



Cradlepoint Release Notes: Rev 6.1.0 Firmware

Products supported/tested:

AER3100/AER3150

AER2100

AER1600/AER1650

IBR1100/IBR1150

IBR600/IBR650

IBR350

MBR1400/MBR1400 HW v2.0

MBR1200b

CBA850

CBA750b

Notes:

Before upgrading to new firmware, it is always a good idea to save the configuration file from your current version. This firmware version will remove a configuration for version 3.2 or lower and will not try to keep your settings.

Revision 5.2.0 was a significant change from previous releases. Updating from prior versions to 5.0.0 through the router UI or ECM will keep all current settings. Factory resetting 5.1.0 and then re-applying a saved configuration from a pre-5.0.0 version may not reset all saved passwords correctly. Downgrading from 5.2.0 or later to an earlier version WILL force a factory reset on the router. Saving a 5.0.0 or later configuration and applying it to an earlier version will change any non-default passwords to an unknown string.

Modems tested (new 6.1.0 modems are in blue text)

USB Modems

Cradlepoint MC200LE-VZ / *Verizon (USA)* / (GPS) Supported on MBR1400, CBA750B Only

Cradlepoint MC200LE2-SP / *Sprint (USA)* / Supported on MBR1400, CBA750B Only

Cradlepoint MC200LP / *Bell, Rogers, Telus (Canada)* / Supported on MBR1400, CBA750B Only

Cradlepoint MC200LP-AT / *AT&T (USA)* / Supported on MBR1400, CBA750B Only

Cradlepoint MC200LP2-EU / *EE (UK), Vodafone (UK, Germany), Tele2 (Sweden), Telia (Sweden)* / Supported on MBR1400, CBA750B Only

Cradlepoint MC300LE-VZ / *Verizon (USA)* / Supported on 2100 Only

Cradlepoint MC300LP / *Bell Mobility, Rogers, Telus (Canada)* / Supported on 2100 Only

Cradlepoint MC300LP-AT / AT&T (USA) / Supported on 2100 Only

Cradlepoint MC300LP2-EU / EE (UK), Vodafone (UK, Germany), Tele2 (Sweden), Telia (Sweden) / Supported on 2100 Only

Cradlepoint MC400LE2-SP / Sprint (USA)

Cradlepoint MC400LPE-AT / AT&T (USA)

Cradlepoint MC400LPE-GN / T-Mobile, C-Spire, US Cellular (USA); Bell Mobility, Rogers, Telus (Canada)

Cradlepoint MC400LPE-SP / Sprint (USA)

Cradlepoint MC400LPE-VZ / Verizon (USA)

Cradlepoint MC400LP3-EU / EE (UK), Vodafone (UK, Germany), Tele2 (Sweden), Telia (Sweden)

Cradlepoint MC400LP6 / Verizon (USA), AT&T (USA), Sprint (USA), Generic (North America, Europe)

Franklin U770 ("Sprint Plug-In-Connect Tri-Mode USB Modem") / Sprint (USA)

Huawei E3276 / Telus (Canada)

Huawei E368 ("AT&T USBConnect Force 4G") / AT&T (USA)

Netgear AC340U ("AT&T Beam") / AT&T (USA)

Netgear AC341U ("NETGEAR® 341U USB Modem") / Sprint (USA)

**supports Netgear firmware 4.07.01.11 and MR2 firmware 45.04.20.00*

Novatel 551L LTE ("Verizon USB551L") / Verizon (USA)

Novatel U620L ("Verizon MiFi® 4G LTE Global USB Modem U620L") / Verizon (USA)

Novatel U679 ("4G LTE Novatel Wireless U679 Turbo Stick") / Bell Mobility (Canada)

Pantech UML295VW ("Verizon 4G LTE USB Modem UML2954G LTE") / Verizon (USA)

**requires Pantech firmware version L0295VWD821F.B4 or later*

Portsmouth PSA1U1M ("Portsmouth USB Client to Analog Modem Adapter") / POTS phone providers

Sierra Wireless 308 USB ("AT&T USBConnect Shockwave") / AT&T (USA)

Sierra Wireless 313U ("AT&T USBConnect Momentum 4G") / AT&T (USA)

Sierra Wireless 320U ("Telstra USB 4G (Sierra AirCard 320U)") / Telstra (Australia)

Sierra Wireless 330U ("4G LTE Sierra Wireless U330 - Turbo Stick") / Bell Mobility (Canada)

Sierra Wireless 330U ("LTE Rocket Stick – Sierra Wireless AirCard 330U") / Rogers (Canada)

ZTE MF683 ("T-Mobile Rocket 3.0 4G Laptop Stick") / T-Mobile (USA)

ExpressCard Modems (MBR1400s, MBR1200B, CBA750B only)

Portsmouth PS6EX1M ("Portsmouth ExCard to Analog Modem Adapter") / POTS phone providers

USB Ethernet Adapters (AER3100, AER3150, 2100, AER1600, AER1650, IBR1100, IBR1150, IBR600, IBR650, MBR1400, MBR1200B, CBA850, CBA750B)

Pluggable USB2-E1000 (“USB 2.0 to 10/100/1000 Gigabit Ethernet LAN”)

New features added in this release

(Not all features are in all products - see their respective Data Sheets)

- Advanced Routing Functionality
 - Added advanced routing protocol (BGP, OSPF, RIP and RIP-NG) support with a new UI and new configuration options including protocol specific features:
 - We strongly recommend that any migrated routing protocol configuration be closely inspected after upgrading.
 - The configuration for routing protocols has changed substantially. A best effort is made to migrate existing configurations to 6.1.0, and any issues are reported in the system log. Some configurations cannot be migrated—when encountered these failures are reported in the system log and the associated router is disabled in the upgraded configuration.
 - Added route filtering to routing protocols via route maps, prefix lists, access lists and community lists as appropriate.
 - Policy-Based Routing (PBR)-lite. Policy-Based Routing allows for the configuration of multiple unique route tables and rule-based policies to tie interfaces and networks to those tables.
 - Added BGP Multipath functionality
 - Anonymous DMVPN on a spoke can handle multiple GRE keys
- (IBR1100) WiFi Client Driver for IBR1100 5GHz radio. This is a new mode for the IBR1100 WiFi driver and it is different than the WiFi as WAN feature. WiFi as WAN is necessary when you want to continue to serve 5GHz WiFi clients. WiFi Client dedicates the 5GHz radio to connecting to an external Access Point and provides better connection stability and performance. WiFi Client can also switch from one Access Point to another in a few seconds, while WiFi as WAN takes significantly longer.
 - Note, in an environment where more than 64 external Access Points are available, the router may take longer to switch from one Access Point to another.
- Improved GPS functionality and stability
- Connection Manager: Added Standby to Availability list. Configuration is used to decrease failover time from one WAN interface to another.
- VPN IKE Phase One allows incoming traffic on ports other than 500
- Certificate Manager can generate certificates with SSL server/client extensions.

- Allow DHCP start and end range to be the same number
- Allow SSH-hopping from the router's CLI to a device on its LAN. We've added a basic SSH client to the router. Users may SSH into any device on either WAN or LAN that is running a SSH server.
 - Configurable options include port, login name, data compression, and session ciphers.
 - Following session ciphers are supported: aes256-ctr, aes192-ctr, aes128-ctr, aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc, blowfish-cbc
 - Client uses aes256-ctr, aes192-ctr, aes128-ctr (PCI-compliant) ciphers by default.
 - Two ways to use different ciphers:
 - Set config/firewall/ssh_admin/weak_ciphers to true and the above list is used.
 - Use -c argument along with comma separated list of ciphers (from supported list)
 - User name can be supplied with -l argument or with user@hostname pair.
 - If client is supplied with a number of hostnames, the last one is used.
- Added Ability to use NAT-TO for remote networks of 0.0.0.0/0 for VPN tunnels
- Added ability to verify peer certificates by x509 Extensions in OpenVPN.
- (LP6 devices) Added Automatic Carrier Selection. Detects the inserted SIM and automatically selects/loads the appropriate modem firmware
- (Cradlepoint modems) Enhancements to System>System Control>Modem Firmware to support multiple local firmware images with a single modem device
- (CBA850) While the default configuration for this router is IP Passthrough, one of the Ethernet LAN ports can be configured to a WAN. Assuming default settings, these changes will enable a WAN Ethernet Port. Initial UI access is through the LAN port, as by default the IP Passthrough port does not allow Admin Access.
 - Set the LAN port to WAN
 - Under Networking -> Local Networks -> Local IP Networks, select the IPPT Interface and edit it. Under Access Control, enable Admin Access. Under IPv4 Settings, you can also set the IPv4 Routing Mode to a different type than IP Passthrough (NAT or Standard) if you wish.
 - Under Networking -> VLAN Interfaces, edit the 'lan' and set the mode to 'WAN'. You will lose connection to the router if you are plugged into this port.
 - You can now connect a WAN cable to what was the LAN port, and use the IP Passthrough port as a LAN port.
 - Set the IP Passthrough port to WAN
 - Under Networking -> VLAN Interfaces, edit the 'IPPT' and set the mode to 'WAN'. You will lose connection to the router if you are plugged into this port.
 - You can now connect a WAN cable to what was the IPPT port, and use the LAN port to communicate with the router.

Security defects fixed

- Cross-Site Scripting attack mitigation. Carve Systems, our security auditors, found two occasions where the router's User Interface was susceptible to an external attack.
 - The WiFi Site Survey did not validate the names of the SSIDs around the router before displaying them on the WiFi as WAN page, so an external SSID with cross-site scripting payload could execute in a router admin's browser.
 - The System log did not validate the names of external users that were not allowed to log into the router either through the UI or through SSH. If the router admin reviewed the Failed Logins they could execute code in the admin's browser.
- UPnP. The version of UPnP we use was vulnerable to a local DoS attack. We updated to a newer version.
- OpenSSL. CVE-2016-0800, aka DROWN attack. The routers are not affected by this vulnerability. We updated to OpenSSL 1.0.1s as part of normal maintenance.
- Updated the supported ciphersuite to Mozilla's suggested compatibility ciphersuite. https://wiki.mozilla.org/Security/Server_Side_TLS

Additional UI/Usability changes

- Added a Status -> Local Network page
- Make ZScaler policy tagging sortable
- New Standby Feature states in Status -> Internet -> Statistics Graph
- Hotspot Services: the Allowed Hosts editor accepts invalid host/domain names
- Hotspot statistics are swapped
- Cannot edit Start range or end range of DHCP Server
- Fixed text alignment on Login page
- Routing Protocol UI Router array sits on 'Loading...' on Firefox 44
- IBR6x0 GPIO page has unsupported options available
- Removed APN setting from First Time Setup Wizard. If automatic APN selection does not resolve to a connection, please use Connection Manager profile configuration to set APNs.
- (Cradlepoint Verizon modems) Added support for new Verizon PLMN 311/270

Defects fixed

- AER1600/AER3100 Factory reset at power on. For these products, do not hold the factory reset button immediately at power on, please wait 1 second until all LEDs come on and then press the factory reset button.
- Hotspotsystem Free Hotspot Package Session Timeout does not work.
- Unable to remote into a Cellular interface while load-balancing is enabled with a wired connection without lowering the MTU on a client PC to 1428 or lower.
- WWAN - Erroneous data usage reported on first connect when viewed on the client router
- Device is not checking into ECM when it should after a failover scenario

- Unable to send device alerts if local domain is unconfigured on the router
- GRE Tunnels not passing traffic if PPTP is unchecked
- Radius/UAM Will Not Save 58 Character Password
- Error message when trying to save a Custom DHCP option that is not in the dropdown list
- Local Certificate (Cradlepoint Secure CA) using SHA-1
- GPS - NMEA enhanced sentences does not log any sentences to client connections.
- Display issue when altering Interfaces for a Local IP network
- LAN scheduler doesn't work correctly
- Umbrella/OpenDNS no longer connects on 6.0.x firmware and newer
- IBR1100:Need to rework how input delay time is displayed for GPIO settings
- VTI tunnel creating multiple pairings with a policy-based VPN
- DHCP Lease Expiration time increments instead of decrements and is showing the incorrect lease time to begin
- IBR1100 with hotspot is causing router lockup and reboot
- FW 6.0.2 doesn't display a warning when a user attempts to add more than 10 remote networks for VPN
- Ignition Sensing behavior issue in 6.0.1 thru 6.0.4, router not powering down when ignition changes to low state
- Hotspot Idle-Timeout not working
- WiFi as WAN: WPA1 and WPA2 Enterprise not saving EAP&TTLs Authentication
- Client List not showing wired clients
- LLDP deadlock breaks Admin access and GET status/ldp
- Static LAN IPv6 configuration does not work
- tcpdump command not handling multi-word expressions correctly
- Creating both tunnel mode and VTI mode VPNs would continually create multiple pairings between endpoints.
- RTC battery alert on AER3100 dashboard constantly popping up despite full battery health.
- Serial console login prompt on AER3100 does not print output from backspace correctly.
- OpenDNS does not work on 6.0.x
- Disabled VPN tunnels are able to go Mature
- Static WiFi clients appearing in Client List showing old DHCP information
- MC400LPE-VZ dual SIMs with two different APNs now allow modem to plug properly
- Dual SIM APN and modem firmware information now displays after SIMs become active
- Configuration changes made via SMS now display in ECM
- Migration of v5.2.4 PPPoE rules with USB-to-Ethernet dongle are now exposed in the UI Ethernet tab

Known issues

- Reputation Services (6.0.1). If you upload a reputation file to the router, save the configuration, factory reset, then reload the configuration file any firewall entries referencing that reputation file will fail. The reputation file is not saved in the exported configuration file.
- IPSec. Certificates do not work if Router Services used (new feature in 5.2.0)
- If any of the router's WAN connections (Ethernet, Wi-Fi as WAN, modem) connects to a device that has the same IP subnet as the router, the router will disable the interface and provide a Bounce Page warning that the WAN interface has a conflict. Simply change the LAN IP Address

on the Network Settings -> WiFi / Local Network Settings page in the UI.

- The CBA850 does not support an external USB-to-Serial adapter when an internal modem is also connected to a Carrier. Please use the internal console port or an Ethernet WAN connection instead.

LTE

- Unless you have a specific service from your carrier, LTE modems will not generally provide an externally-available IP address. Services, such as Remote Management, will not work.

Modem

- Franklin U770. The Modem's Ethernet address conflicts with the default address of the Guest LAN. A warning message is placed in the log and the Guest LAN is disabled. If you change the address of the Guest LAN to a non-conflicting address, this restriction will not occur.
- Sierra Wireless 313U, 330U. When these modems connect on 2G or 3G bands, specifically on GSM 850, they will sometimes cause interference on the USB bus, resulting in the modem not plugging properly. If this occurs, attaching the modem to a USB extension cable will generally fix the problem.
- The following USB modems contain an embedded web server through which many modem settings are configured. To access the modem's web pages, you must be logged in as the router administrator. Once logged in, you can then access the modem web pages at these given IP addresses:

Franklin U770 / <i>Sprint (USA)</i>	-> 192.168.10.1	
Netgear AC341U * / <i>Sprint (USA)</i>	-> 192.168.1.1	(address is configurable)
Pantech UML295VW * <i>Verizon (USA)</i>	-> 192.168.32.2	

* The modem web pages are available only when the modem is operating in NAT mode.

Cradlepoint Release Notes: Rev 6.0.5 Firmware

New features added in this release

(Not all features are in all products - see their respective Data Sheets)

- No Features, defect fix only.

Security defects fixed

- UPnP. The version of UPnP we use is vulnerable to a local DoS attack. UPnP is disabled by default and only available on the LAN, so the exposure is minimal. We will update to a newer version in our next major release.

Defects fixed

- ECM configuration rollback would not work in versions 6.0.2 and 6.0.4
- Fixed a defect with Hotspot support that could cause a router deadlock and then reboot

Known Issues

- Reputation Services (6.0.1). If you upload a reputation file to the router, save the configuration, factory reset, then reload the configuration file any firewall entries referencing that reputation file will fail. The reputation file is not saved in the exported configuration file.
- IPSec. Certificates do not work if Router Services used (new feature in 5.2.0)
- If any of the router's WAN connections (Ethernet, Wi-Fi as WAN, modem) connects to a device that has the same IP subnet as the router, the router will disable the interface and provide a Bounce Page warning that the WAN interface has a conflict. Simply change the LAN IP Address on the Network Settings -> WiFi / Local Network Settings page in the UI.

Cradlepoint Release Notes: Rev 6.0.4 Firmware

New features added in this release

(Not all features are in all products - see their respective Data Sheets)

- No Features, defect fix only.

Security defects fixed

- UPnP. The version of UPnP we use is vulnerable to a local DoS attack. UPnP is disabled by default and only available on the LAN, so the exposure is minimal. We will update to a newer version in our next major release.

Defects fixed

- SNMPv3 had a memory leak when WIIPE MIB modem objects were repeatedly queried.

Known Issues

- Reputation Services (6.0.1). If you upload a reputation file to the router, save the configuration, factory reset, then reload the configuration file any firewall entries referencing that reputation file will fail. The reputation file is not saved in the exported configuration file.

- IPsec. Certificates do not work if Router Services used (new feature in 5.2.0)
- If any of the router's WAN connections (Ethernet, Wi-Fi as WAN, modem) connects to a device that has the same IP subnet as the router, the router will disable the interface and provide a Bounce Page warning that the WAN interface has a conflict. Simply change the LAN IP Address on the Network Settings -> WiFi / Local Network Settings page in the UI.

Cradlepoint Release Notes: Rev 6.0.2 Firmware

New features added in this release

(Not all features are in all products - see their respective Data Sheets)

- Security -> Content Filtering -> Zscaler Secure Web Gateway. Multiple policies (up to three) can be configured.
- Allow HTTPS downloads for Firmware and Modem Updates, and IPS/IDS signatures. The automatic firmware and signature checks will use Cradlepoint's HTTPS servers instead of HTTP. If your network blocks HTTPS traffic (port 443), a control under System -> System Control -> System Firmware -> Allow HTTP Firmware Check will allow backwards compatibility. Customers who redirect Firmware updates to non-Cradlepoint sites are not affected.
- (IBR1100) Allow additional GPIOs using a Serial-to-GPIO cable. The System -> GPIO Configuration menu has been significantly changed to allow adding more readable information about the GPIOs and their alerts.
- (IBR1100) The state of the output GPIO is being reversed to correctly reflect the "high" and "low" active states, as set in the UI. See the Knowledge Base article for more details.
- Only allow one user to access a serial interface at a time. If one user has opened a serial interface and another user needs to use it, a 'serial --force' option is available at the CLI that will disconnect the existing user.
- (CBA850) The external USB port has been enabled even if the router is using PoE. Note that if the router is on PoE and two modems are in use it is possible that the router will reboot from lack of available power.
- System -> SNMP Configuration. The order of modem interfaces shown in an SNMP walk will match the order listed in the Connection Manager WAN Interfaces Profiles & Priority page.

Security defects fixed

- UPnP. The version of UPnP we use is vulnerable to a local DoS attack. UPnP is disabled by default and only available on the LAN, so the exposure is minimal. We will update to a newer version in our next major release.

Additional UI/Usability changes

- System -> Diagnostics -> Speed Test -> Test Type. Added a third test type, TCP Latency/Jitter. This better reflects those measurements. Also changed the Time vs. Data constraints to better control the testing.
- Status -> Internet -> Statistics page scrolls to the bottom of the page on refresh
 - Statistics page is difficult to read at high transfer speeds
- Dashboard WiFi LAN and Ethernet LAN naming and client count issue
- Drag and drop on touch-enabled devices using Chrome does not work
- Modem micro status did not stay open when a user is looking at it
- MBR1400, WiFi Radio showed 2.4GHz after it had been switched to 5GHz
- The Networking -> Routing -> OSPF Remove button did not work correctly
- Enable/Disable VPN button on Status -> Tunnels -> IPsec VPN had issues with Internet Explorer
- Added Registered Carrier to Status->Internet->Connections->Cellular Carrier for Novatel U620L modem (“Verizon MiFi® 4G LTE Global USB Modem U620L”)

Defects fixed

- IPsec VPN: NAT to Address with 0.0.0.0/0 remote network caused exception
- VRRP UI defaults reset
- WiFi Bridge mode broken
- Knowledge Base links updated to correct location
- IPv4 DHCP options renumbered
- Telnet Serial Redirector Linefeed option is ignored on startup until setting is toggled and resaved
- Zscaler Internet Security did not work correctly with router Hotspot services
- (AER3100) WiFi as WAN had issues connecting with Protected Management Frames
- WiFi as WAN doesn't recover from link errors
- DHCP Relay causing abrupt error on initial restart
- IPsec, with more than 1 VTI tunnel additional tunnels establish but don't pass traffic
- Zone NAT port forwarding failing with CP Secure VPN
- OSPF Area ID length limited by UI
- 802.1x authentication sending wrong NAS-Port Type attribute value for Ethernet clients
- Hotspot issues with DNS resolves
- Dashboard WiFi panel is blank
- Unable to edit GPS Server or Client settings
- Can't access admin page (WiFi SSID has apostrophe in it)
- Hotspot bounce and redirect page issues

- PFS disabled in IPSec VPN Tunnels causes uneditable VPN Tunnel
- (IBR1100) Ignition sensing behavior changed
- (IBR650) Missing GPS settings
- Port proxy rules UI available on products that do not support it

Known Issues

- Reputation Services (6.0.1). If you upload a reputation file to the router, save the configuration, factory reset, then reload the configuration file any firewall entries referencing that reputation file will fail. The reputation file is not saved in the exported configuration file.
- IPSec. Certificates do not work if Router Services used (new feature in 5.2.0)
- If any of the router's WAN connections (Ethernet, Wi-Fi as WAN, modem) connects to a device that has the same IP subnet as the router, the router will disable the interface and provide a Bounce Page warning that the WAN interface has a conflict. Simply change the LAN IP Address on the Network Settings -> WiFi / Local Network Settings page in the UI.