MULTITECH®
CREATE • CONNECT • COMMUNICATE

mPower™
EDGE INTELLIGENCE

Programmable embedded software provides enhanced security and enables task execution at the edge for reduced latency and cost optimization.

Meet mPower™ Edge Intelligence,

a new embedded software offering from MultiTech. This innovative new firmware builds on the popular MultiTech application enablement platform, to deliver programmability, network flexibility, enhanced security and manageability for scalable Industrial Internet of Things (IIoT) solutions.

mPower represents the unification and evolution of well-established MultiTech smart router and gateway firmware platforms. In addition to ongoing support of the current feature-sets, gateway customers can enjoy the additional security features currently available on the MultiConnect® rCell 100 Series.

mPower Edge Intelligence simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud data management and analytics, while also providing the programmability and processing capability to execute critical tasks at the edge of the network to reduce latency; control network and cloud services costs, and ensure core functionality – even in instances when network connectivity may not be available.

In response to evolving customer security requirements, mPower Edge Intelligence incorporates a host of new security features including signed firmware validation, enhanced firewall and VPN settings, secure authentication and more.

mPower BENEFITS

- Enhanced security and routing
- Application hosting for real-time response
- Unified user interface across platforms
- Application sharing between platforms
- Synchronous updates across all “intelligent” platforms

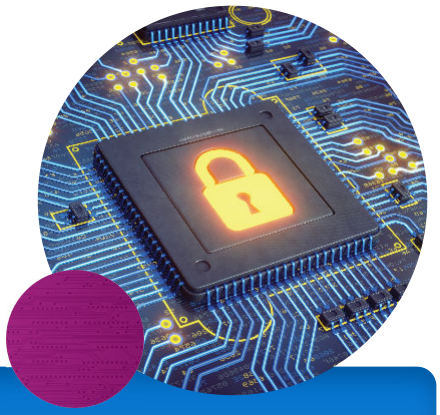
mPower FEATURES

- Secure access
- Secure connectivity
- RADIUS Support
- Remote management
- Enhanced hardware control and debugging

mPower™
EDGE INTELLIGENCE

Industrial-Grade Security

mPower™ Edge Intelligence uses IPSec industry standard data encryption to provide high-performance, secure LAN-to-LAN VPN connections with 3DES or AES encryption using IKE and PSK key management for up to five concurrent VPN tunnels. Additionally a private, secure digital signature with integrity check update technique is now available, minimizing file damage, tampering or loading of invalid firmware. MultiTech signs and distributes firmware updates through a secure standard firmware distribution process and verifies the firmware signature before installation of the firmware for maximum device integrity.



SECURITY

SECURE ACCESS | SECURE CONNECTIVITY | RADIUS SUPPORT | NOTIFICATIONS | DEBUGGING | SERIAL PORT PROTOCOLS | REMOTE MANAGEMENT

HARDWARE CONTROL
Cellular – LoRa – Ethernet – Wi-Fi – BT – GPS/GNSS

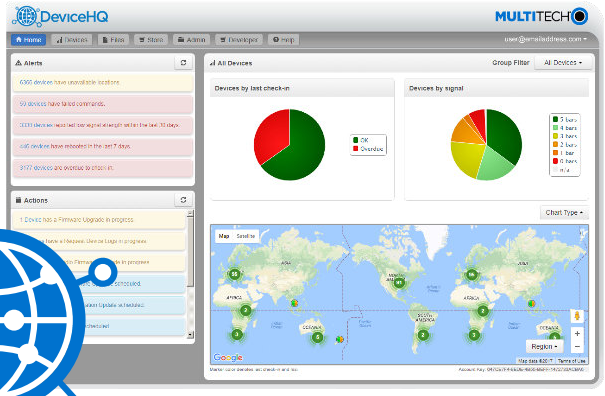
MultiConnect rCell
Cellular Router

Conduit IoT Programmable Gateway
Conduit IP67 Base Station

Conduit AP
Access Point

MultiTech DeviceHQ®

DeviceHQ is a cloud-based tool set for managing the latest generation of MultiTech devices. Its device management functionality enables remote monitoring, upgrades and configuration of entire device populations – whether one or 1 million. DeviceHQ takes remote device management and maintenance to a new level, by providing an application marketplace, allowing users to browse applications, or build their own, then easily deploy them to and customize them for remote devices from anywhere.



DeviceHQ®

mPower™ Enabled MultiTech Devices

MultiConnect® rCell 100 Series Cellular Router

The MultiConnect rCell 100 Series of cellular routers are a part of MultiTech's comprehensive portfolio of cellular connectivity products optimized for M2M (machine-to-machine) communications. With the industry's most cost effective approach to remote device management and shared design approach across multiple cellular technologies, it provides the lowest total cost of ownership to our customers. The MultiConnect rCell 100 Series of cellular routers also offer a long, stable lifecycle, an important consideration for M2M solutions.

MultiConnect® Conduit® Gateway

MultiTech Conduit gateway, ideal for indoor industrial use, is the industry's most configurable, manageable, and scalable communications gateway for industrial IoT applications. The Conduit features two accessory card slots that enable users to plug in MultiConnect® mCard™ accessory cards supporting their preferred wired or wireless interfaces to connect a wide range of assets to the gateway. Available options include a LoRaWAN® mCard capable of supporting thousands of MultiConnect® mDot™ or xDot® long range RF modules connected to remote sensors or actuators.

MultiConnect® Conduit® IP67 Base Station

MultiTech Conduit IP67 Base Station is a ruggedized IoT gateway solution specifically designed for outdoor public or private LoRa® network deployments. This highly scalable and IP67-certified solution is capable of resisting the harshest environmental factors including moisture, dust, wind, rain, snow and heat, supporting LoRaWAN applications in virtually any environment.

MultiConnect® Conduit® AP Access Point

MultiTech Conduit AP Access Point for LoRa technology is a cost-optimized gateway capable of connecting thousands of IoT assets to the cloud utilizing the LoRaWAN protocol. The Access Point is ideal for extending LoRa network coverage in difficult-to-reach areas such as subterranean spaces, and for increased in-building penetration where coverage is weak or not cost-effective.

SPECIFICATIONS	Conduit AP Access Point Conduit IoT Programmable Gateway & Conduit IP67 Base Station MultiConnect rCell Cellular Router			
OPERATING SYSTEM SUPPORT				
Linux Kernel 4.9	Access to hundreds of resolved CVE (Common Vulnerabilities and Exposures)	•	•	•
Yocto 2.2	Open-source collaboration software	•	•	•
IBM Node RED & node.js	Flow-based development tool for visual programming		•	•
Language Support	Python, C/C++, Javascript		•	•
Package upgrade support	Java, Perl, Ruby, Mono C#		•	•
Packages	SQLite (Database), Lighttpd (Web Server), BusyBox (Core Utilities)		•	•
SECURITY				
Linux Kernel 4.9	Access to hundreds of resolved CVE (Common Vulnerabilities and Exposures)	•	•	•
VPN	Up to 5 concurrent tunnels IPSec IKEv1,v2 Open VPN Cipher suite: DHGroup 14 Configurable encryption, Configurable hash, Configurable TLS: 1.0, 1.1, 1.2 Encapsulation: ESP Encryption Methods: 3DES, AES-128, AES-192, AES-256, Authentication: MD5, SHA-1, SHA-2, SHA2-256, SHA2-384, SHA2-512, Key Group: DH2 (1024-bit), DH5 (1536-bit), DH14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit)	•	•	•
MAC Filtering	Accept, reject, drop or log packets based on MAC address	•	•	•
Firewall Rules	SPI Firewall with configurable DNAT, NAT-T, SNAT	•	•	•
DHCP	IPv4 Mask settings allow the connected device to obtain LAN settings automatically or the LAN settings can be configured manually	•	•	•
x.509 Certificates	Support generation and/or import of multiple CA certificates through use of SHA-256. User can add and delete user's root certificates in addition to the certificates from the /etc/ssl by application.	•	•	•
PAP/CHAP	Authentication protocols for secure PPP connections	•	•	•
SMS Security Features	Security requirements for receiving SMS commands from remote users	•	•	•
SECURE ACCESS	Secure main entry to the asset			
Password Strength Controls	Secure passwords required for all user types	•	•	•
User Interface Inactivity Timeout	Automatically log out a user if connection remains dormant for an identified period of time	•	•	•
Administrative Controls	Tools to help restore the configuration of the device	•	•	•
User Accounts	Three types of user accounts: administrator, engineer, and monitor	•	•	•
Firewall Rule Settings	A set of rules that determine how incoming and outgoing packets are handled	•	•	•
Access Configuration	Determines how the device can be accessed and configures the security features that decrease susceptibility to malicious activity	•	•	•
Signed Firmware Upgrade	Signed firmware validation when upgrading firmware	•	•	•
Save and Restore Configuration	Restore the configuration of the device from a PC file	•	•	•
SECURE CONNECTIVITY	Encryption to protect the integrity of data transfer between an asset and a remote server			
OpenVPN	Server and client. Version 2.4.6 VPN: IPSec, IKEv1,v2 Cipher suite: DHGroup 14 Configurable Encryption: AES256, DES, 3DES Configurable Hash: SHA-1, 2, MD5, RSA Configurable TLS: 1.0, 1.1, 1.2 Encapsulation: ESP	•	•	•
GRE Tunnels	Allows the use of a public network to convey data on behalf of two remote private networks	•	•	•
Network-to-Network VPN	Site-to-Site VPNs via Internet Protocol Security (IPsec) tunnels Encryption Methods supported: 3DES, AES-128, AES-192, AES-256, and Advanced, Default Hash Algorithms: SHA-1, SHA-2, and MD5 Default DH Group Algorithms: DH2 (1024-bit), DH5 (1536-bit), DH14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit) and DH24 (2048-bit)	•	•	•
Ciphersuite	SSL/TSL communication using TLS 1.2	•	•	•
RADIUS Support	Secure entry to a network of assets for better monitoring and control			
Secure entry to a network of assets for better monitoring and control		•	•	•
RADIUS protocol supports authentication, user session accounting, and authorization of users to the device.		•	•	•
Notifications	Utilities to help troubleshoot and solve technical problems			
Time-stamped notifications sent to individuals or groups via E-mail message, SMS message, and/or SNMP trap		•	•	•
Sent messages and message status can be managed by Mail Log, Mail Queue, or Notifications Sent		•	•	•

SPECIFICATIONS (continued)

		Conduit AP Access Point	Conduit IoT Programmable Gateway & Conduit IP67 Base Station	MultiConnect rCell Cellular Router
DEBUGGING				
Cellular AT Commands	Communicate directly with device cellular radio using AT commands	•	•	•
Automatic Reboot Timer	Configure device to automatically reboot	•	•	•
Telnet Radio Access	Direct communication with cellular radio	•	•	•
Remote Syslog Server	Stream syslog data and configure logging levels	•	•	•
Statistics Server	Cellular and Ethernet statistics can be saved periodically	•	•	•
Ping Options	Device can ping an IP address to ensure it is operational	•	•	•
Reset Options	Reset hardware modules to assist in identifying problems	•	•	•
SNMP Support	V1,V2,V3 SNMPv3 and authentication protocols MD5 and SHA1 as well as encryption protocols DES and AES-128. configurable multiple SNMP trap servers and SNMP server configurations enhanced SNMP server Web UI allows configuring SNMPv3 security settings for SNMP configurations and SNMP trap servers	•	•	•
DDNS (Dynamic Domain Naming System)	Automatically updates DNS	•	•	•
DHCP (Dynamic domain Naming System)	Supports fixed and dynamic IP addressing	•	•	•
DNS (Dynamic Domain Server)	Manage traffic for the local area network (LAN) and behave as a local DNS forwarder	•	•	•
DHCP (Dynamic Host Configuration Protocol)	Function as a DHCP server and supply network configuration information	•	•	•
SMS Configuration	Troubleshooting commands to store logs to DeviceHQ Remote reboot over SMS Commands to retrieve connection status, radio stats, Ethernet link status APN modification over SMS	•	•	•
Usage Policy	Default policy stating that system is for the use of authorized users only	•	•	•
SERIAL PORT PROTOCOLS	Configurable serial terminal			
The serial terminal connected to the device RS-232 connection can be configured using TCP, UDP, or SSL/TLS server protocol		•	•	•
Device can be configured to use Modbus protocol to communicate with serial devices		•	•	•
REMOTE MANAGEMENT	DeviceHQ platform provides remote access to devices			
Signed Firmware Authentication / Integrity Check	Private, secure, digital signature technique to enable transferring the device firmware safely. The technique will defeat attempts to load invalid firmware files or files that have been subjected to damage or tampering. MultiTech signs and distributes the firmware through a secure, standard firmware distribution process, and verifies the firmware signature before it installs the firmware files to ensure integrity.	•	•	•
Simple Network Management Protocol (SNMP) Support	Used to collect information from, and configure network devices on the IP network.	•	•	•
DeviceHQ	Remote device management platform provides device status and information in a clear graphical format. Manage, monitor, group, configure and upgrade devices remotely	•	•	•
Customizable Web User Interface	User interface can be customized by the customer to include the customer name, look-and-feel, logo, and supporting information (address, phone numbers, website)	•	•	•
HARDWARE CONTROLS (VARIES WITH MODELS)				
Cellular WAN	Support for the latest 4G-LTE networks and legacy 2G and 3G networks	•	•	•
LoRa Networks	Support for regional channel plans and local LoRa requirements		•	•
Ethernet	WAN Connection: Primary or backup connection for data backhaul LAN Connection: Connect to computer, switch or hub	•	•	•
Wi-Fi	802.11 b\g\n access point (up to five client connections) or client mode	•	•	•
BT	A transparent data pipe from a Bluetooth device to a remote server	•	•	•
GPS/GNSS	Global positioning and LoRa-packet time-stamping	•	•	•
Programmability	Uses an open Linux development environment to enable connectivity		•	•

Technology that Transforms

MultiTech is committed to supporting the growth and development of the Internet of Things (IoT) in order to create new customer experiences and unparalleled economic value, while improving quality of life for countless people throughout the world. By providing products and services to connect "things" to the Internet, MultiTech delivers deeper understanding to businesses, governments, organizations and individuals, which will in turn transform the way we live and work.

MultiTech offers a variety of embedded devices as well as modems, routers and gateways that address connectivity across a variety of technologies including analog, Ethernet, cellular, PAN and LPWA. Our diverse, award-winning portfolio reflects the constantly evolving world of the Internet of Things with a product and technology combination to suit virtually any use case.

Our products are designed to ensure the quickest route to market based on your needs, programming capabilities, preferred use of resources and business focus, in order to deliver a faster return on investment and lower total cost of ownership.

Support

MultiTech customers consistently rate us ahead of the competition for the quality of our technical support. That's because we're committed to providing you the information you need to install and maintain your product in a timely, concise and easy-to-understand format. Our commitment to quality and service excellence means you can count on MultiTech products and people to address your needs, while our history of innovation ensures you can stay ahead of the latest technology with a partner who will be there for the life of your solution.

"Simply, Thank You! Thank you for your team... They should all be congratulated for their professionalism and service. They know how to take care of a customer."
Steven,
Founder and CCO

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112 U.S.A.
Tel: 763-785-3500
Toll-Free: 800-328-9717
Email: sales@multitech.com
www.multitech.com

EMEA Headquarters

Multi-Tech Systems (EMEA)
Strata House
264-270 Bath Road
Harlington UB3 5JJ U.K.
Tel: +(44) 118 959 7774
Email: sales@multitech.co.uk
www.multitech.co.uk

MULTITECH®
CREATE • CONNECT • COMMUNICATE

CONNECT WITH MULTITECH

Trademarks and Registered Trademarks: MultiTech and the MultiTech logo, MultiConnect, Conduit, mPower, DeviceHQ: Multi-Tech Systems, Inc.
All other products and technologies are the trademarks or registered trademarks of their respective holders. Features and specifications are subject to change without notice.

2019-06 • 86002219 •

© 2019 Multi-Tech Systems, Inc. All rights reserved.