Product Change Notification
Software Release Notice

MultiConnect® rCell 100 Series Cellular Routers

Date: May 4, 2017

I. Product Change Notification Number
PCN #050417-00

II. Type of Change
This is a software upgrade release for MultiConnect rCell 100 series cellular routers (MTR-xx models) covering 4G, 3G and 2G models that further enhances security and alerts.

III. 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-H6-XX-XX	3G HSPA+ - Europe
MTR-H5-XX-XX	3G HSPA+ - Global
MTR-EV3-XX-XX	3G EV-DO – (Verizon, Sprint, Aeris) – United States
MTR-G3-XX-XX	2G GPRS – Europe
MTR-C2-XX-XX	2G 1xRTT – (Verizon, Sprint, Aeris) – United States

IV. 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 3.6.0

V. Current and New Software (SW) Versions
Current MTR-xx SW: 3.5.6
New MTR-xx SW: 3.6.0

See release notes here: ftp://ftp.multitech.com/wireless/mtr/mtr-release-notes_3.6.0.txt

VI. New Features in SW Release 3.6.0

a) SNMP Notifications or "Traps"

SNMP traps are event driven alerts which will enhance the MTR-xx monitoring features. When a certain event is triggered, customers will have the option to receive notifications through email, SMS, Syslog alert or SNMP traps.

SNMP (Simple Network Management Protocol) is a standard protocol that network devices use to control each other and report critical information. The main advantage of this protocol is that it is supported by many devices, enabling them to operate together. While there are more sophisticated methods available for monitoring and managing network performance, SNMP survives partly because it remains the standard option supported in many pieces of specialized networking hardware.

The most frequently used SNMP messages are traps. These are sent to the manager by an agent when an issue needs to be reported. SNMP traps are quite unique when compared to other message types, since they are the only method that can be directly initiated by a SNMP agent. Other types of messages are either initiated by the SNMP manager or sent as a result of the manager's request. This ability makes SNMP traps indispensable in most networks. It is the most convenient way for an SNMP agent to inform the manager that something wrong is going on.

SNMP traps can be configured to notify a LAN connected SNMP management server when the MTR-xx changes status. (RSSI, thresholds, network state, network channel, IP address, cell info, etc.)

b) Open VPN (Server and Client)

Open VPN is one of the most popular and well-received implementations of VPN technology. It is open source based and uses a customized protocol to achieve secure connectivity using SSL/TLS (Secure Socket Layer) in the process for security. Many VPN providers offer OpenVPN as a preferred protocol for security and reliability reasons.

Strong Security

With security features such as peer authentication using pre-shared keys, certificates and other usual forms of authentication, strong encryption standards using the OpenSSL Library, and HMAC packet authentication, OpenVPN are ideal for customers who want to keep their networks safe and secure from prying eyes and hackers. Also, OpenVPN runs in the user space without root privileges, making it safe and robust.

High Reliability

When OpenVPN goes down, the network is brought to a pause to allow for repair or reconfiguration, thereby ensuring that no data loss or corruption or miscommunication happens. This also acts as an additional layer of security.

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

c) SMS Enhancements

The SMS enhancements further build on those implemented in SW version 3.4.x.

The purpose for SMS commands is to improve troubleshooting in the event an IP connection is suddenly broken and not recovered. SMS allows users to access and control the router even when there is no IP connection. MTR-xx offers the option to limit access to specific users.

Existing SMS commands:

- SMS command to store logs to DeviceHQ
- Remote reboot over SMS
- PPP status, radio stats, Ethernet link status
- APN modification
- Ping over specified interface getting results over SMS

New enhancements

- Configurable event reporting over SMS: Report ping results, active/inactive interface status (serial, Ethernet, Wi-Fi, cellular) and data traffic, WAN failover event.

d) **New Notifications -** SMS, email or SNMP

- Interface failures – Ethernet, Wi-Fi, Cellular
- Data traffic stats – Ethernet, Wi-Fi, Cellular
- WAN Failover event

All events are time-stamped

VII. Installation Instructions

To upgrade using the MTR-xx Web UI to MTR 3.6.0, you must be running at least MTR-xx 3.4.5 firmware.
To upgrade from a previous firmware, upgrading to MTR-xx 3.4.5 is necessary before upgrading to MTR-xx 3.6.0.

You can download the new SW 3.6.0 binary from the product page http://www.multitech.com/brands/multiconnect-rcell-100-series.

I. Click on the corresponding model (i.e. MTR-LAT1-B07-US)
II. Then “DOWNLOADS”
III. Then “mtr-lte_v3.6.0_upgrade.zip”
Note: even though file description reads “lte”, SW 3.6.0 is compatible with all models listed on page 1 of this document
IV. Follow instructions below:

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 as admin 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) Click the Browse button and select the latest version of BIN file, rcell-mtr-upgrade_3.6.0.bin (non-LTE) or rcell-mtrv1-upgrade_3.6.0.bin (LTE)
10) Click the "Start Upgrade" button. Confirm the 5 minute "OK" button.
11) Wait for the unit to upgrade and reboot automatically.

12) Again, browse to the IP address and verify the Main or Home Page indicates the correct version, 3.6.0.

VIII. 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 MultiTech's comprehensive portfolio of cellular connectivity products optimized for M2M (machine-to-machine). These routers come 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.

IX. Additional Information

If you have any questions regarding this Product Change Notification, please contact your Multi-Tech Systems sales representative:

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

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