HiLCOS
The Hirschmann™ BAT Operating System

Information regarding Release

HiLCOS Software Version 10.12 RU8

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Germany

Internet: http://www.beldensolutions.com

2021-05-21

HiLCOS

The Hirschmann™ BAT Operating System

Table of Contents

HiLCOS

The Hirschmann™ BAT Operating System

1. Preface

HiLCOS is the operating system for the Hirschmann OpenBAT (BAT-R and BAT-F), BAT450, BAT867 and BAT WLC products. This document describes the innovations within HiLCOS software release 10.12 RU8, as well as the improvements since the previous version.

2. Known Issues

The use of RSTP together with AutoWDS can lead to an unstable AutoWDS network. It is recommended to use AutoWDS with RSTP disabled.

In very rare cases when adding a new Access Point (AP) in the AutoWDS network interactions between neighboring AutoWDS APs can occur. This can cause short-term disruptions of wireless links.

If APs are added in an AutoWDS network before enabling Auto-Accept, these APs must be accepted manually after switching Auto-Accept.

In rare cases the configuration rollout to a managed AP might take around 30 seconds longer when there is a configuration exchange in a redundant WLAN-Controller architecture.

Using the WLC redundancy feature access points do not re-distribute automatically to the preferred controller.

Broadcast attacks are invisible to the Wireless IDS.

An encrypted HiLCOS configuration, generated with HiLCOS 9.12, cannot be loaded in the current HiLCOS 10.12 release.

In rare cases the BAT867 health monitoring system may restart the device.

LANconfig can use SSH, TFTP, HTTP and HTTPS protocols to communicate with the devices. However due to changes regarding force password change, SSH cannot be used with devices which still have a default password. As soon as the default password is changed on the device, SSH will start working normally.

HiLCOS
The Hirschmann™ BAT Operating System

3. Improvements in HiLCOS 10.12. 6388-RU8

General

- HT and VHT transmission rates are set back to their default values when upgrading to 10.12 RU8 or later. Users can manually apply their settings again after the upgrade, which will then be preserved in future upgrades.
- Default SCEP Encryption setting is changed to AES128 to support managed AP to download their certification via SCEP.
- Increased the default value of the SSH minimum host key length to 2048.
- H.323 ALG will be disabled with the upgrade to 10.12 RU8 or newer. Users can manually apply their settings again after the upgrade, which will then be preserved in future upgrades.
- GPS status is now updated at every second. Previously it was updated in every 5 seconds.

Bugfixes in HiLCOS 10.12-RU8

- Following two issues have been fixed related to Wireless IDS -
  - In previous versions of HiLCOS 10.12 it was not possible to modify a managed AP via LANConfig when a WIDS profile is set by a BAT Controller or WLC at the same time.
  - Disabling a WIDS profile via BAT WLC or Controller did not disable on the Managed AP's local web Interface.
- Industrial HiVision was not detecting BAT devices with SNMPv3 enabled rather detecting it as Ping device onlyThis issue is now fixed by an increase of Max-Login errors to 15 and the default setting is changed accordingly, With this setting present all BAT device are now detected as BAT device via Industrial HiVision.
- BAT device status screen was not displaying the WAN IP address under IPv4 section. This is now fixed.
- Time-of-DFS-rescan input format is corrected for WEB GUI as per the user manual.
- Setting up the internet connection with "mobile interface" was not available in Web Setup Wizard. This is now fixed.
- The Taiwan profile was not showing up in "show wlan" CLI output. This is now fixed and the Taiwan profile is now activated by default on matching products.
- CAPWAP diagnostic trace is corrected when showing values of Convert-to-Unicast and 11ac-Beamforming.

HiLCOS
The Hirschmann™ BAT Operating System

4. Improvements in HiLCOS 10.12.6290-RU7

Bugfixes in HiLCOS 10.12-RU7

General

- Update of Taiwan country profile according to NCC certification for BAT450-F devices:
  - The following subbands are supported
    - 2.4GHz band – channels 1-11 (20MHz) / 1-10 (40MHz)
    - 5 GHz channels 36-48 and 149 -165

- In previous versions of HiLCOS 10.12 it was not possible to reach a WAN interface from the WAN side. This issue is fixed with HiLCOS 10.12-RU7.

- Several fixes regarding OpenSSL vulnerabilities are included to HiLCOS 10.12-RU7:
  - EDIPARTYNAME NULL pointer de-reference (CVE-2020-1971)
  - ECDSA remote timing attack (CVE-2019-1547)
  - Fork Protection (CVE-2019-1549)
  - Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

WLAN

- In Malaysia country profile for 5GHz subband 3 the DFS-Channel Availability Check is disabled. This previously caused several minutes of delay until operation after powering up the device.

- In previous versions of HiLCOS 10.12 the WiFi client address adaptation was not working correctly. This issue is fixed with HiLCOS 10.12-RU7.

- When operating a BAT867 or BAT450-11ac device in client mode within a noisy environment with several sources of interfering signals present, the device radio was in rare cases stopping communication. With HiLCOS 10.12-RU7 several improvement have been introduced to automatically recover from such cases.

- Client devices roaming handover on BAT devices before HiLCOS 10.12-RU7 and HiLCOS 9.12-RU9 was impacted negatively by the following issues:
  - In case of hidden and protected SSID the client was relying on probe response information only. Now the client also gets updated from beacons and outdated values are no longer taken into account. This leads to a better roaming decision.

  - In case the handshake with the new AP is disrupted by interfering signals, the association might fail completely which can lead to a disruption longer than 5 seconds of the communication. In version HiLCOS 10.12-RU7 and HiLCOS 9.12-RU9 this issue is resolved.

HiLCOS
The Hirschmann™ BAT Operating System

5. Improvements in HiLCOS 10.12.6202-RU6

- With the 10.12.6202-RU6 the optional mechanism is added o prevent a packet burst that can occur after an interruption of the WLAN connection (Stuck Transmitter). This also prevents packets from being delayed too long due to the interruption. By discarding the packets, retransmits are possible.

6. Improvements in HiLCOS 10.12.6154-RU5

General

- BAT-Controller devices running HiLCOS 10.12.6003-RU4, were no longer able to successfully manage BAT devices running a different firmware version than 10.12.6003-RU4. As a consequence the radio of these BAT devices remains turned off. This issue is fixed in HiLCOS 10.12. 6154-RU5.
  With 10.12-RU5 on the BAT-Controller it is now tested, that APs running 10.12 and 9.1x software versions can be successfully managed.
- The password complexity check rejected certain password phrases even the complexity requirement was fulfilled for the phrase. This issue is fixed in 10.12.6154-RU5.

HiLCOS
The Hirschmann™ BAT Operating System

7. New features and and improvements in HiLCOS 10.12.6003-RU4

New features and additions in HiLCOS 10.12-RU4

- **The support for the FCC 4.9 GHz Public Safety Spectrum is added.**
  This mode is available for use in US using the Hirschmann EWLAN1 radio module included to OpenBAT-R/-F and BAT450-F products.
  Note: The products have to be ordered containing letter 'P' as approvals-2 within the device product code: e.g. BAT[450]-[R/F]USXXXXXXPXXXXXXXXXZHXX.XX.XX

- **Update of Australia country profile**

Item	Frequency Band	Channel	Max. EIRP	Usage	DFS
1.	2400 MHz to 2500 MHz	1-13	18 dBm	Indoor/Outdoor	No
2.	5150 MHz to 5250 MHz	36-48	23 dBm	Indoor	No
3.	5150 MHz to 5350 MHz	36-64	23 dBm	Indoor/Outdoor	Yes
4.	5470 MHz to 5725 MHz	100-140	30 dBm	Indoor/Outdoor	Yes
5.	5725 MHz to 5850 MHz	149-165	36 dBm	Indoor/Outdoor	No

Bugfixes in HiLCOS 10.12-RU4

General

- A potentially security relevant cross-site scripting issue has been fixed that allowed JavaScript code to be executed from the Public Spot login page. If such code was used, information could be infiltrated which could be used to attack a Public Spot user's system via a manipulated link.
- The Public Spot redirection to the login page was not no longer working after an upgrade to HILCOS 10.12-RU2. This issue fixed.
- An issue in the incorrect SNMP responses to SNMP Bulk requests has been fixed in the HiLCOS SNMP stack.
- An issue that the configuration of the LACP feature was not available has been fixed.
- Stability improvements for the SNMP, the SSH and the TLS when handling malformed packets have been added.
- Misleading bootlog entries from Alive-Test feature have been removed.

WLAN

- Additional configuration setting is added, to provide an optional packet drop after a low level error within the Hirschmann EWLAN radio is detected.

HiLCOS
The Hirschmann™ BAT Operating System

8. Bugfixes and improvements in HiLCOS 10.12.5900-RU3

General

- Improvement in AP stability under WLC cluster.
- TX power of BAT867 is decreased for FCC versions.
- REDcompliance CLI command is available.
- Improvements in LANmonitor.
- HiDiscovery improvements.
- Forced Password Change improvement updates.

WLAN Controller

- Fixed the scenario with continued loss of cluster
- Improvements in WLC Fast Recovery in combinations with Client Roaming

Important Update for WLAN India Country Profile:
Due to the recent regulatory changes in India, India country profile and respective channel sub-bands are modified. Please find the actual state as a table below:

Sub-band	Frequency Band	Channel	Max TX power	Max. EIRP	Usage	DFS
1.	5150 MHz to 5250 MHz	36-48	30 dBm	36 dBm	Indoor	No
1.	5150 MHz to 5350 MHz	36-64	21 dBm	21 dBm	Indoor/Outdoor	Yes
2.	5470 MHz to 5725 MHz	100-140	24 dBm	30 dBm	Outdoor/Indoor	YES
3.	**5725 MHz to 5875 MHz**	**147-173**	**30 dBm**	**36 dBm**	**Indoor/Outdoor**	**No**

As an example, in 5GHz channel number 171 and 173 used to belong to Sub-band 2. Since with this update they now belong to sub-band 3, to keep using the same channels, it is required to change the sub-band number from 2 to 3 and update the configuration.

HiLCOS
The Hirschmann™ BAT Operating System

9. Bugfixes and improvements in HiLCOS 10.12.5700-RU2

General

- Force the user to change the default password at the first login
- Added an option to automatically redirect HTTP requests to HTTPS

WLAN

- Improved P2P connection stability on BAT867 devices

HiLCOS
The Hirschmann™ BAT Operating System

10. Bugfixes and improvements in HiLCOS 10.12.5500-RU1

General

- Update country profile India
- Update country profile Argentina
- Update country profile Malaysia
- Fix for auto load firmware from USB on OpenBAT-R/F devices
- Improved stability WLC Cluster
- GPS MIB objects

WLAN

- New simple mesh-like network
- Improve distribution of clients between access points
- Improve roaming on BAT867 and BAT450 11ac devices
- Improved connection stability on BAT867 devices
- Privileged channels considered when choosing operating channel in DFS band
- Improved BAT867 setup wizard for client mode
- Improved logging for background scanning in client mode

Network Connectivity

- Fix ARP handling of multiple MAC addresses for BAT devices in WLAN client mode and no active client bridge support

HiLCOS
The Hirschmann™ BAT Operating System

11. Overview on new features as of version 10.12.5286-REL

SNMPv3	Hirschmann customers now benefit from improved security in network monitoring thanks to SNMPv3 (Simple Network Management Protocol version 3). This protocol combines user-friendly device monitoring with strong security thanks to its encrypted data communications. And since it is enabled automatically, there is no need for you to make any configuration changes.
Maximum Wi-Fi Quality	Noticeable improvements in the performance, reliability, and range of BAT access points: As of HiLCOS 10.12, all Wi-Fi devices support the highlight features **Airtime Fairness, Adaptive RF Optimization**, the **Wireless Intrusion Detection System**, and many others. What's more, substantial quality improvements give BAT users and administrators the best ever Wi-Fi experience.
Wi-Fi Adaptive RF Optimization	Dynamic selection of the best available Wi-Fi channel: Optimized wireless LAN throughput in case of interference as the access point dynamically selects the best Wi-Fi channel.
Wi-Fi Airtime Fairness	Improved exploitation of the Wi-Fi bandwidth: The fair sharing of wireless transmission times between all of the active clients uses the available bandwidth to maximum effect and improves Wi-Fi performance.
Wi-Fi Adaptive Transmission Power	Ideal for professional backup scenarios in wireless environments: If an access point fails, the transmission power of the remaining access points is increased automatically, so that full Wi-Fi coverage is assured at all times.
Wi-Fi Configurable data rates per SSID	Communication data rates between the access point and Wi-Fi clients can now be tightly controlled for a genuine gain in flexibility. For instance, data rates made unusable by environmental conditions can be excluded from use.
WLAN	The automatic conversion option from Multicast to Unicast data streams enables multiple Wi-Fi clients to stream judder-free, high-resolution video applications. For applications, e.g. Multicast IPTV services, you benefit from an improved performance and a significant quality improvement.
Wi-Fi Flexible access models for Public Spot accounts	The bandwidth that was booked for the Public Spot can now be displayed on vouchers. Also the validity period (time of expiry) of vouchers can be set with shorter time units (days, hours, and minutes).
Performance measurement with iPerf	iPerf, a tool integrated into HiLCOS, allows you to precisely measure the maximum and momentary TCP and UDP throughputs between two devices on the network. The bandwidth losses derived from this can be used to identify and correct bottlenecks on the network.
Higher complexity for device passwords	Improved security with a new password policy requiring at least eight characters consisting of letters, digits and special characters.
Integration of AiRISTAFLOW RTLS	As of now, HiLCOS 10.12 allows the integration of AiRISTAFLOW Real Time Location Systems into Hirschmann infrastructures. Hence, from now on persons, objects, and devices can be positioned professionally and reliably within their Wi-Fi environment.

	Positioning, tracking of mobile machines in a warehouse or even tracing of work tools– the compatibility between Hirschmann and AiRISTAFLOW offers you realtime localization for any business or application field.
IKEv2	IKEv2 ensures that VPN tunnel establishment is faster and more secure. For the first time, encrypted VPN networking is now possible between IPv6-based sites, including those using mixed operation with IPv4.
IKEv1 with IPv6 support	As well as supporting IKEv2, HiLCOS 10.12 also supports IKEv1 for negotiating VPN connections between IPv6 networks.
	More VPN performance and security A Support of AES-GCM for IKEv2 A Support of the elliptic curve Diffie-Hellmann groups (ECDH) 19, 20, 21, and the ECC Brainpool curves 28, 29, and 30 for IKEv2 A Support of RADIUS CoA for IKEv2
IPv6 DHCPv6	Freely configurable DHCPv6 options
LACP	LACP (Link Aggregation Control Protocol) offers a huge added value in terms of reliability. LACP allows bundling of Ethernet connections to a virtual link. Ideal for the installation of redundant connections: If a physical link fails, data traffic will still be transmitted over the other cable. In addition, the possible transmission speed of redundantly connected devices is increased.
IPv6	Variables for IPv6 LAN address and prefix in the action table
ICMPv4 und ICMPv6	Rate limiting for ICMPv4 and ICMPv6 is available
NTP	A Support of MD5 in NTP client and server A NTP server for each ARF net available
Public Spot E-Mail request on login	The Public Spot usage can be made conditional on a user registration by requesting the user‘s e-mail address. The title of the Public Spot login page can be stored in six different languages. You can choose between German, English, Italian, Spanish, and Dutch. The language of the Public Spot login page‘s title depends on the user-defined browser language. The PMS module gives the opportunity to let the user accept the Public Spot‘s terms of use on the PMS login page, too. Additionally, the maximum transmit- and receive bandwidth can be configured for each tariff.
Public Spot Smart Ticket	More security for the Smart Ticket functionality in the Public Spot: Having already been able to allow and block country codes, you can now do the same with individual area codes. This way the abuse of expensive value-added numbers when requesting access to your Public Spot is prevented.
Logging of DNS queries	Client-side DNS requests are optionally sent to an external SYSLOG server for logging and analysis.

HiLCOS
The Hirschmann™ BAT Operating System

12. Detailed list of new features in HiLCOS 10.12.5286-REL

Network Connectivity

- Support for automated rollout via DHCP option 43
- The SCEP client obeys certificate dependencies
- Support for SNMPv3
- The amount of detected devices is shown with ll2mdetect
- NTP client and server support IPv6
- Option for changing EAP-TLS settings, if the BAT device works as 802.1x supplicant
- Support for IKEv2
- The device status display shows an active backup connection and the number of established backup connections
- A backup can be triggered if a memorized route is no longer available (Route Monitor)
- The IPv6 firewall rule „Allow-IPSec“ is enabled by default
- Using syslog, DNS requests can be forwarded to an external syslog server
- HiLCOScap supports IPv6
- Support for IPv6 VPN with IKEv1
- A Syslog server can be enregistered as DNS name or IPv6 address
- WAN connection prio tags are taken over to the VLAN header according to 1TR-112 or DSCP
- The syslog shows the reason for a denied RADIUS server authentication request
- Support for ChaCha20-Poly1305 for SSH
- CA support for SCEP message GetCaCaps
- Adapted IKE and PFS default groups to DH group 14 within VPN
- Registered SIP users are not deleted on configuration changes
- Support for IPerf as server and client
- Switchable configuration protocols
- Added an open ports display in WEBconfig under the „Services“ tab
- Powersaving for Ethernet interfaces is enabled by default
- Removed the VLAN tagging mode „Incoming mixed“
- DHCP lease time is configurable per network
- Password complexity for the main device password and further administrators can be forced

WLAN

- IAPP is disabled if a CAPWAP tunnel is active
- Support for Airtime Fairness
- Radio-field optimization can be done on autonomous Access Points
- Multiple AutoWDS profiles can be configured on a WLC
- Support for Adaptive RF Optimization
- Average Wi-Fi error rates of particular Access Points can be read out on a WLC
- Using the URL variable „%r“, the MAC address of the Access Point to which a client is authenticated can be transmitted in a Public Spot redirect.
- The absolute elapse time of a Public Spot voucher can be configured in minutes and seconds
- Added a counter for displaying failed WPA authentication attempts
- Specified data rates can be configured per SSID
- The Public Spot function „Accept Terms and Conditions“ is utilizable when using PMS
- The displayed columns can be configured within the Public Spot/Manage User wizard

- Surplus blank characters while typing usernames and passwords are removed automatically
- The assigned bandwidth profile for a Public Spot user can be shown on the voucher
- Brute Force protection can be realized by configuring a login blocker
- Added a switch to forward HTTPS connections from unauthenticated clients to the Public Spot gateway
- Added an option to preview the uploaded Public Spot templates via WEBconfig
- Support for Spectral Scan for 802.11ac Wi-Fi modules
- Improved Wi-Fi rate adaption
- The current channel width and used MCS are now displayed in the Wi-Fi interpoints table and in the station table
- Multicast > Unicast transformation for Judder-free IPTV streaming in the Wi-Fi
- As of now, the menus for the Public Spot configuration are generally available within HiLCOS, but can only be used after successful activation of the Public Spot option.
- 802.1x: Availability check for RADIUS server

VPN & Routing

- IKEv2 Load Balancer for load balancing of incoming VPN connections
- Freely configurable DHCPv6 options
- OCSP check in the TLS / Rollout wizard
- Support of AES-GCM for IKEv2
- Support of the elliptic curve Diffie-Hellmann groups (ECDH) 19, 20, 21, and the ECC Brainpool curves 28, 29, and 30 for IKEv2
- Support of RADIUS CoA for IKEv2
- Load Balancer for IKEv2
- Maximum VPN availability thanks to additional backup mechanics
- Variables for IPv6 LAN address and prefix in the action table
- ICMPv4 and ICMPv6 rate limiting
- Support for MD5 in NTP client and server
- NTP server for each ARF net available
- Besides the realm types "Mail Domain" and "MS Domain", the RADIUS server now supports the realm type "MS-CompAuth" by default.
- Blocked IPv4 routes for RFC 1918 networks are no longer activated by default in new configurations.

General

- LACP - virtual Ethernet port bundling for maximized reliability
- Command for switching the firmware with automatic device restart
- File import per Copy & Paste
- Elimination of the port 8080 for WEBconfig and Public Spot

HiLCOS
The Hirschmann™ BAT Operating System

13. Bugfixes and improvements in HiLCOS 10.12.5286-REL

General

- No WAN statistics were sent per SNMP which caused missing displays in e.g. LANmonitor.
- While checking for free addresses, the DHCP server blocked addresses tagged as already allocated with the maximum lease time. These addresses are now blocked for only five minutes.
- The default rule for the Content Filter in the IPv6 firewall captured all protocols and all stations to all stations.
- The ARP implementation included a check to discard received ARP packets with a sender MAC address and set group bit (multi- / broadcast). This could cause a non-functioning layer-2 communication and e.g. a failed ping to a local server.
- Port forwarding of the UDP port 500 did not work as expected in some scenarios.
- If a configuration was read as script, it could not be written back accurately due to error messages within the Public Spot module.
- If a configuration snapshot for synchronizing was bigger than 1 Mbyte, a parameter alignment could not be done by config sync.
- If a BAT device received a time request (NTP via UDP) which contained a “0” checksum, the request was rejected by the internal router service.
- DHCPoE based Internet connections which received an additional masquerading address used this address only for half of the DHCP lease time. On a DHCP renew the address got lost and from that time on the address which was received by DHCP was used.

VPN

- If an additional administrator account should be created using WEBconfig, some fields for configuration parameters and checkboxes for functional rights were missing on the GUI.
- Wi-Fi
- Devices with 802.11ac Wave1 Wi-Fi modules could suddenly restart which was caused by a faulty reset of the Wi-Fi module.
- EAPoL packets for 802.1X authentication were not forwarded by the access point, if protocol filters were configured on the devices (under Wireless-LAN → Security → Protocols), which should discard packets from clients. An explicit “allow” filter for EAPoL packets (Ethertype 888e) solved the problem.
- The Spectral Scan function of WEBconfig led to a freezing browser tab after a short time, so that no Spectral Scan data could be displayed anymore.

WLAN

- The driver for the IEEE 802.11ac Wave1 Wi-Fi modules of the BAT867 product was updated
- Fixed a problem that only particular clients could authenticate to an 802.11ac accesspoint
- Fixed a bug which led to a several minute lasting inaccessibility of an accesspoint in client mode while roaming between base stations
- Check of the DNS server response is now case insensitive
- Fixed a certificate error when an accesspoint tries to connect to a WLC
- ARP packets are now transmitted reliably when using the client bridge mode with IEEE 802.11ac capable Wi-Fi modules.

- The IEEE 802.11ac module of a BAT access point was sending beacons with a data rate of 1 Mbps in the 2.4 GHz band in 802.11gn/mixed mode, as well as in Greenfield mode. This lead to beacons being visible even on an 802.11b client, although the 802.11b mode was disabled in the access point configuration.

Network Connectivity

- Fixed a DNS resolution problem where an explicit DNS forwarding configuration was needed
- Port forwarding of VPN ports 500 and 4500 works again
- Fixed the firewall packet action „Only when default route“
- Variable „DEVICE_URL“ works again when used with the „loadscript“ command
- If a VPN tunnel is established via DynDNS names, the name is re-resolved immediately after a disconnect, so that the tunnel is not established to the previous address
- The Internet configuration wizard sets the correct netmask within WEBconfig
- A dynamic VPN connection can be established via Load Balancer
- Corrected the negotiated WAN interface MTU for IPv6
- Fixed a bug which prevented a 4G backup connection establishment

14. Comments

Backing up the current configuration

Before upgrading your BAT devices to a new HiLCOS version it is essential to backup the configuration data!

Due to extensive features it is not possible to downgrade to a previous firmware without using the backup configuration.

If you want to upgrade devices which are only accessible via router connections or Wi-Fi bridges, please keep in mind to upgrade the remote device first and the local device afterwards.

Please see the HiLCOS reference manual for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems only after internal tests in client environment.
Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by Hirschmann Automation and Control GmbH .

Please note that after upgrading to RU8, HT and VHT transmission rates configuration shall not be preserved. RU8 firmware shall set HT rate as Rx/Tx, and VHT will be MCS9, irrespective of any previous configuration. Syslog shall display it as below-
"Upgrading from 10.12 RU7 or lower version, HT/VHT rate config can't preserved and set to Default"