                                                             |
|           | sprite_config_dump | Not used for cellular devices                                                                                            |
|           | ubus-dump          | A log of ubus calls for network devices and interfaces                                                                   |
|           | uptime             | The device's uptime at the time of generating the report, along with CPU load averages for the past 1, 5, and 15 minutes |

### **/var/log**

The running system log is stored in "messages" until reaching a set line count (1,000 lines by default). Once this limit is exceeded, that file is renamed to "messages.0" and a new running log is written to the now-empty "messages" log.

| Directory | Filename   | Notes                      |
|-----------|------------|----------------------------|
| /var/log  | messages   | Current syslog information |
|           | messages.0 | Roller syslog information  |

### **/var/run**

This directory can be disregarded for most troubleshooting/ diagnostic purposes.

| Directory | Filename  | Notes                                                                                         |
|-----------|-----------|-----------------------------------------------------------------------------------------------|
| /var/run  | all files | Runtime settings for the device -- referenced in the syslog data gathered in /tmp (see above) |



# View system and event logs

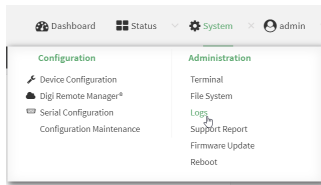
See [Configure options for the event and system logs](#) for information about configuring the information displayed in event and system logs.

## View System Logs

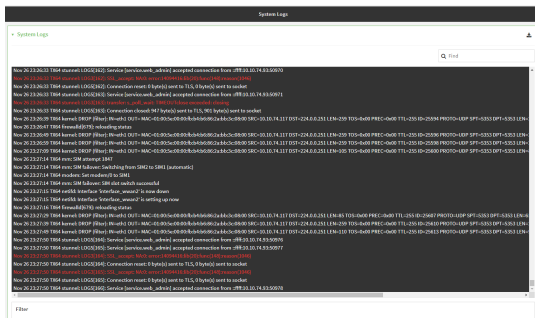


Log into the Connect EZ WebUI as a user with full Admin access rights.

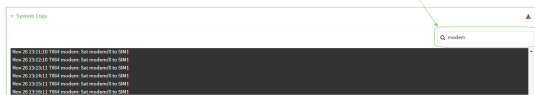
1. On the main menu, click **System > Logs**.



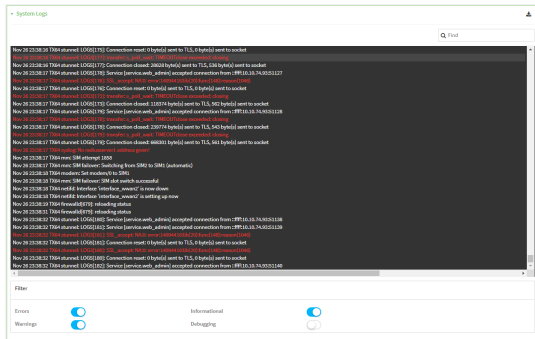
The system log displays:




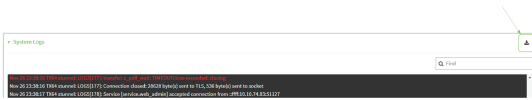
2. Limit the display in the system log by using the **Find** search tool.



3. Use filters to configure the types of information displayed in the system logs.



- Click  to download the system log.



## Command line

- Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
- Use the **show log** command at the Admin CLI prompt:

```
> show log

Timestamp      Message
-----
-----
Nov 26 21:54:34 Connect EZ netifd: Interface 'interface_wan' is setting
up now
Nov 26 21:54:35 Connect EZ firewalld[621]: reloading status
...
>
```

- (Optional) Use the **show log number *num*** command to limit the number of lines that are displayed. For example, to limit the log to the most recent ten lines:

```
> show log number 10

Timestamp      Message
-----
-----
Nov 26 21:54:34 Connect EZ netifd: Interface 'interface_wan' is setting
up now
Nov 26 21:54:35 Connect EZ firewalld[621]: reloading status
...
>
```

- (Optional) Use the **show log filter *value*** command to limit the number of lines that are displayed. Allowed values are **critical**, **warning**, **info**, and **debug**. For example, to limit the event list to only info messages:

```
> show log filter info

Timestamp      Type    Category  Message
-----
-----
Nov 26 22:01:26 info     user
name=admin~service=cli~state=opened~remote=192.168.1.2
```

```
Nov 26 22:01:25 info user
name=admin~service=cli~state=closed~remote=192.168.1.2
...
>
```

5. Type **exit** to exit the Admin CLI.

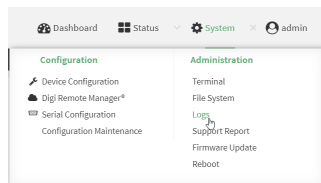
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## View Event Logs

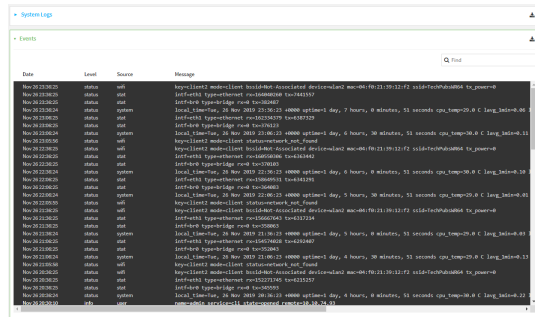
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

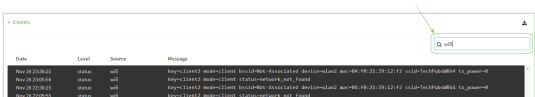
1. On the main menu, click **System > Logs**.



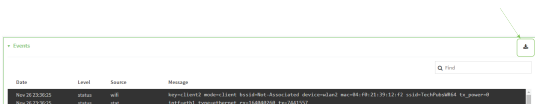
2. Click **System Logs** to collapse the system logs viewer, or scroll down to **Events**.
3. Click **Events** to expand the event viewer.



4. Limit the display in the event log by using the **Find** search tool.



5. Click **Download** to download the event log.



### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the **show event** command at the Admin CLI prompt:

---

```
> show event

Timestamp          Type      Category  Message
-----
Nov 26 21:42:37  status  stat
intf=eth1~type=ethernet~rx=11332435~tx=5038762
Nov 26 21:42:35  status  system   local_time=Thu, 08 Aug 2019 21:42:35
+0000~uptime=3 hours, 0 minutes, 48 seconds
...
>
```

---

3. (Optional) Use the **show event number num** command to limit the number of lines that are displayed. For example, to limit the event list to the most recent ten lines:

---

```
> show event number 10

Timestamp          Type      Category  Message
-----
Nov 26 21:42:37  status  stat
intf=eth1~type=ethernet~rx=11332435~tx=5038762
Nov 26 21:42:35  status  system   local_time=Thu, 08 Aug 2019 21:42:35
+0000~uptime=3 hours, 0 minutes, 48 seconds
...
>
```

---

4. (Optional) Use the **show event table value** command to limit the number of lines that are displayed. Allowed values are **error**, **info**, and **status**. For example, to limit the event list to only info messages:

---

```
> show event table info

Timestamp          Type      Category  Message
-----
Nov 26 22:01:26  info     user
name=admin~service=cli~state=opened~remote=192.168.1.2
Nov 26 22:01:25  info     user
name=admin~service=cli~state=closed~remote=192.168.1.2
...
>
```

---

5. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure syslog servers

You can configure remote syslog servers for storing event and system logs.

### Web

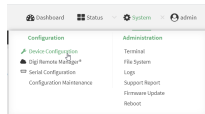
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

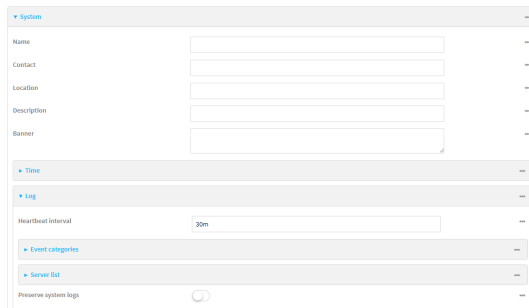
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

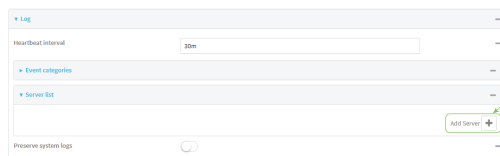


The **Configuration** window is displayed.

3. Click **System > Log**.



4. Add and configure a remote syslog server:
  - a. Click to expand **Server list**.
  - b. For **Add Server**, click **+**.



The log server configuration window is displayed.

Log servers are enabled by default. To disable, toggle off **Enable**.

- c. Type the host name or IP address of the **Server**.
  - d. Select the event categories that will be sent to the server. By default, all event categories are enabled. You can disable logging for error, informational, and status event categories by clicking to toggle off the category.
  - e. For **Syslog egress port**, type the port number to use for the syslog server. The default is **514**.
  - f. For **Protocol**, select the IP protocol to use for communication with the syslog server. Available options are **TCP** and **UDP**. The default is **UDP**.
5. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) To configure remote syslog servers:
  - a. Add a remote server:

```
(config)> add system log remote end
(config system log remote 0)>
```

- b. Enable the server:

```
(config system log remote 0)> enable true
(config system log remote 0)>
```

- c. Set the host name or IP address of the server:

```
(config system log remote 0)> server hostname
(config system log remote 0)>
```

- d. The event categories that will be sent to the server are automatically enabled when the server is enabled.

- To disable informational event messages:

---

```
(config system log remote 0)> info false
(config system log remote 0)>
```

---

- To disable status event messages:

---

```
(config system log remote 0)> status false
(config system log remote 0)>
```

---

- To disable informational event messages:

---

```
(config system log remote 0)> error false
(config system log remote 0)>
```

---

4. Set the port number to use for the syslog server:

---

```
(config system log remote 0)> port value
(config system log remote 0)>
```

---

where *value* is any integer between **1** and **65535**. The default is **514**.

5. Set the IP protocol to use for communication with the syslog server:

---

```
(config system log remote 0)> protocol value
(config system log remote 0)>
```

---

where *value* is either **tcp** or **udp**. The default is **udp**.

6. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

7. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure options for the event and system logs

The default configuration for event and system logging is:

- The heartbeat interval, which determines the amount of time to wait before sending a heartbeat event if no other events have been sent, is set to 30 minutes.
- All event categories are enabled.

To change or disable the heartbeat interval, or to disable event categories, and to perform other log configuration:



Web



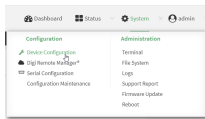
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

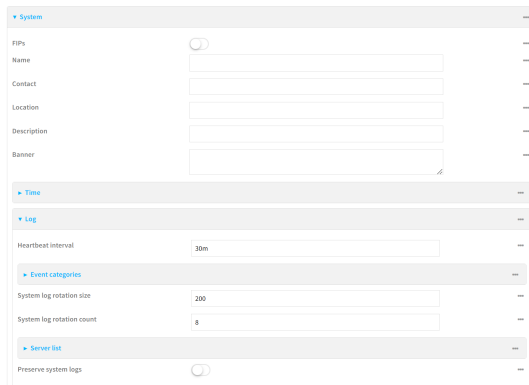
Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **System > Log**.



4. (Optional) To change the **Heartbeat interval** from the default of 30 minutes, type a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent. Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**. For example, to set **Heartbeat interval** to ten minutes, enter **10m** or **600s**. To disable the **Heartbeat interval**, enter **0s**.
5. (Optional) To disable event categories, or to enable them if they have been disabled:
  - a. Click to expand **Event Categories**.
  - b. Click an event category to expand.
  - c. Depending on the event category, you can enable or disable informational events, status events, and error events. Some categories also allow you to set the **Status interval**, which

is the time interval between periodic status events.

You can enable or disable **Enable email notifications** if you want to email a system log event notification to a specified email address. The email address must also be specified before a notification can be sent. To configure, see [Configure an email notification for a system event](#).

You can enable or disable **Enable SNMP traps** if you want system log event information saved to an SNMP trap. At least one SNMP destination must be defined before event information can be saved. To configure, see [Configure an SNMP trap for a system event](#).

6. (Optional) See [Configure syslog servers](#) for information about configuring remote syslog servers to which log messages will be sent.
7. (Optional) To change the system log settings from the defaults, type in a new value.
  - **System log rotation size:** Specify the maximum size (measured in kilobytes) the system log file can reach before log rotation. When the specified size is reached, the system log rotates.  
Default is **200** kb. Minimum is **10** kb.
  - **System log rotation count:** Specify the number of system log files to keep.  
Default is **8**. Minimum is **1**; maximum is **20**.
8. Enable **Preserve system logs** to save the current session's system log after a reboot.  
By default, the Connect EZ device erases system logs each time the device is powered off or rebooted.

---

**Note** You should only enable **Preserve system logs** temporarily to debug issues. Once you are finished debugging, immediately disable **Preserve system logs** to avoid unnecessary wear to the flash memory.

---

9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. (Optional) To change the heartbeat interval from the default of 30 minutes, set a new value. The heartbeat interval determines the amount of time to wait before sending a heartbeat event if no other events have been sent.

```
(config)> system log heartbeat_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **the heartbeat interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config)> system log heartbeat_interval 600s
(config)>
```

---

To disable the heartbeat interval, set the value to **0s**

4. Enable preserve system logs functionality to save the current session's system log after a reboot. By default, the Connect EZ device erases system logs each time the device is powered off or rebooted.

---

**Note** You should only enable **Preserve system logs** temporarily to debug issues. Once you are finished debugging, immediately disable **Preserve system logs** to avoid unnecessary wear to the flash memory.

---



---

```
(config)> system log persistent true
(config)>
```

---

5. (Optional) To disable event categories, or to enable them if they have been disabled:
  - a. Use the question mark (?) to determine available event categories:

---

```
(config)> system log event ?
```

Event categories: Settings to enable individual event categories.

Additional Configuration

```
-----
arping                ARP ping
config                Configuration
dhcpserver            DHCP server
firmware              Firmware
location              Location
netmon                Active recovery
network               Network interfaces
openvpn               OpenVPN
portal                Captive portal
remote                Remote control
restart               Restart
serial                Serial
sms                   SMS commands
speed                 Speed
stat                  Network statistics
user                  User
wol                   Wake-On-LAN
```

---

```
(config)> system log event
```

---

- b. Depending on the event category, you can enable or disable informational events, status events, and error events. Some categories also allow you to set the status interval, which is the time interval between periodic status events. For example, to configure DHCP server logging:

- i. Use the question mark (?) to determine what events are available for DHCP server logging configuration:

```
(config)> system log event dhcpserver ?
...
DHCP server: Settings for DHCP server events. Informational events
are generated
when a lease is obtained or released. Status events report the
current list of
leases.
```

| Parameters      | Current Value |                             |
|-----------------|---------------|-----------------------------|
| info events     | true          | Enable informational events |
| status          | true          | Enable status events        |
| status_interval | 30m           | Status interval             |

```
(config)> system log event dhcpserver
```

- ii. To disable informational messages for the DHCP server:

```
(config)> system log event dhcpserver info false
(config)>
```

- iii. To change the status interval:

```
(config)> system log event dhcpserver status_interval value
(config)>
```

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **the status interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> system log event dhcpserver status_interval 600s
(config)>
```

6. (Optional) See [Configure syslog servers](#) for information about configuring remote syslog servers to which log messages will be sent.
7. Save the configuration and apply the change

```
(config)> save
Configuration saved.
>
```

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Configure an email notification for a system event

You can configure the Connect EZ to send an email notification of a system event.

**Step 1:** Configure the SMTP server that is used to send email notifications when a system log event occurs by enabling the **Email notifications** system log feature.

**Step 2:** Review the system log event categories and select the type of information that you want to save to the system log: errors, informational events, or status events, depending on the event category. To ensure the notification is sent, enable the **Enable email notification** option for the event category.

1. [Log in to the web UI.](#)
2. Click **System > Device Configuration**. The **Configuration** page displays.
3. Expand **System > Log**.
4. Expand **Email notifications**.
5. Click **Enable**. The slider is blue when enabled.
  - a. From the **Server type** list box, select the method used to connect and authenticate with the SMTP server.
  - b. In the **SMTP server name** field, enter the host name or IP address of the SMTP server.
  - c. In the **SMTP server port** field, enter the TCP port of the SMTP server.
  - d. In the **Server user name** field, enter the server login name.
  - e. In the **Server password** field, enter the server password.
  - f. In the **Email from address** field, enter the email address that should be placed in the **From** field on an email.
  - g. In the **Email to address** field, enter the email address that should be placed in the **To** field on an email.
  - h. In the **Email subject** field, enter the text for the subject line of the email.
6. Click **Apply** to save the configuration and apply the change.
7. Review the system log event categories and select the type of information that you want to save to the system log, and enable the **Enable email notification** option. To configure these options, see [Configure options for the event and system logs](#).

## Configure an SNMP trap for a system event

You can configure an SNMP trap destination for a Connect EZ to save system event information.

**Step 1:** Configure an SNMP trap by enabling the **SNMP traps** system log feature.

**Step 2:** Review the system log event categories and select the type of information that you want to save to the system log and the SNMP trap: errors, informational events, or status events, depending on the event category. To ensure the log information is saved to an SNMP trap, enable the **Enable SNMP traps** option for the event category.

1. [Log in to the web UI.](#)
2. Click **System > Device Configuration**. The **Configuration** page displays.
3. Expand **System > Log**.
4. Expand **SNMP traps**.
5. Click **Enable**. The slider is blue when enabled.
6. Add a destination.
  - a. Click **Add Destination**.
  - b. In the **Host Name** field, enter the host name or IP address of the SNMP destination.

- c. In the **Port** field, enter the UDP port of the SNMP destination. The default is **162**.
  - d. In the **Community name** field, enter the SNMP destination community name. The default is **public**.
  - e. Repeat this process to add an additional destination, if needed.
7. Click **Apply** to save the configuration and apply the change.
  8. Review the system log event categories and select the type of information that you want to save to the system log, and enable the **Enable SNMP traps** option. To configure these options, see [Configure options for the event and system logs](#).

## Analyze network traffic

The Connect EZ device includes a network analyzer tool that captures data traffic on any interface and decodes the captured data traffic for diagnostics. You can capture data traffic on multiple interfaces at the same time and define capture filters to reduce the captured data. You can capture up to 10 MB of data traffic in two 5 MB files per interface.

To perform a more detailed analysis, you can download the captured data traffic from the device and view it using a third-party application.

---

**Note** Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See [Save captured data traffic to a file](#).

---

This section contains the following topics:

|                                                         |     |
|---------------------------------------------------------|-----|
| Configure packet capture for the network analyzer ..... | 720 |
| Example filters for capturing data traffic .....        | 729 |
| Capture packets from the command line .....             | 730 |
| Stop capturing packets .....                            | 731 |
| Show captured traffic data .....                        | 732 |
| Save captured data traffic to a file .....              | 733 |
| Download captured data to your PC .....                 | 734 |
| Clear captured data .....                               | 735 |

## Configure packet capture for the network analyzer

To use the network analyzer, you must create one or more packet capture configuration.

### Required configuration items

- The interface used by this packet capture configuration.

### Additional configuration items

- The filter expression for this packet capture configuration.
- Schedule the analyzer to run based on a specified event or at a particular time:
  - The events or time that will trigger the analyzer to run, using this capture configuration.
  - The amount of time that the analyzer session will run.
  - The frequency with which captured events will be saved.

To configure a packet capture configuration:

### ≡ Web

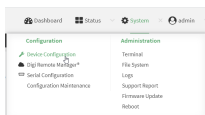
1. Log into Digi Remote Manager, or log into the local Web UI as a user with full Admin access rights.
2. Access the device configuration:

Remote Manager:

- a. Locate your device as described in [Use Digi Remote Manager to view and manage your device](#).
- b. Click the **Device ID**.
- c. Click **Settings**.
- d. Click to expand **Config**.

Local Web UI:

- a. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

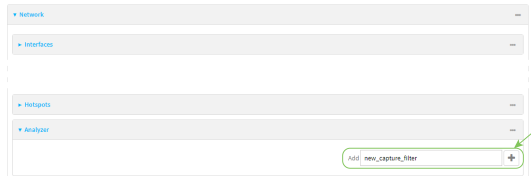


The **Configuration** window is displayed.

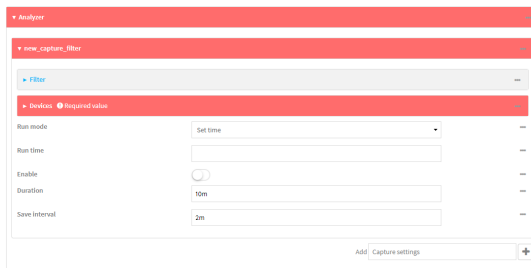
3. Click **Network > Analyzer**.



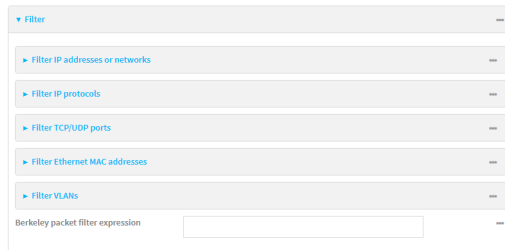
4. For **Add Capture settings**, type a name for the capture filter and click **+**.



The new capture filter configuration is displayed.

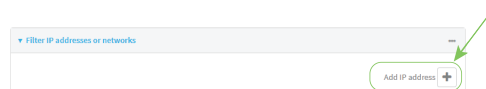


5. (Optional) Add a filter type:
- a. Click to expand **Filter**.



You can select from preconfigured filters to determine which types of packets to capture or ignore, or you can create your own Berkeley packet filter expression.

- b. To create a filter that either captures or ignores packets from a particular IP address or network:
  - i. Click to expand **Filter IP addresses or networks**.
  - ii. Click **+** to add an IP address/network.



- iii. For **IP address or network**, type the IPv4 or IPv6 address (and optional netmask).
- iv. For **Source or destination IP address**, select whether the filter should apply to packets when the IP address/network is the source, the destination, or both.
- v. Click **Ignore this IP address or network** if the filter should ignore packets from this IP address/network. By default, this option is disabled, which means that the filter will capture packets from this IP address/network.
- vi. Click **+** to add additional IP address/network filters.

- c. To create a filter that either captures or ignores packets that use a particular IP protocol:
  - i. Click to expand **Filter IP protocols**.
  - ii. Click **+** to add an IP protocol.
  - iii. For **IP protocol to capture or ignore**, select the protocol. If **Other protocol** is selected, type the number of the protocol.
  - iv. Click **Ignore this protocol** if the filter should ignore packets that use this protocol. By default, this option is disabled, which means that the filter will capture packets that use this protocol.
  - v. Click **+** to add additional IP protocol filters.
- d. To create a filter that either captures or ignores packets from a particular port:
  - i. Click to expand **Filter TCP/UDP port**.
  - ii. Click **+** to add a TCP/UDP port.
  - iii. For **IP TCP/UDP port to capture or ignore**, type the number of the port to be captured or ignored.
  - iv. For **TCP or UDP port**, select the type of transport protocol.
  - v. For **Source or destination TCP/UDP port**, select whether the filter should apply to packets when the port is the source, the destination, or both.
  - vi. Click **Ignore this TCP/UDP port** if the filter should ignore packets that use this port. By default, this option is disabled, which means that the filter will capture packets that use this port.
  - vii. Click **+** to add additional port filters.
- e. To create a filter that either captures or ignores packets from one or more specified MAC addresses:
  - i. Click to expand **Filter Ethernet MAC addresses**.
  - ii. Click **+** to add a MAC address.
  - iii. For **Ethernet MAC address**, type the MAC address to be captured or ignored.
  - iv. For **Source or destination Ethernet MAC address**, select whether the filter should apply to packets when the Ethernet MAC address is the source, the destination, or both.
  - v. Click **Ignore this MAC address** if the filter should ignore packets that use this port. By default, this option is disabled, which means that the filter will capture packets that use this port.
  - vi. Click **+** to add additional MAC address filters.
- f. To create a filter that either captures or ignores packets from one or more VLANs:
  - i. Click to expand **Filter VLANs**.
  - ii. Click **+** to add a VLAN.
  - iii. For **The VLAN to capture or ignore**, type the number of the VLAN.
  - iv. Click **Ignore this VLAN** if the filter should ignore packets that use this port. By default, this option is disabled, which means that the filter will capture packets that use this port.
  - v. Click **+** to add additional VLAN filters.

- g. For **Berkeley packet filter expression**, type a filter using Berkeley Packet Filter (BPF) syntax. See [Example filters for capturing data traffic](#) for examples of filters using BPF syntax.
6. Add one or more interface to the capture filter:
  - a. Click to expand **Device**.
  - b. Click **+** to add an interface to the capture setting instance.



- c. For **Device**, select an interface.
  - d. Repeat to add additional interfaces to the capture filter.
7. (Optional) For **Berkeley packet filter expression**, type a filter using Berkeley Packet Filter (BPF) syntax. See [Example filters for capturing data traffic](#) for examples of filters using BPF syntax.
8. (Optional) Schedule the analyzer to run, using this capture filter, based on a specified event or at a particular time:
  - a. For **Run mode**, select the mode that will be used to run the capture filter. Available options are:
    - **On boot**: The capture filter will run once each time the device boots.
    - **Interval**: The capture filter will start running at the specified interval, within 30 seconds after the configuration change is saved.
      - If **Interval** is selected, in **Interval**, type the interval.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Interval** to ten minutes, enter **10m** or **600s**.
    - **Set time**: Runs the capture filter at a specified time of the day.
      - If **Set Time** is selected, specify the time that the capture filter should run in **Run time**, using the format **HH:MM**
    - **During system maintenance**: The capture filter will run during the system maintenance time window.
  - b. **Enable** the capture filter schedule.
  - c. For **Duration**, type the amount of time that the scheduled analyzer session will run.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Duration** to ten minutes, enter **10m** or **600s**.
  - d. For **Save interval**, type the frequency with which captured events will be saved.  
Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format **number{w|d|h|m|s}**.  
For example, to set **Save interval** to ten minutes, enter **10m** or **600s**.
9. Click **Apply** to save the configuration and apply the change.

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

---

```
> config
(config)>
```

---

3. Add a new capture filter:

---

```
(config)> add network analyzer name
(config network analyzer name)>
```

---

4. Add an interface to the capture filter:

---

```
(config network analyzer name)> add device end device
(config network analyzer name)>
```

---

Determine available devices and the proper syntax.

To determine available devices and proper syntax, use the space bar autocomplete feature:

---

```
(config network analyzer name)> add device end <space>
(config network analyzer name)> add interface end /network/
```

---

Repeat to add additional interfaces.

5. (Optional) Set a filter for the capture filter:
  - a. To create a filter that either captures or ignores packets from a particular IP address or network:
    - i. Add a new IP address/network filter:

---

```
(config network analyzer name)> add filter address end
(config network analyzer name filter address 0)>
```

---

- ii. Set the IPv4 or IPv6 address (and optional netmask):

---

```
(config network analyzer name filter address 0)> address ip_
address[/netmask]
(config network analyzer name filter address 0)>
```

---

- iii. Set whether the filter should apply to packets when the IP address/network is the source, the destination, or both:

---

```
(config network analyzer name filter address 0)> match value
(config network analyzer name filter address 0)>
```

---

where *value* is one of:

- **source:** The filter will apply to packets when the IP address/network is the source.
- **destination:** The filter will apply to packets when the IP address/network is the destination.



- v. (Optional) Set the filter should ignore packets from this protocol:

---

```
(config network analyzer name filter protocol 0)> ignore true
(config network analyzer name filter protocol 0)>
```

---

By default, this option is set to **false**, which means that the filter will capture packets from this protocol.

- vi. Repeat these steps to add additional protocol filters.
- c. To create a filter that either captures or ignores packets from a particular port:
- i. Add a new port filter:

---

```
(config network analyzer name)> add filter port end
(config network analyzer name filter port 0)>
```

---

- ii. Set the transport protocol that should be filtered for the port:

---

```
(config network analyzer name filter port 0)> protocol value
(config network analyzer name filter port 0)>
```

---

where *value* is one of **tcp**, **udp**, or **either**. The default is **either**.

- iii. Set whether the filter should apply to packets when the port is the source, the destination, or both:

---

```
(config network analyzer name filter port 0)> match value
(config network analyzer name filter port 0)>
```

---

where *value* is one of:

- **source**: The filter will apply to packets when the port is the source.
- **destination**: The filter will apply to packets when the port is the destination.
- **either**: The filter will apply to packets when the port is either the source or the destination.

- iv. (Optional) Set the filter should ignore packets from this port:

---

```
(config network analyzer name filter port 0)> ignore true
(config network analyzer name filter port 0)>
```

---

By default, this option is set to **false**, which means that the filter will capture packets from this port.

- v. Repeat these steps to add additional port filters.
- d. To create a filter that either captures or ignores packets from one or more specified MAC addresses:
- i. Add a new MAC address filter:

---

```
(config network analyzer name)> add filter mac_address end
(config network analyzer name filter mac_address 0)>
```

---

- ii. Set the MAC address that should be captured or ignored:

---

```
(config network analyzer name filter mac_address 0)> address value
(config network analyzer name filter mac_address 0)>
```

---

where *value* is the MAC address to be filtered, using colon-hexadecimal notation with lower case, for example, **00:aa:11:bb:22:cc**.

- iii. Set whether the filter should apply to packets when the MAC address is the source, the destination, or both:

---

```
(config network analyzer name filter mac_address 0)> match value
(config network analyzer name filter mac_address 0)>
```

---

where *value* is one of:

- **source:** The filter will apply to packets when the MAC address is the source.
- **destination:** The filter will apply to packets when the MAC address is the destination.
- **either:** The filter will apply to packets when the MAC address is either the source or the destination.

- iv. (Optional) Set the filter should ignore packets from this port:

---

```
(config network analyzer name filter mac_address 0)> ignore true
(config network analyzer name filter mac_address 0)>
```

---

By default, this option is set to **false**, which means that the filter will capture packets from this MAC address.

- v. Repeat these steps to add additional MAC addresses.

- e. To create a filter that either captures or ignores packets from one or more specified VLANs:

- i. Add a new VLAN filter:

---

```
(config network analyzer name)> add filter vlan end
(config network analyzer name filter vlan 0)>
```

---

- ii. Set the VLAN that should be captured or ignored:

---

```
(config network analyzer name filter vlan 0)> vlan value
(config network analyzer name filter vlan 0)>
```

---

where *value* is number of the VLAN.

- iii. (Optional) Set the filter should ignore packets from this VLAN:

---

```
(config network analyzer name filter vlan 0)> ignore true
(config network analyzer name filter vlan 0)>
```

---

By default, this option is set to **false**, which means that the filter will capture packets from this MAC address.

- iv. Repeat these steps to add additional VLANs.
- f. To create a filter using Berkeley Packet Filter (BPF) syntax:

---

```
(config network analyzer name)> filter custom value
(config network analyzer name)>
```

---

where *value* is a filter using Berkeley Packet Filter (BPF) syntax. Values that contain spaces must be enclosed in double quotes (").

See [Example filters for capturing data traffic](#) for examples of filters using BPF syntax.

6. (Optional) Schedule the analyzer to run, using this capture filter, based on a specified event or at a particular time:
  - a. Enable scheduling for this capture filter:

---

```
(config network analyzer name)> schedule enable true
(config network analyzer name)>
```

---

- b. Set the mode that will be used to run the capture filter:

---

```
(config network analyzer name)> when mode
(config network analyzer name)>
```

---

where *mode* is one of the following:

- **boot**: The script will run once each time the device boots.
- **interval**: The script will start running at the specified interval, within 30 seconds after the configuration change is saved. If **interval** is selected, set the interval:

---

```
(config add network analyzer name)> on_interval value
(config add network analyzer name)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **on\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config network analyzer name)> on_interval 600s
(config network analyzer name)>
```

---

- **set\_time**: Runs the script at a specified time of the day. If **set\_time** is set, set the time that the script should run, using the format **HH:MM**

---

```
(config network analyzer name)> run_time HH:MM
(config network analyzer name)>
```

---

- **maintenance\_time**: The script will run during the system maintenance time window.

- c. Set the amount of time that the scheduled analyzer session will run:

---

```
(config network analyzer name)> duration value
(config network analyzer name)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **duration** to ten minutes, enter either **10m** or **600s**:



---

```
(config network analyzer name)> save_interval 600s
(config network analyzer name)>
```

---

- d. Set the frequency with which captured events will be saved:

---

```
(config network analyzer name)> save_interval value
(config network analyzer name)>
```

---

where *value* is any number of weeks, days, hours, minutes, or seconds, and takes the format **number{w|d|h|m|s}**.

For example, to set **save\_interval** to ten minutes, enter either **10m** or **600s**:

---

```
(config network analyzer name)> save_interval 600s
(config network analyzer name)>
```

---

7. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Example filters for capturing data traffic

The following are examples of filters using Berkeley Packet Filter (BPF) syntax for capturing several types of network data. See <https://biot.com/capstats/bpf.html> for detailed information about BPF syntax.

### Example IPv4 capture filters

- Capture traffic to and from IP host 192.168.1.1:

---

```
ip host 192.168.1.1
```

---

- Capture traffic from IP host 192.168.1.1:

---

```
ip src host 192.168.1.1
```

---

- Capture traffic to IP host 192.168.1.1:

---

```
ip dst host 192.168.1.1
```

---

- Capture traffic for a particular IP protocol:

---

```
ip proto protocol
```

---

where *protocol* is a number in the range of **1** to **255** or one of the following keywords: **icmp**, **icmp6**, **igmp**, **pim**, **ah**, **esp**, **vrp6**, **udp**, or **tcp**.

- Capture traffic to and from a TCP port 80:

---

```
ip proto tcp and port 80
```

---

- Capture traffic to UDP port 53:

---

```
ip proto udp and dst port 53
```

---

- Capture traffic from UDP port 53:

---

```
ip proto udp and src port 53
```

---

- Capture to and from IP host 10.0.0.1 but filter out ports 22 and 80:

---

```
ip host 10.0.0.1 and not (port 22 or port 80)
```

---

### Example Ethernet capture filters

- Capture Ethernet packets to and from a host with a MAC address of 00:40:D0:13:35:36:

---

```
ether host 00:40:D0:13:35:36
```

---

- Capture Ethernet packets from host 00:40:D0:13:35:36:

---

```
ether src 00:40:D0:13:35:36:
```

---

- Capture Ethernet packets to host 00:40:D0:13:35:36:

---

```
ether dst 00:40:D0:13:35:36
```

---

## Capture packets from the command line

You can start packet capture at the command line with the [analyzer start](#) command. Alternatively, you can schedule the network analyzer to run based on a specified event or at a particular time. See [Configure packet capture for the network analyzer](#) for information about scheduling packet capturing.

Additional analyzer commands allow you to:

- [Stop capturing packets.](#)
- [Save captured data traffic to a file.](#)
- [Clear captured data.](#)

### Required configuration items

- A configured packet capture. See [Configure packet capture for the network analyzer](#) for packet capture configuration information.

To start packet capture from the command line:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Type the following at the Admin CLI prompt:

---

```
> analyzer start name capture_filter
>
```

---

where *capture\_filter* is the name of a packet capture configuration. See [Configure packet capture for the network analyzer](#) for more information.

To determine available packet capture configurations, use the ?.

---

```
> analyzer start name ?

name: Name of the capture filter to use.
Format:
    test_capture
    capture_ping

> analyzer start name
```

---

You can capture up to 10 MB of data traffic in two 5 MB files per interface.

---

**Note** Data traffic is captured to RAM and the captured data is lost when the device reboots unless you save the data to a file. See [Save captured data traffic to a file](#).

---

## Stop capturing packets

You can stop packet capture at the command line with the [analyzer stop](#) command.

To stop packet capture from the command line:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

---

```
> analyzer stop name capture_filter
>
```

---

where *capture\_filter* is the name of a packet capture configuration. See [Configure packet capture for the network analyzer](#) for more information.

To determine available packet capture configurations, use the ?.

---

```
> analyzer stop name ?

name: Name of the capture filter to use.
Format:
    test_capture
```

---

---

```
capture_ping
> analyzer stop name
```

---

## Show captured traffic data

To view captured data traffic, use the `show analyzer` command. The command output show the following information for each packet:

- The packet number.
- The timestamp for when the packet was captured.
- The length of the packet and the amount of data captured.
- Whether the packet was sent or received by the device.
- The interface on which the packet was sent or received.
- A hexadecimal dump of the packet of up to 256 bytes.
- Decoded information of the packet.

To show captured data traffic:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type `admin` to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

---

```
> show analyzer name capture_filter
```

Packet 1 : Sept-29-2023 12:10:00.287682, Length 60 bytes (Captured Length 60 bytes)

Received on interface eth1

```

      00 40 ff 80 01 20 b4 b6 86 21 b5 73 08 00 45 00  .@... ..
.!..s..E.
      00 28 3d 36 40 00 80 06 14 bc 0a 0a 4a 82 0a 0a  .(=6@... ....J..
      4a 48 cd ae 00 16 a4 4b ff 5f ee 1f d8 23 50 10  JH.....K
._....#P.
      08 02 c7 40 00 00 00 00 00 00 00 00 00 00 00  ...@..... ..

```

```

Ethernet Header
  Destination MAC Addr : 00:40:D0:13:35:36
  Source MAC Addr      : fb:03:53:05:11:2f
  Ethernet Type        : IP (0x0800)
IP Header
  IP Version           : 4
  Header Length        : 20 bytes
  ToS                  : 0x00

```

---

---

```

Total Length      : 40 bytes
ID                : 15670 (0x3d36)
Flags             : Do not fragment
Fragment Offset   : 0 (0x0000)
TTL              : 128 (0x80)
Protocol         : TCP (6)
Checksum         : 0x14bc
Source IP Address : 10.10.74.130
Dest. IP Address  : 10.10.74.72
TCP Header
Source Port      : 52654
Destination Port : 22
Sequence Number  : 2756443999
Ack Number       : 3995064355
Data Offset      : 5
Flags           : ACK
Window          : 2050
Checksum        : 0xc740
Urgent Pointer   : 0
TCP Data
00 00 00 00 00 00          .....

```

>

---

where *capture\_filter* is the name of a packet capture configuration. See [Configure packet capture for the network analyzer](#) for more information.

To determine available packet capture configurations, use the ?.

---

```

> show analyzer name ?

name: Name of the capture filter to use.
Format:
    test_capture
    capture_ping

> show analyzer name

```

---

## Save captured data traffic to a file

Data traffic is captured to RAM and when the device reboots, the data is lost. To retain the captured data, first save the data to a file and then upload the file to a PC.

To save captured traffic data to a file, use the [analyzer save](#) command:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

- Type the following at the Admin CLI prompt:

```
> analyzer save filename filename path path
>
```

where:

- filename*** is the name of the file that the captured data will be saved to.

Determine filenames already in use:

Use the tab autocomplete feature to determine filenames that are currently in use:

```
> analyzer save name <tab>
test1_analyzer_capture      test2_analyzer_capture
> analyzer save name
```

- path*** is the path and filename to save captured traffic to. If a relative path is provided, `/etc/config/analyzer` will be used as the root directory for the path and file.

To transfer the file to your PC, see [Download captured data to your PC](#).

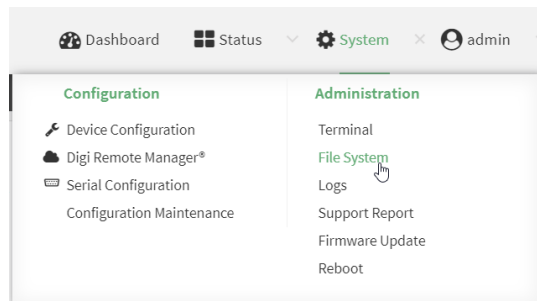
## Download captured data to your PC

After saving captured data to a file (see [Save captured data traffic to a file](#)), you can download the file from the WebUI or from the command line by using the `scp` (secure copy file) command.

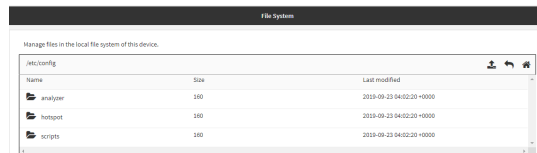
### Web

Log into the Connect EZ WebUI as a user with full Admin access rights.

- On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



- Highlight the **analyzer** directory and click to open the directory.
- Select the saved analyzer report you want to download and click (download).

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type **scp** to use the Secure Copy program to copy the file to your PC:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to remote
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the Connect EZ device.

For example:

To download the traffic saved in the file **/etc/config/analyzer/eth0.pcpng** to a PC with the IP **192.168.210.2**, for a user named **maria**, to the **/home/maria** directory:

---

```
> scp host 192.168.210.2 user maria remote /home/maria local
/etc/config/analyzer/eth0.pcpng to remote

maria@192.168.210.2's password:
eth0.pcpng                100%   11KB  851.3KB/s
00:00
```

---

## Clear captured data

To clear captured data traffic in RAM, use the [analyzer clear](#) command:

### Command line

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Type the following at the Admin CLI prompt:

---

```
> analyzer clear name capture_filter
>
```

---

where *capture\_filter* is the name of a packet capture configuration. See [Configure packet capture for the network analyzer](#) for more information.

To determine available packet capture configurations, use the **?**.

---

```
> analyzer clear name ?

name: Name of the capture filter to use.
Format:
```

---

---

```
test_capture  
capture_ping  
  
> analyzer clear name
```

---

**Note** You can remove data traffic saved to a file using the [rm](#) command.

---



## Use the ping command to troubleshoot network connections

Use the [ping](#) command to troubleshoot connectivity problems.

### Ping to check internet connection

To check your internet connection:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, type the ping command followed by the host name or IP address of the server to be pinged:

---

```
> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=54 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=54 time=10.7 ms
...
>
```

---

3. Type **exit** to exit the Admin CLI.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### Stop ping commands

To stop pings when the number of pings to send (the **count** parameter) has been set to a high value, enter **Ctrl+C**.

## Use the traceroute command to diagnose IP routing problems

Use the **traceroute** command to diagnose IP routing problems. This command traces the route to a remote IP host and displays results. The **traceroute** command differs from [ping](#) in that traceroute shows where the route fails, while ping simply returns a single error on failure.

See the [traceroute](#) command description for command syntax and examples. The **traceroute** command has several parameters. Only **host** is required.

- **host**: The IP address of the destination host.
- **bypass**: Send directly to a host on an attached network.
- **debug**: Enable socket level debugging.
- **dontfragment**: Do not fragment probe packets.
- **first\_ttl**: Specifies with what TTL to start. (Default: 1)
- **gateway**: Route the packet through a specified gateway.
- **icmp**: Use ICMP ECHO for probes.
- **interface**: Specifies the interface.

- **ipchecksums**: Calculate ip checksums.
- **max\_ttl**: Specifies the maximum number of hops. (Default: 30)
- **nomap**: Do not map IP addresses to host names
- **nqueries**: Sets the number of probe packets per hop. (Default: 3)
- **packetlen**: Total size of the probing packet. (Default: -1)
- **pausesecs**: Minimal time interval between probes (Default: 0)
- **port**: Specifies the destination port. (Default: -1)
- **src\_addr**: Chooses an alternative source address.
- **tos**: Set Type of Service. (Default: -1)
- **verbose**: Verbose output.
- **waittime**: Max wait for a response to a probe. (Default: 5)

### Example

This example shows using **traceroute** to verify that the Connect EZ device can route to host **8.8.8.8** ([www.google.com](http://www.google.com)) through the default gateway. The command output shows that **15** routing hops were required to reach the host:

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the Admin CLI prompt, use the **traceroute** command to view IP routing information:

---

```
> traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 52 byte packets
 1 192.168.8.1 (192.168.8.1)  0 ms  0 ms  0 ms
 2 10.10.10.10 (10.10.10.10) 0 ms  2 ms  2 ms
 3 * 10.10.8.23 (10.10.8.23) 1 ms  1 ms
 4 96.34.84.22 (96.34.84.22) 1 ms  1 ms  1 ms
 5 96.34.81.190 (96.34.81.190) 2 ms  2 ms  2 ms
 6 * * *
 7 96.34.2.12 (96.34.2.12)  11 ms 11 ms 11 ms
 8 * * *
 9 8.8.8.8 (8.8.8.8)  11 ms 11 ms 11 ms
>
```

---

By entering a **whois** command on a Unix device, the output shows that the route is as follows:

1. **192/8**: The local network of the Connect EZ device.
2. **192.168.8.1**: The local network gateway to the Internet.
3. **96/8**: Charter Communications, the network provider.
4. **216/8**: Google Inc.

### Stop the traceroute process

To stop the traceroute process, enter **Ctrl-C**.

# Digi Connect EZ regulatory and safety statements

---

## RF exposure statement

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**.

## Federal Communication (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.

## European Community - CE Mark Declaration of Conformity (DoC)

Digi has issued Declarations of Conformity for the Connect EZ concerning emissions, EMC, and safety. For more information, see [www.digi.com/resources/certifications](http://www.digi.com/resources/certifications).

### Important note

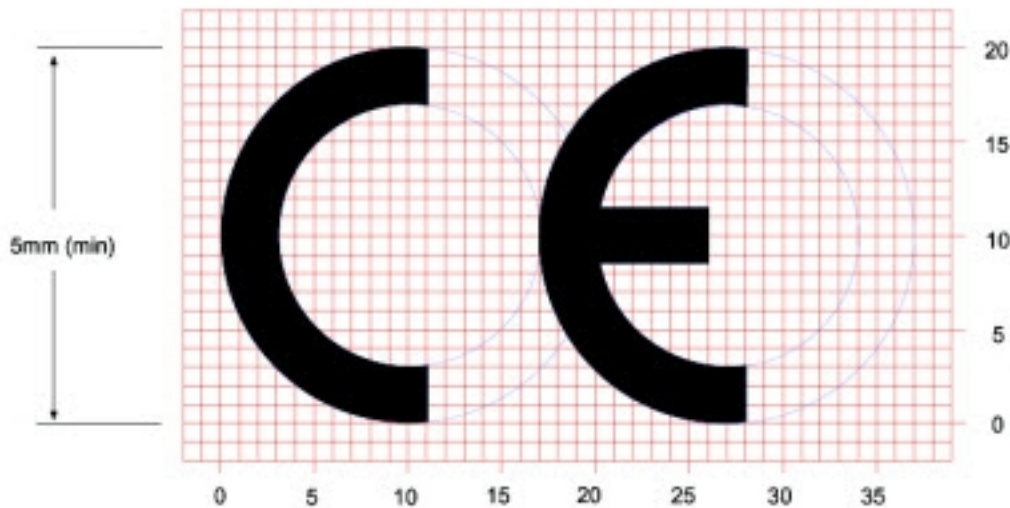
Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

## CE and UKCA OEM labeling requirements

The CE and UKCA markings must be clearly visible and legible when you affix it to the product. If this is not possible, you must attach these marks to the packaging (if any) or accompanying documents.

### CE labeling requirements

The “CE” marking must be affixed to a visible location on the OEM product. The following figure shows 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 5 mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

## UK Conformity Assessed (UKCA) labeling requirements

**UK  
CA**

See [guidance/using-the-ukca-marking](#) for further details.

You must make sure that:

- If you reduce or enlarge the size of your marking, the letters forming the UKCA marking must be in proportion to the version set out below.
- The UKCA marking is at least 5 mm in height – unless a different minimum dimension is specified in the relevant legislation.
- The UKCA marking is easily visible, legible (from 1 January 2023 it must be permanently attached).
- The UKCA marking can take different forms (for example, the color does not have to be solid), as long as it remains visible, legible and maintains the required proportions.

## RoHS compliance statement

All Digi International Inc. products that are compliant with the RoHS Directive (EU Directive 2002/95/EC and subsequent amendments) are marked as **RoHS COMPLIANT**. RoHS COMPLIANT means that the substances restricted by the EU Directive 2002/95/EC and subsequent amendments of the European Parliament are not contained in a finished product above threshold limits mandated by EU Directive 2002/95/EC and subsequent amendments, unless the restrictive substance is subject of an exemption contained in the RoHS Directive. Digi International Inc., cannot guarantee that inventory held by distributors or other third parties is RoHS compliant.

## Safety notices

- Read all instructions before installing and powering the router. You should keep these instructions in a safe place for future reference.
- If the power supply shows signs of damage or malfunction, stop using it immediately, turn off the power and disconnect the power supply before contacting your supplier for a repair or replacement.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. Use only the accessories, attachments, and power supplies provided by the manufacturer-connecting non-approved antennas or power supplies may damage the router, cause interference or create an electric shock hazard, and will void the warranty.
- Do not attempt to repair the product. The router contains no electronic components that can be serviced or replaced by the user. Any attempt to service or repair the router by the user will void the product warranty.
- Ports that are capable of connecting to other apparatus are defined as SELV ports. To ensure conformity with IEC60950 ensure that these ports are only connected to ports of the same type on other apparatus.

## Cautionary statements for Connect EZ

### Residential environment warnings

---

**Note** This equipment meets Class A requirements that may not offer adequate protection to broadcast services within a residential environment.

---

## Product disposal instructions

The WEEE (Waste Electrical and Electronic Equipment: 2002/96/EC) directive has been introduced to ensure that electrical/ electronic products are recycled using the best available recovery techniques to minimize the impact on the environment.



This product contains high quality materials and components which can be recycled. At the end of its life this product **MUST NOT** be mixed with other commercial waste for disposal. Check with the terms and conditions of your supplier for disposal information.

Digi International Ltd WEEE Registration number: WEE/HF1515VJ

## Command line interface

---

This chapter contains the following topics:

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Access the command line interface .....                           | 744 |
| Log in to the command line interface .....                        | 744 |
| Exit the command line interface .....                             | 745 |
| Execute a command from the web interface .....                    | 745 |
| Display help for commands and parameters .....                    | 746 |
| Auto-complete commands and parameters .....                       | 748 |
| Available commands .....                                          | 749 |
| Use the scp command .....                                         | 750 |
| Display status and statistics using the show command .....        | 752 |
| Device configuration using the command line interface .....       | 753 |
| Execute configuration commands at the root Admin CLI prompt ..... | 753 |
| Configuration mode .....                                          | 755 |
| Command line reference .....                                      | 768 |

## Access the command line interface

You can access the Connect EZ command line interface using an SSH connection, a telnet connection, or a serial connection. You can use an open-source terminal software, such as PuTTY or TeraTerm, to access the device through one of these mechanisms.

You can also access the command line interface in the WebUI by using the **Terminal**, or the Digi Remote Manager by using the **Console**.

To access the command line, your device must be configured to allow access, and you must log in as a user who has been configured for the appropriate access.

For further information about configuring access to these services, see:

- Serial: [Serial port](#)
- WebUI: [Configure the web administration service](#)
- SSH: [Configure SSH access](#)
- Telnet: [Configure telnet access](#)

## Log in to the command line interface

### Command line

1. Connect to the Connect EZ device by using a serial connection, SSH or telnet, or the **Terminal** in the WebUI or the **Console** in the Digi Remote Manager. See [Access the command line interface](#) for more information.
  - For serial connections, the default configuration is:
    - **115200** baud rate
    - **8** data bits
    - **no** parity
    - **1** stop bit
    - **no** flow control
  - For SSH and telnet connections, the default IP address of the device is **192.168.2.1** on the **ETH1** port.
2. At the login prompt, enter the username and password of a user with Admin access:

---

```
login: admin
Password: *****
```

---

The default username is **admin**. The default unique password for your device is printed on the device label.

3. Depending on the device configuration, you may be presented with another menu, for example:

---

```
Access selection menu:
```

```
  a: Admin CLI
  q: Quit
```

---



---

```
Select access or quit [admin] :
```

---

Type **a** or **admin** to access the Connect EZ command line.

You will now be connected to the Admin CLI:

---

```
Connecting now...
Press Tab to autocomplete commands
Press '?' for a list of commands and details
Type 'help' for details on navigating the CLI
Type 'exit' to disconnect from the Admin CLI
```

```
>
```

---

See [Command line interface](#) for detailed instructions on using the command line interface.

## Exit the command line interface

### Command line

1. At the command prompt, type **exit**.

---

```
> exit
```

---

2. Depending on the device configuration, you may be presented with another menu, for example:

---

```
Access selection menu:

    a: Admin CLI
    q: Quit

Select access or quit [admin] :
```

---

Type **q** or **quit** to exit.

## Execute a command from the web interface

Log into the Connect EZ WebUI as a user with full Admin access rights.

1. At the main menu, click **Terminal**. The device console appears.

---

```
Connect EZ login:
```

---

2. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

The Admin CLI prompt appears.

---

```
>
```

---

## Display help for commands and parameters

### The help command

When executed from the root command prompt, **help** displays information about autocomplete operations, how to move the cursor on the Connect EZ command line, and other keyboard shortcuts:

---

```
> help

Commands
-----
-
?          Show commands help
<Tab>     Tab completion, displays all valid commands to complete command,
          if only one command is possible, it is used
<Space>   Like tab except shortest prefix is used if command is valid
<Enter>   Enter an input. If quoting then a new line is created instead. If
          the input is invalid then characters will be deleted until a
          prefix for a valid command is found.

Ctrl + A  Move cursor to start of line
Ctrl + E  Move cursor to end of line
Ctrl + W  Delete word under cursor until start of line or [\',", ,\,/,.]
Ctrl + R  If the current input is invalid then characters will be deleted
          until a prefix for a valid command is found.

Ctrl + left  Jump cursor left until start of line or [\',", ,\,/,.]
Ctrl + right Jump cursor right until start of line or [\',", ,\,/,.]

>
```

---

### The question mark (?) command

When executed from the root command prompt, **?** displays available commands:

---

```
> ?

Commands
-----
-
config    View and modify the configuration
exit      Exit the CLI
analyzer  Analyzer commands.
cp        Copy a file or directory.
grep      Grep a file.
help      Show CLI editing and navigation commands.
ls        List a directory.
mkdir     Create a directory.

more      View a file.
mv        Move a file or directory.
ping      Ping a host.
reboot    Reboot the system.
rm        Remove a file or directory.
scp       Copy a file or directory over SSH.
show      Show instance statistics.
ssh       SSH login to a remote server
```

---

---

```

system      System commands.
tail        Tail a file.
telnet      Telnet login to a remote server
traceroute  Print the route packets trace to network host.
.
>

```

---

## Display help for individual commands

When included with a command name, both **?** and **help** provide further information about the command. For example:

1. To display further information about the **show** command, type either **show ?** or **show help**:

---

```

> show ?

Commands
-----
--
analyzer      Show analyzer
arp           Show ARP tables
cloud         Show drm statistics
config        Show config deltas.
containers    Show container statistics.
dhcp-lease    Show DHCP leases.
dns           Show DNS servers.
event         Show event list
ipsec         Show IPsec statistics.
l2tp          Show L2TP statistics.
l2tppath      Show L2TPv3 ethernet statistics.
location      Show loction information.
log           Show syslog.
manufacture   Show manufacturer information.
modbus-gateway Show modbus gateway status & statistics.
nemo          Show NEMO statistics.
network       Show network interface statistics.
ntp           Show NTP information.
openvpn       Show OpenVPN statistics.
route         Show IP routing information.
scep-client   Show SCEP client statistics.
serial        Show serial statistics.
surelink      Show Surelink statistics.
system        Show system statistics.
version       Show firmware version.

> show

```

---

## Use the Tab key or the space bar to display abbreviated help

When executed from the root command prompt, pressing the **Tab** key or the space bar displays an abbreviated list of available commands:

Similar behavior is available with any command name:

---

```
> config network interface <space>
..          ...          defaultip          defaultlinklocal lan
loopback
> config network interface
```

---

## Auto-complete commands and parameters

When entering a command and parameter, press the **Tab** key to cause the command line interface to auto-complete as much of the command and parameter as possible. Typing the space bar has similar behavior. If multiple commands are available that will match the entered text, auto-complete is not performed and the available commands are displayed instead.

Auto-complete applies to these command elements only :

- Command names. For example, typing **net<Tab>** auto-completes the command as **network**.
- Parameter names. For example:
  - **ping hostname int<Tab>** auto-completes the parameter as **interface**.
  - **system b<Tab>** auto-completes the parameter as **backup**.
- Parameter values, where the value is one of an enumeration or an on/off type; for example:

---

```
(config)> serial port1 enable t<Tab>
```

---

auto-completes to

---

```
(config)> serial port1 enable true
```

---

Auto-complete does not function for:

- Parameter values that are string types.
- Integer values.
- File names.
- Select parameters passed to commands that perform an action.

## Available commands

The following commands are available from the Admin CLI prompt:

| Command           | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>config</b>     | Used to view and modify the configuration.<br><br>See <a href="#">Device configuration using the command line interface</a> for more information about using the <b>config</b> command.                                                                                                                                                                                                          |
| <b>exit</b>       | Exits the CLI.                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>analyzer</b>   | Analyzer commands.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>cat</b>        | View a file.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>clear</b>      | Commands to clear the device's status or systems.                                                                                                                                                                                                                                                                                                                                                |
| <b>container</b>  | Create, delete, or interact with a container.                                                                                                                                                                                                                                                                                                                                                    |
| <b>cp</b>         | Copies a file or directory.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>grep</b>       | Grep a file.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>help</b>       | Displays: <ul style="list-style-type: none"> <li>▪ CLI editing and navigation commands, when executed from the root of the Admin CLI prompt.</li> <li>▪ Available commands, syntax diagram, and parameter information, when executed in conjunction with another command.</li> </ul> See <a href="#">Display help for commands and parameters</a> for information about the <b>help</b> command. |
| <b>ls</b>         | Lists the contents of a directory.                                                                                                                                                                                                                                                                                                                                                               |
| <b>mkdir</b>      | Creates a directory.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>monitoring</b> | Monitoring commands.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>more</b>       | Displays the contents of a file.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>mv</b>         | Moves a file or directory.                                                                                                                                                                                                                                                                                                                                                                       |
| <b>ping</b>       | Pings a remote host using Internet Control Message Protocol (ICMP) Echo Request messages.                                                                                                                                                                                                                                                                                                        |
| <b>poweroff</b>   | Powers off the system.                                                                                                                                                                                                                                                                                                                                                                           |
| <b>reboot</b>     | Reboots the Connect EZ device.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>rm</b>         | Removes a file.                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>scp</b>        | Uses the secure copy protocol (SCP) to transfer files between the Connect EZ device and a remote host.                                                                                                                                                                                                                                                                                           |

| Command           | Description                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | See <a href="#">Use the scp command</a> for information about using the <b>scp</b> command.                                                                                                        |
| <b>show</b>       | Displays information about the device and the device's configuration.<br><br>See <a href="#">Display status and statistics using the show command</a> for more information about the show command. |
| <b>speedtest</b>  | Perform a speed test.                                                                                                                                                                              |
| <b>ssh</b>        | SSH login to a remote server.                                                                                                                                                                      |
| <b>system</b>     | Issues commands related to system functionality.                                                                                                                                                   |
| <b>tail</b>       | Tail a file.                                                                                                                                                                                       |
| <b>telnet</b>     | Telnet login to a remote server.                                                                                                                                                                   |
| <b>traceroute</b> | Sends and tracks route packets to a destination host.                                                                                                                                              |

---

**Note** For commands that operate on the Connect EZ's file system, such as the **cp**, **ls**, and **mkdir** commands, see [File system](#) for information about the file system, including how to copy, move and delete files and directories.

---

## Use the scp command

The **scp** command uses Secure Copy Protocol (SCP) to transfer files between the Connect EZ device and a remote host.

### Required configuration items

- The hostname or IP address of the remote host.
- The username and password of the user on the remote host.
- Whether the file is being copied to the Connect EZ device from a remote host, or to the remote host from the Connect EZ device.
  - If the file is being copied to the Connect EZ device from a remote host:
    - The path and filename of the file on the remote host that will be copied to the Connect EZ device.
    - The location on the Connect EZ device where the file will be copied.
  - If the file is being copied to a remote host from the Connect EZ device:
    - The path and filename of the file on the Connect EZ device that will be copied to the remote host.
    - The location on the remote host where the file will be copied.

### Copy a file from a remote host to the Connect EZ device

To copy a file from a remote host to the Connect EZ device, use the **scp** command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to local
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the path and filename of the file on the remote host that will be copied to the Connect EZ device.
- *local-path* is the location on the Connect EZ device where the copied file will be placed.

For example:

To copy firmware from a remote host with an IP address of 192.168.4.1 to the /etc/config directory on the Connect EZ device, issue the following command:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/bin/Connect EZ-24.3.bin
local /etc/config/scripts to local
admin@192.168.4.1's password: adminpwd
Connect EZ-24.3.bin          100%   36MB   11.1MB/s   00:03
>
```

---

### **Transfer a file from the Connect EZ device to a remote host**

To copy a file from the Connect EZ device to a remote host, use the `scp` command as follows:

---

```
> scp host hostname-or-ip user username remote remote-path local local-path to
remote
```

---

where:

- *hostname-or-ip* is the hostname or IP address of the remote host.
- *username* is the name of the user on the remote host.
- *remote-path* is the location on the remote host where the file will be copied.
- *local-path* is the path and filename on the Connect EZ device.

For example:

To copy a support report from the Connect EZ device to a remote host at the IP address of 192.168.4.1:

1. Use the **system support-report** command to generate the report:

---

```
> system support-report path /var/log/
Saving support report to /var/log/support-report-0040D0133536-24-01-12-
12:10:00.bin
Support report saved.
>
```

---

2. Use the **scp** command to transfer the report to a remote host:

---

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/var/log/support-report-00:40:D0:13:35:36-24-01-12-12:10:00.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-24-01-12-12:10:00.bin
>
```

---

## Display status and statistics using the show command

The Connect EZ **show** command display status and statistics for various features.

For example:

### show config

The **show config** command displays all the configuration settings for the device that have been changed from the default settings. This is a particularly useful when troubleshooting the device.

---

```
> show config

auth tacacs+ service "login"
auth user admin password
"$2a$05$WlJQhquI7BgsytkpobKhaeLPtWraGANBcrleEaJX/wJv63JENW/HOu"
add auth user test
add auth user test group end "admin"
add auth user test group end "serial"
auth user test password
"$2a$05$RdGYz1sLKbWrqe6cZjlsd.otg03JZR6n9939XV6EYWUSP0tMAz05W"
network interface lan ipv4 type "dhcp"
network interface lan zone "external"

schema version "445"

>
```

---

### show system

The **show system** command displays system information and statistics for the device, including CPU usage.

---

```
> show system

Model                : Digi Connect EZ
Serial Number       : Connect EZxxxxxxxxxyyyxx
SKU                 : Connect EZ
Hostname            : Connect EZ
MAC Address         : DF:DD:E2:AE:21:18

Hardware Version    : 50001947-01 1P
Firmware Version    : 24.3
Alt. Firmware Version : 24.3
Alt. Firmware Build Date : Fri, Jan 12, 2024 12:10:00
Bootloader Version  : 19.7.23.0-15f936e0ed

Current Time        : Thu, Jan 11, 2024 12:10:00 +0000
CPU                 : 1.4%
Uptime              : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
Temperature         : 40C
Location            :
Contact             :

>
```

---



## show network

The `show network` command displays status and statistics for network interfaces.

```
> show network
```

| Interface        | Proto | Status | Address                         |
|------------------|-------|--------|---------------------------------|
| defaultip        | IPv4  | up     | 192.168.210.1/24                |
| defaultlinklocal | IPv4  | up     | 169.254.100.100/16              |
| lan              | IPv4  | up     | 192.168.2.1                     |
| lan              | IPv6  | up     | 0:0:0:0:0:ffff:c0a8:301         |
| loopback         | IPv4  | up     | 127.0.0.1/8                     |
| wan              | IPv4  | up     | 192.168.3.1/24                  |
| wan              | IPv6  | up     | fd00:2704::240:ffff:fe80:120/64 |

```
>
```

## Device configuration using the command line interface

The `config` command allows for device configuration from the command line. All configuration tasks that can be performed by using the WebUI can also be performed by using the `config` command.

There are two ways to invoke the `config` command from the CLI:

- Execute the `config` command and parameters at the root prompt. See [Execute configuration commands at the root Admin CLI prompt](#) for more information.
- Enter configuration mode by executing the `config` command without any parameters. See [Configuration mode](#) for more information.

## Execute configuration commands at the root Admin CLI prompt

You can execute the `config` command at the root Admin CLI prompt with any appropriate parameters. When the `config` command is used in this way, changes to the device's configuration are automatically saved when the command is executed.

For example, to disable the SSH service from the root prompt, enter the following command:

```
> config service ssh enable false
>
```

The Connect EZ device's ssh service is now disabled.

**Note** When the `config` command is executed at the root prompt, certain configuration actions that are available in configuration mode cannot be performed. This includes validating configuration changes, canceling and reverting configuration changes, and performing actions on elements in lists. See [Configuration mode](#) for information about using configuration mode.

## Display help for the config command from the root Admin CLI prompt

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character after the `config` command.

1. For example:

---

```
> config ?
```

---

Will display the following help information:

---

```
> config ?
```

Additional Configuration

---

```
-
application          Custom scripts
auth                 Authentication
cloud                Central management
firewall             Firewall
monitoring           Monitoring
network              Network
serial               Serial
service              Services
system               System
vpn                  VPN
```

Run "config" with no arguments to enter the configuration editing mode.

```
> config
```

---

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command:

---

```
> config service ?
```

```
Services
```

Additional Configuration

---

```
-
dns                   DNS
mdns                  Service Discovery (mDNS)
multicast             Multicast
ntp                   NTP
remote_control        Remote control
snmp                  SNMP
ssh                   SSH
telnet                Telnet
web_admin              Web administration
```

```
> config service
```

---

3. Next, display help for the **config service ssh** command:

---

```
> config service ssh ?
```

```
SSH: An SSH server for managing the device.
```

---

---

```

Parameters                Current Value
-----
-
enable                    true           Enable
key                       [private]  Private key
port                      22         Port

Additional Configuration
-----
-
acl                       Access control list
mdns

> config service ssh

```

---

4. Lastly, display the allowed values and other information for the **enable** parameter:

---

```

> config service ssh enable ?

Enable: Enable the service.
Format: true, false, yes, no, 1, 0
Default value: true
Current value: true

> config service ssh enable

```

---

## Configuration mode

Configuration mode allows you to perform multiple configuration tasks and validate the changes prior to saving them. You can cancel all changes without saving them at any time. Configuration changes do not take effect until the configuration is saved.

### Enable configuration mode

To enable configuration mode, at the root prompt, enter the **config** command without any parameters:

---

```

> config
(config)>

```

---

When the command line is in configuration mode, the prompt will change to include **(config)**, to indicate that you are currently in configuration mode.

### Enter configuration commands in configuration mode

There are two ways to enter configuration commands while in configuration mode:

- Enter the full command string from the config prompt.  
For example, to disable the ssh service by entering the full command string at the config prompt:

---

```
(config)> service ssh enable false
(config)>
```

---

- Execute commands by moving through the configuration schema.  
For example, to disable the ssh service by moving through the configuration and then executing the **enable false** command:

- At the **config** prompt, enter **service** to move to the **service** node:

---

```
(config)> service
(config service)>
```

---

- Enter **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

- Enter **enable false** to disable the **ssh** service:

---

```
(config service ssh)> enable false
(config service ssh)>
```

---

See [Move within the configuration schema](#) for more information about moving within the configuration.

## Save changes and exit configuration mode

To save changes that you have made to the configuration while in configuration mode, use **save**. The save command automatically validates the configuration changes; the configuration will not be saved if it is not valid. Note that you can also validate configuration changes at any time while in configuration mode by using the **validate** command.

---

```
(config)> save
Configuration saved.
>
```

---

After using **save** to save changes to the configuration, you will automatically exit configuration mode. To return to configuration mode, type **config** again.

## Exit configuration mode without saving changes

You can discard any unsaved configuration changes and exit configuration mode by using the **cancel** command:

---

```
(config)> cancel
>
```

---

After using **cancel** to discard unsaved changes to the configuration, you will automatically exit configuration mode.

## Configuration actions

In configuration mode, configuration actions are available to perform tasks related to saving or canceling the configuration changes, and to manage items and elements in lists. The commands can be listed by entering a question mark (?) at the **config** prompt.

The following actions are available:

| Configuration actions | Description                                                                                                                                                   |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>cancel</b>         | Discards unsaved configuration changes and exits configuration mode.                                                                                          |
| <b>save</b>           | Saves configuration changes and exits configuration mode.                                                                                                     |
| <b>validate</b>       | Validates configuration changes.                                                                                                                              |
| <b>revert</b>         | Reverts the configuration to default settings. See <a href="#">The revert command</a> for more information.                                                   |
| <b>show</b>           | Displays configuration settings.                                                                                                                              |
| <b>add</b>            | Adds a named element, or an element in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>add</b> command with lists.    |
| <b>del</b>            | Deletes a named element, or an element in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>del</b> command with lists. |
| <b>move</b>           | Moves elements in a list. See <a href="#">Manage elements in lists</a> for information about using the <b>move</b> command with lists.                        |

## Display command line help in configuration mode

Display additional configuration commands, as well as available parameters and values, by entering the question mark (?) character at the **config** prompt. For example:

1. Enter ? at the **config** prompt:

```
(config)> ?
```

This will display the following help information:

```
(config)> ?
```

```
Additional Configuration
```

```
-----
```

```
--
```

```
application          Custom scripts
auth                  Authentication
cloud                 Central management
firewall              Firewall
monitoring            Monitoring
network               Network
```

---

```

serial          Serial
service         Services
system         System
vpn            VPN

```

---

```
(config)>
```

---

2. You can then display help for the additional configuration commands. For example, to display help for the **config service** command, use one of the following methods:

- At the **config** prompt, enter **service ?**:

---

```
(config)> service ?
```

---

- At the **config** prompt:
  - a. Enter **service** to move to the **service** node:

---

```
(config)> service
(config service)>
```

---

- b. Enter **?** to display help for the **service** node:

---

```
(config service)> ?
```

---

Either of these methods will display the following information:

---

```
config> service ?
```

```
Services
```

```
Additional Configuration
```

```
-----
```

```
--
```

```

dns             DNS
mdns            Service Discovery (mDNS)
multicast       Multicast
ntp             NTP
remote_control  Remote control
snmp            SNMP
ssh             SSH
telnet          Telnet
web_admin       Web administration

```

```
(config)> service
```

---

3. Next, to display help for the **service ssh** command, use one of the following methods:

- At the **config** prompt, enter **service ssh ?**:

---

```
(config)> service ssh ?
```

---

- At the **config** prompt:
  - a. Enter **service** to move to the **service** node:

---

```
(config)> service
(config service)>
```

---

- b. Enter **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

- c. Enter **?** to display help for the **ssh** node:

---

```
(config service ssh)> ?
```

---

Either of these methods will display the following information:

---

```
(config)> service ssh ?
```

SSH: An SSH server for managing the device.

| Parameters | Current Value |             |
|------------|---------------|-------------|
| enable     | true          | Enable      |
| key        | [private]     | Private key |
| port       | 22            | Port        |

Additional Configuration

---

```
acl          Access control list
mdns
```

---

```
(config)> service ssh
```

---

4. Lastly, to display allowed values and other information for the **enable** parameter, use one of the following methods:

- At the **config** prompt, enter **service ssh enable ?**:

---

```
(config)> service ssh enable ?
```

---

- At the **config** prompt:

- a. Enter **service** to move to the **service** node:

---

```
(config)> service
(config service)>
```

---

- b. Enter **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

- c. Enter **enable ?** to display help for the **enable** parameter:

---

```
(config service ssh)> enable ?
(config service ssh)>
```

---

Either of these methods will display the following information:

---

```
(config)> service ssh enable ?

Enable: Enable the service.
Format: true, false, yes, no, 1, 0
Default value: true
Current value: true

(config)> service ssh enable
```

---

## Move within the configuration schema

You can perform configuration tasks at the CLI by moving within the configuration.

- Move forward one node in the configuration by entering the name of an Additional Configuration option:
  1. At the **config** prompt, type **service** to move to the **service** node:

---

```
(config)> service
(config service)>
```

---

2. Type **ssh** to move to the **ssh** node:

---

```
(config service)> ssh
(config service ssh)>
```

---

3. Type **acl** to move to the **acl** node:

---

```
(config service ssh)> acl
(config service ssh acl)>
```

---

4. Type **zone** to move to the **zone** node:

---

```
(config service ssh acl)> zone
(config service ssh acl zone)>
```

---

You can also enter multiple nodes at once to move multiple steps in the configuration:

---

```
(config)> service ssh acl zone
(config service ssh acl zone)>
```

---

- Move backward one node in the configuration by entering two periods (**..**):

---

```
(config service ssh acl zone)> ..
(config service ssh acl)>
```

---



You can also move back multiples nodes in the configuration by typing multiple sets of two periods:

---

```
(config service ssh acl zone)> .. .. ..
(config service)>
```

---

- Move to the root of the config prompt from anywhere within the configuration by entering three periods (...):

---

```
(config service ssh acl zone)> ...
(config)>
```

---

## Manage elements in lists

While in configuration mode, you can use the **add**, **del**, and **move** action commands to manage elements in a list. When working with lists, these actions require an index number to identify the list item that will be acted on.

### Add elements to a list

When used with parameters that contains lists of elements, the **add** command is used to add an element to the list.

For example, to add an authentication method:

1. Display current authentication method by using the **show** command:

---

```
(config)> show auth method
0 local
(config)>
```

---

2. Add an authentication method by using the **add *index\_item*** command. For example:

- To add the TACACS+ authentication method to the beginning of the list, use the index number **0**:

---

```
(config)> add auth method 0 tacacs+
(config)> show auth method
0 tacacs+
1 local
(config)>
```

---

- To add the TACACS+ authentication method to the end of the list, use the **end** keyword:

---

```
(config)> add auth method end tacacs+
(config)> show auth method
0 local
1 tacacs+
(config)>
```

---

### The end keyword

As demonstrated above, the **end** keyword is used to add an element to the end of a list. Additionally, the **end** keyword is used to add an element to a list that does not have any elements.

For example, to add an authentication group to a user that has just been created:

1. Use the **show** command to verify that the user is not currently a member of any groups:

---

```
(config)> show auth user new-user group
(config)>
```

---

2. Use the **end** keyword to add the admin group to the user's configuration:

---

```
(config)> add auth user new-user group end admin
(config)>
```

---

3. Use the **show** command again to verify that the admin group has been added to the user's configuration:

---

```
(config)> show auth user new-user group
0 admin
(config)>
```

---

### **Delete elements from a list**

When used with parameters that contains lists of elements, the **del** command is used to delete an element in the list.

For example, to delete an authentication method:

1. Use the **show** command to display current authentication method configuration:

---

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

---

2. Delete one of the authentication methods by using the **del *index\_number*** command. For example:

- a. To delete the local authentication method, use the index number **0**:

---

```
(config)> del auth method 0
(config)>
```

---

- b. Use the **show** command to verify that the local authentication method was removed:

---

```
(config)> show auth method
0 tacacs+
1 radius
(config)>
```

---

### **Move elements within a list**

Use the **move** command to reorder elements in a list.

For example, to reorder the authentication methods:

1. Use the **show** command to display current authentication method configuration:

---

```
(config)> show auth method
0 local
1 tacacs+
2 radius
(config)>
```

---

2. To configure the device to use TACACS+ authentication first to authenticate a user, use the **move *index\_number\_1 index\_number\_2*** command:

---

```
(config)> move auth method 1 0
(config)>
```

---

3. Use the **show** command again to verify the change:

---

```
(config)> show auth method
0 tacacs+
1 local
2 radius
(config)>
```

---

## The revert command

The **revert** command is used to revert changes to the Connect EZ device's configuration and restore default configuration settings. The behavior of the revert command varies depending on where in the configuration hierarchy the command is executed, and whether the optional **path** parameter is used. After executing the revert command, you must save the configuration changes by using the **save** command. You can also discard the configuration changes by using the **cancel** command.



**CAUTION!** The **revert** command reverts all changes to the default configuration, not only unsaved changes.

### ***Revert all configuration changes to default settings***

To discard all configuration changes and revert to default settings, use the **revert** command at the config prompt without the optional **path** parameter:

1. At the config prompt, enter **revert**:

---

```
(config)> revert
(config)>
```

---

2. Set the password for the admin user prior to saving the changes:

---

```
(config)> auth user admin password pwd
(config)>
```

---

3. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

### ***Revert a subset of configuration changes to the default settings***

There are two methods to revert a subset of configuration changes to the default settings.

- Enter the **revert** command with the **path** parameter. For example, to revert all changes to the authentication methods configuration:

1. Enter the **revert** command with the **path** set to **auth method**:

---

```
(config)> revert auth method
(config)>
```

---

2. Save the configuration and apply the change

---

```
(config)> save
Configuration saved.
>
```

---

3. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

- Move to the location in the configuration and enter the **revert** command without the **path** parameter. For example:

1. Change to the auth method node:

---

```
(config)> auth method
(config auth method)>
```

---

2. Enter the **revert** command:

---

```
(config auth method)> revert
(config auth method)>
```

---

3. Save the configuration and apply the change

---

```
(config auth method)> save
Configuration saved.
>
```

---

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

- You can also use a combination of both of these methods:

1. Change to the **auth** node:

```
(config)> auth
(config auth)>
```

2. Enter the **revert** command with the **path** set to **method**:

```
(config auth)> revert method
(config auth)>
```

3. Save the configuration and apply the change

```
(config auth)> save
Configuration saved.
>
```

4. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Enter strings in configuration commands

For string parameters, if the string value contains a space, the value must be enclosed in quotation marks. For example, to assign a descriptive name for the device using the **system** command, enter:

```
(config)> system description "Digi Connect EZ"
```

## Example: Create a new user by using the command line

In this example, you will use the Connect EZ command line to create a new user, provide a password for the user, and assign the user to authentication groups.

1. Select the device in Remote Manager and click **Actions > Open Console**, or log into the Connect EZ local command line as a user with full Admin access rights.  
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the command line, type **config** to enter configuration mode:

```
> config
(config)>
```

3. At the config prompt, create a new user with the username **user1**:
  - Method one: Create a user at the root of the config prompt:

```
(config)> add auth user user1
(config auth user user1)>
```

- Method two: Create a user by moving through the configuration:
  - a. At the config prompt, enter **auth** to move to the **auth** node:

---

```
(config)> auth
(config auth)>
```

---

- b. Enter **user** to move to the **user** node:

---

```
(config auth)> user
(config auth user)>
```

---

- c. Create a new user with the username **user1**:

---

```
(config auth user)> add user1
(config auth user user1)>
```

---

4. Configure a password for the user:

---

```
(config auth user user1)> password pwd1
(config auth user user1)>
```

---

5. List available authentication groups:

---

```
(config auth user user1)> show .. .. group
```

```
admin
  acl
    admin
      enable true
    nagios
      enable false
    openvpn
      enable false
      no tunnels
    portal
      enable false
      no portals
    serial
      enable false
      no ports
    shell
      enable false
```

```
serial
  acl
    admin
      enable true
    nagios
      enable false
    openvpn
      enable false
      no tunnels
```

---

---

```
portal
  enable false
  no portals
serial
  enable true
  ports
    0 port1
shell
  enable false
(config auth user user1)>
```

---

6. Add the user to the admin group:

---

```
(config auth user user1)> add group end admin
(config auth user user1)>
```

---

7. Save the configuration and apply the change

---

```
(config auth user user1)> save
Configuration saved.
>
```

---

8. Type **exit** to exit the Admin CLI.

Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

## Command line reference

### **analyzer clear**

Clears the traffic captured by the analyzer.

#### **Syntax**

---

```
analyzer clear <name>
```

---

#### **Parameters**

name: Name of the capture filter to use.

### **analyzer save**

Saves the current captured traffic to a file.

#### **Syntax**

---

```
analyzer save <name> <path>
```

---

#### **Parameters**

name: Name of the capture filter to use.

path: The path and filename to save captured traffic to. If a relative path is provided, /etc/config/analyzer will be used as the root directory for the path and file.

### **analyzer start**

Start a capture session of packets on this devices interfaces.

#### **Syntax**

---

```
analyzer start <name>
```

---

#### **Parameters**

name: Name of the capture filter to use.

### **analyzer stop**

Stops the traffic capture session.

#### **Syntax**

---

```
analyzer stop <name>
```

---

#### **Parameters**

name: Name of the capture filter to use.

### **cat**

View the contents of a file.



**Syntax**

---

```
cat <path>
```

---

**Parameters**

path: The file to view.

**clear dhcp-lease ip-address**

Clear the DHCP lease for the specified IP address.

**Syntax**

---

```
clear dhcp-lease ip-address ADDRESS
```

---

**Parameters**

address: An IPv4 or IPv6 address

**clear dhcp-lease mac**

Clear the DHCP lease for the specified MAC address.

**Syntax**

---

```
clear dhcp-lease mac ADDRESS
```

---

**Parameters**

address: 12-digit, colon-delimited MAC address [00:11:22:AA:BB:CC]

**cp**

Copy a file or directory.

**Syntax**

---

```
cp <source> <destination> [force]
```

---

**Parameters**

source: The source file or directory to copy.

destination: The destination path to copy the source file or directory to.

force: Do not ask to overwrite the destination file if it exists.

**grep**

Grep the contents of a file.

**Syntax**

---

```
grep <match> <path>
```

---

**Parameters**

match: Output all lines in file matching string.  
path: The file to grep.

**help**

Show CLI editing and navigation commands.

**Syntax**

---

help

---

**Parameters**

None

## ls

List a directory.

### Syntax

---

```
ls <path> [show-hidden]
```

---

### Parameters

path: List files and directories under this path.

show-hidden: Show hidden files and directories. Hidden filenames begin with '.'.

## mkdir

Create a directory. Parent directories are created as needed.

### Syntax

---

```
mkdir <path>
```

---

### Parameters

path: The directory path to create.

## modem sms send

Send an SMS message to the provided phone number (MSISDN).

### Syntax

---

```
modem sms send <msisdn> <message> [name STRING] [imei STRING]
```

---

### Parameters

msisdn: Destination phone number (MSISDN).

message: Message to send.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

## modem sms send-binary

Send a binary SMS message to the provided phone number (MSISDN).

### Syntax

---

```
modem sms send-binary <msisdn> <message> [name STRING] [imei STRING]
```

---

### Parameters

msisdn: Destination phone number (MSISDN).

message: Message to send.

name: The configured name of the modem to execute this CLI command on.

imei: The IMEI of the modem to execute this CLI command on.

## monitoring metrics upload

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

### Syntax

---

```
monitoring metrics upload
```

---

### Parameters

None

## monitoring

Commands to clear the device's status or systems.

### ***monitoring metrics***

Device metrics commands.

### **upload**

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

#### ***Parameters***

None

## monitoring metrics upload

Immediately upload current device health metrics. Functions as if a scheduled upload was triggered.

### ***Syntax***

---

```
monitoring metrics upload
```

---

#### **Parameters**

None

## more

View a file.

### ***Syntax***

---

```
more <path>
```

---

#### **Parameters**

path: The file to view.

## mv

Move a file or directory.

### ***Syntax***

---

```
mv <source> <destination> [force]
```

---

#### **Parameters**

source: The source file or directory to move.

destination: The destination path to move the source file or directory to.

force: Do not ask to overwrite the destination file if it exists.

## ping

Ping a host using ICMP echo.

## Syntax

---

```
ping <host> [interface STRING] [source STRING] [ipv6] [size INTEGER] [count INTEGER] [broadcast]
```

---

### Parameters

host: The name or address of the remote host to send ICMP ping requests to. If broadcast is enabled, can be the broadcast address.

interface: The network interface to send ping packets from when the host is reachable over a default route. If not specified, the system's primary default route will be used.

source: The ping command will send a packet with the source address set to the IP address of this interface, rather than the address of the interface the packet is sent from.

ipv6: If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

size: The number of bytes sent in the ICMP ping request. (Minimum: 0, Default: 56)

count: The number of ICMP ping requests to send before terminating. (Minimum: 1, Default: 100)

broadcast: Enable broadcast ping functionality.

## poweroff

Power off the system.

## Syntax

---

```
poweroff
```

---

### Parameters

None

## reboot

Reboot the system.

## Parameters

None

## rm

Remove a file or directory.

## Syntax

---

```
rm <path> [force]
```

---

### Parameters

path: The path to remove.

force: Force the file to be removed without asking.

## scp

Copy a file or directory over SSH.

### Syntax

---

```
scp <local> <remote> <host> <user> <to> [port INTEGER]
```

---

### Parameters

local: The path and name of the file on the local device to copy to or from.

remote: The path and name of the file on the remote host to copy to or from.

host: The hostname or IP address of the remote host.

user: The username to use when connecting to the remote host.

to: Determine whether to copy the file from the local device to the remote host, or from the remote host to the local device.

port: The SSH port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 22)

## show analyzer

Show packets from a specified analyzer capture.

### Syntax

---

```
show analyzer <name>
```

---

### Parameters

name: Name of the capture filter to use.

## show arp

Show ARP tables. If no IP version is specified IPv4 & IPV6 will be displayed.

### Syntax

---

```
show arp [ipv4] [ipv6] [verbose]
```

---

### Parameters

ipv4: Display IPv4 routes. If no IP version is specified IPv4 & IPV6 will be displayed.

ipv6: Display IPv6 routes. If no IP version is specified IPv4 & IPV6 will be displayed.

verbose: Display more information (less concise, more detail).

## show cloud

Show drm status & statistics.

### Syntax

---

```
show cloud
```

---

### Parameters

None

## show config

Show a summary of changes made to the default configuration. The changes shown are not suitable for pasting into a CLI session.

### Syntax

---

```
show config [cli_format]
```

---

### Parameters

*cli\_format*: Show the exact CLI commands required to configure the device from a default configuration. The changes shown are suitable for pasting into a CLI session, although individual output lines maybe context sensitive and unable to be entered in isolation.

## show dhcp-lease

Show DHCP leases.

### Syntax

---

```
show dhcp-lease [all] [verbose]
```

---

### Parameters

*all*: Show all leases (active and inactive (not in etc/config/dhcp.\*lease)).  
*verbose*: Display more information (less concise, more detail).

## show dns

Show DNS servers and associated domains.

### Syntax

---

```
show dns
```

---

### Parameters

None

## show eth

Show ethernet status & statistics.

### Syntax

---

```
show eth [name STRING]
```

---

### Parameters

*name*: Display more details and configuration data for a specific ethernet instance.

## show event

Show event list (high level).



## Syntax

---

```
show event [table <status|error|info>] [number INTEGER]
```

---

### Parameters

table: Type of event log to be displayed (status, error, info).

number: Number of lines to retrieve from log. (Minimum: 1, Default: 20)

## show hotspot

Show hotspot statistics.

## Syntax

---

```
show hotspot [name STRING] [ip STRING]
```

---

### Parameters

name: The configured instance name of the hotspot.

ip: IP address of a specific client, to limit the status display to only this client.

## show ipsec

Show IPsec status & statistics.

## Syntax

---

```
show ipsec [tunnel STRING] [all] [verbose]
```

---

### Parameters

tunnel: Display more details and config data for a specific IPsec tunnel.

all: Display all tunnels including disabled tunnels.

verbose: Display status of one or all tunnels in plain text.

## show l2tp lac

Show L2TP access concentrator status & statistics.

## Syntax

---

```
show l2tp lac [name STRING]
```

---

### Parameters

name: Display more details for a specific L2TP access concentrator.

## show l2tp lns

Show L2TP network server status & statistics.

## Syntax

---

```
show l2tp lns [name STRING]
```

---

**Parameters**

name: Display more details for a specific L2TP network server.

**show l2tpeth**

Show L2TPv3 ethernet tunnel session status and statistics.

**Syntax**

---

```
show l2tpeth [name STRING]
```

---

**Parameters**

name: Display more details for a specific L2TPv3 ethernet tunnel session.

**show location**

Show location information.

**Syntax**

---

```
show location [geofence]
```

---

**Parameters**

geofence: Show geofence information.

**show log**

Show system log (low level).

**Syntax**

---

```
show log [number INTEGER] [filter <critical|warning|debug|info>]
```

---

**Parameters**

number: Number of lines to retrieve from log. (Minimum: 1, Default: 20)

filter: Filters for type of log message displayed (critical, warning, info, debug). Note, filters from the number of messages retrieved not the whole log (this can be very time consuming). If you require more messages of the filtered type, increase the number of messages retrieved using 'number'.

**show manufacture**

Show manufacturer information.

**Syntax**

---

```
show manufacture [verbose]
```

---

**Parameters**

verbose: Display more information (less concise, more detail).

**show modbus-gateway**

Show modbus gateway status & statistics.

### **Syntax**

---

```
show modbus-gateway [verbose]
```

---

### **Parameters**

verbose: Display more information (less concise, more detail).

## **show nemo**

Show NEMO status and statistics.

### **Syntax**

---

```
show nemo [name STRING]
```

---

### **Parameters**

name: Display more details and configuration data for a specific NEMO instance.

## **show network**

Show network interface status & statistics.

### **Syntax**

---

```
show network [interface STRING] [all] [verbose]
```

---

### **Parameters**

interface: Display more details and config data for a specific network interface.

all: Display all interfaces including disabled interfaces.

verbose: Display more information (less concise, more detail).

## **show ntp**

Show NTP status & statistics.

### **Syntax**

---

```
show ntp
```

---

### **Parameters**

None

## **show openvpn client**

Show OpenVPN client status & statistics.

### **Syntax**

---

```
show openvpn client [name STRING] [all]
```

---

**Parameters**

name: Display more details and config data for a specific OpenVPN client.

all: Display all clients including disabled clients.

**show openvpn server**

Show OpenVPN server status & statistics.

**Syntax**

---

```
show openvpn server [name STRING] [all]
```

---

**Parameters**

name: Display more details and config data for a specific OpenVPN server.

all: Display all servers including disabled servers.

**show route**

Show IP routing information.

**Syntax**

---

```
show route [ipv4] [ipv6] [verbose]
```

---

**Parameters**

ipv4: Display IPv4 routes.

ipv6: Display IPv6 routes.

verbose: Display more information (less concise, more detail).

**show scep-client**

Show SCEP client status and statistics.

**Syntax**

---

```
show scep-client [name STRING]
```

---

**Parameters**

name: Display more details and configuration data for a specific SCEP client instance.

**show scripts**

Show scheduled system scripts.

**Syntax**

---

```
show scripts
```

---

**Parameters**

None

## show serial

Show serial status & statistics.

### Syntax

---

```
show serial [port STRING]
```

---

### Parameters

port: Display more details and config data for a specific serial port.

## show surelink interface

Show SureLink status & statistics for network interfaces.

### Syntax

---

```
show surelink interface [name STRING] [all]
```

---

### Parameters

name: The name of a specific network interface.

all: Show all network interfaces.

## show surelink ipsec

Show SureLink status & statistics for IPsec tunnels.

### Syntax

---

```
show surelink ipsec [tunnel STRING] [all]
```

---

### Parameters

tunnel: The name of a specific IPsec tunnel.

all: Show all IPsec tunnels.

## show surelink openvpn

Show SureLink status & statistics for OpenVPN clients.

### Syntax

---

```
show surelink openvpn [client STRING] [all]
```

---

### Parameters

client: The name of the OpenVPN client.

all: Show all OpenVPN clients.

## show surelink state

Show SureLink state & fail counts for each network interfaces.

**Syntax**

---

```
show surelink state
```

---

**Parameters**

None

**show system**

Show system status & statistics.

**Syntax**

---

```
show system [verbose]
```

---

**Parameters**

*verbose*: Display more information (disk usage, etc).

**show version**

Show firmware version.

**Syntax**

---

```
show version [verbose]
```

---

**Parameters**

*verbose*: Display more information (build date).

**show vrrp**

Show VRRP status & statistics.

**Syntax**

---

```
show vrrp [name STRING] [all] [verbose]
```

---

**Parameters**

*name*: Display more details and config data for a specific VRRP instance.

*all*: Display all VRRP instances including disabled instances.

*verbose*: Display all VRRP status and statistics including disabled instances.

**show web-filter**

Show web filter status & statistics.

**Syntax**

---

```
show web-filter
```

---

**Parameters**

None

**speedtest**

Perform a speed test to a remote host using nuttcp or iPerf. The system's primary default route will be used. The speed test will take approximately 30 seconds to complete.

**Syntax**


---

```
speedtest <host> [size INTEGER] [mode <nuttcp|iperf>] [output <text|json>]
```

---

**Parameters**

host: The name or address of the remote speed test host/server.

size: The number of kilobytes sent in the speed test packets. (Minimum: 0, Default: 1000)

mode: The type of speed test protocol to run. (Default: nuttcp)

output: The format of output to display the speed test results as. (Default: text)

**ssh**

Use SSH protocol to log into a remote server.

**Syntax**


---

```
ssh <host> <user> [port INTEGER] [command STRING]
```

---

**Parameters**

host: The hostname or IP address of the remote host.

user: The username to use when connecting to the remote host.

port: The SSH port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 22)

command: The command that will be automatically executed once the SSH session to the remote host is established.

**system backup**

Save the device's configuration to a file. Archives are full backups including generated SSH keys and dynamic DHCP lease information. Command backups are a list of CLI commands required to build the device's configuration.

**Syntax**


---

```
system backup [type <custom-defaults|cli-config|archive>] [path STRING]  
[passphrase STRING] [remove <custom-defaults>]
```

---

**Parameters**

type: The type of backup file to create. Archives are full backups including generated SSH keys and dynamic DHCP lease information. CLI configuration backups are a list of CLI commands used to build the device's configuration. (Default: archive)

path: The file path to save the backup to. (Default: /var/log/)

passphrase: Encrypt the archive with a passphrase.

remove: Remove a backup file.

## system cloud register

Register with Digi Remote Manager account.

### Syntax

---

```
system cloud register <username> <password> [group STRING]
```

---

### Parameters

username: Digi Remote Manager username.

password: Digi Remote Manager password.

group: Group to add device in Digi Remote Manager.

## system disable-cryptography

Erase the device's configuration and reboot into a limited mode with no cryptography available. The device's shell will be accessible over Telnet (port 23) at IP address 192.168.210.1. To return the device to normal operation, perform the configuration erase procedure with the device's ERASE button twice consecutively.

### Syntax

---

```
system disable-cryptography
```

---

### Parameters

None

## system duplicate-firmware

Duplicate the running firmware to the alternate partition so that the device will always boot the same firmware version.

### Syntax

---

```
system duplicate-firmware
```

---

### Parameters

None

## system factory-erase

Erase the device to restore to factory defaults. All configuration and automatically generated keys will be erased.

### Syntax

---

```
system factory-erase
```

---

### Parameters

None



## system find-me

Find Me function to flash LEDs on this device to help users locate the unit.

### Syntax

---

```
system find-me <state>
```

---

### Parameters

state: Find Me control to flash cellular-related LEDs.

## system firmware ota check

Query the Digi firmware server for the latest device firmware version.

### Syntax

---

```
system firmware ota check
```

---

### Parameters

None

## system firmware ota list

Query the Digi firmware server for a list of device firmware versions.

### Syntax

---

```
system firmware ota list
```

---

### Parameters

None

## system firmware ota update

Perform FOTA (firmware-over-the-air) update. The device will be updated to the latest firmware version unless the version argument is used to specify the firmware version.

### Syntax

---

```
system firmware ota update [version STRING]
```

---

### Parameters

version: Firmware version name.

## system firmware update

Update the current firmware image. Upon reboot the new firmware will be run.

### Syntax

---

```
system firmware update <file>
```

---

**Parameters**

file: Firmware filename and path.

**system power ignition off\_delay**

Update the current ignition off delay without changing the configuration.

**Syntax**

---

```
system power ignition off_delay <off_delay>
```

---

**Parameters**

off\_delay: Ignition power off delay. Format: number{h|m|s}, Max: 18h. (Minimum: 0s, Maximum: 18h)

**system restore**

Restore the device's configuration from a backup archive or CLI commands file.

**Syntax**

---

```
system restore <path> [passphrase STRING]
```

---

**Parameters**

path: The path to the backup file.

passphrase: Decrypt the archive with a passphrase.

**system script start**

Run a manual script. Scripts that are disabled, not a manual script, or already running can not be run.

**Syntax**

---

```
system script start <script>
```

---

**Parameters**

script: Script to start.

**system script stop**

Stop an active running script. Scripts scheduled to run again will still run again (disable a script to prevent it from running again).

**Syntax**

---

```
system script stop <script>
```

---

**Parameters**

script: Script to stop.

**system serial clear**

Clears the serial log.

**Syntax**

---

```
system serial clear <port>
```

---

**Parameters**

port: Serial port.

**system serial restart**

Delete and restart the serial log.

**Syntax**

---

```
system serial restart <port>
```

---

**Parameters**

port: Serial port.

**system serial save**

Saves the current serial log to a file.

**Syntax**

---

```
system serial save <port> <path>
```

---

**Parameters**

port: Serial port.

path: The path and filename to save captured traffic to. If a relative path is provided, /etc/config/serial will be used as the root directory for the path and file.

**system serial show**

Displays the serial log on the screen.

**Syntax**

---

```
system serial show <port>
```

---

**Parameters**

port: Serial port.

**system support-report**

Save a support report to a file and include with support requests.

**Syntax**

---

```
system support-report [path STRING]
```

---

**Parameters**

path: The file path to save the support report to. (Default: /var/log/)

**system time set**

Set the local date and time using the timezone set in the system.time.timezone config setting.

**Syntax**

---

```
system time set <datetime>
```

---

**Parameters**

datetime: The date in year-month-day hour:minute:second format (e.g "2021-09-26 12:24:48").

**system time sync**

Set the local time to the first enabled time source that returns valid time information.

**Syntax**

---

```
system time sync
```

---

**Parameters**

None

**system time test**

Test each enabled time source. This test will not affect the device's current local date and time.

**Syntax**

---

```
system time test
```

---

**Parameters**

None

**tail**

Tail a file to see its contents.

**Syntax**

---

```
tail <path> [timeout INTEGER] [filter STRING] [match STRING]
```

---

**Parameters**

path: The file to tail.

timeout: The amount of time in seconds to tail the file. (Default: 10)

filter: Only see output that contains this string.

match: Stop tail when this string is detected in output.

## telnet

Use Telnet protocol to log into a remote server.

### Syntax

---

```
telnet <host> [port INTEGER]
```

---

### Parameters

host: The hostname or IP address of the remote host.

port: The telnet port to use to connect to the remote host. (Minimum: 1, Maximum: 65535, Default: 23)

## traceroute

Print the route packets trace to network host.

### Syntax

---

```
traceroute <host> [ipv6] [gateway STRING] [interface STRING] [first_ttl INTEGER] [max_ttl INTEGER] [port INTEGER] [nqueries INTEGER] [src_addr STRING] [tos INTEGER] [waittime INTEGER] [pausesecs INTEGER] [packetlen INTEGER] [debug] [dontfragment] [icmp] [nomap] [bypass]
```

---

### Parameters

host: The host that we wish to trace the route packets for.

ipv6: If a hostname is defined as the value of the 'host' parameter, use the hosts IPV6 address.

gateway: Tells traceroute to add an IP source routing option to the outgoing packet that tells the network to route the packet through the specified gateway.

interface: Specifies the interface through which traceroute should send packets. By default, the interface is selected according to the routing table.

first\_ttl: Specifies with what TTL to start. (Minimum: 1, Default: 1)

max\_ttl: Specifies the maximum number of hops (max time-to-live value) traceroute will probe. (Minimum: 1, Default: 30)

port: Specifies the destination port base traceroute will use (the destination port number will be incremented by each probe). A value of -1 specifies that no specific port will be used. (Minimum: -1, Default: -1)

nqueries: Sets the number of probe packets per hop. A value of -1 indicated. (Minimum: 1, Default: 3)

src\_addr: Chooses an alternative source address. Note that you must select the address of one of the interfaces. By default, the address of the outgoing interface is used.

tos: For IPv4, set the Type of Service (ToS) and Precedence value. Useful values are 16 (low delay) and 8 (high throughput). Note that in order to use some TOS precedence values, you have to be super user. For IPv6, set the Traffic Control value. A value of -1 specifies that no value will be used. (Minimum: -1, Default: -1)

waittime: Determines how long to wait for a response to a probe. (Minimum: 1, Default: 5)

pausesecs: Minimal time interval between probes. (Minimum: 0, Default: 0)

packetlen: Total size of the probing packet. Default 60 bytes for IPv4 and 80 for Ipv6. A value of -1 specifies that the default value will be used. (Minimum: -1, Default: -1)

debug: Enable socket level debugging.

dontfragment: Do not fragment probe packets.

icmp: Use ICMP ECHO for probes.

nomap: Do not try to map IP addresses to host names when displaying them.

bypass: Bypass the normal routing tables and send directly to a host on an attached network.

## **vtysh**

Opens the integrated shell for FRRouting (FRR), for more information on FRRouting and VTYSH, visit the FRRouting documentation at <https://docs.frrouting.org/projects/dev-guide/en/latest/vtysh.html>.

### **Syntax**

---

vtysh

---

### **Parameters**

None