Connect EZ 4/4i

User Guide

Firmware version 22.2

Revision history—90002459

Revision	Date	Description
C	March 2022	Release of Digi Connect EZ firmware version 22.2: ■ VPN enhancements: • Renamed **VPN** > **IPsec** > **Tunnels** > **Policies** > **Local network setting** to **Local traffic selector** and added **Remote traffic selector**. • Added a **Dynamic** option to the **Local traffic selector** to configuration of a local network by protocol and/or port instead of a network address range. • Added Protocol and Port match criteria for **Local traffic selector** and **Remote traffic selector**. • Added **VPN** > **IPsec** > **Advanced** > **Debug level** to specify the logging verbosity of IPsec messages in the device system logs. ■ Enhancements to communications with Digi Remote Manager: • Enhanced security for communications with Digi Remote Manager by using client-side certificates. • The default URL for the device's Remote Manager connection is now edp12.devicecloud.com. This URL is required to utilize the client-side certificate support. ■ New **Switch SIM** SureLink action for WWAN interfaces, which allows SureLink to be configured to switch to the alternate SIM if the modem is connected but SureLink test are failing. • New **Switch SIM fail count** option to determine how many SureLink failures are required prior to switching to the alternate SIM. ■ New **Socket ID string** option to send the configured text to the remote server(s) when a TCP socket connection is opened to the serial port. ■ New **cat** Admin CLI command for displaying file contents. **Additional change** ■ Update serial port mode documentation.
B	December 2021	Release of DigiConnect EZ firmware version 21.11: ■ Configuration option to allow for automatic update of new firmware (disabled by default). ■ User authentication enhancements: • Added TACACS+ command authorization and accounting for Admin CLI commands.

Revision	Date	Description
		• Added a new username alias to provide an alternate username that allows for special characters in the username. ■ Wi-Fi enhancements: • PKI certificate-based authentication for WPA2/WPA3 Enterprise Wi-Fi client connections, including options for SCEP client integration for automatic certificate generation. • Improved Wi-Fi scanning tool on the **Status** page to automatically setup the underlying basic client-mode settings so the device can scan for nearby APs without requiring the user to first configure the client-mode settings. ■ VPN enhancements: • Added support for PPP-over-L2TP tunnels. • Changed default IPsec IKE DH group to 14 for enhanced compatibility with industry standard settings. ■ Location services enhancements: • New option for Location service to specify the talker ID used in NMEA mesage strings. • Include the mode indicator field in NMEA messages constructed when a GPS fix isn't obtained. ■ SureLink enhancments: • Added new settings under cellular Surelink options to have the device reset the cellular modem if a specified number of Surelink tests fail • Added **show surelink** Admin CLI command. ■ Serial port enhancements: • New option to add and configure an external USB-to-serial adapter. • Disable serial history in remote access mode by default. ■ Support for sending analog and digial I/O health metrics to Digi Remote Manager.
		Additional updates for Connect EZ 4i: Added information for Connect EZ 4i intallations: Connect EZ 4i ONLY: Review installation instructions for hazardous locations
A	November 2021	Initial release of the document.

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.

© 2022 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

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.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi Connect EZ 4/4i User Guide, 90002459 A) in the subject line of your email.

Contents

Digi Connect EZ 4/4i User Guide

Get started with Connect EZ 4/4i

Connect EZ 4i ONLY: Review installation instructions for hazardous locations 19
Step 1: Verify product components 19
    Included equipment for Connect EZ 4/4i 19
    Optional additional cellular equipment 20
Step 2: Connect the power supply 21
Step 3: Connect to site network using an Ethernet LAN 22
Step 4: Connect the device to the network using Wi-Fi 22
    Connect the Wi-Fi antenna 22
    Enable Wi-Fi 22
    Configure Wi-Fi on the device 23
Step 5: Discover the IP address using the Digi Navigator 23
Step 6: Configure RealPort from the Digi Navigator 24
Step 7: Connect to the web UI and update the Connect EZ firmware 25
    Connect to the local Web UI on the Connect EZ 25
    Update the firmware on the Connect EZ 26
Step 8: Connect to Digi Remote Manager 27

Connect equipment to the Connect EZ serial port

Serial Status page 28
Serial connector pinout 28
Serial Status page 29

Hardware

Front panel and LEDs 31
    Wi-Fi LED descriptions 32
    Cell service and signal LED descriptions 33
Back panel 34
Bottom panel 34
Change the password on the Connect EZ 35
Cellular connection: Insert the CORE module 35
    Prerequisites 35
    Connect hardware and connect to a cellular network 36
Mount the Connect EZ device 36
    Attach to a mounting surface using the two mounting tabs 37

Attach to DIN rail with clip ... 37
Use the ERASE button to reset your device to the factory defaults ... 37
Discover the device's IP address: Additional methods ... 38
Discover the IP address using a Micro USB cable ... 38
Manually configure the PC and assign an IP address to the device ... 39
Loose label sample ... 40

Configuration and management

Review Connect EZ default settings ... 43
Local WebUI ... 43
Digi Remote Manager ... 43
Default interface configuration ... 43
Other default configuration settings ... 44
Change the default password for the admin user ... 44
Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point ... 45
Configuration methods ... 47
Using Digi Remote Manager ... 49
Access Digi Remote Manager ... 49
Using the web interface ... 49
Log out of the web interface ... 50
Use the local REST API to configure the Connect EZ device ... 50
Use the GET method to return device configuration information ... 50
Use the POST method to modify device configuration parameters and list arrays ... 52
Use the DELETE method to remove items from a list array ... 53
Access the terminal screen from the web UI ... 54
Using the command line ... 55
Access the command line interface ... 55
Log in to the command line interface ... 55
Exit the command line interface ... 56

Interfaces

Wide Area Networks (WANs) ... 58
Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs) ... 59
Configure WAN/WWAN priority and default route metrics ... 59
WAN/WWAN failover ... 61
Configure SureLink active recovery to detect WAN/WWAN failures ... 62
Configure the device to reboot when a failure is detected ... 72
Disable SureLink ... 80
Example: Use a ping test for WAN failover from Ethernet to cellular ... 83
Using Ethernet devices in a WAN ... 86
Using cellular modems in a Wireless WAN (WWAN) ... 86
Configure a Wide Area Network (WAN) ... 105
Configure a Wireless Wide Area Network (WWAN) ... 113
Show WAN and WWAN status and statistics ... 123
Delete a WAN or WWAN ... 125
Default outbound WAN/WWAN ports ... 126
Local Area Networks (LANs) ... 127
About Local Area Networks (LANs) ... 128
Configure a LAN ... 128
Example: Configure two LANs ... 136
Show LAN status and statistics ... 144
Delete a LAN ... 146

DHCP servers ... 147
Create a Virtual LAN (VLAN) route ... 163
Default services listening on LAN ports ... 166
Bridging ... 167
Configure a bridge ... 168
Show Surelink status and statistics ... 171
Show Surelink status for all interfaces ... 171
Show Surelink status for a specific interface ... 172
Show Surelink status for all IPsec tunnels ... 172
Show Surelink status for a specific IPsec tunnel ... 173
Show Surelink status for all OpenVPN clients ... 173
Show Surelink status for a specific OpenVPN client ... 173

Serial port

Default serial port configuration ... 175
Serial mode options ... 175
View serial port information ... 175
Default serial port configuration ... 175
Configure Login mode ... 176
Configure Remote Access mode ... 180
Configure Application mode ... 186
Configure RealPort mode ... 189
Install RealPort on a Windows computer ... 189
Configure the serial port for RealPort mode ... 191
Configure the RealPort service ... 194
Configure UDP serial mode ... 195
Configure Modbus mode ... 201
Show serial status and statistics ... 206
Log serial port messages ... 206
Digi Navigator application ... 207
Step 6: Configure RealPort from the Digi Navigator ... 207
Step 5: Discover the IP address using the Digi Navigator ... 209
Install the Digi Navigator ... 209
Digi Navigator features ... 210
Connect to and access the Digi Navigator ... 211
Discover the IP address when connected to a network ... 211
Discover the IP address when not on a network ... 212
Manage the RealPort device list ... 212
Access the web UI from the Digi Navigator ... 213
Filter devices for display in the Digi Navigator ... 213
Access Digi Remote Manager from the Digi Navigator ... 214

Wi-Fi

Wi-Fi configuration ... 216
Default access point SSID and password ... 216
Default Wi-Fi configuration ... 216
Configure the Wi-Fi radio's channel ... 218
Configure the Wi-Fi radio to support DFS channels in client mode ... 219
Required configuration items ... 220
Configure the Wi-Fi radio's band and protocol ... 221
Configure the Wi-Fi radio's transmit power ... 223
Configure an open Wi-Fi access point ... 224

Configure a Wi-Fi access point with personal security 229
Configure a Wi-Fi access point with enterprise security 236
Isolate Wi-Fi clients 243
Isolate clients connected to the same access point 243
Isolate clients connected to different access points 244
Configure a Wi-Fi client and add client networks 249
Show Wi-Fi access point status and statistics 258
Show Wi-Fi client status and statistics 259

Hotspot

Hotspot authentication modes 262
Hotspot DHCP server 263
Hotspot security 263
Hotspot configuration 264
Enable hotspot using the default configuration 265
Change the default hotspot SSID 269
Change the default hotspot IP address and subnet 270
Change the default hotspot bandwidth limits 273
Add an Ethernet port to the default hotspot 274
Use policy routes with hotspot 277
Create a new hotspot 278
Configure the hotspot to use local shared password authentication 289
Configure the hotspot to use RADIUS shared password authentication 291
Configure the hotspot to use RADIUS users authentication 294
Configure the hotspot to use HotspotSystem authentication 298
Show hotspot status and statistics 301
Customize the hotspot login page 304
Edit sample hotspot HTML pages 305
Upload custom hotspot HTML pages 306
Restore hotspot default sample pages 308
Hotspot RADIUS attributes 309

Routing

IP routing 311
Configure a static route 312
Delete a static route 314
Policy-based routing 316
Configure a routing policy 316
Routing services 324
Configure routing services 324
Show the routing table 327
Dynamic DNS 328
Configure dynamic DNS 328
Virtual Router Redundancy Protocol (VRRP) 333
VRRP+ 333
Configure VRRP 333
Configure VRRP+ 336
Example: VRRP/VRRP+ configuration 344
Configure device one (master device) 344
Configure device two (backup device) 348
Show VRRP status and statistics 353

Virtual Private Networks (VPN)

IPsec 356
- IPsec data protection 356
- IPsec mode 356
- IPsec modes 356
- Internet Key Exchange (IKE) settings 356
- Authentication 357
- Configure an IPsec tunnel 357
- Configure IPsec failover 384
- Configure SureLink active recovery for IPsec 387
- Show IPsec status and statistics 394
- Debug an IPsec configuration 395
- Configure a Simple Certificate Enrollment Protocol client 396
- Example: SCEP client configuration with Fortinet SCEP server 400
- Disable hardware cryptographic acceleration 405

OpenVPN 407
- Configure an OpenVPN server 408
- Configure an OpenVPN Authentication Group and User 416
- Configure an OpenVPN client by using an .ovpn file 420
- Configure an OpenVPN client without using an .ovpn file 422
- Configure SureLink active recovery for OpenVPN 427
- Show OpenVPN server status and statistics 434
- Show OpenVPN client status and statistics 435

Generic Routing Encapsulation (GRE) 437
- Configuring a GRE tunnel 437
- Show GRE tunnels 441
- Example: GRE tunnel over an IPSec tunnel 442

L2TP 457
- Configure a PPP-over-L2TP tunnel 457
- Configure SureLink active recovery for PPP-over-L2TP 466
- L2TP with IPsec 473
- Show L2TP tunnel status 473

L2TPv3 Ethernet 475
- Configure an L2TPv3 tunnel 475
- Show L2TPV3 tunnel status 479

NEMO 480
- Configure a NEMO tunnel 481
- Show NEMO status 485

Services

Allow remote access for web administration and SSH 488
Configure the web administration service 491
Configure SSH access 500
Use SSH with key authentication 507
- Generating SSH key pairs 507

Configure telnet access 509
Configure DNS 513
- Show DNS server 518

Simple Network Management Protocol (SNMP) 520
- SNMP Security 520
- Configure Simple Network Management Protocol (SNMP) 520
- Download MIBs 524

Location information ... 526
Configure the location service ... 527
Configure the device to use a user-defined static location ... 528
Configure the device to accept location messages from external sources ... 530
Forward location information to a remote host ... 534
Configure geofencing ... 541
Show location information ... 553
Modbus gateway ... 554
Configure the Modbus gateway ... 555
Show Modbus gateway status and statistics ... 568
System time ... 571
Configure the system time ... 571
Manually set the system date and time ... 574
Network Time Protocol ... 575
Configure the device as an NTP server ... 575
Show status and statistics of the NTP server ... 580
Configure a multicast route ... 581
Ethernet network bonding ... 584
Enable service discovery (mDNS) ... 586
Use the iPerf service ... 589
Example performance test using iPerf3 ... 594
Configure the ping responder service ... 594
Example performance test using iPerf3 ... 598

Applications

Configure scripts to run automatically ... 600
Task one: Upload the application ... 600
Task two: Configure the application to run automatically ... 602
Configure scripts to run manually ... 606
Task one: Upload the application ... 606
Task two: Configure the application to run automatically ... 608
Start a manual script ... 611
Stop a script that is currently running ... 612
Show script information ... 613
Run a Python application at the shell prompt ... 614
Start an interactive Python session ... 616
Digidevice module ... 617
Use digidevice.cli to execute CLI commands ... 618
Use digidevice.datapoint to upload custom datapoints to Digi Remote Manager ... 619
Use digidevice.config for device configuration ... 622
Use Python to respond to Digi Remote Manager SCI requests ... 624
Use digidevice runtime to access the runtime database ... 633
Use Python to upload the device name to Digi Remote Manager ... 635
Use Python to access the device location data ... 637
Use Python to set the maintenance window ... 641
Use Python to send and receive SMS messages ... 643
Use Python to access serial ports ... 645
Use the Paho MQTT python library ... 646

User authentication

Connect EZ user authentication ... 651
User authentication methods ... 651

Add a new authentication method ... 653
Delete an authentication method ... 655
Rearrange the position of authentication methods ... 656
Authentication groups ... 658
Change the access rights for a predefined group ... 659
Add an authentication group ... 661
Delete an authentication group ... 665
Local users ... 667
Change a local user's password ... 668
Configure a local user ... 670
Delete a local user ... 678
Terminal Access Controller Access-Control System Plus (TACACS+) ... 680
TACACS+ user configuration ... 681
TACACS+ server failover and fallback to local authentication ... 682
Configure your Connect EZ device to use a TACACS+ server ... 682
Remote Authentication Dial-In User Service (RADIUS) ... 687
RADIUS user configuration ... 688
RADIUS server failover and fallback to local configuration ... 688
Configure your Connect EZ device to use a RADIUS server ... 689
LDAP ... 692
LDAP user configuration ... 694
LDAP server failover and fallback to local configuration ... 695
Configure your Connect EZ device to use an LDAP server ... 695
Configure serial authentication ... 700
Disable shell access ... 702
Set the idle timeout for Connect EZ users ... 703
Example user configuration ... 705
Example 1: Administrator user with local authentication ... 705
Example 2: RADIUS, TACACS+, and local authentication for one user ... 707

Firewall

Firewall configuration ... 714
Create a custom firewall zone ... 714
Configure the firewall zone for a network interface ... 716
Delete a custom firewall zone ... 717
Port forwarding rules ... 718
Configure port forwarding ... 718
Delete a port forwarding rule ... 722
Packet filtering ... 725
Configure packet filtering ... 725
Enable or disable a packet filtering rule ... 729
Delete a packet filtering rule ... 730
Configure custom firewall rules ... 732
Configure captive portals ... 735
Delete captive portals ... 738
Configure Quality of Service options ... 739

System administration

Review device status ... 750
Configure system information ... 751
Update system firmware ... 753
Manage firmware updates using Digi Remote Manager ... 753

Certificate management for firmware images ... 753
Downgrading ... 753
Dual boot behavior ... 757
Update cellular module firmware ... 758
Update modem firmware over the air (OTA) ... 759
Update modem firmware by using a local firmware file ... 761
Reboot your Connect EZ device ... 762
Reboot your device immediately ... 762
Schedule reboots of your device ... 763
Erase device configuration and reset to factory defaults ... 764
Configure the Connect EZ device to use custom factory default settings ... 767
Locate the device by using the Find Me feature ... 769
Configuration files ... 771
Save configuration changes ... 771
Save configuration to a file ... 772
Restore the device configuration ... 773
Schedule system maintenance tasks ... 776
Disable device encryption ... 780
Re-enable cryptography after it has been disabled. ... 781
Configure the speed of your Ethernet ports ... 783

Monitoring

intelliFlow ... 787
Enable intelliFlow ... 787
Use intelliFlow to display average CPU and RAM usage ... 790
Use intelliFlow to display top data usage information ... 791
Use intelliFlow to display data usage by host over time ... 793
Configure NetFlow Probe ... 794

Central management

Digi Remote Manager support ... 800
Certificate-based enhanced security ... 800
Configure Digi Remote Manager ... 800
Collect device health data and set the sample interval ... 807
Enable event log upload to Digi Remote Manager ... 810
Log into Digi Remote Manager ... 811
Use Digi Remote Manager to view and manage your device ... 812
Add a device to Digi Remote Manager ... 813
View Digi Remote Manager connection status ... 813
Configure multiple devices using profiles ... 814
Learn more ... 814

File system

The Connect EZ local file system ... 816
Display directory contents ... 816
Create a directory ... 817
Display file contents ... 818
Copy a file or directory ... 818
Move or rename a file or directory ... 819
Delete a file or directory ... 820

Upload and download files ... 821
Upload and download files by using the WebUI ... 821
Upload and download files by using the Secure Copy command ... 822
Upload and download files using SFTP ... 823

Diagnostics

Perform a speedtest ... 826
Generate a support report ... 826
View system and event logs ... 828
View System Logs ... 828
View Event Logs ... 830
Configure syslog servers ... 832
Configure options for the event and system logs ... 834
Analyze network traffic ... 839
Configure packet capture for the network analyzer ... 840
Example filters for capturing data traffic ... 849
Capture packets from the command line ... 850
Stop capturing packets ... 851
Show captured traffic data ... 851
Save captured data traffic to a file ... 853
Download captured data to your PC ... 854
Clear captured data ... 855
Use the ping command to troubleshoot network connections ... 856
Ping to check internet connection ... 856
Stop ping commands ... 856
Use the traceroute command to diagnose IP routing problems ... 856

Command line interface

Access the command line interface ... 859
Log in to the command line interface ... 859
Exit the command line interface ... 860
Execute a command from the web interface ... 860
Display help for commands and parameters ... 861
The help command ... 861
The question mark (?) command ... 861
Display help for individual commands ... 862
Use the Tab key or the space bar to display abbreviated help ... 863
Auto-complete commands and parameters ... 863
Available commands ... 864
Use the scp command ... 865
Display status and statistics using the show command ... 866
show config ... 866
show system ... 867
show network ... 867
Device configuration using the command line interface ... 867
Execute configuration commands at the root Admin CLI prompt ... 868
Display help for the config command from the root Admin CLI prompt ... 868
Configuration mode ... 870
Enable configuration mode ... 870
Enter configuration commands in configuration mode ... 870
Save changes and exit configuration mode ... 871
Exit configuration mode without saving changes ... 871

Configuration actions 871
Display command line help in configuration mode 872
Move within the configuration schema 874
Manage elements in lists 875
The revert command 877
Enter strings in configuration commands 879
Example: Create a new user by using the command line 879
Command line reference 882
analyzer clear 883
analyzer save 884
analyzer start 884
analyzer stop 884
clear dhcp-lease ip-address 884
clear dhcp-lease mac 885
cp 885
help 885
ls 886
mkdir 887
modem at 887
modem at-interactive 887
modem firmware check 887
modem firmware list 887
modem firmware ota check 888
modem firmware ota list 888
modem firmware ota update 888
modem firmware update 888
modem pin change 889
modem pin disable 889
modem pin enable 889
modem pin status 890
modem pin unlock 890
modem puk status 890
modem puk unlock 890
modem reset 891
modem scan 891
modem sim-slot 891
monitoring 891
monitoring metrics upload 892
more 892
mv 892
ping 892
reboot 894
rm 895
scp 896
show analyzer 896
show arp 896
show cloud 896
show config 897
show dhcp-lease 897
show dns 897
show event 897
show hotspot 897
show ipsec 898
show l2tp lac 898
show l2tp lns 898

show l2tpeth ... 898
show location ... 899
show log ... 899
show manufacture ... 899
show modbus-gateway ... 899
show modem ... 899
show nemo ... 900
show network ... 900
show ntp ... 900
show openvpn client ... 900
show openvpn server ... 901
show route ... 901
show serial ... 901
show scripts ... 901
show surelink interface ... 902
show surelink ipsec ... 902
show surelink openvpn ... 902
show system ... 902
show usb ... 903
show version ... 903
show vrrp ... 903
show web-filter ... 903
show wifi ap ... 903
show wifi client ... 904
show wifi-scanner ... 904
show wifi-scanner blocklist ... 904
show wifi-scanner candidates ... 905
show wifi-scanner log ... 905
speedtest ... 905
ssh ... 905
system backup ... 906
system disable-cryptography ... 906
system duplicate-firmware ... 906
system factory-erase ... 906
system find-me ... 907
system firmware ota check ... 907
system firmware ota list ... 907
system firmware ota update ... 907
system firmware update ... 908
system power ignition off_delay ... 908
system restore ... 908
system script start ... 908
system script stop ... 908
system serial clear ... 909
system serial save ... 909
system serial show ... 909
system serial start ... 909
system serial stop ... 910
system support-report ... 910
system time set ... 910
system time sync ... 910
system time test ... 910
telnet ... 911
traceroute ... 911

Safety warnings

English 914
Bulgarian--български 915
Croatian--Hrvatski 916
French--Français 917
Greek--Ελληνικά 918
Hungarian--Magyar 919
Italian--Italiano 920
Latvian--Latvietis 921
Lithuanian--Lietuvis 922
Polish--Polskie 923
Portuguese--Português 924
Slovak--Slovák 925
Slovenian--Esloveno 926
Spanish--Español 927

Digi Connect EZ regulatory and safety statements

RF exposure statement 928
Federal Communication (FCC) Part 15 Class A 928
European Community - CE Mark Declaration of Conformity (DoC) 928
CE and UKCA OEM labeling requirements 928
    CE labeling requirements 928
    UK Conformity Assessed (UKCA) labeling requirements 929
Innovation, Science, and Economic Development Canada (IC) certifications 930
RoHS compliance statement 930
Cautionary statements for Connect EZ 930
    Residential environment warnings 930
    Safety statements for Connect EZ 4i only 931
Special safety notes for wireless routers 931
Product disposal instructions 932

Digi Connect EZ 4/4i 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.

Get started with Connect EZ 4/4i

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

Connect EZ 4i ONLY: Review installation instructions for hazardous locations

Step 1: Verify product components

Step 2: Connect the power supply

Step 3: Connect to site network using an Ethernet LAN

Step 4: Connect the device to the network using Wi-Fi

Step 5: Discover the IP address using the Digi Navigator

Step 6: Configure RealPort from the Digi Navigator

Step 7: Connect to the web UI and update the Connect EZ firmware

Step 8: Connect to Digi Remote Manager

Optional

- Change the password on the Connect EZ
- Mount the Connect EZ device
- Connect equipment to the Connect EZ serial port
- Cellular connection: Insert the CORE module

Administrators only

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

Connect EZ 4i ONLY: Review installation instructions for hazardous locations

This information is intended for these Connect EZ 4i models:

- Ethernet Gateway: Model 50002072-03 and 50002072-06

Before you begin installing your Connect EZ 4i device, please review these installation instructions for hazardous locations.

- This equipment is suitable for use in Class I, Division 2, Groups A, B, C, D OR non-hazardous locations only.
- All external or field wiring must be in accordance to NFPA 70 Article 501.10(B).
- The unit is intended for fixed installations.
- This equipment is considered open type, only accessible by the use of a tool.
- Antenna connections provide non-incendive energy levels for use in Class I, Division 2, Groups A, B, C and D, Hazardous Locations. Install in accordance with Control Document No. 90002470-88 A.

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: Connect the Wi-Fi antenna.

Included equipment for Connect EZ 4/4i

Equipment	Description
Connect EZ 4 **Connect EZ 4i**	For detailed information about the panels, see: ■ Front panel and LEDs ■ Back panel ■ Bottom panel **Note** Connect EZ 4i only: An industrial power connector is attached to the power jack. (Part number 18000724)
Power supply (Connect EZ 4)	Connect EZ 4 is intended to be powered by a locking barrel output transformer rated 100-240 VAC to 12 VDC, and with a 3 A output. Use the included power supply (part number 24000136). For information about connecting the power supply, see Step 2: Connect the power supply.
Power supply	Connect EZ 4i is intended to be powered by a certified extended temperature power supply pigtail DC cable with output rated at 100-240 VAC to 12 VDC 3 A, -40 C to +74

Equipment	Description
(Connect EZ 4i)	C. Use the included power supply (part number 24000141). For information about connecting the power supply, see Step 2: Connect the power supply.
Ethernet cable	CAT 6 Ethernet cable. Connect to a site network using an Ethernet cable. See Step 3: Connect to site network using an Ethernet LAN.
Wi-Fi antenna	One Wi-Fi antenna is included. ■ 2.4 & 5 GHz ■ 5dBi dipole ■ Digi PN 29000938 See Connect the Wi-Fi antenna.
DIN rail clip	The DIN rail clip connects to the back of the device and is used to mount the device onto a DIN rail. Screws are included. See Attach to DIN rail with clip. The kit includes a DIN rail clip and two screws that meet these requirements: ■ M4 in diameter ■ 5 mm in length ■ Countersunk ■ Phillips #2 ■ Black Steel
Global plug kit (Connect EZ 4)	If you purchased the GLB version of the device, a kit that includes global outlet plugs is included. Use the included kit (part number 18000291).
Global plug kit (Connect EZ 4i)	If you purchased the GLB version of the device, a kit that includes global outlet plugs is included. Use the included kit (part number 18000726).
Loose label	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 Loose label sample. **Note** 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.

Optional additional cellular equipment

These items are required only if you are using a CORE module to connect to a cellular network.

Equipment	Description
CORE module	 **Note** A SIM card is also required.
SIM card	An activated SIM card provided by your cellular network operator. You can insert up to two SIM cards in the CORE module. See Connect hardware and connect to a cellular network. The CORE module supports the standard mini-SIM cards (2FF).
LTE Antenna (2)	Two LTE antennas are included. ■ For connection instructions, see Cellular connection: Insert the CORE module. ■ Digi PN 76002118

Step 2: Connect the power supply

The power supply is included with the device.

- **Connect EZ 4**: Connect EZ 4 is intended to be powered by a locking barrel output transformer rated 100-240 VAC to 12 VDC, and with a 3 A output.
- **Connect EZ 4i**: Connect EZ 4i is intended to be powered by a certified extended temperature power supply pigtail DC cable with output rated at 100-240 VAC to 12 VDC 3 A, -40 C to +74 C.

For more information about the power supplies, see Step 1: Verify product components.

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 web interface.

NEXT STEP: If you are performing the initial device set-up, proceed to the next step: Step 4: Connect the device to the network using Wi-Fi.

Step 4: Connect the device to the network using Wi-Fi

You can use a Wi-Fi connection to connect the Connect EZ to your network. This enables you to access the device's web UI and configure it.

NEXT STEP: If you are performing the initial device set-up, after you have configure Wi-Fi you can proceed to the next step: Step 5: Discover the IP address using the Digi Navigator.

Connect the Wi-Fi antenna

This section explains how to connect the Wi-Fi antenna to the Connect EZ hardware.

1. Orient the device so the top panel faces you.
2. Attach the included Wi-Fi antenna to the device. While gripping the metal connector section with your thumb and forefinger, tighten until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.

NEXT STEP: Continue with the process: Enable Wi-Fi.

Enable Wi-Fi

For more detailed information, see Configure the Wi-Fi radio's channel.

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** > **WiFi**.
4. Click **Enable** to enable Wi-Fi.
5. Click **Apply** to save the configuration and apply the change.

NEXT STEP: Continue with the process: Configure Wi-Fi on the device.

Configure Wi-Fi on the device

You can configure a device to be a Wi-Fi client or a Wi-Fi access point.

Note For more detailed information about Wi-Fi configuration, see Wi-Fi.

Client

You can configure the device as a client that can connect to a Wi-Fi access point.

- Configure a Wi-Fi client and add client networks

Access point

You can configure the device to be a Wi-Fi access point.

- Configure an open Wi-Fi access point
- Configure a Wi-Fi access point with personal security
- Configure a Wi-Fi access point with enterprise security

NEXT STEP: If you are performing the initial device set-up, proceed to the next step: Step 5: Discover the IP address using the Digi Navigator.

Step 5: Discover the IP address using the Digi Navigator

You can use the Digi Navigator to quickly discover the IP address for the Connect EZ.

Make sure you have the device powered and connected the device to your network or computer with an Ethernet cable. See Connect to and access the Digi Navigator.

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. Download and install the **Digi Navigator**.
2. Launch the **Digi Navigator**.
3. 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 Discover the IP address 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 Discover the IP address when not on a network.
4. 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 6: Configure RealPort from the Digi Navigator.

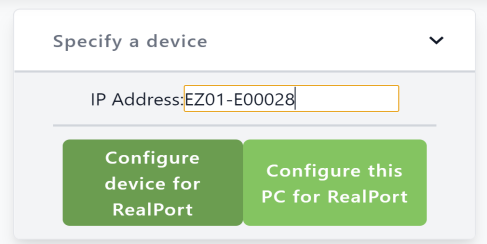
Step 6: Configure RealPort from the Digi Navigator

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.

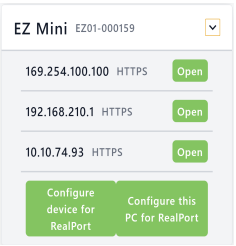
In this step, all serial ports on the device are set to RealPort mode and the RealPort service is enabled. The COM ports on your laptop are also configured.

Note You can also configure the device to accept a Realport connection from the web UI on the device. See Configure RealPort mode.

1. Make sure theConnect EZ is powered on and connected to your network or computer.
2. Download and install the **Digi Navigator**.
3. Launch the **Digi Navigator**.
4. Select the device you want to configure using one of the following methods:
   - **Specify a device**: Expand the **Specify a device** section and enter the IP address or host name for the device.



   - **Select a device**: From the list of devices shown in the **Digi Navigator**, expand the device that you want to configure.



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.



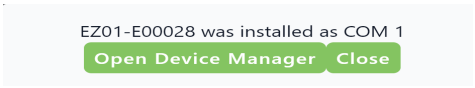
   e. Click **Close** to close the message.
6. Configure RealPort on your computer.

a. Click **Configure this PC for RealPort**.

b. From the **Select starting COM** list box, select the first COM port that should be configured for RealPort. 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:

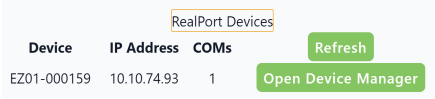
- **Close**: Click **Close** to close the message. Configuration is complete.
- **Open Device Manager**: Click **Open Device Maanger** if you want to do further configuration to the COM ports. The Windows **Properties** dialog displays.

7. If desired, you can verify the RealPort configuration. See Configure the serial port for RealPort mode and Configure the RealPort service.

8. 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**.

a. Launch the **Digi Navigator** if it is not currently open. A list of Connect EZ devices that have RealPort enabled and configured displays in the RealPort Devices section at the bottom of the application screen.

b. Click **Open Device Manager** to open the Windows **Properties** dialog for the COM ports on your computer that are configured for RealPort. For more information, see Manage the RealPort device list.



NEXT STEP: If you are performing the initial device set-up, proceed to the next step: Step 7: Connect to the web UI and update the Connect EZ firmware.

Step 7: 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.

Step 1: Connect to the local Web UI on the Connect EZ

Step 2: Update the firmware on the Connect EZ

NEXT STEP: If you are performing the initial device set-up, proceed to the next step: Step 8: Connect to Digi Remote Manager.

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 **ETH 1** 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
Network activity	Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices.
Digi Remote Manager	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 Using Digi Remote Manager.
Device	Displays the Connect EZ device's status, statistics, and identifying information.
Network Interfaces	Displays the status of the network interfaces configured on the device.

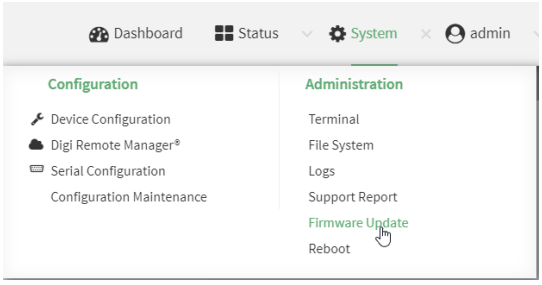
For more information, see Using the web interface.

NEXT STEP: Proceed to the next step: Update the firmware on the Connect EZ.

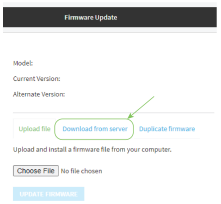
Update the firmware on the Connect EZ

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

1. Log into the Connect EZ Web UI as a user with Admin access.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Download from server**.



4. For **Version:**, select the appropriate version of the device firmware.
5. Click **Update Firmware**.

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 8: Connect to Digi Remote Manager.

Step 8: Connect to Digi Remote Manager

Make user to connect your device to Digi Remote Manager to ensure that you receive automatic notification of firmware updates and security notices. From Remoter 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.
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 4/4i for information on optional steps.

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.

You must use a cable with an RJ50 connector to connect to the Connect EZ with an RJ50 connector. 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.

Serial Status page

The **Serial Status** page contains status information about all of the serial ports available on the device. To get to this page, choose **Status** > **Connections** > **Serial**.

See Serial Status page for more information.

Serial connector pinout

The Connect EZ 4/4i has an RJ50 serial connector. The table below contains the pinout information.

RJ50 pin	EIA-232	EIA-422/485 Full-duplex	EIA-485 Half-duplex
1	RI	TxD-	TxD-
2	DSR	RxD-	RxD-
3	RTS	RTS+	N/A
4	GND	GND	GND
5	TxD	TxD+	TxD+
6	RxD	RxD+	RxD+
7	SG	SG	SG

RJ50 pin	EIA-232	EIA-422/485 Full-duplex	EIA-485 Half-duplex
8	CTS	CTS+	N/A
9	DTR	RTS-	N/A
10	DCD	CTS-	N/A

Serial Status page

The **Serial Status** page contains status information about all of the serial ports available on the device.

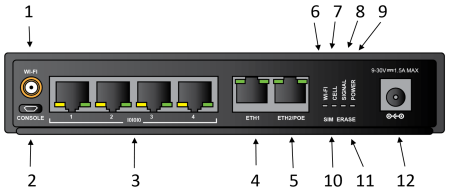
To get to this page, choose **Status** > **Connections** > **Serial**.

Item	Description
configuration icon	Click the (configuration) icon in the upper right corner of the page to access the **Serial Configuration** page. See Serial port for more information.
Status	Displays the connection status. ■ CONNECTED: A terminal, SSH, TCP, or telnet session is active. ■ NO SIGNAL: CTS or DCD is not active on the port.
Port	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. 1. Click the link to connect to the port in the terminal page. 2. In the terminal screen, enter **~b?** to display additional commands. See Access the terminal screen from the web UI for more information about the commands. While you are connected to the terminal, the port status displays in the **Status** column as CONNECTED, and the name of the user logged into the device displays in the **User** column.
Label	A description for the port. You can change this from the **Serial Configuration** 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 Port (above) for more information.
Log	Click the **Log** button to open the **Serial Port Log** page for that port. See Log serial port messages for more information about the page.
User	When the port is connected to a terminal, SSH, TCP, or Telnet connection the name of the user logged into the device displays.

Item	Description
	See the description for Port (above) for more information.
TX/RX Bytes	Displays the total number of bytes that have been transmitted and received.
Signals	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

Hardware

Front panel and LEDs



Item	Name	Description
1	Wi-Fi	Connect a Wi-Fi antenna to the device. For connection instructions, see Connect the Wi-Fi antenna.
2	Console	Use the USB console port to access the web UI on the device if a network is not available. For example, you can use a micro USB cable to connect the device to your laptop and then find the IP address for the device. See Discover the IP address using a Micro USB cable.
3	Serial ports 1-4	Use the serial ports to connect to devices and equipment to the Connect EZ. See Connect equipment to the Connect EZ serial port. The serial port LED shows the status of the connection. ■ **Yellow** (left): The port is in use. The LED may be solid or blink, depending on the traffic speed. ■ **Green** (right): A device is connected to the port.
4	ETH1	Use the ETH1 port to connect the device to your local network, using an Ethernet cable. The ETH1 LED shows the status of the connection. ■ **Yellow** (left): There is activity on the port. ■ **Green** (right): The port is in use.

Item	Name	Description
5	ETH2	Use the ETH 2 port to connect to a second Ethernet port. This is useful for redundancy or if you have more than one network. The ETH2 LED shows the status of the connection. ■ **Yellow** (left): There is activity on the port. ■ **Green** (right): The port is in use.
6	Wi-Fi LED	Shows the status of the Wi-Fi connection. For more information, see Wi-Fi LED descriptions for more information.
7	Cell LED	Shows the status of the cell service connection. The Cell and Signal LEDs work together to display some status information. See Cell service and signal LED descriptions.
8	Signal LED	Shows the strength of the cellular signal. The Cell and Signal LEDs work together to display some status information. See Cell service and signal LED descriptions.
9	Power LED	The Power LED shows the status of the power supply connection. ■ **Solid green**: The power source is connected and power is being supplied to the device. ■ **Flashing green**: The Find Me feature has been activated.
10	SIM button	The SIM button is used to manually toggle between the two SIM slots included in the DIGI Core Module. **Note** This feature is useful only if you have connected the Digi CORE module. See Cellular connection: Insert the CORE module.
11	Erase button	Use this button to reset the device to factory defaults.
12	Power	Connect the power supply. See Connect the power supply.

Wi-Fi LED descriptions

Wi-Fi LED	Description
Off	Both the access point and Wi-Fi client are unconfigured.

Wi-Fi LED	Description
Solid green	Client is connected. (No access point.)
Flash green	Client is searching for connection. (No Access P0int.)
Solid amber	Client is unconfigured. Access point is up.
Solid blue	Client is connected. Access point is up.
Flashing amber/green	Client is searching. Access point is up.
Solid red	An error has occurred.

Cell service and signal LED descriptions

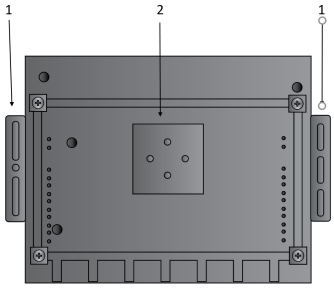
Cell LED	Signal LED	Description
Slow flash red	Slow flash red	Updating modem firmware
Slow flash green	Slow flash green	Recovering modem firmware
Slow flash green	Off	Waiting for modem to appear
Off	Off	Modem not present
Fast flash red	Off	SIM not present
Off	Solid blue	Modem signal strength: 5 bars
Off	Solid green	Modem signal strength: 4 bars
Off	Solid amber	Modem signal strength: 3 bars
Off	Solid red	Modem signal strength: 2 bars
Off	Slow flash red	Modem signal strength: 1 bars
Off	Fast flash red	Modem signal strength: 0 bars
Off	Off	Modem signal strength: *
Solid amber	Off	Cell service: 2G
Solid green	Off	Cell service: 3G
Solid blue	Off	Cell service: 4G
Off	Off	Cell service: None

Back panel



Name	Description
Digi Core Modem	Insert a Digi Core Modem to complete a cellular connection. See Connect hardware and connect to a cellular network.
WWAN-1	Antennas can be attached if the module is used to complete a cellular connection. See Connect hardware and connect to a cellular network.
WWAN-2	Antennas can be attached if the module is used to complete a cellular connection. See Connect hardware and connect to a cellular network.

Bottom panel



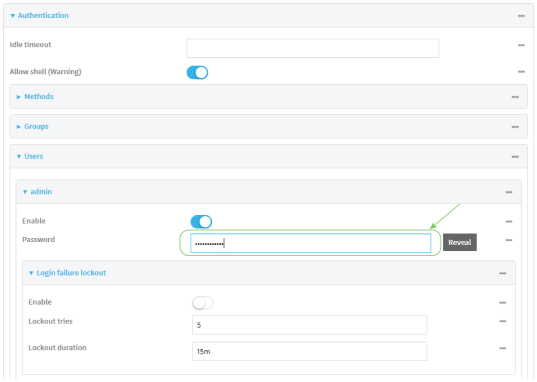
Item	Name	Description
1	Mounting tabs	The mounting tabs on the device are used to mount the device onto a mounting surface. Use round-head M4 size screws. The type and length are dependent on the mounting surface type. Screws are not provided. If you choose not to mount the device, you can permanently remove the mounting tabs with a pliers.
2	DIN rail clip	You can attach a DIN rail clip to the back 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.

Cellular connection: Insert the CORE module

This section explains how to connect the Digi CORE® module and cellular antennas to the Connect EZ hardware.

Prerequisites

- Activated SIM card from your cellular network provider.
- Digi CORE module. This may be included with your device. If it is not, you must purchase one separately.

To connect the hardware and connect to the cellular network:

1. Insert your activated SIM card into the CORE module. The notched end of SIM card should be inserted first, with the gold metal contacts facing down. You will hear a click once the SIM is completely inserted.

   Note If one SIM card is being used, insert the SIM card into the SIM 1 slot.

2. Insert the CORE module into the device.
   a. Orient the device so the front of the device is facing you.
   b. Unscrew the CORE module slot cover from the back of the device.
   c. Insert the CORE module into the slot. Make sure the pin holes on the back of the module match the location of the pins in the slot.
   d. Push the module into the slot.
   e. Push the white handle down until you hear it click.
   f. Optionally, you can screw one of the CORE module cover screws into the center of the handle.
   g. Place the white CORE module cover over the end of the device. Make sure that the antenna labels are oriented correctly.
   h. Push the cover in place.
3. Attach both of the included cellular antennas. While gripping the metal connector section with your thumb and forefinger, tighten until secure. Do not tighten the antenna by holding any part of the plastic antenna housing.

NEXT STEP: After you have connected the hardware, proceed to the next step: Connect hardware and connect to a cellular network.

Connect hardware and connect to a cellular network

This section explains how to connect the Connect EZ hardware and then connect to a cellular network, using a CORE module. You must have purchased a CORE module to be able to connect to the cellular network.

Note As an alternative, you can also use an Ethernet LAN connection. See Connect to site network using an Ethernet LAN.

To connect the hardware and connect to the cellular network:

1. Insert a CORE module with an activated SIM card. See Cellular connection: Insert the CORE module.
2. Plug the power supply cord into at least one of the power supplies on the back of the device. The second power cord can also be plugged in, but it is not required. It is available for power redundancy.
3. Plug the power supply unit into an AC power outlet to power up the Connect EZ.

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

Use screws to attach the device to a surface using the two mounting tabs on the device. The type and length of screw used 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
- 14 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
- 14 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 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.

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 front 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 device's IP address: Additional methods

The IP address is used to login 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

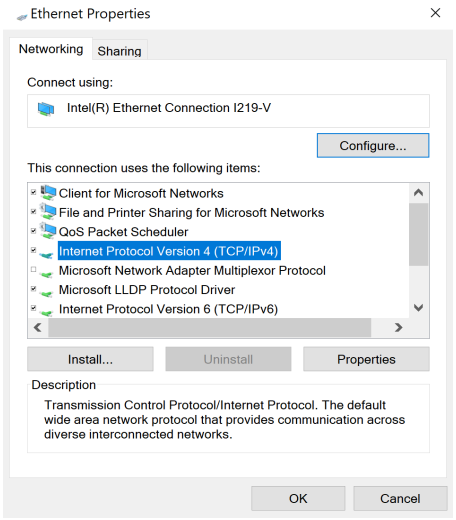
You can manually assign an IP address to the device.

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:

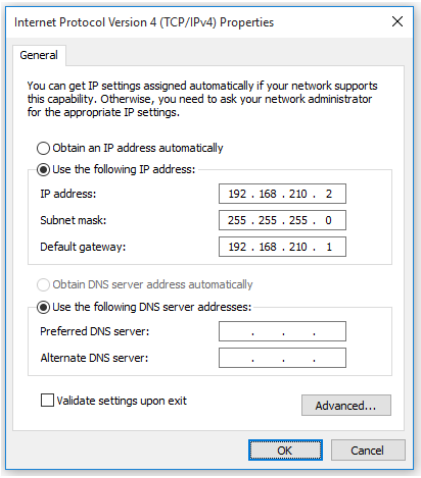
1. On your PC, navigate to the Ethernet network settings dialog.
2. Click the **Internet Protocol Version 4 (TCP/IPv4)** parameter.



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: 192.168.201.1
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**.

Loose label sample

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.



	Item	Description
1	QR code	Scan the QR code to display a semicolon separated list of: ProductName;DeviceID;Password;SerialNumber;SKUPartNumber SKUPartRevision **Note** Note the space between SKUPartNumber and SKUPartRevision Example: Connect EZ 02;00000000-00000000-112233FF-FF445566;PW1234567890;EZ02-123456;EZ02-C000 B
2	Label part number	Label part number and revision level.
3	Product name	Product name, such as Connect EZ Mini, Connect EZ 2, or Connect EZ 4i.
4	Device part number (SKU) and revision	Device part number (SKU number) and revision. For example, EZ02-C000 A
5	Password	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	MAC address	The MAC address for the device.
7	Serial number	The unique serial number assigned to the device. The SN is needed when submitting a Digi support ticket.
8	Device kit part number and revision level	The part number and revision level of the device kit.

Configuration and management

This chapter contains the following topics:

Review Connect EZ default settings 43
Change the default password for the admin user 44
Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point 45
Configuration methods 47
Using Digi Remote Manager 49
Access Digi Remote Manager 49
Using the web interface 49
Use the local REST API to configure the Connect EZ device 50
Access the terminal screen from the web UI 54
Using the command line 55
Access the command line interface 55
Log in to the command line interface 55
Exit the command line interface 56

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
Wide Area Networks (WANs)	■ Modem	■ WWAN1 cellular modem	■ Firewall zone: External ■ WAN priority: Metric=3 ■ SIM failover after 5 attempts
Ethernet Network	■ ETH1	■ Ethernet: ETH1	■ Firewall zone: Edge ■ DHCP client enabled
	■ ETH2	■ Ethernet: ETH2	■ Firewall zone: Edge ■ DHCP client enabled
	■ Loopback	■ Ethernet: Loopback	■ Firewall zone: Loopback ■ IP address: 127.0.0.1/8
	■ Default IP	■ Ethernet: ETH1	■ Firewall zone: Setup ■ IP address 192.168.210.1/24
	■ Default Link-local IP	■ Ethernet: ETH1	■ Firewall zone: Setup ■ IP address 169.254.100.100/16

Other default configuration settings

Feature	Configuration
Central management	■ Digi Remote Manager enabled as the central management service.
Security policies	■ Packet filtering allows all outbound traffic. ■ SSH and web administration: • Enabled for local administration • Firewall zone: Set up
Monitoring	■ Device heath metrics uploaded to Digi Remote Manager at 60 minute interval. ■ SNMP: Disabled

Change the default password for the admin user

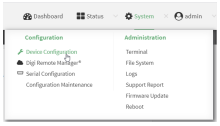
The unique, factory-assigned password for the default **admin** user account is printed on the bottom label of the device and on the loose label included in the package.

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.

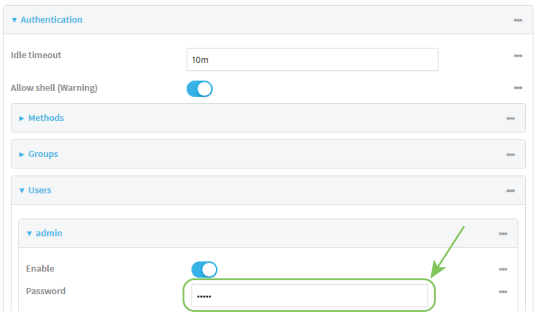
To change the default password for the admin user:

WebUI

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 **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. 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. 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.

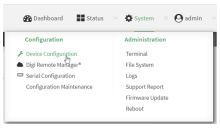
Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point

By default, the SSID and pre-shared key for the preconfigured Wi-Fi access point are:

- Enabled
- SSID: Digi-Connect EZ-*serial_number*
- Encryption: WAP2 Personal (PSK)
- Pre-shared key: The unique password printed on the bottom label of the device.

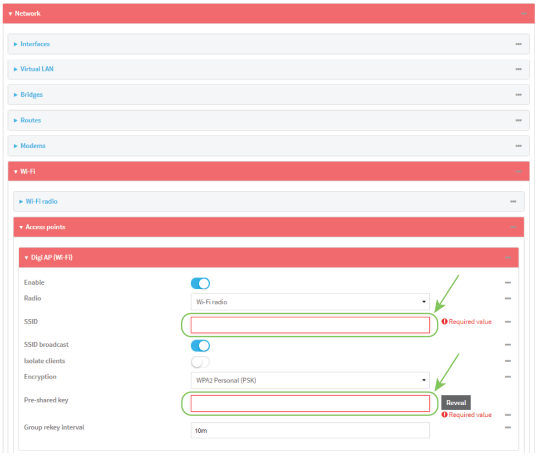
WebUI

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**.

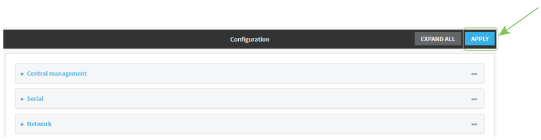


The **Configuration** window is displayed.

3. Click **Network** > **Wi-Fi** > **Digi AP**.



4. Enter a new **SSID** and **Pre-shared key**.
5. 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. Set a new SSID for the **digi_ap** access point:

```
(config)> network wifi ap digi_ap ssid new_ssid
(config)>
```

4. Set a new pre-shared key:

```
(config)> network wifi ap digi_ap encryption key_psk2 new_key
(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.

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 profile which can be applied to other similar devices. See Using Digi Remote Manager for more information about using the Remote Manager to manage and configure your Connect EZ device.
  - The local web interface. See Using the 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:

WebUI

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. No configuration changes are required to begin using the 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.

   Check your email for Digi Remote Manager login instructions.
2. Go to remotemanager.digi.com.
1. Enter your username and password.

   The Digi Remote Manager Dashboard appears.

Using the web interface

To connect to the Connect EZ local WebUI:

1. Use an Ethernet cable to connect the Connect EZ's **ETH2** 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.

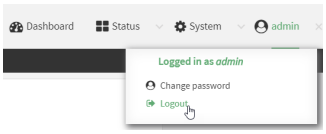
After logging in, the local web admin dashboard is displayed.

The dashboard shows the current state of the device.

Dashboard area	Description
Network activity	Summarizes network statistics: the total number of bytes sent and received over all configured bridges and Ethernet devices.
Digi Remote Manager	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 Using Digi Remote Manager.
Device	Displays the Connect EZ device's status, statistics, and identifying information.
Network Interfaces	Displays the status of the network interfaces configured on the device.
Modems	Provides information about the signal strength and technology of the cellular modem(s).

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:

  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. 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.

4. 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", "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/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 .
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 several physical communications interfaces. These interfaces can be bridged in a Local Area Network (LAN) or assigned to a Wide Area Network (WAN).

This chapter contains the following topics:

Wide Area Networks (WANs) 58
Local Area Networks (LANs) 127
Bridging 167
Show Surelink status and statistics 171

Wide Area Networks (WANs)

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

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

This section contains the following topics:

Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs) 59
Configure WAN/WWAN priority and default route metrics 59
WAN/WWAN failover 61
Configure SureLink active recovery to detect WAN/WWAN failures 62
Configure the device to reboot when a failure is detected 72
Disable SureLink 80
Example: Use a ping test for WAN failover from Ethernet to cellular 83
Using Ethernet devices in a WAN 86
Using cellular modems in a Wireless WAN (WWAN) 86
Configure a Wide Area Network (WAN) 105
Configure a Wireless Wide Area Network (WWAN) 113
Show WAN and WWAN status and statistics 123
Delete a WAN or WWAN 125
Default outbound WAN/WWAN ports 126

Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs)

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 or a cellular modem.
- Several networking parameters for the WAN, such as firewall configuration and IPv4 and IPv6 support.
- Several parameters controlling failover.

Configure WAN/WWAN priority and default route metrics

The Connect EZ device is preconfigured with one Wide Area Network (WAN), named **ETH1**, and one Wireless Wide Area Network (WWAN), named **Modem**. 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 therefor the highest priority WAN. By default, the Wireless WAN (**Modem**) is configured with a metric of **3**, which means it has 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.

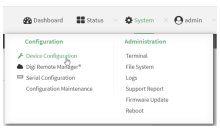
Example: Configure cellular connection as the primary WAN, and the Ethernet connection as backup

Required configuration items

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

WebUI

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. 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. 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. 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.

WAN/WWAN failover

If a connection to a WAN interface is lost for any reason, the Connect EZ device will immediately fail over to the next WAN or WWAN interface, based on WAN priority. See Configure WAN/WWAN priority and default route metrics for more information about WAN priority.

Active vs. passive failure detection

There are two ways to detect WAN or WWAN failure: active detection and passive detection.

- Active detection uses Digi SureLink™ technology to send probe tests to a target host or to test the status of the interface. The WAN/WWAN is considered to be down if there are no responses for a configured amount of time. See Configure SureLink active recovery to detect WAN/WWAN failures for more information about active failure detection.
- Passive detection involves detecting the WAN going down by monitoring its link status by some means other than active detection. For example, if an Ethernet cable is disconnected or the state of a cellular interface changes from **on** to **off**, the WAN is down.

Default Digi SureLink configuration

Beginning with firmware version 20.2.*x*, Surelink is enabled by default for IPv4 on all WAN and WWAN interfaces, and is configured to perform two tests on these interfaces:

- Interface connectivity.
- DNS query to the DNS servers for interface's the network connection.

  DNS servers are typically received as part of the interface's DHCP client connection, although you can manually configure the DNS servers that will be used by SureLink.

  Note If your device is operating on a private APN or on wired network with firewall restrictions, ensure that the DNS servers on your private network allow DNS lookups for my.devicecloud.com; otherwise, the SureLink DNS query test will fail and the Connect EZ device will determine that the interface is down.

By default, these tests will be performed every 15 minutes, with a response timeout of 15 seconds. If the tests fail three consecutive times, the device will reset the network interface to attempt to recover the connection.

Configure SureLink active recovery to detect WAN/WWAN failures

Problems can occur beyond the immediate WAN/WWAN 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

- Enable SureLink.

  SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**ETH1**) and WWAN (**Modem**). It is disabled for IPv6.

  When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.
- The type of probe test to be performed, one of:
  - Test another interface's status: Used to create a failover or coupled relationship between two interfaces. Requires the name of the alternate interface, the IP version to be tested, and the expected status of the alternate interface (either up or down).
  - Ping: Requires the hostname or IP address of the host to be pinged.
  - DNS query: You can perform a DNS query to a named DNS server, or to the DNS servers configured for the WAN.
  - HTTP test: Requires the URL of the host to be tested.
  - Test DNS servers configured for this interface: Tests communication with this interface's DNS servers that are either provided by DHCP, or statically configured.
  - Interface status: Determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

  The preconfigured WAN is configured by default to use SureLink to both test the interface status and perform a test DNS query.

Additional configuration items

- The behavior of the Connect EZ device upon test failure:
  - The default behavior, which is to restart the interface and fail over to the next priority WAN/WWAN.
  - For WWANs, SIM switching (also enabled by default).
  - For WWANs, reset the modem.
  - Reboot the device.
- The interval between connectivity tests.
- The number of probe attempts before the WAN is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

- If the type of probe test is:
  - Ping: Configure the number of bytes in the ping packet.
  - Interface status: Configure the amount of time that the interface is down before it is considered to have failed, and the amount of time it takes to make an initial connection before it is considered down.
- Additional test targets.
- 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.

Order of precedence for SureLink actions

If multiple SureLink actions, such as restarting the interface and rebooting the device, are enabled, the following order of precedence is used:

1. Restart interface
2. Switch to the alternate SIM (for WWANs)
3. Reset the modem (for WWANs)
4. Reboot the device

For example, if SureLink is configured as follows:

- **Restart interface**:
  - **Enabled**
  - **Restart fail count**: **2**
- **Reset modem**:
  - **Enabled**
  - **Reset mode fail count**: **3**
- **Switch SIM**:
  - **Enabled**
  - **Switch SIM fail count**: **5**
- **Reboot device**:
  - **Enabled**
  - **Reboot fail count**: **7**

SureLink will: The device will:

1. First SureLink failure: Nothing will happen.
2. Second SureLink failure: The interface will restart.
3. Third SureLink failure: The modem will reset.
4. Fourth SureLink failure: The interface will restart again.
5. Fifth SureLink failure: The device will switch to the alternate SIM.

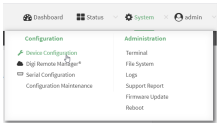
> **Note** The **Switch SIM** behavior only applies if the modem is connected, but SureLink tests are failing. If the modem is not connected, **SIM failover** applies. See Configure a Wireless Wide Area Network (WWAN) for more information about the **SIM failover** option.

6. Sixth SureLink failure: The interface will restart again.
7. Seventh Surelink failure: The device will reboot.

WebUI

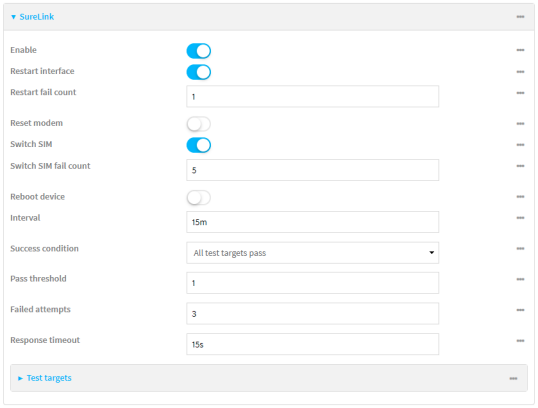
SureLink can be configured for both IPv4 and IPv6.

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. Create a new WAN or WWAN or select an existing one:
   - To create a new WAN or WWAN, see Configure a Wide Area Network (WAN) or Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WAN or WWAN, click to expand the appropriate WAN or WWAN.
5. After creating or selecting the WAN or WWAN, click **IPv4** (or **IPv6**) > **SureLink**.



6. **Enable** SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**ETH1**) and WWAN (**Modem**). It is disabled for IPv6.

   When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.

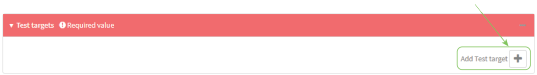
7. **Restart interface** is enabled by default.
   - (Optional) For **Restart fail count**, type or select the number of times that the Surelink test must fail before the interface is restarted. The default is **1**.

8. (Optional) If the interface is a WWAN, enable **Reset modem**.
   - (Optional) For **Reset modem fail count**, type or select the number of times that the Surelink test must fail before the modem is reset. The default is **1**.
9. If the interface is a WWAN, **Switch SIM** is enabled by default. Click to disable.
   - If **Switch SIM** is enabled, for **Switch SIM fail count**, type or select the number of times that the Surelink test must fail before the modem switches to the alternate SIM. The default is **5**.

Note The SureLink **Switch SIM** option differs from the **SIM failover** option, which is set during WWAN configuration. **SIM failover** applies when the modem is unable to connect to a cellular network, whereas **Switch SIM** applies when the WWAN interface is failing SureLink tests even though the modem is connected. See Configure a Wireless Wide Area Network (WWAN) for more information about the **SIM failover** option.

10. (Optional) Enable **Reboot device**.

    If **Reboot device** is enabled at the same time as either **Restart interface** or **Reset modem**, **Reboot device** takes precedence.
    - For **Reboot fail count**, type or select the number of times that the Surelink test must fail before the device is rebooted. The default is **1**.
11. Click to expand **Test targets**.
12. For **Add Test Target**, click ✚.



13. Select the **Test type**:
    - **Test another interface's status**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces. If **Test another interface's status** is selected:
      - For **Test Interface**, select the alternate interface to be tested.
      - For **IP version**, select the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.
      - For **Expected status**, select whether the expected status of the alternate interface is **Up** or **Down**. For example, if **Expected status** is set to **Down**, but the alternate interface is determined to be up, then this test will fail.
    - **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
    - **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
    - **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
    - **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.

- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

    The default is 60 seconds.
  - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

    The default is 60 seconds.

14. Optional active recovery configuration parameters:
    a. Change the **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.

    b. If more than one test target is configured, for **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.

    c. 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.

    d. For **Failed attempts**, type the number of probe attempts before the WAN is considered to have failed.

    e. For **Response timeout**, type the amount of time that the device should wait for a response to a probe 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.

15. (Optional) Repeat this procedure for IPv6.
16. 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. 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 WWAN, or edit an existing one:
   - To create a new WAN or WWAN, see Configure a Wide Area Network (WAN) or Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing WAN or WWAN, change to the WAN or WWAN's node in the configuration schema. For example, for a WAN or WWAN 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 (eth1) and WWAN (modemwwan2). It is disabled for IPv6.

   When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.

   ```
   (config network interface my_wan> ipv4 surelink enable true
   (config network interface my_wan)>
   ```
5. By default, the device is configured to restart the interface when its connection is considered to have failed.

   To disable:

   ```
   (config network interface my_wan ipv4 surelink)> restart false
   (config network interface my_wan ipv4 surelink>
   ```
   - (Optional) Set the number of times that the Surelink test must fail before the interface is restarted:

     ```
     (config network interface my_wan ipv4 surelink)> restart_attempts
     int
     (config network interface my_wan ipv4 surelink>
     ```

     where *int* is any number greater than **0**. The default is **1**.
6. (Optional) If the interface is a WWAN, set the device to reset the modem:

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

- If **reset_modem** is enabled, set the number of times that Surelink tests must fail prior to resetting the modem:

```
(config network interface my_wan ipv4 surelink)> reset_modem_
attempts int
(config network interface my_wan ipv4 surelink>
```

  where *int* is an integer between **1** through **5**. The default is **1**.

7. If the interface is a WWAN, SIM switching is enabled by default. To disable:

```
(config network interface my_wan ipv4 surelink)> switch_sim false
(config network interface my_wan ipv4 surelink>
```

Note The SureLink **switch_sim** option differs from the **sim_failover** option, which is set during WWAN configuration. **sim_failover** applies when the modem is unable to connect to a cellular network, whereas **switch_sim** applies when the WWAN interface is failing SureLink tests even though the modem is connected. See Configure a Wireless Wide Area Network (WWAN) for more information about the **sim_failover** option.

- If **switch_sim** is enabled, set the number of times that Surelink tests must fail prior to switching SIMS:

```
(config network interface my_wan ipv4 surelink)> switch_sim_attempts
int
(config network interface my_wan ipv4 surelink>
```

  where *int* is an integer between **1** through **5**. The default is **5**.

8. (Optional) 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 the reboot parameter is enabled at the same time as either the **restart** or **reset_modem** parameters, the **reboot** parameter takes precedence.

- (Optional) Set the number of times that the Surelink test must fail before the device is rebooted:

```
(config network interface my_wan ipv4 surelink)> reboot_attempts int
(config network interface my_wan ipv4 surelink>
```

  where *int* is any number greater than **0**. The default is **1**.

9. Add a test target:

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

10. 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 **interface_down_time** to ten minutes, enter either **10m** or **600s**:

    ```
    (config network interface my_wan ipv4 surelink target 0)>
    interface_down_time 600s
    (config network interface my_wan ipv4 surelink target 0)>
    ```

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 **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wan ipv4 surelink target 0)>
interface_timeout 600s
(config network interface my_wan ipv4 surelink target 0)>
```

The default is 60 seconds.

- **other**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces:

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

If **other** is set:

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

```
(config network interface my_wan ipv4 surelink target
0)> other_interface /network/interface/eth1
(config network interface my_wan ipv4 surelink target
0)>
```

  - Set the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.

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

where *value* is one of: **any**, **both**, **ipv4**, or **ipv6**.

  - Set the expected status of the alternate interface:

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

where *value* is either **up** or **down**. For example, if **other_status** is set to **down**, but the alternate interface is determined to be up, then this test will fail.

(Optional) Repeat to add additional test targets.

11. Optional active recovery configuration parameters:
    a. 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>
```

    b. 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.

    c. 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**.

    d. 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**.

    e. 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 **timeout** to ten minutes, enter either **10m** or **600s**:

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

    The default is 15 seconds.

12. (Optional) Repeat this procedure for IPv6.

13. Save the configuration and apply the change:

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

  SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**ETH1**) and WWAN (**Modem**). It is disabled for IPv6.

  When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.
- Enable device reboot upon interface failure.
- The type of probe test to be performed, one of:
  - Test another interface's status: Used to create a failover or coupled relationship between two interfaces. Requires the name of the alternate interface, the IP version to be tested, and the expected status of the alternate interface (either up or down).
  - Ping: Requires the hostname or IP address of the host to be pinged.
  - DNS query: You can perform a DNS query to a named DNS server, or to the DNS servers configured for the WAN.
  - HTTP test: Requires the URL of the host to be tested.
  - Test DNS servers configured for this interface: Tests communication with this interface's DNS servers that are either provided by DHCP, or statically configured.
  - Interface status: Determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

Additional configuration items

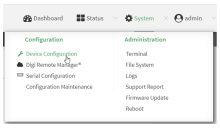
- See Configure SureLink active recovery to detect WAN/WWAN failures for optional SureLink configuration parameters.

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

WebUI

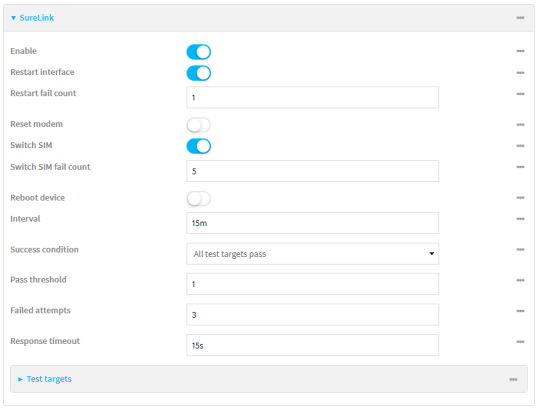
SureLink can be configured for both IPv4 and IPv6.

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. Create a new interface or select an existing one:
   - To create a new interface, see Configure a LAN, Configure a Wide Area Network (WAN), or Configure a Wireless Wide Area Network (WWAN).
   - To edit an existing interface, click to expand the appropriate interface.
5. After creating or selecting the interface, click **IPv4** (or **IPv6**) > **SureLink**.



6. **Enable** SureLink.

   SureLink can be enabled for both IPv4 and IPv6 configurations. By default, SureLink is enabled for IPv4 for the preconfigured WAN (**ETH1**) and WWAN (**Modem**). It is disabled for IPv6.

   When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.

7. **Restart interface** is enabled by default.
   - (Optional) For **Restart fail count**, type or select the number of times that the Surelink test must fail before the interface is restarted. The default is **1**.
8. Enable **Reboot device**.

   If **Reboot device** is enabled at the same time as **Restart interface**, **Reboot device** takes precedence.

- For **Reboot fail count**, type or select the number of times that the Surelink test must fail before the device is rebooted. The default is **1**.

9. Click to expand **Test targets**.
10. For **Add Test Target**, click ✚.



11. Select the **Test type**:
    - **Test another interface's status**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces. If **Test another interface's status** is selected:
      - For **Test Interface**, select the alternate interface to be tested.
      - For **IP version**, select the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.
      - For **Expected status**, select whether the expected status of the alternate interface is **Up** or **Down**. For example, if **Expected status** is set to **Down**, but the alternate interface is determined to be up, then this test will fail.
    - **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
    - **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
    - **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
    - **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
    - **Test the interface status**: The interface is considered to be down based on:
      - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

        The default is 60 seconds.
      - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

        The default is 60 seconds.
12. Optional active recovery configuration parameters:
    a. Change the **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.

b. If more than one test target is configured, for **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.

c. 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.

d. For **Failed attempts**, type the number of probe attempts before the WAN is considered to have failed.

e. For **Response timeout**, type the amount of time that the device should wait for a response to a probe 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.

13. (Optional) Repeat this procedure for IPv6.
14. 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. 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 interface, or edit an existing one:
   - To create a new interface, 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 interface, change to the interface's node in the configuration schema. For example, for a interface 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 (eth1) and WWAN (modemwwan2). It is disabled for IPv6.

   When SureLink is configured for Wireless WANs, SureLink tests are only run if the cellular modem is connected and has an IP address. Use the **SIM failover** options to configure the Connect EZ device to automatically recover the modem in the event that it cannot obtain an IP address. See Configure a Wireless Wide Area Network (WWAN) for details about **SIM failover**.

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

5. By default, the device is configured to restart the interface when its connection is considered to have failed.

   To disable:

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

   - (Optional) Set the number of times that the Surelink test must fail before the interface is restarted:

```
(config network interface my_wan ipv4 surelink)> restart_attempts
int
(config network interface my_wan ipv4 surelink>
```

     where *int* is any number greater than **0**. The default is **1**.

6. 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 the reboot parameter is enabled at the same time as the **restart** parameter, the **reboot** parameter takes precedence.

   - (Optional) Set the number of times that the Surelink test must fail before the device is rebooted:

```
(config network interface my_wan ipv4 surelink)> reboot_attempts int
(config network interface my_wan ipv4 surelink>
```

     where *int* is any number greater than **0**. The default is **1**.

7. Add a test target:

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

8. 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 **interface_down_time** to ten minutes, enter either **10m** or **600s**:

    ```
    (config network interface my_wan ipv4 surelink target 0)>
    interface_down_time 600s
    (config network interface my_wan ipv4 surelink target 0)>
    ```

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 **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config network interface my_wan ipv4 surelink target 0)>
interface_timeout 600s
(config network interface my_wan ipv4 surelink target 0)>
```

The default is 60 seconds.

- **other**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces:

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

If **other** is set:

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

```
(config network interface my_wan ipv4 surelink target
0)> other_interface /network/interface/eth1
(config network interface my_wan ipv4 surelink target
0)>
```

  - Set the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.

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

where *value* is one of: **any**, **both**, **ipv4**, or **ipv6**.

  - Set the expected status of the alternate interface:

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

where *value* is either **up** or **down**. For example, if **other_status** is set to **down**, but the alternate interface is determined to be up, then this test will fail.

(Optional) Repeat to add additional test targets.

9. Optional active recovery configuration parameters:
   a. 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>
```

   b. 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.

   c. 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**.

   d. 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**.

   e. 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 **timeout** to ten minutes, enter either **10m** or **600s**:

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

   The default is 15 seconds.

10. (Optional) Repeat this procedure for IPv6.

11. Save the configuration and apply the change:

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

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

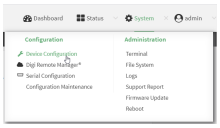
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable SureLink

If your device uses a private APN with no Internet access, or your device has a restricted wired WAN connection that doesn't allow DNS resolution, follow this procedure to disable the default SureLink connectivity tests. You can also disable DNS lookup or other internet activity, while retaining the SureLink interface test.

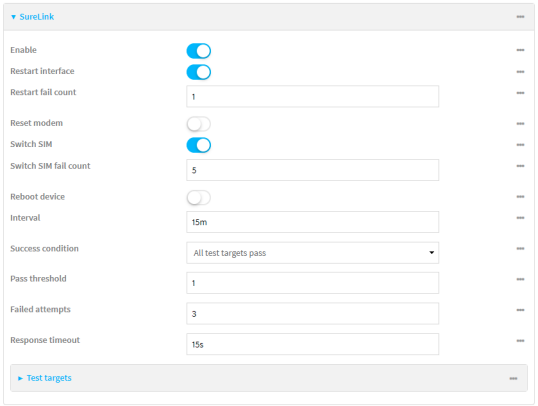
WebUI

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. Select the appropriate WAN or WWAN on which SureLink should be disabled..
5. After selecting the WAN or WWAN, click **IPv4** > **SureLink**.



6. Toggle off **Enable** to disable SureLink.
7. 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. Change to the WAN or WWAN's node in the configuration schema. For example, to disable SureLink for the Modem interface:

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

4. Disable SureLink:

```
(config network interface modem> ipv4 surelink enable false
(config network interface modem)>
```

5. Save the configuration and apply the change:

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

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

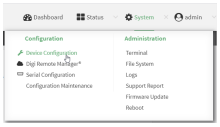
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable DNS lookup

Alternatively, you can disable DNS lookup or other internet activity for device that use a private APN with no Internet access, or that have restricted wired WAN connections that do not allow DNS resolution, while retaining the SureLink interface test. The SureLink interface test determines if the interface has an IP address assigned to it, that the physical link is up, and that a route is present to send traffic out of the network interface.

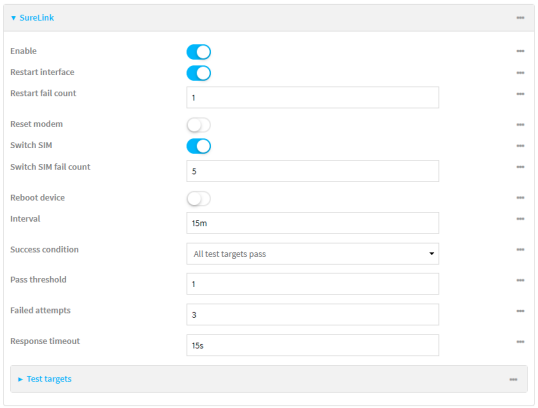
WebUI

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**.

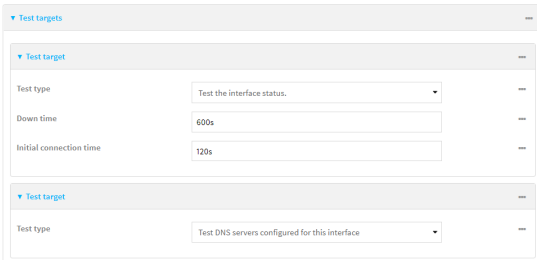


The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Select the appropriate WAN or WWAN on which SureLink should be disabled..
5. After selecting the WAN or WWAN, click **IPv4** > **SureLink**.



6. Click to expand **Test targets**.
7. Click to expand the second test target. This test target has its **Test type** set to **Test DNS servers configured for this interface**.



8. Click the menu icon **(...)** next to the target and select **Delete**.



9. 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. Change to WAN or WWAN's node in the configuration schema. For example, to disable SureLink for an interface named my_wan:

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

4. Determine the index number of the target:

```
(config network interface my_wan)> show ipv4 surelink target
0
        interface_down_time 600s
        interface_timeout 120s
        test interface_up
1
        test dns_configured
(config network interface my_wan)>
```

5. Delete the target:

```
(config network interface my_wan> del ipv4 surelink target 1
(config network interface my_wan)>
```

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.

Example: Use a ping test for WAN failover from Ethernet to cellular

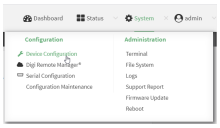
In this example configuration, the **ETH1** interface serves as the primary WAN, while the cellular **Modem** interface serves as the backup WAN.

In this example configuration, SureLink is used over for the **ETH1** interface to send a probe packet of size **256** bytes to the IP host **43.66.93.111** every **10** seconds. If there are three consecutive failed responses, the Connect EZ device brings the **ETH1** interface down and starts using the **Modem** interface. It continues to regularly test the connection to **ETH1**, and when tests on **ETH1** succeed, the device falls back to **ETH1**.

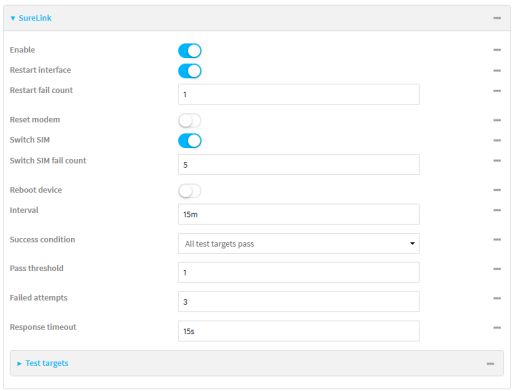
To achieve this WAN failover from the **ETH1** to the **Modem** interface, the WAN failover configuration is:

WebUI

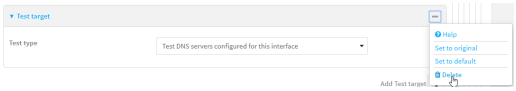
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Configure active recovery on **ETH1**:
   a. Click **Network** > **Interface** > **ETH1** > **IPv4** > **SureLink**.



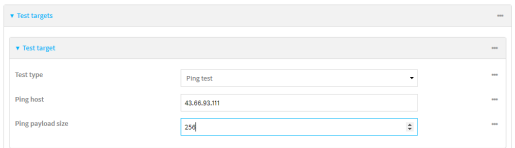
   b. For **Interval**, type **10s**.
   c. Click to expand **Test targets**.
   d. Delete the existing test targets:
      Click the menu icon **(...)** next to each target and select **Delete**.



   e. For **Add Test Target**, click ✚.



   f. For **Test type**, select **Ping test**.
   g. For **Ping host**, type **43.66.93.111**.
   h. For **Ping payload size**, type **256**.



4. Repeat the above step for **Modem** to enable SureLink on that interface.
5. 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. Configure SureLink on **ETH1**:
   a. Set the interval to ten seconds:

```
(config)> network interface eth1 ipv4 surelink interval 10s
(config)>
```

   b. Delete the existing test targets:

```
(config network interface eth1> del ipv4 surelink target 0
(config network interface eth1> del ipv4 surelink target 1
(config network interface eth1)>
```

   c. Add a test target:

```
(config)> add network interface eth1 ipv4 surelink target end
(config network interface eth1 ipv4 surelink target 0)>
```

   d. Set the probe type to ping:

```
(config network interface eth1 ipv4 surelink target 0)> test ping
(config network interface eth1 ipv4 surelink target 0)>
```

   e. Set the packet size to 256 bytes:

```
(config network interface eth1 ipv4 surelink target 0)> ping_size 256
(config network interface eth1 ipv4 surelink target 0)>
```

   f. Set the host to ping:

```
(config network interface eth1 ipv4 surelink target 0)> ping_host
43.66.93.111
(config network interface eth1 ipv4 surelink target 0)>
```

1. Repeat the above step for the cellular **Modem** (modem) interface to enable SureLink on that interface.

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.

Using Ethernet devices in a WAN

The Connect EZ device has two Ethernet devices, named **ETH1** and **ETH2**. You can use these Ethernet interfaces as a WAN when connecting to the Internet, through a device such as a cable modem:

By default, the **ETH1** Ethernet device is configured as a WAN, named **ETH1**, with both DHCP and NAT enabled and using the **External** firewall zone. This means you should be able to connect to the Internet by connecting the **ETH1** Ethernet port to another device that already has an internet connection.

The **ETH2** device is configured as a LAN interface, named **ETH2**, which uses the **Internal** firewall zone.

Using cellular modems in a Wireless WAN (WWAN)

The Connect EZ supports one cellular modem, named **Modem**, which is included in a preconfigured Wireless WAN, also named **Modem**.

The cellular modem can have only one active SIM slot at any one time. For example, **Modem** can have either SIM1 or SIM2 up at one time.

Typically, you configure SIM1 of the cellular modem as the primary cellular interface, and SIM2 as the backup cellular interface. In this way, if the Connect EZ device cannot connect to the network using SIM1, it automatically fails over to SIM2. Connect EZ devices automatically use the correct cellular module firmware for each carrier when switching SIMs.

Configure cellular modem

Configuring the Connect EZ's cellular modem involves configuring the following items:

Required configuration items

- Enable the cellular modem.

  The cellular modem is enabled by default.
- Determine the SIM slot that will be used when connecting to the cellular network.
- Configure the maximum number of interfaces that can use the modem.
- Enable carrier switching, which allows the modem to automatically match the carrier for the active SIM.

  Carrier switching is enabled by default.
- Configure the access technology.
- Determine which cellular antennas to use.

Additional configuration items

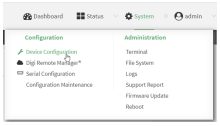
- If **Active SIM slot** is set to **Any**, determine the preferred SIM slot.

  In the event of a failover to a non-preferred SIM, or if manual SIM switching is used to switch to a non-preferred SIM, the modem will attempt to reconnect to the SIM in the preferred SIM slot.

To configure the modem:

WebUI

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. Modem are enabled by default. Click to toggle **Enable** to off to disable.
4. For **Active SIM slot**, select the SIM slot that should be used by the modem, or select **Any** to use any SIM slot. The default is **Any**.
5. If **Active SIM slot** is set to **Any**, for **Preferred SIM slot**, select the SIM slot that should be considered the preferred slot for this modem, or select **None**. In the event of a failover to a non-preferred SIM, or if manual SIM switching is used to switch to a non-preferred SIM, the modem will attempt to reconnect to the SIM in the preferred SIM slot. **None** is the default.
6. For Maximum number of interfaces, type the number of interfaces that can be configured to use this modem. This is used when using dual-APN SIMs. The default is **1**.
7. Enable **Carrier switching** to allow the modem to automatically match the carrier for the active SIM. **Carrier switching** is enabled by default.
8. For **Access technology**, select the type of cellular technology that this modem should use to access the cellular network, or select **All technologies** to configure the modem to use the best available technology. The default is **All technologies**.
9. For **Antennas**, select whether the modem should use the main antenna, the auxiliary antenna, or both the main and auxiliary antennas.
10. 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. Modem configurations are enabled by default. To disable:

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

4. Set the SIM slot that should be used by the modem:

```
(config)> network modem modem sim_slot value
(config)>
```

where *value* is one of the following:

- **any**: Uses either SIM slot.
- **1**: Uses the first SIM slot.
- **2**. Uses the second SIM slot.

The default is **any**.

5. If **sim_slot** is set to **any**, set the SIM slot that should be considered the preferred slot for this modem:

```
(config)> network modem modem sim_slot_preference value
(config)>
```

where *value* is one of the following:

- **none**: Does not consider either SIM slot to be the preferred slot.
- **1**: Configures the first SIM slot as the preferred SIM slot.
- **2**. Configures the second SIM slot as the preferred SIM slot.

In the event of a failover to a non-preferred SIM, or if manual SIM switching is used to switch to a non-preferred SIM, the modem will attempt to reconnect to the SIM in the preferred SIM slot. The default is **none**.

6. Set the maximum number of interfaces. This is used when using dual-APN SIMs. The default is **1**.

```
(config)> network modem modem max_intfs int
(config)>
```

7. Carrier switching allows the modem to automatically match the carrier for the active SIM. **Carrier switching** is enabled by default. To disable:

```
(config)> network modem modem carrier_switch false
(config)>
```

8. Set the type of cellular technology that this modem should use to access the cellular network:

```
(config)> network modem modem access_tech value
(config)>
```

Available options for *value* vary depending on the modem type. To determine available options:

```
(config)> network modem modem access_tech ?

Access technology: The cellular network technology that the modem may
use.
Format:
    2G
    3G
    4G
    4GM
    4GT
    all
Default value: all
Current value: all

(config)>
```

The default is **all**, which uses the best available technology.

9. Set whether the modem should use the main antenna, the auxiliary antenna, or both the main and auxiliary antennas:

```
(config)> network modem modem antenna value
(config)>
```

where *value* is one of the following:

- **main**
- **aux**
- **both**

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.

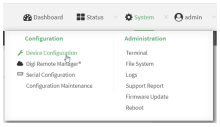
Configure cellular modem APNs

The Connect EZ device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. However, you can configure the system to use a specified APN.

To configure the APN:

WebUI

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. For **APN**, type the Access Point Name (APN) to be used when connecting to the cellular carrier.
4. (Optional) **IP version**:

   For **IP version**, select one of the following:

   - **Automatic**: Requests both IPv4 and IPv6 address.
   - **IPv4**: Requests only an IPv4 address.
   - **IPv6**: Requests only an IPv6 address.

   The default is **Automatic**.
5. (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**.
6. To add additional APNs, for **Add APN**, click ✚ and repeat the preceding instructions.
7. (Optional) To configure the device to bypass its preconfigured APN list and only use the configured APNs, enable **APN list only**.
8. 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. At the config prompt, type:

```
(config)> network interface modem modem apn 0 apn value
(config)>
```

where *value* is the APN for the SIM card.

4. (Optional) To add additional APNs:
   a. Use the **add** command to add a new APN entry. For example:

```
(config)> add network interface modem modem apn end
(config network interface modem modem apn 1)>
```

   b. Set the value of the APN:

```
(config network interface modem modem apn 1)> apn value
(config network interface modem modem apn 1)>
```

   where value is the APN for the SIM card.

5. (Optional) Set the IP version:

```
(config)> network interface modem modem apn 0 ip_version version
(config)>
```

where *version* is one of the following:

- **auto**: Requests both IPv4 and IPv6 address.
- **ipv4**: Requests only an IPv4 address.
- **ipv6**: Requests only an IPv6 address.

The default is **auto**.

6. (Optional) Set the authentication method:

```
(config)> network interface modem modem apn 0 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.

If **auto**, **chap**, or **pap** is selected, enter the **Username** and **Password** required to authenticate:

```
(config)> network interface modem modem apn 0 username name
(config)> network interface modem modem apn 0 password pwd
(config)>
```

The default is **none**.

7. (Optional) To configure the device to bypass its preconfigured APN list and only use the configured APNs:

```
(config)> network interface modem modem apn_lock true
(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 dual APNs

Some cellular carriers offer a dual APN feature that allows a SIM card to be provisioned with two separate APNs that can be used simultaneously. For example, Verizon offers this service as its Split Data Routing feature. This feature provides two separate networking paths through a single cellular modem and SIM card, and allows for configurations such as:

- Segregating public and private traffic, including policy-based routes to ensure that your internal network traffic always goes through the private connection.
- Separation of untrusted Internet traffic from trusted internal network traffic.
- Secure connection to internal customer network without using a VPN.
- Separate billing structures for public and private traffic.
- Site-to-site networking, without the overhead of tunneling for each device.

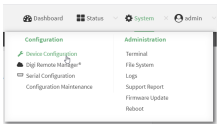
In the following example configuration, all traffic on LAN1 is routed through the public APN to the internet, and all traffic on LAN2 is routed through the private APN to the customer's data center:

To accomplish this, we will create separate WWAN interfaces that use the same modem but use different APNs, and then use routing roles to forward traffic to the appropriate WWAN interface.

Note Dual-APN connections with the Telit LE910-NAv2 module when using a Verizon SIM are not supported. Using an AT&T SIM with the Telit LE910-NAv2 module is supported. The Telit LE910-NAv2 module is used in the 1002-CM04 CORE modem.

WebUI

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.

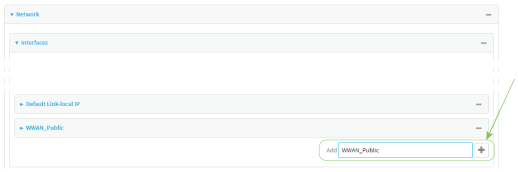
3. Increase the maximum number of interfaces allowed for the modem:
   a. Click **Network** > **Modems** > **Modem**.
   b. For **Maximum number of interfaces**, type **2**.

4. Create the WWAN interfaces:

   In this example, we will create two interfaces named **WWAN_Public** and **WWAN_Private**.

   a. Click **Network** > **Interfaces**.

   b. For **Add Interface**, type **WWAN_Public** and click ✚.



   c. For **Interface type**, select **Modem**.

   d. For **Zone**, select **External**.

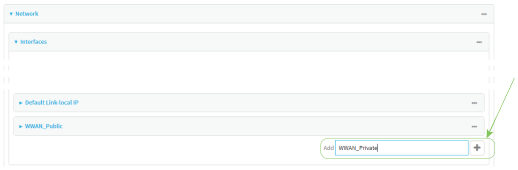
   e. For **Device**, select **Modem** .

   f. (Optional): Configure the public APN. If the public APN is not configured, the Connect EZ will attempt to determine the APN.

      i. Click to expand **APN list** > **APN**.

      ii. For **APN**, type the public APN for your cellular carrier.

   g. For **Add Interface**, type **WWAN_Private** and click ✚.



   h. For **Interface type**, select **Modem**.

   i. For **Zone**, select **External**.

   j. For **Device**, select **Modem** .

      This should be the same modem selected for the **WWAN_Public** WWAN.

   k. Enable **APN list only**.

   l. Click to expand **APN list** > **APN**.

   m. For **APN**, type the private APN provided to you by your cellular carrier.

5. Create the routing policies. For example, to route all traffic from LAN1 through the public APN, and LAN2 through the private APN:

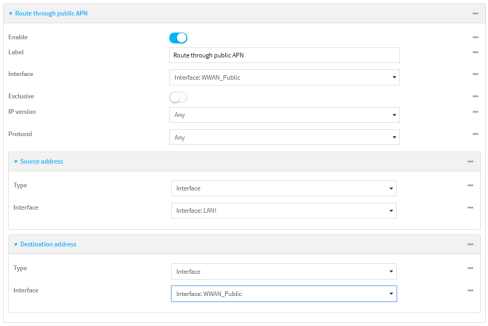
   a. Click **Network** > **Routes** > **Policy-based routing**.

   b. Click the ✚ to add a new route policy.

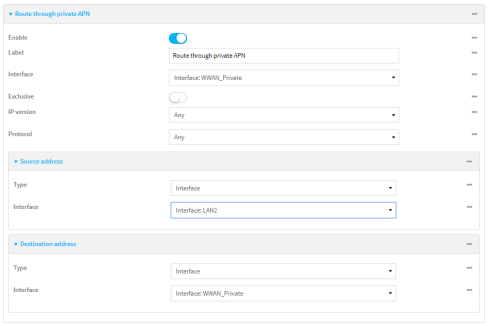


   c. For **Label**, enter **Route through public APN**.

d. For **Interface**, select **Interface: WWAN_Public**.
e. Configure the source address:
    i. Click to expand **Source address**.
    ii. For **Type**, select **Interface**.
    iii. For **Interface**, select **LAN1**.
f. Configure the destination address:
    i. Click to expand **Destination address**.
    ii. For **Type**, select **Interface**.
    iii. For **Interface**, select **Interface: WWAN_Public**.



g. Click the ✚ to add another route policy.
h. For **Label**, enter **Route through private APN**.
i. For **Interface**, select **Interface: WWAN_Private**.
j. Configure the source address:
    i. Click to expand **Source address**.
    ii. For **Type**, select **Interface**.
    iii. For **Interface**, select **LAN2**.
k. Configure the destination address:
    i. Click to expand **Destination address**.
    ii. For **Type**, select **Interface**.
    iii. For **Interface**, select **Interface: WWAN_Private**.



6. 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. Set the maximum number of interfaces for the modem:

```
(config)> network modem modem max_intfs 2
(config)>
```

4. Create the WWAN interfaces:
   a. Create the **WWANPublic** interface:

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

   b. Set the interface type to modem:

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

   c. Set the modem device:

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

   d. (Optional): Set the public APN. If the public APN is not configured, the Connect EZ will attempt to determine the APN.

```
(config network interface WWANPublic)> modem apn public_apn
(config network interface WWANPublic)>
```

   e. Use to periods (**..**) to move back one level in the configuration:

```
(config network interface WWANPublic)> ..
(config network interface)>
```

   f. Create the **WWANPrivate** interface:

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

   g. Set the interface type to modem:

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

h. Set the modem device:

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

i. Enable **APN list only**:

```
(config network interface WWANPrivate)> apn_lock true
(config network interface WWANPrivate)>
```

j. Set the private APN:

```
(config network interface WWANPublic)> modem apn private_apn
(config network interface WWANPublic)>
```

5. Create the routing policies. For example, to route all traffic from LAN1 through the public APN, and LAN2 through the private APN:
   a. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

   b. Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "Route through public apn"
(config network route policy 0)>
```

   c. Set the interface:

```
(config network route policy 0)> interface
/network/interface/WWANPublic
(config network route policy 0)>
```

   d. Configure the source address:
      i. Set the source type to **interface**:

```
(config network route policy 0)> src type interface
(config network route policy 0)>
```

      ii. Set the interface to **LAN1**:

```
(config network route policy 0)> src interface LAN1
(config network route policy 0)>
```

   e. Configure the destination address:
      i. Set the type to **interface**:

```
(config network route policy 0)> dst type interface
(config network route policy 0)>
```

ii. Set the interface to **WWANPublic** :

```
(config network route policy 0)> interface
/network/interface/WWANPublic
(config network route policy 0)>
```

f. Use to periods (**..**) to move back one level in the configuration:

```
(config nnetwork route policy 0)> ..
(config nnetwork route policy)>
```

g. Add a new routing policy:

```
(config network route policy )> add end
(config network route policy 1)>
```

h. Set the label that will be used to identify this route policy:

```
(config network route policy 1)> label "Route through private apn"
(config network route policy 1)>
```

i. Set the interface:

```
(config network route policy 1)> interface
/network/interface/WWANPrivate
(config network route policy 1)>
```

j. Configure the source address:

i. Set the source type to **interface**:

```
(config network route policy 1)> src type interface
(config network route policy 1)>
```

ii. Set the interface to **LAN2**:

```
(config network route policy 1)> src interface LAN2
(config network route policy 1)>
```

k. Configure the destination address:

i. Set the type to **interface**:

```
(config network route policy 1)> dst type interface
(config network route policy 1)>
```

ii. Set the interface to **WWANPrivate** :

```
(config network route policy 1)> interface
/network/interface/WWANPrivate
(config network route policy 1)>
```

6. Save the configuration and apply the change:

```
(config network route policy 1)> 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 manual carrier selection

By default, your Connect EZ automatically selects the most appropriate cellular carrier based on the SIM that is in use and the status of available carriers in your area.

Alternately, you can configure the devices to manually select the carrier, based on the Network PLMN ID. You can also configure the device to use manual carrier selection and fall back to automatic carrier selection if connecting to the manually-configured carrier fails.

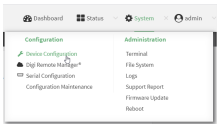
You can use also use the modem scan command at the command line to scan for available carriers and determine their PLMN ID.

Required configuration items

- Select **Manual** or **Manual/Automatic** carrier selection mode.
- The **Network PLMN ID**.

WebUI

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. For **Carrier selection mode**, select one of the following:
   - **Automatic**—The device automatically selects the carrier based on your SIM and cellular network status.
   - **Manual**—The device will only connect to the carrier identified in the **Network PLMN ID**. If the carrier is not available, no cellular connection will be established.
   - **Manual/Automatic**—The device will attempt to connect to the carrier identified in the **Network PLMN ID**. If the carrier is not available, the device will fall back to using automatic carrier selection.
4. If **Manual** or **Manual/Automatic** are selected for **Carrier section mode**, enter the **Network PLMN ID**.

Note You can use themodem scan command at the Admin CLI to scan for available carriers and determine their PLMN ID. See Scan for available cellular carriers for details.

5. 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. At the config prompt, type:

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

   where *value* is one of:

   - **automatic**—The device automatically selects the carrier based on your SIM and cellular network status.
   - **manual**—The device will only connect to the carrier identified in the **Network PLMN ID**. If the carrier is not available, no cellular connection will be established.
   - **manual_automatic**—The device will attempt to connect to the carrier identified in the **Network PLMN ID**. If the carrier is not available, the device will fall back to using automatic carrier selection.
4. If carrier section mode is set to **manual** or **manual_automatic**, set the network PLMN ID:

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

   Note You can use the modem scan command at the Admin CLI to scan for available carriers and determine their PLMN ID. See Scan for available cellular carriers for details.

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.

Scan for available cellular carriers

You can scan for available carriers and determine their network PLMN ID by using the modem scan command at the Admin CLI.

Note For devices using Unitac modems (such as devices with the 1002-CM45 core module), carrier scanning will not work if the modem has an active cellular connection.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. From the main menu, click **Status** > **Modems**.
3. Scroll to the **Connection Status** section and click **SCAN**.

   The **Carrier Scan** window opens.
4. When the **Carrier Scan** window opens, the results of the most recent previous scan are displayed. If there is no previous scan available, or to refresh the list, click **SCAN**.
5. The current carrier is highlighted in green. To switch to a different carrier:
   a. Highlight the appropriate carrier and click **SELECT**.

      The **Carrier selection** dialog opens.
   b. For Carrier selection mode, select one of the following:
      - **Manual/Automatic**: The device will use automatic carrier selection if this carrier is not available.
      - **Manual**: Does not allow the device to use automatic carrier selection if this carrier is not available.

      Note If **Manual** is selected, your modem must support the **Network technology** or the modem will lose cellular connectivity. If you are using a cellular connection to perform this procedure, you may lose your connection and the device will no longer be accessible.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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:

```
> modem scan

Issuing network scan, this may take some time...

 Status     Carrier   PLMN ID  Technology
 ---------  --------  -------  ----------
 Available  T-Mobile  310260   4G
 Available  T-Mobile  310260   3G
 Available  AT&T      310410   4G
 Available  Verizon   311480   4G
 Available  311 490   311490   4G
 Available  313 100   313100   4G

>
```

Show cellular status and statistics

You can view a summary status for all cellular modems, or view detailed status and statistics for a specific modem.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **Status**.
3. Under **Connections**, click **Modems**.

   The modem status window is displayed

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 modem command:
   - To view a status summary for the modem:

```
> show modem

Modem  SIM             Status     APN        Signal Strength
-----  --------------  ---------  ---------  --------------------
modem  1 (ready)       connected  1234       Good (-84 dBm)

>
```

   - To view detailed status and statistics, use the show modem name *name* command:

```
> show modem name modem

 modem: [Telit] LM940
 ------------------------------------------------------------------------
-----------
 IMEI                      : 781154796325698
 Model                     : LM940
 FW Version                : 24.01.541_ATT
 Revision                  : 24.01.541

 Status
 ------
 State                     : connected
 Signal Strength           : Good (-85 dBm)
 Bars                      : 2/5
 Access Mode               : 4G
 Network Technology (CNTI): LTE
 Band                      : B2
 Temperature               : 34C

 wwan1 Interface
```

```
---------------
APN                       : 1234
IPv4 surelink             : passing
IPv4 address              : 189.232.229.47
IPv4 gateway              : 189.232.229.1
IPv4 MTU                  : 1500
IPv4 DNS server(s)        : 245.144.162.207, 245.144.162.208

IPv6 surelink             : passing
IPv6 address              : 11f6:4680:0d67:59d2:552b:3429:81a8:f1ea
IPv6 gateway              : ff50:d95d:7e98:abe8:3030:9138:4f25:f51b
IPv6 MTU                  : 1500

TX bytes                  : 127941
RX bytes                  : 61026
Uptime                    : 10 hrs, 56 mins (39360s)

SIM
---
SIM Slot                  : 1
SIM Status                : ready
IMSI                      : 61582122197895
ICCID                     : 26587628655003992180
SIM Provider              : AT&T

4G
--
RSRQ                      : Good (-11.0 dB)
RSRP                      : Good (-93.0 dBm)
RSSI                      : Excellent (-64.0 dBm)
SNR                       : Good (6.4 dB)

>
```

Unlock a SIM card

A SIM card can be locked if a user tries to set an invalid PIN for the SIM card too many times. In addition, some cellular carriers require a SIM PIN to be added before the SIM card can be used. If the SIM card is locked, the Connect EZ device cannot make a cellular connection.

Command line

To unlock a SIM card:

1. Log into the Connect EZ command line as a user with Admin access.

   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 modem puk unlock command to set a new PIN for the SIM card:

```
> modem puk unlock puk_code new_pin modem_name
>
```

For example, to unlock a SIM card in the modem named **modem** with PUK code **12345678**, and set the new SIM PIN to **1234**:

```
> modem puk unlock 12345678 1234 modem
>
```

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 If the SIM remains in a locked state after using the unlock command, contact your cellular carrier.

Signal strength for cellular connections

See Show cellular status and statistics for procedures to view this information.

Signal strength for 4G connections

For 4G connections, the **RSRP** value determines signal strength.

- **Excellent**: > **-90 dBm**
- **Good**: **-90 dBm** to **-105 dBm**
- **Fair**: **-106 dBm** to **-115 dBm**
- **Poor**: **-116 dBm** to **-120 dBm**
- **No service**: **< -120 dBm**

Signal strength for 3G and 2G connections

For 3G and 2G cellular connections, the current **RSSI** value determines signal strength.

- **Excellent**: > **-70 dBm**
- **Good**: **-70 dBm** to **-85 dBm**
- **Fair**: **-86 dBm** to **-100 dBm**
- **Poor**: **< -100 dBm** to **-109 dBm**
- **No service**: **-110 dBm**

Tips for improving cellular signal strength

If the signal strength LEDs or the signal quality for your device indicate **Poor** or **No service**, try the following things to improve signal strength:

- Move the Connect EZ device to another location.
- Try connecting a different set of antennas, if available.
- Purchase a Digi Antenna Extender Kit:
  - Antenna Extender Kit, 1m
  - Antenna Extender Kit, 3m

AT command access

To run AT commands from the Connect EZ command line:

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 **modem at-interactive** and press **Enter**. Type **n** if you do not want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the cellular network.
3. At the Admin CLI prompt, use the modem at-interactive command to begin an interactive AT command session:

```
> modem at-interactive


Do you want exclusive access to the modem?  (y/n) [y]:
```

4. Type **n** if you do not want exclusive access. This allows you to send AT commands to the device while still allowing the device to connect, disconnect, and/or reconnect to the cellular network.

   The following is an example interactive AT command:

```
> modem at-interactive

Do you want exclusive access to the modem? (y/n) [y]: n
Starting terminal access to modem AT commands.
Note that the modem is still in operation.

To quit enter '~.' ('~~.' if using an ssh client) and press ENTER

Connected
ati
Manufacturer: Sierra Wireless, Incorporated
Model: MC7455
Revision: SWI9X30C_02.24.03.00 r6978 CARMD-EV-FRMWR2 2017/03/02 13:36:45
MEID: 35907206045169
IMEI: 359072060451693
IMEI SV: 9
FSN: LQ650551070110
+GCAP: +CGSM
OK
```

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 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 or bridge that is used by the WAN.
- Configure the WAN as a DHCP client.

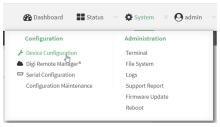
Additional configuration items

- 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: always, never, or only when this interface is the primary default route.
  - When to use DNS servers for this interface.
  - Whether to include the Connect EZ device's hostname in DHCP requests.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- IPv6 configuration:
  - The metric for IPv6 routes associated with the WAN.
  - The relative weight for IPv6 routes associated with the WAN.
  - The IPv6 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 IPv6 Maximum Transmission Unit (MTU) of the WAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - When to use DNS servers for this interface.
  - Whether to include the Connect EZ device's hostname in DHCP requests.
  - Active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- MAC address denylist and allowlist.

To create a new WAN or edit an existing WAN:

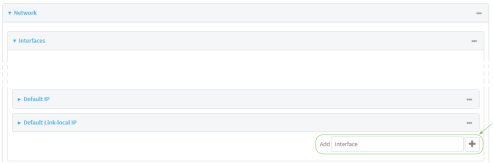
WebUI

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**.



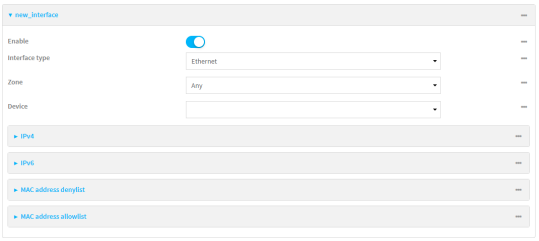
The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. 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, click **Enable**.

5. For **Interface type**, leave at the default setting of **Ethernet**.
6. For **Zone**, select **External**.
7. For **Device**, select an Ethernet device, a Wi-Fi client, or a bridge. See Bridging for more information about bridging.
8. (Optional) Click to expand **802.1x** to configure 802.1x port based network access control.

   The Connect EZ can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

   a. Click to expand **Authentication**.
   b. Click **Enable server** to enable the 802.1x authenticator on the Connect EZ device.
   c. Type the **Server IP address** of the authentication server.
   d. **Server Port number** defaults to **1812**. Type a new port number for the authentication server if different than the default.
   e. Type the **Server Password** for the authentication server.
   f. Set the **Reauth** period.
   g. (Optional) Click to expand **Accounting**.
   h. Click **Enable server** to enable 802.1x authentication auditing on the Connect EZ device.

i. Type the **Server IP address** of the auditing server.

j. **Server Port number** defaults to **1813**. Type a new port number for the auditing server if different than the default.

k. Type the **Server Password** for the auditing server.

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**.

         See Configure WAN/WWAN priority and default route metrics for further information about metrics.

      ii. 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.

      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.

      iv. Set the **MTU**.

      v. 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.

      vi. 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.

   d. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring **Active recovery**.

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**.

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

g. 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.

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

i. Set the **MTU**.

j. 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.

k. 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 denylist**.

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

a. Click to expand **MAC address denylist**.

b. For **Add MAC address**, click ✚.

c. Type the **MAC address**.

12. (Optional) Click to expand **MAC address allowlist**.

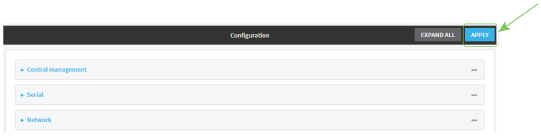
If allowlist entries are specified, incoming packets will only be accepted from the listed MAC addresses.

a. Click to expand **MAC address allowlist**.

b. For **Add MAC address**, click ✚.

c. Type the **MAC address**.

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 Wi-Fi device, or a bridge. See Bridging for more information about bridging.
   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/WWAN 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.

vi. 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.

```
(config network interface my_wan)> ipv4 dhcp_hostname true
(config network interface my_wan)>
```

- 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.

b. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring active recovery.

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/WWAN priority and default route metrics for further information about metrics.

8. (Optional) To configure 802.1x port based network access control:

   Note The Connect EZ can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

   a. Enable the 802.1x authenticator on the Connect EZ device:

   ```
   (config network interface my_wan)> 802_1x authentication enable true
   (config network interface my_wan)>
   ```

   b. Set the IP address of the authentication server:

   ```
   (config network interface my_wan)> 802_1x authentication ip IPv4_
   address
   (config network interface my_wan)>
   ```

   c. Set the password for the authentication server:

   ```
   (config network interface my_wan)> 802_1x authentication password
   password
   (config network interface my_wan)>
   ```

   d. The authentication server port number defaults to **1812**. To set an alternate port number:

   ```
   (config network interface my_wan)> 802_1x authentication port port
   (config network interface my_wan)>
   ```

   e. Set the frequency period for reauthorization:

   ```
   (config network interface my_wan)> 802_1x authentication reauth_period
   value
   (config network interface my_wan)>
   ```

   where *value* is an integer between **0** and **86400**. The default is **3600**.

   f. (Optional) Configure 802.1x authentication auditing:

      i. Enable authentication auditing on the Connect EZ device:

      ```
      (config network interface my_wan)> 802_1x accounting enable true
      (config network interface my_wan)>
      ```

      ii. Set the IP address of the accounting server:

      ```
      (config network interface my_wan)> 802_1x accounting ip IPv4_
      address
      (config network interface my_wan)>
      ```

      iii. Set the password for the accounting server:

      ```
      (config network interface my_wan)> 802_1x accounting password
      password
      (config network interface my_wan)>
      ```

iv. The accounting server port number defaults to **1813**. To set an alternate port number:

```
(config network interface my_wan)> 802_1x accounting port port
(config network interface my_wan)>
```

9. (Optional) Configure the MAC address deny list.

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

   a. Add a MAC address to the denylist:

   ```
   (config network interface my_wan)> add mac_denylist end mac_address
   (config network interface my_wan)>
   ```

   where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

   b. Repeat for each additional MAC address.

10. (Optional) Configure the MAC address allowlist.

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

    a. Add a MAC address to the allowlist:

    ```
    (config network interface my_wan)> add mac_allowlist end mac_address
    (config network interface my_wan)>
    ```

    where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

    b. Repeat for each additional MAC address.

11. Save the configuration and apply the change:

    ```
    (config network interface my_wan)> 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 a Wireless Wide Area Network (WWAN)

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

Required configuration items

- The interface type: **Modem**.
- The firewall zone: **External**.
- The cellular modem that is used by the WWAN.

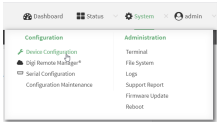
Additional configuration items

- SIM selection for this WWAN.
- The SIM PIN.

- The SIM phone number for SMS connections.
- Enable or disable roaming.
- SIM failover configuration.
- APN configuration.
- The custom gateway/netmask.
- 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: always, never, or only when this interface is the primary default route.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.
- IPv6 configuration:
  - The metric for IPv6 routes associated with the WAN.
  - The relative weight for IPv6 routes associated with the WAN.
  - The IPv6 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 IPv6 Maximum Transmission Unit (MTU) of the WAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - SureLink active recovery configuration. See Configure SureLink active recovery to detect WAN/WWAN failures for further information.

WebUI

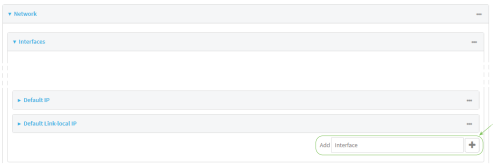
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.

4. Create the WWAN or select an existing WWAN:
   - To create a new WWAN, for **Add interface**, type a name for the WWAN and click ✚.

   - To edit an existing WWAN, click to expand the WWAN.

     New WWANs are enabled by default. To disable, click **Enable**.
5. For **Interface type**, select **Modem**.
6. The WWAN is enabled by default. Click **Enable** to disable, or to enable if it has been disabled.
7. **Interface type** defaults to **Modem**.
8. For **Zone**, select **External**.
9. For **Device**, select the cellular modem.
10. For **Match SIM by**, select a SIM matching criteria to determine when this WWAN should be used:
    - If **SIM slot** is selected, for **Match SIM slot**, select which SIM slot must be in active for this WWAN to be used.
    - If **Carrier** is selected, for **Match SIM carrier**, select which cellular carrier must be in active for this WWAN to be used.
    - If **PLMN identifier** is selected, for **Match PLMN identifier**, type the PLMN id that must be in active for this WWAN to be used.
    - If **IMSI** is selected, for **Match IMSI**, type the International Mobile Subscriber Identity (IMSI) that must be in active for this WWAN to be used.
    - If **ICCID** is selected, for **Match ICCID**, type the unique SIM card ICCID that must be in active for this WWAN to be used.
11. Type the **PIN** for the SIM. Leave blank if no PIN is required.
12. Type the **Phone number** for the SIM, for SMS connections.

    Normally, this should be left blank. It is only necessary to complete this field if the SIM does not have a phone number or if the phone number is incorrect.
13. **Roaming** is enabled by default. Click to disable.
14. For **Carrier selection mode**, select one of the following:
    - **Automatic**: The cellular carrier is selected automatically by the device.
    - **Manual**: The cellular carrier must be manually configured. If the configured network is not available, no cellular connection will be established.
    - **Manual/Automatic**: The carrier is manually configured. If the configured network is not available, automatic carrier selection is used.

    If **Manual** or **Manual/Automatic** is selected:

    a. For **Network PLMN ID**, type the PLMN ID for the cellular network.

    b. For **Network technology**, select the technology that should be used. The default is **All technologies**, which means that the best available technology will be used.

Note If **Manual** is configured for **Carrier selection mode** and a specific network technology is selected for the **Network technology**, your modem must support the selected technology or no cellular connection will be established. If you are using a cellular connection to perform this procedure, you may lose your connection and the device will no longer be accessible.

15. **SIM failover** is enabled by default, which means that the modem will automatically fail over from the active SIM to the next available SIM when the active SIM fails to connect. If enabled:
    a. For **Connection attempts before SIM failover**, type the number of times that the device should attempt to connect to the active SIM before failing over to the next available SIM.
    b. For **SIM failover alternative**, configure how SIM failover will function if automatic SIM switching is unavailable:
        - **None**: The device will perform no alternative action if automatic SIM switching is unavailable.
        - **Reset modem**: The device will reset the modem if automatic SIM switching is unavailable.
        - **Reboot device**: The device will reboot if automatic SIM switching is unavailable.
16. For **APN list** and **APN list only**, the Connect EZ device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. See Configure cellular modem APNs for further information and instructions for setting an APN.
17. (Optional) To configure the IP address of a custom gateway or a custom netmask:
    a. Click **Custom gateway** to expand.
    b. Click **Enable**.
    c. For **Gateway/Netmask**, enter the IP address and netmask of the custom gateway. To override only the gateway netmask, but not the gateway IP address, use all zeros for the IP address. For example, **0.0.0.0./32** will use the network-provided gateway, but with a /32 netmask.
18. Optional IPv4 configuration items:
    a. Click **IPv4** to expand.
    b. IPv4 support is **Enabled** by default. Click to disable.
    c. Set the **Metric**.

    See Configure WAN/WWAN priority and default route metrics for further information about metrics.
    d. 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.
    e. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
    f. Set the **MTU**.
    g. For **Use DNS**:
        - **Always**: DNS will always be used for this WWAN; 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 WWAN when the WWAN is the primary route.
- **Never**: Never use DNS servers for this WWAN.

The default setting is **When primary default route**.

19. Optional IPv6 configuration items:
    a. Click **IPv6** to expand.
    b. IPv6 support is **Enabled** by default. Click to disable.
    c. Set the **Metric**.

    See Configure WAN/WWAN priority and default route metrics for further information about metrics.
    d. 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.
    e. Set the **Management priority**. This determines which interface will have priority for central management activity. The interface with the highest number will be used.
    f. Set the **MTU**.
    g. For **Use DNS**:
        - **Always**: DNS will always be used for this WWAN; 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 WWAN when the WWAN is the primary route.
        - **Never**: Never use DNS servers for this WWAN.

    The default setting is **When primary default route**.
1. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring **SureLink**.

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 WWAN or edit an existing one:
    - To create a new WWAN named **my_wwan**:

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

- To edit an existing WWAN named **my_wwan**, change to the my_wwan node in the configuration schema:

```
(config)> network interface my_wwan
(config network interface my_wwan)>
```

4. Set the appropriate firewall zone:

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

See Firewall configuration for further information.

5. Select a cellular modem:
   a. Enter **modem device ?** to view available modems and the proper syntax.

```
(config network interface my_wwan)> modem device ?

Device: The modem used by this network interface.
Format:
  modem
Current value:

(config network interface my_wwan)> device
```

   b. Set the device:

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

6. Set theSIM matching criteria to determine when this WWAN should be used:

```
(config network interface my_wwan)> modem match value
(config network interface my_wwan)>
```

Where *value* is one of:

- **any**
- **carrier**

  Set the cellular carrier must be in active for this WWAN to be used:

  a. Use **?** to determine available carriers:

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

Match SIM carrier: The SIM carrier match criteria. This
interface is applied when the SIM card is
provisioned from the carrier.
Format:
  AT&T
  Rogers
  Sprint
  T-Mobile
```

```
  Telstra
  Verizon
  Vodafone
  other
Default value: AT&T
Current value: AT&T

(config network interface my_wwan)>
```

b. Set the carrier:

```
(config network interface my_wwan)> modem carrier value
(config network interface my_wwan)>
```

- **iccid**

  Set the unique SIM card ICCID that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem iccid ICCID
(config network interface my_wwan)>
```

- **imsi**

  Set the International Mobile Subscriber Identity (IMSI) that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem imsi IMSI
(config network interface my_wwan)>
```

- **plmn_id**

  Set the PLMN id that must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem plmn_id PLMN_ID
(config network interface my_wwan)>
```

- **sim_slot**

  Set which SIM slot must be in active for this WWAN to be used:

```
(config network interface my_wwan)> modem sim_slot value
(config network interface my_wwan)>
```

  where *value* is either **1** or **2**.

7. Set the PIN for the SIM. Leave blank if no PIN is required.

```
(config network interface my_wwan)> modem pin value
(config network interface my_wwan)>
```

8. Set the phone number for the SIM, for SMS connections:

```
(config network interface my_wwan)> modem phone num
(config network interface my_wwan)>
```

Normally, this should be left blank. It is only necessary to complete this field if the SIM does not have a phone number or if the phone number is incorrect.

9. Roaming is enabled by default. To disable:

```
(config network interface my_wwan)> modem roaming false
(config network interface my_wwan)>
```

10. Set the carrier selection mode:

```
(config network interface my_wwan)> modem operator_mode value
(config network interface my_wwan)>
```

where *value* is one of:

- **automatic**: The cellular carrier is selected automatically by the device.
- **manual**: The cellular carrier must be manually configured. If the configured network is not available, no cellular connection will be established.
- **manual_automatic**: The carrier is manually configured. If the configured network is not available, automatic carrier selection is used.

If **manual** or **manual_automatic** is set:

a. Set the Network PLMN ID:

```
(config network interface my_wwan)> modem operator PLMN_ID
(config network interface my_wwan)>
```

b. Set the cellular network technology:

```
(config network interface my_wwan)> modem operator_technology value
(config network interface my_wwan)>
```

where *value* is one of:

- **all**: The best available technology will be used.
- **2G**: Only 2G technology will be used.
- **3G**: Only 3G technology will be used.
- **4G**: Only 4G technology will be used.
- **NR5G-NSA**: Only 5G non-standalone technology will be used.
- **NR5G-SA**: Only 5G standalone technology will be used.

The default is **all**.

Note If **manual** is configured forthe carrier selection mode and a specific network technology is selected for the cellular network technology, your modem must support the selected technology or no cellular connection will be established. If you are using a cellular connection to perform this procedure, you may lose your connection and the device will no longer be accessible.

11. SIM failover is enabled by default, which means that the modem will automatically fail over from the active SIM to the next available SIM when the active SIM fails to connect. To disable:

```
(config network interface my_wwan)> modem sim_failover false
(config network interface my_wwan)>
```

If enabled:

a. Set the number of times that the device should attempt to connect to the active SIM before failing over to the next available SIM:

```
(config network interface my_wwan)> modem sim_failover_retries num
(config network interface my_wwan)>
```

The default setting is **5**.

b. Configure how SIM failover will function if automatic SIM switching is unavailable:

```
(config network interface my_wwan)> modem sim_failover_alt value
(config network interface my_wwan)>
```

where *value* is one of:

- **none**: The device will perform no alternative action if automatic SIM switching is unavailable.
- **reset**: The device will reset the modem if automatic SIM switching is unavailable.
- **reboot**: The device will reboot if automatic SIM switching is unavailable.

12. The Connect EZ device uses a preconfigured list of Access Point Names (APNs) when attempting to connect to a cellular carrier for the first time. After the device has successfully connected, it will remember the correct APN. As a result, it is generally not necessary to configure APNs. See Configure cellular modem APNs for further information and instructions for setting an APN.
13. (Optional) To configure the IP address of a custom gateway or a custom netmask:
    a. Enable the custom gateway:

```
(config network interface my_wwan)> modem custom_gw enable true
(config network interface my_wwan)>
```

    b. Set the IP address and netmask of the custom gateway:

```
(config network interface my_wwan)> modem custom_gw gateway ip_
address/netmask
(config network interface my_wwan)> modem custom_gw
```

    To override only the gateway netmask, but not the gateway IP address, use all zeros for the IP address. For example, **0.0.0.0./32** will use the network-provided gateway, but with a /32 netmask.
14. Optional IPv4 configuration items:
    a. IPv4 support is enabled by default. To disable:

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

    b. Set the metric:

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

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

c. 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_wwan)> ipv4 weight num
(config network interface my_wwan)>
```

d. 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_wwan)> ipv4 mgmt num
(config network interface my_wwan)>
```

e. Set the MTU:

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

f. Configure when the WWAN's DNS servers will be used:

```
(config network interface my_wwan)> ipv4  dns value
(config network interface my_wwan)>
```

Where *value* is one of:

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

The default setting is **primary**.

15. Optional IPv6 configuration items:

a. IPv6 support is enabled by default. To disable:

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

b. Set the metric:

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

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

c. 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_wwan)> ipv4 weight num
(config network interface my_wwan)>
```

d. 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_wwan)> ipv4 mgmt num
(config network interface my_wwan)>
```

e. Set the MTU:

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

f. Configure when the WWAN's DNS servers will be used:

```
(config network interface my_wwan)> ipv4  dns value
(config network interface my_wwan)>
```

Where *value* is one of:

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

The default setting is **primary**.

g. See Configure SureLink active recovery to detect WAN/WWAN failures for information about configuring active recovery.

Show WAN and WWAN status and statistics

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. From the menu, click **Status**.
3. Under **Networking**, click **Interfaces**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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
 modem              IPv4   up       10.200.1.101/30
 modem              IPv6   down

>
```

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
 modem              IPv4   up       modem   external  wwan1     3       10
 modem              IPv6   down     modem   external  wwan1     3       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.

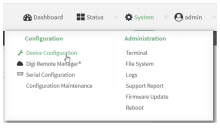
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a WAN or WWAN

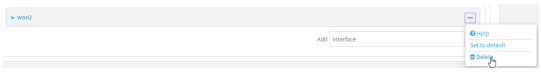
Follow this procedure to delete any WANs and WWANs that have been added to the system. You cannot delete the preconfigured WAN, **ETH1**, or the preconfigured WWAN, **Modem**.

WebUI

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 menu icon (**...**) next to the name of the WAN or WWAN to be deleted and select **Delete**.



5. 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. Use the **del** command to delete the WAN or WWAN. For example, to delete a WWAN named my_wwan:

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

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.

Default outbound WAN/WWAN ports

The following table lists the default outbound network communications for Connect EZ WAN/WWAN interfaces:

Description	TCP/UDP	Port number
Digi Remote Manager connection to my.devicecloud.com	TCP	3199
NTP date/time sync to time.devicecloud.com	UDP	123
DNS resolution using WAN-provided DNS servers	UDP	53
HTTPS for modem firmware downloads from firmware.accns.com	TCP	443

Local Area Networks (LANs)

The Connect EZ device is preconfigured with the following Local Area Networks (LANs):

You can modify configuration settings for **ETH2**, and you can create new LANs.

This section contains the following topics:

About Local Area Networks (LANs) 128
Configure a LAN 128
Example: Configure two LANs 136
Show LAN status and statistics 144
Delete a LAN 146
DHCP servers 147
Create a Virtual LAN (VLAN) route 163
Default services listening on LAN ports 166

About Local Area Networks (LANs)

A Local Area Network (LAN) connects network devices together, such as Ethernet or Wi-Fi, in a logical Layer-2 network.

The following diagram shows a LAN connected to the **ETH2** Ethernet device and the **Digi AP** access point. Once the LAN is configured and enabled, the devices connected to the network interfaces can communicate with each other, as demonstrated by the **ping** commands.

Configure a LAN

Configuring a Local Area Network (LAN) involves configuring the following items:

Required configuration items

- The interface type: either **Ethernet**, **IP Passthrough**, or **PPPoE**.
- The firewall zone: **Internal**.
- The network device or bridge that is used by the LAN.
- The IPv4 address and subnet mask for the LAN. While it is not strictly necessary for a LAN to have an IP address, if you want to send traffic from other networks to the LAN, you must configure an IP address.

> **Note** By default, **ETH2** is set to an IP address of 192.168.2.1 and uses the IP subnet of 192.168.2.0/24. If the **ETH1** Ethernet device is being used by a WAN with the same IP subnet, you should change the default IP address and subnet of LAN1.

Additional configuration items

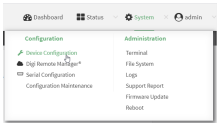
- Additional IPv4 configuration:
  - The metric for IPv4 routes associated with the LAN.
  - The relative weight for IPv4 routes associated with the LAN.
  - The IPv4 management priority of the LAN. The active interface with the highest management priority will have its address reported as the preferred contact address for central management and direct device access.
  - The IPv4 Maximum Transmission Unit (MTU) of the LAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - IPv4 DHCP server configuration. See DHCP servers for more information.
- IPv6 configuration:
  - The metric for IPv6 routes associated with the LAN.
  - The relative weight for IPv6 routes associated with the LAN.
  - The IPv6 management priority of the LAN. 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 IPv6 Maximum Transmission Unit (MTU) of the LAN.
  - When to use DNS: always, never, or only when this interface is the primary default route.
  - The IPv6 prefix length and ID.
  - IPv6 DHCP server configuration. See DHCP servers for more information.

- MAC address denylist and allowlist.

To create a new LAN or edit an existing LAN:

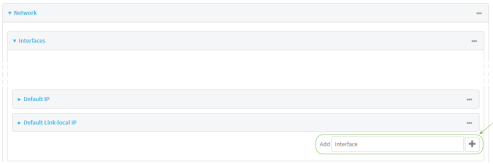
WebUI

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**.



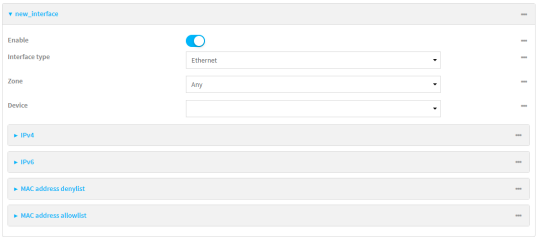
The **Configuration** window is displayed.

3. Click **Network** > **Interfaces**.
4. Create the LAN or select an existing LAN:
   - To create a new LAN, for **Add interface**, type a name for the LAN and click ✚.



   - To edit an existing LAN, click to expand the LAN.

The Interface configuration window is displayed.



New LANs are enabled by default. To disable, click **Enable**.

5. For **Interface type**, leave at the default setting of **Ethernet**.
6. For **Zone**, select the appropriate firewall zone. See Firewall configuration for further information.
7. For **Device**, select an Ethernet device, a Wi-Fi access point, or a bridge. See Bridging for more information about bridging.
8. (Optional) Click to expand **802.1x** to configure 802.1x port based network access control.

   The Connect EZ can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

   a. Click to expand **Authentication**.
   b. Click **Enable server** to enable the 802.1x authenticator on the Connect EZ device.
   c. Type the **Server IP address** of the authentication server.

d. **Server Port number** defaults to **1812**. Type a new port number for the authentication server if different than the default.
e. Type the **Server Password** for the authentication server.
f. Set the **Reauth** period.
g. (Optional) Click to expand **Accounting**.
h. Click **Enable server** to enable 802.1x authentication auditing on the Connect EZ device.
i. Type the **Server IP address** of the auditing server.
j. **Server Port number** defaults to **1813**. Type a new port number for the auditing server if different than the default.
k. Type the **Server Password** for the auditing server.

9. Configure IPv4 settings:
   a. Click to expand **IPv4**.

      IPv4 support is enabled by default.
   b. For **Type**, select **Static IP address**.
   c. 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.
   d. Optional IPv4 configuration items:
      i. Set the **Metric**.
      ii. 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.
      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.
      iv. Set the **MTU**.
   e. Enable the DHCP server:
      i. Click to expand **DHCP server**.
      ii. Click **Enable**.

      See DHCP servers for information about configuring the DHCP server.
10. See Configure DHCP relay for information about configuring **DHCP relay**.
11. (Optional) Configure IPv6 settings:
    a. Click to expand **IPv6**.
    b. **Enable** IPv6 support.
    c. For **Type**, select **IPv6 prefix delegration**.
    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. 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.

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

i. Set the **MTU**.

12. (Optional) Click to expand **MAC address denylist**.

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

    a. Click to expand **MAC address denylist**.

    b. For **Add MAC address**, click ✚.

    c. Type the **MAC address**.

13. (Optional) Click to expand **MAC address allowlist**.

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

    a. Click to expand **MAC address allowlist**.

    b. For **Add MAC address**, click ✚.

    c. Type the **MAC address**.

14. 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 LAN or edit an existing one:

   - To create a new LAN named **my_lan**:

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

   - To edit an existing LAN named **my_lan**, change to the **my_lan** node in the configuration schema:

```
(config)> network interface my_lan
(config network interface my_lan)>
```

4. Set the appropriate firewall zone:

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

See Firewall configuration for further information.

5. Select an Ethernet device, a Wi-Fi device, or a bridge. See Bridging for more information about bridging.
   a. Enter **device ?** to view available devices and the proper syntax.

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

Current value:

(config network interface my_lan)> device
```

   b. Set the device for the LAN:

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

6. Configure IPv4 settings:
   - IPv4 support is enabled by default. To disable:

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

   - The LAN is configured by default to use a static IP address for its IPv4 configuration. To configure the LAN to be a DHCP client, rather than using a static IP addres:

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

     These instructions assume that the LAN will use a static IP address for its IPv4 configuration.

   a. Set the IPv4 address and subnet of the LAN interface. Use the format *IPv4_address*/*netmask*, for example, 192.168.2.1/24.

```
(config network interface my_lan)> ipv4 address ip_address/netmask
(config network interface my_lan)>
```

   b. Optional IPv4 configuration items:
      i. Set the IP metric:

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

      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_lan)> ipv4 weight num
(config network interface my_lan)>
```

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_lan)> ipv4 mgmt num
(config network interface my_lan)>
```

iv. Set the MTU:

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

c. Enable the DHCP server:

```
(config network interface my_lan)> ipv4 dhcp_server enable true
```

See DHCP servers for information about configuring the DHCP server.

7. (Optional) Configure IPv6 settings:

a. Enable IPv6 support:

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

b. Set the IPv6 type to DHCP:

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

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_lan)> ipv6 ?

IPv6

 Parameters                Current Value
 ------------------------------------------------------------------------
----------
 enable                    true              Enable
 metric                    0                 Metric
 mgmt                      0                 Management priority
 mtu                       1500              MTU
 prefix_id                 1                 Prefix ID
 prefix_length             48                Prefix length
 type                      prefix_delegation  Type
 weight                    10                Weight

 Additional Configuration
 ------------------------------------------------------------------------
----------
```

```
 connection_monitor          Active recovery
 dhcpv6_server               DHCPv6 server

(config network interface my_lan)>
```

View default settings for the IPv6 DHCP server:

```
(config network interface my_lan)> ipv6 dhcpv6_server ?

DHCPv6 server: The DHCPv6 server settings for this network interface.

 Parameters                  Current Value
 ------------------------------------------------------------------------
----------
 enable                      true           Enable

(config network interface my_lan)>
```

d. Modify any of the remaining default settings as appropriate. For example, to change the minimum length of the prefix:

```
(config network interface my_lan)> ipv6 prefix_length 60
(config network interface my_lan)>
```

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

See Configure WAN/WWAN priority and default route metrics for further information about metrics.

8. (Optional) To configure 802.1x port based network access control:

Note The Connect EZ can function as an 802.1x authenticator; it does not function as an 802.1x supplicant.

a. Enable the 802.1x authenticator on the Connect EZ device:

```
(config network interface my_lan)> 802_1x authentication enable true
(config network interface my_lan)>
```

b. Set the IP address of the authentication server:

```
(config network interface my_lan)> 802_1x authentication ip IPv4_
address
(config network interface my_lan)>
```

c. Set the password for the authentication server:

```
(config network interface my_lan)> 802_1x authentication password
password
(config network interface my_lan)>
```

d. The authentication server port number defaults to **1812**. To set an alternate port number:

```
(config network interface my_lan)> 802_1x authentication port port
(config network interface my_lan)>
```

e. Set the frequency period for reauthorization:

```
(config network interface my_lan)> 802_1x authentication reauth_period
value
(config network interface my_lan)>
```

where *value* is an integer between **0** and **86400**. The default is **3600**.

f. (Optional) Configure 802.1x authentication auditing:

i. Enable authentication auditing on the Connect EZ device:

```
(config network interface my_lan)> 802_1x accounting enable true
(config network interface my_lan)>
```

ii. Set the IP address of the accounting server:

```
(config network interface my_lan)> 802_1x accounting ip IPv4_
address
(config network interface my_lan)>
```

iii. Set the password for the accounting server:

```
(config network interface my_lan)> 802_1x accounting password
password
(config network interface my_lan)>
```

iv. The accounting server port number defaults to **1813**. To set an alternate port number:

```
(config network interface my_lan)> 802_1x accounting port port
(config network interface my_lan)>
```

9. (Optional) Configure the MAC address deny list.

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

a. Add a MAC address to the denylist:

```
(config network interface my_lan)> add mac_denylist end mac_address
(config network interface my_lan)>
```

where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

b. Repeat for each additional MAC address.

10. (Optional) Configure the MAC address allowlist.

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

a. Add a MAC address to the allowlist:

```
(config network interface my_lan)> add mac_allowlist end mac_address
(config network interface my_lan)>
```

where *mac_address* is a hyphen-separated MAC address, for example, 32-A6-84-2E-81-58.

b. Repeat for each additional MAC address.

11. Save the configuration and apply the change:

```
(config network interface my_lan)> 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.

Example: Configure two LANs

The default configuration of the Connect EZ consists of one WAN (named **ETH1**), one WWAN (**Modem**), and one LAN (**ETH2**). For Connect EZW Wi-Fi enabled devices, the default configuration of the **ETH2** uses a bridge that consists of two devices, the **ETH2** Ethernet device and the **Digi AP** Wi-Fi access point.

In this example, we will:

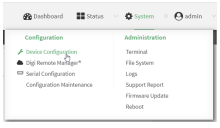
1. Create a new Wi-Fi access point (Connect EZW models only).
2. Create a new bridge that consists of the new access point and the **ETH1** device.

   In this configuration, the **ETH1** device will no longer be part of a WAN. Internet access will be provided by the cellular modem.
3. Create two new LANs:
   - **LAN1** will be configured to use the new bridge.
   - **LAN2** will be configured to use the **ETH2** device.

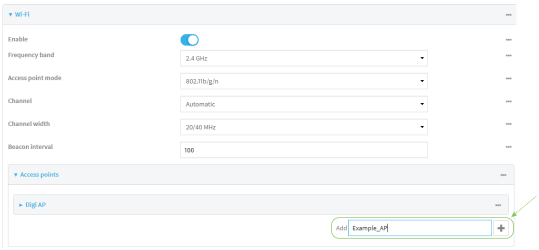
Task one: Create a new access point (Connect EZW models only)

WebUI

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**.

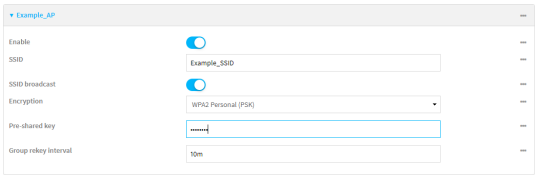


   The **Configuration** window is displayed.
3. Click **Network** > **Wi-Fi** > **Access points**.
4. For **Add Wi-Fi access point**, type **Example_AP** for the name of the new access point and click ✚.

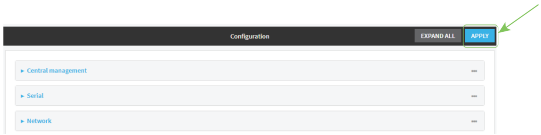


The Wi-Fi access point configuration window is displayed.

5. For **SSID**, type **Example_SSID**.
6. Type a **Pre-shared key** that clients will use to access the AP.



7. 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 access point:

```
(config)> add network wifi ap Example_AP
(config network wifi ap Example_AP)>
```

New access points are enabled by default.

4. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap Example_AP)> ssid Example_SSID
(config network wifi ap Example_AP)>
```

SSID broadcasting is enabled by default for new access points.

5. Set the security for the access point to WPA2:

```
(config network wifi ap Example_AP)> encryption type wpa2
(config network wifi ap Example_AP)>
```

6. Set the password that clients will use when connecting to the access point:

```
(config network wifi ap Example_AP)> encryption key_psk2 password
(config network wifi ap Example_AP)>
```

7. Save the configuration and apply the change:

```
(config network wireless ap Example_AP)> save
Configuration saved.
>
```

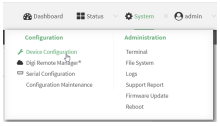
8. Type **exit** to exit the Admin CLI.

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

Task two: Create a new bridge (Connect EZW)

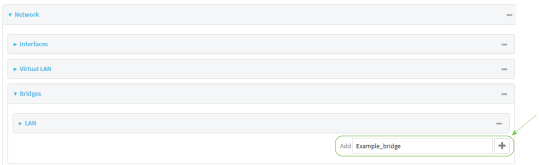
WebUI

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** > **Bridges**.
4. For **Add Bridge**, type **Example_bridge** and click ✚.

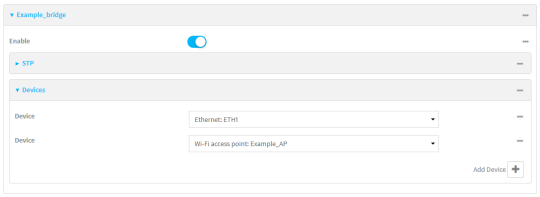


   The new bridge configuration window is displayed.



5. Click to expand **Devices**.
6. For **Add Device**, click ✚.
7. For Device, select **Ethernet: ETH1**.

8. Click ✚ again to add another device.
9. For Device, select **Wi-Fi access point: Example_AP**.



10. (Optional) Enable Spanning Tree Protocol (STP).

    STP is used when using multiple LANs on the same device, to prevent bridge loops and other routing conflicts.

    a. Click **STP**.
    b. Click **Enable**.
    c. For **Forwarding delay**, enter the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data. The default is **2** seconds.
11. 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 bridge:

```
(config)> add network bridge Example_bridge
(config network bridge Example_bridge)>
```

   New access points are enabled by default.
4. Use the Tab key (twice) to determine available devices:

```
(config network bridge Example_bridge)> add device end [TAB][TAB]
/network/device/eth1              /network/device/eth2
/network/device/loopback          /network/bridge/lan
/network/wifi/ap/digi_ap          /network/wifi/ap/Example_AP
(config network bridge Example_bridge)> add device end /network/
```

5. Add the **eth1** Ethernet device:

```
(config network bridge Example_bridge)> add device end
/network/device/eth1
(config network bridge Example_bridge)>
```

6. Add the **Example_AP** Wi-Fi access point:

```
(config network bridge Example_bridge)> add device end
/network/wireless/ap/Example_AP
(config network bridge Example_bridge)>
```

7. (Optional) Enable Spanning Tree Protocol (STP).

   STP is used when using multiple LANs on the same device, to prevent bridge loops and other routing conflicts.

   a. Enable STP:

```
(config network bridge Example_bridge)> stp enable true
```

   b. Set the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data:

```
(config network bridge Example_bridge)> stp forward_delay num
(config)>
```

   The default is **2** seconds.

8. Save the configuration and apply the change:

```
(config network bridge Example_bridge)> save
Configuration saved.
>
```

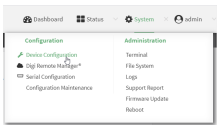
9. Type **exit** to exit the Admin CLI.

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

Task three: Create the LANs

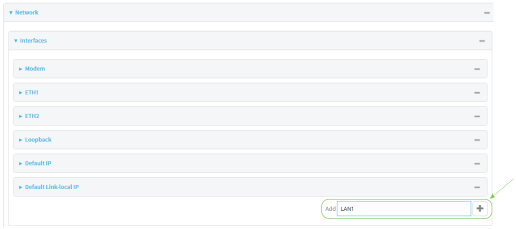
WebUI

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**.

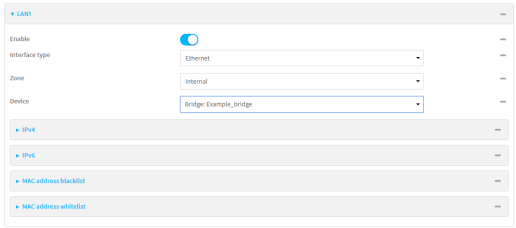


   The **Configuration** window is displayed.

3. Create **LAN1**:
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface:**, type **LAN1** and click ✚.



   c. For **Zone**, select **Internal**.
   d. For **Device**:
      - If you are configuring a Wi-Fi enabled Connect EZW , select **Bridge: Example_bridge**.
      - If you are configuring a non-Wi-Fi Connect EZ, select **Ethernet: ETH1**.



   e. Click to expand **IPv4**.
   f. For **Address**, type **192.168.3.1/24**.
   g. Click to expand **DHCP server**.
   h. Click **Enable**.
4. Create LAN2:
   a. Click **Network** > **Interfaces**.
   b. For **Add Interface:**, type **LAN2** and click ✚.
   c. For **Zone**, select **Internal**.
   d. For **Device**, select **Ethernet: ETH2**.
   e. Click to expand **IPv4**.
   f. For **Address**, type **192.168.4.1/24**.
   g. Click to expand **DHCP server**.
   h. Click **Enable**.
5. 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 the LAN1 interface:
   a. Add the interface:

```
(config)> add network interface LAN1
(config network interface LAN1)>
```

   b. Configure the LAN1 interface:
      i. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface LAN1)> device ?

Device: The network device used by this network interface.
Format:
  /network/device/eth1
  /network/device/eth2
  /network/bridge/LAN
  /network/bridge/Example_bridge
  /network/wireless/ap/digi_ap
  /network/wireless/ap/Example_AP
Current value:

(config network interface LAN1)> device
```

      ii. Set the device for the LAN1 interface:
         - If you are configuring a Wi-Fi enabled Connect EZW , set the device to **/network/bridge/Example_bridge**.

```
(config network interface LAN1)> device
/network/bridge/Example_bridge
(config network interface LAN1)>
```

         - If you are configuring a non-Wi-Fi Connect EZ, set the device to **/network/device/eth1** .

```
(config network interface LAN1)> device /network/device/eth1
(config network interface LAN1)>
```

   c. Configure the firewall zone for the LAN1 interface to **internal**:

```
(config network interface LAN1)> zone internal
(config network interface LAN1)>
```

d. Configure the IPv4 address for the LAN1 interface:

```
(config network interface LAN1)> ipv4 address 192.168.3.1/24
(config network interface LAN1)>
```

e. Enable the DHCP server for the LAN1 interface:

```
(config network interface LAN1)> ipv4 dhcp_server enable true
(config network interface LAN1)>
```

4. Create the LAN2 interface:
   a. Add the interface:

```
(config)> add network interface LAN2
(config network interface LAN2)>
```

   b. Configure the LAN2 interface:
      i. Enter **device ?** to view available devices and the proper syntax.

```
(config network interface LAN2)> device ?

Device: The network device used by this network interface.
Format:
  /network/device/eth1
  /network/device/eth2
  /network/bridge/LAN
  /network/bridge/Example_bridge
  /network/wireless/ap/digi_ap
  /network/wireless/ap/Example_AP
Current value:

(config network interface LAN2)> device
```

      ii. Set the device for the LAN2 interface:

```
(config network interface LAN2)> device /network/device/eth1
(config network interface LAN2)>
```

   c. Configure the firewall zone for the LAN2 interface to **internal**:

```
(config network interface LAN2)> zone internal
(config network interface LAN2)>
```

   d. Configure the IPv4 address for the LAN2 interface:

```
(config network interface LAN2)> ipv4 address 192.168.4.1/24
(config network interface LAN2)>
```

   e. Enable the DHCP server for the LAN2 interface:

```
(config network interface LAN2)> ipv4 dhcp_server enable true
(config network interface LAN2)>
```

5. Save the configuration and apply the change:

```
(config network interface LAN2)> 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.

Task four: Verify the new configuration

The final step in this example is to verify the new configuration.

1. Verify that LAN1 is operating correctly:
   a. Connect a device to LAN1 through the **ETH1** Ethernet port, or by connecting to the Example_AP Wi-Fi1 access point.
   b. Verify that the device has been provided an IP address from the LAN DHCP server in the 192.168.3.* subnet.
2. Verify that LAN2 is operating correctly:
   a. Connect a device to LAN2 through the **ETH2** Ethernet port.
   b. Verify that the device has been provided an IP address from the LAN2 DHCP server in the 192.168.4.* subnet.

Show LAN status and statistics

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. From the menu, click **Status**.
3. Under **Networking**, click **Interfaces**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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
```

```
 modem              IPv4   up       10.200.1.101/30
 modem              IPv6   down

>
```

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
 modem             IPv4   up       modem   external  wwan1     3       10
 modem             IPv6   down     modem   external  wwan1     3       10

>
```

4. Enter **show network interface *name*** at the Admin CLI prompt to display additional information about a specific LAN. For example, to display information about ETH2, enter **show network interface *eth2***:

```
> show network interface eth2

 lan1 Interface Status
 --------------------
 Device              : eth2
 Zone                : internal

 IPv4 Status         : up
 IPv4 Type           : static
 IPv4 Address(es)    : 192.168.2.1/24
 IPv4 Gateway        :
 IPv4 MTU            : 1500
 IPv4 Metric         : 5
 IPv4 Weight         : 10
 IPv4 DNS Server(s)  :

 IPv6 Status         : up
 IPv6 Type           : prefix
 IPv6 Address(es)    : fd00:2704::1/48
 IPv6 Gateway        :
 IPv6 MTU            : 1500
 IPv6 Metric         : 5
 IPv6 Weight         : 10
 IPv6 DNS Server(s)  :
```

```
>
```

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

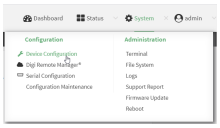
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a LAN

Follow this procedure to delete any LANs that have been added to the system. You cannot delete the preconfigured LAN, **LAN1**.

WebUI

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 menu icon (**...**) next to the name of the LAN to be deleted and select **Delete**.



5. 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. Use the **del** command to delete the LAN. For example, to delete a LAN named my_lan:

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

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.

DHCP servers

You can enable DHCP on your Connect EZ device to assign IP addresses to clients, using either:

- The DHCP server for the device's local network, which assigns IP addresses to clients on the device's local network. Addresses are assigned from a specified pool of IP addresses. For a local network, the device uses the DHCP server that has the IP address pool in the same IP subnet as the local network.

  When a host receives an IP configuration, the configuration is valid for a particular amount of time, known as the lease time. After this lease time expires, the configuration must be renewed. The host renews the lease time automatically.
- A DHCP relay server, which forwards DHCP requests from clients to a DHCP server that is running on a separate device.

Configure a DHCP server

Note These instructions assume you are configuring the device to use its local DHCP server. For instructions about configuring the device to use a DHCP relay server, see Configure DHCP relay.

Required configuration items

- Enable the DHCP server.

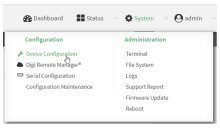
Additional configuration items

- The lease address pool: the range of IP addresses issued by the DHCP server to clients.
- Lease time: The length, in minutes, of the leases issued by the DHCP server.

- The Maximum Transmission Units (MTU).
- The domain name suffix appended to host names.
- The IP gateway address given to clients.
- The IP addresses of the preferred and alternate Domain Name Server (DNS), NTP servers, and WINS severs that are given to clients.
- The TFTP server name.
- The filepath and name of the bootfile on the TFTP server.
- Custom DHCP options. See Configure DHCP options for information about custom DHCP options.
- Static leases. See Map static IP addresses to hosts for information about static leases.

WebUI

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 to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server**.
6. **Enable** the DHCP server.
7. (Optional) For **Lease time**, type the amount of time that a DHCP lease is 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 **Lease time** to ten minutes, enter **10m** or **600s**.

   The default is 12 hours.
8. (Optional) For **Lease range start** and **Lease range end**, type the lowest and highest IP address that the DHCP server will assign to a client. This value represents the low order byte of the address (the final triplet in an IPv4 address, for example, 192.168.2.**xxx**). The remainder of the IP address will be based on the LAN's static IP address as defined in the **Address** field.

   Allowed values are between **1** and **254**, and the default is **100** for **Lease range start** and **250** for **Lease range end**.
9. Optional DHCP server settings:
   a. Click to expand **Advanced settings**.
   b. For **Gateway**, select either:
      - **None**: No gateway is broadcast by the DHCP server. Client destinations must be resolvable without a gateway.
      - **Automatic**: Broadcasts the Connect EZ device's gateway.

- **Custom**: Allows you to identify the IP address of a **Custom gateway** to be broadcast.

The default is **Automatic**.

c. For **MTU**,

- **None**: An MTU of length **0** is broadcast. This is not recommended.
- **Automatic**: No MTU is broadcast and clients will determine their own MTU.
- **Custom**: Allows you to identify a **Custom MTU** to be broadcast.

The default is **Automatic**.

d. For **Domain name suffix**, type the domain name that should be appended to host names.

e. For **Primary** and **Secondary DNS**, **Primary** and **Secondary NTP server**, and **Primary** and **Secondary WINS server**, select either:

- **None**: No server is broadcast.
- **Automatic**: Broadcasts the Connect EZ device's server.
- **Custom**: Allows you to identify the IP address of the server.

f. For **Bootfile name**, type the relative path and file name of the bootfile on the TFTP server.

g. For **TFTP server** name, type the IP address or host name of the TFTP server.

10. See Configure DHCP options for information about **Custom DHCP options**.
11. See Map static IP addresses to hosts for information about **Static leases**.
12. 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. Enable the DHCP server for an existing LAN. For example, to enable the DHCP server for a LAN named **my_lan**:

```
(config)> network interface my_lan ipv4 dhcp_server enable true
(config)>
```

   See Configure a LAN for information about creating a LAN.

4. (Optional) Set the amount of time that a DHCP lease is valid:

```
(config)> network interface my_lan ipv4 dhcp_server lease_time 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 **network interface my_lan ipv4 dhcp_server lease_time** to ten minutes, enter either **10m** or **600s**:

```
(config)> network interface my_lan ipv4 dhcp_server lease_time 600s
(config)>
```

5. (Optional) Set the lowest IP address that the DHCP server will assign to a client. This value represents the low order byte of the address (the final triplet in an IPv4 address, for example, 192.168.2.**xxx**). The remainder of the IP address will be based on the LAN's static IP address as defined in the **address** parameter.

```
(config)> network interface my_lan ipv4 dhcp_server lease_start num
(config)>
```

Allowed values are between **1** and **254**, and the default is **100**.

6. (Optional) Set the highest IP address that the DHCP server will assign to a client:

```
(config)> network interface my_lan ipv4 dhcp_server lease_end num
(config)>
```

Allowed values are between **1** and **254**, and the default is **250**.

7. Optional DHCP server settings:
   a. Click to expand **Advanced settings**.
   b. Determine how the DHCP server should broadcast the gateway server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced gateway
value
(config)>
```

where **value** is one of:

- **none**: No gateway is broadcast by the DHCP server. Client destinations must be resolvable without a gateway.
- **auto**: Broadcasts the Connect EZ device's gateway.
- **custom**: Allows you to identify the IP address of a custom gateway to be broadcast:

```
(config)> network interface my_lan ipv4 dhcp_server advanced
gateway_custom ip_address
(config)>
```

The default is **auto**.

   c. Determine how the DHCP server should broadcast the the MTU:

```
(config)> network interface my_lan ipv4 dhcp_server advanced mtu value
(config)>
```

where **value** is one of:

- **none**: An MTU of length **0** is broadcast. This is not recommended.
- **auto**: No MTU is broadcast and clients will determine their own MTU.

- **custom**: Allows you to identify a custom MTU to be broadcast:

```
(config)> network interface my_lan ipv4 dhcp_server advanced
mtu_custom mtu
(config)>
```

The default is **auto**.

d. Set the domain name that should be appended to host names:

```
(config)> network interface my_lan ipv4 dhcp_server advanced domain_
suffix name
(config)>
```

e. Set the IP address or host name of the primary and secondary DNS, the primary and secondary NTP server, and the primary and secondary WINS servers:

```
(config)> network interface my_lan ipv4 dhcp_server advanced primary_
dns value
(config)> network interface my_lan ipv4 dhcp_server advanced
secondary_dns value
(config)> network interface my_lan ipv4 dhcp_server advanced primary_
ntp value
(config)> network interface my_lan ipv4 dhcp_server advanced
secondary_ntp value
(config)> network interface my_lan ipv4 dhcp_server advanced primary_
wins value
(config)> network interface my_lan ipv4 dhcp_server advanced
secondary_wins value
(config)>
```

where **value** is one of:

- **none**: No server is broadcast.
- **auto**: Broadcasts the Connect EZ device's server.
- **custom**: Allows you to identify the IP address of the server. For example:

```
(config)> network interface my_lan ipv4 dhcp_server advanced
primary_dns_custom ip_address
(config)>
```

The default is **auto**.

f. Set the IP address or host name of the TFTP server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced nftp_
server ip_address
(config)>
```

g. Set the relative path and file name of the bootfile on the TFTP server:

```
(config)> network interface my_lan ipv4 dhcp_server advanced bootfile
filename
(config)>
```

8. See Configure DHCP options for information about custom DHCP options.
9. See Map static IP addresses to hosts for information about static leases.
10. Save the configuration and apply the change:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease
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.

Map static IP addresses to hosts

You can configure the DHCP server to assign static IP addresses to specific hosts.

Required configuration items

- IP address that will be mapped to the device.
- MAC address of the device.

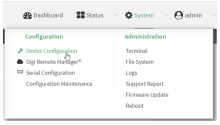
Additional configuration items

- A label for this instance of the static lease.

To map static IP addresses:

WebUI

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 to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Static leases**.
6. For **Add Static lease**, click ✚.
7. Type the **MAC address** of the device associated with this static lease.

8. Type the **IP address** for the static lease.

Note The IP address here should be outside of the DHCP server's configured lease range. See Configure a DHCP server for further information about the lease range.

9. (Optional) For **Hostname**, type a label for the static lease. This does not have to be the device's actual hostname.
10. Repeat for each additional DHCP static lease.
11. 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. Add a static lease to the DHCP server configuration for an existing LAN. For example, to add static lease to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_server advanced static_
lease end
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)>
```

   See Configure a LAN for information about creating a LAN.
4. Set the MAC address of the device associated with this static lease, using the colon-separated format:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)> mac 00:40:D0:13:35:36
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)>
```

5. Set the IP address for the static lease:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)> ip 10.01.01.10
(network interface my_lan ipv4 dhcp_server advanced static_lease 0)>
```

Note The IP address here should be outside of the DHCP server's configured lease range. See Configure a DHCP server for further information about the lease range.

6. (Optional) Set a label for this static lease:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)> name label
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)>
```

7. Save the configuration and apply the change:

```
(config network interface my_lan ipv4 dhcp_server advanced static_lease
0)> 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 current static IP mapping

To view your current static IP mapping:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Networking**, click **DHCP Leases**.

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. Show the static lease configuration. For example, to show the static leases for a lan named **my_lan**:

```
(config)> show network interface my_lan ipv4 dhcp_server advanced static_
lease
0
    ip 192.168.2.10
    mac BF:C3:46:24:0E:D9
    no name
1
    ip 192.168.2.11
    mac E3:C1:1F:65:C3:0E
```

```
    no name
(config)>
```

4. Type **cancel** to exit configuration mode:

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

5. Type exit to exit the Admin CLI.

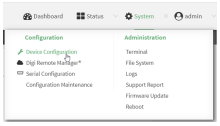
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete static IP mapping entries

To delete a static IP entry:

WebUI

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 to expand an existing LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Static leases**.
6. Click the menu icon (**...**) next to the name of the static lease to be deleted and select **Delete**.



7. 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. Show the static lease configuration. For example, to show the static leases for a lan named **my_lan**:

```
(config)> show network interface my_lan ipv4 dhcp_server advanced static_
lease
0
    ip 192.168.2.10
    mac BF:C3:46:24:0E:D9
    no name
1
    ip 192.168.2.11
    mac E3:C1:1F:65:C3:0E
    no name
(config)>
```

4. Use the **del *index_number*** command to delete a static lease. For example, to delete the static lease for the device listed in the above output with a mac address of BF:C3:46:24:0E:D9 (index number **0**):

```
(config)> del network interface lan1 ipv4 dhcp_server advanced static_
lease 0
(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.

Configure DHCP options

You can configure DHCP servers running on your Connect EZ device to send certain specified DHCP options to DHCP clients. You can also set the user class, which enables you to specify which specific DHCP clients will receive the option. You can also force the command to be sent to the clients.

DHCP options can be set on a per-LAN basis, or can be set for all LANs. A total of 32 DHCP options can be configured.

Required configuration items

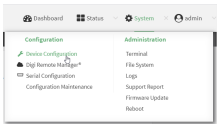
- DHCP option number.
- Value for the DHCP option.

Additional configuration items

- The data type of the value.
- Force the option to be sent to the DHCP clients.
- A label for the custom option.

WebUI

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 to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Click to expand **IPv4** > **DHCP server** > **Advanced settings** > **Custom DHCP option**.
6. For **Add Custom option**, click ✚.

   Custom options are enabled by default. To disable, uncheck **Enable**.
7. For **Option number**, type the DHCP option number.
8. For **Value**, type the value of the DHCP option.
9. (Optional) For **Label**, type a label for the custom option.
10. (Optional) If **Forced send** is enabled, the DHCP option will always be sent to the client, even if the client does not ask for it.
11. (Optional) For **Data type**, select the data type that the option uses. If the incorrect data type is selected, the device will send the value as a string.
12. 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. Add a custom DHCP option to the DHCP server configuration for an existing LAN. For example, to add static lease to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_server advanced custom_
option end
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

See Configure a LAN for information about creating a LAN.

4. Custom options are enabled by default. To disable:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> enable false
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

5. Set the option number for the DHCP option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> option 210
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

6. Set the value for the DHCP option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> value_str value
(network interface my_lan ipv4 dhcp_server advanced custom_option 0)>
```

7. (Optional) Set a label for this custom option:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> name label
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

8. (Optional) To force the DHCP option to always be sent to the client, even if the client does not ask for it:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> force true
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

9. (Optional) Set the data type that the option uses.

   If the incorrect data type is selected, the device will send the value as a string.

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)> datatype value
(config network interface my_lan ipv4 dhcp_server advanced custom_option
0)>
```

   where *value* is one of:

   - **1byte**
   - **2byte**
   - **4byte**
   - **hex**
   - **ipv4**
   - **str**

   The default is **str**.

10. Save the configuration and apply the change:

```
(config network interface my_lan ipv4 dhcp_server advanced custom_option
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.

Configure DHCP relay

DHCP relay allows a router to forward DHCP requests from one LAN to a separate DHCP server, typically connected to a different LAN.

For the Connect EZ device, DHCP relay is configured by providing the IP address of a DHCP relay server, rather than an IP address range. If both the DHCP relay server and an IP address range are specified, DHCP relay is used, and the specified IP address range is ignored.

Multiple DHCP relay servers can be provided for each LAN. If multiple relay servers are provided, DHCP requests are forwarded to all servers without waiting for a response. Clients will typically use the IP address from the first DHCP response received.

Configuring DHCP relay involves the following items:

Required configuration items

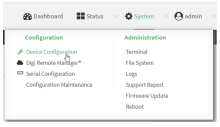
- Disable the DHCP server, if it is enabled.
- IP address of the primary DHCP relay server, to define the relay server that will respond to DHCP requests.

Additional configuration items

- IP address of additional DHCP relay servers.

WebUI

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 to expand an existing LAN, or create a new LAN. See Configure a LAN.
5. Disable the DHCP server, if it is enabled:
   a. Click to expand **IPv4** > **DHCP server**.
   b. Click **Enable** to toggle off the DHCP server.
6. Click to expand **DHCP relay**.

7. For **Add DHCP Server:**, click ✚.
8. For **DHCP server address**, type the IP address of the relay server.
9. Repeat for each additional DHCP relay server.
10. 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. Add a DHCP relay server to an existing LAN. For example, to add a server to a LAN named **my_lan**:

```
(config)> add network interface my_lan ipv4 dhcp_relay end
(config network interface lan1 my_lan dhcp_relay 0)>
```

   See Configure a LAN for information about creating a LAN.
4. Set the IP address of the DHCP relay server:

```
(config network interface my_lan ipv4 dhcp_relay 0)> address 10.10.10.10
(config network interface my_lan ipv4 dhcp_relay 0)>
```

5. (Optional) Add additional DHCP relay servers:
   a. Move back one step in the configuration schema by typing two periods (**..**):

```
(config network interface my_lan ipv4 dhcp_relay 0)> ..
(config network interface my_lan ipv4 dhcp_relay)>
```

   b. Add the next server:

```
(config network interface lan1 ipv4 dhcp_relay)> add end
(config network interface lan1 ipv4 dhcp_relay 1)>
```

   c. Set the IP address of the DHCP relay server:

```
(config network interface my_lan ipv4 dhcp_relay 1)> address
10.10.10.11
(config network interface my_lan ipv4 dhcp_relay 1)>
```

   d. Repeat for each additional relay server.

1. Disable the DHCP server, if it is enabled:

```
(config network interface my_lan ipv4 dhcp_relay 1)> .. .. dhcp_server
enable false
(config network interface my_lan ipv4 dhcp_relay 1)>
```

6. Save the configuration and apply the change:

```
(config network interface lan1 ipv4 dhcp_relay 1)> 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 DHCP server status and settings

View DHCP status to monitor which devices have been given IP configuration by the Connect EZ device and to diagnose DHCP issues.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Networking**, click **DHCP Leases**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 dhcp-lease command at the Admn CLI prompt:

```
> show dhcp-lease

 IP Address     Hostname         Expires
 -------------  ---------------  -------
 192.168.2.194  MTK-ENG-USER1
 192.168.2.195  MTK-ENG-USER2

>
```

3. Additional information can be returned by using the show dhcp-lease verbose command:

```
> show dhcp-lease verbose

 IP Address     Hostname      Expires                   Type     Active
MAC Address
 -------------  --------      ------------------------  -------  ------
-----------------
```

```
 192.168.2.194  MTK-ENG-USER1 May 19 08:25:11 UTC 2021  Dynamic  Yes
ba:ba:2c:13:8c:71
 192.168.2.195  MTK-ENG-USER2 May 20 11:32:12 UTC 2021  Dynamic  Yes
09:eb:10:f0:bc:16

>
```

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.

Create a Virtual LAN (VLAN) route

Virtual LANs (VLANs) allow splitting a single physical LAN into separate Virtual LANs. This is useful for security reasons, and also helps to reduce broadcast traffic on the LAN.

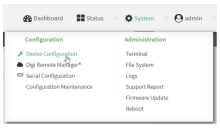
Required configuration items

- Device to be assigned to the VLAN.
- The VLAN ID. The TCP header uses the VLAN ID to identify the destination VLAN for the packet.

To create a VLAN:

WebUI

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** > **Virtual LAN**.
4. Type a name for the VLAN and click ✚.
5. Select the **Device**.
6. Type or select a unique numeric **ID** for the VLAN ID.
7. 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. Add the VLAN:

```
(config)> add network vlan name
(config)>
```

4. Set the device to be used by the VLAN:

   a. View a list of available devices:

```
(config network vlan vlan1)> device ?

Device: The Ethernet device to use for this virtual LAN
Format:
  /network/device/eth1
  /network/device/eth2
  /network/device/loopback
  /network/vlan/vlan1
  /network/bridge/lan
  /network/wireless/ap/digi_ap
Current value:

(config network vlan vlan1)>
```

   b. Add the device:

```
(config network vlan vlan1)> device /network/device/
(config network vlan vlan1)>
```

5. Set the VLAN ID:

```
(config network vlan vlan1)> id value
```

   where *value* is an integer between **1** and **4095**.

6. Save the configuration and apply the change:

```
(config network vlan vlan1)> 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.

Default services listening on LAN ports

The following table lists the default services listening on the specified ports on the Connect EZ LAN interfaces:

Description	TCP/UDP	Port numbers
DNS server	UDP	53
DHCP server	UDP	67 and 68
SSH server	TCP	22
Web UI	TCP	443 (also listens on port 80, then redirects to port 443

Bridging

Bridging is a mechanism to create a single network consisting of multiple devices, such as Ethernet devices and wireless access points.

This section contains the following topics:

Configure a bridge 168

Configure a bridge

Required configuration items

- A name for the bridge.

  Bridges are enabled by default.
- Devices to be included in the bridge.

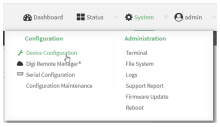
Additional configuration items

- Enable Spanning Tree Protocol (STP).

To create a bridge:

WebUI

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** > **Bridges**.
4. For **Add Bridge**, type a name for the bridge and click ✚.
5. Bridges are enabled by default. To disable, uncheck **Enable**.
6. Add devices to the bridge:
   a. Click to expand **Devices**.
   b. For **Add device**, click ✚.
   c. Select the **Device**.
   d. Repeat to add additional devices.

   Note The MAC address of the bridge is taken from the first available device in the list.
7. (Optional) Enable Spanning Tree Protocol (STP).

   STP is used when using multiple LANs on the same device, to prevent bridge loops and other routing conflicts.
   a. Click **STP**.
   b. Click **Enable**.
   c. For **Forwarding delay**, enter the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data. The default is **2** seconds.
8. Click **Apply** to save the configuration and apply the change.


Configuration
EXPAND ALL
APPLY
Central management
Serial
Network

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 the bridge:

```
(config)> add network bridge my_bridge
(config network bridge my_bridge)>
```

4. Bridges are enabled by default.
   - To disable:

```
(config network bridge my_bridge)> enable false
(config network bridge my_bridge)>
```

   - To enable if it has been disabled:

```
(config network bridge my_bridge)> enable true
(config network bridge my_bridge)>
```

5. Add devices to the bridge:
   a. Determine available devices:

```
(config network bridge my_bridge)> .. .. interface lan device ?


Default value: /network/lan
Current value: /network/lan

(config network bridge my_bridge)>
```

   b. Add the appropriate device. For example, to add the **Digi AP** Wi-Fi access point:

```
(config network bridge my_bridge)> add device end
/network/wireless/ap/digi_ap
(config)>
```

Note The MAC address of the bridge is taken from the first available device in the list.

6. (Optional) Enable Spanning Tree Protocol (STP).

   STP is used when using multiple LANs on the same device, to prevent bridge loops and other routing conflicts.

   a. Enable STP:

```
(config network bridge my_bridge)> stp enable true
```

b. Set the number of seconds that the device will spend in each of the listening and learning states before the bridge begins forwarding data:

```
(config network bridge my_bridge)> stp forward_delay num
(config)>
```

The default is **2** seconds.

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 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 status for all interfaces

To show the Surelink status all interfaces, use the show surelink interface all command:

1. Log into the Connect EZ command line as a user with Admin access.

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

>
```

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. Log into the Connect EZ command line as a user with Admin access.

   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

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

>
```

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. Log into the Connect EZ command line as a user with Admin access.

   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 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

>
```

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 IPsec tunnel

To show the Surelink status a specific IPsec tunnel, use the show surelink ipsec tunnel *name* command:

1. Log into the Connect EZ command line as a user with Admin access.

   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 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

>
```

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 OpenVPN clients

To show the Surelink status all OpenVPN clients, use the show surelink openvpn client all command:

1. Log into the Connect EZ command line as a user with Admin access.

   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 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

>
```

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 OpenVPN client

To show the Surelink status a specific OpenVPN client, use the show surelink openvpn client *name* command:

1. Log into the Connect EZ command line as a user with Admin access.

   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 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

>
```

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 port

Connect EZ devices have multiple serial ports that provide 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.
- 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 Digi Navigator application.
- UDP serial: Provides access to the serial port using UDP.
- Modbus: Allows the device to function as a Modbus protocol gateway.

View serial port information

- Show serial status and statistics
- Log serial port messages

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**

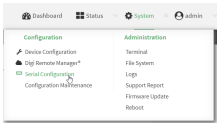
Configure Login mode

Login mode allows the user to log into the device through the serial port.

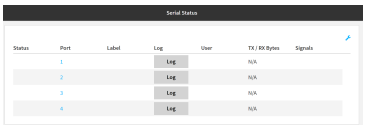
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

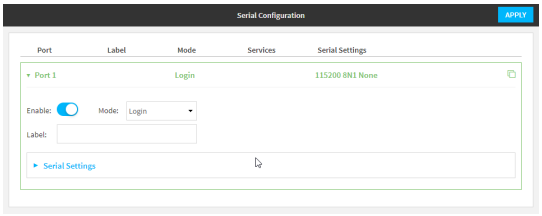


The **Serial Configuration** page is displayed.



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 **Login**.
5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

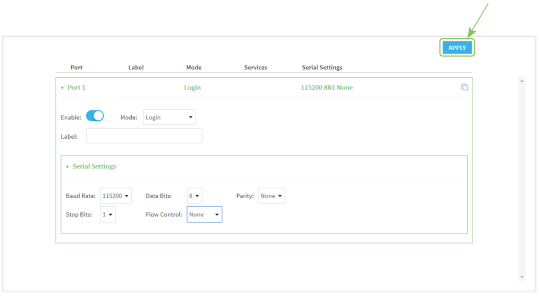
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. For **Signalling**, select the electrical signaling interface type used on this serial port:
   - **RS-232**
     - Enable **RTS Toggle** if you want to enable RTS toggling during transmission on this serial 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**.
   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.

   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.



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. 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.

```
(config)> serial port1 altpin true
(config)>
```

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

   If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6.
   - **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)>path-parambaudrate rate
   (config)>
   ```

9. Set the number of data bits used by the device to which you want to connect:

   ```
   (config)>path-paramdatabits bits
   (config)>
   ```

10. Set the type of parity used by the device to which you want to connect:

    ```
    (config)>path-paramparity 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)>path-paramstopbits bits
    (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.

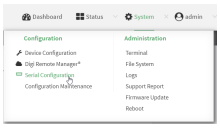
Configure Remote Access mode

Remote Access mode allows for remote access to another device that is connected to the serial port.

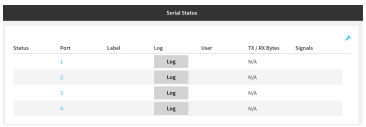
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

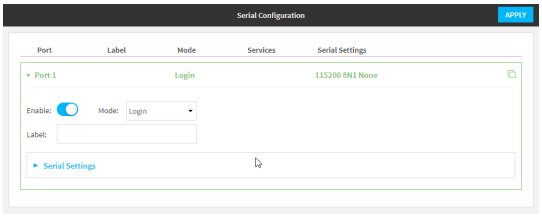


   The **Serial Configuration** page is displayed.



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 **Remote Access**. This is the default.
5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

   If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.
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**.

   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**.

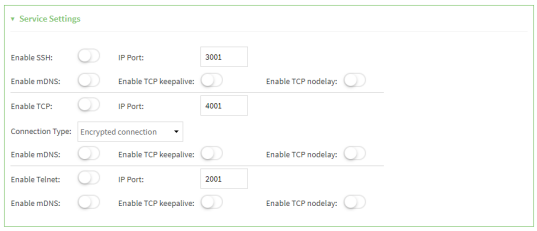
   c. **Parity**: For **Parity**, select the type of parity used by the device to which you want to connect. The default is **None**.

   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**.

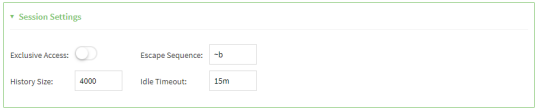
   e. **Flow control**: For **Flow control**, select the type of flow control used by the device to which you want to connect. The default is **None**.

9. Click **Enable** to enable the data framing feature.
10. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.
11. For **Idle Time**, enter the length of time the device should wait before sending the packet.
12. For **End Pattern**, enter the end pattern. The packet is sent when this pattern is received from the serial port.
13. Click **Strip End Pattern** if you want to remove the end pattern from the packet before it is sent.
14. 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.

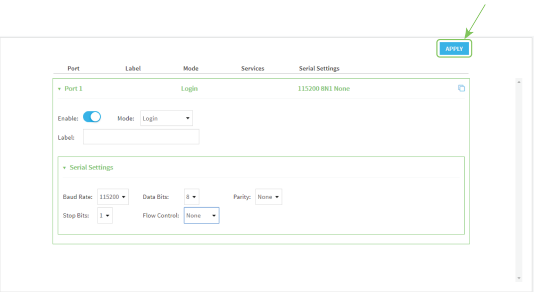


15. Expand **Autoconnect Settings**.
    a. Click **Enable** to enable the autoconnect feature.
    b. For **Connection Trigger**, select the option that describes the type of event that should trigger the connection.
    c. For **Outbound Connection Type**, select the option that describes the method 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 @.
    e. For **IP Port**, enter the TCP port of the remote server (1-65535).
    f. Click **Enable TCP keepalive** to enable TCP keepalive on the connection.
    g. Click **Enable TCP nodelay** to enable TCP nodelay on the connection.
16. Expand **Session Settings**.



    a. Enable **Exclusive access** to limit access to the serial port to a single active session.
    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.
17. 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.
18. Click **Apply** to save the configuration and apply the change.

    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.



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. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the mode:

```
(config)> serial port1 mode remoteaccess
(config)>
```

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

```
(config)> serial port1 altpin true
(config)>
```

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

   If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6.
   - **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)>path-parambaudrate rate
(config)>
```

9. Set the number of data bits used by the device to which you want to connect:

```
(config)>path-paramdatabits bits
(config)>
```

10. Set the type of parity used by the device to which you want to connect:

```
(config)>path-paramparity 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)>path-paramstopbits bits
(config)>
```

12. Configure the session settings.
    a. Set the characters used to start an escape sequence:

```
(config)>path-paramescape 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)>path-paramexclusive 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)>path-paramhistory bytes
(config)
```

    The default is **4000** bytes.
    d. Set the amount of time to wait before disconnecting due to user inactivity:

```
(config)>path-paramidle_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)>path-paramidle_timeout 600s
(config)
```

    The default is **15m**.
13. Configure monitor settings.
    a. (Optional) Enable monitoring of CTS (Clear to Send) changes on this port:

```
(config)>path-parammonitor cts true
(config)
```

    b. (Optional) Enable monitoring of DCD (Data Carrier Detect) changes on this port:

```
(config)>path-parammonitor dcd 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.

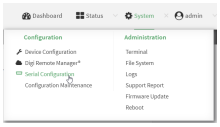
Configure Application mode

Application mode provides access to the serial device from Python applications.

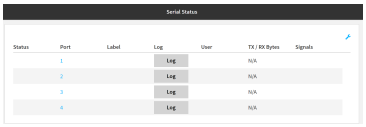
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

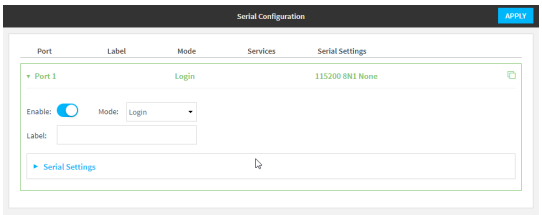


The **Serial Configuration** page is displayed.



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. (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.

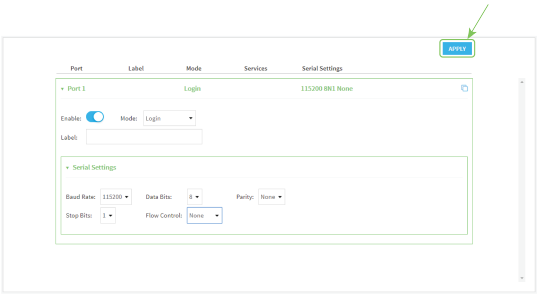
   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

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.

   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.



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. 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.

```
(config)> serial port1 altpin true
(config)>
```

This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6.
   - **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 RealPort mode

You can configure the Connect EZ to communicate with your computer using RealPort.

Note If you are using the Windows OS, you can also enable and configure RealPort mode for the Connect EZ device and your computer from the **Digi Navigator**. See Digi Navigator application.

Step 1: Install Realport

You can install RealPort on a computer with either a Windows OS or a Linux OS.

- **Windows**: For the Windows installation process, see Install RealPort on a Windows computer.
- **Linux**: For the Linux installation process, refer to the Get started: Install RealPort for LINUX in the **RealPort Installation User's Guide**.

Step 2: Configure the serial ports for RealPort mode

You should perform this process on each of the serial ports on the device. See Configure the serial port for RealPort mode.

Step 3: Configure the RealPort service

To complete RealPort configuration on the Connect EZ, you must enable and configure the RealPort service. See Configure the RealPort service.

Install RealPort on a Windows computer

You must download and run the RealPort utility.

Step 1: Download and run Digi Device Discovery Utility

1. Navigate to www.digi.com/support/realport.
2. From the **Operating System Specific Drivers** list box, select the appropriate Microsoft Windows option. A list of driver options appears.
3. Click the desired **RealPort for Windows** version. The file is downloaded, and a Windows Explorer window launches, showing the RealPort files.

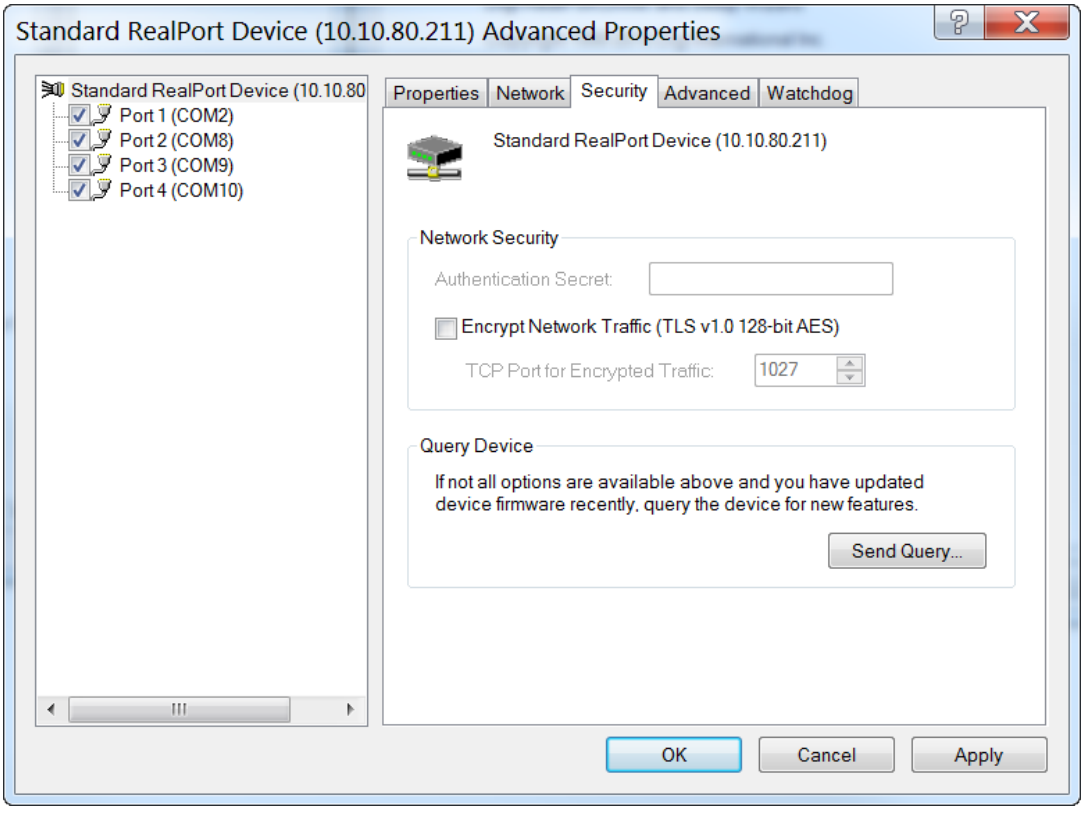
4. When the download is complete, open the .zip file and click the **setup.exe** file. The **Digi RealPort Setup Wizard** appears.
5. Select **Add a New Device**.
6. Follow the steps in the wizard to install RealPort.
7. Click **Finish** to close the wizard.

Step 2: Configure Encrypted RealPort

Encrypted RealPort is a security feature that maintains data integrity. It prevents unauthorized changes in data, including intentional destruction or alteration, tampering, duplication, or accidental loss. Encrypted RealPort also prevents disclosure to unauthorized individuals or processes. If your data is sensitive, Encrypted RealPort is strongly recommended.

To implement Encrypted RealPort:

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** field has a default value of **1027**. The entry must match the device's TCP port setting. You can verify the setting on the device using the web interface on the device.
   a. Open browser window.
   b. Enter the IP address in the URL address bar to access the web interface.
   c. Choose **Network > Network Services Settings**.
   d. Select the **Enable Encrypted RealPort** option and verify that the port number is **1027**.
   e. Click **Apply**.
9. Click **OK**.
10. Click **Apply**.

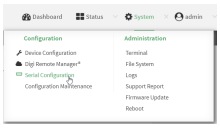
Configure the serial port for RealPort mode

RealPort mode allows you to use Realport.

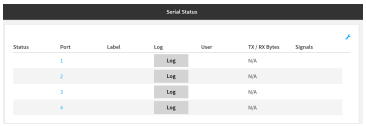
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

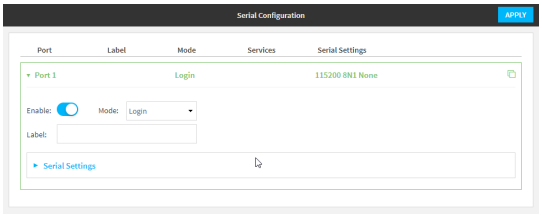


   The **Serial Configuration** page is displayed.



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 **RealPort**.

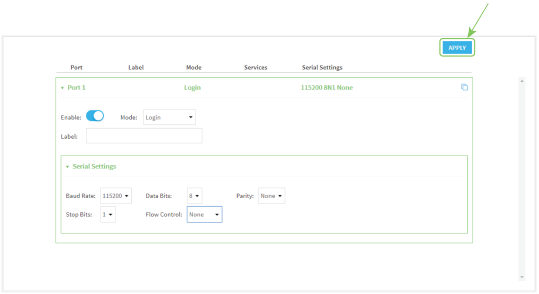
5. Leave **Sharing Mode** at the default, **None**.
6. (Optional) For **Label**, enter a label that will be used when referring to this port.
7. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

   If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.
8. 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**.
9. Click **Apply** to save the configuration and apply the change.

   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.



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. The serial port is enabled by default. To disable:

```
(config)> serial port1 enable false
(config)>
```

4. Set the signal mode:

```
(config)> serial port1 signal mode value
(config)>
```

where **value** is one of:

- **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**.

5. Enable **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

```
(config)> serial port1 altpin true
(config)>
```

This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6. Set a label that will be used when referring to this port.

```
(config)> serial port1 label label
(config)>
```

7. (Optional) Set a label that will be used when referring to this port.

```
(config)> serial port1 label 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 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.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
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**.
7. Enable **Encryption** to enable encryption of data. This is enabled by default.
8. (Optional) For **Shared Secret**, enter the key to ensure secure communication. Leave this field blank to disable authentication.
9. 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 disabled by default.
10. Enable **RealPort Keepalive** to send RealPort keepalive packets. This is enabled by default.
11. Enable **TCP Port Keepalive** to send TCP keepalive packets. This is disabled by default.
12. Click **Apply** to save the configuration and apply the change.

    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.

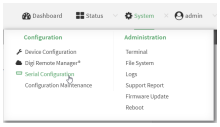
Configure UDP serial mode

The UDP serial mode option in the serial port configuration provides access to the serial port using UDP.

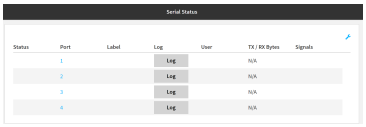
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

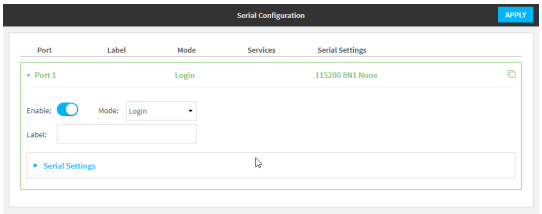


The **Serial Configuration** page is displayed.



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 to expand the port that you want to configure for UDP serial mode.



The serial port is enabled by default. To disable, toggle off **Enable**.

4. For **Mode**, select **UDP serial**.
   The default is **Login**.
5. (Optional) For **Label**, enter a label that will be used when referring to this port.
6. 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.

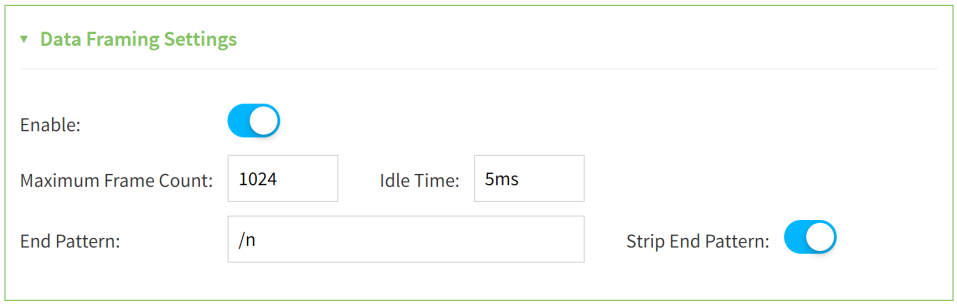
The default is **RS-232**.

7. Expand **Serial Settings**.



   a. For **Baud rate**, select the baud rate used by the device to which you want to connect.
   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**.



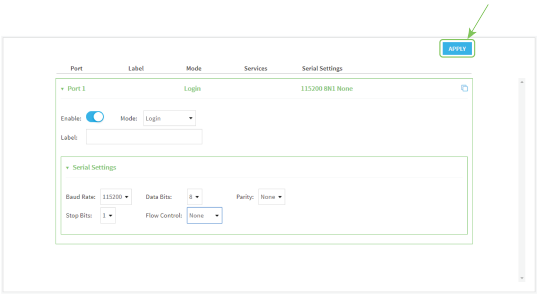
   a. Click **Enable** to enable the data framing feature.
   b. For **Maximum Frame Count**, enter the maximum size of the packet. The default is **1024**.
   c. For **Idle Time**, enter the length of time the device should wait before sending the packet.
   d. For **End Pattern**, enter the end pattern. 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.

9. Expand **UDP Serial Settings**.



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

    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.



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. 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.

```
(config)> serial port1 altpin true
(config)>
```

This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6.
   - **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)>
```

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. Enable data framing:

```
(config)>serial port1 framing enable true
(config)
```

14. Set the maximum size of the packet:

```
(config)>serial port1 framing max_count int
(config)
```

The default is **1024**.

15. 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**.

16. 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)
```

17. 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)
```

18. Set the UDP port:

```
(config)> serial port1 udp port port
(config)>
```

The default is **4001**.

19. (Optional) Enter a string that should be added at the beginning of each packet:

```
(config)> serial port1 udp socketid backslash-escaped-string
(config)>
```

20. 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 upd 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 hostanme-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)>
```

21. Save the configuration and apply the change:

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

22. 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.

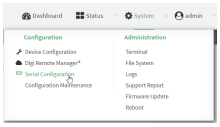
Configure Modbus mode

Modbus mode allows you to use the serial port for Modbus. See Modbus gateway.

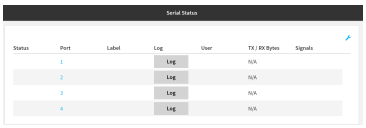
To change the configuration to match the serial configuration of the device to which you want to connect:

WebUI

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

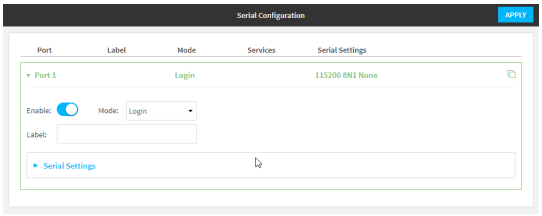


The **Serial Configuration** page is displayed.



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 **Altpin** to use the Altpin feature. **Altpin** is disabled by default.

   This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

   If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

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**.

   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**.

1. Set the baud rate used by the device to which you want to connect:

```
(config)>path-parambaudrate rate
(config)>
```

2. Set the number of data bits used by the device to which you want to connect:

```
(config)>path-paramdatabits bits
(config)>
```

3. Set the type of parity used by the device to which you want to connect:

```
(config)>path-paramparity parity
(config)>
```

Allowed values are:

- **even**
- **odd**
- **none**

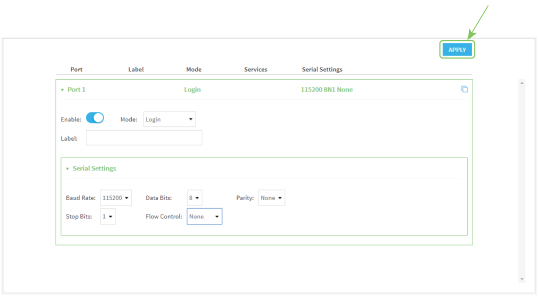
The default is **none**.

4. Set the stop bits used by the device to which you want to connect:

```
(config)>path-paramstopbits bits
(config)>
```

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

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.



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. 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.

```
(config)> serial port1 altpin true
(config)>
```

This feature should be enabled when you are using a modem and an 8-pin cable and you need CD (Carrier Detect). When enabled, the DTR on pin 1 drives DCD.

If altpin is disabled, the hardware signal on RJ45 pin 1 becomes DSR instead of DCD. This alternative can be used if DCD is not required, and DSR is needed instead.

6.
   - **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. 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**.
   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**.

1. Set the baud rate used by the device to which you want to connect:

```
(config)>path-parambaudrate rate
(config)>
```

2. Set the number of data bits used by the device to which you want to connect:

```
(config)>path-paramdatabits bits
(config)>
```

3. Set the type of parity used by the device to which you want to connect:

```
(config)>path-paramparity parity
(config)>
```

   Allowed values are:

   - **even**
   - **odd**
   - **none**

   The default is **none**.

4. Set the stop bits used by the device to which you want to connect:

```
(config)>path-paramstopbits bits
(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.

Show serial status and statistics

To show the status and statistics for the serial port:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Connections**, click **Serial**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

Log serial port messages

To display and configure the serial port log:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**
3. Under **Connections**, click **Serial**.
4. Click **Log**.

   The **Serial port log** window displays.
5. Click **Start** to start serial port logging.
6. Click **Stop** to stop serial port logging if it has been started.
7. Click **Refresh** to refresh the log display.
8. Click **Download** to download the serial port log.

9. (Optional) For **Log size**, configure the maximum allowed log size for the serial port log. The default is **65536**.

Digi Navigator application

You can use the **Digi Navigator** application with the Connect EZ device to discover device IP addresses, install and configure RealPort, and verify connection to the network.

Before you begin

Your device must be connected to your network or a laptop before you can access the Digi Navigator after it has been installed.

Use the Digi Navigator application features

These features can be performed from the **Digi Navigator**.

- Configure RealPort
- Discover the device's IP address

Install and configure the Digi Navigator application

- Install the Digi Navigator
- Connect to and access the Digi Navigator
- Digi Navigator features
- Discover the IP address when connected to a network
- Discover the IP address when not on a network
- Manage the RealPort 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

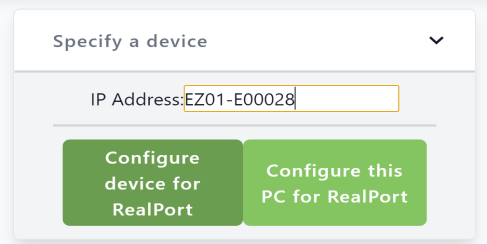
Step 6: Configure RealPort from the Digi Navigator

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.

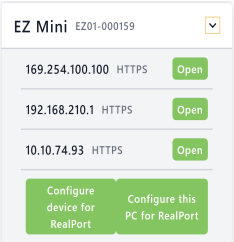
In this step, all serial ports on the device are set to RealPort mode and the RealPort service is enabled. The COM ports on your laptop are also configured.

Note You can also configure the device to accept a Realport connection from the web UI on the device. See Configure RealPort mode.

1. Make sure theConnect EZ is powered on and connected to your network or computer.
2. Download and install the **Digi Navigator**.
3. Launch the **Digi Navigator**.
4. Select the device you want to configure using one of the following methods:
    - **Specify a device**: Expand the **Specify a device** section and enter the IP address or host name for the device.



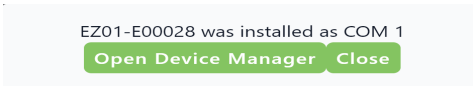
- **Select a device**: From the list of devices shown in the **Digi Navigator**, expand the device that you want to configure.



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.

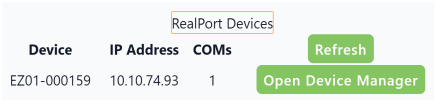


   e. Click **Close** to close the message.
6. Configure RealPort on your computer.
   a. Click **Configure this PC for RealPort**.
   b. From the **Select starting COM** list box, select the first COM port that should be configured for RealPort. The number of COM ports configured matches the number of 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 Maanger** if you want to do further configuration to the COM ports. The Windows **Properties** dialog displays.

7. If desired, you can verify the RealPort configuration. See Configure the serial port for RealPort mode and Configure the RealPort service.
8. 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**.
   a. Launch the **Digi Navigator** if it is not currently open. A list of Connect EZ devices that have RealPort enabled and configured displays in the RealPort Devices section at the bottom of the application screen.
   b. Click **Open Device Manager** to open the Windows **Properties** dialog for the COM ports on your computer that are configured for RealPort. For more information, see Manage the RealPort device list.



NEXT STEP: If you are performing the initial device set-up, proceed to the next step: Step 7: Connect to the web UI and update the Connect EZ firmware.

Step 5: Discover the IP address using the Digi Navigator

You can use the Digi Navigator to quickly discover the IP address for the Connect EZ.

Make sure you have the device powered and connected the device to your network or computer with an Ethernet cable. See Connect to and access the Digi Navigator.

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. Download and install the **Digi Navigator**.
2. Launch the **Digi Navigator**.
3. 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 Discover the IP address 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 Discover the IP address when not on a network.
4. 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 6: Configure RealPort from the Digi Navigator.

Install the Digi Navigator

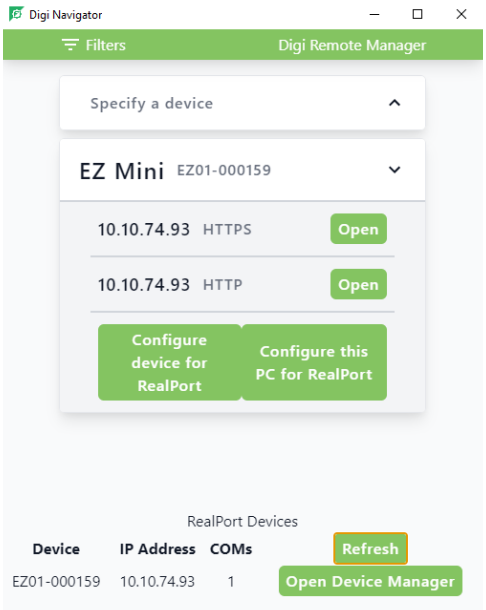
This section explains how to download and install the **Digi Navigator** application.

Note Microsoft Visual C++ must be installed to ensure that Realport can be installed. Microsoft Visual C++ is installed by default during the Digi Navigator install process, if it is not already installed on your computer.

1. Navigate to the Digi Connect EZ drivers support page.
2. Click **Digi Navigator** to start the download.
3. Click the downloaded file to install the tool.
4. If Microsoft Visual C++ is not currently installed on your computer, the installation process for this application begins.
   a. Click **OK** to begin installation.
   b. The Microsoft Visual C++ installation screen closes automatically when installation is complete.
5. Click **Finish** to complete installation of the Digi Navigator.

Digi Navigator features

All features of the Digi Navigator are available from the main application screen.



Section	Description
Green toolbar	From the toolbar at the top of the screen, you can apply filters and access Digi Remote Manager. **Filters**: Click **Filters** to expand the filters section and apply Device Filters, Service Filters, and Default IP Filters. Click **Filters** again to minimize the filters section. **Digi Remote Manager**: Click **Digi Remote Manager** to launch Remote Manager.
Specify a device	Expand the **Specify a device** section to enter the IP address of a Connect EZ device and then configure the device to use RealPort.

Section	Description
Connect EZ device	Expand a device to be able to access the web UI for the device and configure the device to use RealPort. ■ **Access web UI**: Click **Open** to access the web UI for the device. ■ **Configure RealPort**: Click **Configure device for Realport** and **Configure this PC for RealPort** to configure the device to use RealPort.
RealPort Devices	Click **RealPort Devices** at the bottom of the screen to display a list of devices that are configured to use RealPort.

Connect to and access the Digi Navigator

Your device must be connected to your network or a laptop before you can access the Digi Navigator.

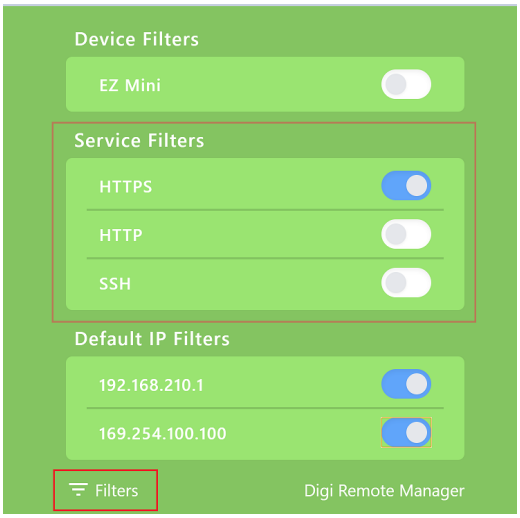
1. Connect a power supply to the device and power it on.
2. Use an Ethernet cable to connect the device to your network or computer.

- If you are connected to a computer, you will need to determine the default IP address.
- If you are connected to your network, the Connect EZ is automatically assigned an IP address.

Discover the IP address when connected to a network

To discover the IP address for a Connect EZ device connected to your network, the Digi Navigator uses the HTTPS service by default. Other services can be used, if needed.

1. Make sure your device is connected to the network and the Digi Navigator is installed.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.

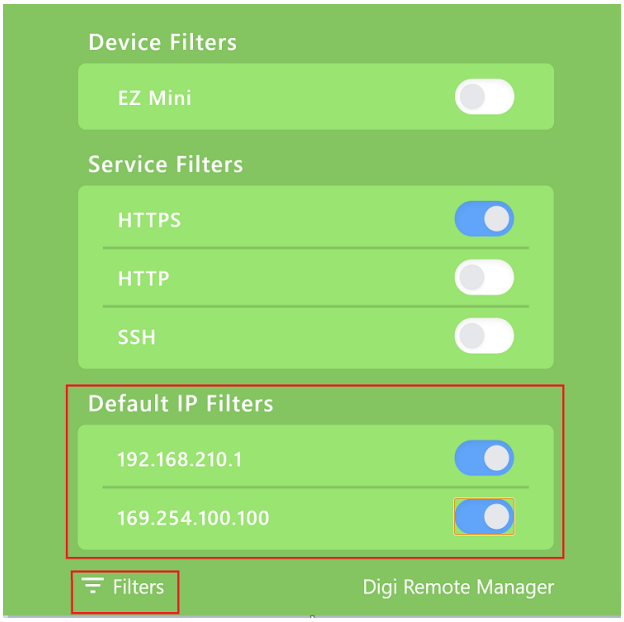


4. In the **Services Filters** section, click the enable button to enable the services that you want to use to find an IP address.
5. Click **Filters** at the bottom of the expanded toolbar to minimize the toolbar and hide the filters.

Discover the IP address when not on a network

If the Connect EZ device is directly connected to a computer or connected to a network with no DHCP server, a default IP address is found for the device. You can specify the filters used to find a default IP address.

1. Make sure your device is connected to the network and the Digi Navigator is installed.
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 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.

Manage the RealPort device list

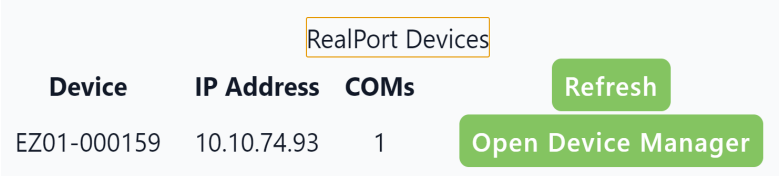
After you have enabled and configured RealPort on at least one Connect EZ device, a list of configured devices displays at the bottom of the **Digi Navigator** application screen. Using the available buttons, you can refresh the list and easily access the COM port configuration on your computer.

Refresh

Click **Refresh** to update the list of Connect EZ devices that have RealPort enabled and configured.

Open Device Manager

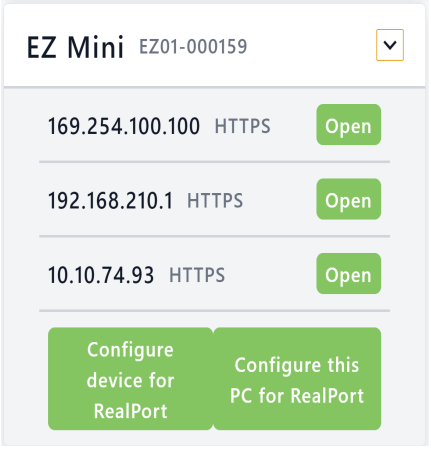
Click **Open Device Manager** to open the Windows **Properties** dialog on your computer to access the configured COM ports. The number of COM ports configured for RealPort matches the number of serial ports on the device.



Access the web UI from the Digi Navigator

You can access the web user interface for the device from the Digi Navigator.

1. Make sure you have the device powered and connected the device to your network or computer with an Ethernet cable. See Connect to and access the Digi Navigator.
2. Launch the **Digi Navigator**.
3. From the list of devices shown in the **Digi Navigator**, expand the device that you want to configure.

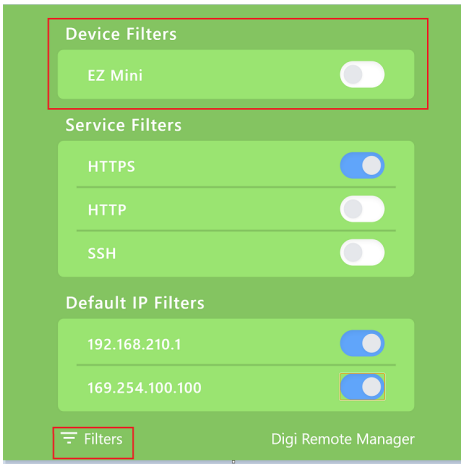


4. Click **Open** next to the IP address you want to use. The login screen for the web UI launches.
   a. Enter the user name and password for the Connect EZ in the **Username** and **Password** fields.
   b. Click **Login**.

Filter devices for display in the Digi Navigator

You can use the Digi Navigator filters to determine the types of Connect EZ devices you want to display. Only the devices that are powered on and connected to your network can be included in the Digi Navigator display.

1. Make sure you have the device powered and connected the device to your network or computer with an Ethernet cable. See Connect to and access the Digi Navigator.
2. Launch the **Digi Navigator**.
3. Click **Filters** from the green toolbar to expand the toolbar and display the filter options.



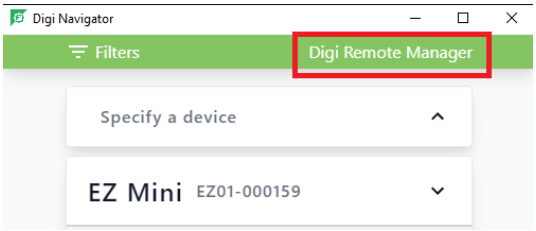
4. In the **Device Filters** section, a list of the Connect EZ types display. All types are disabled by default, and when all are disabled, all types are displayed.
5. To filter the types that are displayed, click the enable slider for the types you want to display. Only the enabled types will display, 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 Connect EZ.

For information about using Digi Remote Manager, refer to the *Digi Remote Manager User Guide*.

1. Make sure you have the device powered and connected the device to your network or computer with an Ethernet cable. See Connect to and access the Digi Navigator.
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**.

Wi-Fi

This chapter contains the following topics:

Wi-Fi configuration 216
Configure the Wi-Fi radio's channel 218
Configure the Wi-Fi radio to support DFS channels in client mode 219
Configure the Wi-Fi radio's band and protocol 221
Configure the Wi-Fi radio's transmit power 223
Configure an open Wi-Fi access point 224
Configure a Wi-Fi access point with personal security 229
Configure a Wi-Fi access point with enterprise security 236
Isolate Wi-Fi clients 243
Configure a Wi-Fi client and add client networks 249
Show Wi-Fi access point status and statistics 258
Show Wi-Fi client status and statistics 259

Wi-Fi configuration

Connect EZ device has Wi-Fi radio. You can configure the Wi-Fi radio for Wi-Fi access point mode or Wi-Fi client mode. By default, the Connect EZ radio is configured to use access point mode.

Default access point SSID and password

By default, the Connect EZ device has access point enabled. The default SSID for the access points is:

Digi-Connect EZ-*serial_number*

The password for the default access point is the unique password as found on the device's label. See Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point for information about changing the default SSID and password.

Default Wi-Fi configuration

The default Wi-Fi configuration of the Connect EZ device is:

- Wi-Fi radio:

	Default setting
Enabled or **disabled**	Disabled
Frequency band	2.4 GHz
TX power percentage	100
Access point mode	802.11b/g/n
Channel	Automatic
Channel width	20/40 MHz
Beacon interval	100

- Access point:

	Default setting
Name	Digi AP
Enabled or **disabled**	Enabled
SSID	Digi-Connect EZ-*serial_number*
SSID broadcast	Enabled
Encyrption	WAP2 Personal (PSK)
Pre-shared key	The unique password printed on the bottom label of the device.
Group rekey interval	10 minutes

- Client mode connections: none.

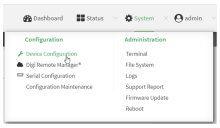
Configure the Wi-Fi radio's channel

By default, the Wi-Fi radio is configured to automatically select the best channel to use with respect to other Wi-Fi networks. You can configure a specific channel to use for the Wi-Fi radio by using the following steps.

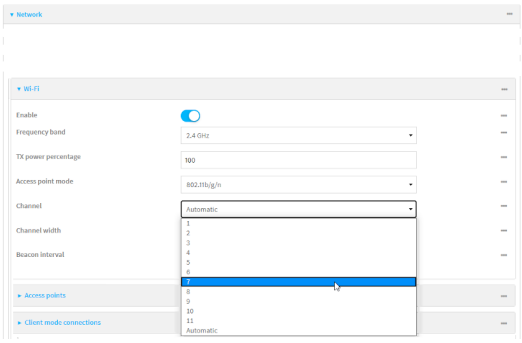
- **2.4 GHz band**—Channels 1 to 11 are supported. Channels 12, 13, and 14 are not supported.
- **5 GHz band**—By default, only non-Dynamic Frequency Selection (DFS) channels are supported. You can also enable support for DFS channels in client mode. See Configure the Wi-Fi radio to support DFS channels in client mode for information about enabling DFS support.

WebUI

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** > **WiFi**.
4. For **Channel**, select the channel. Only channels appropriate for the band are displayed.



5. 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. Set the channel for the radio:
   a. Determine the band for the radio:

```
(config)> network wifi radio phy0 band
2400mhz
(config)>
```

   b. Set the channel for the Wi-Fi radio:

```
(config)> network wifi radio phy0 2400mhz channel value
(config)>
```

   where *value* is:
   - For 2.4 GHz:
     - **1** through **11**
     - **auto**
   - For 5 GHz:
     - **36**
     - **40**
     - **44**
     - **48**
     - **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 Wi-Fi radio to support DFS channels in client mode

Dynamic Frequency Selection (DFS) is a mechanism for Wi-Fi connections to use 5 GHz frequencies that are normally reserved for non-Wi-Fi proposes. In addition to the standard non-DFS channels (36, 40, 44, and 48), your Connect EZ can be configured to have one or more Wi-Fi clients that can connect to external Wi-Fi access points that support DFS channels:

- DFS channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, and 144
- Higher 5GHz non-DFS channels 149, 153, 157, 161, and 165

The Wi-Fi access point must also support connections on these channels.

If DFS functionality is enabled, the Connect EZ must be rebooted after saving the configuration changes to re-initialize the Wi-Fi module.

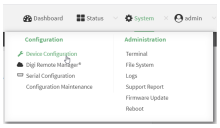
Note If DFS functionality is enabled, any access points enabled on the Connect EZ device will not be started.

Required configuration items

- Enable DFS support.
- One or more configured Wi-Fi clients. See Configure a Wi-Fi client and add client networks for details.

WebUI

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** > **WiFi**.
4. For **Frequency band**, select **5 GHz**.
5. Click to enable **DFS Client Support**.

Note When **DFS Client Support** is enabled, any enabled access points that use this radio will not be started and cannot be used as access points.

6. 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. Set the channel for the radio:
   a. Set the band for the radio to 5 GHz:

```
(config)> network wifi radio phy0 band 5000mhz
(config)>
```

   b. Enable DFS client support :

```
(config)> network wifi radio phy0 5000mhz dfs_client true
(config)>
```

   Note When DFS client support is enabled, any enabled access points that use this radio will not be started and cannot be used as access points.

4. Save the configuration and apply the change:

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

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

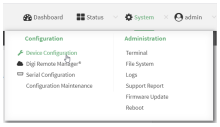
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the Wi-Fi radio's band and protocol

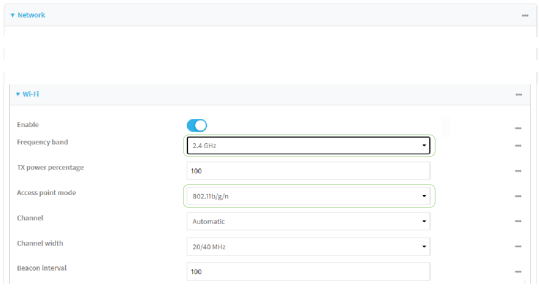
For Wi-Fi radios that support both 2.4 GHz and 5 GHz modes, you can configure the band. .

WebUI

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** > **WiFi**.
4. For **Frequency band**, select either **2.4 GHz** or **5 GHz**.
5. For **Access point mode**, select the appropriate mode. Only modes appropriate for the selected band are displayed.



6. 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. Set channel for the radio:
   a. Set the band for the radio:

```
(config)> network wifi radio phy0 band value
(config)>
```

   where *value* is either **2400mhz** or **5000mhz**.
   b. Set the mode for the Wi-Fi radio. For example:
      - If the Wi-Fi radio has a band of **2400mhz**:

```
(config)> network wifi radio phy0 2400mhz mode value
(config)>
```

        where *value* is one of **b**, **bg**, **bgn**, **g**, **gn**, or **n**.
      - If the Wi-Fi radio has a band of **5000mhz**:

```
(config)> network wifi radio phy0 5000mhz mode value
(config)>
```

        where *value* is one of **ac**, **acn**, or **n**.

4. Save the configuration and apply the change:

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

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

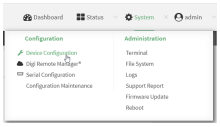
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the Wi-Fi radio's transmit power

The default Wi-Fi transmit power that the Wi-Fi radio will use when in access point or client mode is 100 percent. You can configure the Wi-Fi radio to transmit at a lower power.

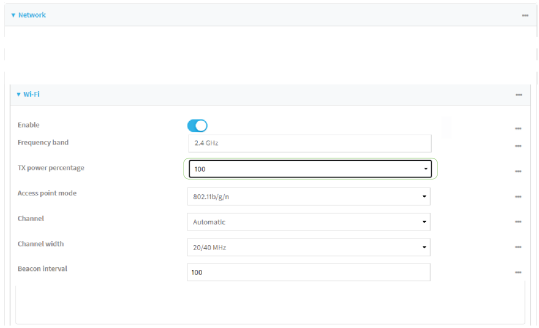
WebUI

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** > **WiFi**.
4. For **Tx power percentage**, type or select the appropriate percentage for the Wi-Fi radio's transmit power.



5. 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. Set the transmit power percentage for the radio:

   ```
   (config)> network wifi radio phy0 tx_power value
   (config)>
   ```

   where *value* is any integer between 1 and 100 and represents the percentage of transmit power that the Wi-Fi module should use.
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 an open Wi-Fi access point

This procedure configures a Wi-Fi access point that does not require a password for client connections.

By default, the Connect EZ device comes with one preconfigured access point, **Digi AP**. You cannot delete default access points, but you can modify them or you can create your own access points.

Required configuration items

- Enable the Wi-Fi access point
- The Service Set Identifier (SSID) for the access point.
- Configure open security for the access point.
- LAN/bridge assignment. Once you configure a Wi-Fi access point, you must assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

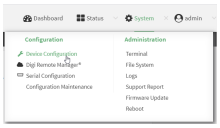
Additional configuration items

- Determine whether to broadcast the access point's SSID.
- Determine whether to isolate clients connected to this access point, so that they cannot communicate with each other.
- The amount of time to wait before changing the group key.

To configure a Wi-Fi access point with no security:

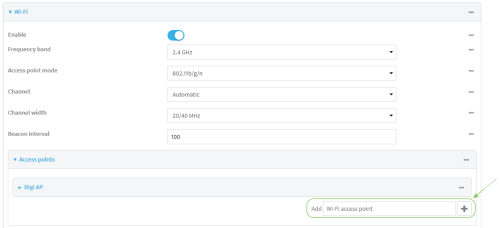
WebUI

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**.



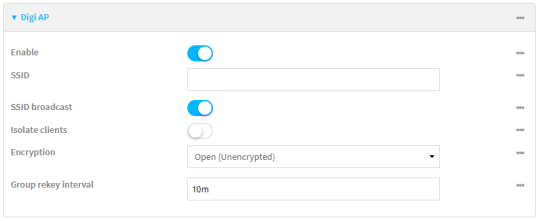
The **Configuration** window is displayed.

3. Click **Network** > **WiFi** > **Access points**.
4. Create a new access point or modify an existing access point:
   - To create a new access point, for **Add WiFi access point:**, type a name for the access point and click ✚.



   - To modify an existing access point, click to expand the access point.

The Wi-Fi access point configuration window is displayed.



5. For **SSID**, type the SSID. Up to 32 characters are allowed.
6. Enable **SSID broadcast** to configure the radio to broadcast the SSID.
7. (Optional) Enable **Isolate clients** to prevent clients that are connected to this access point from communicating with each other. See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.
8. For **Encryption**, select one of the following:
   - **Open (Unencrypted)** No encryption is used.
   - **WPA3 Enhanced Open (OWE)** Uses Opportunistic Wireless Encryption (OWE) technology to provide encryption for Wi-Fi networks that do not use password protection.

> **Note** Only select **WPA3 Enhanced Open (OWE)** if you know that all Wi-Fi clients connecting to this device will have WPA3 capabilities.

9. (Optional) For **Group rekey interval**, type the amount of time to wait before changing the group key.

   The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

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

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

   Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.
10. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

    The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.
11. Click **Apply** to save the configuration and apply the change.



Command line

Configure a new Access point

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 access point:

```
(config)> add network wifi ap new_AP
(config network wifi ap new_AP)>
```

   New access points are enabled by default.
4. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap new_AP)> ssid my_SSID
(config network wifi ap new_AP)>
```

   SSID broadcasting is enabled by default for new access points.

5. Set the security for the access point to an open security method:

```
(config network wifi ap new_AP)> encryption type value
(config network wifi ap new_AP)>
```

where *value* is either:

- **none**: No encryption is used.
- **owe**: Uses WPA3 Enhanced Open, which uses Opportunistic Wireless Encryption (OWE) technology to provide encryption for Wi-Fi networks that do not use password protection.

> **Note** Only select **owe** if you know that all Wi-Fi clients connecting to this device will have WPA3 capabilities.

6. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_clients true
(config)>
```

See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

7. (Optional) Set the amount of time to wait before changing the group key.

The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

```
(config network wifi ap new_AP)> encryption group_rekey value
(config network wifi ap new_AP)>
```

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

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

```
(config network wireless ap new_AP)> encryption group_rekey 600s
(config network wireless ap new_AP)>
```

Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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.

Edit an existing Access point

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. Show available access points:

```
(config)> network wifi ap ?

 Additional Configuration
 ------------------------------------------------------------------------
-------
 digi_ap                  Digi AP

(config)>
```

4. Set the SSID for the appropriate access point:

```
(config)> network wifi ap digi_ap ssid my_SSID
(config)>
```

5. SSID broadcasting is enabled by default for the preconfigured access points. If SSID broadcasting is disabled:

```
(config)> network wifi ap digi_ap ssid_broadcast true
(config)>
```

6. Set the security for the access point to an open security method:

```
(config network wifi ap new_AP)> encryption type value
(config network wifi ap new_AP)>
```

   where *value* is either:

   - **none**: No encryption is used.
   - **owe**: Uses WPA3 Enhanced Open, which uses Opportunistic Wireless Encryption (OWE) technology to provide encryption for Wi-Fi networks that do not use password protection.

     Note Only select **owe** if you know that all Wi-Fi clients connecting to this device will have WPA3 capabilities.

7. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_client true
(config)>
```

See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

8. (Optional) Set the amount of time to wait before changing the group key.

   The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

   ```
   (config)> network wifi ap digi_ap encryption group_rekey 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 **group rekey interval** to ten minutes, enter either **10m** or **600s**:

   ```
   (config)> network wireless ap digi_ap encryption group_rekey 600s
   (config)>
   ```

   Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

   The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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 a Wi-Fi access point with personal security

The WPA and WPA2 personal security modes allow a Wi-Fi access point to authenticate clients by using a preshared key that the client enters when connecting to the access point.

By default, the Connect EZ device comes with one preconfigured access point, **Digi AP**. You cannot delete default access points, but you can modify them or you can create your own access points.

Required configuration items

- Enable the Wi-Fi access point
- The Service Set Identifier (SSID) for the access point.

- Configure security for the access point to use personal security.
- The password (preshared key) that clients will used to connect to the access point.
- LAN/bridge assignment. Once you configure a Wi-Fi access point, you must assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

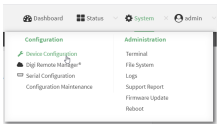
Additional configuration items

- Determine whether to broadcast the access point's SSID.
- Determine whether to isolate clients connected to this access point, so that they cannot communicate with each other.
- The amount of time to wait before changing the group key.

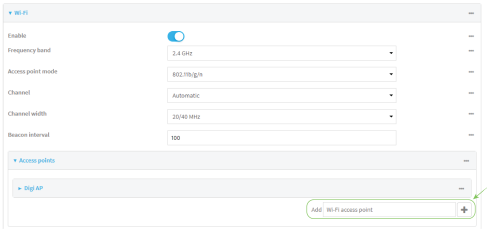
To configure a Wi-Fi access point to use personal security:

WebUI

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**.

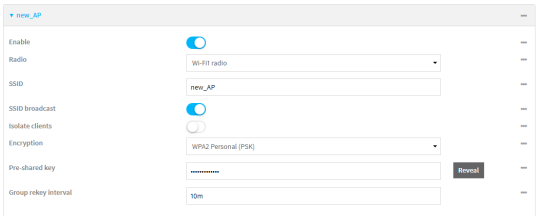


   The **Configuration** window is displayed.
3. Click **Network** > **WiFi** > **Access points**.
4. Create a new access point or modify an existing access point:
   - To create a new access point, for **Add WiFi access point:**, type a name for the access point and click ✚.



   - To modify an existing access point, click to expand the access point.

   The Wi-Fi access point configuration window is displayed.



5. For **SSID**, type the SSID. Up to 32 characters are allowed.

6. Enable **SSID broadcast** to configure the radio to broadcast the SSID.
7. (Optional) Enable **Isolate clients** to prevent clients that are connected to this access point from communicating with each other. See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.
8. For **Encryption**, select one of the following:
   - **WPA Personal (PSK)**: All Wi-Fi clients must support WPA to be able to authenticate.
   - **WPA/WPA2 Personal (PSK)**: Wi-Fi clients that support WPA and WPA2 are able to authenticate.
   - **WPA2 Personal (PSK)**: All Wi-Fi clients must support WPA2 to be able to authenticate.
   - **WPA2-PSK/WPA3-SAE mixed mode**: Wi-Fi clients that support WPA2 and WPA3 are able to authenticate.
   - **WPA3 Personal (SAE)**: All Wi-Fi clients must support WPA3 to be able to authenticate.

   Note Only select **WPA3 Personal (SAE)** if you know that all Wi-Fi clients connecting to this device will have WPA3 capabilities.
9. For **Pre-shared key**, enter the password that clients will use when connecting to the access point.
10. (Optional) For **Group rekey interval**, type the amount of time to wait before changing the group key.

    The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

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

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

    Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.
11. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

    The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.
12. Click **Apply** to save the configuration and apply the change.



Command line

Configure a new Access point

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 access point:

```
(config)> add network wifi ap new_AP
(config network wifi ap new_AP)>
```

   New access points are enabled by default.
4. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap new_AP)> ssid my_SSID
(config network wifi ap new_AP)>
```

   SSID broadcasting is enabled by default for new access points.
5. Set the security for the access point to a personal security option:

```
(config network wifi ap new_AP)> encryption type value
(config network wifi ap new_AP)>
```

   where *value* is one of:

   - **psk**: Uses WPA Personal (PSK). All Wi-Fi clients must support WPA to be able to authenticate.
   - **mixedpsk**: Uses mixed WPA/WPA2 Personal (PSK) mode. Wi-Fi clients that support WPA and WPA2 are able to authenticate.
   - **psk2**: Uses WPA2 Personal (PSK) mode. All Wi-Fi clients must support WPA2 to be able to authenticate.
   - **psk2sae**: Uses WPA2-PSK/WPA3-AES mixed mode. Wi-Fi clients that support WPA2 and WPA3 are able to authenticate.
   - **sae**: Uses WPA3 Personal mode. All Wi-Fi clients must support WPA3 to be able to authenticate.

```
(config network wifi ap new_AP)> encryption type psk2sae
(config network wifi ap new_AP)>
```

6. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_clients true
(config)>
```

   See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

7. Set the password that clients will use when connecting to the access point:

```
(config network wifi ap new_AP)> encryption key_type password
(config network wifi ap new_AP)>
```

where *key_type* varies depending on the selection for encryption **type**, above:

- If **type** is set to **psk**, *key_type* is **key_psk**.
- If **type** is set to **mixedpsk**, *key_type* is **key_mixedpsk**.
- If **type** is set to **psk2**, *key_type* is **key_psk2**.
- If **type** is set to **psk2sae**, *key_type* is **key_psk2sae**.
- If **type** is set to **sae**, *key_type* is **key_sae**.

For example, if **type** is set to **psk2sae**, set **key_psk2sae** to the appropriate password:

```
(config network wifi ap new_AP)> encryption type psk2sae
(config network wifi ap new_AP)> encryption key_psk2sae abcd1234
(config network wifi ap new_AP)>
```

Note The encryption key type must correspond to the configured encryption type. If you set an encyrption key type that does not correspond to the configured encryption type, you will not be able to save the configuration.

8. (Optional) Set the amount of time to wait before changing the group key.

The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

```
(config network wifi ap new_AP)> encryption group_rekey value
(config network wifi ap new_AP)>
```

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

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

```
(config network wireless ap new_AP)> encryption group_rekey 600s
(config network wireless ap new_AP)>
```

Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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.

Edit an existing Access point

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. Show available access points:

```
(config)> network wifi ap ?

 Additional Configuration
 ------------------------------------------------------------------------
-------
 digi_ap                  Digi AP

(config)>
```

4. Set the SSID for the appropriate access point:

```
(config)> network wifi ap digi_ap ssid my_SSID
(config)>
```

5. SSID broadcasting is enabled by default for the preconfigured access points. If SSID broadcasting is disabled:

```
(config)> network wifi ap digi_ap ssid_broadcast true
(config)>
```

6. Set the security for the access point to a personal security option:

```
(config network wifi ap new_AP)> encryption type value
(config network wifi ap new_AP)>
```

   where *value* is one of:

   - **psk**: Uses WPA Personal (PSK). All Wi-Fi clients must support WPA to be able to authenticate.
   - **mixedpsk**: Uses mixed WPA/WPA2 Personal (PSK) mode. Wi-Fi clients that support WPA and WPA2 are able to authenticate.
   - **psk2**: Uses WPA2 Personal (PSK) mode. All Wi-Fi clients must support WPA2 to be able to authenticate.
   - **psk2sae**: Uses WPA2-PSK/WPA3-AES mixed mode. Wi-Fi clients that support WPA2 and WPA3 are able to authenticate.

- **sae**: Uses WPA3 Personal mode. All Wi-Fi clients must support WPA3 to be able to authenticate.

```
(config network wifi ap new_AP)> encryption type psk2sae
(config network wifi ap new_AP)>
```

7. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_client true
(config)>
```

See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

8. Set the password that clients will use when connecting to the access point:

```
(config)> network wifi ap digi_ap encryption key_psk2 password
(config)>
```

9. (Optional) Set the amount of time to wait before changing the group key.

   The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

```
(config)> network wifi ap digi_ap encryption group_rekey 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 **group rekey interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network wireless ap digi_ap encryption group_rekey 600s
(config)>
```

Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

   The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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 a Wi-Fi access point with enterprise security

The WPA2 enterprise security mode allows a Wi-Fi access point to authenticate clients by using one or more RADIUS servers. When the Wi-Fi access point receives a connection request from a client, it authenticates the client with the RADIUS server before allowing the client to connect.

Using enterprise security modes allows each client to have different usernames and passwords configured in the RADIUS server, rather than using preshared key on the Connect EZ device.

By default, the Connect EZ device comes with one preconfigured access point, **Digi AP**. You cannot delete default access points, but you can modify them or you can create your own access points.

Required configuration items

- Enable the Wi-Fi access point
- The Service Set Identifier (SSID) for the access point.
- Configure security for the access point to WPA2 enterprise.
- The IP address for one or more RADIUS servers.
- The secret key for one or more RADIUS servers.
- LAN/bridge assignment. Once you configure a Wi-Fi access point, you must assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

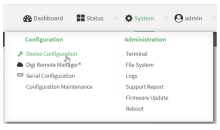
Additional configuration items

- Determine whether to broadcast the access point's SSID.
- Determine whether to isolate clients connected to this access point, so that they cannot communicate with each other.
- The server port for one or more RADIUS server.
- The amount of time to wait before changing the group key.

To configure a Wi-Fi access point with WPA2 enterprise security:

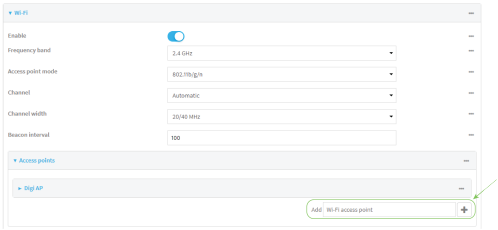
WebUI

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**.



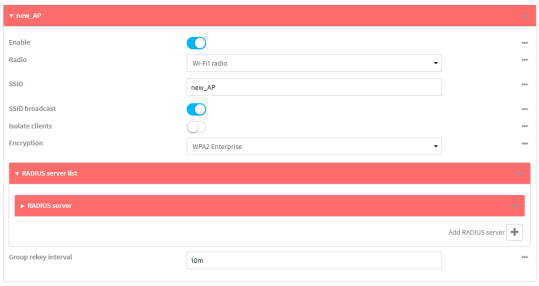
   The **Configuration** window is displayed.
3. Click **Network** > **WiFi** > **Access points**.

4. Create a new access point or modify an existing access point:
   - To create a new access point, for **Add WiFi access point:**, type a name for the access point and click ✚.

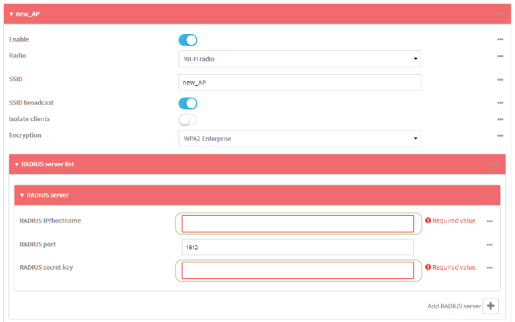


   - To modify an existing access point, click to expand the access point.

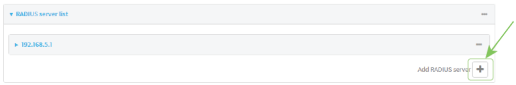
   The Wi-Fi access point configuration window is displayed.



5. For **SSID**, type the SSID. Up to 32 characters are allowed.
6. Enable **SSID broadcast** to configure the radio to broadcast the SSID.
7. (Optional) Enable **Isolate clients** to prevent clients that are connected to this access point from communicating with each other. See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.
8. For **Encryption**, select **WPA2 Enterprise**.
9. Configure one or more RADIUS servers:
   a. Click to expand **RADIUS server list**.
   b. Click to expand **RADIUS server**.
   c. For **RADIUS IP/hostname**, type the IP address or hostname of the RADIUS server.
   d. (Optional) Change the **RADIUS port**. The default port is 1812.
   e. For **RADIUS secret key**, type the secret key as configured on the RADIUS server.



f. To add additional RADIUS servers, click ✚



10. (Optional) For **Group rekey interval**, type the amount of time to wait before changing the group key.

    The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

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

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

    Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

11. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

    The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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



Command line

Configure a new Access point

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 access point:

```
(config)> add network wifi ap new_AP
(config network wifi ap new_AP)>
```

   New access points are enabled by default.

4. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap new_AP)> ssid my_SSID
(config network wifi ap new_AP)>
```

   SSID broadcasting is enabled by default for new access points.

5. Set the security for the access point to **wpa2**:

```
(config network wifi ap new_AP)> encryption type wpa2
(config network wifi ap new_AP)>
```

6. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_clients true
(config)>
```

   See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

7. Configure one or more RADIUS servers:
   a. Set the IP address of the RADIUS server:

```
(config network wifi ap new_AP)> encryption radius_servers 0 host IP_
address
(config network wifi ap new_AP)>
```

   b. Set the secret key as configured on the RADIUS server:

```
(config network wifi ap new_AP)> encryption radius_servers 0 key
secret_key
(config network wifi ap new_AP)>
```

   c. (Optional) Set the RADIUS server's port. The default is 1812.

```
(config network wifi ap new_AP)> encryption radius_servers 0 port port
(config network wifi ap new_AP)>
```

   d. (Optional) Add and configure additional radius servers:
      i. Add a server:

```
(config network wifi ap new_AP)> add encryption radius_servers end
(config network wifi ap new_AP encryption radius_servers 1)>
```

      ii. Configure the new server as described above. For example, set the server IP address:

```
(config network wifi ap new_AP encryption radius_servers 1)> host
IP_address
(config network wifi ap new_AP encryption radius_servers 1)>
```

      iii. Repeat for additional radius servers.

8. (Optional) Set the amount of time to wait before changing the group key.

The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

```
(config network wifi ap new_AP)> encryption group_rekey value
(config network wifi ap new_AP)>
```

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

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

```
(config network wireless ap new_AP)> encryption group_rekey 600s
(config network wireless ap new_AP)>
```

Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

   The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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.

Edit an existing Access point

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. Show available access points:

```
(config)> network wifi ap ?

 Additional Configuration
 ------------------------------------------------------------------------
-------
 digi_ap                  Digi AP
```

```
(config)>
```

4. Set the SSID for the appropriate access point:

```
(config)> network wifi ap digi_ap ssid my_SSID
(config)>
```

5. SSID broadcasting is enabled by default for the preconfigured access points. If SSID broadcasting is disabled:

```
(config)> network wifi ap digi_ap ssid_broadcast true
(config)>
```

6. Set the security for the access point to **wpa2**:

```
(config network wifi ap new_AP)> encryption type wpa2
(config network wifi ap new_AP)>
```

7. (Optional) Determine whether to prevent clients that are connected to this access point from communicating with each other:

```
(config)> network wifi ap digi_ap isolate_client true
(config)>
```

See Isolate Wi-Fi clients for information about how to prevent clients connected to different access points from communicating with each other.

8. Set the IP address or hostname of the RADIUS server:

```
(config)> network wifi ap digi_ap encryption host_wpa2 hostname
(config)>
```

9. Set the secret key as configured on the RADIUS server:

```
(config)> network wifi ap digi_ap encryption key_wpa2 secret_key
(config)>
```

10. (Optional) Set the RADIUS server's port. The default is 1812.

```
(config)> network wifi ap digi_ap encryption port_wpa2 port
(config)>
```

11. (Optional) Set the amount of time to wait before changing the group key.

The group key is shared by all in clients of the access point, and after a client has disconnected, it will be able to use the group key to decrypt broadcast packets until the key is changed.

```
(config)> network wifi ap digi_ap encryption group_rekey 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 **group rekey interval** to ten minutes, enter either **10m** or **600s**:

```
(config)> network wireless ap digi_ap encryption group_rekey 600s
(config)>
```

Increasing the time between rekeys can improve connectivity issues in noisy environments. To disable group rekeys, set to **0**. This will allow any client that has previously connected to see all broadcast traffic on the wireless network until the Wi-Fi radio is restarted. The default is 10 minutes.

1. Assign the Wi-Fi access point to a LAN interface or to a bridge. See Configure a LAN and Configure a bridge for more information.

   The access point must be assigned to an active LAN, or a bridge that is assigned to an active LAN.

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.

Isolate Wi-Fi clients

Client isolation prevents wireless clients connected to the Connect EZ device from communicating with other clients. There are two mechanisms for client isolation configuration:

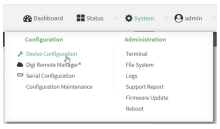
- Isolate clients connected to the same access point
- Isolate clients connected to different access points

This section provides instructions for both mechanisms.

Isolate clients connected to the same access point

WebUI

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** > **WiFi** > **Access points**.
4. Create a new access point or modify an existing access point. See Configure an open Wi-Fi access point, Configure a Wi-Fi access point with personal security, or Configure a Wi-Fi access point with enterprise security.
5. Enable **Isolate clients**.
6. 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 access point or modify an existing access point. See Configure an open Wi-Fi access point, Configure a Wi-Fi access point with personal security, or Configure a Wi-Fi access point with enterprise security.
4. (Optional) Set the client isolation:

```
(config)> network wifi ap digi_ap isolate_client true
(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.

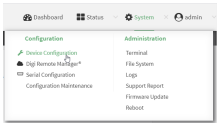
Isolate clients connected to different access points

Isolating clients that are on different access points involves the following steps:

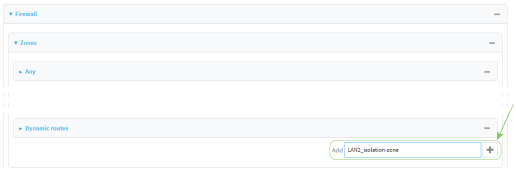
1. Assign the access points to separate LAN interfaces.
2. Assign those LAN interfaces to separate firewall zones.
3. Create firewall filters to prevent traffic between the two firewall zones.

WebUI

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. Configure the firewall:
   a. Click **Firewall** > **Zones**.
   b. In **Add Zone**, enter **LAN2_isolation_zone** for the name of the zone and click ✚.



Note We will be creating **LAN2** later in the procedure.

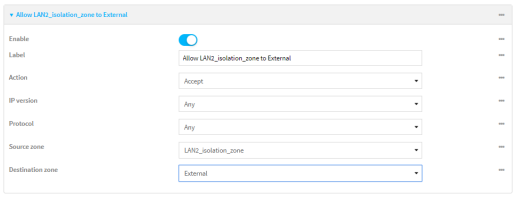
c. Create a firewall filter to provide internet access for the **LAN2_isolation_zone**:

i. For **Add packet filter**, click ✚.

ii. For **Label**, type **Allow LAN2_isolation_zone to External**.

iii. For **Source zone**, select **LAN2_isolation_zone**.

iv. For **Destination zone**, select **External**.



d. Create a firewall filter to drop traffic from the **Internal** zone (used by the **LAN1** interface) to the **LAN2_isolation_zone**:

i. Click **Firewall** > **Packet filtering**.

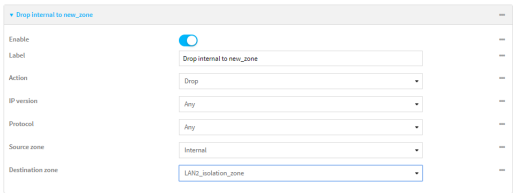
ii. For **Add packet filter**, click ✚.

iii. For **Label**, type **Drop traffic from Internal to LAN2_isolation_zone**.

iv. For **Action**, select **Drop**.

v. For **Source zone**, select **Internal**.

vi. For **Destination zone**, select **LAN2_isolation_zone**.



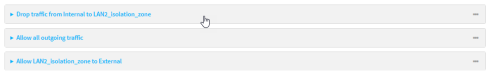
e. Rearrange the firewall filters.

Firewall filters are applied in the order that they are listed. As a result, in order to drop traffic from the **Internal** zone to the **LAN2_isolation_zone**, this filter must be listed prior to the **Allow all outgoing traffic filter**, which allows the **Internal** zone to have access to any zone.

To move the **Drop traffic from Internal to LAN2_isolation_zone** filter to the top of the list:

i. Click the filter title.

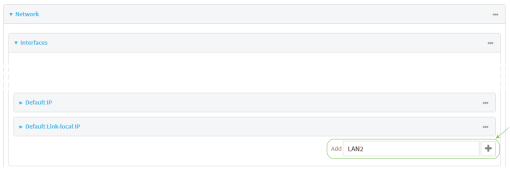
ii. Drag-and-drop the filter to the top of the list.



4. Create a new LAN:

By default, the Connect EZ device comes with one preconfigured LAN, which includes the default access point. We will use that LAN for the access point, and create a new LAN for the access point.

a. Click **Configuration** > **Network** > **Interfaces**.
b. For **Add interface**, type a name for the LAN and click ✚.



c. For **Zone**, select **LAN2_isolation_zone**.
d. For **Device**, select.
e. Click to expand **IPv4**.
f. For **Address**, type an IP address and subnet for the LAN.
g. Click to expand **DHCP server**.
h. **Enable** the DHCP server.

5. 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. Configure a new access point:
   a. Create a new access point:

```
(config)> add network wifi ap new_AP
(config network wifi ap new_AP)>
```

   New access points are enabled by default.

   b. Set the SSID for the Wi-Fi access point. Up to 32 characters are allowed.

```
(config network wifi ap new_AP)> ssid my_SSID
(config network wifi ap new_AP)>
```

   c. Set the security for the access point:

```
(config network wifi ap new_AP)> encryption type value
(config network wifi ap new_AP)>
```

   where value is one of:

- **none**
- **psk**
- **psk2**
- **wpa2**:

d. Complete other encryption-related fields as appropriate based on the type of encryption. See Configure an open Wi-Fi access point, Configure a Wi-Fi access point with personal security, or Configure a Wi-Fi access point with enterprise security for details.

4. Configure the firewall:

a. Return to the root config prompt by typing three periods (**...**):

```
(config network wifi ap new_AP)> ...
(config)>
```

b. Add a new firewall zone named **LAN2_isolation_zone**. We will be creating **LAN2** later in the procedure.

```
(config)> add firewall zone LAN2_isolation_zone
(config firewall zone LAN2_isolation_zone)>
```

c. Create a firewall filter to provide internet access for the **LAN2_isolation_zone**.

i. Return to the root config prompt by typing three periods (**...**):

```
(config firewall zone LAN2_isolation_zone)> ...
(config)>
```

ii. Add the new packet filter:

```
(config)> add firewall filter end
(config firewall filter 1)>
```

iii. Set the label for the filter:

```
(config firewall filter 1)> label "Allow LAN2_isolation_zone to
External"
(config firewall filter 1)>
```

iv. Set the source zone to **LAN2_isolation_zone**:

```
(config firewall filter 1)> src_zone LAN2_isolation_zone
(config firewall filter 1)>
```

v. Set the destination zone to **external**:

```
(config firewall filter 1)> dst_zone external
(config firewall filter 1)>
```

d. Create a firewall filter to drop traffic from the **Internal** zone (used by the **LAN1** interface) to the **LAN2_isolation_zone**:

Firewall filters are applied in the order that they are listed. As a result, in order to drop traffic from the **Internal** zone to the **LAN2_isolation_zone**, this filter must be added before the **Allow all outgoing traffic** filter, which allows the **Internal** zone to have access

to any zone. In this example, we will add the new to the first position in the list (index position **0**).

i. Add the new packet filter:

```
(config firewall filter 1)> add .. 0
(config firewall filter 0)>
```

ii. Set the label for the filter:

```
(config firewall filter 0)> label "Drop traffic from Internal to
LAN2_isolation_zone"
(config firewall filter 0>
```

iii. Set the source zone to **internal**:

```
(config firewall filter 0)> src_zone internal
(config firewall filter 0)>
```

iv. Set the destination zone to **LAN2_isolation_zone**:

```
(config firewall filter 0)> dst_zone LAN2_isolation_zone
(config firewall filter 0)>
```

v. Set the filter to drop traffic between the zones:

```
(config firewall filter 0)> action drop
(config firewall filter 0)>
```

5. Create a new LAN:

   By default, the Connect EZ device comes with one preconfigured LAN, which includes the default access point. We will use that LAN for the access point, and create a new LAN for the access point.

   a. Return to the root config prompt by typing three periods (**...**):

```
(config firewall filter 0)> ...
(config)>
```

   b. Add the new LAN:

```
(config)> add network interface LAN2
(config network interface LAN2)>
```

   c. Set the device to :

```
(config network interface LAN2)> device /network/wifi/ap/
(config network interface LAN2)>
```

   d. Set the zone to **LAN2_isolation_zone**:

```
(config network interface LAN2)> zone LAN2_isolation_zone
(config network interface LAN2)>
```

e. Set the IP address and subnet mask of the LAN:

```
(config network interface LAN2)> ipv4 address address/mask
(config network interface LAN2)>
```

f. Enable the DHCP server:

```
(config network interface LAN2)> ipv4 dhcp_server enable true
(config network interface LAN2)>
```

6. Save the configuration and apply the change:

```
(config network interface LAN2)> 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 Wi-Fi client and add client networks

Required configuration items

- Create the Wi-Fi client.
- The Connect EZ device's Wi-Fi radio that the Wi-Fi client will use.
- SSID of the access point that the client will log into.
- The encryption type used by the access point:
  - If a personal or mixed mode option is selected, identify the Pre-shared key.
  - If an enterprise option is selected:
    - Select the Extensible Authentication Protocol (EAP), one of:
      - TLS: Client certificate authentication.

        If TLS is selected, include:
        - The username.
        - The CA certificate in PEM format.
        - The client certificate in PEM format.
        - The private key in PEM format.
        - (Optional) The private key passphrase.
      - PEAP: Username/password authentication.

        If PEAP is selected, identify the username and password.
      - SCEP certificates: Simple Certificate Enrollment Protocol (SCEP) certificate management.

        If SCEP certificates is selected:

    - Identify the username.
    - Select the SCEP client. See Configure a Simple Certificate Enrollment Protocol client for information about SCEP clients.
- WAN assignment. Once you configure a Wi-Fi client, you must assign the Wi-Fi client to a WAN. See Wide Area Networks (WANs) and Wireless Wide Area Networks (WWANs) for further information.

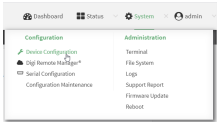
Additional configuration items

- Enable and configure background scanning, which allows the Wi-Fi client to move between access points that have the same SSID as their signal strength varies.
- Additional access points that client will attempt to use. If connection to one access point fails, the device will attempt to connect to the next access point in the list.

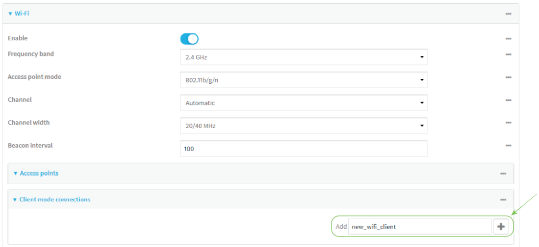
To configure a Wi-Fi client:

WebUI

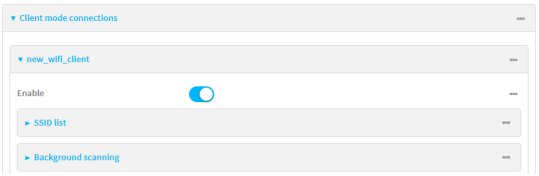
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **WiFi** > **Client mode connections**.
4. For **Add WiFi client:**, type the name of the client and click ✚.



   The Wi-Fi client configuration window is displayed.



   New Wi-Fi clients are enabled by default. To disable, or to enable a client if it has been disabled, click **Enable**.

5. Configure the Wi-Fi network that the client will use:
   a. Click to expand **SSID list**.
   b. Enter the **SSID** of the access point that the client will use to connect to the Wi-Fi network.
   c. Select the type of **Encryption** used by the access point.
      - If a personal or mixed mode is selected, for **Pre-shared key**, enter the password that the client will use to connect to the access point.
      - If **WPA2 Enterprise** is selected:
        - Select the **Extensible Authentication Protocol (EAP)**, one of:
          - **TLS**: Client certificate authentication.

            If **TLS** is selected, include:
            - The **Username**.
            - The **CA certificate** in PEM format.
            - The **Client certificate** in PEM format.
            - The **Private key** in PEM format.
            - (Optional) The **Private key passphrase**.
          - **PEAP**: Username/password authentication.

            If **PEAP** is selected, identify the **Username** and **Password**.
          - **SCEP certificates**: Simple Certificate Enrollment Protocol (SCEP) certificate management.

            If **SCEP certificates** is selected:
            - Identify the **Username**.
            - Select the **SCEP Client**. See Configure a Simple Certificate Enrollment Protocol client for information about SCEP clients.
6. (Optional) Configure **Background scanning**.

   Background scanning allows the device to scan for nearby access points and to move between access points that have the same SSID that is configured for the client connection, based on the signal strength of the access points.
   a. Click to expand **Background scanning**.



   b. Click **Enable background scanning** to enable.
   c. For **Scan threshold**, enter a value in dB that is used to determine the scanning frequency. The allowed value is an integer between-**113** and **0**.

      The **Scan threshold** works with the **Short interval** and **Long interval** options to determine how often the device should scan for available access points:
      - If the signal strength from the access point to which the client is currently connected is below the **Scan threshold**, it will use the **Short interval** to determine how often to scan for available access points.

- If the signal strength from the access point to which the client is currently connected is stronger the **Scan threshold**, it will use the **Long interval** to determine how often to scan for available access points.
- If **Short interval** and **Long interval** are set to the same value, **Scan threshold** is ignored. For example, the default configuration has both **Short interval** and **Long interval** set to **1** second, which means that the device will scan for access points once per second regardless of the **Scan threshold**.

d. For **Short interval**, type the number of seconds to wait between scans for access points, when the signal strength from the access point to which the client is currently connected is below the **Scan threshold**.

e. For **Long interval**, type the number of seconds to wait between scans for access points, when the signal strength from the access point to which the client is currently connected is stronger than the **Scan threshold**.

f. Click to expand **Scan frequencies list**.

The Connect EZ device has three preconfigured channels that will be scanned for available access points:

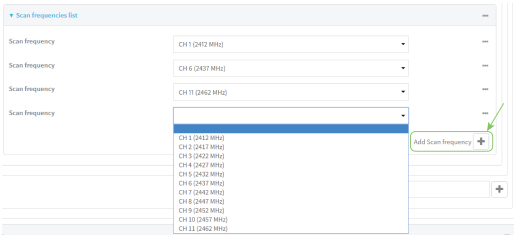
- Channel 1 (2412 MHz)
- Channel 6 (2437 MHz)
- Channel 11 (2462 MHz)

You can delete the preconfigured channels and add additional channels. At least one channel is required.

g. To delete a preconfigured channel, click the menu icon (**...**) next to the channel and select **Delete**.



h. To add a channel, click **Add Scan frequency** and select the appropriate channel.



7. 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 Wi-Fi client:

```
(config)> add network wifi client new_client
(config network wifi client new_client)>
```

   New clients are enabled by default.
4. Configure the Wi-Fi network that the client will use:
   a. Set the SSID of the access point that the client will use to connect to the Wi-Fi network:

```
(config network wifi client new_client)> ssid 0 ssid value
(config network wifi client new_client)>
```

      where *value* is the SSID of the access point.
   b. Set the encryption type for the access point:

```
(config network wifi client new_client)> ssid 0 encryption type value
(config network wifi client new_client)>
```

      where *value* is the type of encryption used by the access point. Allowed values are:
      - **none**: no encryption.
      - **owe**: WPA3 Enhanced Open, which uses Opportunistic Wireless Encryption (OWE) technology to provide encryption for Wi-Fi networks that do not use password protection.
      - **psk**: WPA personal encryption.
      - **mixedpsk**: Uses both WPA and WPA2 personal encryption.
      - **psk2**: WPA2 personal encryption.
      - **psk2sae**: Uses WPA2-PSK/WPA3-AES mixed mode.
      - **sae**: Uses WPA3 Personal mode.
      - **wpa2**: WPA2 enterprise encryption.
   c. If the type of encryption is set to:
      - **psk**, **mixedpsk**, **psk2**, **psk2sae**, or **sae**, set the password that the client will use to connect to the access point:

```
(config network wifi client new_client)> ssid 0 encryption key_
psk2 password
(config network wifi client new_client)>
```

- **wpa2**:
  i. Set the Extensible Authentication Protocol (EAP):

```
(config network wifi client new_client)> ssid 0 encryption
eap_type value
(config network wifi client new_client)>
```

  where *value* is one of:

  - **peap**: Username/password authentication. If **peap** is set:
    i. Set the username:

```
(config network wifi client new_client)> ssid 0
encryption id_wpa2 username
(config network wifi client new_client)>
```

    ii. Set the password:

```
(config network wifi client new_client)> ssid 0
encryption password_wpa2 password
(config network wifi client new_client)>
```

  - **scep**: Simple Certificate Enrollment Protocol (SCEP) certificate management. If **scep** is set:
    i. Set the username:

```
(config network wifi client new_client)> ssid 0
encryption id_wpa2 username
(config network wifi client new_client)>
```

    ii. Set the SCEP client:
      i. Use the **?** to determine available SCEP clients:

```
(config network wifi client new_client)> ssid 0
encryption scep_client ?

SCEP Client: The SCEP client which this Wi-Fi
client will use to download the
necessary keys and certificates from the SCEP
server.
Format:
  SCEP_test_client
  SCEP_test_client1
Current value:

(config network wifi client new_client)>
```

      ii. Set the SCEP client, for example:

```
(config network wifi client new_client)> ssid 0
encryption scep_client SCEP_test_client
(config network wifi client new_client)>
```

See Configure a Simple Certificate Enrollment Protocol client for information about SCEP clients.

- **tls**: Client certificate authentication. If **tls** is selected:
  i. Set the username:

```
(config network wifi client new_client)> ssid 0
encryption id_wpa2 username
(config network wifi client new_client)>
```

  ii. Set the CA certificate by using the **ca_cert** paramater and pasting the certificte in PEM format:

```
(config network wifi client new_client)> ssid 0
encryption ca_cert certificate
(config network wifi client new_client)>
```

  iii. Set the client certificate by using the **client_cert** paramater and pasting the certificte in PEM format:

```
(config network wifi client new_client)> ssid 0
encryption client_cert certificate
(config network wifi client new_client)>
```

  iv. Set the private key by using the **private_key** paramater and pasting the private key in PEM format:

```
(config network wifi client new_client)> ssid 0
encryption private_key key
(config network wifi client new_client)>
```

  v. (Optional) Set the private key passphrase:

```
(config network wifi client new_client)> ssid 0
encryption private_key_passphrase passphrase
(config network wifi client new_client)>
```

5. (Optional) Configure background scanning.

   Background scanning allows the device to scan for nearby access points and to move between access points that have the same SSID that is configured for the client connection, based on the signal strength of the access points.

   a. Enable background scanning:

```
(config network wifi client new_client)> background_scanning enable
true
(config network wifi client new_client)>
```

   b. Set the scan threshold (**bgscan_strength**), in dB, that is used to determine the scanning frequency.

```
(config network wifi client new_client)> bgscan_strength value
(config network wifi client new_client)>
```

where *value* is an integer between **-113** and **0**.

The scan threshold works with the short and long intervals (**bgscan_short_interval** and **bgscan_long_interval**) to determine how often the device should scan for available access points:

- If the signal strength from the access point to which the client is currently connected is below the value of **bgscan_strength**, it will use **bgscan_short_interval** to determine how often to scan for available access points.
- If the signal strength from the access point to which the client is currently connected is stronger than the value of **bgscan_strength**, it will use **bgscan_long_interval** to determine how often to scan for available access points.
- If **bgscan_short_interval** and **bgscan_long_interval** are set to the same value, **bgscan_strength** is ignored. For example, the default configuration has both **bgscan_short_interval** and **bgscan_long_interval** set to **1** second, which means that the device will scan for access points once per second regardless of the value of **bgscan_strength**.

c. Set the number of seconds to wait between scans for access points, when the signal strength from the access point to which the client is currently connected is below the value of **bgscan_strength**:

```
(config network wifi client new_client)> bgscan_short_interval value
(config network wifi client new_client)>
```

where value is any integer greater than 0. The default is **1**.

d. Set the number of seconds to wait between scans for access points, when the signal strength from the access point to which the client is currently connected is greater than the value of **bgscan_strength**:

```
(config network wifi client new_client)> bgscan_long_interval value
(config network wifi client new_client)>
```

where value is any integer greater than 0. The default is **1**.

e. Configure the frequencies that will be scanned for available access points.

The Connect EZ device has three preconfigured frequencies:

- 2412 MHz
- 2437 MHz
- 2462 MHz

You can delete the preconfigured frequencies and add additional frequencies. At least one frequencies is required.

f. To delete a preconfigured frequencies:

i. Use the **show** command to determine the index number of the channel to be deleted:

```
(config network wifi client new_client)> show background_scanning
scan_freq
```

```
0 2412
1 2437
2 2462
(config network wifi client new_client)>
```

ii. Use the appropriate index number to delete the channel. For example, to delete the 2412 frequency:

```
(config network wifi client new_client)> del 0
(config network wifi client new_client)>
```

g. To add a frequency:

i. Use the **?** with an existing index number to determine the allowed values for frequencies:

```
(config network wifi client new_client)> background_scanning scan_
freq 1

Scan frequency: Enable this frequency in the background scan.
Format:
  2412
  2417
  2422
  2427
  2432
  2437
  2442
  2447
  2452
  2457
  2462
Current value: 2437
```

ii. Add the appropriate frequency. For example, to add the **2457** frequency to the end of the list:

```
(config network wifi client new_client)> add background_scanning
scan_freq end 2457
(config network wifi client new_client)>
```

6. Save the configuration and apply the change:

```
(config network wireless client new_client)> 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 Wi-Fi access point status and statistics

You can show summary status for all Wi-Fi access points, and detailed status and statistics for individual Wi-Fi access points.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**.
3. Under **Connections**, click **Wi-Fi** > **Access Points**.

Command line

Show summary of Wi-Fi access points

To show the status and statistics for Wi-Fi access points, use the show wifi ap command.

1. Log into the Connect EZ command line as a user with Admin access.

   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 wifi ap**:

```
> show wifi ap

 AP        Enabled  Status  SSID           BSSID
 --------  -------  ------  -------------  -----------------
 my_AP     true     up      my_SSID        01:41:D1:14:36:37
 digi_ap   true     up      Digi2          00:40:D0:13:35:36

>
```

3. To view information about both active and inactive access points, include the **all** parameter:

```
> show wifi ap all

 AP        Enabled  Status  SSID           BSSID
 --------  -------  ------  -------------  -----------------
 my_AP     true     up      my_SSID        01:41:D1:14:36:37
 digi_ap   true     up      Digi2          00:40:D0:13:35:36
 digi_ap2  false    down

>
```

Show detailed status and statistics of a specific Wi-Fi access point

To show a detailed status and statistics of a Wi-Fi access point, use the **show wifi ap name *name*** command.

1. Log into the Connect EZ command line as a user with Admin access.

   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 wifi ap name *name***:

```
> show wifi ap name my_AP

 my_AP Access Point Status
 -------------------------
 Enabled                  : true
 Status                   : up

 SSID                     : my_AP
 Security                 : none

 Channel                  :
 Channel Width            :
 Radio                    : wifi
 BSSID                    : 01:41:D1:14:36:37

 Client             Signal  RX Bytes  TX Bytes  Uptime
 -----------------  ------  --_-----  --------  ------
 cc:c0:78:34:d5:a2  -68     260997    279481    801

>
```

Show Wi-Fi client status and statistics

You can show summary status for all Wi-Fi clients, and detailed status and statistics for individual Wi-Fi clients.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**.
3. Under **Connections**, click **Wi-Fi** > **Clients**.

Command line

Show summary of Wi-Fi clients

To show the status and statistics for Wi-Fi client, use the show wifi client command.

1. Log into the Connect EZ command line as a user with Admin access.

   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 wifi client**:

```
> show wifi client

 Client     Enabled  SSID      Status  Signal  MAC Address
 ---------  -------  --------  ------  ------  -----------------
 my_client  true     my_SSID   up      -43     91:fe:86:d1:0e:81
```

```
>
```

3. To view information about both active and inactive clients, include the **all** parameter:

```
> show wifi client all

Client     Enabled  SSID      Status  Signal  MAC Address
---------  -------  --------  ------  ------  -----------------
my_client  true     my_SSID   up      -43     91:fe:86:d1:0e:81
client2    true     SSID2     down
>
```

Show detailed status and statistics of a specific Wi-Fi client

To show a detailed status and statistics of a Wi-Fi client, use the **show wifi client name *name*** command.

1. Log into the Connect EZ command line as a user with Admin access.

   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 wifi cleint name *name***:

```
> show wifi client name my_client

 Client                  : my_client
 Enabled                 : true
 SSID                    : my_SSID
 Status                  : up
 Signal                  : -43
 MAC Address             : 91:fe:86:d1:0e:81
 Channel                 : 48
 Radio                   : wifi1
 TX Power                : 23
 Link Quality            : 67/70
 BSSID                   : 6D:B9:DD:BD:EE:C4

>
```

Hotspot

Your Connect EZ device offers the ability to create a publicly available hotspot, which allows you to provide internet access to users while restricting their ability to access other functionality on the Connect EZ device, as well as applying bandwidth limits, authenticating users, and other features. The Connect EZ device's implementation of hotspot uses a "captive portal" page—a web page that is displayed to users when they first connect to the hotspot and requires users to perform some specific action before they are granted access to the internet, such as accepting terms of use, logging in with a shared password or a username/password combination, or using a payment service to purchase web access via your hotspot.

Authentication of hotspot users can be performed by the device itself, by an external RADIUS server or other remote server, or by HotspotSystem (a cloud-based hotspot management and billing service). The device provides sample html pages to be used for authentication, and you can modify these pages, add your own pages, or host HTML login pages on a remote web server.

Note Sample HTML pages provided by your Connect EZ device are located in the **/etc/config/hotspot** directory on your device's filesystem. The files are created when you enable a hotspot and its associated access point or bridge for the first time, and cannot be accessed prior to that.

This chapter contains the following topics:

Hotspot authentication modes 262
Hotspot DHCP server 263
Hotspot security 263
Hotspot configuration 264
Show hotspot status and statistics 301
Customize the hotspot login page 304
Hotspot RADIUS attributes 309

Hotspot authentication modes

During hotspot configuration, you select one the following authentication modes for the hotspot:

- **Click-through**: Requires each user to accept the terms and conditions. The sample HTML page included with your Connect EZ device for click-through authentication is **terms.html**.

  See Create a new hotspot for information about configuring hotspot for click-through authentication.

- **Local shared password**: Requires each user to enter a password. This password is validated locally on the Connect EZ device, and the password is the same for all users. The sample HTML page included with your Connect EZ device for local shared password authentication is **password.html**.

  See Configure the hotspot to use local shared password authentication for information about configuring hotspot for local shared password authentication.

- **RADIUS shared password**: Requires each user to enter a password. This password is validated by an external RADIUS server, and the password is the same for all users. The RADIUS server should be "white listed" by including it in the **Walled garden** > **Allowed domains** or **Walled garden** > **Allowed subnets** setting for the hotspot, which allows unauthenticated hotspot clients to access the server for authentication. The sample HTML page included with your Connect EZ device for RADIUS shared password authentication is **password.html**.

  See Configure the hotspot to use RADIUS shared password authentication for information about configuring hotspot for RADIUS shared password authentication.

- **RADIUS users**: Requires each user to enter username and password credentials that are established on an external RADIUS server. The credentials are validated by the RADIUS server. The RADIUS server should be "white listed" by including it in the **Walled garden** > **Allowed domains** or **Walled garden** > **Allowed subnets** setting for the hotspot, which allows unauthenticated hotspot clients to access the server for authentication. The sample HTML page included with your Connect EZ device for RADIUS shared password authentication is **login.html**.

  See Configure the hotspot to use RADIUS users authentication for information about configuring hotspot for RADIUS users authentication.

- **HotspotSystem**: Requires each user to be authenticated by HotspotSystem, a cloud hotspot service that supports various free and paid authentication methods, including social media account, SMS, voucher, and PayPal. Domains needed for HotspotSystem authenticatiuon, payment options, and social media login should be "white listed" by including them in the **Walled garden** > **Allowed domains** or **Walled garden** > **Allowed subnets** setting for the hotspot, which allows unauthenticated hotspot clients to access them for authentication. When **HotspotSystem** is selected for the authentication mode, the browser is redirected to the **HotspotSystem** web page.

  See Configure the hotspot to use HotspotSystem authentication for information about configuring hotspot for HotspotSystem authentication.

Prior to authentication, a hotspot client that attempts to make an HTTP request to any domain other than those included in white-listed sites in the **Walled garden** > **Allowed domains** or **Walled garden** > **Allowed subnets** settings will be redirected to the login webpage. HTTPS requests will time out, because the hotspot cannot provide a valid SSL certificate for the requested domain. Requests made via any other protocol will also time out. Most operating systems will detect this scenario and automatically notify users to open the login page in a web browser.

Hotspot DHCP server

When the hotspot is enabled on the Connect EZ device, it automatically enables a DHCP server. During hotspot configuration, you assign an IPv4 address to the hotspot, and the DHCP server then uses the subnet of the hotspot's IP address, along with the hotspot's subnet mask, to assign IPv4 addresses to clients that connect to the hotspot.

To prevent the hotspot's DHCP server from assigning IP addresses that are already in use elsewhere in your local network, the hotspot must use a subnet that is not currently being used in your local network.

Hotspot security

A typical hotspot is an open network. This means that traffic transferred between the hotspot and the hotspot clients is not encrypted and can be intercepted by a packet sniffer or similar technology. However, the sample HTML login pages provided with your Connect EZ device use CHAP-MD5 authentication, providing a level of security during the authentication process. Additionally, websites that use the HTTPS protocol provide end-to-end encryption between the browser and the web server.

Hotspot clients are typically untrusted and only given access to the WAN interface on the device. The hotspot firewall zone settings prevent hotspot clients from accessing any of the other interfaces on the device (such as the LAN and VPN interfaces). Additionally, the hotspot zone prevents hotspot clients from accessing the device itself (for example, via the web interface or SSH).

Hotspot configuration

This section provides information about enabling and configuring the default hotspot that is provided with your Connect EZ installation, as well as creating a new hotspot and configuring the type of authentication mode you select for your hotspot.

This section contains the following topics:

Enable hotspot using the default configuration 265
Change the default hotspot SSID 269
Change the default hotspot IP address and subnet 270
Change the default hotspot bandwidth limits 273
Add an Ethernet port to the default hotspot 274
Use policy routes with hotspot 277
Create a new hotspot 278
Configure the hotspot to use local shared password authentication 289
Configure the hotspot to use RADIUS shared password authentication 291
Configure the hotspot to use RADIUS users authentication 294
Configure the hotspot to use HotspotSystem authentication 298

Enable hotspot using the default configuration

The default configuration of the Connect EZ device's hotspot is:

	Default configuration
Hotspot	■ Name: **hotspot** ■ Disabled ■ Authentication mode: Click-through ■ IP address: 10.1.0.1/24 ■ DHCP server: Automatically enabled ■ DHCP server lease range: 100-250 ■ Bandwidth limits: • Maximum download speed: 10000 Kbps • Maximum upload speed: 10000 Kbps
Bridge	■ Name: **hotspot_bridge** ■ Disabled ■ 2.4 GHz Wi-Fi access point: **Digi Hotspot AP (Wi-Fi1)**
Access points	■ Name: **Digi Hotspot AP (Wi-Fi1)** ■ Disabled ■ SSID: Digi Hotspot ■ Encryption: Open (unencrypted) ■ Hotspot access points should be set to open (unencrypted). See Hotspot security for further information.
LAN	■ Name: **LAN hotspot** ■ Disabled ■ Device: hotspot_bridge ■ IP address: 192.168.100.1/30 This IP address is not used by the hotspot or the hotspot's DHCP server. It must be a unique IP address that is not used elsewhere in your network. ■ DHCP server: Disabled ■ The hotspot will use the hotspot's DHCP server rather than the LAN's DHCP server.

To use the default hotspot with click-through authentication, enable the hotspot, the bridge, the access points, and the LAN.

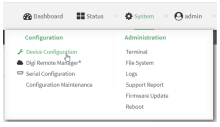
In additional to enabling the default hotspot configuration, you may also want to:

- Change the default hotspot SSID.
- Change the default authentication method:
  - Configure the hotspot to use local shared password authentication.
  - Configure the hotspot to use RADIUS shared password authentication.

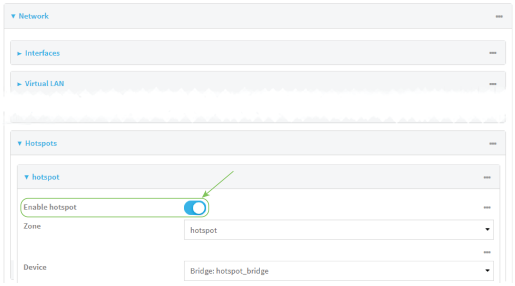
  - Configure the hotspot to use RADIUS users authentication.
  - Configure the hotspot to use HotspotSystem authentication.
- Change the default hotspot IP address and subnet.
- Modify the sample local HTML page that the Connect EZ device uses by default for click-through authentication. See Edit sample hotspot HTML pages for information.

WebUI

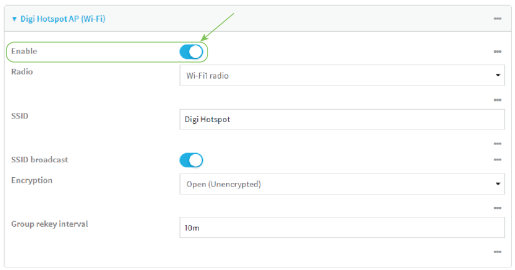
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Enable the hotspot:
   a. Click **Network** > **Hotspots** > **hotspot**.
   b. Click **Enable hotspot**.



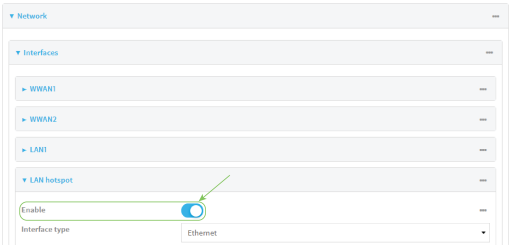
4. Enable the hotspot access points:
   a. Click **Network** > **Wi-Fi** > **Access points** > **Digi Hotspot AP (Wi-Fi1)**.
   b. Click **Enable**.



5. Enable the hotspot bridge:
   a. Click **Network** > **Bridges** > **hotspot_bridge**.
   b. Click **Enable**.



6. Enable the hotspot LAN:
   a. Click **Network** > **Interface** > **LAN** > **LAN hotspot**.
   b. Click **Enable**.



7. 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. Enable the hotspot:

```
(config)> network hotspot hotspot enable true
(config)>
```

4. Enable the hotspot access points:
5. Enable the hotspot bridge:

```
(config)> network bridge hotspot_bridge enable true
(config)>
```

6. Enable the hotspot LAN:

```
(config)> network interface lan_hotspot 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.

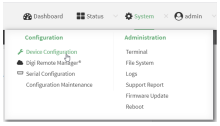
Change the default hotspot SSID

Required configuration items

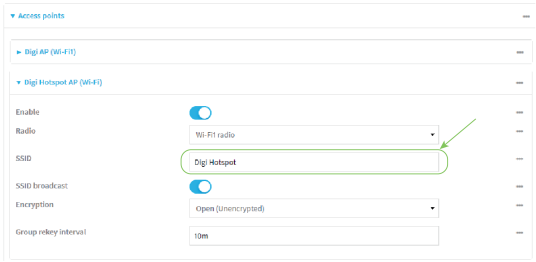
- Enable default hotspot configuration. See Enable hotspot using the default configuration for instructions.
- An SSID for the hotspot.

WebUI

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** > **Wi-Fi** > **Access points** > **Digi Hotspot AP (Wi-Fi1)**.
4. Change the default SSID, **Digi Hotspot**, to your preferred value.



5. 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. Change the SSID for **digi_hotspot_ap** to your preferred value:

```
(config)> network wifi ap digi_hotspot_ap ssid value
```

where *value* is a string of 1 to 32 characters. If the value contains spaces, enclose in quote marks (**"**).

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.

Change the default hotspot IP address and subnet

Required configuration items

- Enable default hotspot configuration. See Enable hotspot using the default configuration for instructions.
- An IP address and subnet for the hotspot.

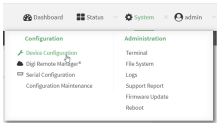
Additional configuration items

- Hotspot DHCP server settings:
  - Lease time.
  - Lease range start and end.

To change the default hotspot IP address and subnet:

WebUI

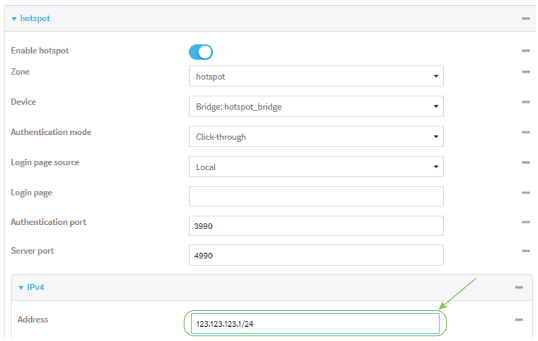
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Network** > **Hotspots** > **hotspot**.
4. Click to expand **IPv4**.

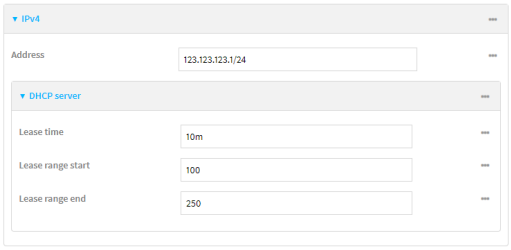
5. For **Address**, enter a new IP address and subnet mask.



6. (Optional) Change the default DHCP server configuration.

Note The hotspot DHCP server is automatically enabled and cannot be disabled.

a. Click to expand **DHCP server**.



b. For **Lease time**, type the amount of time that a client DHCP lease is valid. The default is 10 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 **Lease time** to ten minutes, enter **10m** or **600s**.

c. For **Lease range start**, type the lowest IP address in the range to assign to hotspot clients. The value entered here represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address. The default is **100**.

d. For **Lease range end**, type the highest IP address in the range to assign to hotspot clients. The value entered here represents the low order byte of the IP address, and when DHCP addresses are assigned to client, this number is combined with the subnet of the hotspot's static IP address. The default is **250**.

7. 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. Change the default hotspot IP address and subnet mask:

```
(config)> network hotspot hotspot ipv4 address ip_address/mask
(config)>
```

4. (Optional) Change the default DHCP server configuration.

   Note The hotspot DHCP server is automatically enabled and cannot be disabled.

   a. Set the amount of time that a client DHCP lease is valid:

```
(config)> network hotspot hotspot ipv4 address dhcp_server lease_time
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 **lease_time** to ten minutes, enter either **10m** or **600s**:

```
(config)> network hotspot hotspot ipv4 dhcp_server lease_time 600s
(config)>
```

   The default is 10 minutes.

   b. Set the lowest IP address in the range to assign to hotspot clients. This value represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address.

```
(config)> network hotspot hotspot ipv4 address dhcp_server lease_start
value
(config)>
```

   where *value* is any integer between **1** and **254**. The default is **100**.

   c. Set the highest IP address in the range to assign to hotspot clients. This value represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address.

```
(config)> network hotspot hotspot ipv4 address dhcp_server lease_end
value
(config)>
```

   where *value* is any integer between **1** and **254**. The default is **250**.

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.

Change the default hotspot bandwidth limits

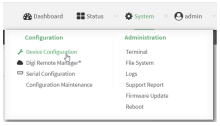
Required configuration items

- Enable default hotspot configuration. See Enable hotspot using the default configuration for instructions.
- Maximum download speed, in Kbps.
- Maximum upload speed, in Kbps.

To change the default hotspot IP address and subnet:

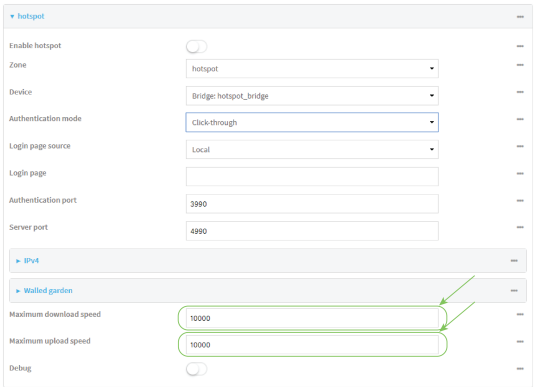
WebUI

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** > **Hotspots** > **hotspot**.
4. For **Maximum download speed**, type the maximum download speed in kilobytes per second (Kbps).
5. For **Maximum upload speed**, type the maximum upload speed in kilobytes per second (Kbps).



6. 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. Change the default maximum download speed:

```
(config)> network hotspot hotspot bandwidth_max_down value
(config)>
```

   where *value* is an integer between 1 and 100000 and represents the maximum download speed in Kbps.
4. Change the default maximum upload speed:

```
(config)> network hotspot hotspot bandwidth_max_up value
(config)>
```

   where *value* is an integer between 1 and 100000 and represents the maximum upload speed in Kbps.
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.

Add an Ethernet port to the default hotspot

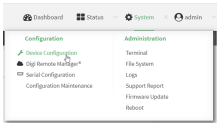
Required configuration items

- Enable default hotspot configuration. See Enable hotspot using the default configuration for instructions.
- Ethernet port to be added to the hotspot.

To add an Ethernet port to the default hotspot:

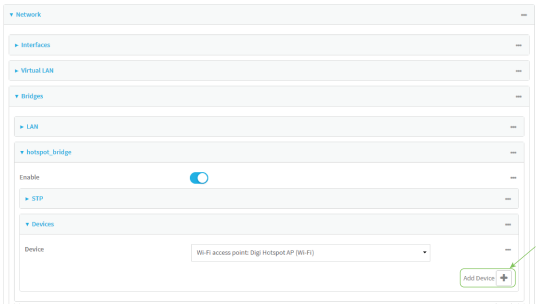
WebUI

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**.

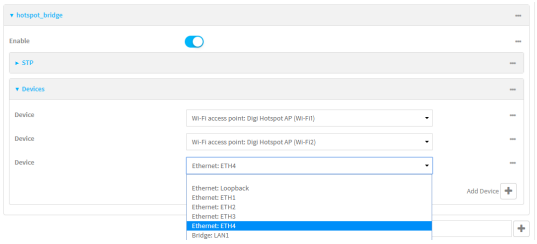


The **Configuration** window is displayed.

3. Click **Network** > **Bridges** > **hotspot_bridge** > **Devices**.
4. Click the **+** to add a new device.



5. By default, For **Device**, select the appropriate Ethernet port.



By default, the **ETH1** device is configured as the device for the **ETH1** interface, and **ETH2** is configured as a device in the **LAN1** bridge, which is used by the **ETH2** interface. As a result, when you add an Ethernet port to the hotspot, you may need to reconfigure the Ethernet port configuration for other interfaces. For example, to remove the **ETH2** port from the **LAN1** bridge:

a. Click **Network** > **Bridges** > **LAN1** > **Devices**.
b. Click the **...** menu icon next to the **Ethernet: ETH2** device entry and select **Delete**.



6. 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. Display a list of available devices by using the tab autocomplete feature:

```
(config)> add network bridge hotspot_bridge device end /network/<tab>
/network/device/eth1              /network/device/eth2
/network/device/loopback          /network/bridge/hotspot_bridge
/network/bridge/lan               /network/wifi/ap/digi_ap
/network/wifi/ap/digi_hotspot_ap
(config)> add network bridge hotspot_bridge device end /network/
```

4. Add a new device. For example, to add the **ETH2** device:

```
(config)> add network bridge hotspot_bridge device end
/network/device/eth2
(config)>
```

   By default, the **ETH1** device is configured as the device for the **ETH1** interface, and **ETH2** is configured as a device in the **LAN1** bridge, which is used by the **ETH2** interface. As a result, when you add an Ethernet port to the hotspot, you may need to reconfigure the Ethernet port configuration for other interfaces. For example, to remove the **ETH2** port from the **LAN1** bridge:

   a. Display the current **LAN1** bridge configuration:

```
(config)> show network bridge lan device
0 /network/device/eth2
1 /network/wifi/ap/digi_ap
(config)>
```

   b. Use the index number, **0**, to remove the **ETH2** device from the **LAN1** bridge:

```
(config)> del network bridge lan1 device 0
(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.

Use policy routes with hotspot

When creating policy routes for hotspots, the source address should be set to use the **hotspot** zone:

WebUI

1. Create a new routing policy. See Configure a routing policy for instructions.
2. During configuration, for **Source address**:
   a. For **Type**, select **Zone**.
   b. For **Zone**, select **hotspot**.
3. Click **Apply** to save the configuration and apply the change.



Command line

1. Create a new routing policy. See Configure a routing policy for instructions.
2. During configuration, set the source address type to **zone**:

```
(config network route policy 0)> src type zone
(config network route policy 0)>
```

3. Set the zone to **hotspot**:

```
(config network route policy 0)> src zone hotspot
(config network route policy 0)>
```

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.

Create a new hotspot

Required configuration items

- A device or bridge for the hotstpot.
  - If a bridge is used, it must be included in an interface with an assigned IP address.
- The authentication mode:
  - If **Local shared password** is selected for the authentication mode, include the password.
  - If **RADIUS shared password** or **RADIUS users** is selected for the authentication mode, include RADIUS configuration information.
  - If **HotspotSystem** is selected for the authentication mode, include HotspotSystem configuration information.

    See Hotspot authentication modes for more information about authentication modes.
- The login page source, either **Local** or **Remote**.
  - If **Remote** is selected, include the IP address of fully-qualified domain name of the remote web server that serves the login page.
- An IP address and subnet for the hotspot.

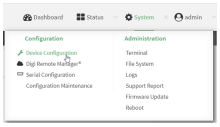
Additional configuration items

- If the login page source is **Local**, include the name of the local HTML file, if different than the default.
- If the login page source is **Remote**, include the shared secret that the remote server and the hotspot. Used with cloud-based hotspot providers.
- The **Authentication port** used by the hotspot.
- The **Server port** used by the hotspot.
- Hotspot DHCP server settings:
  - Lease time.
  - Lease range start and end.
- Walled garden configuration:
  - Domains that clients connected to the hotspot can access prior to the client being authenticated.
  - Subnets that clients connected to the hotspot can access prior to the client being authenticated.
- Maximum download speed, in Kbps.
- Maximum upload speed, in Kbps.
- Enable verbose logging.

To create a new hotspot:

WebUI

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. (Optional) Create new access points for the hotspot.

   You can also use existing access points for the hotspot. Access Points that are assigned to a hotspot or to a bridge used by a hotspot cannot be used for any other purpose.

   If more than one access point is being used by the hotspot, you must create a bridge that includes the access points.

   a. Click **Configuration** > **Network** > **WiFi** > **Access points**.
   b. For **Add WiFi access point:**, type a name for the access point and click ✚.
   c. For **Radio**, select the appropriate Wi-Fi radio.
   d. For **SSID**, type the SSID. Up to 32 characters are allowed.

      This will be the SSID used by clients to connect to the hotspot. If you are creating multiple access points, each access point must have the same SSID.
   e. For **Encryption**, select **Open (Unencrypted)**.

      Hotspot access points must use open (unencrypted) communication. See Hotspot security for more information.
   f. Add additional access points by following the above instructions.

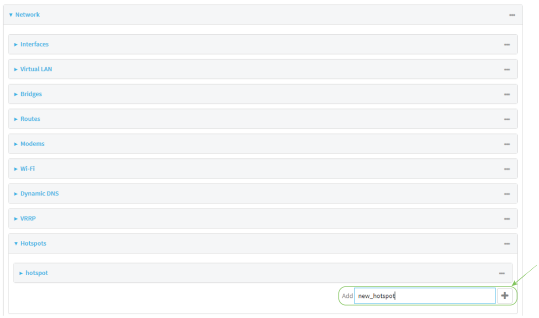
4. (Optional) Create a new bridge and interface for the hotspot.

   Note Hotspot bridges must also be part of an interface with a configured IP address.

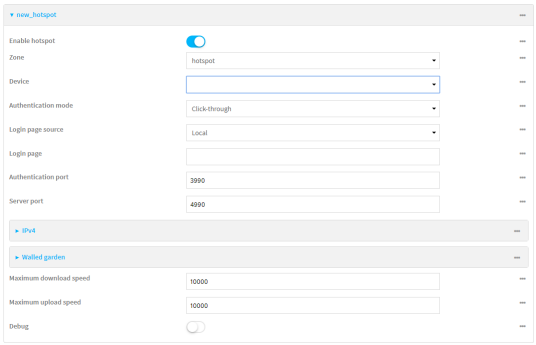
   a. Click **Network** > **Bridges**.
   b. For **Add Bridge:**, type a name for the bridge and click ✚.
   c. Add devices to the bridge:
      i. Click to expand **Devices**.
      ii. For **Add device**, click ✚.
      iii. Select the **Device**.
      iv. Repeat to add additional devices.
   d. Create an interface for the bridge:
      i. Click **Configuration** > **Network** > **Interfaces**.
      ii. For **Add Interface**, create a new interface and click ✚.
      iii. For **Device**, select the bridge created above.
      iv. Click to expand **IPv4**.
      v. For Address, enter an IP address and subnet mask for the LAN. This IP address must be unique from all other interfaces.

Note This IP address is not the IP address of the hotspot. The hotspot IP address is configured during hotspot configuration.

5. Click **Network** > **Hotspots**.
6. For **Add Hotspot**, enter a name for the hotspot and click ✚.



The new hotspot configuration appears.



7. Hotspots are enabled by default when they are created. To disable, click **Enable hotspot**.
8. For **Zone**, leave at the default setting of **hotspot**. The **hotspot** firewall zone provides the necessary firewall rules for hotspot functionality.
9. For **Device**, select an access point, and Ethernet port, or a bridge.
10. For **Authentication Mode**, select one of the following:
    - **Click-through**: Requires each user to accept the terms and conditions.
    - **Local shared password**: Requires each user to enter a password. This password is validated locally on the Connect EZ device, and the password is the same for all users.

      See Configure the hotspot to use local shared password authentication for information about configuring hotspot for local shared password authentication.
    - **RADIUS shared password**: Requires each user to enter a password. This password is validated by an external RADIUS server, and the password is the same for all users.

      See Configure the hotspot to use RADIUS shared password authentication for information about configuring hotspot for RADIUS shared password authentication.
    - **RADIUS users**: Requires each user to enter username and password credentials that are established on an external RADIUS server. The credentials are validated by the RADIUS server.

See Configure the hotspot to use RADIUS users authentication for information about configuring hotspot for RADIUS users authentication.

- **HotspotSystem**: Requires each user to be authenticated by HotspotSystem, a cloud hotspot service that supports various free and paid authentication methods, including social media account, SMS, voucher, and PayPal.

  See Configure the hotspot to use HotspotSystem authentication for information about configuring hotspot for HotspotSystem authentication.

11. For **Login page source**, select either:
    - **Local**: Uses an HTML page for authentication that is stored locally on the Connect EZ device's filesystem, in the **/etc/config/hotspot** directory. Note that the **hotspot** directory is not visible until hotspot has been enabled for the first time.
    - **Remote**: Uses an HTML page for authentication that is served by a remote web server.

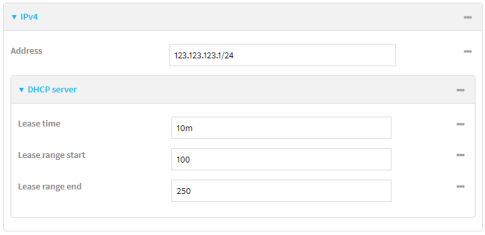
    This parameter is not available if **HotspotSystem** is selected for the **Authentication mode**.
12. (Optional) If **Local** is selected for **Login page source**, for **Login page**, type the name of the local HTML file used for authentication. This parameter is not available if **HotspotSystem** is selected for the **Authentication mode**.

    Normally, this field should be left blank, and the device will use the default authentication HTML page. See Hotspot authentication modes for information about the default authentication HTML page used for each authentication mode.

    If you upload a custom HTML file that uses a filename other than the default filename, type the custom filename here. See Upload custom hotspot HTML pages for more information about creating and uploading custom HTML files.
13. (Optional) For **Authentication port**, type the port number that the hotspot authentication server will used. The default is **3990**.
14. (Optional) For **Server port**, type the port number of the hotspot server. The default is **4990**.
15. If **Remote** is selected for **Login page source**, click to expand **Remote web server**.
    a. For **FQDN**, type the IP address or fully-qualified domain name or the remote web server that will be used for client authentication.
    b. (Optional) For **Secret**, type the shared secret that the remote server and the hotspot. Used with cloud-based hotspot providers.
    c. (Optional) Change the default DHCP server configuration.

    Note The hotspot DHCP server is automatically enabled and cannot be disabled.

    i. Click to expand **DHCP server**.

    ii. For **Lease time**, type the amount of time that a client DHCP lease is valid. The default is 10 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 **Lease time** to ten minutes, enter **10m** or **600s**.

iii. For **Lease range start**, type the lowest IP address in the range to assign to hotspot clients. The value entered here represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address. The default is **100**.

iv. For **Lease range end**, type the highest IP address in the range to assign to hotspot clients. The value entered here represents the low order byte of the IP address, and when DHCP addresses are assigned to client, this number is combined with the subnet of the hotspot's static IP address. The default is **250**.

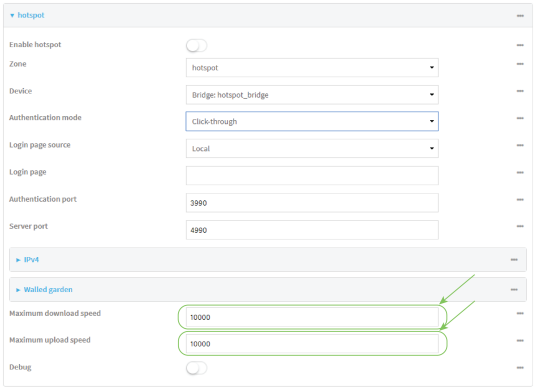
16. Click to expand **Walled garden**.

Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. If external servers are used for client authentication, such as a RADIUS server or HotspotSystem, they should be included in the walled garden settings. If **Remote** has been selected for **Login page source**, the domain for the web server that is being use to serve the remote HTML files must be included in the white list defined in these fields.

- To add domains that can be accessed by the client prior to authentication:
  a. Click to expand **Allowed domains**.
  b. Click ✚ to add a domain.
  c. For **Domain**, type the hostname of the allowed domain.
  d. Repeat to add additional domains.
- To add subnets that can be accessed by the client prior to authentication:
  a. Click to expand **Allowed subnets**.
  b. Click ✚ to add a subnet.
  c. For **Subnet**, type an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.
  d. Repeat to add additional subnets.

17. (Optional) For **Maximum download speed**, type the maximum download speed in kilobytes per second (Kbps).

18. (Optional) For **Maximum upload speed**, type the maximum upload speed in kilobytes per second (Kbps).



19. (Optional) Click **Debug** to enable verbose logging to the system log.

20. 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. (Optional) Create new access points for the hotspot.

   You can also use existing access points for the hotspot. Access Points that are assigned to a hotspot or to a bridge used by a hotspot cannot be used for any other purpose.

   If more than one access point is being used by the hotspot, you must create a bridge that includes the access points.

   a. Create a new access point:

```
(config)> add network wifi ap new_hotspot_AP1
(config network wifi ap new_hotspot_AP1)>
```

   New access points are enabled by default.

   b. Set the SSID:

```
(config network wifi ap new_hotspot_AP1)> ssid my_SSID
(config network wifi ap new_hotspot_AP1)>
```

   This will be the SSID used by clients to connect to the hotspot. If you are creating multiple access points, each access point must have the same SSID. Up to 32 characters are allowed.

   c. Set the encryption to open:

```
(config network wifi ap new_hotspot_AP1)> encryption type none
(config network wifi ap new_hotspot_AP1)>
```

   Hotspot access points must use open (unencrypted) communication. See Hotspot security for more information.

   d. Type **...** to return to the config prompt:

```
(config network wifi ap new_hotspot_AP1)> ...
(config)>
```

   e. Add additional access points by following the above instructions.

4. (Optional) Create a new bridge and interface for the hotspot.

Note Hotspot bridges must also be part of an interface with a configured IP address.

a. Create a bridge:

```
(config)> add network bridge new_hotspot_bridge
(config network bridge new_hotspot_bridge)>
```

b. Add devices to the bridge:

i. Determine available devices:

```
(config network bridge new_hotspot_bridge)> .. .. interface lan
device ?


Default value: /network/lan
Current value: /network/lan

(config network bridge new_hotspot_bridge)>
```

ii. Add the appropriate device. For example, to add the **Digi AP** Wi-Fi access point:

```
(config network bridge new_hotspot_bridge)> add device end
/network/wireless/ap/digi_ap
(config)>
```

c. Type **...** to return to the config prompt:

```
(config network bridge new_hotspot_bridge)> ...
(config)>
```

d. Create an interface for the bridge:

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

e. Add the new bridge to the interface:

```
(config network interface hotspot_bridge_interface)> device
/network/bridge/new_hotspot_bridge
(config network interface hotspot_bridge_interface)>
```

f. Set an IP address for the interface.

Note This IP address is not the IP address of the hotspot. The hotspot IP address is configured during hotspot configuration.

```
(config network interface hotspot_bridge_interface)> ipv4 address ip_
address/netmask
(config network interface hotspot_bridge_interface)>
```

g. Type **...** to return to the config prompt:

```
(config network interface hotspot_bridge_interface)> ...
(config)>
```

5. Create a new hotspot:

```
(config)> add network hotspot new_hotspot
(config network hotspot new_hotspot)>
```

New hotspots are enabled by default.

- To disable:

```
(config network hotspot new_hotspot)> enable false
(config network hotspot new_hotspot)>
```

- To enable, it it has been disabled:

```
(config network hotspot new_hotspot)> enable true
(config network hotspot new_hotspot)>
```

6. Add devices to the bridge:
   a. Determine available devices:

```
(config network bridge new_hotspot_bridge)> .. .. interface lan device
?


Default value: /network/lan
Current value: /network/lan

(config network bridge new_hotspot_bridge)>
```

   b. Add the appropriate device. For example, to add the **Digi AP** Wi-Fi access point:

```
(config network bridge new_hotspot_bridge)> add device end
/network/wireless/ap/digi_ap
(config)>
```

7. Set an access point, and Ethernet port, or a bridge for the hotspot's device:
   a. Determine available devices:

```
(config network hotspot new_hotspot)> device ?

Device: Device to use for this hotspot interface.
Format:
  /network/device/eth1
  /network/device/eth2
  /network/device/loopback
  /network/bridge/hotspot_bridge
  /network/bridge/lan
  /network/bridge/new_hotspot_bridge
```

```
  /network/wifi/ap/digi_ap
  /network/wifi/ap/digi_hotspot_ap
  /network/wifi/ap/new_hotspot_ap
Current value:

(config network hotspot new_hotspot)>
```

b. Add the device:

```
(config network hotspot new_hotspot)> device /network/bridge/new_
hotspot_bridge
(config network hotspot new_hotspot)>
```

8. Set the authentication mode:

```
(config network hotspot new_hotspot)> auth value
(config network hotspot new_hotspot)>
```

where *value* is one of:

- **click_through**: Requires each user to accept the terms and conditions.
- **local_shared_password**: Requires each user to enter a password. This password is validated locally on the Connect EZ device, and the password is the same for all users.

  See Configure the hotspot to use local shared password authentication for information about configuring hotspot for local shared password authentication.
- **radius_shared_password**: Requires each user to enter a password. This password is validated by an external RADIUS server, and the password is the same for all users.

  See Configure the hotspot to use RADIUS shared password authentication for information about configuring hotspot for RADIUS shared password authentication.
- **radius_user**: Requires each user to enter username and password credentials that are established on an external RADIUS server. The credentials are validated by the RADIUS server.

  See Configure the hotspot to use RADIUS users authentication for information about configuring hotspot for RADIUS users authentication.
- **hotspotsystem**: Requires each user to be authenticated by HotspotSystem, a cloud hotspot service that supports various free and paid authentication methods, including social media account, SMS, voucher, and PayPal.

  See Configure the hotspot to use HotspotSystem authentication for information about configuring hotspot for HotspotSystem authentication.

9. Set the login page source. (This option is not available if **auth** is set to **hotspotsystem**.)

```
(config network hotspot new_hotspot)> login value
(config network hotspot new_hotspot)>
```

where *value* is either:

- **local**: Uses an HTML page for authentication that is stored locally on the Connect EZ device's filesystem, in the **/etc/config/hotspot** directory. Note that the **hotspot** directory is not visible until hotspot has been enabled for the first time.
- **remote**: Uses an HTML page for authentication that is served by a remote web server.

10. (Optional) If **local** is selected for **login**, set the name of the local HTML file used for authentication. (This option is not available if **auth** is set to **hotspotsystem**.)

```
(config network hotspot new_hotspot)> local_page HTML_filename
(config network hotspot new_hotspot)>
```

Normally, this parameter should be left blank, and the device will use the default authentication HTML page. See Hotspot authentication modes for information about the default authentication HTML page used for each authentication mode.

If you upload a custom HTML file that uses a filename other than the default filename, type the custom filename here. See Upload custom hotspot HTML pages for more information about creating and uploading custom HTML files.

11. (Optional) Set the port number that the hotspot authentication server will used.

```
(config network hotspot new_hotspot)> auth_port port
(config network hotspot new_hotspot)>
```

The default is **3990**.

12. (Optional) Set the port number of the hotspot server.

```
(config network hotspot new_hotspot)> server_port port
(config network hotspot new_hotspot)>
```

The default is **4990**.

13. If **remote** is selected for **login**:

    a. Set the IP address or fully-qualified domain name or the remote web server that will be used for client authentication:

```
(config network hotspot new_hotspot)> remote url address
(config network hotspot new_hotspot)>
```

    a. (Optional) Set the shared secret that the remote server and the hotspot. Used with cloud-based hotspot providers.

```
(config network hotspot new_hotspot)> remote secret secret
(config network hotspot new_hotspot)>
```

14. (Optional) Change the default DHCP server configuration.

Note The hotspot DHCP server is automatically enabled and cannot be disabled.

    a. Set the amount of time that a client DHCP lease is valid:

```
(config network hotspot new_hotspot)> ipv4 address dhcp_server lease_
time value
(config network hotspot new_hotspot)>
```

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 **lease_time** to ten minutes, enter either **10m** or **600s**:

```
(config network hotspot new_hotspot)> ipv4 dhcp_server lease_time 600s
(config network hotspot new_hotspot)>
```

The default is 10 minutes.

b. Set the lowest IP address in the range to assign to hotspot clients. This value represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address.

```
(config network hotspot new_hotspot)> ipv4 address dhcp_server lease_
start value
(config network hotspot new_hotspot)>
```

where *value* is any integer between **1** and **254**. The default is **100**.

c. Set the highest IP address in the range to assign to hotspot clients. This value represents the low order byte of the IP address, and is combined with the subnet of the hotspot's static IP address.

```
(config network hotspot new_hotspot)> ipv4 address dhcp_server lease_
end value
(config network hotspot new_hotspot)>
```

where *value* is any integer between **1** and **254**. The default is **250**.

15. Set walled garden settings.

Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. If external servers are used for client authentication, such as a RADIUS server or HotspotSystem, they should be included in the walled garden settings.

- Add domains that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden domains end
domain_name
                                                    (config network hotspot new
```

Repeat to add additional domains.

- Add IP addresses and subnets that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden subnets end
value
                                          (config network hotspot new_hotspot)>
```

where *value* is an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.

Repeat to add additional IP addresses or subnets.

16. (Optional) Change the default maximum download speed:

```
(config network hotspot new_hotspot)> bandwidth_max_down value
(config network hotspot new_hotspot)>
```

where *value* is an integer between 1 and 100000 and represents the maximum download speed in Kbps.

17. (Optional) Change the default maximum upload speed:

```
(config network hotspot new_hotspot)> bandwidth_max_up value
(config network hotspot new_hotspot)>
```

where *value* is an integer between 1 and 100000 and represents the maximum upload speed in Kbps.

18. (Optional) Enable verbose logging to the system log:

```
(config network hotspot new_hotspot)> debug true
(config network hotspot new_hotspot)>
```

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 the hotspot to use local shared password authentication

Local shared password authentication requires each user to enter a password. This password is validated locally on the Connect EZ device, and the password is the same for all users.

By default, the router redirects unauthenticated users to the HTML authentication page located on the router at **etc/config/hotspot/password.html**. You can customize the authentication page as needed, or host an authentication page on a remote server. See Customize the hotspot login page for further information.

Required configuration items

- Create a new hotspot or Enable hotspot using the default configuration.
- Select local shared password authentication.
- The local password that will be used for authentication.

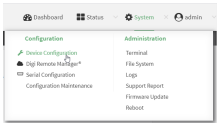
Additional configuration items

- Modify the local HTML authentication page, **/etc/config/hotspot/password.html**, or enter the name of an alternative HTML authentication page stored in the same directory, or identify a remote web server to host the HTML authentication page and include that server in the "white list" of servers that unauthenticated hotspot clients can access. See Customize the hotspot login page for further information.

Hotspot LAN configuration:

Configure hotspot for local shared password authentication from the WebUI

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. Create a new hotspot or Enable hotspot using the default configuration.
4. During hotspot configuration, for **Authentication mode**, select **Local shared password** .
5. For **Local shared password**, type the password that all users will be required to enter to authentication with the hotspot.
6. Click **Apply** to save the configuration and apply the change.



Configure hotspot for local shared password authentication from the 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 hotspot or Enable hotspot using the default configuration.
4. Set the authentication mode to **local-shared-password**:

```
(config)> network hotspot hotspot_name auth local-shared-password
(config)>
```

5. Set the password that all users will be required to enter to authentication with the hotspot:

```
(config)> network hotspot hotspot_name local_shared_password password
(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 the hotspot to use RADIUS shared password authentication

RADIUS shared password authentication requires each user to enter a password. This password is validated by an external RADIUS server, and the password is the same for all users.

Create a user on the RADIUS server with the username **guest**. The password assigned at the RADIUS server for the user **guest** is the shared password that your hotspot users should enter to authenticate to the hotspot via the RADIUS server.

By default, the router redirects unauthenticated users to the HTML authentication page located on the router at **etc/config/hotspot/password.html**. You can customize the authentication page as needed, or host an authentication page on a remote server. See Customize the hotspot login page for further information.

Required configuration items

- Create a new hotspot or Enable hotspot using the default configuration.
- Select RADIUS shared password authentication.
- IP address or hostname of the primary RADIUS server.
- A user on the RADIUS server with the username **guest**.
- RADIUS server secret.
- RADIUS NAS ID.
- Domain name or subnet of the RADIUS server included in the "white list" of servers that unauthenticated hotspot clients can access.

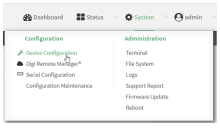
Additional configuration items

- IP address or hostname of the secondary RADIUS server to be used if the primary RADIUS server is unreachable.
- Modify the local HTML authentication page, **/etc/config/hotspot/password.html**, or enter the name of an alternative HTML authentication page stored in the same directory, or identify a remote web server to host the HTML authentication page and include that server in the "white list" of servers that unauthenticated hotspot clients can access. See Customize the hotspot login page for further information.

Hotspot LAN configuration:

Configure hotspot for RADIUS shared password authentication from the WebUI

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. Create a new hotspot or Enable hotspot using the default configuration.

4. During hotspot configuration, for **Authentication mode**, select **RADIUS shared password** .
5. Click to expand **Radius**.
   a. For **Primary server name**, enter the IP address or fully-qualified domain name of the primary RADIUS server to use to authenticate hotspot users.
   b. (Optional) For **Secondary server name**, enter the IP address or fully-qualified domain name of the backup RADIUS server to use to authenticate hotspot users if the primary RADIUS server is not available.
   c. (Optional) For **Port**, type the port number to use for RADIUS authentication requests. The default is **1812**.
   d. (Optional) For **Accounting port**, type the port number to use for RADIUS accounting requests. The default is **1813**.
   e. For **Secret**, enter the shared secret for the RADIUS server. This is configured on the RADIUS server.
   f. For **NAS ID**, enter the unique Network Access Server (NAS) identifier used by the RADIUS server. The default is **hotspot**.
   g. (Optional) Enable Swap Octets to swap the meaning of the input octets/packets and output octets/packets RADIUS attributes. This can fix issues if the data limits and/or accounting reports appear to be reversed on the RADIUS server. The default is disabled.
6. Click to expand **Walled garden**.

   Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of the RADIUS server(s) that are being used for authentication.

   - To add domains that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed domains**.
     b. Click ✚ to add a domain.
     c. For **Domain**, type the hostname of the allowed domain.
     d. Repeat to add additional domains.
   - To add subnets that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed subnets**.
     b. Click ✚ to add a subnet.
     c. For **Subnet**, type an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.
     d. Repeat to add additional subnets.
7. Click **Apply** to save the configuration and apply the change.



Configure hotspot for RADIUS shared password authentication from the 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 hotspot or Enable hotspot using the default configuration.
4. Set the authentication mode to **radius-shared-password**:

```
(config)> network hotspot hotspot_name auth radius-shared-password
(config)>
```

5. Configure the RADIUS server:
   a. Set the fully qualified domain name or IP address of the primary RADIUS server:

```
(config)> network hotspot hotspot_name radius primary_radius_server
address
(config)>
```

   b. (Optional) Set the fully qualified domain name or IP address of the secondary RADIUS server, used if the primary RADIUS server is unreachable:

```
(config)> network hotspot hotspot_name radius backup_radius_server
address
(config)>
```

   c. (Optional) Set the port number to use for RADIUS authentication requests.

```
(config)> network hotspot hotspot_name radius auth_port port
(config)>
```

   The default is **1812**.
   d. (Optional) Set the port number to use for RADIUS accounting requests.

```
(config)> network hotspot hotspot_name radius acct_port port
(config)>
```

   The default is **1813**.
   e. Set the shared secret for the RADIUS server. This is configured on the RADIUS server.

```
(config)> network hotspot hotspot_name radius secret secret
(config)>
```

   f. Set the unique Network Access Server (NAS) identifier used by the RADIUS server:

```
(config)> network hotspot hotspot_name radius nas_id id
(config)>
```

   The default is **hotspot**.

g. (Optional) Enable Swap Octets to swap the meaning of the input octets/packets and output octets/packets RADIUS attributes. This can fix issues if the data limits and/or accounting reports appear to be reversed on the RADIUS server:

```
(config)> network hotspot hotspot_name radius swap octets true
(config)>
```

The default is disabled.

6. Set walled garden settings.

Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of the RADIUS server(s) that are being used for authentication.

- Add domains that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden domains end
domain_name
(config network hotspot new_hotspot)>
```

Repeat to add additional domains.

- Add IP addresses and subnets that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden subnets end
value
(config network hotspot new_hotspot)>
```

where *value* is an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.

Repeat to add additional IP addresses or subnets.

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 the hotspot to use RADIUS users authentication

RADIUS users authentication requires each hotspot user to enter a username and password. Users are created on an external RADIUS server, and the username and password is validated by the external RADIUS server.

By default, the router redirects unauthenticated users to the HTML authentication page located on the router at **etc/config/hotspot/login.html**. You can customize the authentication page as needed, or host an authentication page on a remote server. See Customize the hotspot login page for further information.

Required configuration items

- Create a new hotspot or Enable hotspot using the default configuration.
- Select RADIUS users authentication.
- IP address or hostname of the primary RADIUS server.
- Users configured on the RADIUS server.
- RADIUS server secret.
- RADIUS NAS ID.
- Domain name or subnet of the RADIUS server included in the "white list" of servers that unauthenticated hotspot clients can access.

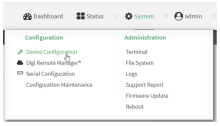
Additional configuration items

- IP address or hostname of the secondary RADIUS server to be used if the primary RADIUS server is unreachable.
- Modify the local HTML authentication page, **/etc/config/hotspot/login.html**, or enter the name of an alternative HTML authentication page stored in the same directory, or identify a remote web server to host the HTML authentication page and include that server in the "white list" of servers that unauthenticated hotspot clients can access. See Customize the hotspot login page for further information.

Hotspot LAN configuration:

Configure hotspot for RADIUS users authentication from the WebUI

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. Create a new hotspot or Enable hotspot using the default configuration.
4. During hotspot configuration, for **Authentication mode**, select **RADIUS users** .
5. Click to expand **Radius**.
   a. For **Primary server name**, enter the IP address or fully-qualified domain name of the primary RADIUS server to use to authenticate hotspot users.
   b. (Optional) For **Secondary server name**, enter the IP address or fully-qualified domain name of the backup RADIUS server to use to authenticate hotspot users if the primary RADIUS server is not available.
   c. (Optional) For **Port**, type the port number to use for RADIUS authentication requests. The default is **1812**.
   d. (Optional) For **Accounting port**, type the port number to use for RADIUS accounting requests. The default is **1813**.

e. For **Secret**, enter the shared secret for the RADIUS server. This is configured on the RADIUS server.

f. For **NAS ID**, enter the unique Network Access Server (NAS) identifier used by the RADIUS server. The default is **hotspot**.

g. (Optional) Enable Swap Octets to swap the meaning of the input octets/packets and output octets/packets RADIUS attributes. This can fix issues if the data limits and/or accounting reports appear to be reversed on the RADIUS server. The default is disabled.

6. Click to expand **Walled garden**.

   Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of the RADIUS server(s) that are being used for authentication.

   - To add domains that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed domains**.
     b. Click ✚ to add a domain.
     c. For **Domain**, type the hostname of the allowed domain.
     d. Repeat to add additional domains.
   - To add subnets that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed subnets**.
     b. Click ✚ to add a subnet.
     c. For **Subnet**, type an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.
     d. Repeat to add additional subnets.

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



Configure hotspot for RADIUS users authentication from the 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 hotspot or Enable hotspot using the default configuration.

4. Set the authentication mode to **radius-users**:

```
(config)> network hotspot hotspot_name auth radius-users
(config)>
```

5. Configure the RADIUS server:
   a. Set the fully qualified domain name or IP address of the primary RADIUS server:

```
(config)> network hotspot hotspot_name radius primary_radius_server
address
(config)>
```

   b. (Optional) Set the fully qualified domain name or IP address of the secondary RADIUS server, used if the primary RADIUS server is unreachable:

```
(config)> network hotspot hotspot_name radius backup_radius_server
address
(config)>
```

   c. (Optional) Set the port number to use for RADIUS authentication requests.

```
(config)> network hotspot hotspot_name radius auth_port port
(config)>
```

   The default is **1812**.

   d. (Optional) Set the port number to use for RADIUS accounting requests.

```
(config)> network hotspot hotspot_name radius acct_port port
(config)>
```

   The default is **1813**.

   e. Set the shared secret for the RADIUS server. This is configured on the RADIUS server.

```
(config)> network hotspot hotspot_name radius secret secret
(config)>
```

   f. Set the unique Network Access Server (NAS) identifier used by the RADIUS server:

```
(config)> network hotspot hotspot_name radius nas_id id
(config)>
```

   The default is **hotspot**.

   g. (Optional) Enable Swap Octets to swap the meaning of the input octets/packets and output octets/packets RADIUS attributes. This can fix issues if the data limits and/or accounting reports appear to be reversed on the RADIUS server:

```
(config)> network hotspot hotspot_name radius swap octets true
(config)>
```

   The default is disabled.

6. Set walled garden settings.

   Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of the RADIUS server(s) that are being used for authentication.

- Add domains that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden domains end
domain_name
(config network hotspot new_hotspot)>
```

  Repeat to add additional domains.

- Add IP addresses and subnets that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden subnets end
value
(config network hotspot new_hotspot)>
```

  where *value* is an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.

  Repeat to add additional IP addresses or subnets.

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 the hotspot to use HotspotSystem authentication

You can configure Connect EZ hotspot to use HotspotSystem, a cloud hotspot service that supports various free and paid authentication methods, including social media account, SMS, voucher, and PayPal.

By default, the router redirects unauthenticated users to the HTML authentication page located on the router at **etc/config/hotspot/login.html**. You can customize the authentication page as needed, or host an authentication page on a remote server. See Customize the hotspot login page for further information.

Required configuration items

- Create a new hotspot or Enable hotspot using the default configuration.
- Select HotspotSystem authentication.
- Create and configure a HotspotSystem account.
- The Operator name and location ID for the HotspotSystem.

Additional configuration items

- Modify the local HTML authentication page, **/etc/config/hotspot/login.html**, or enter the name of an alternative HTML authentication page stored in the same directory, or identify a remote web server to host the HTML authentication page and include that server in the "white

list" of servers that unauthenticated hotspot clients can access. See Customize the hotspot login page for further information.

Hotspot LAN configuration:

Configure a HotspotSystem account

1. Sign up for an operator account. Go to HotspotSystem signup.
2. Add a new location for the hotspot. Take care when selecting the Business Model because some options cannot be changed after you create the location. Go to Add a new location.
3. Click **Modify Hotspot Data & Settings**.
4. Click **Splash Page Settings**.
5. Set **Internal Login URL** to **http://{UAMIP}:{UAMPORT}/prelogin**.
6. Set **Internal Logout URL** to **http://{UAMIP}:{UAMPORT}/logoff**.
7. Click **Submit**.

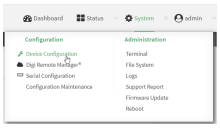
Configure allowed domains

HotspotSystem uses various additional domains for payment processing and social media login. While unauthorized users are automatically able to access **hotspotsystem.com**, your hotspot configuration may require unauthorized users to have access to additional domains. These domains need to be listed by the **Allowed garden** > **Allowed domains** option. For example, this may include sites like the following:

- **PayPal** and other payment processors require access to a number of domains, depending on which services you select. Contact HotspotSystem for an up-to-date list of domains that need to be whitelisted.
- **FREE Social login** requires a number of domains, depending on which services you select. Refer to the following page for an up-to-date list of social login domains that need to be whitelisted: Whitelist for hotspot free social login.

Configure hotspot for HotspotSystem authentication from the WebUI

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. Create a new hotspot or Enable hotspot using the default configuration.
4. During hotspot configuration, for **Authentication mode**, select **HotspotSystem**.

5. Click to expand **HotspotSystem**.
   a. For **Operator name**, type the operator name that you registered with **hotspotsystem.com**.
   b. For **Location ID**, type the location ID of this hotspot. The default is **1**.
6. Click to expand **Walled garden**.

   Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of supporting servers for payment or other external login and authentication (such as social media sites).

   - To add domains that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed domains**.
     b. Click ✚ to add a domain.
     c. For **Domain**, type the hostname of the allowed domain.
     d. Repeat to add additional domains.
   - To add subnets that can be accessed by the client prior to authentication:
     a. Click to expand **Allowed subnets**.
     b. Click ✚ to add a subnet.
     c. For **Subnet**, type an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.
     d. Repeat to add additional subnets.
7. Click **Apply** to save the configuration and apply the change.



Configure hotspot for HotspotSystem authentication from the 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 hotspot or Enable hotspot using the default configuration.
4. Set the authentication mode to **hotspotsystem**:

```
(config)> network hotspot hotspot_name auth hotspotsystem
(config)>
```

5. Configure **HotspotSystem**:
   a. Set the operator name that you registered with **hotspotsystem.com**.

```
(config)> network hotspot hotspot_name hotspotsystem operator name
(config)>
```

   b. Set the location ID of this hotspot.

```
(config)> network hotspot hotspot_name hotspotsystem location value
(config)>
```

   where *value* is any integer. The default is **1**.
6. Set walled garden settings.

   Walled garden settings define the "white list" of domains and subnets that unauthenticated clients are able to access. Include the domain or subnet of supporting servers for payment or other external login and authentication (such as social media sites).

   - Add domains that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden domains end
domain_name
(config network hotspot new_hotspot)>
```

     Repeat to add additional domains.
   - Add IP addresses and subnets that can be accessed by the client prior to authentication:

```
(config network hotspot new_hotspot)> add walled_garden subnets end
value
(config network hotspot new_hotspot)>
```

     where *value* is an IPv4 address and optional subnet mask, using the format *IPv4_address*[/*netmask*], or the keyword **any**.

     Repeat to add additional IP addresses or subnets.
7. Save the configuration and apply the change:

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

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

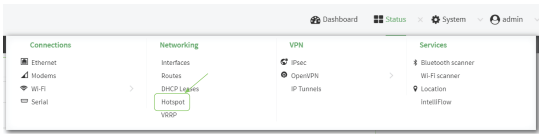
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show hotspot status and statistics

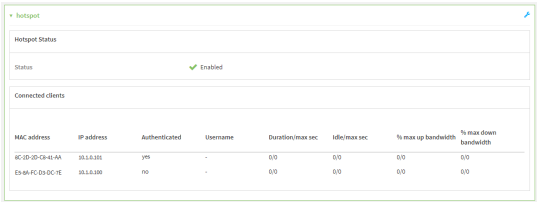
WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**

3. Under **Networking**, click **Hotspot**.



The **Hotspot** status page is displayed.



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 hotspot command at the Admin CLI prompt:

```
> show hotspot

 Hotspot      Enabled  Status  Device
 -----------  -------  ------  --------------
 hotspot      true     up      hotspot_bridge
 new_hotspot  false    down    new_hotspot_ap

>
```

3. Enter the **show hotspot name *hotspot_name*** command at the Admin CLI prompt to display information about clients connected to a specific hotspot:

```
> show hotspot name hotspot

 MAC Address        IP Address  Auth  Username  Duration/max sec
Idle/max sec  %/max up bandwidth  %/max down bandwidth
 -----------------  ----------  ----  --------  ----------------  -------
-----  ------------------  --------------------
 8C-2D-2D-C8-41-AA  10.1.0.101  yes   mariev    0/0               0/0
      0/0                 0/0
 E5-8A-FC-D3-DC-7E  10.1.0.100  no    -         0/0               0/0
      0/0                 0/0

>
```

4. Enter the **show hotspot ip *ip_address*** command at the Admin CLI prompt to display information about clients connected to a specific hotspot:

```
> show hotspot ip hotspot 10.1.0.101

 MAC Address        IP Address  Auth  Username  Duration/max sec
Idle/max sec  %/max up bandwidth  %/max down bandwidth
 -----------------  ----------  ----  --------  ----------------  -------
-----  ------------------  --------------------
 8C-2D-2D-C8-41-AA  10.1.0.101  yes   mariev    0/0               0/0
      0/0                 0/0

>
```

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.

Customize the hotspot login page

The Connect EZ device provides three sample HTML webpages for use with the hotspot feature. When hotspot is enabled for the first time, the sample webpages are installed to the **/etc/config/hotspot** folder on the device's filesystem. By default, the hotspot redirects users to one of the sample webpages based on the authentication mode being used. See Hotspot authentication modes for information about which HTML file is used for each authentication mode. The sample HTML webpages use **ChilliLibrary.js** to perform authentication. Do not modify **ChilliLibrary.js**.

You can customize the sample HTML pages, or replace them with your own page, so that hotspot users will be redirected to your custom HTML page when they log into the hotspot. You can also host the HTML pages on an external web server, rather than on the Connect EZ device. See Create a new hotspot for information about configuring the HTML page that the hotspot will use.

This section contains the following topics:

Edit sample hotspot HTML pages 305
Upload custom hotspot HTML pages 306
Restore hotspot default sample pages 308

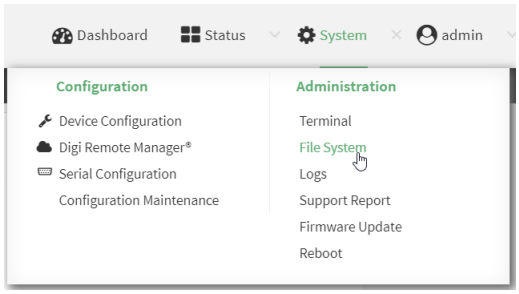
Edit sample hotspot HTML pages

To edit the sample HTML pages, download the files and edit the files on your local machine. After they have been edited, upload the edited files to the Connect EZ device.

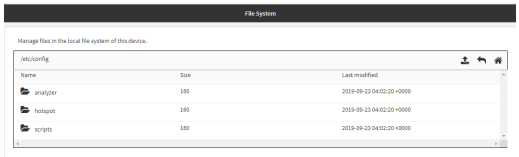
The edited HTML page should call the same JavaScript functions that the sample HTML pages do. Additional pages and assets can be uploaded to the hotspot folder, and additional subfolders can be created as needed. Supported file extensions include: .html, .gif, .js, .jpg, .mp4, .ogv, .png, .swf, .json, and .dat.

WebUI

1. Download the sample HTML file:
   a. Log into the Connect EZ WebUI as a user with Admin access.
   b. On the menu, click **System**. Under **Administration**, click **File System**.



   The **File System** page appears.



   c. Highlight the **hotspot** directory and click ↱ to open the directory.
   d. Select the HTML file you want to edit and click ⬇ (download).

> **Note** The files in the **hotspot** directory are only available after hotspot has been enabled for the first time.

2. On your local machine, edit the file as needed.
3. Upload the edited file:
   a. In the Connect EZWebUI, return to the **hotspot** directory.
   b. Click ⬆ (upload).
   c. Use the local file system to browse to the location of the edited HTML file. Select the file and click **Open** to upload the file.

Command line

Use the scp command to download and upload the sample HTML files using utilities.

1. Log into the Connect EZ command line as a user with Admin access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Download the file to your local machine. For example:

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/etc/config/hotspot/login.html to remote
admin@192.168.4.1's password: adminpwd
login.html
>
```

Note The files in the **hotspot** directory are only available after hotspot has been enabled for the first time.

3. On your local machine, edit the file as needed.
4. Upload the edited file from your local machine the the Connect EZ device. For example:

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/etc/config/hotspot/login.html to local
admin@192.168.4.1's password: adminpwd
login.html
>
```

Upload custom hotspot HTML pages

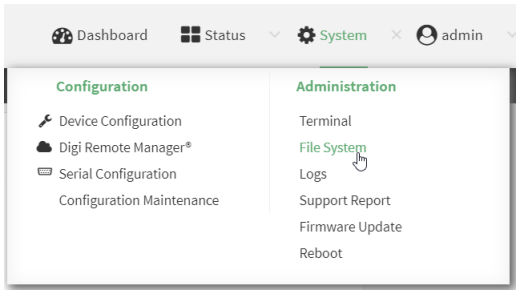
Rather than editing the sample HTML pages, you can upload a custom login page with a different filename.

The new page should include **ChilliLibrary.js** and call the same JavaScript functions that the sample HTML pages do. Additional pages and assets can be uploaded to the hotspot folder, and additional subfolders can be created as needed. Supported file extensions include: .html, .gif, .js, .jpg, .mp4, .ogv, .png, .swf, .json, and .dat.

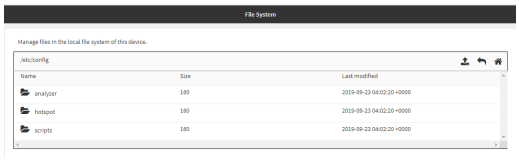
You can configure the Connect EZ device to use your custom HTML page using either the WebUI or the command line:

WebUI

1. Upload your custom HTML file to the Connect EZ device's filesystem:
   a. Log into the Connect EZ WebUI as a user with Admin access.
   b. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



c. Highlight the **hotspot** directory and click ↱ to open the directory.

d. Click ⬆ (upload).

e. Browse to the location of the HTML file on your local machine. Select the file and click **Open** to upload the file.

2. Configure the hotspot to use your custom HTML file:

a. On the menu, click **Network** > **Hotspot**.

b. Click the name of the appropriate hotspot to expand.

c. Ensure that **Login page source** is set to **Local**.

d. For **Login page**, type the name of your custom HTML file.

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



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the scp command to upload the edited file from your local machine the the Connect EZ device. For example:

```
> scp host 192.168.4.1 user admin remote /home/admin/temp/ local
/etc/config/hotspot/custom.html to local
```

3. Configure the hotspot to use your custom HTML file:

a. Type **config** to change to configuration mode:

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

b. Set **login** to **local-page**:

```
(config)> network hotspot hotspot_name login local
(config)>
```

c. Set **local-page** to your custom HTML file:

```
(config)> network hotspot hotspot_name local-page custom.html
```

d. Save the configuration and apply the change:

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

e. 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.

Restore hotspot default sample pages

If you have customized the sample HTML pages without making a backup of the samples, you may wish to restore the original version of the HTML pages without doing a factory reset.

The **hotspot** directory and files are loaded when the hotspot is enabled, and you can restore the default pages by doing the following:

1. Log into the Connect EZ command line as a user with Admin access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the mv command to change the name of the existing hotspot directory:

```
> mv /etc/config/hotspot /etc/config/hotspot_modified.
>
```

3. Use the WebUI or the command line to disable all hotspots and then reenable them. This will recreate the default hotspot directory. For example:

   a. Type **config** to change to configuration mode:

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

   b. Disable the hotspot:

```
(config)> network hotspot hotspot_name enabled false
(config)>
```

   c. Save the configuration and apply the change:

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

   d. Type **config** again to change to configuration mode:

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

   e. Reenable the hotspot:

```
(config)> network hotspot hotspot_name enabled true
(config)>
```

f. Save the configuration and apply the change:

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

g. 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.

Hotspot RADIUS attributes

The RADIUS server may send attributes to the hotspot to affect the operation of a client session. For example, here are some of the RADIUS attributes that the hotspot handles:

- Session-Timeout
- Idle-Timeout
- Acct-Interim-Interval
- WISPr-Redirection-URL
- WISPr-Session-Terminate-Time
- ChilliSpot-Max-Input-Octets
- ChilliSpot-Max-Output-Octets
- ChilliSpot-Max-Total-Octets

Also, if the RADIUS server requests it, the hotspot will send accounting information back to the RADIUS server. For example, here are some of the RADIUS attributes that the hotspot sends:

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Session-Time
- Acct-Input-Packets
- Acct-Output-Packets
- Acct-Input-Gigawords
- Acct-Output-Gigawords

Routing

This chapter contains the following topics:

IP routing 311
Show the routing table 327
Dynamic DNS 328
Virtual Router Redundancy Protocol (VRRP) 333

IP routing

The Connect EZ device uses IP routes to decide where to send a packet it receives for a remote network. The process for deciding on a route to send the packet is as follows:

1. The device examines the destination IP address in the IP packet, and looks through the IP routing table to find a match for it.
2. If it finds a route for the destination, it forwards the IP packet to the configured IP gateway or interface.
3. If it cannot find a route for the destination, it uses a default route.
4. If there are two or more routes to a destination, the device uses the route with the longest mask.
5. If there are two or more routes to a destination with the same mask, the device uses the route with the lowest metric.

This section contains the following topics:

Configure a static route 312
Delete a static route 314
Policy-based routing 316
Configure a routing policy 316
Routing services 324
Configure routing services 324

Configure a static route

A static route is a manually configured routing entry. Information about the route is manually entered rather than obtained from dynamic routing traffic.

Required configuration items

- The destination address or network.
- The interface to use to reach the destination.

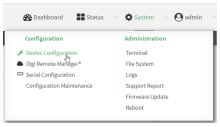
Additional configuration items

- A label used to identify this route.
- The IPv4 address of the gateway used to reach the destination.
- The metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.
- The Maximum Transmission Units (MTU) of network packets using this route.

To configure a static route:

WebUI

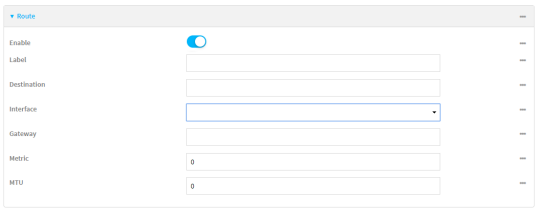
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **Routes** > **Static routes**.
4. Click the ✚ to add a new static route.



   The new static route configuration page is displayed:



   New static route configurations are enabled by default. To disable, click to toggle **Enable** to off.

5. (Optional) For **Label**, type a label that will be used to identify this route.
6. For **Destination**, type the IP address or network of the destination of this route.

   For example, to route traffic to the 192.168.47.0 network that uses a subnet mask of 255.255.255.0, type **192.168.47.0/24**. The **any** keyword can also be used to route packets to any destination with this static route.
7. For **Interface**, select the interface on the Connect EZ device that will be used with this static route.
8. (Optional) For **Gateway**, type the IPv4 address of the gateway used to reach the destination. Set to blank if the destination can be accessed without a gateway.
9. (Optional) For **Metric**, type the metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.
10. (Optional) For **MTU**, type the Maximum Transmission Units (MTU) of network packets using this route.
11. 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. Add a new static route:

```
(config)> add network route static end
(config network route static 0)>
```

   New static route instances are enabled by default. To disable:

```
(config network route static 0)> enable false
(config network route static 0)>
```

4. (Optional) set a label that will be used to identify this route. For example:

```
(config network route static 0)> label "route to accounting network"
(config network route static 0)>
```

5. Set the IP address or network of the destination of this route. For example:

```
(config network route static 0)> destination ip_address[/netmask]
(config network route static 0)>
```

For example, to route traffic to the 192.168.47.0 network that uses a subnet mask of 255.255.255.0:

```
(config network route static 0)> dst 192.168.47.0/24
(config network route static 0)>
```

The **any** keyword can also be used to route packets to any destination with this static route.

6. Set the interface on the Connect EZ device that will be used with this static route:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

   ```
   (config network route static 0)> interface /network/interface/eth1
   (config network route static 0)>
   ```

7. (Optional) Set the IPv4 address of the gateway used to reach the destination. Set to blank if the destination can be accessed without a gateway.

   ```
   (config network route static 0)> gateway IPv4_address
   (config network route static 0)>
   ```

8. (Optional) Set the metric for the route. When multiple routes are available to reach the same destination, the route with the lowest metric is used.

   ```
   (config network route static 0)> metric value
   (config network route static 0)>
   ```

   where *value* is an interger between **0** and **65535**. The default is **0**.

9. (Optional) Set the Maximum Transmission Units (MTU) of network packets using this route:

   ```
   (config network route static 0)> mtu integer
   (config network route static 0)>
   ```

10. Save the configuration and apply the change:

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

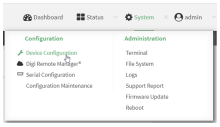
11. Type **exit** to exit the Admin CLI.

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

Delete a static route

WebUI

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** > **Routes** > **Static routes**.
4. Click the menu icon (**...**) for a static route and select **Delete**.



5. 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. Determine the index number of the static route to be deleted:

```
(config)> show network route static
0
    dst 10.0.0.1
    enable true
    no gateway
    interface /network/interface/lan1
    label new_static_route
    metric 0
    mtu 0
1
    dst 192.168.5.1
    enable true
    gateway 192.168.5.1
    interface /network/interface/lan2
    label new_static_route_1
```

```
    metric 0
    mtu 0
(config)>
```

4. Use the index number to delete the static route:

```
(config)> del network route static 0
(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.

Policy-based routing

Normally, a routing device determines how to route a network packet based on its destination address. However, you can use policy-based routing to forward the packet based on other criteria, such as the source of the packet. For example, you can configure the Connect EZ device so that high-priority traffic is routed through the cellular connection, while all other traffic is routed through an Ethernet (WAN) connection.

Policy-based routing for the Connect EZ device uses the following criteria to determine how to route traffic:

- Firewall zone (for example, internal/outbound traffic, external/inbound traffic, or IPSec tunnel traffic).
- Network interface (for example, the cellular connection, the WAN, or the LAN).
- IPv4 address.
- IPv6 address.
- MAC address.
- Domain.
- Protocol type (TCP, UDP, ICMP, or all).

The order of the policies is important. Routing policies are processed sequentially; as a result, if a packet matches an earlier policy, it will be routed using that policy's rules. It will not be processed by any subsequent rules.

Configure a routing policy

Required configuration items

- The packet matching parameters. It can any combination of the following:
  - Source interface.
  - Source address. This can be a firewall zone, an interface, a single IPv4/IPv6 address or network, or a MAC address.

- Destination address. This can be a firewall zone, an interface, a single IPv4/IPv6 address or network, or a domain.
- Protocol. This can be **any**, **tcp**, **udp** or **icmp**.
- Source port. This is only used if the protocol is set to **tcp** or **udp**.
- Destination port. This is only used if protocol is set to **tcp** or **udp**.

- The network interface used to reach the destination.

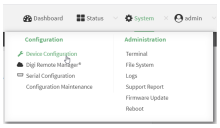
Additional configuration items

- A label for the routing policy.
- Whether packets that match this policy should be dropped when the gateway interface is disconnected, rather than forwarded through other interfaces.

To configure a routing policy:

WebUI

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** > **Routes** > **Policy-based routing**.
4. Click the ✚ to add a new route policy.



   The new route policy page is displayed:

   New route policies are enabled by default. To disable, click to toggle **Enable** to off.
5. (Optional) For **Label**, type a label that will be used to identify this route policy.
6. For **Interface**, select the interface on the Connect EZ device that will be used with this route policy.
7. (Optional) Enable **Exclusive** to configure the policy to drop packets that match the policy when the gateway interface is disconnected, rather than forwarded through other interfaces.
8. For **IP version**, select **Any**, **IPv4**, or **IPv6**.
9. For **Protocol**, select **Any**, **TCP**, **UDP**, or **ICMP**.
   - If **TCP** or **UDP** is selected for **Protocol**, type the port numbers of the **Source port** and **Destination port**, or set to **any** to match for any port.

- If **ICMP** is selected for **Protocol**, type the ICMP type and optional code, or set to **any** to match for any ICMP type.

10. For **DSCP**, type the 6-bit hexadecimal Differentiated Services Code Point (DSCP) field match criteria. This will match packets based on the DHCP field within the ToS field of the IP header.
11. Configure source address information:
    a. Click to expand **Source address**.
    b. For **Type**, select one of the following:
        - **Zone**: Matches the source IP address to the selected firewall zone. See Firewall configuration for more information about firewall zones.
        - **Interface**: Matches the source IP address to the selected interface's network address.
        - **IPv4 address**: Matches the source IP address to the specified IP address or network. Use the format ***IPv4_address***[**/*netmask***], or use **any** to match any IPv4 address.
        - **IPv6 address**: Matches the source IP address to the specified IP address or network. Use the format ***IPv6_address***[**/*prefix_length***], or use **any** to match any IPv6 address.
        - **MAC address**: Matches the source MAC address to the specified MAC address.
12. Configure the destination address information:
    a. Click to expand **Destination address**.
    b. For **Type**, select one of the following:
        - **Zone**: Matches the destination IP address to the selected firewall zone. See Firewall configuration for more information about firewall zones.
        - **Interface**: Matches the destination IP address to the selected interface's network address.
        - **IPv4 address**: Matches the destination IP address to the specified IP address or network. Use the format *IPv4_address*/[*netmask*], or use **any** to match any IPv4 address.
        - **IPv6 address**: Matches the destination IP address to the specified IP address or network. Use the format *IPv6_address*/[*prefix_length*], or use **any** to match any IPv6 address.
        - **Domain**: Matches the destination IP address to the specified domain names. To specify domains:
            i. Click to expand **Domains**.
            ii. Click the ✚ to add a domain.
            iii. For **Domain**, type the domain name.
            iv. Repeat to add additional domains.
        - **Default route**: Matches packets destined for the default route, excluding routes for local networks.
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. Add a new routing policy:

```
(config)> add network route policy end
(config network route policy 0)>
```

   New route policies are enabled by default. To disable:

```
(config network route policy 0)> enable false
(config network route policy 0)>
```

4. (Optional) Set the label that will be used to identify this route policy:

```
(config network route policy 0)> label "New route policy"
(config network route policy 0)>
```

5. Set the interface on the Connect EZ device that will be used with this route policy:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config network route policy 0)> interface /network/interface/eth1
(config network route policy 0)>
```

6. (Optional) Enable **exclusive** to configure the policy to drop packets that match the policy when the gateway interface is disconnected, rather than forwarded through other interfaces:

```
(config network route policy 0)> exclusive true
(config network route policy 0)>
```

7. Select the IP version:

```
(config network route policy 0)> ip_version value
(config network route policy 0)>
```

   where *value* is one of **any**, **ipv4**, or **ipv6**.

8. Set the protocol:

```
(config network route policy 0)> protocol value
(config network route policy 0)>
```

where *value* is one of:

- **any**: All protocols are matched.
- **tcp**: Source and destination ports are matched:
  a. Set the source port:

```
(config network route policy 0)> src_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the source port.
  b. Set the destination port:

```
(config network route policy 0)> dst_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the destination port.
- **upd**: Source and destination ports are matched:
  a. Set the source port:

```
(config network route policy 0)> src_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the source port.
  b. Set the destination port:

```
(config network route policy 0)> dst_port value
(config network route policy 0)>
```

  where *value* is the port number, or the keyword **any** to match any port as the destination port.
- **icmp**: The ICMP protocol is matched. Identify the ICMP type:

```
(config network route policy 0)> icmp_type value
(config network route policy 0)>
```

  where *value* is the ICMP type and optional code, or set to **any** to match for any ICMP type.

9. Set the source address type:

```
(config network route policy 0)> src type value
(config network route policy 0)>
```

where *value* is one of:

- **zone**: Matches the source IP address to the selected firewall zone. Set the zone:
  a. Use the **?** to determine available zones:

```
(config network route policy 0)> src zone ?

Zone: Match the IP address to the specified firewall zone.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup

Default value: any
Current value: any

(config network route policy 0)> src zone
```

  b. Set the zone. For example:

```
(config network route policy 0)> src zone external
(config network route policy 0)>
```

  See Firewall configuration for more information about firewall zones.
- **interface**: Matches the source IP address to the selected interface's network address. Set the interface:
  a. Use the **?** to determine available interfaces:
  b. Set the interface. For example:

```
(config network route policy 0)> src interface
/network/interface/eth1
(config network route policy 0)>
```

- **address**: Matches the source IPv4 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> src address value
(config network route policy 0)>
```

  where value uses the format ***IPv4_address***[**/*netmask***], or **any** to match any IPv4 address.
- **address6**: Matches the source IPv6 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> src address6 value
(config network route policy 0)>
```

where value uses the format ***IPv6_address***[**/*prefix_length***], or **any** to match any IPv6 address.

- **mac**: Matches the source MAC address to the specified MAC address. Set the MAC address to be matched:

```
(config network route policy 0)> src mac MAC_address
(config network route policy 0)>
```

10. Set the destination address type:

```
(config network route policy 0)> dst type value
(config network route policy 0)>
```

where *value* is one of:

- **zone**: Matches the destination IP address to the selected firewall zone. Set the zone:
  a. Use the **?** to determine available zones:

```
(config network route policy 0)> dst zone ?

Zone: Match the IP address to the specified firewall zone.
Format:
  any
  dynamic_routes
  edge
  external
  internal
  ipsec
  loopback
  setup

Default value: any
Current value: any

(config network route policy 0)> dst zone
```

  b. Set the zone. For example:

```
(config network route policy 0)> dst zone external
(config network route policy 0)>
```

  See Firewall configuration for more information about firewall zones.

- **interface**: Matches the destination IP address to the selected interface's network address. Set the interface:

a. Use the **?** to determine available interfaces:

b. Set the interface. For example:

```
(config network route policy 0)> dst interface
/network/interface/eth1
(config network route policy 0)>
```

- **address**: Matches the destination IPv4 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> dst address value
(config network route policy 0)>
```

where value uses the format ***IPv4_address***[**/*netmask***], or **any** to match any IPv4 address.

- **address6**: Matches the destination IPv6 address to the specified IP address or network. Set the address that will be matched:

```
(config network route policy 0)> dst address6 value
(config network route policy 0)>
```

where value uses the format ***IPv6_address***[**/*prefix_length***], or **any** to match any IPv6 address.

- **mac**: Matches the destination MAC address to the specified MAC address. Set the MAC address to be matched:

```
(config network route policy 0)> dst mac MAC_address
(config network route policy 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.

Routing services

Your Connect EZ includes support for dynamic routing services and protocols. The following routing services are supported:

Service or protocol	Information
RIP	The IPv4 Routing Information Protocol (RIP) service supports RIPv2 (RFC2453) and RIPv1 (RFC1058).
RIPng	The IPv6 Routing Information Protocol (RIP) service supports RIPng (RFC2080).
OSPFv2	The IPv4 Open Shortest Path First (OSPF) service supports OSPFv2 (RFC2328).
OSPFv3	The IPv6 Open Shortest Path First (OSPF) service supports OSPFv3 (RFC2740).
BGP	The Border Gateway Protocol (BGP) service supports BGP-4 (RFC1771).
IS-IS	The IPv4 and IPv6 Intermediate System to Intermediate System (IS-IS) service.

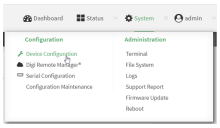
Configure routing services

Required configuration items

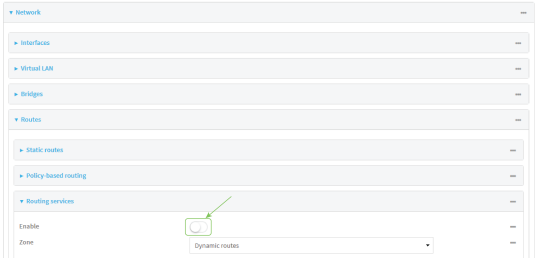
- Enable routing services.
- Enable and configure the types of routing services that will be used.

WebUI

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** > **Routes** > **Routing services**.
4. Click **Enable**.



   The default firewall zone setting, **Dynamic routes**, is specifically designed to work with routing services and should be left as the default.
5. Configure the routing services that will be used:
   a. Click to expand a routing service.
   b. **Enable** the routing service.
   c. Complete the configuration of the routing service.
6. 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. Enable routing services:

```
(config)> network route service enable true
(config)>
```

4. Configure routing services that will be used:
   a. Use the **?** to display available routing services:

```
(config)> network route service ?

Routing services: Settings for dynamic routing services and protocols.

 Parameters                Current Value
 ------------------------------------------------------------------------
----------
 enable                    true            Enable
 zone                      dynamic_routes  Zone

 Additional Configuration
 ------------------------------------------------------------------------
----------
 bgp                       BGP
 isis                      IS-IS
 ospfv2                    OSPFv2
 ospfv3                    OSPFv3
 rip                       RIP
 ripng                     RIPng

(config)>
```

   b. Enable a routing service that will be used. For example, to enable the RIP service:

```
(config)> network route service rip enable true
(config)>
```

   c. Complete the configuration of the routing service. For example, use the **?** to view the available parameters for the RIP service:

```
(config)> network route service rip ?

 Parameters                Current Value
 ------------------------------------------------------------------------
----------
 ecmp                      false          Allow ECMP
 enable                    true           Enable

 Additional Configuration
 ------------------------------------------------------------------------
----------
 interface                 Interfaces
 neighbour                 Neighbours
```

```
redis                          Route redistribution
timer                          Timers

(config)>
```

5. Save the configuration and apply the change:

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

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

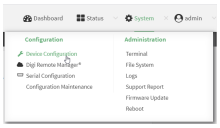
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show the routing table

To display the routing table:

WebUI

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 **Status** > **Routes**.

   The **Network Routing** window is displayed.
4. Click **IPv4 Load Balance** to view IPv4 load balancing.
5. Click **IPv6 Load Balance** to view IPv6 load balancing.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 route:

   You can limit the display to only IPv4 entries by using **show route ipv4**, or to IPv6 entries by using **show route ipv6**. You can also display more information by adding the **verbose** option to the **show route** and **show route *ip_type*** commands.
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.

Dynamic DNS

The Domain Name System (DNS) uses name servers to provide a mapping between computer-readable IP addresses and human-readable hostnames. This allows users to access websites and personal networks with easy-to-remember URLs. Unfortunately, IP addresses change frequently, invalidating these mappings when they do. Dynamic DNS has become the standard method of addressing this problem, allowing devices to update name servers with their new IP addresses.

By providing the Connect EZ device with the domain name and credentials obtained from a dynamic DNS provider, the router can automatically update the remote nameserver whenever your WAN or public IP address changes.

Your Connect EZ device supports a number of Dynamic DNS providers as well as the ability to provide a custom provider that is not included on the list of providers.

Configure dynamic DNS

This section describes how to cofigure dynamic DNS on a Connect EZ device.

Required configuration items

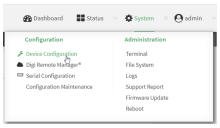
- Add a new Dynamic DNS service.
- The interface that has its IP address registered with the Dynamic DNS provider.
- The name of a Dynamic DNS provider.
- The domain name that is linked to the interface's IP address.
- The username and password to authenticate with the Dynamic DNS provider.

Additional configuration items

- If the Dynamic DNS service provider is set to **custom**, identify the URL that should be used to update the IP address with the Dynamic DNS provider.
- The amount of time to wait to check if the interface's IP address needs to be updated.
- The amount of time to wait to force an update of the interface's IP address.
- The amount of time to wait for an IP address update to succeed before retrying the update.
- The number of times to retry a failed IP address update.

WebUI

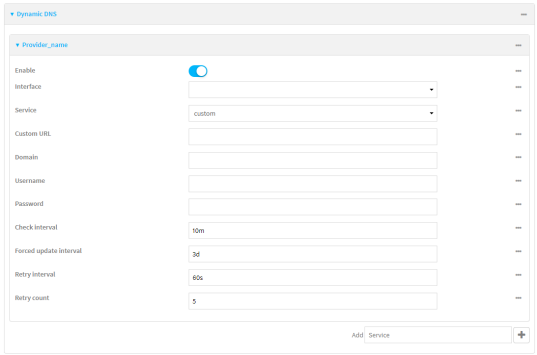
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **Dynamic DNS**.
4. Type a name for this Dynamic DNS instance in **Add Service** and click ✚.



   The Dynamic DNS configuration page displays.



   New Dynamic DNS configurations are enabled by default. To disable, click to toggle **Enable** to off.
5. For **Interface**, select the interface that has its IP address registered with the Dynamic DNS provider.
6. For **Service**, select the Dynamic DNS provider, or select **custom** to enter a custom URL for the Dynamic DNS provider.
7. If **custom** is selected for **Service**, type the **Custom URL** that should be used to update the IP address with the Dynamic DNS provider.
8. Type the **Domain** name that is linked to the interface's IP address.
9. Type the **Username** and **Password** used to authenticate with the Dynamic DNS provider.
10. (Optional) For **Check Interval**, type the amount of time to wait to check if the interface's IP address needs to be updated.

    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 **Check interval** to ten minutes, enter **10m** or **600s**.

11. (Optional) For **Forced update interval**, type the amount of time to wait to force an update of the interface's IP address.

    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 **Forced update interval** to ten minutes, enter **10m** or **600s**.

    The setting for **Forced update interval** must be larger than the setting for **Check Interval**.

12. (Optional) For **Retry interval**, type the amount of time to wait for an IP address update to succeed before retrying the update.

    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 **Retry interval** to ten minutes, enter **10m** or **600s**.

13. (Optional) For **Retry count**, type the number of times to retry a failed IP address update.
14. 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. Add a new Dynamic DNS instance. For example, to add an instance named **new_ddns_instance**:

```
(config)> add network ddns new_ddns_instance
(config network ddns new_ddns_instance)>
```

   New Dynamic DNS instances are enabled by default. To disable:

```
(config network ddns new_ddns_instance)> enable false
(config network ddns new_ddns_instance)>
```

4. Set the interface for the Dynamic DNS instance:
   a. Use the **?** to determine available interfaces:
   b. Set the interface. For example:

```
(config network ddns new_ddns_instance)> interface eth1
(config network ddns new_ddns_instance)>
```

5. Set the Dynamic DNS provider service:
   a. Use the **?** to determine available services:

```
(config network ddns new_ddns_instance)> service ?

Service: The provider of the dynamic DNS service.
Format:
  custom
  3322.org
  changeip.com
  ddns.com.br
  dnsdynamic.org
  ...

Default value: custom
Current value: custom

(config network ddns new_ddns_instance)> service
```

   b. Set the service:

```
(config network ddns new_ddns_instance)> service service_name
(config network ddns new_ddns_instance)>
```

6. If **custom** is configured for **service**, set the custom URL that should be used to update the IP address with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> custom url
(config network ddns new_ddns_instance)>
```

7. Set the domain name that is linked to the interface's IP address:

```
(config network ddns new_ddns_instance)> domain domain_name
(config network ddns new_ddns_instance)>
```

8. Set the username to authenticate with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> username name
(config network ddns new_ddns_instance)>
```

9. Set the password to authenticate with the Dynamic DNS provider:

```
(config network ddns new_ddns_instance)> password pwd
(config network ddns new_ddns_instance)>
```

10. (Optional) Set the amount of time to wait to check if the interface's IP address needs to be updated:

```
(config network ddns new_ddns_instance)> check_interval value
(config network ddns new_ddns_instance)>
```

    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 **check_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> check_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **10m**.

11. (Optional) Set the amount of time to wait to force an update of the interface's IP address:

```
(config network ddns new_ddns_instance)> force_interval value
(config network ddns new_ddns_instance)>
```

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 **force_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> force_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **3d**.

12. (Optional) Set the amount of time to wait for an IP address update to succeed before retrying the update:

```
(config network ddns new_ddns_instance)> retry_interval value
(config network ddns new_ddns_instance)>
```

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 **retry_interval** to ten minutes, enter either **10m** or **600s**:

```
(config network ddns new_ddns_instance)> retry_interval 600s
(config network ddns new_ddns_instance)>
```

The default is **60s**.

13. (Optional) Set the number of times to retry a failed IP address update:

```
(config network ddns new_ddns_instance)> retry_count value
(config network ddns new_ddns_instance)>
```

where *value* is any interger. The default is **5**.

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.

Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) is a standard for gateway device redundancy and failover that creates a "virtual router" with a floating IP address. Devices connected to the LAN then use this virtual router as their default gateway. Responsibility for the virtual router is assigned to one of the VRRP-enabled devices on a LAN (the "master router"), and this responsibility transparently fails over to backup VRRP devices if the master router fails. This prevents the default gateway from being a single point of failure, without requiring configuration of dynamic routing or router discovery protocols on every host.

Multiple Connect EZ devices can be configured as VRRP devices and assigned a priority. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of the virtual router is mapped to the backup device with the next highest priority. Each VRRP router is configured with a unique LAN IP address, and the same shared VRRP address.

VRRP+

VRRP+ is an extension to the VRRP standard that uses network probing to monitor connections through VRRP-enabled devices and can dynamically change the priority of the devices, including changing devices from master to backup, and from backup to master, even if the device has not failed. For example, if a host becomes unreachable on the far end of a network link, then the physical default gateway can be changed by adjusting the VRRP priority of the Connect EZ device connected to the failing link. This provides failover capabilities based on the status of connections behind the router, in addition to the basic VRRP device failover. For Connect EZ devices, SureLink is used to probe network connections.

VRRP+ can be configured to probe a specified IP address by either sending an ICMP echo request (ping) or attempting to open a TCP socket to the IP address.

Configure VRRP

This section describes how to configure VRRP on a Connect EZ device.

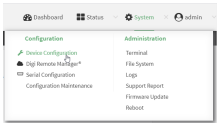
Required configuration items

- Enable VRRP.
- The interface used by VRRP.
- The Router ID that identifies the virtual router instance. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool.
- The VRRP priority of this device.
- The shared virtual IP address for the VRRP virtual router. Devices connected to the LAN will use this virtual IP address as their default gateway.

See Configure VRRP+ for information about configuring VRRP+, an extension to VRRP that uses network probing to monitor connections through VRRP-enabled devices and dynamically change the VRRP priorty of devices based on the status of their network connectivity.

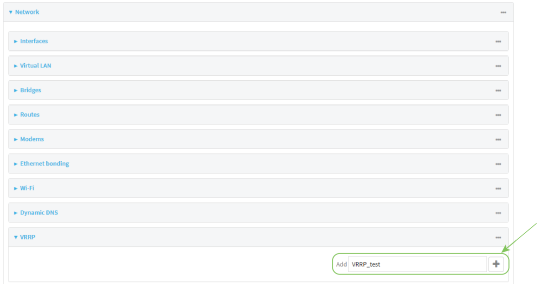
WebUI

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**.

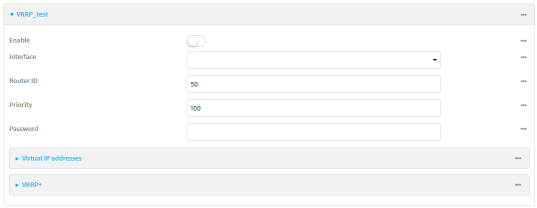


The **Configuration** window is displayed.

3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click **+**.

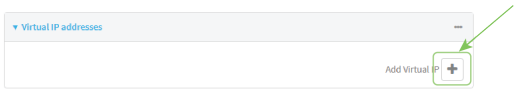


The new VRRP instance configuration is displayed.



5. Click **Enable**.
6. For **Interface**, select the interface on which this VRRP instance should run.
7. For **Router ID** field, type the ID of the virtual router instance. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool. Allowed values are from **1** and **255**, and it is configured to **50** by default.
8. For **Priority**, type the priority for this router in the group. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of the virtual router is mapped to the backup device with the next highest priority. If this device's actual IP address is being used as the virtual IP address of the VRRP pool, then the priority of this device should be set to **255** . Allowed values are from **1** and **255**, and it is configured to **100** by default.
9. (Optional) For **Password**, type a password that will be used to authenticate this VRRP router with VRRP peers. If the password length exceeds 8 characters, it will be truncated to 8 characters.

10. Configure the virtual IP addresses associated with this VRRP instance:
    a. Click to expand **Virtual IP addresses**.
    b. Click ✚ to add a virtual IP address.



    c. For **Virtual IP**, type the IPv4 or IPv6 address for a virtual IP of this VRRP instance.
    d. (Optional) Repeat to add additional virtual IPs.
11. See Configure VRRP+ for information about configuring VRRP+.
12. 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. Add a VRRP instance. For example:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the interface on which this VRRP instance should run:
    a. Use the **?** to determine available interfaces:
    b. Set the interface, for example:

```
(config network vrrp VRRP_test)> interface /network/interface/eth2
(config network vrrp VRRP_test)>
```

    c. Repeat for additional interfaces.
6. Set the router ID. The Router ID must be the same on all VRRP devices that participate in the same VRRP device pool. Allowed values are from **1** and **255**, and it is configured to **50** by default.

```
(config network vrrp VRRP_test)> router_id int
(config network vrrp VRRP_test)>
```

7. Set the priority for this router in the group. The router with the highest priority will be used as the master router. If the master router fails, then the IP address of the virtual router is mapped to the backup device with the next highest priority. If this device's actual IP address is being used as the virtual IP address of the VRRP pool, then the priority of this device should be set to **255** . Allowed values are from **1** and **255**, and it is configured to **100** by default.

```
(config network vrrp VRRP_test)> priority int
(config network vrrp VRRP_test)>
```

8. (Optional) Set a password that will be used to authenticate this VRRP router with VRRP peers. If the password length exceeds 8 characters, it will be truncated to 8 characters.

```
(config network vrrp VRRP_test)> password pwd
(config network vrrp VRRP_test)>
```

9. Add a virtual IP address associated with this VRRP instance. This can be an IPv4 or IPv6 address.

```
(config network vrrp VRRP_test)> add virtual_address end ip_address
(config network vrrp VRRP_test)>
```

   Additional virtual IP addresses can be added by repeating this step with different values for *ip_address*.

10. Save the configuration and apply the change:

```
(config network vrrp new_vrrp_instance)> 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 VRRP+

VRRP+ is an extension to the VRRP standard that uses SureLink network probing to monitor connections through VRRP-enabled devices and adjust devices' VRRP priority based on the status of the SureLink tests.

This section describes how to configure VRRP+ on a Connect EZ device.

Required configuration items

- Both master and backup devices:
  - A configured and enabled instance of VRRP. See Configure VRRP for information.
  - Enable VRRP+.

- WAN interfaces to be monitored by using VRRP+.

  Note SureLink is enabled by default on all WAN interfaces, and should not be disabled on the WAN interfaces that are being monitored by VRRP+.

  If multiple WAN interfaces are being monitored on the same device, the VRRP priority will be adjusted only if all WAN interfaces fail SureLink tests.

- The amount that the VRRP priority will be modified when SureLink determines that the VRRP interface is not functioning correctly.
- Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses.

■ Backup devices only:

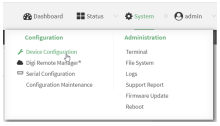
- Enable and configure SureLink on the VRRP interface.
- Set the IP gateway to the IP address of the VRRP interface on the master device.

Additional configuration items

■ For backup VRRP devices, enable the ability to monitor the VRRP master, so that a backup device can increase its priority when the master device fails SureLink tests.

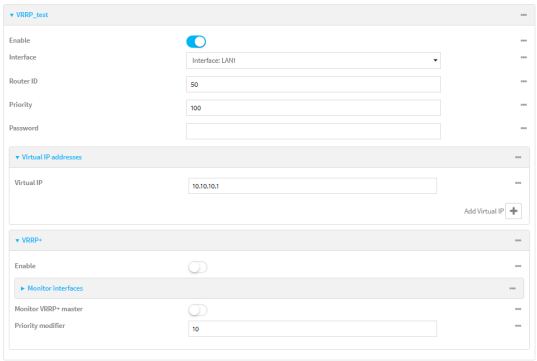
WebUI

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**.



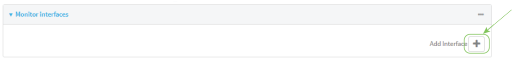
   The **Configuration** window is displayed.
3. Click **Network** > **VRRP**.
4. Create a new VRRP instance, or click to expand an existing VRRP instance.

   See Configure VRRP for information about creating a new VRRP instance.
5. Click to expand **VRRP+**.



6. Click **Enable**.

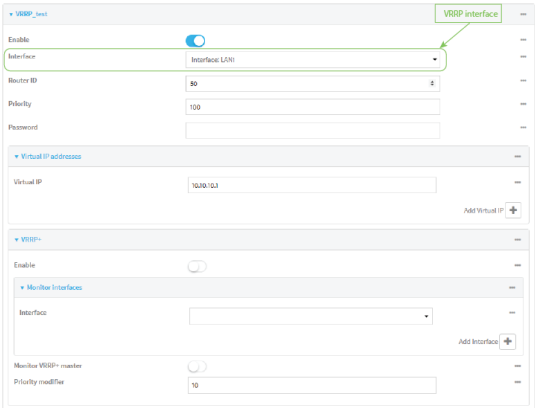
7. Add interfaces to monitor:
   a. Click to expand **Monitor interfaces**.
   b. Click ✚ to add an interface for monitoring.



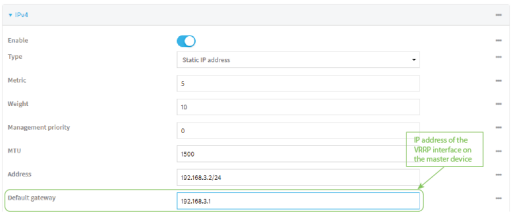
   c. For **Interface**, select the local interface to monitor. Generally, this will be a cellular or WAN interface.
   d. (Optional) Click ✚ again to add additional interfaces.
8. (Optional) For backup devices, click to enable **Monitor VRRP+ master**.

   This parameter allows a backup VRRP device to monitor the master device, and increase its priority when the master device is failing SureLink tests. This can allow a device functioning as a backup device to promote itself to master.
9. For **Priority modifier**, type or select the amount that the device's priority should be decreased due to SureLink connectivity failure, and increased when SureLink succeeds again.

   Along with the priority settings for devices in this VRRP pool, the amount entered here should be large enough to automatically demote a master device when SureLink connectivity fails. For example, if the VRRP master device has a priority of **100** and the backup device has a priority of **80**, then the **Priority modifier** should be set to an amount greater than **20** so that if SureLink fails on the master, it will lower its priority to below **80**, and the backup device will assume the master role.
10. Configure the VRRP interface. The VRRP interface is defined in the **Interface** parameter of the VRRP configuration, and generally should be a LAN interface:



   To configure the VRRP interface:
   a. Click to expand **Network** > **Interfaces**.
   b. Click to expand the appropriate VRRP interface (for example, **LAN1**).
   c. For backup devices, for **Default Gateway**, type the IP address of the VRRP interface on the master device.

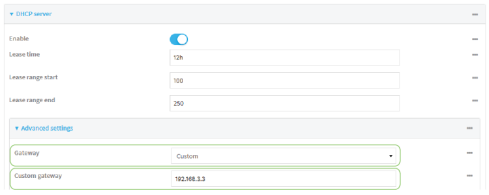


d. Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses:

   i. Click to expand **DHCP Server** > **Advanced settings**.

   ii. For **Gateway**, select **Custom**.

   iii. For **Custom gateway**, enter the IP address of one of the virtual IPs used by this VRRP instance.



e. For backup devices, enable and configure SureLink on the VRRP interface. Generally, this should be a LAN interface; VRRP+ will then monitor the LAN using SureLink to determine if the interface has network connectivity and promote a backup to master if SureLink fails.

   i. Click to expand **IPv4** > **SureLink**.

   ii. Click **Enable**.

   iii. For **Interval**, type a the amount of time to wait between connectivity tests. To guarantee seamless internet access for VRRP+ purposes, SureLink tests should occur more often than the default of 15 minutes.

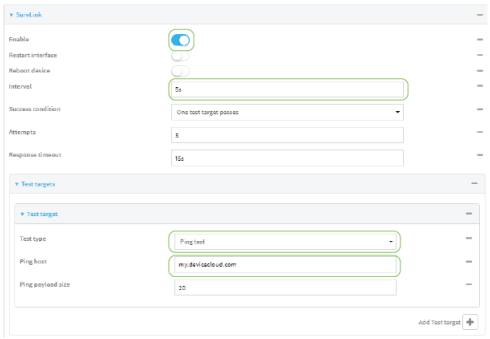
   Allowed values are any number of weeks, days, hours, minutes, or seconds, and take the format ***number***{**w|d|h|m|s**}. For example, to set **Interval** to five seconds, enter **5s**.

   iv. Click to expand **Test targets** > **Test target**.

   v. Configure the test target. For example, to configure SureLink to verify internet connectivity on the LAN by pinging my.devicecloud.com:

      i. For **Test Type**, select **Ping test**.

      ii. For **Ping host**, type **my.devicecloud.com**.



11. 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 VRRP instance, or edit an existing one. See Configure VRRP for information about creating a new VRRP instance.
4. Enable VRRP+:

```
(config)> network vrrp VRRP_test vrrp_plus enable true
(config)>
```

5. Add interfaces to monitor. Generally, this will be a cellular or WAN interface.
   a. Use the **?** to determine available interfaces:
   b. Set the interface, for example:

```
(config)> add network vrrp VRRP_test vrrp_plus monitor_interface end
/network/interface/modem
(config)>
```

   c. (Optional) Repeat for additional interfaces.
6. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success:

```
(config)> network vrrp VRRP_test vrrp_plus weight value
(config)>
```

where *value* is an integer between **1** and **254**. The default is **10**.

Along with the priority settings for devices in this VRRP pool, the amount entered here should be large enough to automatically demote a master device when SureLink connectivity fails. For example, if the VRRP master device has a priority of **100** and the backup device has a priority of **80**, then **weight** should be set to an amount greater than **20** so that if SureLink fails on the master, it will lower its priority to below **80**, and the backup device will assume the master role.

7. (Optional) For backup devices, enable the ability for the device to monitor the master device. This allows a backup VRRP device to monitor the master device, and increase its priority when the master device is failing SureLink tests. This can allow a device functioning as a backup device to promote itself to master.

```
(config)> network vrrp VRRP_test vrrp_plus monitor_master true
(config)>
```

8. Configure the VRRP interface:
   a. Configure the VRRP interface's DHCP server to use a custom gateway that corresponds to one of the VRRP virtual IP addresses:
      i. Set the DHCP server gateway type to custom:

```
(config)> network interface eth2 ipv4 dhcp_server advanced gateway
custom
(config)>
```

      ii. Determine the VRRP virtual IP addresses:

```
(config)> show network vrrp VRRP_test virtual_address
0 192.168.3.3
1 10.10.10.1

(config)>
```

      iii. Set the custom gateway to one of the VRRP virtual IP addresses. For example:

```
(config)> network interface eth2 ipv4 dhcp_server advanced
gateway_custom 192.168.3.3
(config)>
```

   b. For backup devices, set the default gateway to the IP address of the VRRP interface on the master device. For example:

```
(config)> network interface eth2 ipv4 gateway 192.168.3.1
(config)>
```

   c. For backup devices, enable and configure SureLink on the VRRP interface.
      i. Determine the VRRP interface. Generally, this should be a LAN interface; VRRP+ will then monitor the LAN using SureLink to determine if the interface has network connectivity and promote a backup to master if SureLink fails.

```
(config)> show network vrrp VRRP_test interface
/network/interface/eth2
(config)>
```

ii. Enable SureLink on the interface:

```
(config)> network interface eth2 ipv4 surelink enable true
(config)>
```

iii. Set the amount of time to wait between connectivity tests:

```
(config)> network interface eth2 ipv4 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 **5s**:

```
(config)> network interface eth2 ipv4 surelink interval 5s
(config)>
```

iv. Create a SureLink test target:

```
(config)> add network interface eth2 ipv4 surelink target end
(config network interface eth2 ipv4 surelink target 0)>
```

v. Configure the type of test for the test target:

```
(config network interface eth2 ipv4 surelink target 0)> test value
(config network interface eth2 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 eth2 ipv4 surelink target 0)>
    ping_host host
    (config network interface eth2 ipv4 surelink target 0)>
    ```

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

    ```
    (config network interface eth2 ipv4 surelink target 0)>
    ping_size [num]
    (config network interface eth2 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 eth2 ipv4 surelinktarget 0)>
dns_server ip_address
(config network interface eth2 ipv4 surelinktarget 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 eth2 ipv4 surelink target 0)>
    http_url value
    (config network interface eth2 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 eth2 ipv4 surelink target 0)>
    interface_down_time value
    (config network interface eth2 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 **interface_down_time** to ten minutes, enter either **10m** or **600s**:

    ```
    (config network interface eth2 ipv4 surelink target 0)>
    interface_down_time 600s
    (config network interface eth2 ipv4 surelink target 0)>
    ```

    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 eth2 ipv4 surelink target 0)>
    interface_timeout value
    (config network interface eth2 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 **interface_timeout** to ten minutes, enter either **10m** or **600s**:

```
(config network interface eth2 ipv4 surelink target 0)>
interface_timeout 600s
(config network interface eth2 ipv4 surelink target 0)>
```

The default is 60 seconds.

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.

Example: VRRP/VRRP+ configuration

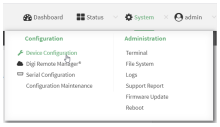
This example configuration creates a VRRP pool containing two Connect EZ devices:

Configure device one (master device)

WebUI

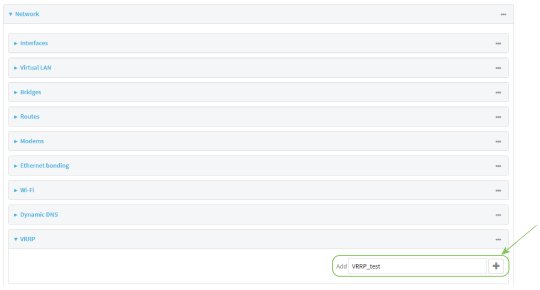
Task 1: Configure VRRP on device one

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**.

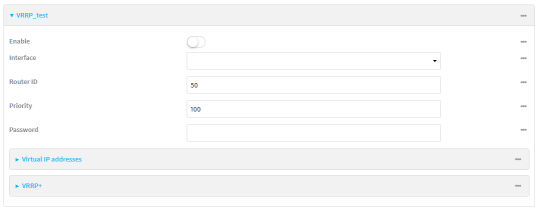


The **Configuration** window is displayed.

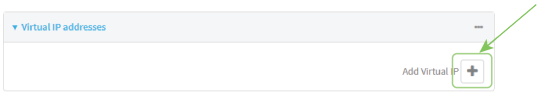
3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click ✚.



The new VRRP instance configuration is displayed.



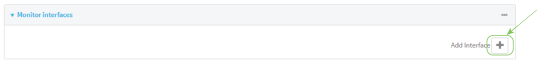
5. Click **Enable**.
6. For **Interface**, select **Interface: ETH2**.
7. For **Router ID**, leave at the default setting of **50**.
8. For **Priority**, leave at the default setting of **100**.
9. Click to expand **Virtual IP addresses**.
10. Click ✚ to add a virtual IP address.



11. For **Virtual IP**, type **192.168.3.3**.

Task 2: Configure VRRP+ on device one

1. Click to expand **VRRP+**.
2. Click **Enable**.
3. Click to expand **Monitor interfaces**.
4. Click ✚ to add an interface for monitoring.



5. Select **Interface: Modem**.
6. For **Priority modifier**, type **30**.

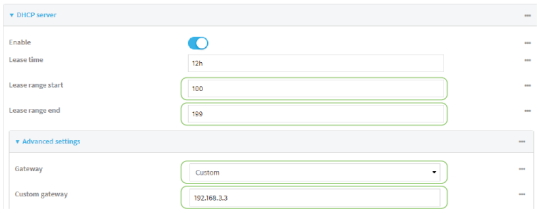
Task 3: Configure the IP address for the VRRP interface, ETH2, on device one

1. Click **Network** > **Interfaces** > **ETH2** > **IPv4**
2. For **Address**, type **192.168.3.1/24**.



Task 4: Configure the DHCP server for ETH2 on device one

1. Click to expand **Network** > **Interfaces** > **ETH2** > **IPv4** > **DHCP Server**
2. For **Lease range start**, leave at the default of **100**.
3. For **Lease range end**, type **199**.
4. Click to expand **Advanced settings**.
5. For **Gateway**, select **Custom**.
6. For **Custom gateway**, enter **192.168.3.3**.



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



Command line

Task 1: Configure VRRP on device one

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 the VRRP instance:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the VRRP interface to ETH2:

```
(config network vrrp VRRP_test)> interface /network/interface/eth2
(config network vrrp VRRP_test)>
```

6. Add the virtual IP address associated with this VRRP instance.

```
(config network vrrp VRRP_test)> add virtual_address end 192.168.3.3
(config network vrrp VRRP_test)>
```

Task 2: Configure VRRP+ on device one

1. Enable VRRP+:

```
(config network vrrp VRRP_test)> vrrp_plus enable true
(config network vrrp VRRP_test )>
```

2. Add the interface to monitor:

```
(config network vrrp VRRP_test)> add vrrp_plus monitor_interface end
/network/interface/modem
(config network vrrp VRRP_test)>
```

3. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success to **30**:

```
(config network vrrp VRRP_test )> network vrrp VRRP_test vrrp_plus weight
30
(config network vrrp VRRP_test )>
```

Task 3: Configure the IP address for the VRRP interface, ETH2, on device one

1. Type **...** to return to the root of the config prompt:

```
(config network vrrp VRRP_test )> ...
(config)>
```

2. Set the IP address for ETH2:

```
(config)> network interface eth2 ipv4 address 192.168.3.1/24
(config)>
```

Task 4: Configure the DHCP server for ETH2 on device one

1. Set the start and end addresses of the DHCP pool to use to assign DHCP addresses to clients:
   a. Set the start address to **100**:

```
(config)> network interface eth2 ipv4 dhcp_server lease_start 100
(config)>
```

   b. Set the end address to **199**:

```
(config)> network interface eth2 ipv4 dhcp_server lease_end 199
(config)>
```

2. Set the DHCP server gateway type to custom:

```
(config)> network interface eth2 ipv4 dhcp_server advanced gateway custom
(config)>
```

3. Set the custom gateway to **192.168.3.3**:

```
(config)> network interface eth2 ipv4 dhcp_server advanced gateway_custom
192.168.3.3
(config)>
```

4. Save the configuration and apply the change:

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

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

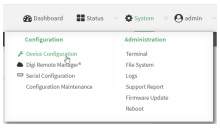
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure device two (backup device)

WebUI

Task 1: Configure VRRP on device two

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**.

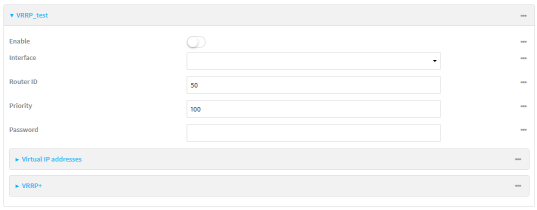


   The **Configuration** window is displayed.

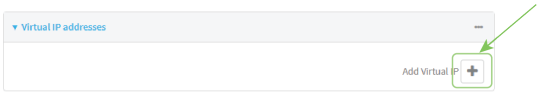
3. Click **Network** > **VRRP**.
4. For **Add VRRP instance**, type a name for the VRRP instance and click ✚.



   The new VRRP instance configuration is displayed.



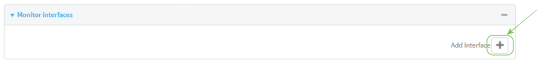
5. Click **Enable**.
6. For **Interface**, select **Interface: ETH2**.
7. For **Router ID**, leave at the default setting of **50**.
8. For **Priority**, type **80**.
9. Click to expand **Virtual IP addresses**.
10. Click ✚ to add a virtual IP address.



11. For **Virtual IP**, type **192.168.3.3**.

Task 2: Configure VRRP+ on device two

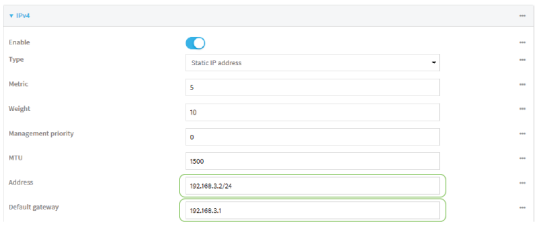
1. Click to expand **VRRP+**.
2. Click **Enable**.
3. Click to expand **Monitor interfaces**.
4. Click ✚ to add an interface for monitoring.



5. Select **Interface: Modem**.
6. Click to enable **Monitor VRRP+ master**.
7. For **Priority modifier**, type **30**.

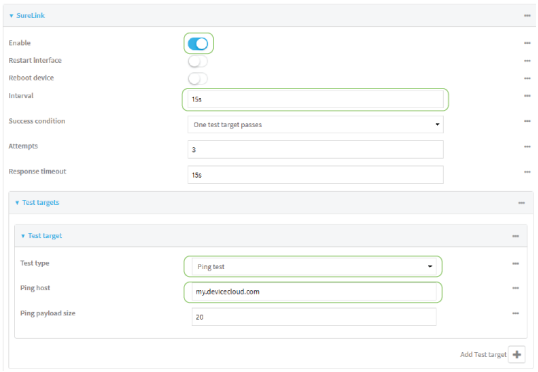
Task 3: Configure the IP address for the VRRP interface, ETH2, on device two

1. Click **Network** > **Interfaces** > **ETH2** > **IPv4**
2. For **Address**, type **192.168.3.2/24**.
3. For **Default gateway**, type the IP address of the VRRP interface on the master device, configured above in Task 3, step 2 (**192.168.3.1**).



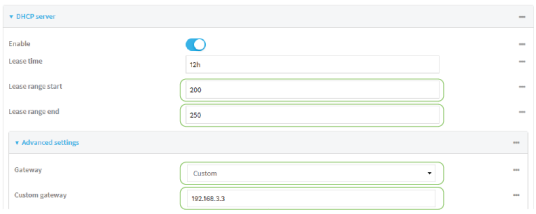
Task 4: Configure SureLink for ETH2 on device two

1. Click **Network** > **Interfaces** > **ETH2** > **IPv4** > **SureLink**.
2. Click **Enable**.
3. For **Interval**, type **15s**.
4. Click to expand **Test targets** > **Test target**.
5. For **Test Type**, select **Ping test**.
6. For **Ping host**, type **my.devicecloud.com**.



Task 5: Configure the DHCP server for ETH2 on device two

1. Click to expand **Network** > **Interfaces** > **ETH2** > **IPv4** > **DHCP Server**
2. For **Lease range start**, type **200**.
3. For **Lease range end**, type **250**.
4. Click **Advanced settings**.
5. For **Gateway**, select **Custom**.
6. For **Custom gateway**, enter **192.168.3.3**.



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



Command line

Task 1: Configure VRRP on device two

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 the VRRP instance:

```
(config)> add network vrrp VRRP_test
(config network vrrp VRRP_test)>
```

4. Enable the VRRP instance:

```
(config network vrrp VRRP_test)> enable true
(config network vrrp VRRP_test)>
```

5. Set the VRRP interface to ETH2:

```
(config network vrrp VRRP_test)> interface /network/interface/eth2
(config network vrrp VRRP_test)>
```

6. Add the virtual IP address associated with this VRRP instance.

```
(config network vrrp VRRP_test)> add virtual_address end 192.168.3.3
(config network vrrp VRRP_test)>
```

Task 2: Configure VRRP+ on device two

1. Enable VRRP+:

```
(config network vrrp VRRP_test)> vrrp_plus enable true
(config network vrrp VRRP_test )>
```

2. Add the interface to monitor:

```
(config network vrrp VRRP_test)> add vrrp_plus monitor_interface end
/network/interface/modem
(config network vrrp VRRP_test)>
```

3. Enable the ability to monitor the master device:

```
(config network vrrp VRRP_test)> vrrp_plus monitor_master true
(config network vrrp VRRP_test)>
```

4. Set the amount that the device's priority should be decreased or increased due to SureLink connectivity failure or success to **30**:

```
(config network vrrp VRRP_test )> network vrrp VRRP_test vrrp_plus weight
30
(config network vrrp VRRP_test )>
```

Task 3: Configure the IP address for the VRRP interface, ETH2, on device two

1. Type **...** to return to the root of the config prompt:

```
(config network vrrp VRRP_test )> ...
(config)>
```

2. Set the IP address for ETH2:

```
(config)> network interface eth2 ipv4 address 192.168.3.2
(config)>
```

3. Set the default gateway to the IP address of the VRRP interface on the master device, configured above in Task 3, step 2 (**192.168.3.1**).

```
(config)> network interface eth2 ipv4 gateway 192.168.3.1
(config)>
```

Task 4: Configure SureLink for ETH2 on device two

1. Enable SureLink on the ETH2 interface:

```
(config)> network interface eth2 ipv4 surelink enable true
(config)>
```

2. Create a SureLink test target:

```
(config)> add network interface eth2 ipv4 surelink target end
(config network interface eth2 ipv4 surelink target 0)>
```

3. Set the type of test to ping:

```
(config network interface eth2 ipv4 surelink target 0)> test ping
(config network interface eth2 ipv4 surelink target 0)>
```

4. Set **my.devicecloud.com** as the hostname to ping:

```
(config network interface eth2 ipv4 surelink target 0)> ping_host
my.devicecloud.com
(config network interface eth2 ipv4 surelink target 0)>
```

Task 5: Configure the DHCP server for ETH2 on device two

1. Type **...** to return to the root of the configuration prompt:

```
(config network interface eth2 ipv4 surelink target 0)> ...
(config)>
```

2. Set the start and end addresses of the DHCP pool to use to assign DHCP addresses to clients:
   a. Set the start address to **200**:

```
(config)> network interface eth2 ipv4 dhcp_server lease_start 200
(config)>
```

b. Set the end address to **250**:

```
(config)> network interface eth2 ipv4 dhcp_server lease_end 250
(config)>
```

3. Set the DHCP server gateway type to custom:

```
(config)> network interface eth2 ipv4 dhcp_server advanced gateway custom
(config)>
```

4. Set the custom gateway to **192.168.3.3**:

```
(config)> network interface eth2 ipv4 dhcp_server advanced gateway_custom
192.168.3.3
(config)>
```

5. Save the configuration and apply the change:

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

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

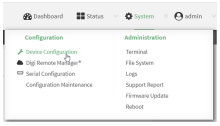
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Show VRRP status and statistics

This section describes how to display VRRP status and statistics for a Connect EZ device. VRRP status is available from the Web UI only.

WebUI

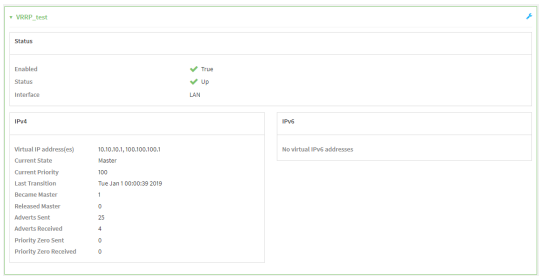
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.

3. Click **Status** > **VRRP**.

   The **Virtual Router Redundancy Protocol** window is displayed.



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 vrrp:

```
> show vrrp

 VRRP       Status  Proto  State   Virtual IP
 ----       ------  -----  ------  -------------
 VRRP_test  Up      IPv4   Backup  10.10.10.1
 VRRP_test  Up      IPv4   Backup  100.100.100.1
>
```

3. To display additional information about a specific VRRP instance, at the Admin CLI prompt, type show vrrp name *name*:

```
> show vrrp name VRRP_test

 VRRP_test VRRP Status
 ---------------------
 Enabled                  : True
 Status                   : Up
 Interface                : lan

 IPv4
   ----
   Virtual IP address(es) : 10.10.10.1, 100.100.100.1
   Current State          : Master
   Current Priority       : 100
   Last Transition        : Tue Jan  1 00:00:39 2019
   Became Master          : 1
   Released Master        : 0
   Adverts Sent           : 71
   Adverts Received       : 4
   Priority Zero Sent     : 0
   Priority zero Received : 0

>
```

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 356
OpenVPN 407
Generic Routing Encapsulation (GRE) 437
L2TP 457
L2TPv3 Ethernet 475
NEMO 480

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 authenticaton

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:**
  - 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:

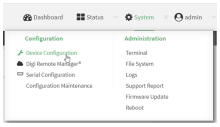
- Determine whether the device should use UDP encapsulation even when it does not detect that NAT is being used.
- If using IPsec failover, identify the primary tunnel during configuration of the backup tunnel.
- The Network Address Translation (NAT) keep alive time.
- The protocol, either Encapsulating 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.

Note if the remote networks for an IPsec tunnel overlap with the networks for a WAN internet connection (wired, cellular, or otherwise), you must configure a static route to direct the traffic either through the IPsec tunnel, or through the WAN (outside of the IPsec tunnel). See Configure a static route for information about configuring a static route.

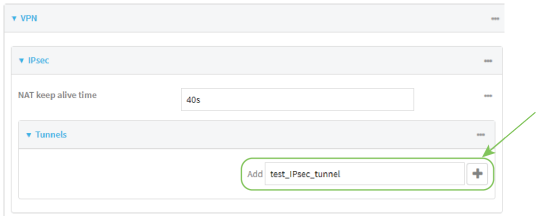
WebUI

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**.

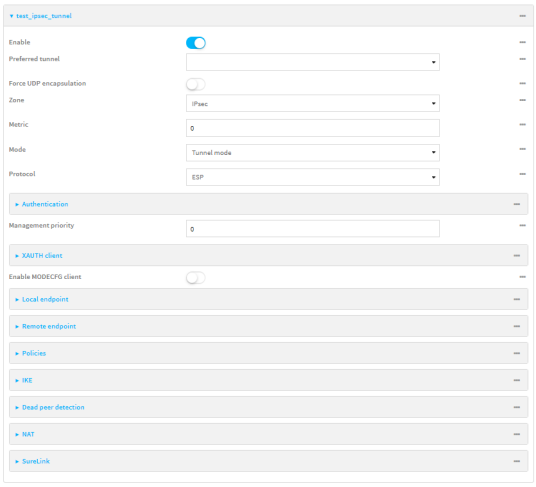


The **Configuration** window is displayed.

3. Click **VPN** > **IPsec**.
4. Click to expand **Tunnels**.
5. For **Add IPsec tunnel**, type a name for the tunnel and click ✚.



The new IPsec tunnel configuration is displayed.

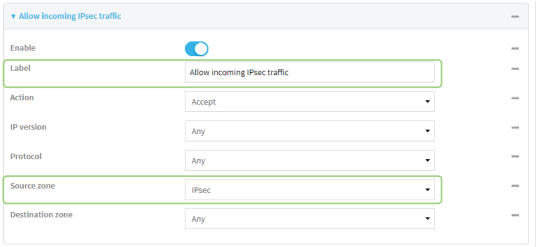


6. The IPsec tunnel is enabled by default. To disable, click **Enable**.
7. (Optional) **Preferred tunnel** provides an optional mechanism for IPsec failover behavior. See Configure IPsec failover for more information.
8. (Optional) Enable **Force UDP encapsulation** to force the tunnel to use UDP encapsulation even when it does not detect that NAT is being used.
9. 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:

a. Click to expand **Firewall** > **Packet filtering**.
b. For **Add packet filter**, click ✚.
c. For **Label**, type **Allow incoming IPsec traffic**.
d. For **Source zone**, select **IPsec**.

Leave all other fields at their default settings.

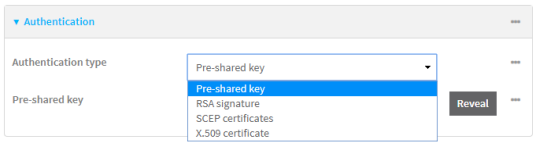


---

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. Click to expand **Authentication**.



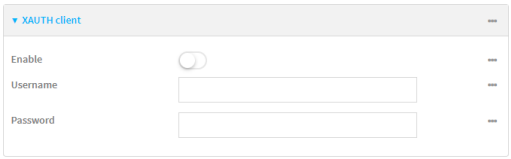
    a. For **Authentication type**, select one of the following:
        - **Pre-shared key**: Uses a pre-shared key (PSK) to authenticate with the remote peer.
            i. Type the **Pre-shared key**.
        - **Asymmetric pre-shared keys**: Uses asymmetric pre-shared keys to authenticate with the remote 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.
        - **RSA signature**: Uses a private RSA key to authenticate with the remote peer.
            i. For **Private key**, paste the device's private RSA key in PEM format.
            ii. Type the **Private key passphrase** that is used to decrypt the private key. Leave blank if the private key is not encrypted.
            iii. For **Peer public key**, paste the peer's public RSA key in PEM format.
        - **SCEP certificates**: Uses Simple Certificate Enrollment Protocol (SCEP) to download a private key, certificates, and an optional Certificate Revocation List (CRL) to the Connect EZ device from a SCEP server.

          You must create the SCEP client prior to configuring the IPsec tunnel. See Configure a Simple Certificate Enrollment Protocol client for instructions.
            i. For **SCEP Client**, select the SCEP client.
        - **X.509 certificate**: Uses private key and X.509 certificates to authenticate with the remote peer.
            i. For **Private key**, paste the device's private RSA key in PEM format.
            ii. Type the **Private key passphrase** that is used to decrypt the private key. Leave blank if the private key is not encrypted.
            iii. For **Certificate**, paste the local X.509 certificate in PEM format.

iv. For Peer verification, select either:

- **Peer certificate**: For **Peer certificate**, paste the peer's X.509 certificate in PEM format.
- **Certificate Authority**: For **Certificate Authority chain**, paste the Certificate Authority (CA) certificates. These must include all peer certificates in the chain up to the root CA certificate, in PEM format.

15. (Optional) For **Management Priority**, set the management priority for this IPsec tunnel. A tunnel that is up and has the highest priority will be used for central management and direct device access.
16. (Optional) To configure the device to connect to its remote peer as an XAUTH client:
    a. Click to expand **XAUTH client**.



    b. Click **Enable**.
    c. Type the **Username** and **Password** that the device will use to authenticate as an XAUTH client with the peer.
17. (Optional) Click **Enable MODECFG client** to receive configuration information, such as the private IP address, from the remote peer.
18. Click to expand **Local endpoint**.
    a. For **Type**, select either:
        - **Default route**: Uses the same network interface as the default route.
        - **Interface**: Select the **Interface** to be used as the local endpoint.
    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.

19. 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.

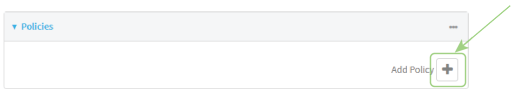
- **KeyID**: The ID will be interpreted as a Key ID and sent as an ID_KEY_ID IKE identity.

  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.

20. Click to expand **Policies**.

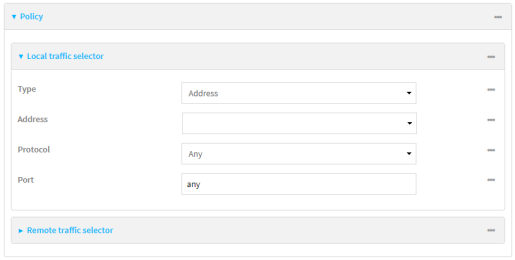
    Policies define the network traffic that will be encapsulated by this tunnel.

    a. Click ✚ to create a new policy.



    The new policy configuration is displayed.

    b. Click to expand **Local traffic selector**.



    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:

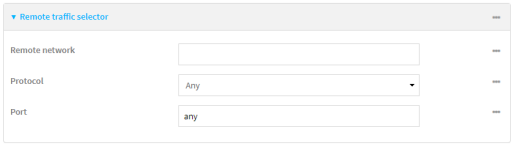
    - **Any**: Matches any protocol.
    - **TCP**: Matches TCP protocol only.
    - **UDP**: Matches UDP protocol only.
    - **ICMP**: Matches ICMP requests only.
    - **Other protocol**: Matches an unlisted protocol.

      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**.



g. For **Remote network**, enter the IP address and optional netmask of the remote network.

h. For **Protocol**, select one of the following:

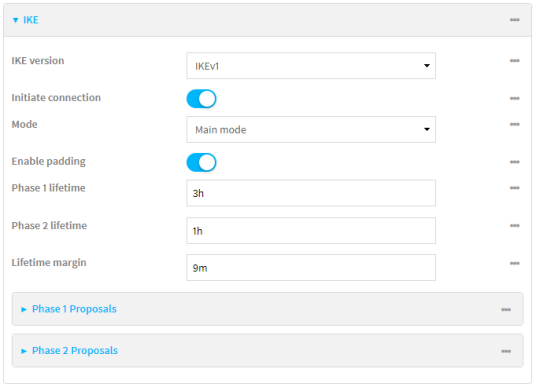
- **Any**: Matches any protocol.
- **TCP**: Matches TCP protocol only.
- **UDP**: Matches UDP protocol only.
- **ICMP**: Matches ICMP requests only.
- **Other protocol**: Matches an unlisted protocol.

  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**.

21. Click to expand **IKE**.



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** > **Hostname** 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**.

22. (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.

23. (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.

24. See Configure SureLink active recovery for IPsec for information about IPsec **Active recovery**.

25. (Optional) Click **Advanced** to set various IPsec-related time out, keep alive, and related values.

26. 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. 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:
    a. 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.

    b. 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**, **aes192**, **aes256**, or **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**, or **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**, **aes192**, **aes256**, or **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**, or **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:

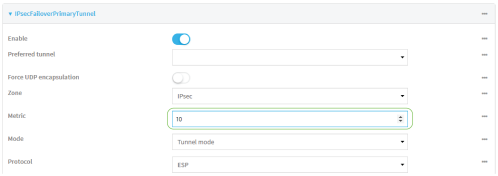
- **Metric**: 20
- **Local endpoint** > **Interface**: ETH2
- **Remote endpoint** > **Hostname**: 192.168.10.1

In this configuration:

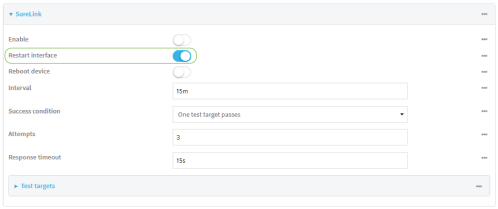
1. Tunnel_1 will normally be used for traffic destined for the 192.168.10.1 endpoint.
2. If pings to 192.168.10.2 fail, SureLink will shut down the tunnel and renegotiate its IPsec connection.
3. While Tunnel_1 is down, Tunnel_2 will be used for traffic destined for the 192.168.10.1 endpoint.

WebUI

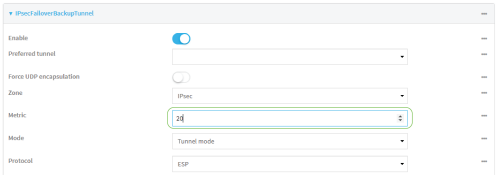
1. Configure the primary IPsec tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a low value (for example, **10**).



   - Configure SureLink for the primary IPsec tunnel and enable **Restart interface**. See Configure SureLink active recovery for IPsec for instructions.



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**).



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)>
```

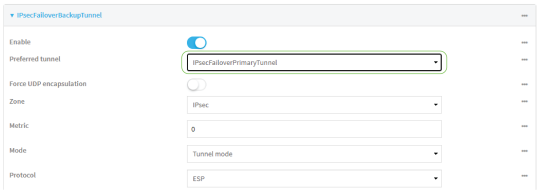
2. Create a backup IPsec tunnel. Configure this tunnel to use the same local and remote endpoints as the primary tunnel. See Configure an IPsec tunnel for instructions.
   - During configuration of the IPsec tunnel, set the metric to a value that is higher than the metric of the primary tunnel (for example, **20**):

```
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)> metric 20
(config vpn ipsec tunnel IPsecFailoverBackupTunnel)>
```

IPsec failover using Preferred tunnel

WebUI

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:



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 active recovery.
- The behavior of the Connect EZ device upon IPsec failure: either
  - Restart the IPsec interface
  - Reboot the device.

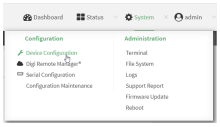
Additional configuration items

- 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 attempts before the IPsec connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

To configure the Connect EZ device to regularly probe the IPsec connection:

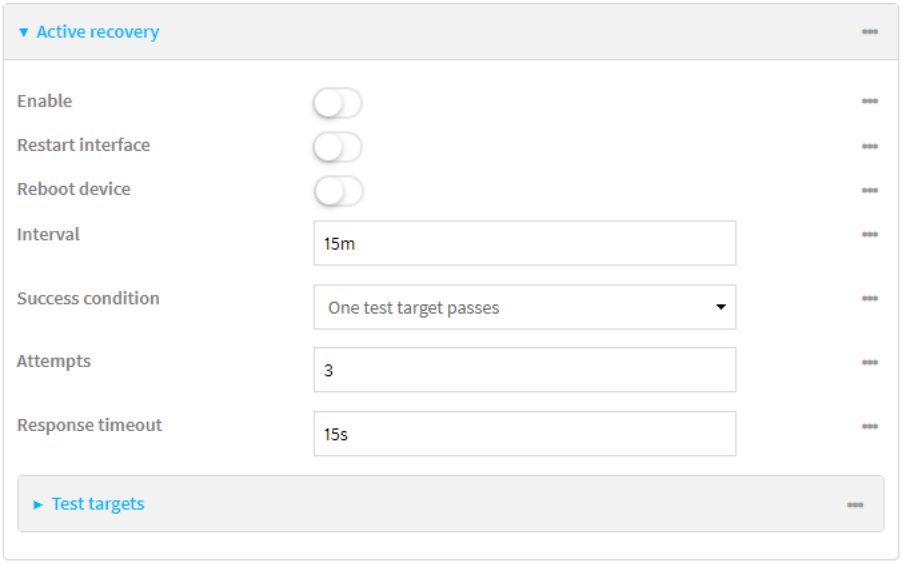
WebUI

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 **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 **Active recovery**.



6. **Enable** active recovery.
7. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
8. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.
9. Change the **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.
10. For **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
11. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.

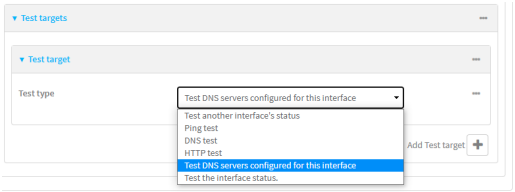
12. For **Response timeout**, type the amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

    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.

13. Add a test target:
    a. Click to expand **Test targets**.
    b. For **Add Test target**, click **+**.
    c. Select the **Test type**:



- **Test another interface's status**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces. If **Test another interface's status** is selected:
  - For **Test Interface**, select the alternate interface to be tested.
  - For **IP version**, select the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.
  - For **Expected status**, select whether the expected status of the alternate interface is **Up** or **Down**. For example, if **Expected status** is set to **Down**, but the alternate interface is determined to be up, then this test will fail.
- **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
- **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
- **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
- **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

    The default is 60 seconds.
  - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

The default is 60 seconds.

14. 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 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 active recovery:

```
(config vpn ipsec tunnel ipsec_example)> surelink enable true
(config vpn ipsec tunnel ipsec_example)>
```

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

```
(config vpn ipsec tunnel ipsec_example)> surelink restart true
(config vpn ipsec tunnel ipsec_example)>
```

   This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

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

```
(config vpn ipsec tunnel ipsec_example)> surelink reboot enable
(config vpn ipsec tunnel ipsec_example)>
```

7. Set the **Interval** between connectivity tests:

```
(config vpn ipsec tunnel ipsec_example)> surelink interval 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 **interval** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> surelink interval 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is 15 minutes.

8. Determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

```
(config vpn ipsec tunnel ipsec_example)> surelink success_condition value
(config vpn ipsec tunnel ipsec_example)>
```

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

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

```
(config vpn ipsec tunnel ipsec_example)> surelink  attempts num
(config vpn ipsec tunnel ipsec_example)>
```

The default is **3**.

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

```
(config vpn ipsec tunnel ipsec_example)> surelink timeout 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example)> surelink timeout 600s
(config vpn ipsec tunnel ipsec_example)>
```

The default is 15 seconds.

11. Configure test targets:
    a. Add a test target:

```
(config vpn ipsec tunnel ipsec_example)> add surelink target end
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

    b. Set the test type:

```
(config vpn ipsec tunnel ipsec_example surelink target 0)> test value
(config vpn ipsec tunnel ipsec_example 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 vpn ipsec tunnel ipsec_example surelink target 0)>
    ping_host host
    (config vpn ipsec tunnel ipsec_example surelink target 0)>
    ```

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

    ```
    (config vpn ipsec tunnel ipsec_example surelink target 0)>
    ping_size [num]
    (config vpn ipsec tunnel ipsec_example 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 vpn ipsec tunnel ipsec_example surelink target 0)>
    dns_server ip_address
    (config vpn ipsec tunnel ipsec_example 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 vpn ipsec tunnel ipsec_example surelink target 0)>
    http_url value
    (config vpn ipsec tunnel ipsec_example 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 vpn ipsec tunnel ipsec_example surelink target 0)>
    interface_down_time value
    (config vpn ipsec tunnel ipsec_example 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example surelink target 0)>
interface_down_time 600s
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

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 vpn ipsec tunnel ipsec_example surelink target 0)>
interface_timeout value
(config vpn ipsec tunnel ipsec_example 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn ipsec tunnel ipsec_example surelink target 0)>
interface_timeout 600s
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

The default is 60 seconds.

- **other**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces:

```
(config vpn ipsec tunnel ipsec_example surelink target 0)>
other value
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

If **other** is set:

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

```
(config vpn ipsec tunnel ipsec_example surelink
target 0)> other_interface /network/interface/eth1
(config vpn ipsec tunnel ipsec_example surelink
target 0)>
```

  - Set the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.

```
(config vpn ipsec tunnel ipsec_example surelink target 0)>
other_ip_version value
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

where *value* is one of: **any**, **both**, **ipv4**, or **ipv6**.

  - Set the expected status of the alternate interface:

```
(config vpn ipsec tunnel ipsec_example surelink target 0)>
other_status value
(config vpn ipsec tunnel ipsec_example surelink target 0)>
```

where *value* is either **up** or **down**. For example, if **other_status** is set to **down**, but the alternate interface is determined to be up, then this test will fail.

12. Save the configuration and apply the change:

```
(config vpn ipsec tunnel ipsec_example connection_monitor target 0)> 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.

Show IPsec status and statistics

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status** > **IPsec**.

   The **IPsec** page appears.
3. 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. Log into the Connect EZ command line as a user with Admin access.

   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.

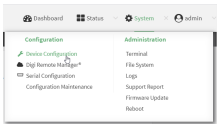
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

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.

WebUI

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 **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. 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. 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

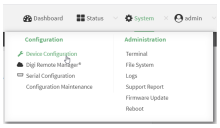
- Enable the SCEP client.
- The fully-qualified domain name of the SCEP server to be used for certificate requests.
- The challenge password provided by the SCEP server that the SCEP client will use when making SCEP requests.
- The distinguished name to be used for the CSR.
- The file name of the Certificate Revocation List (CRL) from the Certificate Authority (CA).

Additional configuration

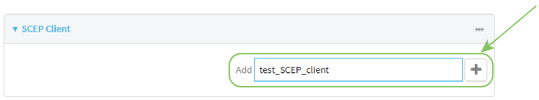
- The number of days that the certificate enrollment can be renewed, prior to the request expiring.

WebUI

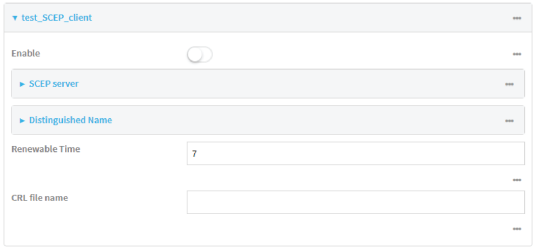
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Network** > **SCEP Client**.
4. For **Add clients**, enter a name for the SCEP client and click ✚.



   The new SCEP client configuration is displayed.

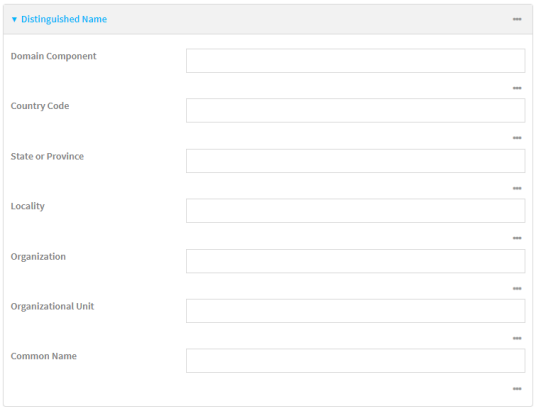


5. Click **Enable** to enable the SCEP client.
6. For **Renewable Time**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value is configured on the SCEP server, and is used by the Connect EZ device to determine when to start attempting to auto-renew an existing certificate. The default is **7**.
7. (Optional) For CRL file name, type the filename of the Certificate Revocation List (CRL) from the CA.

   The CRL is stored on the Connect EZ device in the /etc/config/scep_client/*client_name* directory.
8. Click to expand **SCEP server**.



9. For **FQDN**, type the fully qualified domain name or IP address of the SCEP server.
10. (Optiona) 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.
11. 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.
12. For **Password**, type the challenge password as configured on the SCEP server.
13. Click to expand **Distinguished Name**.



14. Type the value for each appropriate Distinguished Name attribute.
15. 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. 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. (Optiona) Set a CA idenity 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. 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)>
```

11. (Optional) Set the filename of the Certificate Revocation List (CRL) from the CA.

    The CRL is stored on the Connect EZ device in the /etc/config/scep_client/*client_name* directory.

```
(config network scep_client scep_client_name)> crl_name name
(config network scep_client scep_client_name)>
```

12. Save the configuration and apply the change:

```
(config network scep_client scep_client_name)> 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.

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:

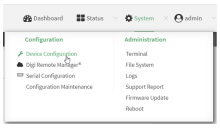
1. Enable ports for SCEP services:
   a. From the menu, select **Network** > **Interfaces**.
   b. Select the appopriate port and click **Edit**.
   c. For **Access Rights** > **Services**, enable the following services:
      - **HTTPS** > **SCEP**
      - **HTTPS** > **CRL Downloads**
      - **HTTP** > **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

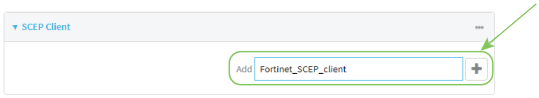
On the Connect EZ device:

WebUI

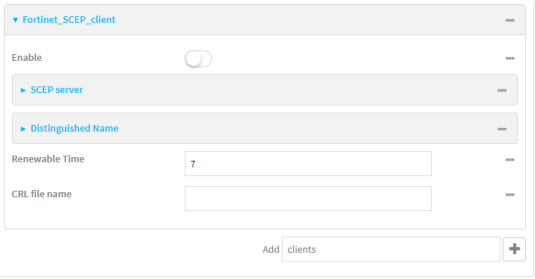
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



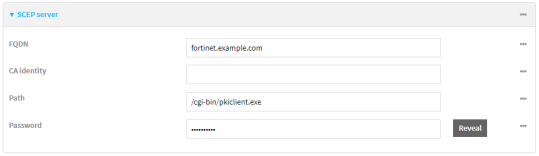
   The **Configuration** window is displayed.
3. Click **Network** > **SCEP Client**.
4. For **Add clients**, enter a name for the SCEP client and click **+**.



   The new SCEP client configuration is displayed.

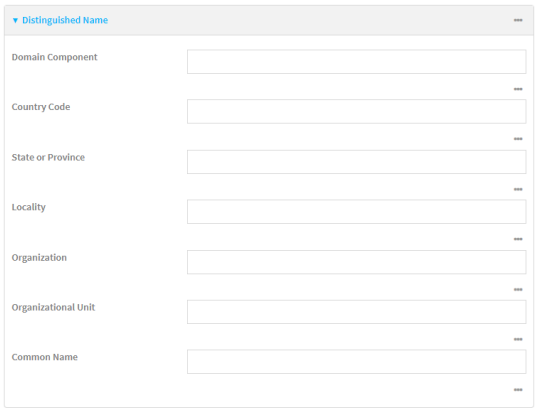


5. Click **Enable** to enable the SCEP client.
6. For **Renewable Time**, type the number of days that the certificate enrollment can be renewed, prior to the request expiring. This value must match the setting of the **Allow renewal *x* days before the certified is expired** option on the Fortinet server.
7. (Optional) For CRL file name, type the filename of the Certificate Revocation List (CRL) from the CA. The filename of the CRL corresponds to the Certificate ID of the CA created on the Fortinet server, for example, **fortinet_example_ca.crl**.
8. Click to expand **SCEP server**.



9. For **FQDN**, type the fully qualified domain name or IP address of the Fortinet server.
10. For **Password**, type the challenge password. This corresponds to the **Default enrollment password** on the Fortinet server.

11. Click to expand **Distinguished Name**.



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. 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. 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) Set the filename of the Certificate Revocation List (CRL) from the CA.

   The CRL is stored on the Connect EZ device in the /etc/config/scep_client/*client_name* directory.

```
(config network scep_client Fortinet_SCEP_client)> crl_name name
(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.

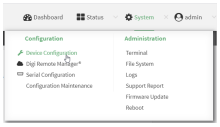
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Disable hardware cryptographic acceleration

If you are experiencing problems when using IPSEC, such as the kernel crashing or unexpected package loss, disabling hardware cryptographic acceleration may correct the problem.

WebUI

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. Select **System**.
4. Click to disable **HW crypto acceleration**.
5. Click **Apply** to save the configuration and apply the change.



The device must be rebooted for the change to take effect. See Reboot your Connect EZ device.

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. Disable hardware cryptographic acceleration:

```
(config)> system hycrypto false
>
```

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.

The device must be rebooted for the change to take effect. See Reboot your Connect EZ 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.

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).

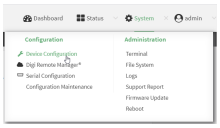
- Active recovery configuration. See Configure SureLink active recovery for OpenVPN for information about OpenVPN active recovery.

Additional configuration items

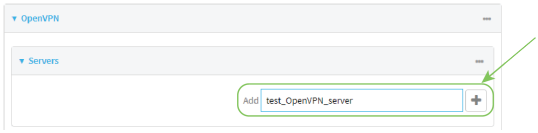
- The route metric for the OpenVPN server.
- The range of IP addresses that the OpenVPN server will provide to clients.
- The TCP/UDP port to use. By default, the Connect EZ device uses port **1194**.
- Access control list configuration to restrict access to the OpenVPN server through the firewall.
- Additional OpenVPN parameters.

WebUI

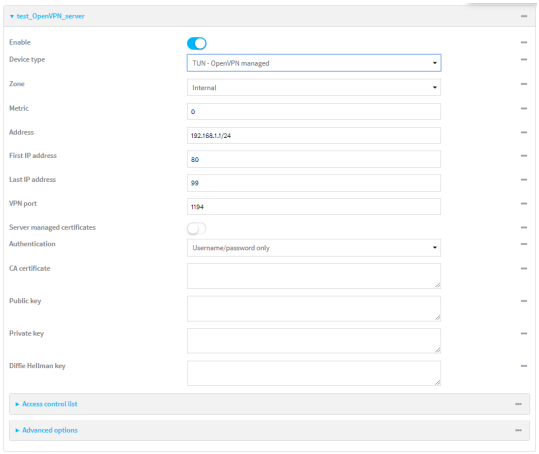
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **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, click **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 Connect EZ 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. 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. 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
     ```

     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 list 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.

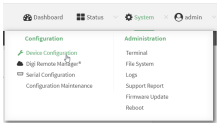
Configure an OpenVPN Authentication Group and User

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.

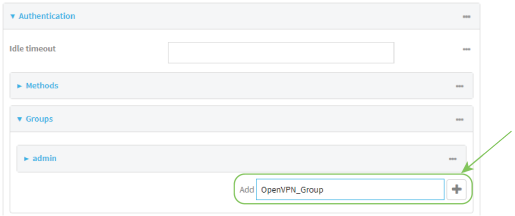
WebUI

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**.

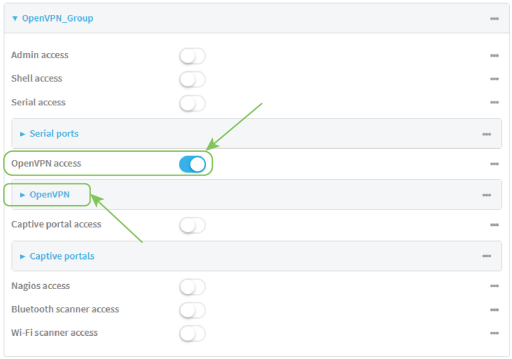


The **Configuration** window is displayed.

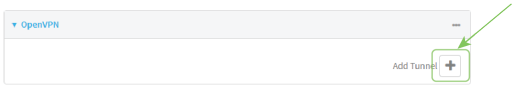
3. Add an OpenVPN authentication group:
   a. Click **Authentication** > **Groups**.
   b. For **Add Group**, type a name for the group (for example, **OpenVPN_Group**) and click ✚.



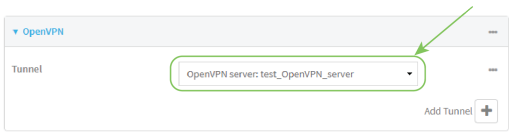
The new authentication group configuration is displayed.



   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.

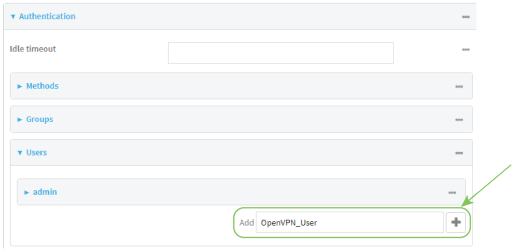


   f. For **Tunnel**, select an OpenVPN tunnel to which users of this group will have access.



   g. Repeat to add additional OpenVPN tunnels.

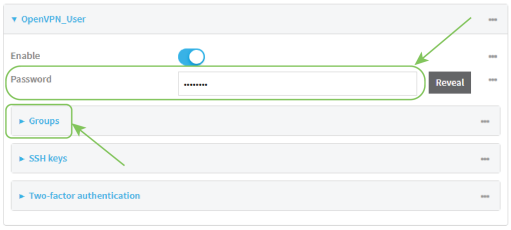
4. Add an OpenVPN authentication user:
   a. Click **Authentication** > **Users**.
   b. For **Add**, type a name for the user (for example, **OpenVPN_User**) and click **+**.



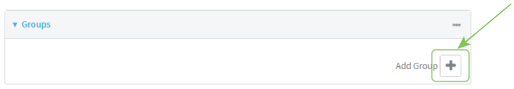
   c. Type a password for the user.

      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.

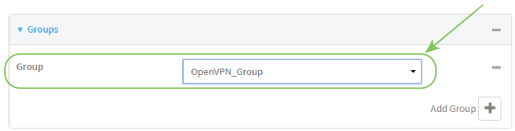
   d. Click to expand the **Groups** node.



   e. Click **+** to add a group to the user.



   f. Select a **Group** with **OpenVPN access** enabled.



5. 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. 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.

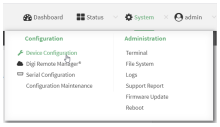
Additional configuration items

- 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.

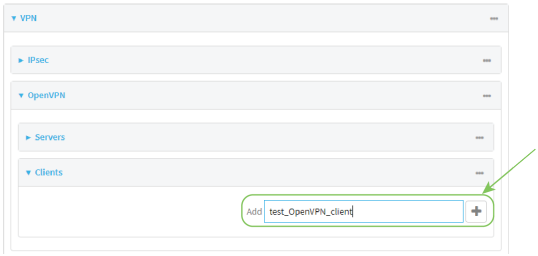
WebUI

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**.

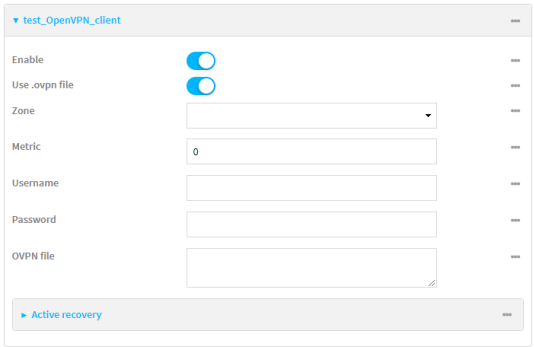


The **Configuration** window is displayed.

3. Click **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, click **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. 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. 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).

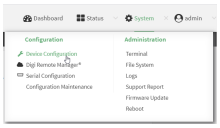
Additional configuration items

- 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.

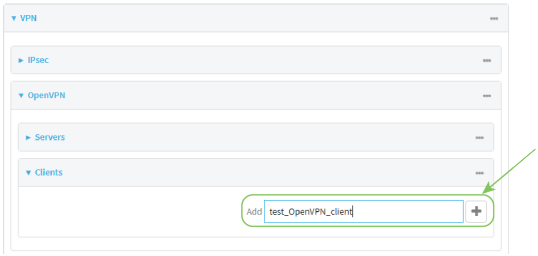
WebUI

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**.

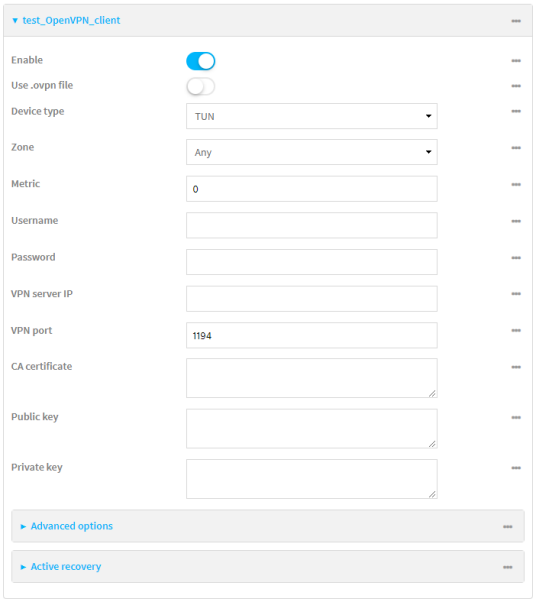


The **Configuration** window is displayed.

3. Click **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, click **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.
7. For **Device type**, select the mode used by the OpenVPN server, either **TUN** or **TAP**.
8. For **Zone**, select the firewall zone for the OpenVPN client.
9. (Optional) Select the **Metric** for the OpenVPN client. If multiple active routes match a destination, the route with the lowest metric will be used.
10. (Optional) For **Username** and **Password**, type the login credentials as configured on the OpenVPN server.
11. For **VPN server IP**, type the IP address of the OpenVPN server.
12. (Optional) Set the **VPN port** used by the OpenVPN server. The default is **1194**.
13. 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.
14. (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. 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. 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 active recovery.
- The behavior of the Connect EZ device upon OpenVPN failure: either
  - Restart the OpenVPN interface
  - Reboot the device.

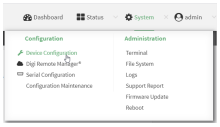
Additional configuration items

- 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 attempts before the OpenVPN connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

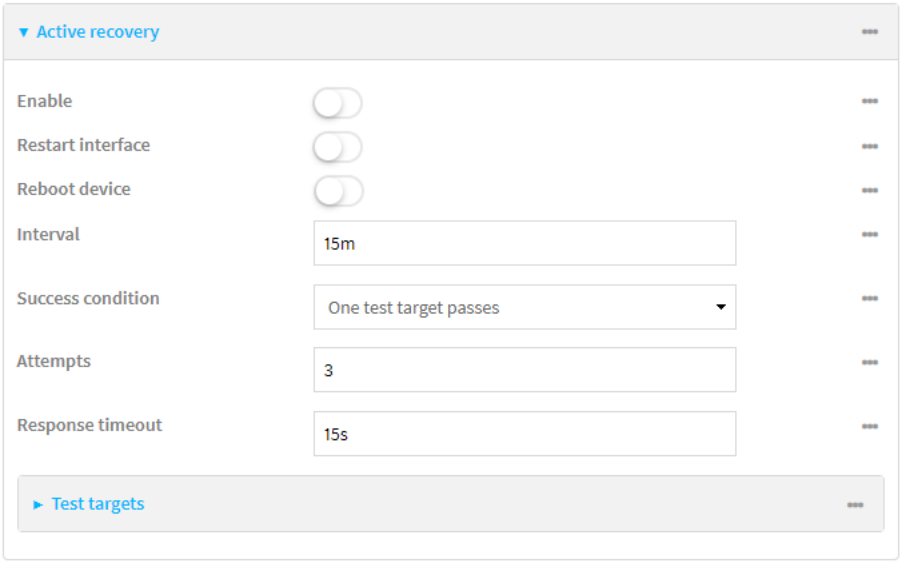
To configure the Connect EZ device to regularly probe the OpenVPN connection:

WebUI

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 **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 **Active recovery**.



6. **Enable** active recovery.
7. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
8. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.
9. Change the **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**.

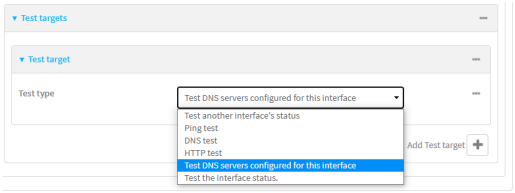
   The default is 15 minutes.
10. For **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.

11. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.
12. For **Response timeout**, type the amount of time that the device should wait for a response to a probe 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.
13. Add a test target:
    a. Click to expand **Test targets**.
    b. For **Add Test target**, click **+**.
    c. Select the **Test type**:



- **Test another interface's status**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces. If **Test another interface's status** is selected:
  - For **Test Interface**, select the alternate interface to be tested.
  - For **IP version**, select the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.
  - For **Expected status**, select whether the expected status of the alternate interface is **Up** or **Down**. For example, if **Expected status** is set to **Down**, but the alternate interface is determined to be up, then this test will fail.
- **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
- **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
- **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
- **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.
- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

    The default is 60 seconds.

- **Initial connection time**: The amount of time to wait for an initial connection to the interface before this 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**.

  The default is 60 seconds.

14. 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 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 active recovery:

```
(config vpn openvpn client openvpn_client1)> surelink enable true
(config vpn openvpn client openvpn_client1)>
```

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

```
(config vpn openvpn client openvpn_client1)> surelink restart true
(config vpn openvpn client openvpn_client1)>
```

   This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

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

```
(config vpn openvpn client openvpn_client1)> surelink reboot enable
(config vpn openvpn client openvpn_client1)>
```

7. Set the **Interval** between connectivity tests:

```
(config vpn openvpn client openvpn_client1)> surelink interval value
(config vpn openvpn client openvpn_client1)>
```

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 vpn openvpn client openvpn_client1)>
```

The default is 15 minutes.

8. Determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

```
(config vpn openvpn client openvpn_client1)> surelink success_condition
value
(config vpn openvpn client openvpn_client1)>
```

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

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

```
(config vpn openvpn client openvpn_client1)> surelink  attempts num
(config vpn openvpn client openvpn_client1)>
```

The default is **3**.

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

```
(config vpn openvpn client openvpn_client1)> surelink timeout value
(config vpn openvpn client openvpn_client1)>
```

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 vpn openvpn client openvpn_client1)>
```

The default is 15 seconds.

11. Configure test targets:
    a. Add a test target:

```
(config vpn openvpn client openvpn_client1)> add surelink target end
(config vpn openvpn client openvpn_client1 surelink target 0)>
```

b. Set the test type:

```
(config vpn openvpn client openvpn_client1 surelink target 0)> test
value
(config vpn openvpn client openvpn_client1 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 vpn openvpn client openvpn_client1 surelink target
    0)> ping_host host
    (config vpn openvpn client openvpn_client1 surelink target
    0)>
    ```

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

    ```
    (config vpn openvpn client openvpn_client1 surelink target
    0)> ping_size [num]
    (config vpn openvpn client openvpn_client1 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 vpn openvpn client openvpn_client1 surelink target
    0)> dns_server ip_address
    (config vpn openvpn client openvpn_client1 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 vpn openvpn client openvpn_client1 surelink target
    0)> http_url value
    (config vpn openvpn client openvpn_client1 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 vpn openvpn client openvpn_client1 surelink target
0)> interface_down_time value
(config vpn openvpn client openvpn_client1 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink target
0)> interface_down_time 600s
(config vpn openvpn client openvpn_client1 surelink target
0)>
```

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 vpn openvpn client openvpn_client1 surelink target
0)> interface_timeout value
(config vpn openvpn client openvpn_client1 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 **timeout** to ten minutes, enter either **10m** or **600s**:

```
(config vpn openvpn client openvpn_client1 surelink target
0)> interface_timeout 600s
(config vpn openvpn client openvpn_client1 surelink target
0)>
```

The default is 60 seconds.

- **other**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces:

```
(config vpn openvpn client openvpn_client1 surelink target
0)> other value
(config vpn openvpn client openvpn_client1 surelink target
0)>
```

If **other** is set:

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

```
(config vpn openvpn client openvpn_client1 surelink
target 0)> other_interface /network/interface/eth1
```

```
(config vpn openvpn client openvpn_client1 surelink
target 0)>
```

- Set the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.

```
(config vpn openvpn client openvpn_client1 surelink target
0)> other_ip_version value
(config vpn openvpn client openvpn_client1 surelink target
0)>
```

where *value* is one of: **any**, **both**, **ipv4**, or **ipv6**.

- Set the expected status of the alternate interface:

```
(config vpn openvpn client openvpn_client1 surelink target
0)> other_status value
(config vpn openvpn client openvpn_client1 surelink target
0)>
```

where *value* is either **up** or **down**. For example, if **other_status** is set to **down**, but the alternate interface is determined to be up, then this test will fail.

12. Save the configuration and apply the change:

```
(config vpn openvpn client openvpn_client1 connection_monitor target 0)>
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.

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:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status** > **OpenVPN** > **Servers**.

   The **OpenVPN Servers** page appears.
3. 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. Log into the Connect EZ command line as a user with Admin access.

   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:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status** > **OpenVPN** > **Clients**.

   The **OpenVPN Clients** page appears.
3. 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. Log into the Connect EZ command line as a user with Admin access.

   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.

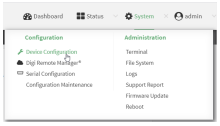
Additional configuration items

- A GRE key.
- Enable the device to respond to keepalive packets.

Task One: Create a GRE loopback endpoint interface

WebUI

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. 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, or to enable if it has been disabled, click **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. 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. 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.
>
```

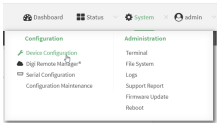
8. Type **exit** to exit the Admin CLI.

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

Task Two: Configure the GRE tunnel

WebUI

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 **VPN** > **IP Tunnels**.
4. For **Add IP tunnel**, type a name for the GRE tunnel and click ✚.
5. **Enable** the tunnel.

   New tunnels are enabled by default. To disable, or to enable if it has been disabled, click **Enable**.
6. For **Local endpoint**, select the GRE endpoint interface created in Task One.
7. For **Remote endpoint**, type the IP address of the GRE endpoint on the remote peer.
8. (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 interger between 0 and 4294967295, or an IP address.
9. (Optional) **Enable keepalive reply** to enable the device to reply to Cisco GRE keepalive packets.
10. 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. 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 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)>
```

5. 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)>
```

6. (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 interger between 0 and 4294967295, or an IP address.

7. (Optional) Enable the device to reply to Cisco GRE keepalive packets:

```
(config vpn iptunnel gre_example)> keepalive true
(config vpn iptunnel gre_example)>
```

8. Save the configuration and apply the change:

```
(config vpn iptunnel gre_example)> 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 GRE tunnels

To view information about currently configured GRE tunnels:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **Status** > **IP tunnels**.

   The **IP Tunnels**page appears.
3. 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**.

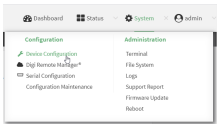
3. Create a GRE tunnel named **gre_tunnel2**:
   a. **Local endpoint** set to the IPsec endpoint interface, **Interface: ipsec_endpoint2**.
   b. Remote endpoint set to the IP address of the GRE tunnel on Connect EZ-1, **172.30.0.1**.
4. Create an interface named **gre_interface2** and add it to the 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, **172.31.1.1/30**.

Configuration procedures

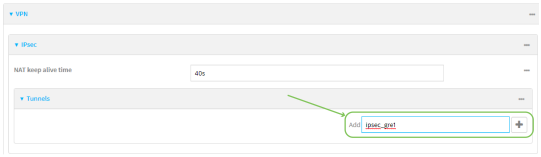
Configure the Connect EZ-1 device
Task one: Create an IPsec tunnel

WebUI

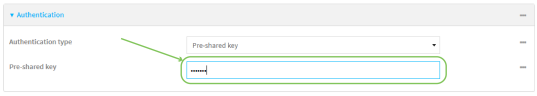
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



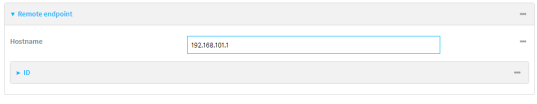
   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec** > **Tunnels**.
4. For **Add IPsec Tunnel**, type **ipsec_gre1** and click ✚.



5. Click to expand **Authentication**.
6. For **Pre-shared key**, type **testkey**.

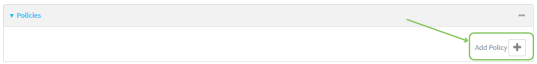


7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the Connect EZ-2 device.

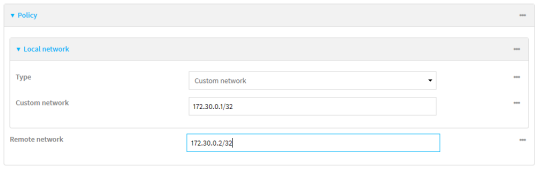


9. Click to expand **Policies**.

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, **172.30.0.1/32**.
14. For **Remote network**, type the IP address and subnet of the remote GRE tunnel, **172.30.0.2/32**.



15. 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. 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)>
```

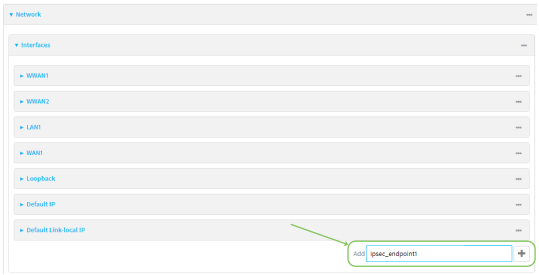
10. Save the configuration and apply the change:

```
(config ipsec tunnel ipsec_gre1 policy 0)> save
Configuration saved.
>
```

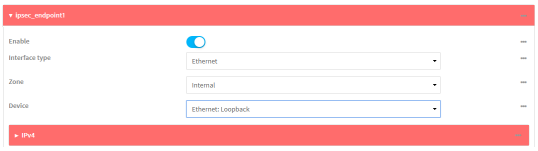
Task two: Create an IPsec endpoint interface

WebUI

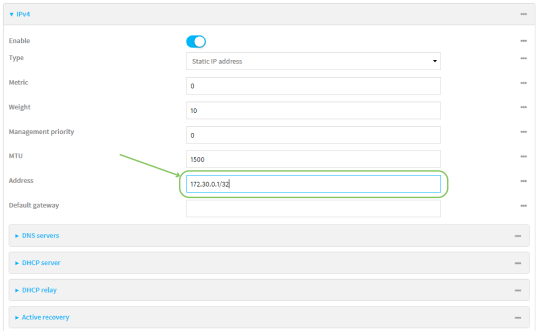
1. Click **Network** > **Interface**.
2. For **Add Interface**, type **ipsec_endpoint1** and click **+**.



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)>
```

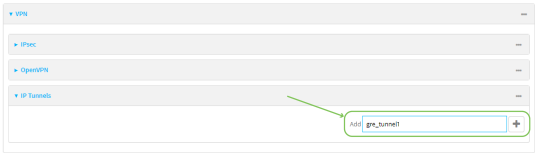
6. Save the configuration and apply the change:

```
(config vpn ipsec tunnel ipsec_endpoint1 policy 0)> save
Configuration saved.
>
```

Task three: Create a GRE tunnel

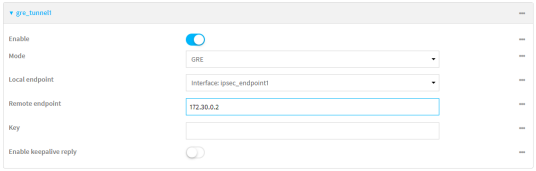
WebUI

1. Click **VPN** > **IP Tunnels**.
2. For **Add IP Tunnel**, type **gre_tunnel1** and click **+**.

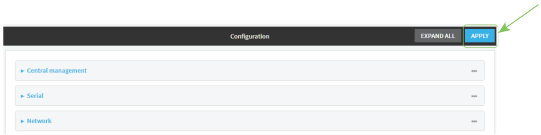


3. For **Local endpoint**, select the IPsec endpoint interface created in Task two (**Interface: ipsec_endpoint1**).

4. For **Remote endpoint**, type the IP address of the GRE tunnel on Connect EZ-2, **172.30.0.2**.



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)>
```

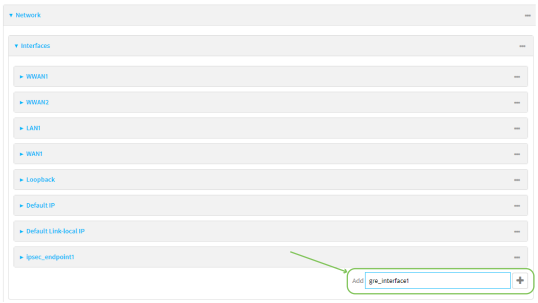
5. Save the configuration and apply the change:

```
(config vpn iptunnel gre_tunnel1)> save
Configuration saved.
>
```

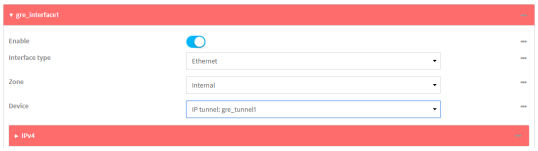
Task four: Create an interface for the GRE tunnel device

WebUI

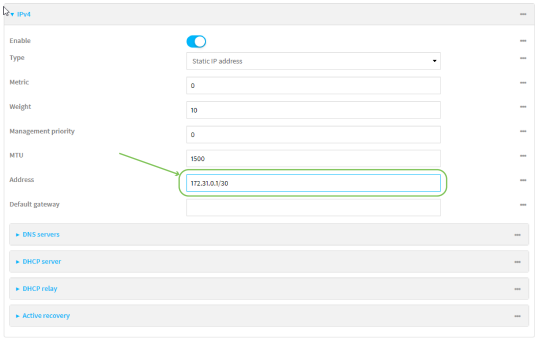
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **gre_interface1** and click **+**.



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.
>
```

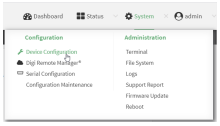
7. Type **exit** to exit the Admin CLI.

   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

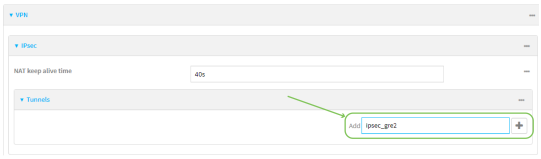
WebUI

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**.

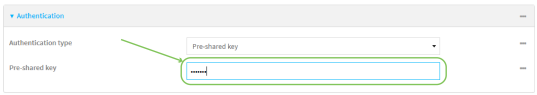


   The **Configuration** window is displayed.
3. Click **VPN** > **IPsec** > **Tunnels**.

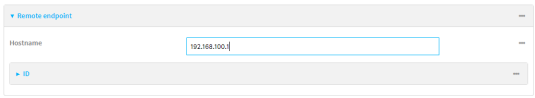
4. For **Add IPsec Tunnel**, type **ipsec_gre2** and click ✚.



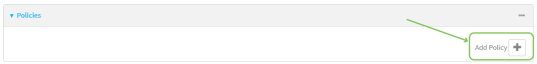
5. Click to expand **Authentication**.
6. For **Pre-shared key**, type the same pre-shared key that was configured for the Connect EZ-1 (**testkey**).



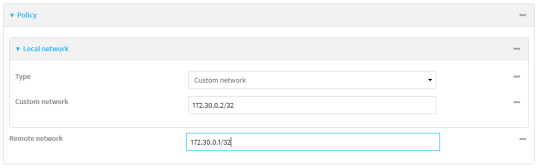
7. Click to expand **Remote endpoint**.
8. For **Hostname**, type public IP address of the Connect EZ-1 device.



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**.



15. 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. Add an IPsec tunnel named **ipsec_gre2**:

```
(config)> add vpn ipsec tunnel ipsec_gre2
(config vpn ipsec tunnel ipsec_gre2)>
```

4. 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)>
```

5. 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)>
```

6. Add a policy:

```
(config vpn ipsec tunnel ipsec_gre2)> add policy end
(config vpn ipsec tunnel ipsec_gre2 policy 0)>
```

7. 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)>
```

8. 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)>
```

9. 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)>
```

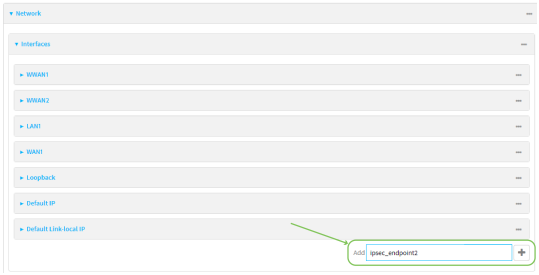
10. Save the configuration and apply the change:

```
(config vpn ipsec tunnel ipsec_gre2 policy 0)> save
Configuration saved.
>
```

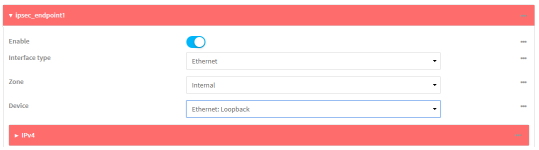
Task two: Create an IPsec endpoint interface

WebUI

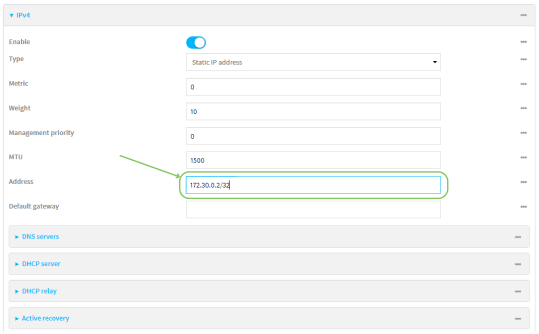
1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **ipsec_endpoint2** and click **+**.



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.
>
```

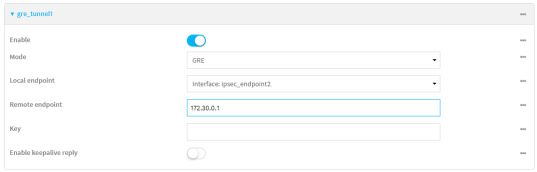
Task three: Create a GRE tunnel

WebUI

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)>
```

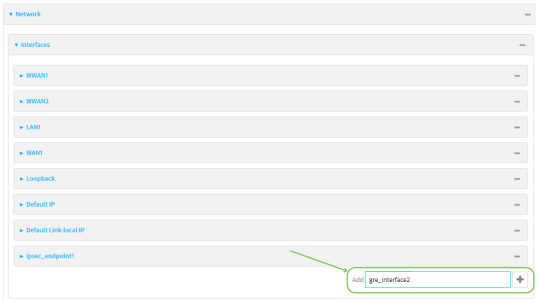
5. Save the configuration and apply the change:

```
(config vpn iptunnel gre_tunnel2)> save
Configuration saved.
>
```

Task four: Create an interface for the GRE tunnel device

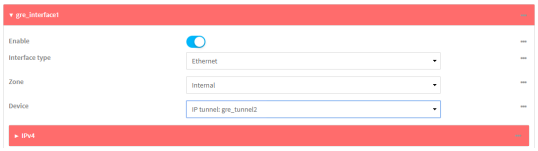
WebUI

1. Click **Network** > **Interfaces**.
2. For **Add Interface**, type **gre_interface2** and click **+**.

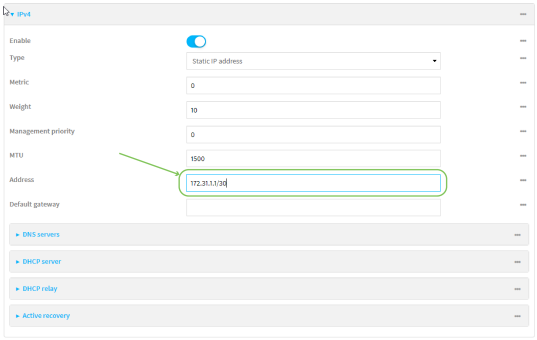


3. For **Zone**, select **Internal**.

4. For **Device**, select the GRE tunnel created in Task three (**IP tunnel: gre_tunnel2**).



5. Click to expand **IPv4**.
6. For **Address**, type **172.31.1.1/30** 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_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 **172.31.0.1/30** as the virtual IP address on the GRE tunnel:

```
(config network interface gre_interface2)> ipv4 address 172.31.1.1/30
(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.

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.

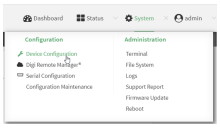
Additional configuration items

- The UDP port that L2TP servers will listen on, if other than the deafult 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.
  - SureLink options for the tunnel.

- 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.

WebUI

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 **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 Connect EZ 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, click to 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.
   k. For SureLink, see Configure SureLink active recovery for PPP-over-L2TP.
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, click to toggle off **Enable**.
   d. For **L2TP access concentrator**, type the IP addressof 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**.

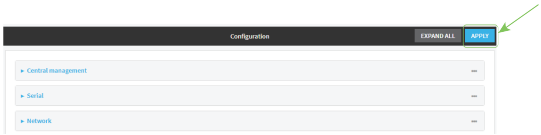
h. (Optional) For **Authentication method**, select the authentication method, one of:
   - **None**: No authentication is required.
   - **Automatic**: The device will attempt to connect using CHAP first, and then PAP.
   - **CHAP**: Uses the Challenge Handshake Authentication Profile (CHAP) to authenticate.
   - **PAP**: Uses the Password Authentication Profile (PAP) to authenticate.
   - If **Automatic**, **CHAP**, or **PAP** 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. 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. (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
```

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 list 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)>
```

i. To configure SureLink active recovery for the L2TP access connector, see Configure SureLink active recovery for PPP-over-L2TP.

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.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.

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.

If **auto**, **chap**, or **pap** 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.

Configure SureLink active recovery for PPP-over-L2TP

You can configure the Connect EZ device to regularly probe PPP-over-L2TP access concatenators to determine if the connection has failed and take remedial action.

Required configuration items

- A valid PPP-over-L2TP configuration. See Configure a PPP-over-L2TP tunnel for configuration instructions.
- Enable PPP-over-L2TP active recovery.
- The behavior of the Connect EZ device upon PPP-over-L2TP failure: either
  - Restart the PPP-over-L2TP interface
  - Reboot the device.

Additional configuration items

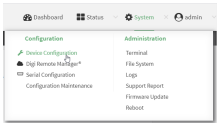
- The interval between connectivity tests.
- Whether the interface should be considered to have failed if one of the test targets fails, or all of the test targets fail.

- The number of probe attempts before the PPP-over-L2TP connection is considered to have failed.
- The amount of time that the device should wait for a response to a probe attempt before considering it to have failed.

To configure the Connect EZ device to regularly probe the PPP-over-L2TP connection:

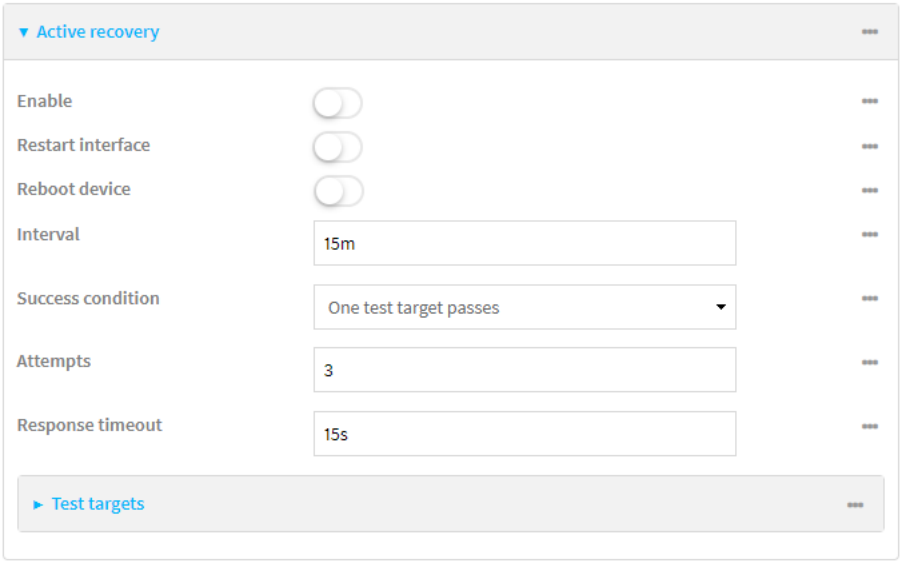
WebUI

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 **VPN** > **PPP-over-L2TP**.
4. Create a new PPP-over-L2TP access concatenator or select an existing one:
   - To create a new L2TP access concatenator , see Configure a PPP-over-L2TP tunnel.
   - To edit an existing L2TP access concatenator , click to expand the appropriate tunnel.
5. After creating or selecting the PPP-over-L2TP access concatenator, click **Active recovery**.



6. **Enable** active recovery.
7. For **Restart interface**, enable to configure the device to restart the interface when its connection is considered to have failed. This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.
8. For **Reboot device**, enable to instruct the device to reboot when the WAN connection is considered to have failed.

9. Change the **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**}.

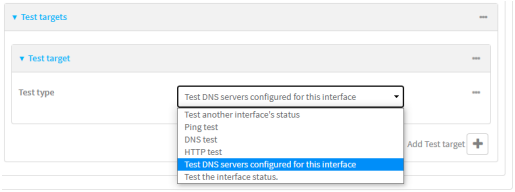
   For example, to set **Interval** to ten minutes, enter **10m** or **600s**.

   The default is 15 minutes.
10. For **Success condition**, determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets.
11. For **Attempts**, type the number of probe attempts before the WAN is considered to have failed.
12. For **Response timeout**, type the amount of time that the device should wait for a response to a probe 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.
13. Add a test target:
    a. Click to expand **Test targets**.
    b. For **Add Test target**, click **+**.
    c. Select the **Test type**:



- **Test another interface's status**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces. If **Test another interface's status** is selected:
  - For **Test Interface**, select the alternate interface to be tested.
  - For **IP version**, select the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.
  - For **Expected status**, select whether the expected status of the alternate interface is **Up** or **Down**. For example, if **Expected status** is set to **Down**, but the alternate interface is determined to be up, then this test will fail.
- **Ping test**: Tests connectivity by sending an ICMP echo request to the hostname or IP address specified in **Ping host**. You can also optionally change the number of bytes in the **Ping payload size**.
- **DNS test**: Tests connectivity by sending a DNS query to the specified **DNS server**.
- **HTTP test**: Tests connectivity by sending an HTTP or HTTPS GET request to the URL specified in **Web servers**. The URL should take the format of **http[s]://*hostname*/[*path*]**.
- **Test DNS servers configured for this interface**: Tests connectivity by sending a DNS query to the DNS servers configured for this interface.

- **Test the interface status**: The interface is considered to be down based on:
  - **Down time**: The amount of time that the interface can be down before this 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 **Down time** to ten minutes, enter **10m** or **600s**.

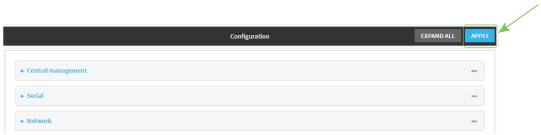
    The default is 60 seconds.
  - **Initial connection time**: The amount of time to wait for an initial connection to the interface before this test is considered to have failed.

    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**.

    The default is 60 seconds.

14. 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 PPP-over-L2TP access concatenator , or edit an existing one:
   - To create a new PPP-over-L2TP access concatenator , see Configure a PPP-over-L2TP tunnel.
   - To edit an existing PPP-over-L2TP access concatenator , change to the PPP-over-L2TP access concatenator node in the configuration schema. For example, for an PPP-over-L2TP access concatenator named **lac_tunnel**, change to the **lac_tunnel** node in the configuration schema:

```
(config)> vpn l2tp lac lac_tunnel
(config vpn l2tp lac lac_tunnel)>
```

4. Enable active recovery:

```
(config vpn l2tp lac lac_tunnel)> surelink enable true
(config vpn l2tp lac lac_tunnel)>
```

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

```
(config vpn l2tp lac lac_tunnel)> surelink restart true
(config vpn l2tp lac lac_tunnel)>
```

This is useful for interfaces that may regain connectivity after restarting, such as a cellular modem.

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

```
(config vpn l2tp lac lac_tunnel)> surelink reboot enable
(config vpn l2tp lac lac_tunnel)>
```

7. Set the **Interval** between connectivity tests:

```
(config vpn l2tp lac lac_tunnel)> surelink interval value
(config vpn l2tp lac lac_tunnel)>
```

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 l2tp lac lac_tunnel)> surelink interval 600s
(config vpn l2tp lac lac_tunnel)>
```

The default is 15 minutes.

8. Determine whether the interface should fail over based on the failure of one of the test targets, or all of the test targets:

```
(config vpn l2tp lac lac_tunnel)> surelink success_condition value
(config vpn l2tp lac lac_tunnel)>
```

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

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

```
(config vpn l2tp lac lac_tunnel)> surelink  attempts num
(config vpn l2tp lac lac_tunnel)>
```

The default is **3**.

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

```
(config vpn l2tp lac lac_tunnel)> surelink timeout value
(config vpn l2tp lac lac_tunnel)>
```

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 l2tp lac lac_tunnel)> surelink timeout 600s
(config vpn l2tp lac lac_tunnel)>
```

The default is 15 seconds.

11. Configure test targets:
    a. Add a test target:

```
(config vpn l2tp lac lac_tunnel)> add surelink target end
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

    b. Set the test type:

```
(config vpn l2tp lac lac_tunnel surelink target 0)> test value
(config vpn l2tp lac lac_tunnel 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 vpn l2tp lac lac_tunnel surelink target 0)> ping_host
host
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

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

```
(config vpn l2tp lac lac_tunnel surelink target 0)> ping_size
[num]
(config vpn l2tp lac lac_tunnel 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 vpn l2tp lac lac_tunnel surelink target 0)> dns_
server ip_address
(config vpn l2tp lac lac_tunnel 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 vpn l2tp lac lac_tunnel surelink target 0)> http_url
value
(config vpn l2tp lac lac_tunnel 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 vpn l2tp lac lac_tunnel surelink target 0)>
interface_down_time value
(config vpn l2tp lac lac_tunnel 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 **interval** to ten minutes, enter either **10m** or **600s**:

```
(config vpn l2tp lac lac_tunnel surelink target 0)>
interface_down_time 600s
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

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 vpn l2tp lac lac_tunnel surelink target 0)>
interface_timeout value
(config vpn l2tp lac lac_tunnel 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 **interval** to ten minutes, enter either **10m** or **600s**:

```
(config vpn l2tp lac lac_tunnel surelink target 0)>
interface_timeout 600s
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

The default is 60 seconds.

- **other**: Allows you to test another interface's status, to create a failover or coupled relationship between interfaces:

```
(config vpn l2tp lac lac_tunnel surelink target 0)> other
value
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

If **other** is set:

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

```
(config vpn l2tp lac lac_tunnel surelink target 0)>
other_interface /network/interface/eth1
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

  - Set the alternate interface's IP version. This allows you to determine the alternate interface's status for a particular IP version.

```
(config vpn l2tp lac lac_tunnel surelink target 0)> other_
ip_version value
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

where *value* is one of: **any**, **both**, **ipv4**, or **ipv6**.

- Set the expected status of the alternate interface:

```
(config vpn l2tp lac lac_tunnel surelink target 0)> other_
status value
(config vpn l2tp lac lac_tunnel surelink target 0)>
```

where *value* is either **up** or **down**. For example, if **other_status** is set to **down**, but the alternate interface is determined to be up, then this test will fail.

See Show Surelink status and statistics for information about showing Surelink status for IPsec tunnels.

L2TP with IPsec

L2TP is commonly used in conjunction with IPsec in transport mode (to provide security).

Your Connect EZ supoorts 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

WebUI

Show the status of L2TP access connectors from the WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status**. Under VPN, select **L2TP** > **Access Connectors**.

   The **L2TP Access Connectors** page appears.
3. 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

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status**. Under VPN, select **L2TP** > **Network Servers**.

   The **L2TP Network Servers** page appears.
3. 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. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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

>
```

3. To display details about a specific tunnel:

```
> show l2tp lns name lns_test2

 lns_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.

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.

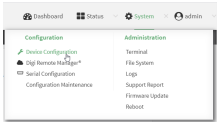
Additional configuration items

- 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.

WebUI

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 **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. 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. 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 **upd**.

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

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status**. Under VPN, select **L2TPv3 Ethernet**.

   The **L2TPv3 Ethernet** page appears.
3. To view configuration details about an L2TPV3 tunnel, click the (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 L2TPv3 Ethernet tunnels, type the following at the prompt:

```
> show l2tpeth

 Tunnel Session     Enabled  Device        Status
 -----------------  -------  ------------  ------
 test/session/test  true     le_test_test  up

>
```

3. 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 Byptes                : 3,120

>
```

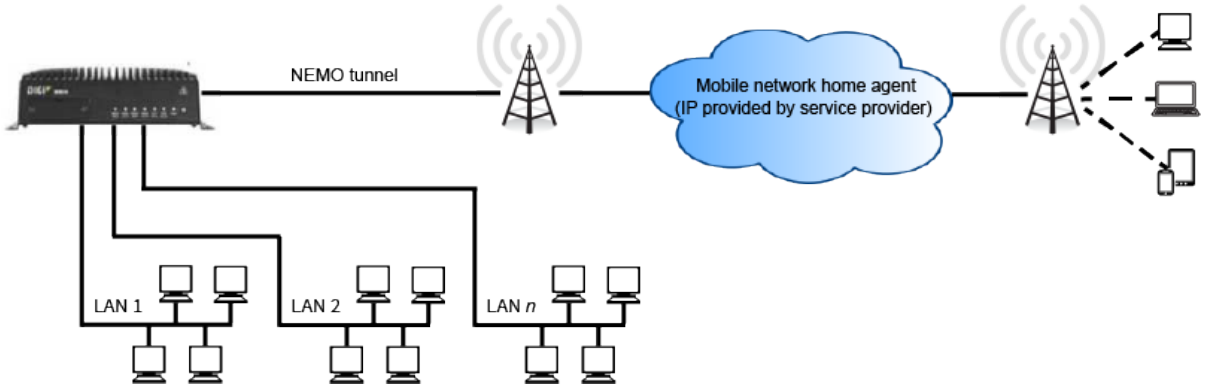
4. Type **exit** to exit the Admin CLI.

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

NEMO

Network Mobility (NEMO) is a mobile networking technology that provides access to one or more Local Area Networks (LANs) on your device. NEMO creates a tunnel between the home agent on the mobile private network and the Connect EZ device, isolating the connection from internet traffic and advertising the IP subnets of the LANs for remote access and device management.

Dynamic Mobile Network Routing (DMNR) is the implementation of NEMO for Verizon Wireless Private Networks. DMNR support requires the use of Verizon SIM cards that have DMNR enabled.



Configure a NEMO tunnel

Configuring an NEMO tunnel with a remote device involves configuring the following items:

Required configuration items

- Enable the NEMO tunnel.

  The NEMO tunnel is enabled by default.
- The IP address of the NEMO virtual network interface.
- The firewall zone of the NEMO tunnel.
- The IP address of the NEMO home agent server. This is provided by your cellular carrier.
- The home agent's authentication key. This is provided by your cellular carrier.
- Home agent registration lifetime. This is provided by your cellular carrier.
- The local network interfaces that will be advertised on NEMO.

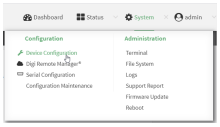
Additional configuration items

- The home agent Software Parameter Index (SPI).
- Path MTU discovery.

  Path MTU discovery is enabled by default. If it is disabled, identify the MTU.
- Care of address: the local network interface that is used to communicate with the peer.
  - If set to **Interface**, identify the local interface to be used. Generally, this will be the Wirelesss WAN (**Modem**).
  - If set to **IP address**, enter the IP address.
- The local network of the GRE endpoint negotiated by NEMO.
  - If the local network is set to Interface, identify the local interface to be used.

WebUI

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 **VPN** > **NEMO**.

The NEMO tunnel is enabled by default. To disable, click to toggle off **Enable**.

4. For **Home IP address**, type the IPv4 address of the NEMO virtual network interface.
5. For **Zone**, select **Internal**.

The Internal firewall zone configures the Connect EZ device to trust traffic going to the tunnel and allows it through the network.

6. For **Home agent server IP** address, type the IPv4 address of the NEMO home agent. This is provided by your cellular carrier.
7. For **Key**, type the key used to authenticate to the home agent. This is provided by your cellular carrier.
8. For **Home agent SPI**, type the Security Parameter Index (SPI) value, which is used in the authentication extension when registering. This should be normally left at the default setting of **256** unless your service provider indicates a different value.
9. For **Home agent registration lifetime, in seconds**, type the number of seconds number of seconds until the authorization key expires. This is provided by your cellular carrier.
10. For **MTU discovery**, leave enabled to determine the maximum transmission unit (MTU) size.

If disabled, for **MTU**, type the MTU size. The default MTU size for LANs on the Connect EZ device is 1500. The MTU size of the NEMO tunnel will be smaller, to take into account the required headers.

11. Click to expand **Care of address** to configure the local WAN interface of the internet facing network.
    a. For **Type**, select the method to determine the local network interface that is used to communicate with the peer.
        - If **Default route** is selected, the network interface that is used will be the same as the default route.
        - If **Interface** is selected, specify the local network interface.
        - If **IP address** is selected, type the IP address.

    The default is **Default route**.
12. Click to expand **GRE tunnel local endpoint**.
    a. For **Type**, select the local endpoint of the GRE endpoint negotiated by NEMO.
        - If **Default route** is selected, the network interface that is used will be the same as the default route.
        - If **Interface** is selected, specify the local network interface.

    The default is **Default route**.

13. Click to expand **Local networks**.
    a. For **Add Interface**, click ✚ to add a local network to use as a virtual NEMO network interface.



    b. For **Interface**, select the local interface to use as a virtual NEMO network interface. Generally, this will be the a Local Area Network (LAN).
    c. (Optional) Repeat for additional interfaces.
14. 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. Add a NEMO tunnel. For example, to add a NEMO tunnel named **nemo_example**:

```
(config)> add vpn nemo nemo_example
(config vpn nemo nemo_example)>
```

   The NEMO tunnel is enabled by default. To disable:

```
(config vpn nemo nemo_example)> enable false
(config vpn nemo nemo_example)>
```

4. Set the IPv4 address of the NEMO virtual network interface:

```
(config vpn nemo nemo_example)> home_address IPv4_address
(config vpn nemo nemo_example)>
```

5. Set the IPv4 address of the NEMO home agent. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> home_agent IPv4_address
(config vpn nemo nemo_example)>
```

6. Set the key used to authenticate to the home agent. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> key value
(config vpn nemo nemo_example)>
```

7. Set the the number of seconds number of seconds until the authorization key expires. This is provided by your cellular carrier.

```
(config vpn nemo nemo_example)> lifetime integer
(config vpn nemo nemo_example)>
```

   Allowed values are any integer between 1 and 65535.

8. MTU discovery is enabled by default, which allows the device to determine the maximum transmission unit (MTU) size. To disable:

```
(config vpn nemo nemo_example)> mtu_discovery false
(config vpn nemo nemo_example)>
```

   If disabled, set the MTU size. The default MTU size for LANs on the Connect EZ device is 1500. The MTU size of the NEMO tunnel will be smaller, to take into account the required headers.

```
(config vpn nemo nemo_example)> mtu integer
(config vpn nemo nemo_example)>
```

   Allowed values are any integer between 68 and 1476.

9. Set the Security Parameter Index (SPI) value, which is used in the authentication extension when registering. This should be normally left at the default setting of **256** unless your service provider indicates a different value.

```
(config vpn nemo nemo_example)> spi integer
(config vpn nemo nemo_example)>
```

   Allowed values are any integer between 256 and 4294967295.

10. Set the firewall zone for the NEMO tunnel to internal:

```
(config vpn nemo nemo_example)> zone internal
(config vpn nemo nemo_example)>
```

    The Internal firewall zone configures the Connect EZ device to trust traffic going to the tunnel and allows it through the network.

11. Configure the Care-of-Address, the local WAN interface of the internet facing network.
    a. Set the method to determine the Care-of-Address:

```
(config vpn nemo nemo_example)> coaddress type value
(config vpn nemo nemo_example)>
```

    where *value* is one of:

    - **defaultroute**: Uses the same network interface as the default route.
    - **interface**

      If **interface** is used, set the interface:

      i. Use the **?** to determine available interfaces:

      ii. Set the interface. For example:

```
(config vpn nemo nemo_example)> coaddress interface eth1
(config vpn nemo nemo_example)>
```

- **ip**

  If **ip** is used, set the IP address:

  ```
  (config vpn nemo nemo_example)> coaddress address IP_address
  (config vpn nemo nemo_example)>
  ```

The default is **defaultroute**.

12. Set the GRE tunnel local endpoint:
    a. Set the method to determine the GRE tunnel local endpoint:

    ```
    (config vpn nemo nemo_example)> tun_local type value
    (config vpn nemo nemo_example)>
    ```

    where *value* is one of:

    - **defaultroute**: Uses the same network interface as the default route.
    - **interface**

      If **interface** is used, set the interface.

      i. Use the **?** to determine available interfaces:

      ii. Set the interface. For example:

      ```
      (config vpn nemo nemo_example)> tun_local interface eth1
      (config vpn nemo nemo_example)>
      ```

    The default is **defaultroute**.

13. Configure one or more local networks to use as a virtual NEMO network interface. Generally, this will be a Local Area Network (LAN):
    a. Add a local network to use as a virtual NEMO network interface:

    ```
    (config vpn nemo nemo_example)> add network end eth2
    (config vpn nemo nemo_example)>
    ```

    b. (Optional) Repeat for additional interfaces.

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.

Show NEMO status

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, select **Status** > **NEMO**.

   The **NEMO** page appears.
3. To view configuration details about an NEMO tunnel, click the (configuration) icon in the upper right of the tunnel's status pane.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 NEMO tunnels, type the following at the prompt:

```
> show nemo

 NEMO  Enable  Status  Address  Agent    CoAddress
 ----  ------  ------  -------  -------  ----------
 demo  false
 test  true    up      1.2.3.4  4.3.2.1  10.10.10.1

>
```

3. To display details about a specific tunnel:

```
> show nemo name test

 test NEMO Status
 ----------------
 Enabled                  : true
 Status                   : up
 Home Agent               : 4.3.2.1
 Care of Address          : 10.10.10.1
 Interface                : modem
 GRE Tunnel               : 10.10.10.1 === 4.3.2.1
 Metric                   : 255
 MTU                      : 1476
 Lifetime (Actual)        : 600

 Local Network  Subnet          Status
 -------------  --------------  ----------
 lan1           192.168.2.1/24  Advertized
 LAN2           192.168.3.1/24  Advertized


>
```

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.

Services

This chapter contains the following topics:

Allow remote access for web administration and SSH 488
Configure the web administration service 491
Configure SSH access 500
Use SSH with key authentication 507
Configure telnet access 509
Configure DNS 513
Simple Network Management Protocol (SNMP) 520
Location information 526
Modbus gateway 554
System time 571
Network Time Protocol 575
Configure a multicast route 581
Ethernet network bonding 584
Enable service discovery (mDNS) 586
Use the iPerf service 589
Configure the ping responder service 594

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:

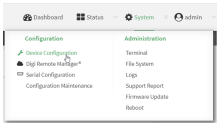
- The Connect EZ device must have a publicly reachable IP address.
- The **External** firewall zone must be added to the web administration or SSH service. See Firewall configuration for information on zones.
- See Set the idle timeout for Connect EZ users for information about setting the inactivity 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

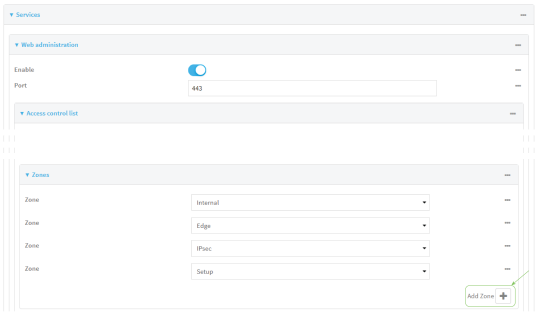
WebUI

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**.

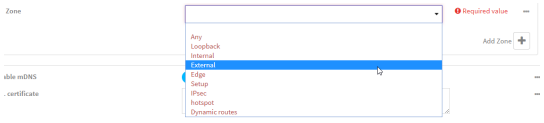


The **Configuration** window is displayed.

3. Click **Services** > **Web administration** > **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. 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. Add the external zone to the web administration service:

```
(config)> add service web_admin acl zone end external
(config)>
```

4. Save the configuration and apply the change:

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

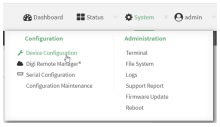
5. Type **exit** to exit the Admin CLI.

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

Add the External firewall zone to the SSH service

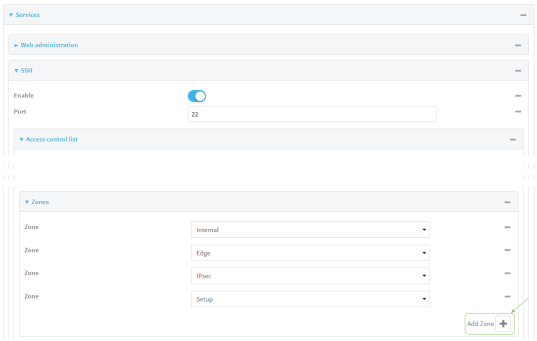
WebUI

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**.

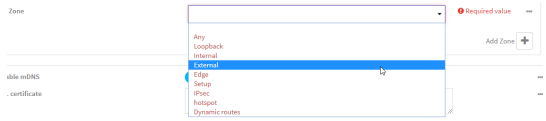


   The **Configuration** window is displayed.
3. Click **Configuration** > **Services** > **SSH** > **Access Control List** > **Zones**.

4. For **Add Zone**, click ✚.



5. Select **External**.



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



Command line

1. 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. 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.

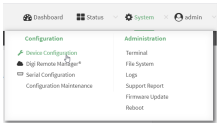
See Set the idle timeout for Connect EZ users for information about setting the inactivity timeout for the web administration services.

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:

WebUI

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 **Services** > **Web administration**.
4. Click **Enable**.
5. 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. Enable or disable the web administration service:
   - To enable the service:

```
(config)> service web_admin enable true
(config)>
```

   - To disable the sevice:

```
(config)> service web_admin enable false
(config)>
```

4. Save the configuration and apply the change:

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

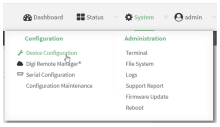
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

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 **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 Connect EZ 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.

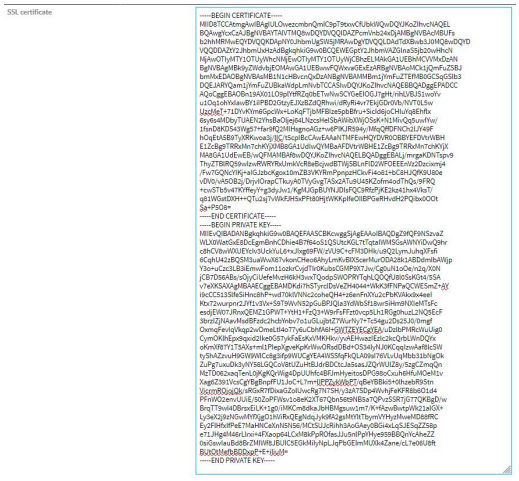
6. Multicast DNS (mDNS) is enabled by default. mDNS is a protocol that resolves host names in small networks that do not have a DNS server. To disable mDNS, or enable it if it has been disabled, click **Enable mDNS**.
7. For **SSL certificate**, if you have your own signed SSL certificate, paste the 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. For **Allow legacy encryption protocols**, enable this option to allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and

later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.

9. **View** is set to **Auto** by default and normally should not be changed.
10. **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**.
11. 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. 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 administratrion 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 administratrion 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
```

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 list 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-----
MIID8TCCAtmgAwIBAgIULOwezcmbnQmIC9pT9txwCfUbkWQwDQYJKoZIhvcNAQEL
BQAwgYcxCzAJBgNVBAYTAlVTMQ8wDQYDVQQIDAZPcmVnb24xDjAMBgNVBAcMBUFs
b2hhMRMwEQYDVQQKDApNY0JhbmUgSW5jMRAwDgYDVQQLDAdTdXBwb3J0MQ8wDQYD
VQQDDAZtY2JhbmUxHzAdBgkqhkiG9w0BCQEWEGptY2JhbmVAZGlnaS5jb20wHhcN
MjAwOTIyMTY1OTUyWhcNMjEwOTIyMTY1OTUyWjCBhzELMAkGA1UEBhMCVVMxDzAN
BgNVBAgMBk9yZWdvbjEOMAwGA1UEBwwFQWxvaGExEzARBgNVBAoMCk1jQmFuZSBJ
bmMxEDAOBgNVBAsMB1N1cHBvcnQxDzANBgNVBAMMBm1jYmFuZTEfMB0GCSqGSIb3
DQEJARYQam1jYmFuZUBkaWdpLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAOBn19AX01LO9plYtfRZq0bETwNwSCYGeEIOGJ7gHt/rihLVBJS1woYv
u1Oq1ohYxIawBY1iIPBD2GtzyEJXzBZdQRhwi/dRyRi4vr7EkjGDr0Vb/NVT0L5w
UzcMeT+71DYvKYm6GpcWx+LoKqFTjbMFBIze5pbBfru+SicId6joCHIuYq8Ehflx
6sy6s4MDbyTUAEN2YhsBaOljej64LNzcsHeISbAWibXWjOSsK+N1MivQq5uwIYw/
1fsnD8KDS43Wg57+far9fQ2MIHsgnoAGz+w6PIKJR594y/MfqQffDFNCh2lJY49F
hOqEtA5B9TyXRKwoa3j/lIC/t5cpIBcCAwEAAaNTMFEwHQYDVR0OBBYEFDVtrWBH
E1ZcBg9TRRxMn7chKYjXMB8GA1UdIwQYMBaAFDVtrWBHE1ZcBg9TRRxMn7chKYjX
MA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBALj/mrgaKDNTspv9
ThyZTBlRQ59wIzwRWRYRxUmkVcR8eBcjwdBTWjSBLnFlD2WFOEEEnVz2Dzcixmj4
/Fw7GQNcYIKj+aIGJzbcKgox10mZB3VKYRmPpnpzHCkvFi4o81+bC8HJQfK9U80e
vDV0/vA5OB2j/DrjvlOrapCTkuyA0TVyGvgTASx2ATu9U45KZofm4odThQs/9FRQ
+cwSTb5v47KYffeyY+g3dyJw1/KgMJGpBUYNJDIsFQC9RfzPjKE2kz41hx4VksT/
q81WGstDXH++QTu2sj7vWkFJH5xPFt80HjtWKKpIfeOIlBPGeRHvdH2PQibx0OOt
Sa+P5O8=
-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDgZ9fQF9NSzvaZ
WLX0WatGxE8DcEgmBnhCDhie4B7f64oS1QSUtcKGL7tTqtaIWMSGsAWNYiDwQ9hr
c8hCV8wWXUEYcIv3UckYuL6+xJIxg69FW/zVU9C+cFM3DHk/u9Q2LymJuhqXFsfi
6CqhU42zBQSM3uaWwX67vkonCHeo6AhyLmKvBIX5cerMurODA28k1ABDdmIbAWjp
Y3o+uCzc3LB3iEmwFom11ozkrCvjdTIr0KubsCGMP9X7Jw/Cg0uN1oOe/n2q/X0N
jCB7D56ABs/sOjyCiUefeMvzH6kH3wxTQodpSWOPRYTqhLQOQfU8l0SsKGt4/5SA
v7eXKSAXAgMBAAECggEBAMDKdi7hSTyrclDsVeZH4044+WkK3fFNPaQCWESmZ+AY
i9cCC513SlfeSiHnc8hP+wd70klVNNc2coheQH4+z6enFnXYu2cPbKVAkx9x4eeI
```

```
Ktx72wurpnr2JYf1v3Vx+S9T9WvN52pGuBPJQla3YdWbSf18wr5iHm9NXIeMTsFc
esdjEW07JRnxQEMZ1GPWT+YtH1+FzQ3+W9rFsFFzt0vcp5Lh1RGg0huzL2NQ5EcF
3brzIZjNAavMsdBFzdc2hcbYnbv7o1uGLujbtZ7WurNy7+Tc54gu2Ds25J0/0mgf
OxmqFevIqVkqp2wOmeLtI4o77y6uCbhfA6I+GWTZEYECgYEA/uDzlbPMRcWuUig0
CymOKlhEpx9qxid2Ike0G57ykFaEsKxVMKHkv/yvAEHwazIEzlc2kcQrbLWnDQYx
oKmXf87Y1T5AXs+ml1PlepXgveKpKrWwORsdDBd+OS34lyNJ0KCqqIzwAaf8lcSW
tyShAZzvuH9GW9WlCc8g3ifp9WUCgYEA4WSSfqFkQLA09sI76VLvUqMbb31bNgOk
ZuPg7uxuDk3yNY58LGQCoV8tUZuHtBJdrBDCtcJa5sasJZQrWUlZ8y/5zgCZmqQn
MzTD062xaqTenL0jKgKQrWig4DpUUhfc4BFJmHyeitosDPG98oCxuh6HfuMOeM1v
Xag6Z391VcsCgYBgBnpfFU1JoC+L7m+lIPPZykWbPT/qBeYBBki5+0lhzebR9Stn
VicrmROjojQk/sRGxR7fDixaGZolUwcRg7N7SH/y3zA7SDp4WvhjFeKFR8b6O1d4
PFnWO2envUUiE/50ZoPFWsv1o8eK2XT67Qbn56t9NB5a7QPvzSSR7jG77QKBgD/w
BrqTT9wl4DBrsxEiLK+1g0/iMKCm8dkaJbHBMgsuw1m7/K+fAzwBwtpWk21alGX+
Ly3eX2j9zNGwMYfXjgO1hViRxQEgNdqJyk9fA2gsMtYltTbymVYHyzMweMD88fRC
Ey2FlHfxIfPeE7MaHNCeXnN5N56/MCtSUJcRihh3AoGAey0BGi4xLqSJESqZZ58p
e71JHg4M46rLlrxi+4FXaop64LCxM8kPpROfasJJu5nlPpYHye959BBQnYcAheZZ
0siGswIauBd8BrZMIWf8JBUIC5EGkMiIyNpLJqPbGEImMUXk4Zane/cL7e06U8ft
BUtOtMefbBDDxpP+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 protocl:

     ```
     (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) Configure the device to allow legacy encryption protocols.

   Legacy encryption protocols allow clients to connect to the HTTPS session by using encryption protocols older than TLS 1.2, in addition to TLS 1.2 and later protocols. This option is disabled by default, which means that only TLS 1.2 and later encryption protocols are allowed with HTTPS connections.

   To enable legacy encryption protocols:

   ```
   (config)> service web_admin legacy_encryption true
   (config)>
   ```

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.

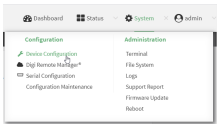
See Set the idle timeout for Connect EZ users for information about setting the inactivity timeout for the SSH service.

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:

WebUI

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 **Services** > **SSH**.
4. Click **Enable**.
5. 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. Enable or disable the SSH service:
   - To enable the service:

```
(config)> service ssh enable true
(config)>
```

   - To disable the sevice:

```
(config)> service ssh enable false
(config)>
```

4. Save the configuration and apply the change:

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

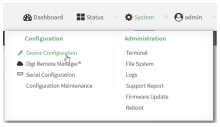
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

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 **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 Connect EZ 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-helman-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. 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. 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
```

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 list 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 protocl:

```
(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 entires in the form of an OpenSSH sshd_config file. For example, to enable the diffie-helman-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

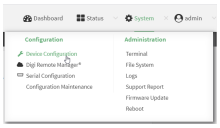
- Name for the user
- SSH public key for the user

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.

WebUI

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 **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. 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. 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.

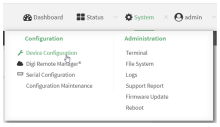
See Set the idle timeout for Connect EZ users for information about setting the inactivity timeout for the telnet service.

Enable the telnet service

The telnet service is disabled by default. To enable the service:

WebUI

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 **Services** > **telnet**.
4. Click **Enable**.
5. 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. Enable the telnet service:

```
(config)> service telnet enable true
(config)>
```

4. Save the configuration and apply the change:

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

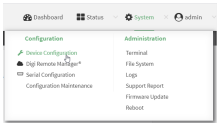
5. Type **exit** to exit the Admin CLI.

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

Configure the service

WebUI

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 **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 Connect EZ 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. 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. 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
```

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 list 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.

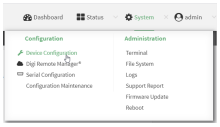
- Specific host names and their IP addresses.

  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:

WebUI

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 **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 Connect EZ 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 **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 **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) 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.
10. (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.
11. 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. 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
     ```

     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 list 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) 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)>
```

9. (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)>
```

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.

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. Log into the Connect EZ command line as a user with Admin access.

   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).

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.

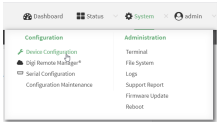
Additional configuration items

- The port used by the SNMP agent.
- Authentication type (either MD5 or SHA).
- Privacy protocol (either DES or AES).
- Privacy passphrase, if different that the SNMP user password.
- Enable Multicast DNS (mDNS) support.

To configure the SNMP agent on your Connect EZ device:

WebUI

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 **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 Connect EZ 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) Click **Enable version 2c access** to enable read-only access to SNMP version 2c.
14. 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. 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
```

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 list 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) Enable read-only access to to SNMP version 2c.

```
(config)> service snmp enable 2c true
(config)>
```

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.

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:

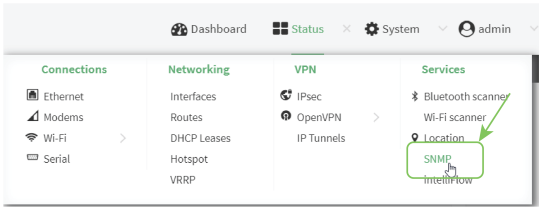
WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. Enable SNMP.

   See Configure Simple Network Management Protocol (SNMP) for information about enabling and configuring SNMP support on the Connect EZ device.

3. 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.



4. 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:

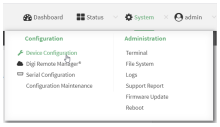
Configure the location service 527
Configure the device to use a user-defined static location 528
Configure the device to accept location messages from external sources 530
Forward location information to a remote host 534
Configure geofencing 541
Show location information 553

Configure the location service

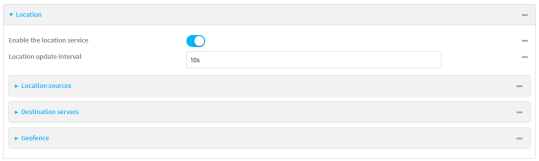
The location service is enabled by default. You can disable it, or you can enable it if it has been disabled.

WebUI

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 **Services** > **Location**.



4. The location service is enabled by default. To disable, or to enable if it has been disabled, click **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 set a static location for the device, see Configure the device to use a user-defined static location.
   b. To accept location information from an external location-enabled server, see Configure the device to accept location messages from external sources.

   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. For information about configuring **Destination servers**, see Forward location information to a remote host.
8. For information about configuring **Geofence**, see Configure geofencing.
9. 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. 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.
>
```

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

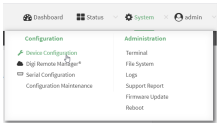
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure the device to use a user-defined static location

You can configured your Connect EZ device to use a user-defined static location.

WebUI

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 **Services** > **Location** > **Location sources**.
4. Click **+** to add a location source.
5. (Optional) Type a **Label** for this location source.
6. For **Latitude**, type the latitude of the device. Allowed values are **-90** and **90**, with up to six decimal places.
7. For **Longitude**, type the longitude of the device. Allowed values are **-180** and **180**, with up to six decimal places.
8. For **Altitude**, type the altitude of the device. Allowed values are an integer followed by **m** or **km**, for example, **100m** or **1km**.
9. 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.
10. 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. 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)>
```

5. Set the **type** of location source to **server**:

```
(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.

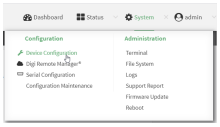
Required configuration items

- 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:

WebUI

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 **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 Connect EZ 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. 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. 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
```

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 list 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.

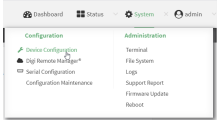
Additional configuration items

- 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:

WebUI

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 **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, 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.
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. 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. 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 **upd** 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**, 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.

     a. 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)>
```

     b. 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.

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 alphanumerical 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:

      a. 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)>
```

      b. 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:

a. Change to the **filter_nmea** node:

```
(config service location forward 0)> filter_nmea
(config service location forward 0 filter_nmea)>
```

b. 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:

  a. 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.

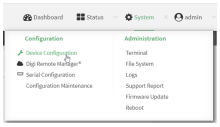
  Multiple actions can be configured for each type of event. For each action:
  - The type of action, either a factory erase or executing a custom script.
  - If a custom script is used:
    - The script that will be executed.
    - Whether to log output and errors from the script.
    - The maximum memory 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.

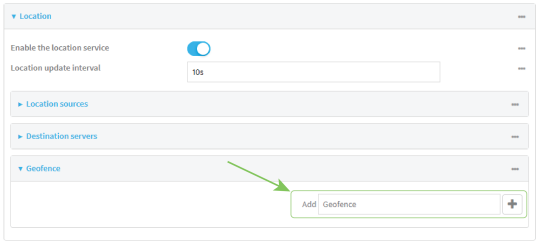
WebUI

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 **Services** > **Location** > **Geofence**.
4. For **Add Geofence**, type a name for the geofence and click **+**.



The geofence is enabled by default. Click **Enable** to disable, or to enable if it has been disabled.

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**}.

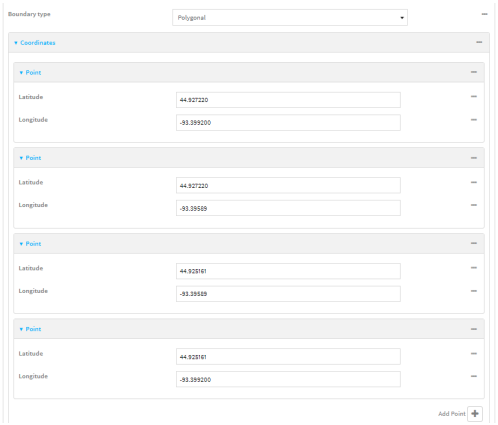
   For example, to set **Update interval** to ten minutes, enter **10m** or **600s**.

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:

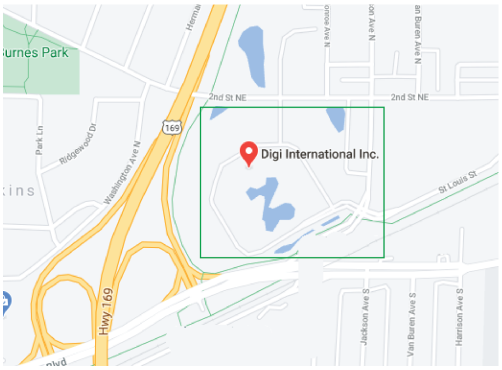
- For **Latitude**, any integer between **-90** and **90**, with up to six decimal places.
- For **Longitude**, any integer between **-180** and **180**, with up to six decimal places.

d. Click **+** again to add an additional point, and continue adding points to create the desired polygon.

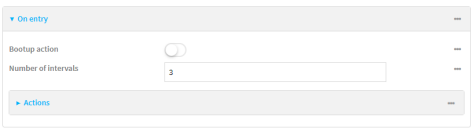
For example, to configure a square polygon around the Digi headquarters, configure a polygon with four points:



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**.



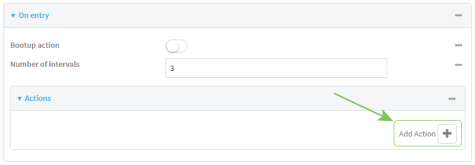
     b. (Optional) Enable **Bootup action** to configure the device to perform the **On entry** actions if the device is inside the geofence when it boots.

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 it spawned processes.

Allowed values are any integer followed by one of the following: **b**|**bytes**|**KB**|**k**|**MB**|**M**|**GB**|**G**|**TB**|**T**.

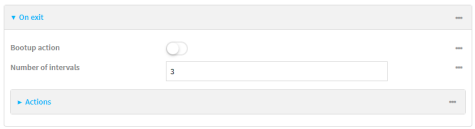
For example. the allocate one megabyte of memory to the script and its spawned processes, type **1MB** or **1M**.

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**.



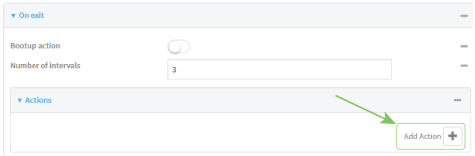
b. (Optional) Enable **Bootup action** to configure the device to perform the **On exit** actions if the device is inside the geofence when it boots.

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 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 it 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. 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. 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 vortices:

```
(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)>
```

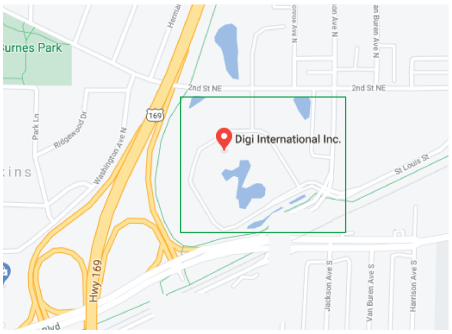
where *int* is:

- 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**:

i. 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 proceeding file path will be used to invoke the script interpreter. If not, then the default shell will be used.

ii. 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)>
```

iii. 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)>
```

iv. (Optional) Set the maximum amount of system memory that will be available for the script and it 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. the 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**:

i. 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.

ii. 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)>
```

iii. 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)>
```

iv. (Optional) Set the maximum amount of system memory that will be available for the script and it 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. the 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)>
```

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_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.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**.
3. 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. Log into the Connect EZ command line as a user with Admin access.

   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 : Thurs, 03 March 2022 10:16:23 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. Log into the Connect EZ command line as a user with Admin access.

   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 Connect EZ gateway allows for communication between buses and and networks that use the Modbus protocol.

This section contains the following topics:

Configure the Modbus gateway 555
Show Modbus gateway status and statistics 568

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.

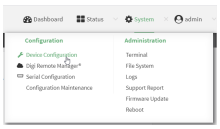
Additional configuration items

- 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.

WebUI

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**.



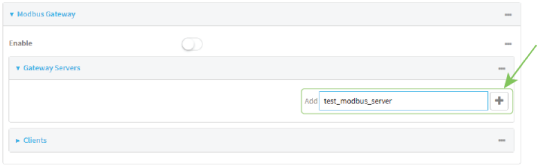
   The **Configuration** window is displayed.
3. Click **Services** > **Modbus Gateway**.



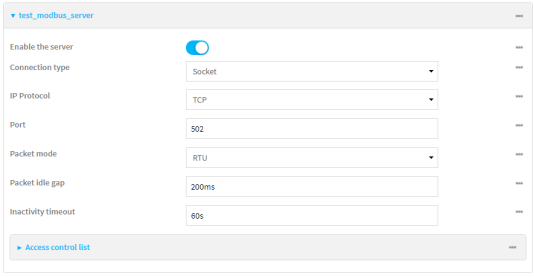
4. Click **Enable** to enable the gateway.
5. Click **Debug** to allow verbose logging in the system log.

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.



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*** {**ms|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 Connect EZ device:

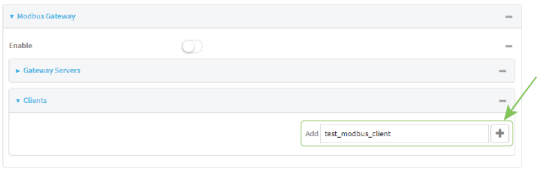
a. Click **Interfaces**.
b. For **Add Interface**, click ✚.
c. For **Interface**, select the appropriate interface from the dropdown.
d. Click ✚ again to allow access through additional interfaces.

- 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.

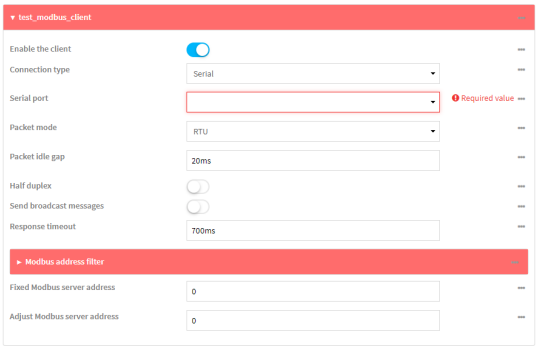
10. Repeat these steps to configure additional servers.

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*** {**ms|s**}.

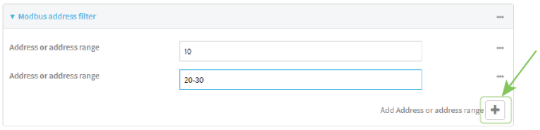
   For example, to set **Packet idle gap** to 20 milliseconds, enter **20ms**.
7. If **Connection type** is set to **Socket**, for **Inactivity timeout**, type the amount of time to wait before disconnecting the socket when it has become inactive.

   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 Connect EZ 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 ***number*ms**.
    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 ✚.



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 Modbuss 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. 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. 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*{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 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 ***number*ms**.

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 Modbuss 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.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. 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. Log into the Connect EZ command line as a user with Admin access.

   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**. 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**, 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

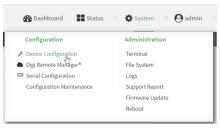
- The time zone for the Connect EZ device.
- If t least one upstream NTP server for synchronization.

Additional Configuration Options

- Additional upstream NTP servers.

WebUI

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 **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. 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. (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. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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 2022-03-03 10:16:23
   >
   ```
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**.

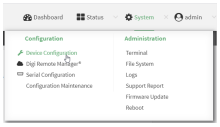
Additional Configuration Options

- 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:

WebUI

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 **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 Connect EZ 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. 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. 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
```

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 list 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)>
```

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 status and statistics of the NTP server

You can display status and statistics for active NTP servers

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**.
3. Under **Services**, click **NTP**.

   The NTP server status page is displayed.

Command line

Show NTP information

1. Log into the Connect EZ command line as a user with Admin access.

   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 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.

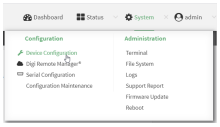
Configure a multicast route

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:

WebUI

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 **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, uncheck **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 mutlicast 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. 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. 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 mutlicast 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.

Ethernet network bonding

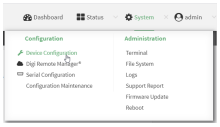
The Connect EZ device supports bonding mode for the Ethernet network. This allows you to configure the device so that Ethernet ports share one IP address. When both ports are being used, they act as one Ethernet network port.

Required configuration items

- Enable Ethernet bonding.
- The mode, either:
  - Active-backup. Provides fault tolerance.
  - Round-robin. Provides load balancing as well as fault tolerance.
- The Ethernet devices in the bonded pool.

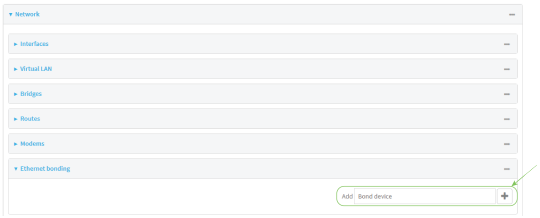
WebUI

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.

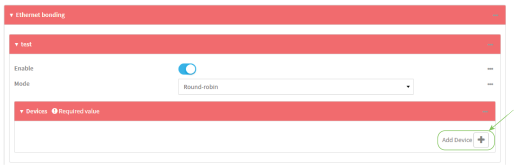
3. Click **Network** > **Ethernet bonding**.
4. For **Add Bond device**, click ✚



The bond device is enabled by default. To disable, click to toggle off **Enable**.

5. For **Mode**, selected either:
   - **Active-backup**: Transmits data on only one of the bonded devices at a time. When the active device fails, the next available device in the list is chosen. This mode provides for fault tolerance.
   - **Round-robin**: Alternates between bonded devices to provide load balancing as well as fault tolerance.
6. Click to expand **Devices**.

7. Add Ethernet devices:
   a. For **Add device**, click ✚



   b. For **Device**, select an Ethernet device to participate in the bond pool.
   c. Repeat for each appropriate Ethernet device.
8. 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. Add a network bond:

```
(config)> add network bond name
(config network bond name)>
```

   The new network bond is enabled by default. To disable:

```
(config network bond name)> enable false
(config network bond name)>
```

4. Set the mode:

```
(config network bond name)> mode value
(config network bond name)>
```

   where value is either:

   - **active-backup**: Transmits data on only one of the bonded devices at a time. When the active device fails, the next available device in the list is chosen. This mode provides for fault tolerance.
   - **round-robin**: Alternates between bonded devices to provide load balancing as well as fault tolerance.

5. Add Ethernet devices:
   a. Use the **?** to determine available devices:

```
(config network bond name)> ... network device ?

 Additional Configuration
 ------------------------------------------------------------------------
-------

 loopback

(config network bond name)>
```

   b. Add a device:

```
(config network bond name)> add device /network/device/
(config network bond name)>
```

   c. Repeat to add additional devices.
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.

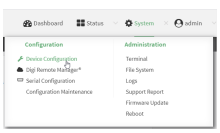
Enable service discovery (mDNS)

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.

WebUI

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 **Services** > **Service Discovery (mDNS)**.
4. **Enable** the mDNS service.
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 Connect EZ 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. 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. Enable the mDNS service:

```
(config)> service mdns enable true
(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
     ```

     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 list 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, to determine, for example, whether a cellular connection is providing expected throughput.

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

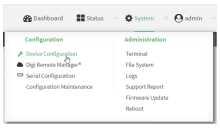
- The port that the Connect EZ device's iPerf server will use to listen for incoming connections.
- The access control list for the iPerf server.

  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:

WebUI

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**.

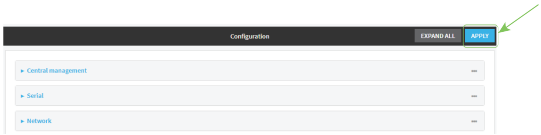


The **Configuration** window is displayed.

3. Click **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 Connect EZ 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. 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. 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
```

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 list 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             sender
[  4]   0.00-10.00  sec   313 MBytes   262 Mbits/sec                  receiver

iperf Done.
$
```

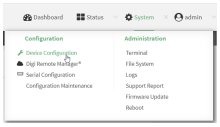
Configure the ping responder service

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:

WebUI

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 **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 Connect EZ 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. 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. 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
```

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 list 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             sender
[  4]   0.00-10.00  sec   313 MBytes   262 Mbits/sec                  receiver

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:

Configure scripts to run automatically 600
Configure scripts to run manually 606
Start a manual script 611
Stop a script that is currently running 612
Show script information 613
Run a Python application at the shell prompt 614
Start an interactive Python session 616
Digidevice module 617
Use Python to access serial ports 645
Use the Paho MQTT python library 646

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.
- Enable the application to be run script .
- Select whether the script should run:
  - When the device boots.
  - At a specified time.
  - At a specified interval.
  - During system maintenance.

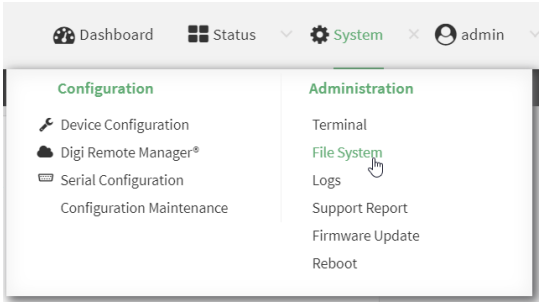
Additional configuration items

- 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.

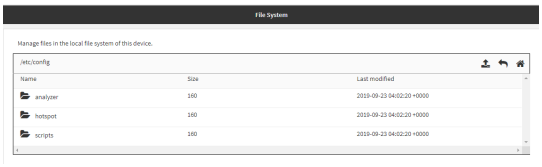
Task one: Upload the application

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the **scripts** directory and click to open the directory.
4. Click (upload).
5. 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. Log into the Connect EZ command line as a user with Admin access.

   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.

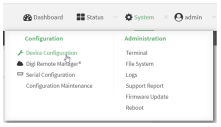
Note You can also create scripts by using the **vi** command when logged in with shell access.

Task two: Configure the application to run automatically

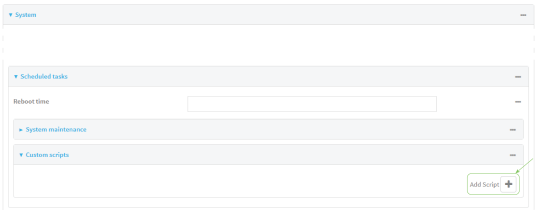
Note This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

WebUI

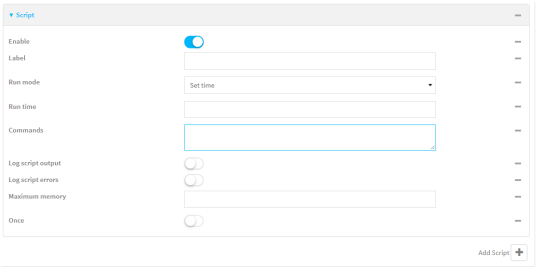
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **System** > **Scheduled tasks** > **Custom scripts**.
4. For **Add Script**, click ✚.



   The script configuration window is displayed.



   Custom scripts are enabled by default. To disable, click **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**, enter the commands that will execute the script.

   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. 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. 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 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.

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.

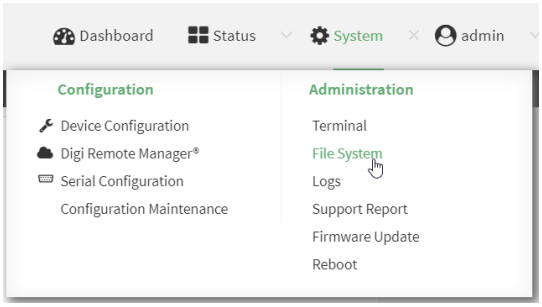
Additional configuration items

- 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.

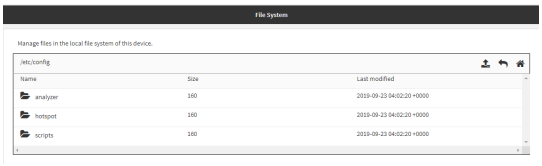
Task one: Upload the application

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the **scripts** directory and click ↱ to open the directory.
4. Click ⬆ (upload).
5. 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. Log into the Connect EZ command line as a user with Admin access.

   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.

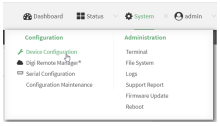
Note You can also create scripts by using the **vi** command when logged in with shell access.

Task two: Configure the application to run automatically

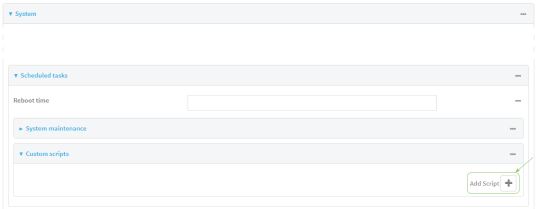
Note This feature does not provide syntax or error checking. Certain commands can render the device inoperable. Use with care.

WebUI

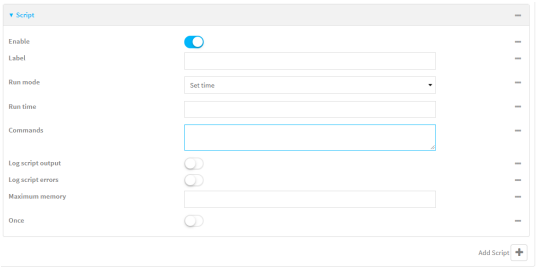
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **System** > **Scheduled tasks** > **Custom scripts**.
4. For **Add Script**, click ✚.



   The script configuration window is displayed.



Custom scripts are enabled by default. To disable, click **Enable** to toggle off.

5. (Optional) For **Label**, provide a label for the script.
6. For **Run mode**, select **Manual**.
7. For **Commands**, enter the commands that will execute the script.

   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. 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. 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 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**|**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.

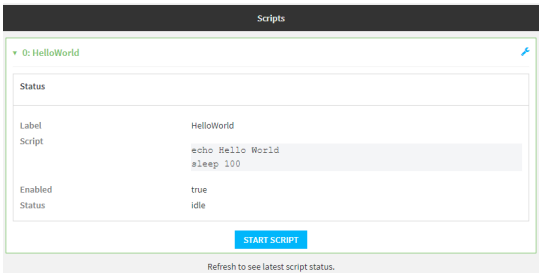
Start a manual script

You can start a script that is enabled and configured to have a run mode of **Manual**. See

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



3. For scripts that are enabled and configured to have a run mode of **Manual**, click **Start Script** to start the script.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

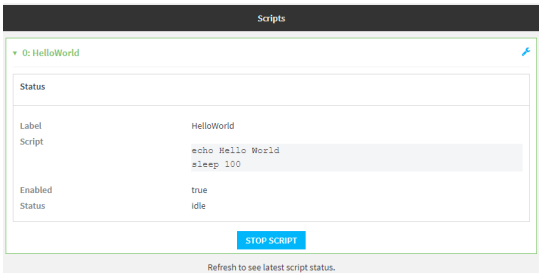
Stop a script that is currently running

You can stop a script that is currently running.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



3. For scripts that are currently running, click **Stop Script** to stop the script.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

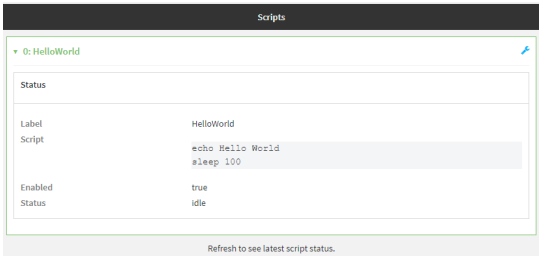
Show script information

You can view status and statistics about location information from either the WebUI or the command line.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. At the **Status** page, click **Scripts**.

   The **Scripts** page displays:



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

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**.

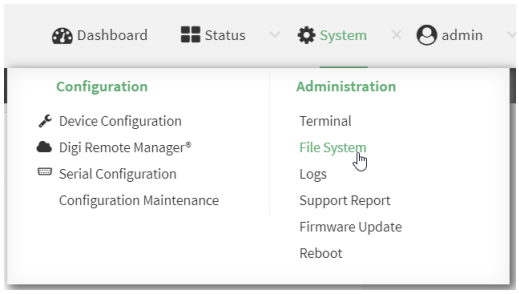
Note Python applications cannot be run from the Admin CLI. You must access the device shell in order to run Python applications from the command line. See Authentication groups for information about configuring authentication groups that include shell access.

1. Upload the Python application to the Connect EZ device:

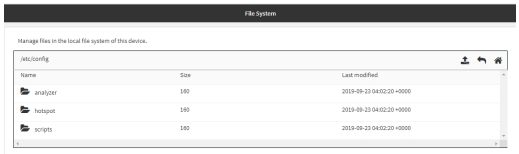
WebUI

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

b. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



c. Highlight the **scripts** directory and click ↱ to open the directory.

d. Click ⬆ (upload).

e. 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. Log into the Connect EZ command line as a user with Admin access.

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. Log into the Connect EZ 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
```

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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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()**.

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 618
Use digidevice.datapoint to upload custom datapoints to Digi Remote Manager 619
Use digidevice.config for device configuration 622
Use Python to respond to Digi Remote Manager SCI requests 624
Use digidevice runtime to access the runtime database 633
Use Python to upload the device name to Digi Remote Manager 635
Use Python to access the device location data 637
Use Python to set the maintenance window 641
Use Python to send and receive SMS messages 643

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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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 EZ-000065
  SKU                      : Connect EZ
  Hostname                 : Connect EZ
  MAC Address              : DF:DD:E2:AE:21:18

  Hardware Version         : 50001947-01 1P
  Firmware Version         : 22.2.9.85
  Alt. Firmware Version    : 22.2.9.85
  Alt. Firmware Build Date : Thurs, 03 March 2022 10:16:23
  Bootloader Version       : 19.7.23.0-15f936e0ed

  Current Time             : Thurs, 03 March 2022 10:16:23 +0000
  CPU                      : 1.4%
  Uptime                   : 6 days, 6 hours, 21 minutes, 57 seconds
(541317s)
  Temperature              : 40C

>>>
```

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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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', 'wwan1',
'wwan2']
```

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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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)
>>>
```

5. Use the **set()** method to make changes to the configuration:

```
>>> cfg.set("system.name", "New-Name")
>>>
```

6. Use the **commit()** method to save the changes:

```
>>> cfg.commit()
True
>>>
```

7. 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**:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **config** submodule:

```
>>> from digidevice import config
>>>
```

4. Use the help command with **config**:

```
>>> help(config)
Help on module acl.config in acl:

NAME
acl.config - Python interface to ACL configuration (libconfig).
...
```

5. 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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 callbackup 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.

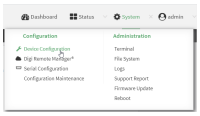
3. For both devices:

   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:

   WebUI

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

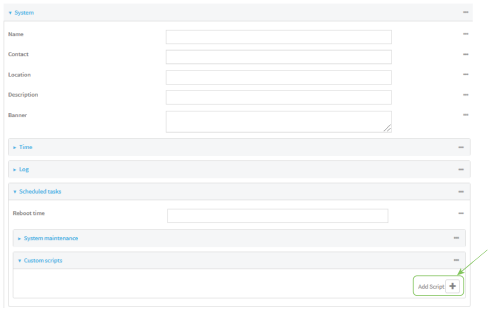
   ii. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

   The **Configuration** window is displayed.

   iii. Click **System** > **Scheduled tasks** > **Custom scripts**.

iv. Click ✚ to add a custom script.

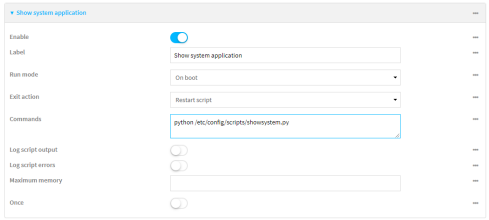


v. For **Label**, type **Show system application**.

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. 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.

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. Log into the Connect EZ 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 targest:
   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         : 22.2.9.85
          Bootloader Version       : 1
```

```
          Firmware Build Date      : Thurs, 03 March 2022 10:16:23
          Schema Version           : 461

          Timezone                 : UTC
          Current Time             : Thurs, 03 March 2022 10:16:23
          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         : 22.2.9.85
          Bootloader Version       : 1
          Firmware Build Date      : Thurs, 03 March 2022 10:16:23
          Schema Version           : 461

          Timezone                 : UTC
          Current Time             : Thurs, 03 March 2022 10:16:23
          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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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()
>>>
```

8. 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**:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **runt** submodule:

```
>>> from digidevice import runt
>>>
```

4. Use the help command with **runt**:

```
>>> help(runt)

Help on module acl.runt in digidevice:

NAME
acl.runt - Python interface to ACL runtime database (runtd).
...
```

5. 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. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] 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 Managerby accessing help for **digidevice.name**:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **name** submodule:

```
>>> from digidevice import name
>>>
```

4. 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
...
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Use Python to access the device location data

The **location** submodule enables access to the location data for the Connect EZ device.

The module takes a snapshot of location data stored in the runt database. The location data snapshot can be subsequently updated by using the update method.

Determine if the device's location

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **location** submodule:

```
>>> from digidevice import location
```

4. Use the **valid_fix** object to determine if the device has a valid fix:

```
>>> loc = location.Location()
>>> loc.valid_fix
True
>>>
```

5. Use the **position** object to return the device's position:

```
>>> loc.position
(44.926195299999998, -93.397084499999999, 292.39999399999999)
>>>
```

   The coordinates are returned in the following order:

   latitude, *longitude*, *altitude*

   altitude is in meters.

6. You can also return only one of the coordinate positions:
   - Use the **latitude** object to return the latitude:

```
>>> loc.latitude
44.926195299999998
>>>
```

   - Use the **longitude** object to return the longitude:

```
>>> loc.longitude
-93.397084499999999
>>>
```

   - Use the **altitude** object to return the altitude, in meters:

```
>>> loc.altitude
292.39999399999999
>>>
```

7. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Update the location data

The **location** submodule takes a snapshot of the current location and stores it in the runtime database. You can update this snapsot:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
```

```
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **location** submodule:

```
>>> from digidevice import location
```

4. Update the location object with the latest location data:

```
>>> loc = location.Location()
>>> loc.position
>>> (44.926195299999998, -93.397084499999999, 292.39999399999999)
>>> loc.update()
>>> loc.position
44.926231, -93.397923, 289.439229
>>>
```

5. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Output location data in json format

The **location** submodule takes a snapshot of the current location and stores it in the runtime database. You can update this snapsot

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **json** submodule:

```
>>> import json
```

4. Import the **location** submodule:

```
>>> from digidevice import location
```

5. Print the location data in json format:

```
>>> geojson_data = location.Location().geojson
>>> print(json.dumps(geojson_data, indent=4))
{
    "type": "Feature",
    "geometry": {
        "type": "Point",
        "coordinates" [
```

```
            44.926195299999998,
            -93.397084499999999,
            273.20001200000002
        ]
    },
    "properties": {
        "direction": "None",
        "horizontal_velocity": "0.0",
        "latitude.deg_min_sec": "44* 54' 45.586\" N",
        "longitude.deg_min_sec": "93* 33' 52.334\" W",
        "num_satellites": "12",
        "quality": "Standard GNSS (2D/3D)",
        "selected_source_idx": "0",
        "source": "USB (/dev/ttyACM0)",
        "source_idx.0.altitude": "273.200012",
        "source_idx.0.direction": "None",
        "source_idx.0.horizontal_velocity": "0.195489",
        "source_idx.0.label": "usb",
        "source_idx.0.latitude": "44.902662",
        "source_idx.0.latitude.deg_min_sec": "44* 55' 45.065\" N",
        "source_idx.0.longitude": "-93.560648",
        "source_idx.0.longitude.deg_min_sec": "93* 16' 52.966\" W",
        "source_idx.0.num_satellites": "12",
        "source_idx.0.quality": "Standard GNSS (2D/3D)",
        "source_idx.0.utc_date_time": "Mar-03-2022 10:16:23",
        "source_idx.0.vertical_velocity": "0.0",
        "source_idx.1.label": "gnss",
        "source_idx.1.quality": "No Fix / Invalid",
        "state": "Enabled, signal",
        "utc_date_time": "Mar-03-2022 10:16:23",
        "vertical_velocity": "0.0"
    }
}
>>>
```

6. Use **Ctrl-D** to exit the Python session. You can also exit the session using **exit()** or **quit()**.

Help for the digidevice location module

Get help for the digidevice location module:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
```

```
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **location** submodule:

```
>>> from digidevice import location
>>>
```

4. Use the help command with **location**:

```
>>> help(location)
Help on module digidevice.location in digidevice:

NAME
digidevice.location - digidevice.location - API for accessing location
data
...
```

5. 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.

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **maintenance** module:

```
>>> from digidevice import maintenance
>>>
```

4. To determine the current service state of the device:

```
>>> maintenance.state()
'IN_SERVICE'
>>>
```

5. To set the device to out of service:

```
>>> maintenance.out_of_service()
>>> maintenance.state()
'OUT_OF_SERVICE'
>>>
```

6. 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:

1. Log into the Connect EZ 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 3.6.13 (default, May  9 2021, 22:49:59)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

3. Import the **maintenance** submodule:

```
>>> from digidevice import maintenance
>>>
```

4. 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()**.

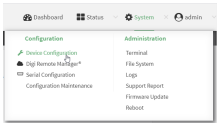
Use Python to send and receive SMS messages

You can create Python scripts that send and receive SMS message in tandem with the Digi Remote Manager or Digi aView 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

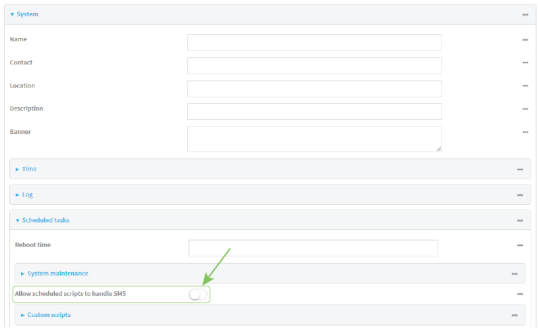
WebUI

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 **System** > **Scheduled tasks**.
4. Click to enable **Allow scheduled scripts to handle SMS**.



5. 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. At the config prompt, type:

```
(config)> system schedule sms_script_handling 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.

See Configure scripts to run automatically for more information about scheduling scripts.

Example digidevice.sms code

The following example code receives an SMS message and sends a response:

```
#!/usr/bin/python3.6


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 occured while waiting")
        print(err)
    COND.release()
    my_callback.unregister_callback()
```

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 information about configuring a serial port in Application mode.

To use Python to access serial ports:

1. Log into the Connect EZ 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. Determine the path to the serial port:

   ```
   # ls /dev/serial/
   by-id   by-path   by-usb   port1
   #
   ```

3. At the shell prompt, use the **python** command with no parameters to enter an interactive Python session:

   ```
   # python
   Python 3.6.13 (default, May  9 2021, 22:49:59)
   [GCC 8.3.0] on linux
   Type "help", "copyright", "credits" or "license" for more information.
   >>>
   ```

4. Import the **serial** module:

   ```
   >>> import serial
   >>>
   ```

5. 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
   >>>
   ```

6. 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)
```

User authentication

This chapter contains the following topics:

Connect EZ user authentication 651
User authentication methods 651
Authentication groups 658
Local users 667
Terminal Access Controller Access-Control System Plus (TACACS+) 680
Remote Authentication Dial-In User Service (RADIUS) 687
LDAP 692
Configure serial authentication 700
Disable shell access 702
Set the idle timeout for Connect EZ users 703
Example user configuration 705

Connect EZ user authentication

User authentication on the Connect EZ has the following features and default configuration:

Feature	Description	Default configuration
Idle timeout	Determines how long a user session can be idle before the system automatically disconnects.	■ 10 minutes.
Allow shell	If disabled, prevents all authentication prohibits access to the shell prompt for all authentication groups. 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.	■ Enabled.
Methods	Determines how users are authenticated for access: **local users**, **TACACS+**, or **RADIUS**.	■ **local users**.
Groups	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.	■ **admin**: Provides the logged-in user with administrative and shell access. ■ **serial**: Provides the logged-in user with access to serial ports.
Users	Defines local users for the Connect EZ.	■ **admin**: Belongs to both the **admin** and **serial** groups.
TACACS+	Configures support for TACACS+ (Terminal Access Controller Access-Control System Plus) servers and users.	■ Not configured.
RADIUS	Configures support for RADIUS (Remote Authentication Dial-In User Service) servers and users.	■ Not configured.
LDAP	Configures support for LDAP (Lightweight Directory Access Protocol) servers and users.	■ Not configured.
Serial	Configures authentication for serial TCP and autoconnect services.	■ Not configured.

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

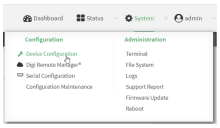
Required configuration items

- The types of authentication method to be used:

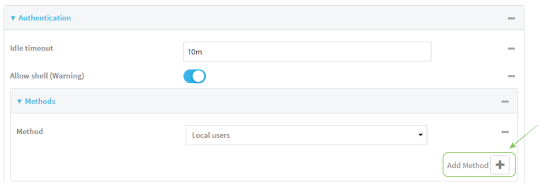
To add an authentication method:

WebUI

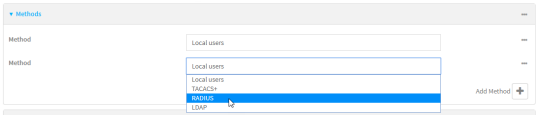
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **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. 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. Add the new authentication method to the appropriate location in the list:
   - To determine the current list of authentication methods:
     a. 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.
     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.
>
```

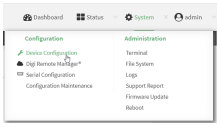
5. Type **exit** to exit the Admin CLI.

   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

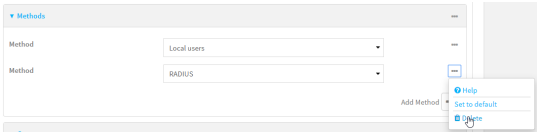
WebUI

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 **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. 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. 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.

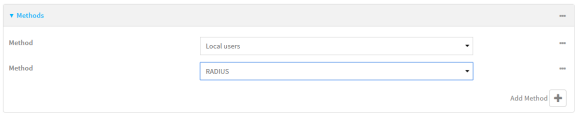
Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Rearrange the position of authentication methods

WebUI

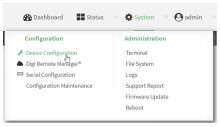
Authentication methods are reordered by changing the method type in the **Method** drop-down for each authentication method to match the appropriate order.

For example, the following configuration has **Local users** as the first method, and **RADIUS** as the second.



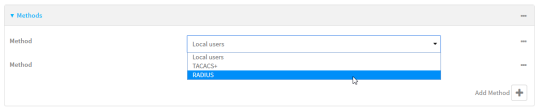
To reorder these so that **RADIUS** is first and **Local users** is second:

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

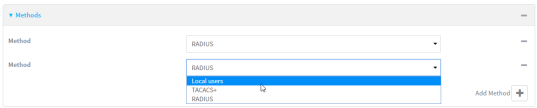


The **Configuration** window is displayed.

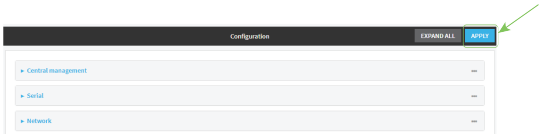
3. Click to expand the first **Method**.
4. In the **Method** drop-down, select **RADIUS**.



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. 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. 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:

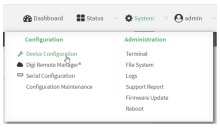
Change the access rights for a predefined group 659
Add an authentication group 661
Delete an authentication group 665

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:

WebUI

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**.



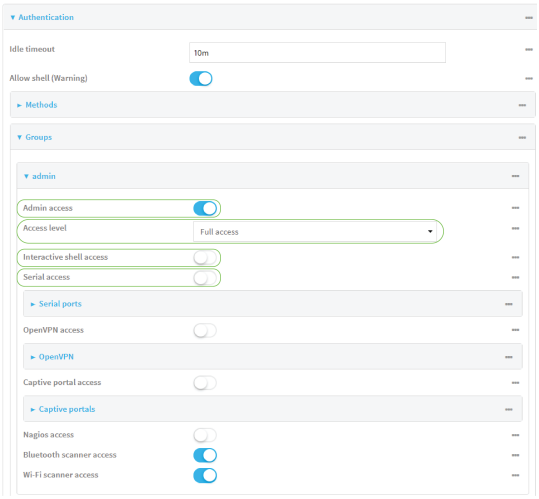
   The **Configuration** window is displayed.
3. Click **Authentication** > **Groups**.
4. Click the authentication group to be changed, either **admin** or **serial**, to expand its configuration node.
5. Click the box next to the following options, as appropriate, to enable or disable access rights for 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**.
   - **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.
   - **Serial access**



6. 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. 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.

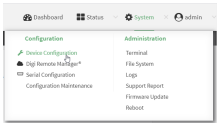
Additional configuration items

- 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:

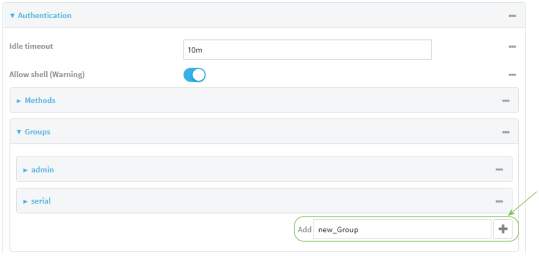
WebUI

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**.

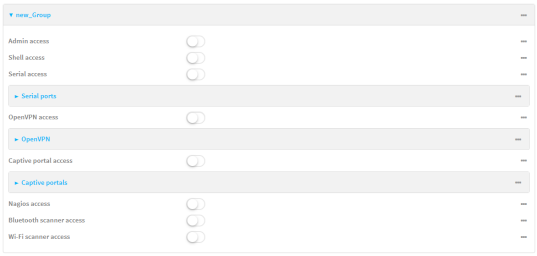


The **Configuration** window is displayed.

3. Click **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**.
   - **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.
   - **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. (Optional) Enable users that belong to this group to query the device for Nagios monitoring by checking the box next to **Nagios access**.
9. (Optional) Enable users that belong to this group to access the Bluetooth scanning service by checking the box next to **Bluetooth scanner access**.
10. (Optional) Enable users that belong to this group to access the Wi-Fi scanning service by checking the box next to **Wi-Fi scanner access**.
11. 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. 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. (Optional) Enable users that belong to this group to access the Bluetooth scanning service:

```
(config)> auth group test acl bluetooth_scanner enable true
(config)>
```

8. (Optional) Enable users that belong to this group to access the Wi-Fi scanning service:

```
(config)> auth group group test acl wifi_scanner enable true
(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.

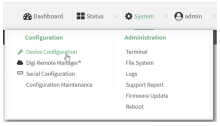
Delete an authentication group

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:

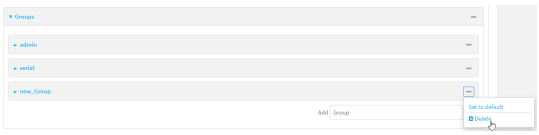
WebUI

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 **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. 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. 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 preconfiged 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:

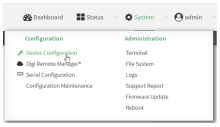
Change a local user's password 668
Configure a local user 670
Delete a local user 678

Change a local user's password

To change a user's password:

WebUI

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**.

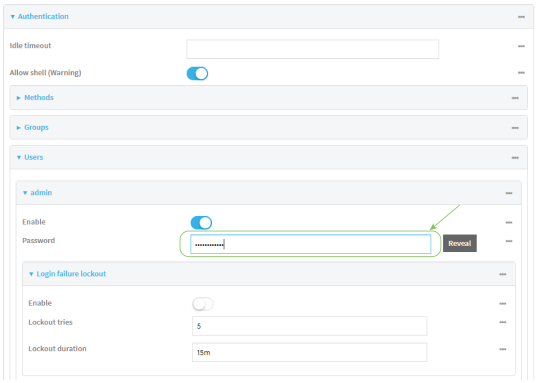


The **Configuration** window is displayed.

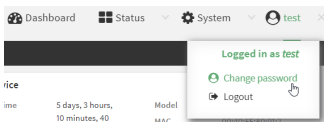
3. Click **Authentication** > **Users**.
4. Click the username to expand the user's configuration node.
5. For **Password**, enter the new password. The password must be at least eight characters long and must contain at least one uppercase letter, one lowercase letter, one number, and one special character.

   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 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. 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. 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

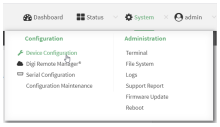
- An alias for the user. Because the username cannot contain any special characters, such as hyphens (-) or periods (.), an alias allows the user to log in using a name that contains special characters.
- The number of unsuccessful login attempts before the user is locked out of the system.

- 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.

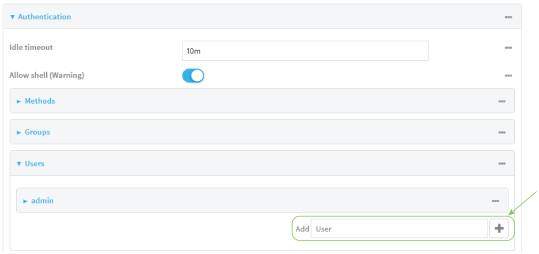
To configure a local user:

WebUI

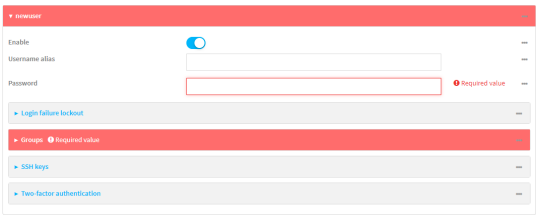
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Authentication** > **Users**.
4. 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, click to toggle off **Enable**.

5. (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.
6. 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.
7. Click to expand **Login failure lockout**.

   The login failure lockout feature is enabled by default. To disable, click to toggle off **Enable**.

   a. For **Lockout tries**, type the number of unsuccessful login attempts before the user is locked out of the device. The default is **5**.

   b. 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.
8. Add groups for the user.

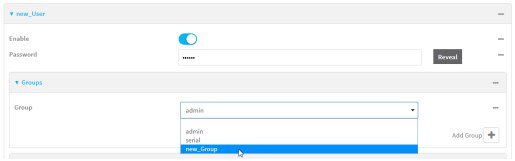
   Groups define user access rights. See Authentication groups for information about configuring groups.

   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**.

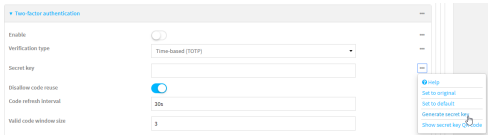
   b. In **Add SSH key**, paste or type a public encryption key that this user can use for passwordless SSH login and click ✚.
10. (Optional) Configure two-factor authentication for SSH, telnet, and serial console login:

    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. 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. 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.

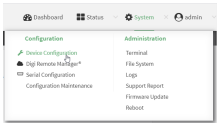
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a local user

To delete a user from your Connect EZ:

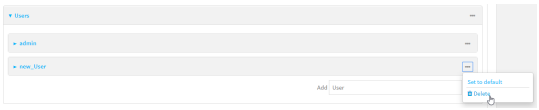
WebUI

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 **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. 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. 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 681
TACACS+ server failover and fallback to local authentication 682
Configure your Connect EZ device to use a TACACS+ server 682

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.

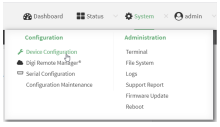
Additional configuration items

- 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.

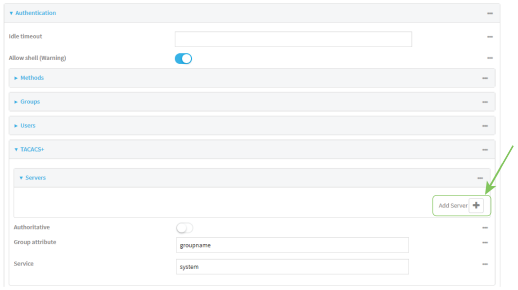
WebUI

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 **Authentication** > **TACACS+** > **Servers**.
4. Add TACACS+ servers:
   a. For **Add server**, click ✚.

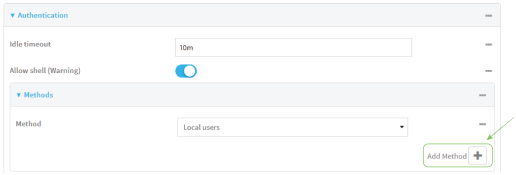


   b. For **Hostname**, type the hostname or IP address of the TACACS+ server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 49.
   d. For **Secret**, type the TACACS+ server's shared secret. This is configured in the key parameter of the TACACS+ server's tac_plus.conf file, for example:

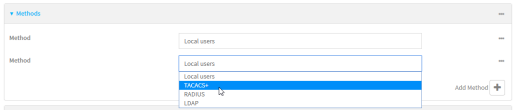
```
key = testing123
```

   e. (Optional) Click ✚ again to add additional TACACS+ servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being used if TACACS+ authentication fails. Other authentication methods will only be used if the TACACS+ server is unavailable.
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 the first successful authentication result is returned. 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. 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. (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 688
RADIUS server failover and fallback to local configuration 688
Configure your Connect EZ device to use a RADIUS server 689

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

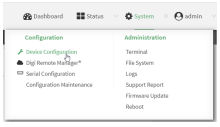
- Define the RADIUS server IP address or domain name.
- Define the RADIUS server shared secret.
- Add RADIUS as an authentication method for your Connect EZ device.

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.

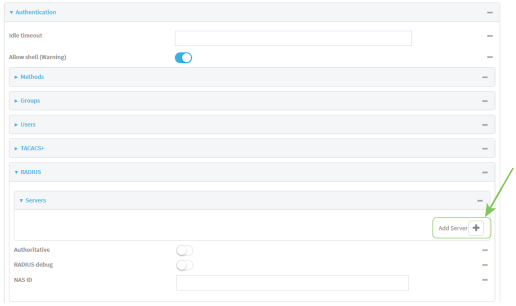
WebUI

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 **Authentication** > **RADIUS** > **Servers**.

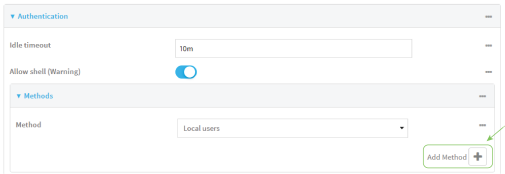
4. Add RADIUS servers:
   a. For **Add server**, click ✚.



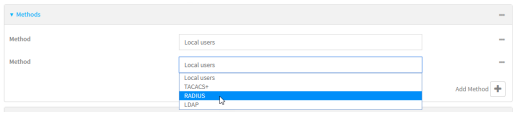
   b. For **Hostname**, type the hostname or IP address of the RADIUS server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 1812.
   d. For **Secret**, type the RADIUS server's shared secret. This is configured in 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 used if RADIUS authentication fails. Other authentication methods will only be used if the RADIUS server is unavailable.
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 the first successful authentication result is returned. 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. 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. (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 694
LDAP server failover and fallback to local configuration 695
Configure your Connect EZ device to use an LDAP server 695

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

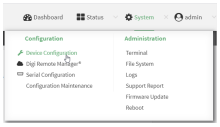
- Define the LDAP server IP address or domain name.
- Add LDAP as an authentication method for your Connect EZ device.

Additional configuration items

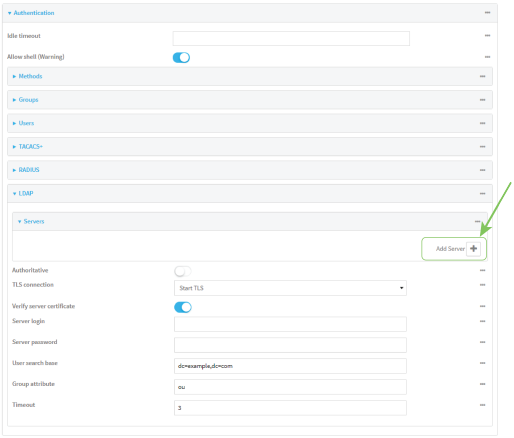
- Whether other user authentication methods should be used in addition to the LDAP server, or if the LDAP server should be considered the authoritative login method.
- The LDAP server port. It is configured to 389 by default.
- Whether to use Transport Layer Security (TLS) when communicating with the 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.

WebUI

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**.

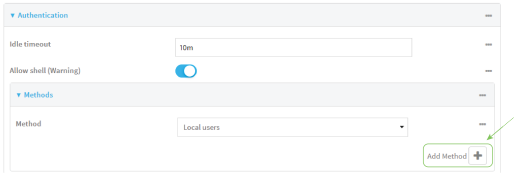


   The **Configuration** window is displayed.
3. Click **Authentication** > **LDAP** > **Servers**.
4. Add LDAP servers:
   a. For **Add server**, click ✚.

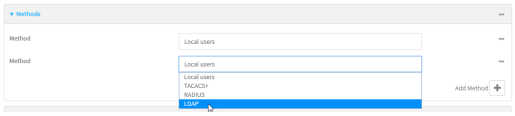


   b. For **Hostname**, type the hostname or IP address of the LDAP server.
   c. (Optional) Change the default **Port** setting to the appropriate port. Normally this should be left at the default setting of port 389 for non-TLS and 636 for TLS.
   d. (Optional) Click ✚ again to add additional LDAP servers.
5. (Optional) Enable **Authoritative** to prevent other authentication methods from being used if LDAP authentication fails. Other authentication methods will only be used if the LDAP server is unavailable.
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 the first successful authentication result is returned. 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. 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. (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.

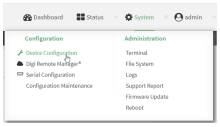
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure serial authentication

This section describes how to configure authentication for serial access.

WebUI

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 **Authentication** > **Serial**.
4. (Optional) For **TLS identity certificate**, paste a TLS certificate and private key in PEM format. If empty, the certificate for the web administration service is used. See Configure the web administration service for more information.
5. For **Peer authentication**, select the method used to verify the certificate of a remote peer.
6. **Include standard CAs** is enabled by default. This allows peers with certificates that have been signed by standard Certificate Authorities (CAs) to authenticate.
7. Click to expand **Custom certificate authorities** to add the public certificates of custom CAs.
   a. For **Add CA certificate**, type the name of a custom CA and click ✚.
   b. Paste the public certificate for the custom CA in PEM format.
   c. Repeat for additional custom CA certificates.
8. Click to expand **Peer certificates** to add the public certificates of trusted peers.
   a. For **Add Peer certificate**, type the name of a trusted peer and click ✚.
   b. Paste the public certificate for the trusted peer in PEM format.
   c. Repeat for additional trusted peer certificates.

9. 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. (Optional) Paste a TLS certificate and private key in PEM format:

```
(config)> auth serial identiy "cert-and-private-key"
(config)>
```

4. Set the method used to verify the certificate of a remote peer:

```
(config)> auth serial verify value
(config)>
```

   where *value* is either:

   - **ca**: Uses certificate authorities (CAs) to verify.
   - **peer**: Uses the remote peer's public certificate to verify.
5. By default, peers with certificates that have been signed by standard Certificate Authorities (CAs) are allowed to authenticate. To disable:

```
(config)> auth serial ca_standard false
(config)>
```

6. Add the public certificate for a custom certificate authority:

```
(config)> add auth serial ca_certs CA-cert-name "cert-and-private-key"
(config)>
```

   where:

   - *CA-cert-name* is the name of the certificate for the custom certificate authority.
   - *cert-and-private-key* is the certificate and private key for the custom certificate authority.

   Repeat for additional custom certificate authorities.
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.

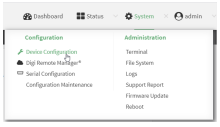
Disable shell access

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.

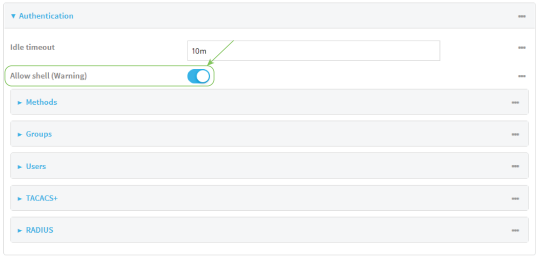
WebUI

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 **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. 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. 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.

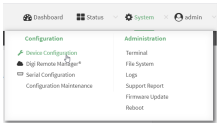
Set the idle timeout for Connect EZ users

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.

WebUI

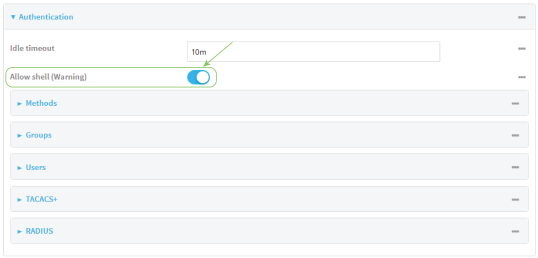
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **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. 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. 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.

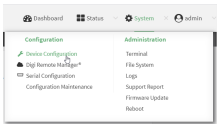
Example user configuration

Example 1: Administrator user with local authentication

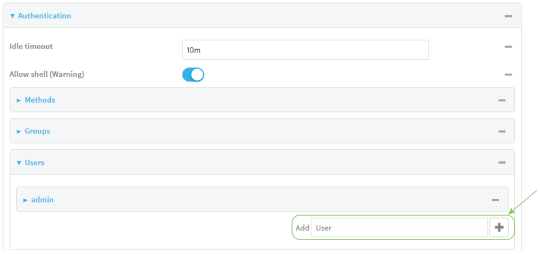
Goal: To create a user with administrator rights who is authenticated locally on the device.

WebUI

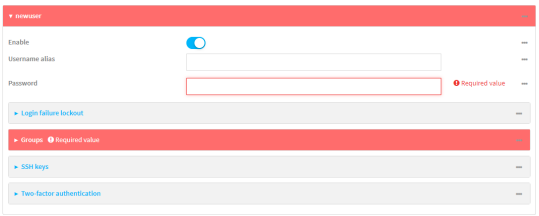
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **Authentication** > **Users**.
4. In **Add User:** enter a name for the user and click ✚.



   The user configuration window is displayed.



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. 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. 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.

WebUI

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:

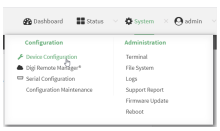
   ```
   $ sudo gedit /etc/tacacs+/tac_plus.conf
   ```

   b. Add a TACACS+ user to the **tac_plus.conf** file:

   ```
   user = admin1 {
          name ="Admin1 for TX64"
          pap = cleartext password1
          service = system {
                  groupname = admin
                  }
          }
   }
   ```

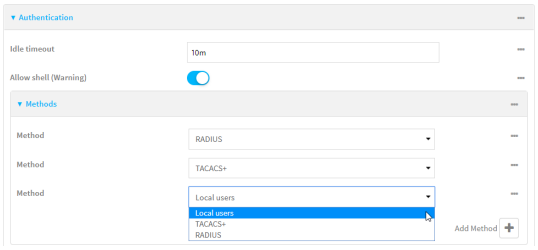
   In this example:
   - The user's username is **admin1**.
   - The user's password is **password1**.
   - The authentication group on the Connect EZ device, **admin**, is identified in the **groupname** parameter.

   c. Save and close the **tac_plus.conf** file.
3. Log into the Connect EZ WebUI as a user with full Admin access rights.
4. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.

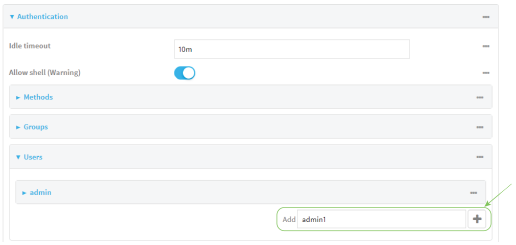


The **Configuration** window is displayed.

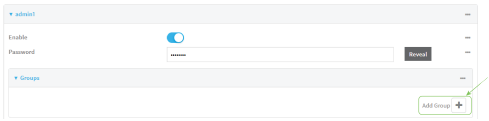
5. Configure the authentication methods:
   a. Click **Authentication** > **Methods**.
   b. For **Method**, select **RADIUS**.
   c. For **Add Method**, click ✚ to add a new method.
   d. For the new method, select **TACACS+**.
   e. Click ✚ to add another new method.
   f. For the new method, select **Local users**.



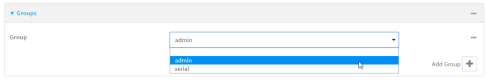
6. Create the local user:
   a. Click **Authentication** > **Users**.
   b. In **Add User:**, type **admin1** and click ✚.



   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. 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.

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 714
Port forwarding rules 718
Packet filtering 725
Configure custom firewall rules 732
Configure captive portals 735
Configure Quality of Service options 739

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.

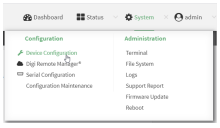
Create a custom firewall zone

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:

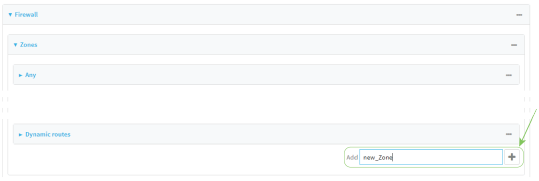
WebUI

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**.

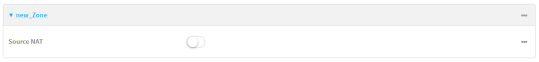


   The **Configuration** window is displayed.
3. Click **Firewall** > **Zones**.

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. 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. Add the new zone. For example, to add a zone named **my_zone**:

```
(config)> add firewall zone my_zone
(config firewall zone my_zone)>
```

4. (Optional) Enable Network Address Translation (NAT):

```
(config firewall zone my_zone)> src_nat true
(config firewall zone my_zone)>
```

5. Save the configuration and apply the change:

```
(config firewall zone my_zone)> 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.

See Configure the firewall zone for a network interface for information about how to configure network interfaces to use a zone.

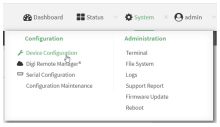
Configure the firewall zone for a network interface

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**.

WebUI

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** > **ETH2**.
4. For **Zone**, select **External**.
5. 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. 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.

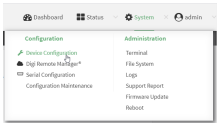
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a custom firewall zone

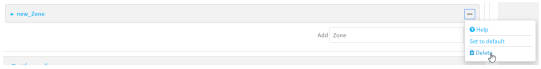
You cannot delete preconfigured firewall zones. To delete a custom firewall zone:

WebUI

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 **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. 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. 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

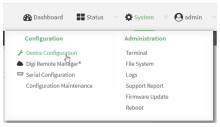
- A label for the port forwarding rule.
- The IP version (either IPv4 or IPv6) that incoming network connections must match.
- The protocols that incoming network connections must match.

- 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:

WebUI

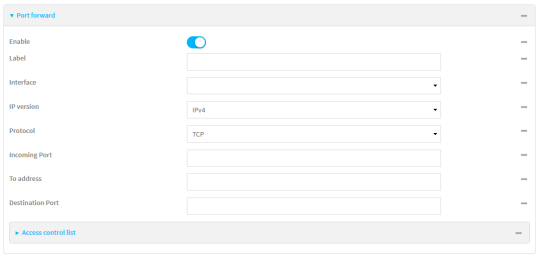
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



   The **Configuration** window is displayed.
3. Click **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, click to 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. 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. 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 **upd**. 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.

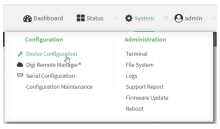
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a port forwarding rule

To delete a port forwarding rule:

WebUI

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 **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. 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. 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.

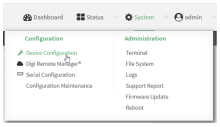
Additional configuration requirements

- 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:

WebUI

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**.



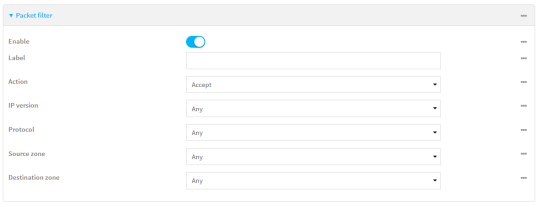
The **Configuration** window is displayed.

3. Click **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, click to 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. 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)>
```

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**
   - **upd**

   The default is **any**.

9. Save the configuration and apply the change:

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

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

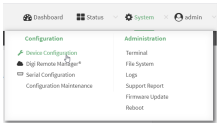
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Enable or disable a packet filtering rule

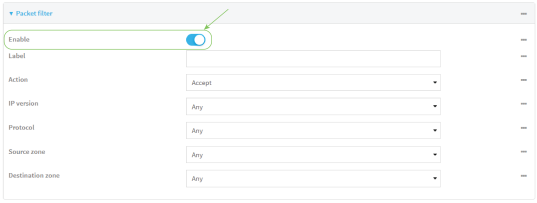
To enable or disable a packet filtering rule:

WebUI

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 **Firewall** > **Packet filtering**.
4. Click the appropriate packet filtering rule.
5. Click **Enable** to toggle the rule between enabled and disabled.



6. 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. 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.

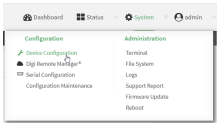
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a packet filtering rule

To delete a packet filtering rule:

WebUI

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 **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. 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. 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)>
```

4. To delete the rule, use the index number with the **del** command. For example:

```
(config)> del firewall filter 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.

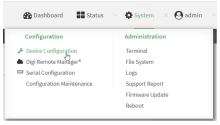
Configure custom firewall rules

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:

WebUI

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 **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. 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. 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)>
```

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.

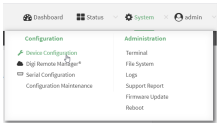
Configure captive portals

Captive portals are commonly used on public-access networks to require users to login or accept terms and conditions before accessing the internet.

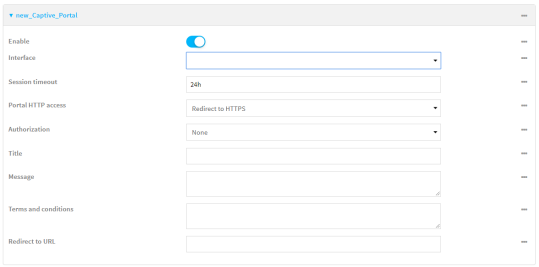
To configure captive portals:

WebUI

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 **Firewall** > **Captive portals**.
4. For **Add captive portal:**, enter a name for the portal and click ✚.



   The captive portal configuration window is displayed.

   The captive portal is enabled by default. To disable, click to toggle off **Enable**.
5. For **Interface**, select the network interface for the portal.

   Traffic received on this interface's network device will not be forwarded unless the client has been granted access.
6. For **Session timeout**, type the amount of time that a user session remains valid. After the session times out, the user will be required to log in again.

   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 **Session timeout** to ten minutes, enter **10m** or **600s**.
7. For **Portal HTTP access**, configure whether the portal can be accessed over an insecure connection.
   - **Allow**: Allows access to the portal page over an insecure connection (HTTP port 80).
   - **Redirect to HTTPS**: Automatically redirects the request to a secure connection (HTTPS port 443).
   - **Disallow**: Does not allow access over an insecure connection (HTTP port 80).

Note This setting does not affect access to HTTP port 80 after the client has been granted access to the portal.

8. For **Authorization**, select the method that will be used to authorize the user:
   - **None**: Users are not required to enter any information to access the portal.
   - **User login**: Users are required to authenticate with an account on this device. Users must be part of a user group that allows access to this portal.
   - **Collect user information**: Users are required to complete a form to continue. The form fields may be customize.
9. (Optional) For **Title**, enter the title of the portal page that the user will see when accessing the portal.
10. (Optional) For **Message**, enter a message that will appear on the portal page.
11. (Optional) For **Terms and Conditions**, enter the terms and conditions that ill appear on the portal page. Users will be required to agree to the terms and conditions before being granted access to the portal.
12. (Optional) For **Redirect to URL**, enter the URL to which the user will be directed when granted access to the portal. If left blank, the user will be directed to the domain of the URL in the original access request.
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. To create an active portal called **portal1**:

```
(config)> add firewall portal portal1
(config firewall portal portal1)>
```

   Captive portals are enabled by default. To disable the portal:

```
(config firewall portal portal1)> enable false
(config firewall portal portal1)>
```

4. Set the network interface for the portal. Traffic received on this interface's network device will not be forwarded unless the client has been granted access.

a. Use the **?** to determine available interfaces:

b. Set the interface. For example:

```
(config firewal portal portal1)> interface /network/interface/eth1
(config firewal portal portal1)>
```

5. Set the amount of time that a user session remains valid. After the session times out, the user will be required to log in again.

```
(config firewall portal portal1)> timeout value
(config firewall portal portal1)>
```

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 **Session timeout** to ten minutes, enter either **10m** or **600s**:

```
(config firewall portal portal1)> timeout 600s
(config firewall portal portal1)>
```

6. Configure whether the portal can be accessed over an insecure connection.

```
(config firewall portal portal1)> http value
(config firewall portal portal1)>
```

where *value* is one of:

- **allow**: Allows access to the portal page over an insecure connection (HTTP port 80).
- **redirect**: Automatically redirects the request to a secure connection (HTTPS port 443).
- **disallow**: Does not allow access over an insecure connection (HTTP port 80).

Note This setting does not affect access to HTTP port 80 after the client has been granted access to the portal.

7. Set the method that will be used to authorize the user:

```
(config firewall portal portal1)> auth value
(config firewall portal portal1)>
```

where *value* is one of:

- **none**: Users are not required to enter any information to access the portal.
- **login**: Users are required to authenticate with an account on this device. Users must be part of a user group that allows access to this portal.
- **info**: Users are required to complete a form to continue. The form fields may be customize.

8. (Optional) Set the title of the portal page that the user will see when accessing the portal:

```
(config firewall portal portal1)> title "Corporate portal"
(config firewall portal portal1)>
```

9. (Optional) Set a message that will appear on the portal page:

```
(config firewall portal portal1)> message "Welcome to the corporate web
portal"
(config firewall portal portal1)>
```

10. (Optional) Set the terms and conditions that ill appear on the portal page. Users will be required to agree to the terms and conditions before being granted access to the portal.

```
(config firewall portal portal1)> terms "Accept the terms and conditions
of this portal"
(config firewall portal portal1)>
```

11. (Optional) Set the URL to which the user will be directed when granted access to the portal. If left blank, the user will be directed to the domain of the URL in the original access request.

```
(config firewall portal portal1)> url https://myportal.com
(config firewall portal portal1)>
```

12. Save the configuration and apply the change:

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

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

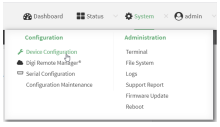
    Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete captive portals

To delete captive portals:

WebUI

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 **Firewall** > **Captive portals**.
4. Click the down caret (▾) next to the appropriate captive portal and select **Delete**.
5. 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. To delete a captive portal, use the **del** command. For example:

```
(config)> del firewall portal portal1
```

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 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:

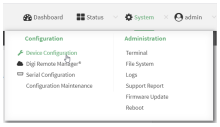
- **Outbound** provides an example of matching packets as they are routed from the device onto the WAN interface.
- **Inbound** provides an example of matching packets as they are routed from the device onto a LAN interface.

These example bindings are disabled by default.

Enable the preconfigured bindings

WebUI

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 **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. 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. Enable one of the preconfiged 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.
>
```

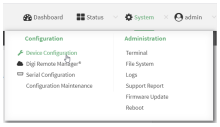
7. Type **exit** to exit the Admin CLI.

   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

WebUI

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**.

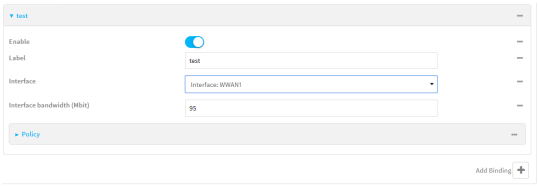


   The **Configuration** window is displayed.

3. Click **Firewall** > **Quality of Service**.
4. For **Add Binding**, click ✚.



   The quality of service binding configuration window is displayed.



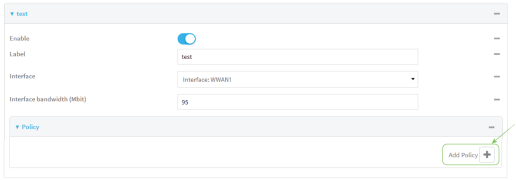
5. **Enable** the binding.
6. (Optional) Type a **Label** for the binding.
7. Select an **Interface** to queue egress packets on. The binding will only match traffic that is being sent out on this interface.
8. (Optional) For **Interface bandwidth (Mbit)**, set the maximum egress bandwidth of the interface, 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:

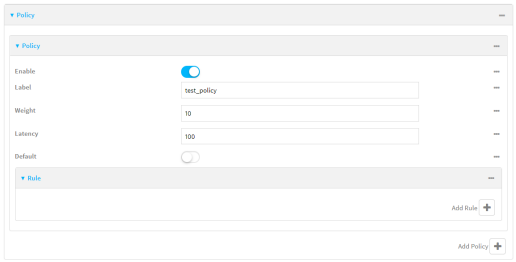
   At least one policy is required for each binding. Each policy can contain up to 30 rules.

   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, click **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.

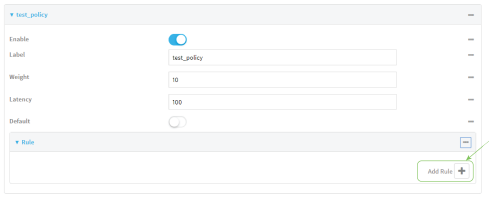
   e. For **Latency**, type the maximum delay before the transmission of packets. A lower latency means that the packets will be scheduled more quickly for transmission.

   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.

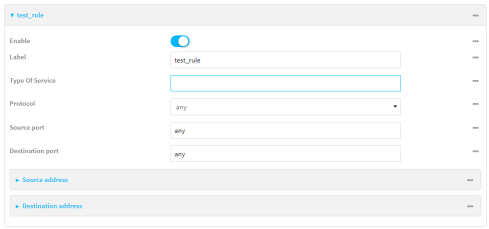
   g. If **Default** is disabled, you must configure at least one rule:

      i. Click to expand **Rule**.

      ii. For **Add Rule**, click ✚.



      The QoS binding policy rule configuration window is displayed.



New QoS binding policy rules are enabled by default. To disable, click **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. 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. 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.

System administration

This chapter contains the following topics:

Review device status 750
Configure system information 751
Update system firmware 753
Update cellular module firmware 758
Reboot your Connect EZ device 762
Erase device configuration and reset to factory defaults 764
Locate the device by using the Find Me feature 769
Configuration files 771
Schedule system maintenance tasks 776
Disable device encryption 780
Configure the speed of your Ethernet ports 783

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:

WebUI

To display system information:

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **Status**.

   A secondary menu appears, along with a status panel.
3. 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. Log into the Connect EZ command line as a user with Admin access.

     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 EZ-000065
  SKU                      : Connect EZ
  Hostname                 : Connect EZ
  MAC Address              : DF:DD:E2:AE:21:18

  Hardware Version         : 50001947-01 1P
  Firmware Version         : 22.2.9.85
  Alt. Firmware Version    : 22.2.9.85
  Alt. Firmware Build Date : Thurs, 03 March 2022 10:16:23
  Bootloader Version       : 19.7.23.0-15f936e0ed

  Current Time             : Thurs, 03 March 2022 10:16:23 +0000
  CPU                      : 1.4%
  Uptime                   : 6 days, 6 hours, 21 minutes, 57 seconds
(541317s)
  Temperature              : 40C

>
```

- Show more detailed system information:
  1. Log into the Connect EZ command line as a user with Admin access.

     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 EZ-000065
  SKU                      : Connect EZ
  Hostname                 : Connect EZ
  MAC Address              : DF:DD:E2:AE:21:18

  Hardware Version         : 50001947-01 1P
  Firmware Version         : 22.2.9.85
  Alt. Firmware Version    : 22.2.9.85
  Alt. Firmware Build Date : Thurs, 03 March 2022 10:16:23
  Bootloader Version       : 19.7.23.0-15f936e0ed
  Schema Version           : 715

  Timezone                 : UTC
  Current Time             : Thurs, 03 March 2022 10:16:23 +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
  Disk
  ----
  Load Average             : 0.09, 0.10, 0.08
  RAM Usage                : 127.843MB/1880.421MB(6%)
  Disk /etc/config Usage   : 18.421MB/4546.371MB(0%)
  Disk /opt Usage          : -4523.-46MB/549.304MB(-822%)
  Disk /overlay Usage      : MB/MB(%)
  Disk /tmp Usage          : 0.007MB/256.0MB(0%)
  Disk /var Usage          : 1.765MB/256.0MB(1%)

>
```

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

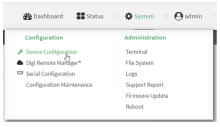
- A name for the device.
- The name of a contact for the device.

- 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:

WebUI

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 **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. 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. 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-22.2.9.85.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

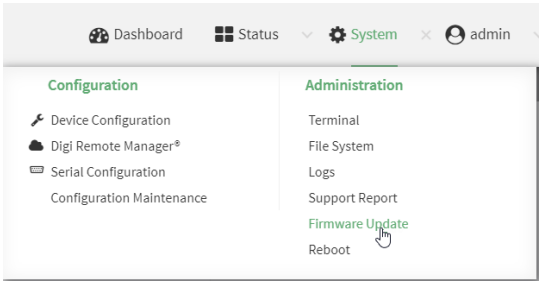
Beginning with firmware version 22.2.9.x, the Connect EZ device uses certificate-based communication for enhanced security when connecting to Digi Remote Manager. If you downgrade your firmware from version 22.2.9.x to version 21.11.x or previous, your device will no longer be able to communicate with Remote Manager.

To remedy this issue, select the device in Remote Manager and select **Actions** > **Reset Device Certificate**.

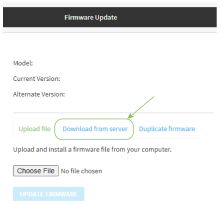
Update firmware over the air (OTA) from the Digi firmware server

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Download from server**.



4. For **Version:**, select the appropriate version of the device firmware.
5. Click **Update Firmware**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 21.11.60.63
Checking for latest Connect EZ firmware...
Newest firmware version available to download is '22.2.9.85'
```

```
Device firmware update from '21.11.60.63' to '22.2.9.85' is needed
>
```

3. Use the **modem firmware ota list** command to list available firmware on the Digi firmware repository.

```
> system firmware ota list
21.11.60.63
22.2.9.85
>
```

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 '22.2.9.85'...
Downloaded firmware /tmp/cli_firmware.bin remaining
Applying firmware version '22.2.9.85'...
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 22.2.9.85
Downloading firmware version '22.2.9.85'...
Downloaded firmware /tmp/cli_firmware.bin remaining
Applying firmware version '22.2.9.85'...
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
>
```

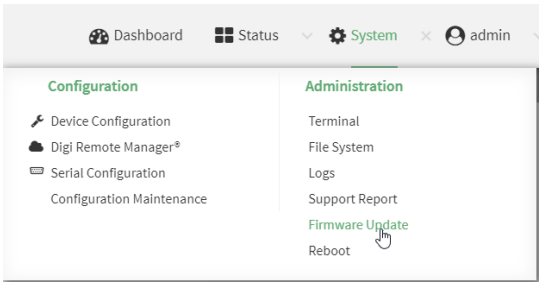
b. Reboot the device:

```
> reboot
>
```

Update firmware from a local file

WebUI

1. Download the Connect EZ operating system firmware from the Digi Support FTP site to your local machine.
2. Log into the Connect EZ WebUI as a user with Admin access.
3. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



4. Click **Choose file**.
5. Browse to the location of the firmware on your local file system and select the file.
6. Click **Update Firmware**.

Command line

1. Download the Connect EZ operating system firmware from the Digi Support FTP site to your local machine.
2. Log into the Connect EZ command line as a user with Admin access.

   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:

```
> 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-
22.2.9.85.bin local /etc/config/ to local
admin@192.168.4.1's password: adminpwd
Connect EZ-22.2.9.85.bin                          100%    36MB    11.1MB/s        00:03
>
```

4. Verify that the firmware file has been successfully uploaded to the device:

```
> ls /etc/config/scripts
-rw-r--r--    1 root     root      37511229 May 16 20:10 Connect EZ-
22.2.9.85.bin
-rw-r--r--    1 root     root          2580 May 16 16:44 accns.json
...
>
```

5. Update the firmware by entering the system firmware update command, specifying the firmware file name:

```
> system firmware update file Connect EZ-22.2.9.85.bin
36632K
netflash: got "/etc/config/Connect EZ-22.2.9.85.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              : 22.2.9.85
 MAC                     : 0040FF800120
 Model                   : Digi Connect EZ
 Current Time            : Thurs, 03 March 2022 10:16:23 +0000
 Uptime                  : 42 seconds (42s)

>
```

Dual boot behavior

By default, the Connect EZ device stores two copies of firmware in two flash memory banks:

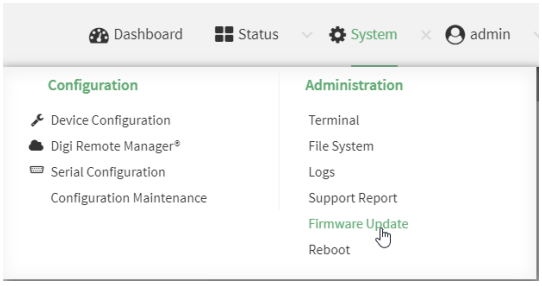
- The current firmware version that is used to boot the device.
- A copy of the firmware that was in use prior to your most recent firmware update.

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.

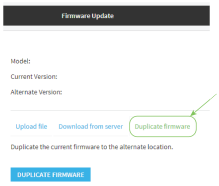
If the device consistently looses power during the boot process, this may result in the current firmware being marked as invalid and the device downgrading to a previous version of the firmware. As a result of this behavior, you can use the following procedure to guarantee that the same firmware is stored in both memory banks:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Administration**, click **Firmware Update**.



3. Click **Duplicate firmware**.



4. Click **Duplicate Firmware**.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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:

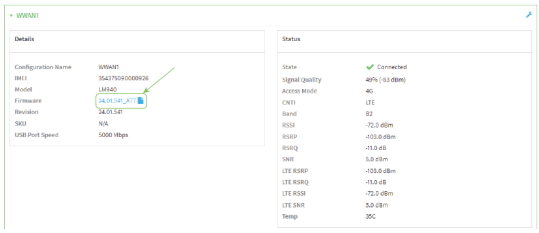
```
> system duplicate-firmware
>
```

Update cellular module firmware

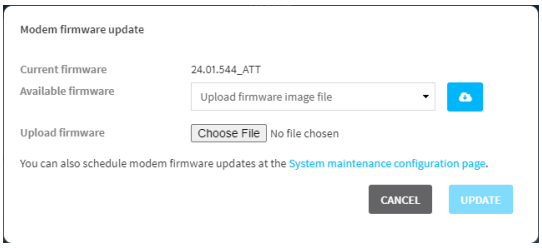
You can update modem firmware by downloading firmware from the Digi firmware repository, or by uploading firmware from your local storage onto the device. You can also schedule modem firmware updates. See Schedule system maintenance tasks for details.

WebUI

1. (Optional) Download the appropriate modem firmware from the Digi repository to your local machine.
2. Log into the Connect EZ WebUI as a user with Admin access.
3. From the main menu, click **Status** > **Modems**.
4. Click the modem firmware version.



The **Modem firmware update** window opens.



5. To update using firmware from the Digi firmware repository:
   a. Click to view available versions.
   b. For Available firmware, select the firmware.
6. To update using firmware from your local file system:
   a. Click **Choose File**.
   b. Select the firmware.
7. To schedule firmware updates, click **System maintenance configuration page**. See Schedule system maintenance tasks for details.
8. Click **Update**.

Command line

Update modem firmware over the air (OTA)

You can update your modem firmware by querying the Digi firmware repository to determine if there is new firmware available for your modem and performing an OTA modem firmware update:

1. Log into the Connect EZ command line as a user with Admin access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. Use the **modem firmware ota check** command to determine if new modem firmware is available on the Digi firmware repository.

```
> modem firmware ota check

Checking for latest ATT firmware ...
Retrieving modem firmware list ...
Newest firmware version available to download is '24.01.5x4_ATT'
Modem firmware update from '24.01.544_ATT' to '24.01.5x4_ATT' is needed
24.01.5x4_ATT
24.01.544_ATT

>
```

3. Use the **modem firmware ota list** command to list available firmware on the Digi firmware repository.

```
>  modem firmware ota list

Retrieving modem firmware list ...
25.20.664_CUST_044_3
25.20.666_CUST_067_1
25.20.663_CUST_040

>
```

4. Perform an OTA firmware update:
   - To perform an OTA firmware update by using the most recent available modem firmware from the Digi firmware repository, type:

```
>  modem firmware ota update

Checking for latest Generic firmware ...
Retrieving modem firmware list ...
Newest firmware version available to download is '25.20.666_CUST_
067_1'
Retrieving download location for modem firmware '25.20.666_CUST_067_
1' ...

>
```

   - 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 **modem firmware ota list** command. For example::

```
>  modem firmware ota update version 24.01.5x4_ATT

Retrieving download location for modem firmware '24.01.5x4_ATT' ...
Downloading modem firmware '24.01.5x4_ATT' to '/opt/LE910C4_
NF/Custom_Firmware' ...
Modem firmware '24.01.5x4_ATT' downloaded
Updating modem firmware ...
Programming modem firmware ...
```

```
Found modem ...
Validate modem firmware ...
Getting ready for update ...
Stopping services ...
Running update pass 1 of 3 ...
Restarting services ...
-----------------------------
Successfully updated firmware
Modem firmware update complete

>
```

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.

Update modem firmware by using a local firmware file

You can update your modem firmware by uploading a modem firmware file to your Connect EZ device. Firmware should be uploaded to /opt/*MODEM_MODEL*/Custom_Firmware, for example, /opt/LM940/Custom_Firmware.

Modem firmware can be downloaded from Digi here. Follow instructions on this page to determine the cellular module used by your device. After downloading, use tar or a similar unzipping tool to extract the firmware prior to uploading to the device. Note that the firmware file may not have a tar.gz extension, but it is a tar file and can be unzipped with tar or a similar tool. See Use the scp command for information about uploading files to the Connect EZ device.

1. Log into the Connect EZ command line as a user with Admin access.

   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.

2. Use the **modem firmware check** command to determine if new modem firmware is available on local device.

```
> modem firmware check

Checking for latest ATT firmware in flash ...
Newest firmware version available in flash is '05.05.58.00_ATT_005.026_
000'
Modem firmware up to date
05.05.58.00_ATT_005.026_000

> modem firmware check
```

3. Use the **modem firmware list** command to list available firmware on the Connect EZ device.

```
>  modem firmware list

ATT, 24.01.544_ATT, current
Generic, 24.01.514_Generic, image
Verizon, 24.01.524_Verizon, image
```

```
ATT, 24.01.544_ATT, image
Sprint, 24.01.531-B003_Sprint, image

>
```

4. To perform an firmware update by using a local file, use the **version** parameter to identify the appropriate firmware version as determined using the **modem firmware check** or **modem firmware list** command. For example::

```
>  modem firmware update version 24.01.5x4_ATT

Updating modem firmware ...

----------------------------
Successfully updated firmware
Modem firmware update complete

>
```

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.

Reboot your Connect EZ device

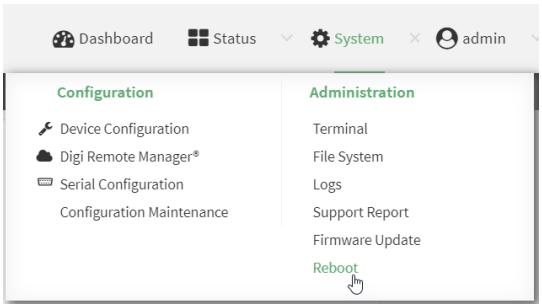
You can reboot the Connect EZ device immediately or schedule a reboot for a specific time every day.

Note You may want to save your configuration settings to a file before rebooting. See Save configuration to a file.

Reboot your device immediately

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. From the main menu, click **System**.
3. Click **Reboot**.



4. Click **Reboot** to confirm that you want to reboot the device.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

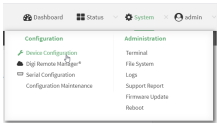
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **admin** to access the Admin CLI.
2. At the prompt, type:

```
> reboot
```

Schedule reboots of your device

WebUI

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. 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. 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. 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, the 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:

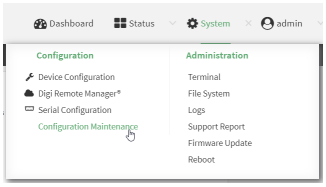
- Erases all automatically generated certificates and keys.
- With firmware release 22.2.9.x and newer, erases the client-side certificate used for communication with Digi Remote Manager.

  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.

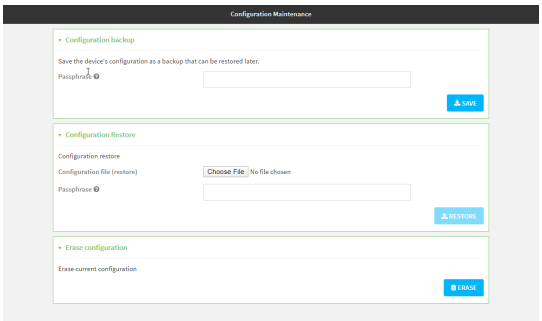
You can also reset the device to the default configuration without removing scripts, keys, and logfiles by using the **revert** command.

WebUI

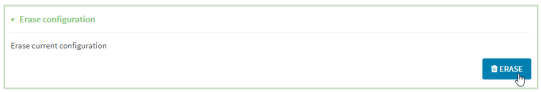
1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



   The **Configuration Maintenance** windows is displayed.



3. In the **Erase configuration** section, click **ERASE**.



4. Click **CONFIRM**.
5. 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).

When you first log into the WebUI or the command line, you will be required the change the SSID and pre-shared key (password) for the preconfigured Wi-Fi access point before you can save any configuration changes. See Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point for instructions.

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. Log into the Connect EZ command line as a user with Admin access.

   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).

      When you first log into the WebUI or the command line, you will be required the change the SSID and pre-shared key (password) for the preconfigured Wi-Fi access point before you can save any configuration changes. See Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point for instructions.

   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 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 releasethe **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).

When you first log into the WebUI or the command line, you will be required the change the SSID and pre-shared key (password) for the preconfigured Wi-Fi access point before you can save any configuration changes. See Reset default SSID and pre-shared key for the preconfigured Wi-Fi access point for instructions.

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. 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. 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.

Configure the Connect EZ device to use 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.

Note To clear the custom default configuration, press the RESET button, wait for the device to reboot, then press the RESET button again.

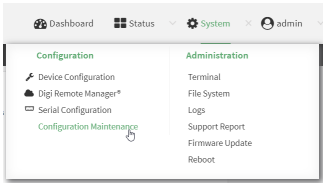
Required configuration items

- Custom factory default file

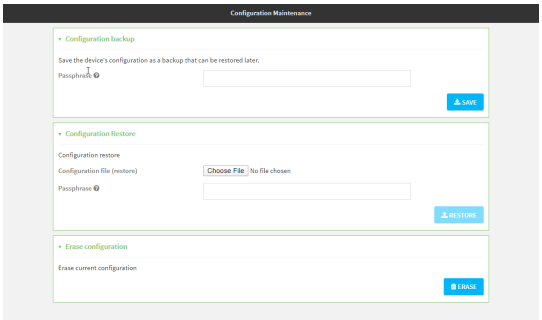
WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. Configure your Connect EZ device to match the desired custom factory default configuration.

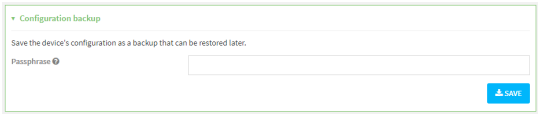
   For example, you may want to configure the device to use a custom APN or a particular network configuration, so that when you reset the device to factory defaults, it will automatically have your required network configuration.
3. On the main menu, click **System**. Under **Configuration**, click **Configuration Maintenance**.



   The **Configuration Maintenance** windows is displayed.

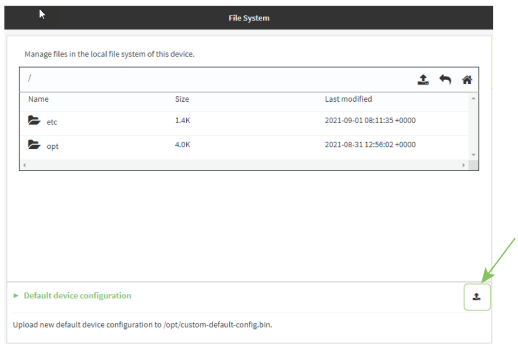


4. In the **Configuration backup** section, click **SAVE**.



   Do not set a **Passphrase** for the configuration backup. The file will be downloaded using your browser's standard download process.
5. After the configuration backup file has been downloaded, rename the file to:

   custom-default-config.bin
6. Upload the file to the device:
   a. From the main menu, select **System** > **Filesystem**.
   b. Under **Default device configuration**, click .



c. Select the file from your local file system.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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. 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.

Locate the device by using the Find Me feature

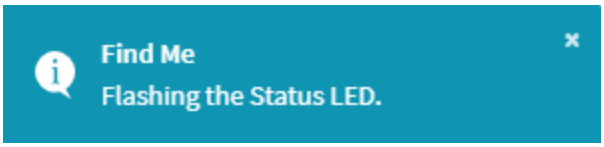
Use the **Find Me** feature to cause LEDs on the device to blink, which can help you to identify the specific device.

To use this feature:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **Find Me**.

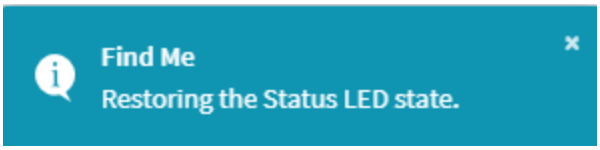
   A notification message appears, noting that the LED is flashing on the device. Click the **x** in the message to close it.



3. On the menu, click **System** again. Ablue circle next to **Find Me** is blinking, indicating that the **Find Me** feature is active.

4. 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. Log into the Connect EZ command line as a user with Admin access.

   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
>
```

Configuration files

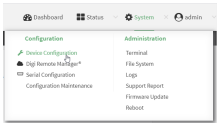
The Connect EZ configuration file, /etc/config/accns.json, contains all configuration changes that have been made to the device. It does not contain the complete device configuration; it only contains changes to the default configuration. Both the default configuration and the changes contained in the 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.

WebUI

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. Make any necessary configuration changes.
4. 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. Make any necessary configuration changes.
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.

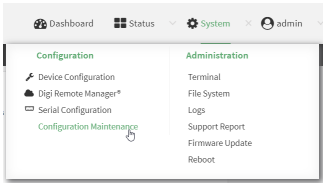
Save configuration to a file

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.

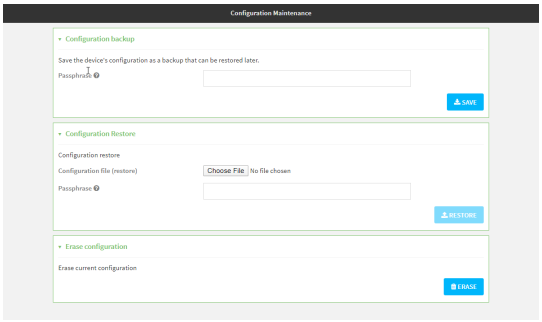
WebUI

This procedure creates a binary archive file containing the device's configuration, certificates and keys, and other information.

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



   The **Configuration Maintenance** windows is displayed.



3. In the **Configuration backup** section:
   a. (Optional) To encrypt the configuration using a passphrase, for **Passphrase (save/restore)**, enter the passphrase.
   b. Click **SAVE**.

   The file will be downloaded using your browser's standard download process.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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:

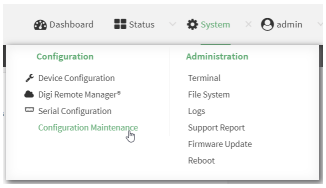
```
> scp host 192.168.4.1 user admin remote /home/admin/bin/ local
/etc/config/backup-archive-0040FF800120-19.05.17-19.01.17.bin to remote
```

Restore the device configuration

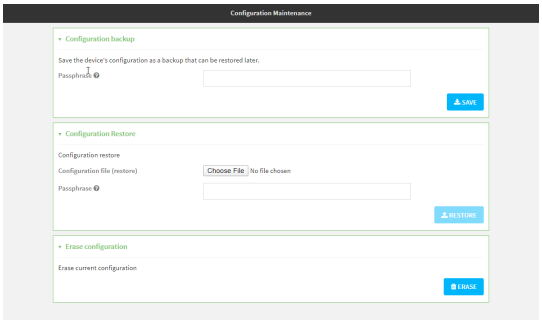
You can restore a configuration file to your Connect EZ device by using a backup from the device, or a backup from a similar device.

WebUI

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



The **Configuration Maintenance** windows is displayed.



3. 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**.
4. Click **CONFIRM**.

   The configuration will be restored and the device will be rebooted.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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-0040FF800120-22.2.9.85-19.23.42.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-0040FF800120-22.2.9.85-
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.

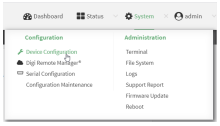
You can also schedule custom scripts to run during the maintenance window. See Configure scripts to run automatically for more information.

Required configuration items

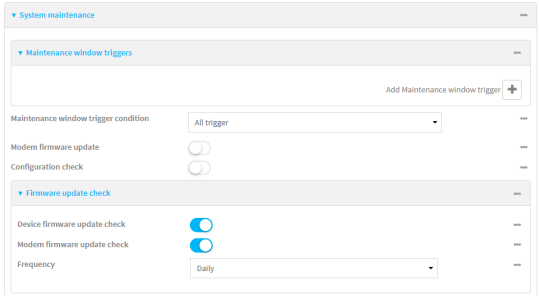
- Events that trigger the maintenance window to begin.
- Whether all configured triggers, or only one of the triggers, must be met.
- The tasks to be performed. Options are:
  - Firmware updates.
  - Digi Remote Manager configuration check.
- Whether the device will check for updates to the device firmware.
- Whether the device will check for updates to the modem firmware.
- The frequency (daily, weekly, or monthly) that checks for firmware updates will run.

WebUI

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 **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. (Optional) Click to enable **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.

   Note If your device is managed by a Digi Remote Manager configuration, the configuration manages the device's firmware version. You should not enable this option.

8. (Optional) Click to enable **Modem firmware update** to instruct the system to look for any updated modem firmware during the maintenance window. If updated firmware is found, it will then be installed. Modem firmware update looks for updated firmware both on the local device and over the network, using either a WAN or cellular connection.

9. (Optional) Click to enable **Configuration check** to allow for the configuration to be updated, including by custom scripts, during the maintenance window.
10. (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 to automated checking for device firmware updates.
    c. **Modem firmware update check** is enabled by default. This enables to automated checking for modem firmware updates.
    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**.
11. 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. 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)>
```

ii. 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. (Optional)) 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 either a WAN or cellular connection.

```
(config)> system schedule maintenance device_fw_update value
(config)>
```

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

Note If your device is managed by a Digi Remote Manager configuration, the configuration manages the device's firmware version. You should not enable this option.

5. (Optional) Configure the device to look for any updated modem 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 either a WAN or cellular connection.

```
(config)> system schedule maintenance modem_fw_update value
(config)>
```

where *value* is either **true** or **false**. **yes** or **no**, and **1** or **0** are also allowed.

6. (Optional) Configure automated checking for device 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. Set how often automated checking for device firmware should take place:

```
(config)> system schedule maintenance frequency value
(config)>
```

   where *value* is either **daily**, **weekly**, or **monthly**. **daily** is the default.

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.

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 and WWAN. 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. Log into the Connect EZ command line as a user with Admin access.

   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.

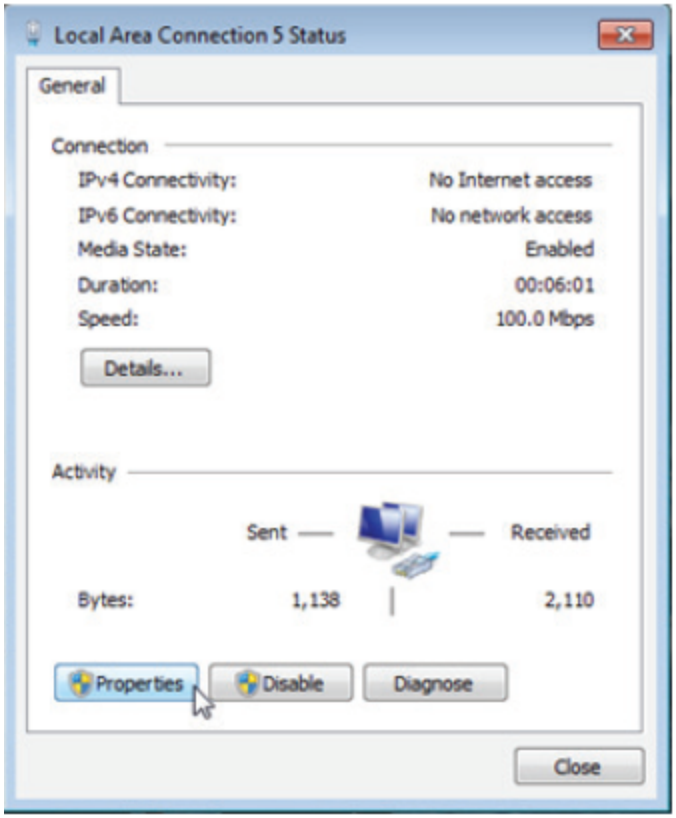
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Re-enable cryptography after it has been disabled.

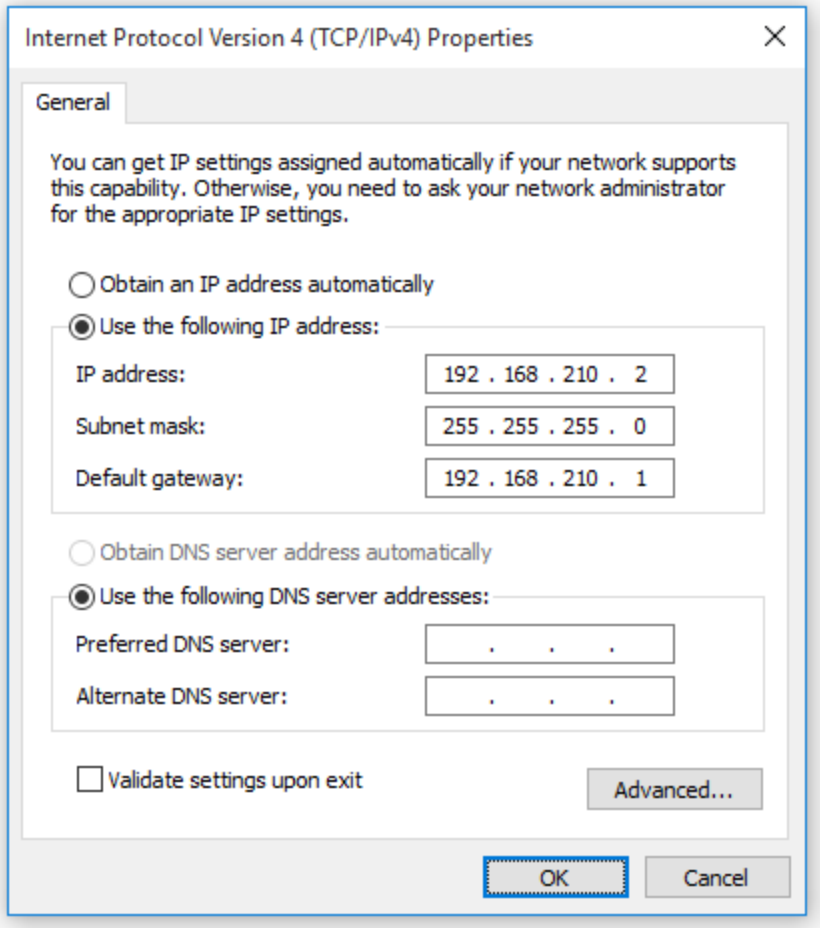
To re-enable cryptography:

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 ETH1 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
```

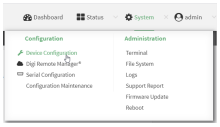
This will re-enable encryption and leave the device at its factory default setting.

Configure the speed of your Ethernet ports

You can configure the speed of your Connect EZ device's Ethernet ports.

WebUI

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** > **Device**.
4. Click to expand the Ethernet port to be configured.
5. For **Speed**, select the appropriate speed for the Ethernet port, or select **Auto** to automatically detect the speed. The default is **Auto**.
6. 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. At the config prompt, type:

```
(config)> network device eth_port value
```

where:

- *eth_port* is the name of the Ethernet port (for example, **eth1**)
- *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.

Monitoring

This chapter contains the following topics:

intelliFlow 787
Configure NetFlow Probe 794

intelliFlow

intelliFlow monitors system information, network data usage, and traffic information, and displays the information in a series of charts available in the local WebUI. To use intelliFlow, the Connect EZ must be powered on and 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.

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 dymanic; 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.

Note When intelliFlow is enabled and the device is connected to Digi aView, it adds an estimated 50MB of data usage for the device by reporting the metrics to aView. intelliflow does not currently work with Digi Remote Manager.

Enable intelliFlow

Required configuration items

- Enable intelliFlow.

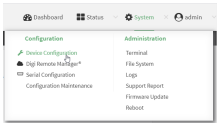
Additional configuration items

- The firewall zone for internal clients being monitored by intelliFlow.

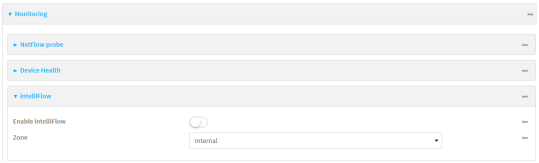
To enable intelliFlow:

WebUI

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 **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. 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. 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.

Use intelliFlow to display average CPU and RAM usage

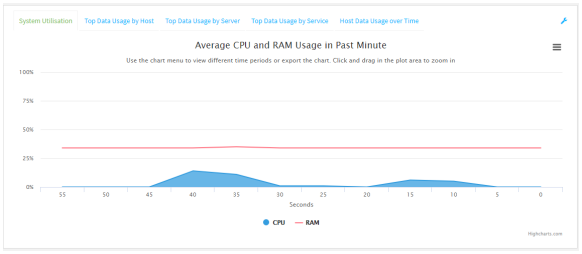
This procedure is only available from the WebUI.

To display display average CPU and RAM usage:

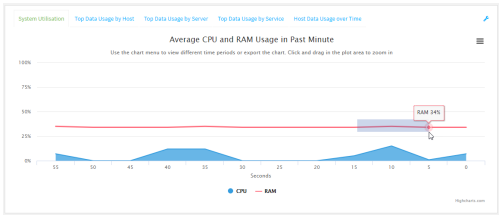
WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.

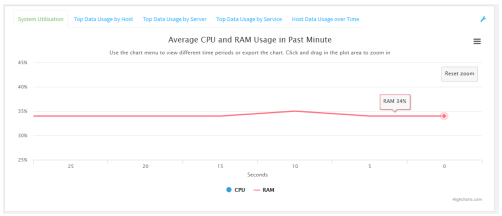
The System Utilisation chart is displayed:



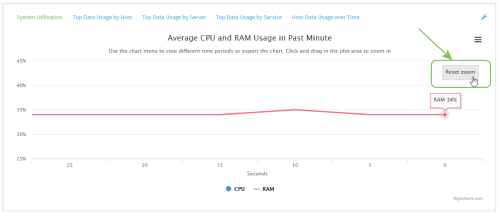
- Display more granular information:
  1. Click and drag over an area in the chart to zoom into that area and provide more granular information.



  2. Release to display the selected portion of the chart:



3. Click **Reset zoom** to return to the original display:

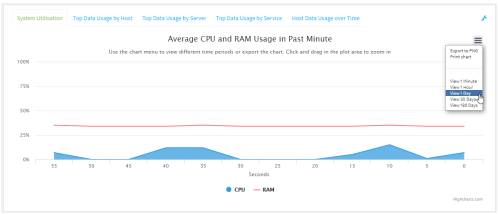


- Change the time period displayed by the chart.

  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:

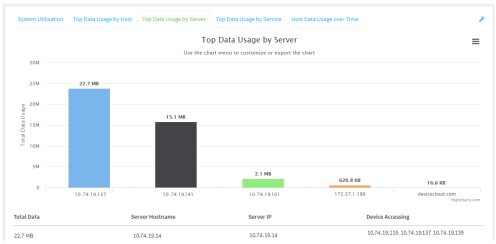
WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.

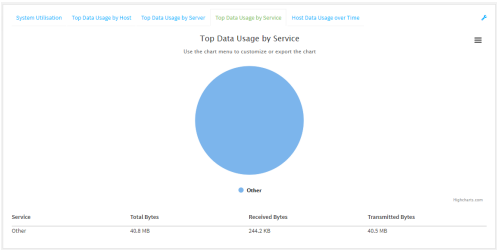
4. Display a data usage chart:
   - To display the **Top Data Usage by Host** chart, click **Top Data Usage by Host**.



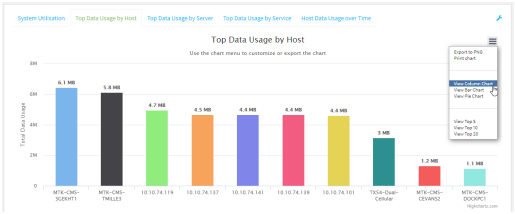
   - To display the **Top Data Usage by Server** chart, click **Top Data Usage by Server**.



   - To display the **Top Data Usage by Service** chart, click **Top Data Usage by Service**.

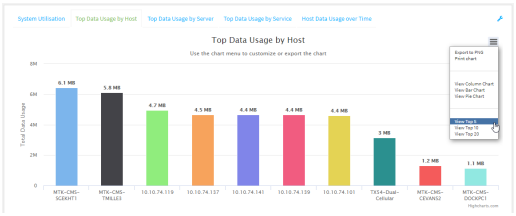


5. Change the type of chart that is used to display the data:
   a. Click the menu icon (☰).
   b. Select the type of chart.



6. 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.



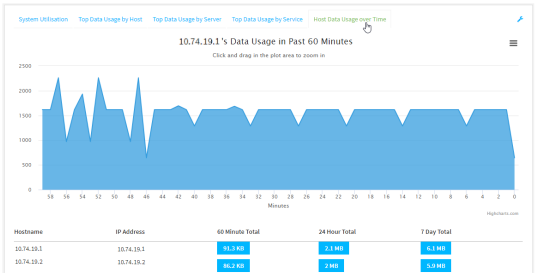
7. Save or print the chart.
   a. Click the menu icon (☰).
   b. To save the chart to your local filesystem, select **Export to PNG**.
   c. To print the chart, select **Print chart**.

Use intelliFlow to display data usage by host over time

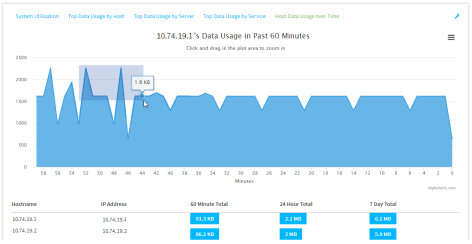
To generate a chart displaying a host's data usage over time:

WebUI

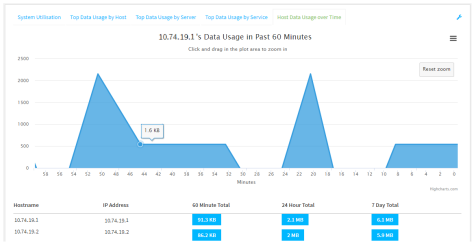
1. Log into the Connect EZ WebUI as a user with Admin access.
2. If you have not already done so, enable intelliFlow. See Enable intelliFlow.
3. From the menu, click **Status** > **intelliFlow**.
4. Click **Host Data Usage Over Time**.



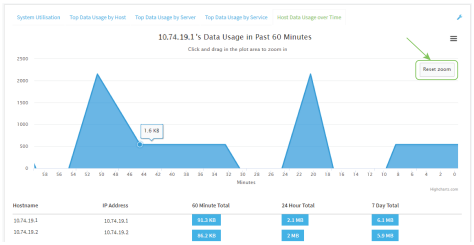
- Display more granular information:
  a. Click and drag over an area in the chart to zoom into that area and provide more granular information.



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.

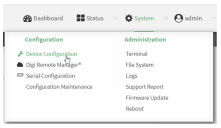
Additional configuration items

- 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.

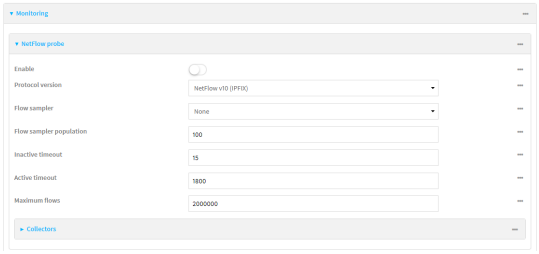
To probe network traffic and export statistics to NetFlow collectors:

WebUI

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 **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. 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. 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 800
Certificate-based enhanced security 800
Configure Digi Remote Manager 800
Collect device health data and set the sample interval 807
Enable event log upload to Digi Remote Manager 810
Log into Digi Remote Manager 811
Use Digi Remote Manager to view and manage your device 812
Add a device to Digi Remote Manager 813
View Digi Remote Manager connection status 813
Configure multiple devices using profiles 814
Learn more 814

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. You can also select to use Digi aView as the cloud-based management system. See *Digi aView User Guide* for information about aView.

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 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 new URL of edp12.devicecloud.com is for device communication only. Use my.devicecloud.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 Digi Remote Manager

By default, your Connect EZ device is configured to use central management using Digi Remote Manager.

Additional configuration options

These additional configuration settings are not typically configured, but you can set them as needed:

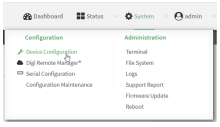
- Disable the Digi Remote Manager connection if it is not required. You can also configure an alternate cloud-based central management application.
- Change the reconnection timer.
- The non-cellular keepalive timeout.
- The cellular keepalive timeout.

- The keepalive count before the Remote Manager connection is dropped.
- SMS support.
- HTTP proxy server support.

To configure Digi Remote Manager:

WebUI

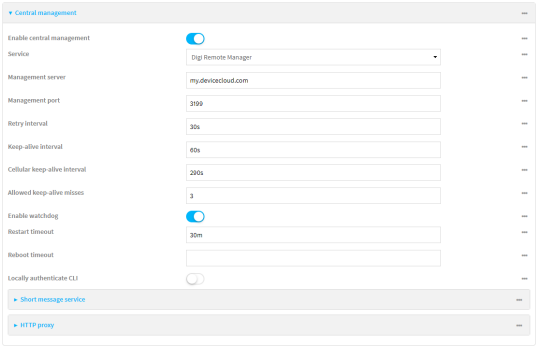
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



The **Configuration** window is displayed.

3. Click **Central management**.

   The Central management configuration window is displayed.



   Digi Remote Manager support is enabled by default. To disable, click **Enable central management**.

4. (Optional) For **Service**, select either **Digi Remote Manager** or **Digi aView**. The default is **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 infomation.
   - Firmware prior to version 22.2.9.x, the default is the Digi Remote Manager server, my.devicecloud.com.

6. (Optional) For **Management port**, type the destination port for the remote cloud services connection. The default is **3199**.
7. (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**.
8. (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**.
9. (Optional) For **Cellular 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 cellular interface. The default is 290 seconds.

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

   For example, to set **Cellular keep-alive interval** to ten minutes, enter **10m** or **600s**.

10. (Optional) For **Allowed keep-alive misses**, type the number of allowed keep-alive misses. The default is **3**.
11. **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.
12. 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 servicesis 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.
13. (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.
14. (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.
    d. (Optional) Type the **Service identifier**.
15. (Optional) Configure the Connect EZ device to communicate with remote cloud services by using an HTTP proxy server:
    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**.
16. 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. Digi Remote Manager support is enabled by default. To disable Digi Remote Manager support:

```
(config)> cloud enable false
(config)>
```

4. (Optional) Set the service:

```
(config)> cloud service value
(config)>
```

   where *value* is either:

   - **drm**: Digi Remote Manager
   - **aview**: Digi aView

   The default is Digi Remote Manager.
5. (Optional) Set the URL for the central management server. The default is the Digi Remote Manager server, my.devicecloud.com.

```
(config)> cloud drm drm_url url
(config)>
```

6. (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)>
```

7. (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)>
```

8. (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 cellular interface. Allowed values are from 30 seconds to two hours. The default is 290 seconds.

   ```
   (config)> cloud drm cellular_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 cellular keep-alive interval** to ten minutes, enter either **10m** or **600s**:

   ```
   (config)> cloud drm cellular_keep_alive 600s
   (config)>
   ```

9. 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)>
   ```

10. 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)>
    ```

11. 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 servicesis 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.

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 drm_phone_number
(config)>
```

    c. (Optional) Set the service identifier:

```
(config)> cloud drm sms sercice_id id
(config)>
```

1. (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)>
```

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.

Collect device health data and set the sample interval

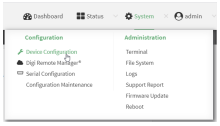
You can enable or disable the collection of device health data to upload to Digi Remote Manager, and configure the interval between health sample uploads. By default, device health data upload is enabled, and the health sample interval is set to 60 minutes.

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:

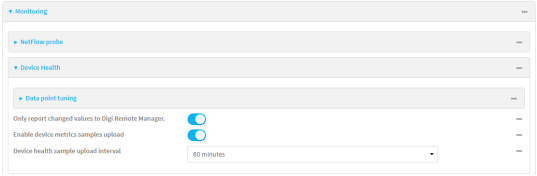
WebUI

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 **Monitoring** > **Device Health**.



4. (Optional) Click to expand **Data point tuning**.

   Data point tuning options allow to you 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, click to 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. 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. 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.
5. 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**.

6. (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
       cellular
                rx
                        bytes
                                enable true
                tx
                        bytes
                                enable true
       eth
                rx
                        bytes
                                enable true
                tx
                        bytes
                                enable true
       serial
                rx
                        bytes
                                enable true
                tx
                        bytes
                                enable true
cellular
       1
                rx
                        bytes
                                enable true
                        packets
                                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)>
```

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.

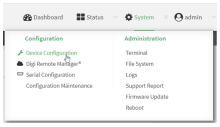
Enable event log upload to Digi Remote Manager

You can configure your device to upload the event log to Digi Remote Manager, and configure the interval between event log uploads.

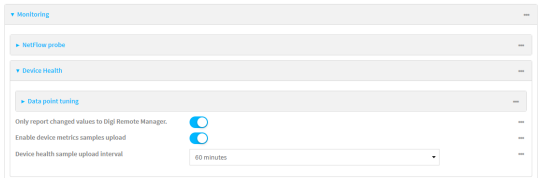
To enable the event log upload, or disable it if it has been disabled, and to change the upload interval:

WebUI

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 **Monitoring** > **Device event logs**.



4. Click **Enable event log uploads**.
5. For **Device event log upload interval**, select the interval between health sample uploads.
6. 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. 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)>
     ```

4. 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.

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.

Log into Digi Remote Manager

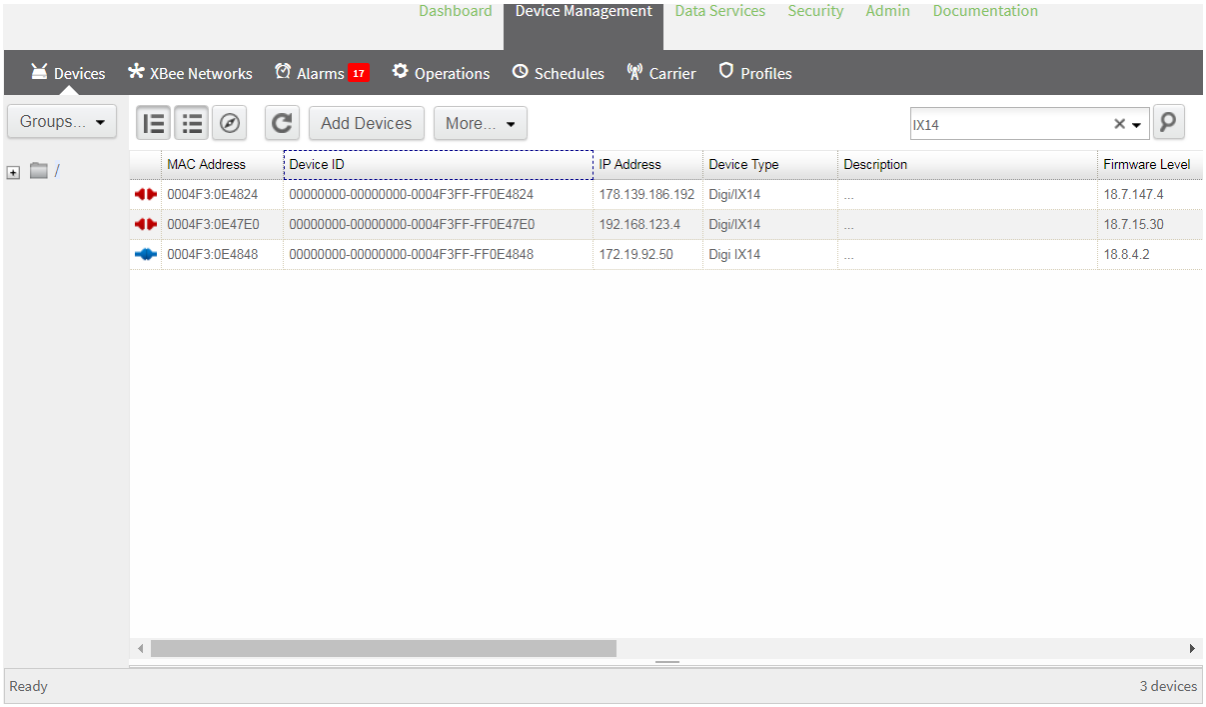
To start Digi Remote Manager

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.
4. Log into your Digi Remote Manager account.

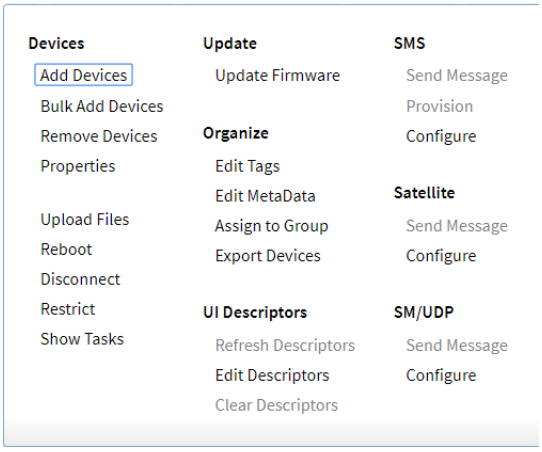
Use Digi Remote Manager to view and manage your device

To view and manage your device:

1. If you have not already done so, connect to your Digi Remote Manager account.
2. Click **Device Management** to display a list of your devices.
3. Use the Search bar to locate the device you want to manage.



4. Select the device and click **Properties** to view general information for the device.
5. Click the **More** menu to perform a task.



Add a device to 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. Click **Add Devices**.
4. Select **MAC Address** and enter the Ethernet MAC address for your device.
5. For **Install Code**, 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. Click **Add**.
7. Click **OK**.

Digi Remote Manager adds your Connect EZ device to your account and it appears in the **Device Management** view.

View Digi Remote Manager connection status

To view the current Digi Remote Manager configuration:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. The dashboard includes a Digi Remote Manager status pane:

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. View the central management configuration:

```
(config)> show cloud
drm
       cellular_keep_alive 290s
       drm_url my.devicecloud.com
       keep_alive 60s
       keep_alive_misses 3
       retry_interval 30s
enable true
(config)>
```

1. Type **cancel** to exit configuration mode:

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

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.

To view the status of your device's connection to Remote Manager, use the show cloudcommand at the command line:

Command line

```
> show cloud

 Device Cloud Status
 -------------------

 Status    : Connected
 Server    : my.devicecloud.com
 Device ID : 00000000-00000000-0040FFFF-FF0F4594
>
```

The **Device ID** is the unique identifier for the device, as used by the Remote Manager.

Configure multiple devices using profiles

Digi recommends you take advantage of Digi Remote Manager profiles to manage multiple Connect EZ routers. 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 Digi Remote Manager account.
3. In Digi Remote Manager, create a profile based on the configured Connect EZ.
4. Apply the profile to the Connect EZ devices you need to configure.

Digi Remote Manager provides multiple methods for applying profiles to registered devices. You can also include site-specific settings with a profile to override settings on a device-by-device basis.

Learn more

- For information on using Digi Remote Manager to configure and manage Connect EZ routers, see the *Digi Remote Manager User Guide*.
- For information on using Digi Remote Manager APIs to develop custom applications, see the *Digi Remote Manager Programmer Guide*.

File system

This chapter contains the following topics:

The Connect EZ local file system 816
Display directory contents 816
Create a directory 817
Display file contents 818
Copy a file or directory 818
Move or rename a file or directory 819
Delete a file or directory 820
Upload and download files 821

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, such as cellular module images. The writable directories within the filesystem are:

- /tmp
- /opt
- /etc/config

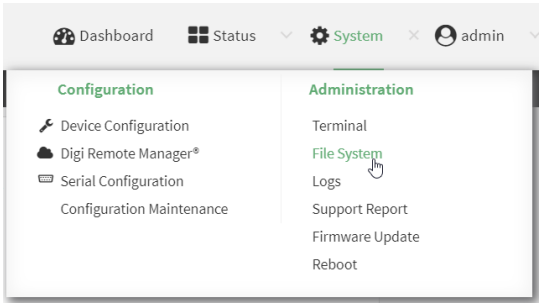
Files stored in the /tmp directory do not persist across reboots. Therefore, /tmp is a good location to upload temporary files, such as files used for firmware updates. Files stored in /opt and /etc/config do persist across reboots, but are deleted if a factory reset of the system is performed. See Erase device configuration and reset to factory defaults for more information.

Display directory contents

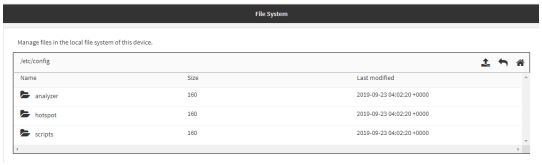
To display directory contents by using the WebUI or the Admin CLI:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight a directory and click ↱ to open the directory and view the files in the directory.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 **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
...
>
```

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.

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:

1. Log into the Connect EZ command line as a user with Admin access.

   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 **mkdir /*path*/*dir_name***. For example, to create a directory named **temp** in **/etc/config**:

```
> mkdir /etc/config/temp
>
```

3. 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
>
```

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.

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. Log into the Connect EZ command line as a user with Admin access.

   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 contenct of the file **accns.json** in **/etc/config**:

```
> more /etc/config/accns.json
{
    "auth":
        "user": {
            "admin": {
                "password":
"$2a$05$W1sls1oxsadf/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. Log into the Connect EZ command line as a user with Admin access.

   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 **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/
>
```

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 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**:

1. Log into the Connect EZ command line as a user with Admin access.

   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:

```
> mv /etc/config/scripts/test.py /etc/config/scripts/final.py
>
```

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 move **test.py** from **/etc/config/scripts** to **/opt**:

1. Log into the Connect EZ command line as a user with Admin access.

   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:

```
> mv /etc/config/scripts/test.py /opt/
>
```

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

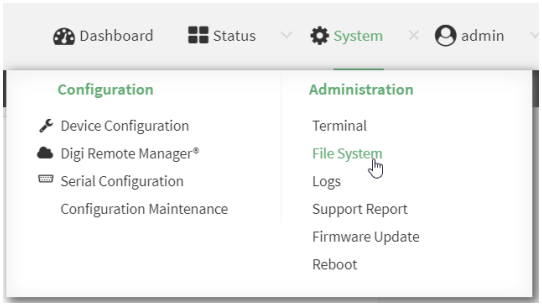
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Delete a file or directory

To delete a file or directory by using the WebUI or the Admin CLI:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the directory containing the file to be deleted and click to open the directory.
4. Highlight the file to be deleted and click .
5. Click **OK** to confirm.

Command line

To delete a file named **test.py** in **/etc/config/scripts**:

1. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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.

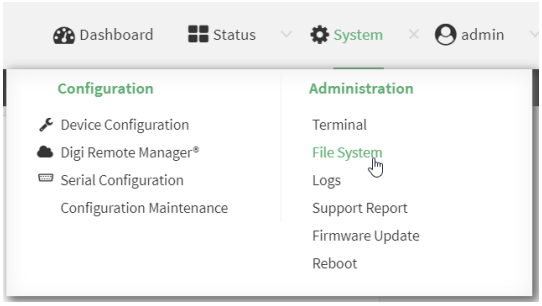
Upload and download files

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.

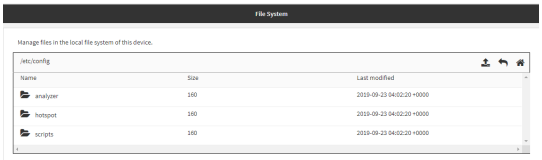
Upload and download files by using the WebUI

Upload files

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



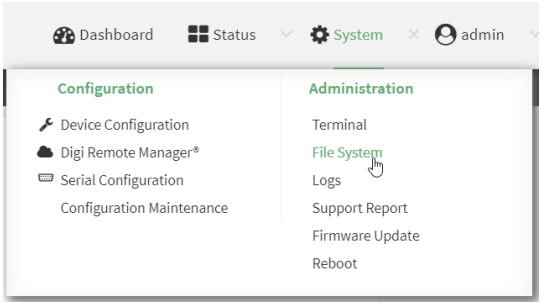
   The **File System** page appears.



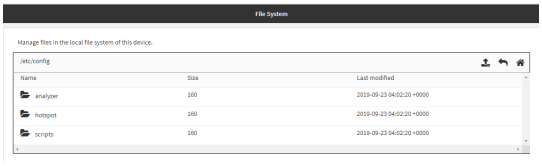
3. Highlight the directory to which the file will be uploaded and click ↩ to open the directory.
4. Click ⬆ (upload).
5. Browse to the location of the file on your local machine. Select the file and click **Open** to upload the file.

Download files

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the directory to which the file will be uploaded and click ↱ to open the directory.
4. 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-
22.2.9.85.bin local /etc/config/scripts to local
admin@192.168.4.1's password: adminpwd
Connect EZ-22.2.9.85.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 /var/log/
   Saving support report to /var/log/support-report-0040D0133536-22-03-03-
   10:16:23.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:D0:13:35:36-22-03-03-10:16:23.bin to remote
   admin@192.168.4.1's password: adminpwd
   support-report-0040D0133536-22-03-03-10:16:23.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-22.2.9.85
Uploading Connect EZ-22.2.9.85 to Connect EZ-22.2.9.85
Connect EZ-22.2.9.85
          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 826
Generate a support report 826
View system and event logs 828
Configure syslog servers 832
Configure options for the event and system logs 834
Analyze network traffic 839
Use the ping command to troubleshoot network connections 856
Use the traceroute command to diagnose IP routing problems 856

Perform a speedtest

To perform a speedtest:

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

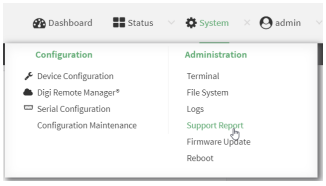
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Generate a support report

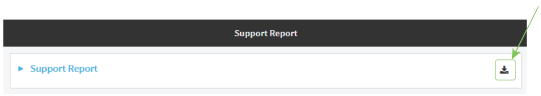
To generate and download a support report:

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **System**. Under **Administration**, click **Support Report**.



3. Click to generate and download the support report.



Attach the support report to any support requests.

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 /var/log/
Saving support report to /var/log/support-report-0040D0133536-22-03-03-
10:16:23.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:D0:13:35:36-22-03-03-10:16:23.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-22-03-03-10:16:23.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.

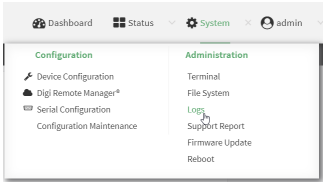
View system and event logs

See Configure options for the event and system logs for information about configuring the information displayed in event and system logs.

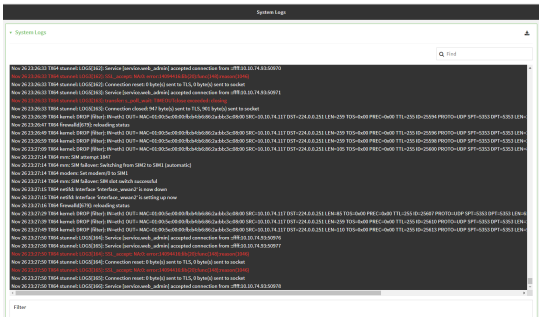
View System Logs

WebUI

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



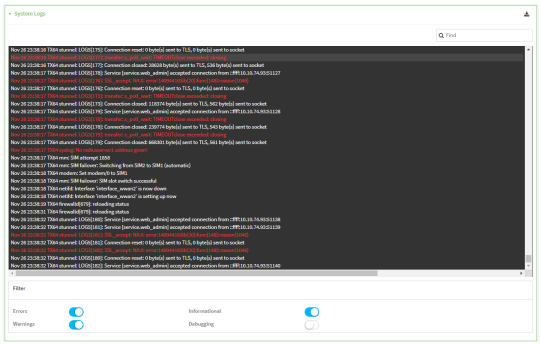
The system log displays:



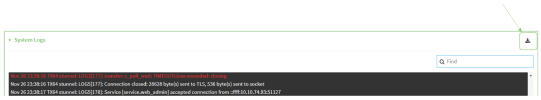
3. Limit the display in the system log by using the **Find** search tool.



4. Use filters to configure the types of information displayed in the system logs.



5. Click to download the system log.



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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 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
...
>
```

3. (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
...
>
```

4. (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
```

```
...
>
```

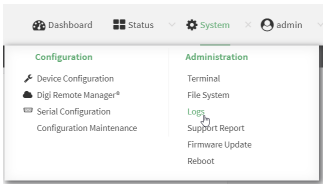
5. Type **exit** to exit the Admin CLI.

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

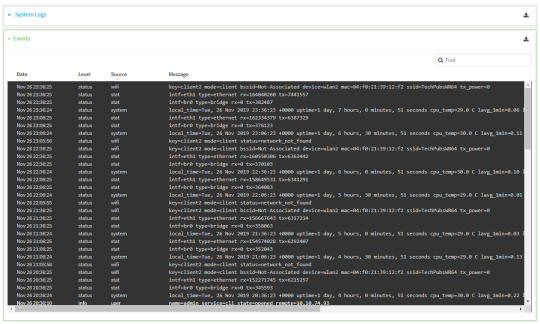
View Event Logs

WebUI

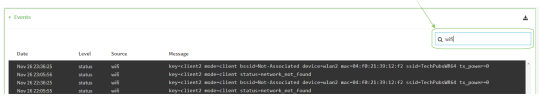
1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the main menu, click **System** > **Logs**.



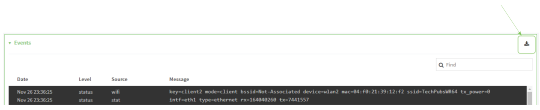
3. Click ▾ **System Logs** to collapse the system logs viewer, or scroll down to **Events**.
4. Click ▸ **Events** to expand the event viewer.



5. Limit the display in the event log by using the **Find** search tool.



6. Click 🡻 to download the event log.



Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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.

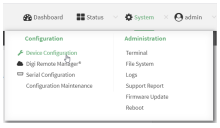
   Depending on your device configuration, you may be presented with an **Access selection menu**. Type **quit** to disconnect from the device.

Configure syslog servers

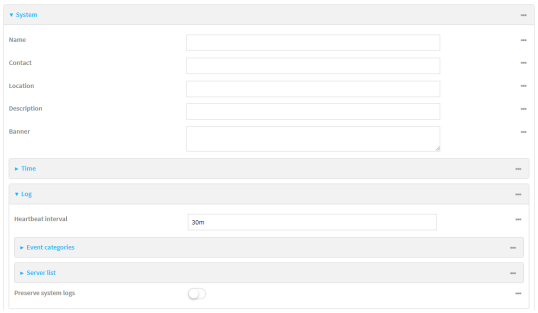
You can configure remote syslog servers for storing event and system logs.

WebUI

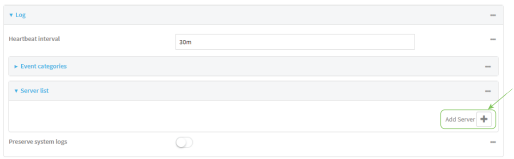
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



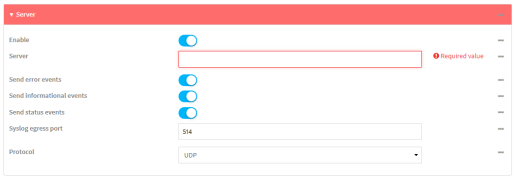
   The **Configuration** window is displayed.
3. Click **System** > **Log**.



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, click to 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 **UPD**. The default is **UPD**.

5. 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. (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

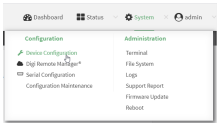
The default configuration for event and system logging is:

- 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.

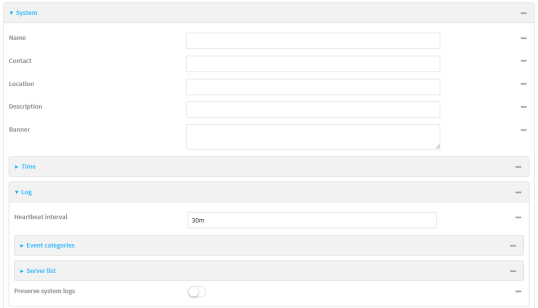
To change or disable the heartbeat interval, or to disable event categories, and to perform other log configuration:

WebUI

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 **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.
6. (Optional) See Configure syslog servers for information about configuring remote syslog servers to which log messages will be sent.
7. 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.
8. 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. (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
 modem                     Modem
 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
 wireless                  WiFi
 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                      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.

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 840
Example filters for capturing data traffic 849
Capture packets from the command line 850
Stop capturing packets 851
Show captured traffic data 851
Save captured data traffic to a file 853
Download captured data to your PC 854
Clear captured data 855

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.

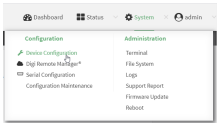
Additional configuration items

- 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.

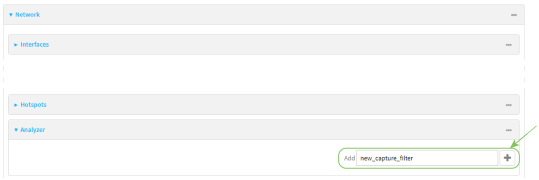
To configure a packet capture configuration:

WebUI

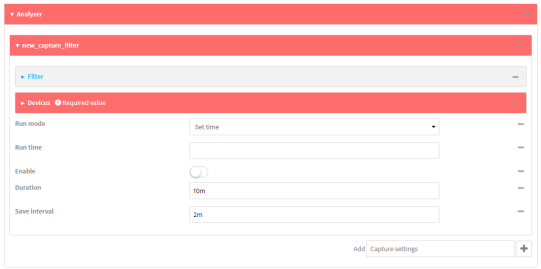
1. Log into the Connect EZ WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



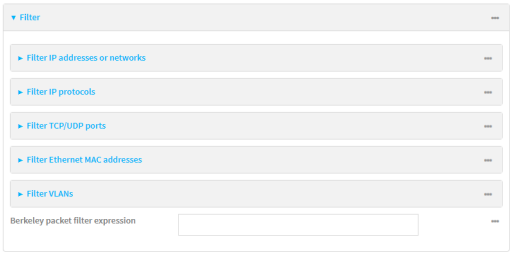
   The **Configuration** window is displayed.
3. Click **Network** > **Analyzer**.
4. For **Add Capture settings**, type a name for the capture filter and click **+**.



   The new capture filter configuration is displayed.

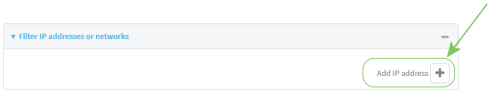


5. (Optional) Add a filter type:
   a. Click to expand **Filter**.



   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, is 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, is option is disabled, which means that the filter will capture packets that use this protocol.
      v. Click ✚ to add additional IP protocols 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 ingored.
      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, is 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 ingored.

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, is 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, is 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. 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. 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.
      - **either**: The filter will apply to packets when the IP address/network is either the source or the destination.

      iv. (Optional) Set the filter should ignore packets from this IP address/network:

```
(config network analyzer name filter address 0)> ignore true
(config network analyzer name filter address 0)>
```

      By default, is option is set to **false**, which means that the filter will capture packets from this IP address/network.

      v. Repeat these steps to add additional IP address filters.
   b. To create a filter that either captures or ignores packets that use a particular IP protocol:

i. Add a new IP protocol filter:

```
(config network analyzer name)> add filter protocol end
(config network analyzer name filter protocol 0)>
```

ii. Use the **?** to determine available protocols and the appropriate format:

```
(config network analyzer name filter protocol 0)> protocol ?

IP protocol to capture or ignore: IP protocol to capture or
ignore.
Format:
  ah
  esp
  gre
  icmp
  icmpv6
  igmp
  ospf
  other
  tcp
  udp
  vrrp
Current value:

(config network analyzer name filter protocol 0)>
```

iii. Set the protocol:

```
(config network analyzer name filter protocol 0)> protocol value
(config network analyzer name filter protocol 0)>
```

iv. If other is set for the protocol, set the number of the protocol:

```
(config network analyzer name filter protocol 0)> protocol_other
value
(config network analyzer name filter protocol 0)>
```

where *value* is an integer between 1 and 255 and represents the the number of the protocol.

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, is 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, is 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 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, is 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 be captured or ignored:

```
(config network analyzer name filter vlan 0)> vlan value
(config network analyzer name filter vlan 0)>
```

where *value* is number o 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, is 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**, **vrrp**, **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. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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 : Mar-03-2022 10:16:23.287682, 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               ...@.... ....

    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 anaylzer name ?

name: Name of the capture filter to use.
Format:
  test_capture
  capture_ping

> show anaylzer 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. Log into the Connect EZ command line as a user with Admin access.

   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 save filename filename name capture_filter
   >
   ```

   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
     ```

   - *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 save name ?

name: Name of the capture filter to use.
Format:
  test_capture
  capture_ping

> analyzer save name
```

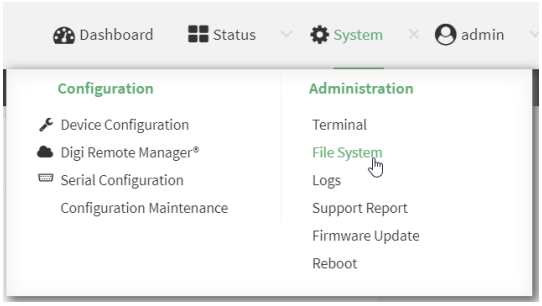
The file is stored in the **/etc/config/analyzer** directory. To transfer the file to your PC, see Download captured data to your PC.

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.

WebUI

1. Log into the Connect EZ WebUI as a user with Admin access.
2. On the menu, click **System**. Under **Administration**, click **File System**.



The **File System** page appears.



3. Highlight the **analyzer** directory and click ↱ to open the directory.
4. Select the saved analyzer report you want to download and click ⬇ (download).

Command line

1. Log into the Connect EZ command line as a user with Admin access.

   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. Log into the Connect EZ command line as a user with Admin access.

   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 **?**:

```
> anaylzer clear name ?

name: Name of the capture filter to use.
Format:
  test_capture
  capture_ping

> anaylzer 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 troubleshoot connectivity problems.

Ping to check internet connection

To check your internet connection:

1. Log into the Connect EZ command line as a user with Admin access.

   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)
- **pausemsecs**: 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) through the default gateway. The command output shows that **15** routing hops were required to reach the host:

1. Log into the Connect EZ command line as a user with Admin access.

   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**.

Command line interface

This chapter contains the following topics:

Access the command line interface 859
Log in to the command line interface 859
Exit the command line interface 860
Execute a command from the web interface 860
Display help for commands and parameters 861
Auto-complete commands and parameters 863
Available commands 864
Use the scp command 865
Display status and statistics using the show command 866
Device configuration using the command line interface 867
Execute configuration commands at the root Admin CLI prompt 868
Configuration mode 870
Command line reference 882

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 .
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

1. Log into the Connect EZ WebUI as a user with Admin access.
2. At the main menu, click **Terminal**. The device console appears.

```
Connect EZ login:
```

3. Log into the Connect EZ command line as a user with Admin access.

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.
 help         Show CLI editing and navigation commands.
 ls           List a directory.
 mkdir        Create a directory.
 modem        Modem commands.
 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.
 system       System commands.
 traceroute   Print the route packets trace to network host.
```

```
 update      Update firmware.

>
```

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
 ------------------------------------------------------------------------
--

 arp             Show ARP tables
 cloud           Show drm statistics
 config          Show config deltas.
 dhcp-lease      Show DHCP leases.
 dns             Show DNS servers.
 event           Show event list
 ipsec           Show IPsec statistics.
 location        Show loction information.
 log             Show syslog.
 manufacture     Show manufacturer information.
 modbus-gateway Show modbus gateway status & statistics.
 modem           Show modem statistics.
 network         Show network interface statistics.
 ntp             Show NTP information.
 openvpn         Show OpenVPN statistics.
 route           Show IP routing information.
 serial          Show serial statistics.
 surelink        Show Surelink statistics.
 system          Show system statistics.
 version         Show firmware version.
 wifi            Show Wi-Fi statistics.

 > 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
config	Used to view and modify the configuration. See Device configuration using the command line interface for more information about using the **config** command.
exit	Exits the CLI.
cp	Copies a file or directory.
help	Displays: ■ CLI editing and navigation commands, when executed from the root of the Admin CLI prompt. ■ Available commands, syntax diagram, and parameter information, when executed in conjunction with another command. See Display help for commands and parameters for information about the **help** command.
ls	Lists the contents of a directory.
mkdir	Creates a directory.
modem	Executes modem commands.
more	Displays the contents of a file.
mv	Moves a file or directory.
ping	Pings a remote host using Internet Control Message Protocol (ICMP) Echo Request messages.
reboot	Reboots the Connect EZ device.
rm	Removes a file.
scp	Uses the secure copy protocol (SCP) to transfer files between the Connect EZ device and a remote host. See Use the scp command for information about using the **scp** command.
show	Displays information about the device and the device's configuration. See Display status and statistics using the show command for more information about the show command.
system	Issues commands related to system functionality.
traceroute	Sends and tracks route packets to a destination host.
update	Updates the device firmware.

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-
22.2.9.85.bin local /etc/config/scripts to local
admin@192.168.4.1's password: adminpwd
Connect EZ-22.2.9.85.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 /var/log/
Saving support report to /var/log/support-report-0040D0133536-22-03-03-
10:16:23.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:D0:13:35:36-22-03-03-10:16:23.bin to remote
admin@192.168.4.1's password: adminpwd
support-report-0040D0133536-22-03-03-10:16:23.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$05$WlJQhquI7BgsytkpobKhaeLPtWraGANBcrlEaJX/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.otg03JZR6n9939XV6EYWUSP0tMAzO5W"
```

```
network interface lan ipv4 type "dhcp"
network interface lan zone "external"
network interface modem modem apn 0 apn "00000.000"
network interface modem modem apn_lock "true"
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 EZ-000065
  SKU                      : Connect EZ
  Hostname                 : Connect EZ
  MAC Address              : DF:DD:E2:AE:21:18

  Hardware Version         : 50001947-01 1P
  Firmware Version         : 22.2.9.85
  Alt. Firmware Version    : 22.2.9.85
  Alt. Firmware Build Date : Thurs, 03 March 2022 10:16:23
  Bootloader Version       : 19.7.23.0-15f936e0ed

  Current Time             : Thurs, 03 March 2022 10:16:23 +0000
  CPU                      : 1.4%
  Uptime                   : 6 days, 6 hours, 21 minutes, 57 seconds (541317s)
  Temperature              : 40C

>
```

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:

  1. At the **config** prompt, enter **service** to move to the **service** node:

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

  2. Enter **ssh** to move to the **ssh** node:

     ```
     (config service)> ssh
     (config service ssh)>
     ```

  3. 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
cancel	Discards unsaved configuration changes and exits configuration mode.
save	Saves configuration changes and exits configuration mode.
validate	Validates configuration changes.
revert	Reverts the configuration to default settings. See The revert command for more information.
show	Displays configuration settings.
add	Adds a named element, or an element in a list. See Manage elements in lists for information about using the **add**

Configuration actions	Description
	command with lists.
del	Deletes a named element, or an element in a list. See Manage elements in lists for information about using the **del** command with lists.
move	Moves elements in a list. See Manage elements in lists for information about using the **move** 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. 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. 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 883
analyzer save 884
analyzer start 884
analyzer stop 884
clear dhcp-lease ip-address 884
clear dhcp-lease mac 885
cp 885
help 885
ls 886
mkdir 887
modem at 887
modem at-interactive 887
modem firmware check 887
modem firmware list 887
modem firmware ota check 888
modem firmware ota list 888
modem firmware ota update 888
modem firmware update 888
modem pin change 889
modem pin disable 889
modem pin enable 889
modem pin status 890
modem pin unlock 890
modem puk status 890
modem puk unlock 890
modem reset 891
modem scan 891
modem sim-slot 891
monitoring 891
monitoring metrics upload 892
more 892
mv 892
ping 892
reboot 894
rm 895
scp 896
show analyzer 896
show arp 896
show cloud 896
show config 897
show dhcp-lease 897
show dns 897
show event 897
show hotspot 897
show ipsec 898
show l2tp lac 898
show l2tp lns 898
show l2tpeth 898
show location 899
show log 899
show manufacture 899
show modbus-gateway 899

show modem 899
show nemo 900
show network 900
show ntp 900
show openvpn client 900
show openvpn server 901
show route 901
show serial 901
show scripts 901
show surelink interface 902
show surelink ipsec 902
show surelink openvpn 902
show system 902
show usb 903
show version 903
show vrrp 903
show web-filter 903
show wifi ap 903
show wifi client 904
show wifi-scanner 904
show wifi-scanner blocklist 904
show wifi-scanner candidates 905
show wifi-scanner log 905
speedtest 905
ssh 905
system backup 906
system disable-cryptography 906
system duplicate-firmware 906
system factory-erase 906
system find-me 907
system firmware ota check 907
system firmware ota list 907
system firmware ota update 907
system firmware update 908
system power ignition off_delay 908
system restore 908
system script start 908
system script stop 908
system serial clear 909
system serial save 909
system serial show 909
system serial start 909
system serial stop 910
system support-report 910
system time set 910
system time sync 910
system time test 910
telnet 911
traceroute 911

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> <filename>
```

Parameters

name: Name of the capture filter to use.

filename: The filename to save captured traffic to. The file will be saved to the device's /etc/config/analyzer directory.

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.

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.

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 at

Send an AT command to the modem and display the response.

Syntax

```
modem at <cmd> [name STRING] [imei STRING]
```

Parameters

cmd: The AT command string.

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 at-interactive

Start an AT command session on the modem's AT serial port.

Syntax

```
modem at-interactive [name STRING] [imei STRING]
```

Parameters

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 firmware check

Inspect /opt/[MODEM_MODEL]/Custom_Firmware/ directory for new modem firmware file.

Syntax

```
modem firmware check [name STRING] [imei STRING]
```

Parameters

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 firmware list

List modem firmware files found in the /opt/[MODEM_MODEL]/ directory.

Syntax

```
modem firmware list [name STRING] [imei STRING]
```

Parameters

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 firmware ota check

Query the Digi firmware server for the latest remote modem firmware version.

Syntax

```
modem firmware ota check [name STRING] [imei STRING]
```

Parameters

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 firmware ota list

Query the Digi firmware server for a list of modem firmware versions.

Syntax

```
modem firmware ota list [name STRING] [imei STRING]
```

Parameters

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 firmware ota update

Perform FOTA (firmware-over-the-air) update. The modem will be updated to the latest modem firmware image unless a specific firmware version is specified.

Syntax

```
modem firmware ota update [name STRING] [imei STRING] [version STRING]
```

Parameters

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.

version: Firmware version name.

modem firmware update

Update modem firmware using local firmware file. The modem will be updated to the firmware specified in the /opt/[MODEM_MODEL]/Custom_Firmware/ directory unless a specific firmware version is specified.

Syntax

```
modem firmware update [name STRING] [imei STRING] [version STRING]
```

Parameters

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.

version: Firmware version name.

modem pin change

Change the SIM's PIN code.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin change <old-pin> <new-pin> [name STRING] [imei STRING]
```

Parameters

old-pin: The SIM's PIN code.

new-pin: The PIN code to change to.

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 pin disable

Disable the PIN lock on the SIM card that is active in the modem.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin disable <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

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 pin enable

Enable the PIN lock on the SIM card that is active in the modem. The SIM card will need to be unlocked before each use.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin enable <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

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 pin status

Print the PIN lock status and the number of PIN enable/disable/unlock attempts remaining. The SIM will be PUK locked when there are no remaining retries.

Syntax

```
modem pin status [name STRING] [imei STRING]
```

Parameters

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 pin unlock

Temporarily unlock the SIM card with a PIN code. Set the PIN field in the modem interface's configuration to unlock the SIM card automatically before use.

Warning: Attempting to use an incorrect PIN code may PUK lock the SIM.

Syntax

```
modem pin unlock <pin> [name STRING] [imei STRING]
```

Parameters

pin: The SIM's PIN code.

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 puk status

Print the PUK status and the number of PUK unlock attempts remaining.

Syntax

```
modem puk status [name STRING] [imei STRING]
```

Parameters

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 puk unlock

Unlock the SIM with a PUK code from the SIM provider.

Syntax

```
modem puk unlock <puk> <new-pin> [name STRING] [imei STRING]
```

Parameters

puk: The SIM's PUK code.

new-pin: The PIN code to change to.

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 reset

Reset the modem hardware (reboot it). This can be useful if the modem has stopped responding to the network or is behaving inconsistently.

Syntax

```
modem reset [name STRING] [imei STRING]
```

Parameters

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 scan

List of carriers present in the network.

Syntax

```
modem scan [name STRING] [imei STRING]
```

Parameters

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 sim-slot

Show or change the modem's active SIM slot. This applies only to modems with multiple SIM slots.

Syntax

```
modem sim-slot <slot> [name STRING] [imei STRING]
```

Parameters

slot: The SIM slot to change to.

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

Commands to clear the device's status or systems.

monitoring metrics

Device metrics commands.

uplaod

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.

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 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 modem

Show modem status & statistics.

Syntax

```
show modem [name STRING] [imei STRING] [verbose]
```

Parameters
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.
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 serial

Show serial status & statistics.

Syntax

```
show serial [port STRING]
```

Parameters

port: Display more details and config data for a specific serial port.

show scripts

Show scheduled system scripts.

Syntax

```
show scripts
```

Parameters

None

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 system

Show system status & statistics.

Syntax

```
show system [verbose]
```

Parameters

verbose: Display more information (disk usage, etc).

show usb

Show USB information.

Syntax

```
show usb
```

Parameters

None

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

show wifi ap

Display details for Wi-Fi access points.

Syntax

```
show wifi ap [name STRING] [all]
```

Parameters
name: Display more details for a specific Wi-Fi access point.
all: Display all Wi-Fi access points including disabled Wi-Fi access points.

show wifi client

Display details for Wi-Fi client mode connections.

Syntax

```
show wifi client [name STRING] [all]
```

Parameters
name: Display more details for a specific Wi-Fi client mode connection.
all: Display all Wi-Fi clients including disabled Wi-Fi client mode connections.

show wifi-scanner

Show Wi-Fi scanner information.

wifi-scanner blocklist
Show transmitters that have been evaluated as static and not included in the output log.

Parameters
None

wifi-scanner candidates
Show transmitters detected during the most recent observation period but not evaluated as static.

Parameters
None

wifi-scanner log
Show output log for the last update interval.

Parameters
None

show wifi-scanner blocklist

Show transmitters that have been evaluated as static and not included in the output log.

Syntax

```
show wifi-scanner blocklist
```

Parameters

None

show wifi-scanner candidates

Show transmitters detected during the most recent observation period but not evaluated as static.

Syntax

```
show wifi-scanner candidates
```

Parameters

None

show wifi-scanner log

Show output log for the last update interval.

Syntax

```
show wifi-scanner log
```

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 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 save

Saves the current serial log to a file.

Syntax

```
system serial save <port> <filename>
```

Parameters

port: Serial port.

filename: The filename to save the serial log. The file will be saved to the device's /etc/config/serial directory.

system serial show

Displays the serial log on the screen.

Syntax

```
system serial show <port>
```

Parameters

port: Serial port.

system serial start

Start logging data on a serial port.

Syntax

```
system serial start <port> [size INTEGER]
```

Parameters

port: Serial port.

size: Maximum size of serial log. (Default: 65536)

system serial stop

Start logging data on a serial port.

Syntax

```
system serial stop <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

Perform a NTP query to the configured server(s) and set the local time to the first server that responds.

Syntax

```
system time sync
```

Parameters

None

system time test

Test the configured NTP server(s) for connectivity. This test will not affect the device's current local date and time.

Syntax

```
system time test
```

Parameters

None

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] [pausemsecs 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)

pausemsecs: 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.

Safety warnings

English
Bulgarian--български
Croatian--Hrvatski
French--Français
Greek--Ελληνικά
Hungarian--Magyar
Italian--Italiano
Latvian--Latvietis
Lithuanian--Lietuvis
Polish--Polskie
Portuguese--Português
Slovak--Slovák
Slovenian--Esloveno
Spanish--Español

English



Operation of this equipment in a residential environment could cause radio interference.



For ambient temperatures above 60° C, this equipment must be installed in a Restricted Access Location only.

Connect EZ 4i only



Explosion Hazard. Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.



Explosion Hazard – Substitution of components may impair suitability for Class I, Division 2.



The extended temperature plug-in power supply (76002079 / 24000141) that is included with the EZ04-IAG4-EXT and EZ04-IA00-EXT kits is not certified for C1D2 and must not be used in C1D2-rated hazardous locations.

Bulgarian--български



Работата с това оборудване в жилищна среда може да причини радиосмущения.



За околни температури над 60 ° C, това оборудване трябва да се инсталира само на място с ограничен достъп.

Само Connect EZ 4i



Опасност от експлозия. Не изключвайте оборудването, освен ако токът не е бил изключен или ако е известно, че зоната не е опасна.



Опасност от експлозия. Заместването на компонентите може да наруши пригодността за клас I, раздел 2.



Включеното захранване с разширена температура (76002079 /24000141), което е включено в комплектите EZ04-IAG4-EXT и EZ04-IA00-EXT, не е сертифицирано за C1D2 и не трябва да се използва в опасни места с рейтинг C1D2.

Croatian--Hrvatski



Rad ove opreme u stambenom okruženju mogao bi prouzročiti radio smetnje.



Za okolne temperature iznad 60 ° C, ova oprema mora biti instalirana samo na mjestu s ograničenim pristupom.

Samo Connect EZ 4i



Opasnost od eksplozije. Odspojite opremu osim ako je napajanje isključeno ili ako je poznato da područje nije opasno.



Opasnost od eksplozije. Zamjena komponenata može naštetiti prikladnosti za klasu I, odjel 2.



Priključno napajanje s produženom temperaturom (76002079 /24000141) koje je uključeno u komplete EZ04-IAG4-EXT i EZ04-IA00-EXT nije certificirano za C1D2 i ne smije se koristiti na opasnim mjestima s ocjenom C1D2.

French--Français



L'utilisation de cet équipement dans un environnement résidentiel peut provoquer des interférences radio.



Pour des températures ambiantes supérieures à 60 °C, cet équipement doit être installé uniquement dans un emplacement à accès restreint.

Connect EZ 4i uniquement



Risque d'explosion. Ne débranchez pas l'équipement à moins que l'alimentation n'ait été coupée ou que la zone ne soit pas dangereuse.



Risque d'explosion. La substitution de composants peut nuire à l'aptitude à la classe I, division 2.



Le bloc d'alimentation enfichable à température étendue (76002079 / 24000141) qui est inclus avec les kits EZ04-IAG4-EXT et EZ04-IA00-EXT n'est pas certifié pour C1D2 et ne doit pas être utilisé dans des emplacements dangereux classés C1D2.

Greek--Ελληνικά



Η λειτουργία αυτού του εξοπλισμού σε οικιστικό περιβάλλον μπορεί να προκαλέσει παρεμβολές ραδιοφώνου.



Για θερμοκρασίες περιβάλλοντος άνω των 60 ° C, αυτός ο εξοπλισμός πρέπει να εγκατασταθεί μόνο σε θέση περιορισμένης πρόσβασης

Μόνο Connect EZ 4i



Κίνδυνος έκρηξης. Μην αποσυνδέετε τον εξοπλισμό εκτός εάν έχει απενεργοποιηθεί η τροφοδοσία ή είναι γνωστό ότι η περιοχή δεν είναι επικίνδυνη.



Κίνδυνος έκρηξης. Η αντικατάσταση των εξαρτημάτων ενδέχεται να επηρεάσει την καταλληλότητα για την κατηγορία I, Division 2.



Το πρόσθετο τροφοδοτικό εκτεταμένης θερμοκρασίας (76002079 /24000141) που περιλαμβάνεται στα κιτ EZ04-IAG4-EXT και EZ04-IA00-EXT δεν είναι πιστοποιημένο για C1D2 και δεν πρέπει να χρησιμοποιείται σε επικίνδυνες τοποθεσίες με βαθμολογία C1D2.

Hungarian--Magyar



A berendezés lakókörnyezetben történő működtetése rádiózavarokat okozhat.



60 ° C feletti környezeti hőmérséklet esetén ezt a berendezést csak korlátozott hozzáférésű helyre kell telepíteni.

Csak Connect EZ 4i



Robbanásveszély. Csak akkor válassza le a berendezést, ha kikapcsolták az áramellátást, vagy ha a területről ismert, hogy nem veszélyes.



Robbanásveszély. Az alkatrészek cseréje ronthatja az alkalmasságot az I. osztály 2. osztályához.



Az EZ04-IAG4-EXT és EZ04-IA00-EXT készletekhez mellékelt kiterjesztett hőmérsékletű, dugaszolható tápegység (76002079 /24000141) nem C1D2 tanúsítvánnyal rendelkezik, és nem használható C1D2 besorolású veszélyes helyeken.

Italian--Italiano



Il funzionamento di questa apparecchiatura in un ambiente residenziale potrebbe causare interferenze radio.



Per temperature ambiente superiori a 60° C, questa apparecchiatura deve essere installata solo in un luogo ad accesso limitato.

Solo Connect EZ 4i



Pericolo di esplosione. Non scollegare l'apparecchiatura a meno che l'alimentazione non sia stata disattivata o che l'area non sia nota come non pericolosa.



Pericolo di esplosione. La sostituzione dei componenti può compromettere l'idoneità per la Classe I, Divisione 2.



L'alimentatore plug-in per temperatura estesa (76002079 / 24000141) incluso con i kit EZ04-IAG4-EXT e EZ04-IA00-EXT non è certificato per C1D2 e non deve essere utilizzato in aree pericolose classificate C1D2.

Latvian--Latvietis



Šīs ierīces darbība dzīvojamā vidē var izraisīt radio traucējumus.



Ja apkārtējā temperatūra pārsniedz 60 ° C, šī iekārta jāuzstāda tikai ierobežotas piekļuves vietā.

Tikai Connect EZ 4i



Sprādziena briesmas. Neatvienojiet aprīkojumu, ja vien barošana nav izslēgta vai ir zināms, ka apkārtne nav bīstama.



Sprādziena briesmas. Komponentu aizstāšana var mazināt piemērotību I klases 2. nodaļai.



Paplašinātās temperatūras kontaktdakšas barošanas avots (76002079 /24000141), kas iekļauts komplektos EZ04-IAG4-EXT un EZ04-IA00-EXT, nav sertificēts C1D2, un to nedrīkst izmantot bīstamās vietās ar C1D2 novērtējumu.

Lithuanian--Lietuvis



Naudojant šią įrangą gyvenamojoje aplinkoje, gali kilti radijo trukdžių.



Esant aukštesnei nei 60 ° C aplinkos temperatūrai, ši įranga turi būti montuojama tik riboto patekimo vietoje.

Tik Connect EZ 4i



Sprogimo pavojus. Neatjunkite įrangos, nebent išjungtas maitinimas arba žinoma, kad vietovė nėra pavojinga.



Sprogimo pavojus. Pakeitus komponentus, gali sumažėti tinkamumas I klasės 2 skyriui.



Išplėstinės temperatūros kištukinis maitinimo šaltinis (76002079 /24000141), kuris yra komplekte su EZ04-IAG4-EXT ir EZ04-IA00-EXT, nėra sertifikuotas C1D2 ir negali būti naudojamas pavojingose vietose, kuriose yra C1D2 įvertinimas.

Polish--Polskie



Praca tego sprzętu w środowisku mieszkalnym może powodować zakłócenia radiowe.



W przypadku temperatur otoczenia powyżej 60°C urządzenie to należy instalować wyłącznie w miejscach o ograniczonym dostępie.

Tylko Connect EZ 4i



Zagrożenie wybuchem. Nie odłączaj sprzętu, chyba że zostało wyłączone zasilanie lub obszar nie jest niebezpieczny.



Zagrożenie wybuchem. Zamiana części może pogorszyć przydatność do klasy I, dział 2.



Zasilacz wtykowy o zwiększonej temperaturze (76002079 / 24000141), który jest dołączony do zestawów EZ04-IAG4-EXT i EZ04-IA00-EXT, nie jest certyfikowany dla C1D2 i nie może być używany w lokalizacjach niebezpiecznych C1D2.

Portuguese--Português



A operação deste equipamento em um ambiente residencial pode causar interferência de rádio.



Para temperaturas ambientes acima de 60 ° C, este equipamento deve ser instalado apenas em locais de acesso restrito.

Connect EZ 4i apenas



Risco de explosão. Não desconecte o equipamento a menos que a alimentação tenha sido desligada ou a área seja conhecida como não perigosa.



Risco de explosão. A substituição de componentes pode prejudicar a adequação para Classe I, Divisão 2.



A fonte de alimentação plug-in de temperatura estendida (76002079/24000141) incluída nos kits EZ04-IAG4-EXT e EZ04-IA00-EXT não é certificada para C1D2 e não deve ser usada em locais perigosos com classificação C1D2.

Slovak--Slovák



Prevádzka tohto zariadenia v obytnom prostredí by mohla spôsobiť rádiové rušenie.



Pri teplotách okolia nad 60 ° C musí byť toto zariadenie inštalované iba na mieste s obmedzeným prístupom.

Iba Connect EZ 4i



Nebezpečenstvo výbuchu. Neodpájajte zariadenie, pokiaľ nebolo vypnuté napájanie alebo nie je známe, že oblasť nie je nebezpečná.



Nebezpečenstvo výbuchu. Nahradenie komponentov môže zhoršiť vhodnosť pre triedu I, divíziu 2.



Zásuvný napájací zdroj s predĺženou teplotou (76002079 /24000141), ktorý je súčasťou súprav EZ04-IAG4-EXT a EZ04-IA00-EXT, nie je certifikovaný pre C1D2 a nesmie sa používať v nebezpečných oblastiach s klasifikáciou C1D2.

Slovenian--Esloveno



Delovanje te opreme v stanovanjskem okolju lahko povzroči radijske motnje.



Pri temperaturah okolice nad 60 ° C mora biti ta oprema nameščena samo na lokaciji z omejenim dostopom.

Solo Connect EZ 4i only



Nevarnost eksplozije. Opreme ne odklapljajte, razen če je bilo napajanje izključeno ali če je znano, da območje ni nevarno.



Nevarnost eksplozije. Nadomestitev komponent lahko poslabša ustreznost razreda I, oddelek 2.



Vtični napajalnik s podaljšano temperaturo (76002079 /24000141), ki je vključen v komplete EZ04-IAG4-EXT in EZ04-IA00-EXT, ni certificiran za C1D2 in se ga ne sme uporabljati na nevarnih lokacijah z oceno C1D2.

Spanish--Español



El funcionamiento de este equipo en un entorno residencial puede provocar interferencias de radio.



Para temperaturas ambiente superiores a 60 ° C, este equipo debe instalarse únicamente en una ubicación de acceso restringido.

Solo Connect EZ 4i



Peligro de explosión. La sustitución de componentes puede afectar la idoneidad para la Clase I, División 2.



Peligro de explosión. La sustitución de componentes puede afectar la idoneidad para la Clase I, División 2.



La fuente de alimentación enchufable de temperatura extendida (76002079/24000141) que se incluye con los kits EZ04-IAG4-EXT y EZ04-IA00-EXT no está certificada para C1D2 y no debe usarse en ubicaciones peligrosas clasificadas como C1D2.

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.

Important note

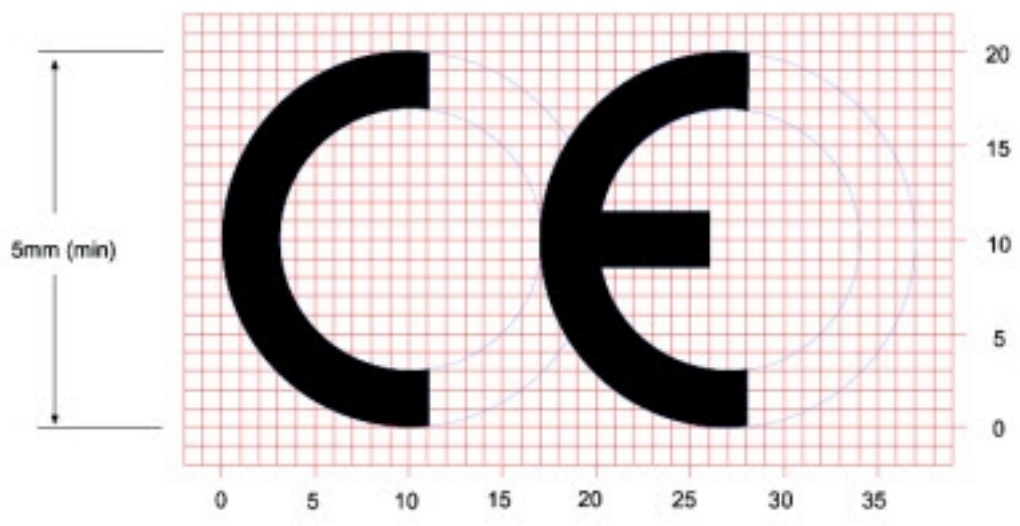
Digi customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. Refer to the radio regulatory agency in the desired countries of operation for more information.

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.

Innovation, Science, and Economic Development Canada (IC) certifications

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

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

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.

Safety statements for Connect EZ 4i only

CAUTION! Hot surface!
To avoid burns when handling the device surface, wait at least one half hour after switching off the device before handling the surface.

PRUDENCE! Surface chaude!
Pour éviter les brûlures lors de la manipulation de la surface de l'appareil, attendez au moins une demi-heure après avoir éteint l'appareil avant de manipuler la surface.

Special safety notes for wireless routers

Digi International products are designed to the highest standards of safety and international standards compliance for the markets in which they are sold. However, cellular-based products contain radio devices which require specific consideration. Take the time to read and understand the following guidance. Digi International assumes no liability for an end user's failure to comply with these precautions.



Wireless routers incorporate a wireless radio module. Users should ensure that the antenna(s) is (are) positioned at least 1 meter away from themselves and other persons in normal operation.
When in a hospital or other health care facility, observe the restrictions on the use of mobile phones. Do not use the router in areas where guidelines posted in sensitive areas instruct users to switch off mobile phones. Medical equipment may be sensitive to RF energy.
The operation of cardiac pacemakers, other implanted medical equipment and hearing aids can be affected by interference from cellular terminals such as the wireless routers when places close to the device. If in doubt about potential danger, contact the physician or the manufacturer of the device to verify that the equipment is properly shielded. Pacemaker patients are advised to keep the wireless router away from the pacemaker while it is on.



Wireless routers must NOT be operated on aircraft. The operation of wireless appliances in an aircraft is forbidden to prevent interference with communications systems. Failure to observe these instructions may lead to the suspension or denial of cellular services to the offender, legal action, or both.



As with any electrical equipment, do not operate the router in the presence of flammable gases, fumes or potentially explosive atmospheres. Do not use radio devices anywhere that blasting operations occur.



Wireless routers receive and transmit radio frequency energy when power is on. Interference can occur when using the router close to TV sets, radios, computers or inadequately shielded equipment. Follow any special regulations and always power off your router wherever forbidden or when it may cause interference or danger.



SOS IMPORTANT! Wireless routers operate using radio signals and cellular networks cannot be guaranteed to connect in all possible conditions. Therefore, never rely solely upon any wireless device for life critical communications.

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/HF1515VU