Product Change Notification
Software Release Notice

MultiConnect® rCell 100 Series Cellular Routers

mPower™ Edge Intelligence
New Firmware Available

Date: July 2, 2019

I. Product Change Notification Number
PCN # 070219-00

II. Type of Change
This is a software upgrade release for MultiConnect® rCell 100 series cellular routers (MTR-xx models) covering 4G and 3G models that further enhances security and flexibility.

III. mPower™ Edge Intelligence
mPower™ Edge Intelligence represents the unification and evolution of well-established MultiTech smart router and gateway firmware platforms. This new embedded software offering, builds on its popular application enablement platform, to deliver programmability, network flexibility, enhanced security and manageability for scalable Industrial Internet of Things (IIoT) solutions.

In response to evolving customer security requirements, mPower Edge Intelligence incorporates a host of new security features including 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.

mPower Edge Intelligence also simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud data management and analytics, while also providing the 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.

IV. Models Covered

Base model number	Description
MTR-LAT1-XX-XX	4G LTE (AT&T, T-Mobile, Rogers) – United States/Canada
MTR-LVW2-XX-XX	4G LTE (Verizon) – United States
MTR-LEU1-XX-XX	4G LTE – Europe
MTR-H5-XX-XX	3G HSPA+ - Global
MTR-H6-XX-XX	3G HSPA - Europe

V. Minimum System Requirements

To install the upgrade, your device must have software (SW) version 3.4.5 or higher. If lower, please, install 3.4.5 before loading version 5.0.0

VI. Current and New Software (SW) Versions

Current MTR-xx SW: 4.1.0
New MTR-xx SW: 5.0.0
See release notes here: ftp://ftp.multitech.com/wireless/mtr/mtr-release-notes_5.0.0.txt

VII. Features in SW Release 5.0.0

		MTR-XX
Operating System Support		
Linux Kernel 4.9	Access to hundreds of resolved CVE (Common Vulnerabilities and Exposures)	•
Yocto 2.2	Open-source collaboration software	•
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:	•

		MTR-XX
	• 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**	
Remote authentication using Remote Authentication Dial-In User Service (RADIUS).		•
RADIUS protocol supports authentication, user session accounting, and authorization of users to the device.		•
Notifications	**Capability of sending time-stamped alerts on a number of measurable device metrics**	
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		•
Debugging	**Utilities to help troubleshoot and solve technical problems**	
Cellular AT Commands	Communicate directly with device cellular radio using AT commands	•
Automatic Reboot Timer	Configure device to automatically reboot	•
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	**Device HQ 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.	•

		MTR-XX
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 Model)		
Cellular WAN	Support for the latest 4G-LTE networks and legacy 3G networks	•
Ethernet	WAN Connection: Primary or backup connection for data backhaul LAN Connection: Connect to computer, switch or hub	•
WiFi	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	•
Programmability	Uses an open Linux development environment to enable connectivity	*

**Beta feature - under development*

VIII. Installation Instructions

The signed firmware and unsigned firmware are separate files. (Note: to install the unsigned software, signature verification must first be disabled in the Web UI).

NOTE:
To upgrade using the MTR-xx Web UI to MTR 5.0.0, you must be running at least MTR-xx 3.4.5 firmware.
To upgrade from a previous legacy firmware, upgrading to MTR-xx 3.4.5 is necessary before upgrading to MTR-xx 5.0.0

Upgrading to 5.0.0.

Note: Backup your configuration before performing this upgrade. If the firmware upgrade fails, or it does not show the login page again, wait an additional 10 minutes. Power the MTR, off and on and browse to the IP address to check the version. If the version does not show the latest, then the upgrade was not successful. Try to perform the firmware upgrade again by repeating all the steps.

1) Save the firmware binary file to a directory on your workstation.
2) Using the workstation browser, enter the IP address of the MTR (i.e. http://192.168.2.1).
3) Login with admin user and enter the admin password.
4) Click "Administration" tab on left side menu bar.
5) Click "Save/Restore".
6) Click "save Configuration to File" to save a backup file. A popup window will appear.
7) Select "save File" and click "OK" button.
8) Now click "Firmware Upgrade" tab on left side menu.
9) This version of firmware has a Firmware validation option.
Review the Firmware Upgrade Help for further information.

10) Click the Browse button and select the latest version of BIN file:
Use the respective -signed upgrade file based on the Firmware validation option setting.

- (for non-LTE): rcell-mtr-upgrade_5.0.0.bin
- (for non-LTE): rcell-mtr-upgrade_5.0.0-signed.bin
- (for LTE): rcell-mtrv1-upgrade_5.0.0.bin
- (for LTE): rcell-mtrv1-upgrade_5.0.0-signed.bin

11) Click the "start Upgrade" button, confirm the 10 minute "OK" button.
12) Wait for the unit to upgrade and reboot automatically.
13) Again, browse to the IP address, login and verify the Home Page indicates the correct version, 5.0.0.

IX. About MultiConnect® rCell 100 Series Cellular Routers

The MultiConnect rCell is a compact, intelligent and fully-featured communications platform that provides cellular capabilities for fixed and mobile applications. It is intended for use in settings such as:

- Remotely monitoring solar micro-inverters, tanks, pipelines, meters, pumps and valves in any energy, utility, or industrial application
- The MultiConnect rCell 100 Series family has also been successfully deployed by professionals in emergency services, vending, remote patient monitoring, renewable energy systems, process automation and mobile applications (truck, rail, and boat).

The MultiConnect rCell 100 Series (MTR-xx) of cellular routers are a part of the MultiTech comprehensive portfolio of cellular connectivity products optimized for M2M (machine-to-machine). The MultiConnect rCell comes with no cost access to DeviceHQ® which is MultiTech's cloud platform service to monitor and manage deployed MultiConnect rCell cellular routers in the field.

X. Additional Information

If you have any questions regarding this Product Change Notification, please contact your MultiTech sales representative:

World Headquarters – U.S.
+(763) 785-3500 | sales@multitech.com

EMEA Headquarters – UK:
+(44) 118 959 7774 | sales@multitech.co.uk