HiLCOS
The Hirschmann™ BAT Operating System

Information regarding Release

HiLCOS Software Version 10.34-RU4

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

Internet: http://www.beldensolutions.com

2023-03-17

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, BAT450-F, BAT867, BAT-WLC and BAT Controller Virtual product. This document provides an overview of important information regarding HiLCOS software release 10.34-RU4.

Please note the HiLCOS 10.34-RU4 does NOT support the LTE modem in BAT450-F products (BAT450-F..W9L…).

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.

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. Bugfixes and improvements in version 10.34.5895-RU4

- Improved BAT867 radio stability.
- Added trace messages for access point mode in case of connectivity issues between the access point & client.
- GPS output now is shown with increased accuracy (additional decimal).
- Fixed Configuration Upload and Download function compatibility for Industrial HiVision Tool.
- PMK Lifetime parameter is now configurable on WLAN Controller.
- Firewall for IPv4 enabled by default.
- Default value of TCP max connection has been updated to 200 for all BAT devices except WLC.

HiLCOS
The Hirschmann™ BAT Operating System

4. Overview on new features as of version 10.34.5725-RU3

The following three new features and improvements are support with version 10.34.5725-RU3.

1) NG Wireless support tool

One challenge for setting up and operating a WLAN installation are events on the WLAN device that can impact the performance or quality of WLAN links. Thus, it is sometimes essential to have extended logging and information acquisition capabilities to understand the WLAN environment and the corresponding behavior of a WLAN installation.

The WLAN-Diagnostics feature gathers various WLAN information logged over time in a single table. The gathered information is made available for automated processing via SNMP or can be exported as .csv file. This way analysis tools, technicians and support staff can analyze the available information.

In summary, this feature will help to simplify and accelerate the diagnostic, fixing, and optimization of WLAN issues.

Here you find the WLAN-Diagnostics table:
HiLCOS Menu Tree > Status > WLAN > WLAN-Diagnostics

For additional details please refer to the HiLCOS User and Configuration Manual.

2) Syslog Enhancement

Syslog enhanced/improved to provide the more detailed debugging information related to system events. Following categories of syslog has been added.

- **Channel change**
  FORMAT: [WLAN-<INTF>] Switched channel from <X> to <X> in [with in <X>ms] [EIRP <X>dBM][DFS active/inactive]

- **Time**
  FORMAT: System time changed to <X> fro <Y> - Time difference <Z>

- **Antenna**
  FORMAT: [WLAN-<INTF>] Antenna port <> is not receiving data

- **Connect**
  FORMAT:
  (connection/roam) (successful/failed) to/from <NAME> (on channel XX) (in XXX msec)
  It will also display 802.11r/k/v , LDPC , STBC , Guard Interval , Frame aggregation
  Initiate Fast Roaming/Roaming old AP <NAME> channel <X> New AP <NAME> channel <X> strength <Y>

- **Link**
  FORMAT: [ETH-X] link up : <x>Mbs, (full/half) duplex, flow control (Enable/Disable)

- **Radar detection**
  FORMAT:Radar Pattern MinDur=<W>, ETSI constant PRF type <X>, channel <Y> is blocked for at least <Z> min

- **Power**
  FORMAT:
  SFT Tx-Power :<X>

SFP Rx-Power :<Y>

- **SNMP info Name and Location**
  FORMAT:
  DEVICE Location (Changed) :<NAME>
  DEVICE Name (Changed) :<NAME>

- **Regulatory profile**
  All allowed channels for a particular sub-band including EIRP/Transmit powers & also DFS scheme if applicable are shown.
  FORMAT:

Notice	[WLAN-2] 5 GHz Sub-band 2: 149, 153, 157, 161, 165; Tx power 27 dBm; EIRP 33 dBm; DFS not required
Notice	[WLAN-2] 5 GHz Sub-band 1: 36, 40, 44, 48; Tx power 14 dBm; EIRP 20 dBm; DFS not required
Notice	[WLAN-2] 2.4 GHz Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11; Tx power 28 dBm; EIRP 34 dBm;
Notice	[WLAN-2] Allowed Channels for 2.4/5 GHz Indoor-Only-Operation: Disabled
Notice	[WLAN-2] Operating on channel 11(20MHz) [EIRP 15 dBm]
Alarm	Link down
Notice	Interface INTRANET added, with IP address 192.168.70.100 and netmask 255.255.255.0 on VLAN 0, interface
Notice	Interface DMZ added, with IP address 0.0.0.0 and netmask 255.255.255.0 on VLAN 0, interface tag is 0
Notice	[WLAN-1] 5 GHz Sub-band 2: 149, 153, 157, 161, 165; Tx power 27 dBm; EIRP 33 dBm; DFS not required
Notice	[WLAN-1] 5 GHz Sub-band 1: 36, 40, 44, 48; Tx power 14 dBm; EIRP 20 dBm; DFS not required
Notice	[WLAN-1] 2.4 GHz Channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11; Tx power 28 dBm; EIRP 34 dBm;
Notice	[WLAN-1] Allowed Channels for 2.4/5 GHz Indoor-Only-Operation: Disabled

- **Temperature**
  FORMAT: Device reached a new Maximum tempreture of <X> degree Celcius

- **Security Warnings**
  Upon boot or affected configuration changes, there is a warning about insecure configuration
  FORMAT:
  Security Warning: <TFTP/Telnet/HTTP/WPA1/> protocol is active of IFX <logical interface>
  Security Warning: WEP/WPA1, WPA2 enabled on <Logical interface> <SSID Information>

3) Changes to default configuration

- **Client Bridge**
  Client Bridge Support is changed from “No” to “Yes”.

- **Direct traffic between stations**
  Direct traffic between stations is changed from “YES” to “NO”

- **WPA version**
  The default WPA encryption is changed from “WPA2” to “WPA2/3”.

- **Fast roaming**
  The default WPA2/3 key management is changed from “Standard” to “Fast roaming & Standard”

- **Encrypt management frames**
  The default setting to encrypt management frames is changed from “No” to “Optional”

- **Simultaneous roaming**
  Simultaneous roaming for both WLAN interfaces is disabled by default.

HiLCOS
The Hirschmann™ BAT Operating System

5. Bugfixes and improvements in version 10.34.5725-RU3

- Security fix XML file handling
- In case BAT-Controller-Virtual is upgraded to HiLCOS 10.34.5565-RU2 without active license, the WebIF will show a black screen. This issue is fixed in HiLCOS version 10.34.5725-RU3. Thus in case the black screen is observed it can be resolved either by upgrading the BAT-Controller-Virtual to HiLCOS 10.34.5725-RU3 or by activating the license
- WPA2 must use portVersion as 2 however there are implementations sending ProtVersion 1 for WPA2 which was causing the problem .

  Fix: Protocol version check corrected for specific scenario.
- For Singpore country profile the channel selection in 5GHz subband 3 was not working. This issue is fixed with 10.34.5725-RU3.

HiLCOS
The Hirschmann™ BAT Operating System

6. Bugfixes and improvements in version 10.34.5565-RU2

General

- Additional counters for “Beacon Timeout Events” is added.

Bugfixes in HiLCOS 10.34.5565-RU2

- OpenSSL vulnerability - CVE-2022-0778
- Security fix in L2Firewall
- Improved robustness in AP WLC connection within WLC Fast-Redundancy application.
- Improved client roaming handover times in case of AP failures in a roaming scenario.
- Malaysia country profile update: 40MHz bandwidth channel pairing is added for channel 165 and 169 in 5GHz band.
- Russia country profile update: 40MHz bandwidth channel pairing is added for channel 140 and 144 in 5GHz band.
- US country profile update: For BAT450-11ac devices the radio transmission power in 5GHz band 1 is increased to the regulatory limits.

7. Bugfixes and improvements in version 10.34.5402-RU1

- The China country profile has been implemented that channels from the U-NII-1 band and the U-NII-2A band are configurable in HiLCOS via the 5GHz subband-1 and subband-2. Since this way of implementation was not in line with other countries, the China profile is now harmonized.
  With version 10.34.5402-RU1, the channels from the U-NII-1 band and U-NII-2A band are both configurable within the 5GHz subband-1 setting.
- On BAT450-F devices misleading errors messages regarding optical Ethernet ports have been present. This is corrected with version 10.34.5402-RU1.
- For BAT450-F 11ac devices the transmission power was limited too much when operating in the US country profile on a channel in the 5GHz U-NII-1 band.

HiLCOS
The Hirschmann™ BAT Operating System

8. Overview on new features as of version 10.34.5250-Rel / 10.34.5402-RU1

WPA3 - State-of-the-art Wi-Fi security

The latest generation of Wi-Fi encryption - WPA3 (Wi-Fi Protected Access) - now offers you more security for your WLAN infrastructure. As the successor of WPA2, WPA3 offers important extensions and security features for small („WPA3-Personal“) and large networks („WPA3-Enterprise“). With HiLCOS 10.34, all Hirschmann BAT access points and WLAN routers support the new Wi-Fi security standard.

Client Management – for best-ever Wi-Fi

Client Management steers Wi-Fi clients to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes. The popular Band Steering and Client Steering, which so far were separate features, have now been combined and even operate without a WLAN controller if desired.

TLS 1.3

Support of the new TLS 1.3 protocol increases the security of device access via WEBconfig.

Enhanced Open

Thanks to the introduction of additional data encryption, Enhanced Open improves the security of clients in open Wi-Fis.

Elliptic Curve Digital Signature Algorithm (ECDSA)

IKEv2 now supports the Elliptic Curve Digital Signature Algorithm (ECDSA) authentication method. Shorter keys combined with high-efficiency encryption provide the same security.

IKEv2 split DNS

Split DNS allows DNS to resolve specific internal domains to a VPN tunnel, with other DNS requests using a public DNS server.

IKEv2 fragmentation

Fragmentation of IKEv2 messages (per RFC 7383) is handled by the VPN router itself, eliminating the need for the transport network to fragment IKE packets.

Enhanced client reservations in the DHCPv6 server

In the DHCPv6 server, client addresses or prefixes can now be assigned either by means of DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649).

LEPS-U & LEPS-MAC

Keep control of who is in your Wi-Fi. With LEPS-U, individual clients or entire groups each receive a unique Wi-Fi password for an SSID. Using LEPS-MAC, you additionally authenticate the clients by their MAC address—ideal for secure corporate networks.

WAN Policy-Based NAT

WAN Policy-Based NAT allows an easy assignment of static WAN IPv4 addresses to desired services. Due to a NAT action in the firewall rules internal addresses are masked behind a WAN address from the Internet access provider. Ideal for scenarios e.g. for the operation of mail servers and web servers with different WAN addresses.

OCSP responder – more power for Smart Certificate

Maximum security with VPN access: Smart Certificate is the easy way to create digital certificates with your Hirschmann device—without any need for an external certificate authority. This feature has now been extended to include the OCSP (Online Certificate Status Protocol) network protocol, which

enables clients to automatically and efficiently query the integrated CA for the status of X.509 certificates.

LISP (Locator / ID Separation Protocol) support

The Locator / ID Separation Protocol (LISP) is a new routing architecture. LISP allows the implementation of highly scalable networks with an integrated routing protocol, tunneling, and overlays. Ideal for service providers or enterprise networks.

Public Spot CSV import

Public Spot management is now even easier: Hotspot users are easily imported and exported by text file (CSV).

9. Detailed list of new features in HiLCOS 10.34.5250-Rel / 10.34.5402-RU1

General

- WEBconfig: Requests for the unencrypted site on port 80 are automatically redirected to the secure site (port 443). This behavior is activated automatically after a device reset.
- “Boot-Cause” is available as an environment variable.
- The RADIUS server supports user-defined RADIUS attributes per RADIUS user.
- A search on the CLI is possible via “find” command.
- Administrators from the table “Further administrators” do no longer have read- or write permission within this table.
- The readscript option “-o” suppresses the output of passwords within scripts.
- The new command “ssldefaults” can be executed from the CLI. After answering a confirmation promt, the SSL/TLS settings in all submenus of the current configuration are reset to default values.
- “clear“ command for deleting the current console display
- A target interface can now be specified for the CLI command “ll2mdetect“ (parameter “-i“).
- The output of the CLI command “show job“ now shows the complete CPU load.
- The DSCP tag for internal services can now be configured.
- Physical Ethernet ports are now enclosed within the Ifx- and lf-tables of the SNMP-IF-MIB.
- The timeout for UDP connections in the firewall was increased to 120 seconds.
- The SMTP client’s internally used SSL/TLS version can now be configured.
- Support for TLS 1.3 in WEBconfig
- Support for RSA-PSS signing in the SCEP-CA
- A loopback- / sender address is now configurable for use in the alive test.
- The table “Status / Config / Event log“ has been extended to 256 rows.

Routing & VPN

- The configuration logic of the IPv6 WAN interfaces has been changed.
- WAN Policy-Based NAT: WAN Policy-Based NAT allows address translation (masking) of connections based on firewall rules.
- OCSP responder/server for online certificate check
- Support for LISP (Locator/ID Separation Protocol)
- Configurable target port for IKEv2 and switchable encapsulation (UDP, HTTPS)
- Adaption of the IKEv1/IPSec default crypto algorithms to current standards
- Adaption of the TLS default crypto algorithms to current standards
- Adaption of the SCEP default crypto algorithms to current standards
- BGP: Support for LISP route redistribution
- BGP: The administrative routing distance can be configured per policy.

- Redistribution of RIP routes in BGP
- A particular sender address can be configured for DNS forwarding.
- Besides the Rollout wizard another four programmable WEBconfig wizards can be uploaded.
- The form for Dynamic VPN registration is no longer available
- Enhanced support for DHCP option 43 in the DHCPv4 server
- Support for DHCP option 82 in the DHCPv4 server
- A sender address (loopback address) can be configured via the DHCP relay agent.
- The function automatic WAN tag creation has been omitted
- Option for automatic WAN tag generation omitted.
- The switch for configuring the building of the IPSec SAs is no longer available. IPSec SAs are now built combined.
- Application routing and -control in the IPv4- and IPv6 firewall
- Evaluation of DSCP tags in the IPv6 firewall
- IKEv2 IPv6 CFG mode addresses can be assigned to clients based on the prefix allocated by the provider.
- Support for address allocation in the DHCPv6 server
- Support for IKEv2 cookie notification
- Support for IKEv2 Split DNS
- Support for IKEv2 fragmentation
- ECDSA support for IKEv2 authentication

Wi-Fi

- Support for 802.11r in WiFi client mode
- Support for 802.11k
- Support for 802.11v
- Support for WPA3
- Enhanced Open for improved client security in open Wi-Fis
- WLAN Client Management
  WLAN Client Management permanently directs Wi-Fi clients to the ideal access point and frequency band. As a consequence, this feature improves the quality of wireless networks regardless of their dimension. The popular, but so far separated functions Band Steering and Client Steering are hereby combined and provided even without operating a WLAN controller.
- LEPS-U
  LEPS-U (LANCOM Enhanced Passphrase Security - User) gives you the opportunity to specify an individual Wi-Fi password for an SSID for individual clients or whole groups.
- Public Spot user accounts / RADIUS user accounts can be imported and exported via CSV files.
- Public Spot with login after statement of agreement: The point of time for the the day account limits reset is now configurable.
- Active Public Spot sessions are terminated when deleting the user via the “Manage user” wizard.
- The former Public Spot user list has been removed and is no longer supported. Existing configurations are converted to RADIUS entries automatically.
- Support for a dynamic negotiation of the PoE power via LLDP instead of class-based
- The configuration item “Transfer only unicasts, suppress broad- and multicast” is now available for BAT-Controller devices.
- The controller based automatic radio field optimization now considers DFS channels, too.
- The e-mail notification for Wi-Fi events can now be enabled/disabled via button.
- The 802.11n Wi-Fi module rate adaption now considers the configured transmission power limitation when selecting rates.
- As an alternative to transmission power limitation the target EIRP (transmission power) is now configurable for Wi-Fi.
- Added a configuration option for reducing the sensitivity for received Wi-Fi packets
- Passwords for already existing users are now editable in the Public Spot user management.

- If a channel preference is configured in the 5 GHz band, the access point falls back to the preferred channel after radar detection and the expiration of the respective lock wait.

10. Comments & Limitations

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.

LIMITATIONS:

- When roaming, the BAT advertise MAC addresses belonging to the whole BRG-1 instead of only ETH-1 attached MAC addresses to new AP. As consequence addresses learnt on WLAN 1 are used as source address for the LLC broadcasts when WLAN-1 is roaming leading to a wrong address learning on all the switches in the LAN behind the AP.