WatchGuard Wi-Fi Cloud Release Notes

Latest Wi-Fi Cloud Update	31 May 2019
Release Notes Revision Date	31 May 2019
Current Wi-Fi Cloud Version	8.6.0-646

Introduction

WatchGuard Wi-Fi Cloud is a powerful, cloud-based, enterprise-level wireless management solution that enables you to configure and monitor your WatchGuard AP devices from anywhere. WatchGuard AP devices deliver fast, reliable wireless access while providing industry-leading wireless security, guest engagement, and analytic tools.

For a full description of Wi-Fi Cloud features and functionality, see WatchGuard Wi-Fi Cloud Help.

WatchGuard periodically updates the WatchGuard Wi-Fi Cloud service to provide additional functionality and resolve reported issues. For information on the enhancements and resolved issues in each update, see the Enhancements and Resolved Issues section.

Enhancements and Resolved Issues

Analyze 5.1 Update: 24 May 2019

- Facebook has recently implemented new compliance requirements about the storage and use of opt-in demographic profile information (age and gender) collected from guest Wi-Fi users. This data will no longer be available from the Wi-Fi Cloud-managed Facebook app, and profile information such as age and gender will appear as "Unspecified" in Analyze reports. For more information, see Impact of Facebook data privacy changes on WatchGuard Wi-Fi Cloud.
- A new Host field is available in the approval email sent during the Guestbook self-registration host approval work flow. This helps the default email approver know the context of the host for the guest registrant.
- Support for TLS versions 1.0 and 1.1 is disabled. TLS v 1.2 connections are now mandatory for administrator connections to Analyze and captive portal splash page connections.

Engage Update: 17 May 2019

Wireless clients that use the Chrome web browser v74.0.3729.131 or later can now successfully log in to a portal splash page.

To enable this change on the splash page after the update, you must open your splash page configuration in Engage and save the settings to the campaign (no changes required).

WatchGuard Wi-Fi Cloud Version 8.6.0-646: 16 April 2019

This is a maintenance release that provides firmware version consistency across all WatchGuard AP platforms.

- AP120, AP320, AP322, AP325, and AP420: 8.6.0-646
- AP125: 8.6.0-644.3

Engage Update: 18 March 2019

A display issue where image carousels could not be edited with some types of web browsers is resolved.

Analyze and Engage Update: 23 February 2019

- **Guest Passphrase for Web Form Captive Portals** — The Web Form captive portal now supports the ability for multiple guest users to log in to the portal with a single passphrase that you define in the portal configuration. This enables you to set up a captive portal splash page where guest users only need to type a passphrase to gain access.
- **HTTP Pre-Validation for Web Form Guest Users** — You can now pre-validate guest user credentials in the Web Form plug-in with your own third-party CRM validation system. You can configure an external HTTP end-point and define any number of custom fields to validate during guest user login.
- **Audit Logs and GDPR Compliance** — As part of GDPR compliance, you can now delete audit logs in Analyze based on the age of data.
- **Guestbook Enhancements for Self-Registration** — The self-registration option for the Guestbook plug-in has been enhanced to improve the work flow of guest user approval. You can now configure the host email address to receive only a notification about guests that self-register for access. Host approval is only required if you have configured that option.
- **Social Media Plug-In API Updates** — Facebook and LinkedIn plug-in APIs have been updated to support the most recent versions.

Resolved Issues

- Captive portal authentication with RADIUS now works correctly after you submit invalid credentials in the initial login attempt.
- A content spoofing vulnerability in Analyze has been resolved.

Previous Updates

WatchGuard Wi-Fi Cloud Version 8.6.0-644: 15 December 2018

- You can now add the same SSID profile across both radios of an AP if the SSID profile has dynamic VLANs configured.
- APs now correctly report PoE+ power usage when two or more APs are connected to certain types of PoE+ injectors.

Go Update: 2 December 2018

- Non-standard URLs and URL paths can now be correctly entered for the Redirect URL of a guest access portal in Go.
- Content filtering in Go now uses Neustar UltraRecursive DNS servers.

WatchGuard Wi-Fi Cloud Discover: 3 October 2018

Discover is a powerful cognitive Wi-Fi monitoring and troubleshooting tool that combines the power of large cloud data and advanced analytics intelligence to monitor the health of your Wi-Fi networks and automate Wi-Fi troubleshooting. Discover provides an easy-to-read big picture overview with the ability to narrow down the focus to specific details to identify and solve connectivity and performance issues on your network.

Discover provides these features:

- View a live snapshot of the client journey through several connection phases across all your locations
- Examine detailed client and AP events to quickly troubleshoot issues
- View baseline charts for client failures, application experience, and performance
- Receive alerts when a network anomaly occurs above baseline thresholds
- Perform client connectivity tests using WatchGuard APs with a third radio to continuously test if application experience, network performance, and Wi-Fi connectivity is within expected baselines
- Remote troubleshooting with live spectrum analysis and client debugging

Discover is available as a new feature on your Wi-Fi Cloud Launchpad Dashboard. For more information. see About Discover in the *Wi-Fi Cloud Help*.

WatchGuard Wi-Fi Cloud Version 8.6.0-634: 21 July 2018

New Features and Enhancements

- **Automatic Power Control Enhancements** — Automatic transmit power control thresholds are now configurable. You can configure the Minimum and Maximum Tx Power Range, Loudness Threshold, and Connectivity Threshold. Default values are provided for optimized power control.
- **Secure EoGRE Tunnels with IPSec** — 802.11ac Wave 2 APs (AP325 and AP420) now support tunneling with EoGRE over IPSec in either Tunnel or Transport mode. You can use IPSec in conjunction with EoGRE to provide encryption for encapsulated data to provide a secure and flexible VPN solution.
- **AP Auto Upgrade Enhancements** — You can now perform manual AP software updates outside of an expired automatic update window.

- **VoIP-aware Scanning** — You can now select VoIP-aware background scanning for 802.11ac Wave 2 APs (AP325 and AP420) to optimize high priority traffic during background scanning. Make sure that SSIDs added to the radio settings have the Application Visibility option enabled for traffic detection. If you enable VoIP-aware scanning on Wave 1 APs (AP120, AP320, AP322), this will disable background scanning on these APs.
- **Third-Party Analytics Integration Interval** — The minimum send interval for updating a third-party server with visibility analytics is reduced from 1 minute to 10 seconds. This enables you to send more immediate analytics data to the third-party server. You can configure an interval between 10 and 3600 seconds. The default interval is 600 seconds (10 minutes). This is configured in the Third Party Analytics Integration settings in a Device Template.
- **Full Client Isolation** — The client isolation option now provides complete wireless isolation between clients connected to different APs, the same AP, or different radios of the same AP. This is useful in typical guest Wi-Fi access deployments. With full client isolation, wireless clients also cannot communicate with wired-side hosts on the same network.
- **SSID VLAN Monitoring** — You now have the option to disable SSID VLAN monitoring if you do not want the AP to monitor VLANs corresponding to the SSIDs defined on the VLAN. This optimizes the use of IP addresses by not creating an automatic bridge interface for every VLAN on an SSID. SSID VLAN Monitoring is enabled by default.
- **Disable AP LED support** — You can now disable LED activity for 802.11ac Wave 2 APs (AP325 and AP420). This enables you to hide any visible LED activity on your APs for security reasons. This option is configured in a device template, and cannot be configured for individual APs.
- **HTTPS Redirection Support for Captive Portal** — Support is added for secure HTTPS redirection to a configured captive portal. A user that is connected to an SSID with a configured Captive Portal will now be successfully redirected to the portal when the user attempts to access an HTTPS site. HTTPS redirection is disabled by default.
- **Client Location Tag in Portal Request** — Wi-Fi Cloud now sends the location tag of a client in a portal redirect URL. This enables you to determine the location of the client that initiates the portal request.
- **No IP Address Required on VLAN for Captive Portal** — IP addresses are no longer assigned to the AP bridge interface. Previously the AP would receive a DHCP IP address on all VLANs that are configured in SSID profiles or configured in the Device Template as a VLAN to monitor.
- **Configuration Support for MU-MIMO** — You can now disable the MU-MIMO capability on 802.11ac wave 2 APs (AP325 and AP420). This option is useful for cases when clients encounter bandwidth issues when both SU-MIMO and MU-MIMO clients connect simultaneously to wave 2 APs.
- **Device Template Migration to Consolidated Template** — You can now migrate your existing AP model specific device templates to the consolidated model configuration template.
- **DCS Enhancements** — Dynamic Channel Switching (DCS) has been optimized for high density wireless environments to prevent frequent channel changes.

Analyze Enhancements

- **Reduced Portal Downtime during Upgrades** — Captive Portal splash page downtimes are greatly reduced during Wi-Fi Cloud maintenance and upgrades to minimize impact to Wi-Fi users.
- **Pre-validation for Guest Login** — Support is added for additional pre-validation for guest users that log in to a Wi-Fi network. You can configure an external HTTPS end-point for use with the SMS plug-in and define any number of custom fields to validate during guest login.

- **GDPR Compliance** — The default captive portal splash pages designed by the Engage application, including logo and terms and conditions usage, are modified to be compliant for GDPR.

Resolved Issues

- APs can now receive an IP address and no client connection issues occur when a SSID is configured with more than 32 VLANs (including dynamic VLANs).
- An AP420 in Cloud Integration Point (CIP) mode can now integrate successfully with a configured controller to allow import of APs.
- Cisco WLC integration now supports AIR-AP1815I and AIR-AP1832I access points.
- The country of operation for WatchGuard APs is defined by WatchGuard geolocation services when an AP first connects to Wi-Fi Cloud. The country of operation is no longer displayed anywhere in the Manage configuration.
- Ethernet link issues and communications interruption for APs and their connected clients no longer occur.
- A problem that caused some clients to display as active after it had disconnected from an AP has been resolved.
- SSH IP whitelisting now correctly works on an AP420 configured in Cloud Integration Point (CIP) mode.
- Email alerts are now delivered to the configured email address for soft mobile hotspot AP events.
- The maximum length of a host name for a client under DHCP option 12 has been increased from 16 to 64.
- The **Zip Before Email** setting for scheduled reports now works correctly.
- The **Guard Interval** option in a Device Template in Manage is renamed to **Long or Short Guard Interval**.
- The vulnerabilities identified in CVE-2017-11176 and CVE-2015-4000 are resolved.

WatchGuard Wi-Fi Cloud Version 8.5.0-658: 31 May 2018

- PoE+ power detection issue resolved for AP325 devices.
- Added support for the AP125.
- Resolved issues with Google integration by adding support for Unicode handling for Google JSON files.

WatchGuard Wi-Fi Cloud Update: 9 March 2018

- Updated terms for Norton ConnectSafe content filtering in WatchGuard Go. Norton ConnectSafe is intended for use by small deployments. For large enterprise deployments, you must subscribe to Norton ConnectSafe Enterprise.
- Removed Google+ social media authentication plug-in for splash pages in Analyze and Engage.

WatchGuard Wi-Fi Cloud Version 8.5.0-646: 26 January 2018

New Features and Enhancements

- **Automatic Transmit Power Control** — APs can now dynamically adjust and optimize their transmit power in coordination with other APs to provide optimal coverage and minimize interference. Transmit power adjustments automatically occur depending on the transmit power and RSSI of neighboring APs, AP failures, and newly deployed APs in the vicinity. This feature requires that Background Scanning be enabled on APs or the use of AP420 devices with a third scanning radio.

- **Cloud Integration Point** — Cloud Integration Point (CIP) enables the integration of WatchGuard Wi-Fi Cloud with on-premise WLAN controllers such as Aruba Mobility Controller, Cisco Wireless LAN Controller (WLC), and HP Multi-Service Mobility (MSM) Controller. CIP enables Wi-Fi Cloud to retrieve information about devices managed by these third-party controllers and use this information for Wireless Intrusion Prevention System (WIPS) classification and location tracking of devices. ArcSight ESM and Syslog integration with CIP enables you to use your own existing infrastructure to manage Wi-Fi Cloud events and logs. CIP integration is only supported with AP420 devices.
- **Consolidated Device Templates** — Device templates are now configured independently of the AP hardware platform type. All AP models are now managed through a single configuration within the template instead of having a separate configuration for each device type. Model-specific settings are only used by the AP model to which the settings apply.
- **Background Scanning and WIPS** — Background scanning on a radio has now been decoupled from WIPS security scanning. You can enable Background Scanning for use in radio communications optimization without enabling additional WIPS scanning. To enable security scanning, select **Wireless Security Features** in the Background Scanning advanced settings in a device template.
- **RADIUS Profiles** — For easier RADIUS configuration, you can now create RADIUS configuration profiles that can be applied to any feature that uses RADIUS instead of having to configure the same RADIUS settings in each SSID profile. After the upgrade, any existing RADIUS configurations will be converted to RADIUS Profiles and applied to the appropriate SSIDs.
- **RADIUS MAC Authentication Enhancements** — If a client's secondary authentication fails, the client can now be assigned either an SSID Profile or a Role Profile. If a client successfully completes secondary authentication, they are assigned a Role Profile.
- **AP Upgrades over Port 443** — AP upgrades now occur securely over TCP port 443. If this port is unavailable or blocked, the upgrade process will use TCP port 80.
- **AP Firmware Downgrade** — You can now update the firmware of an AP to a previous firmware version.
- **Suspicious AP Monitoring** — You can monitor APs that you do not manage by marking them as "Suspicious". This allows you to track performance data for the AP.
- **Splash Page Authentication Enhancements** — Wireless clients no longer need to re-authenticate to a captive portal splash page when an AP reboots or while the client roams between APs.
- **Enhanced Bridging Client Detection** — Advanced techniques have been added to detect if authorized clients are bridging between the authorized network and another network.
- **DFS Channel Enhancements** — Added DFS channel support for the AP420. DFS channels on all AP models are now disabled by default. You must explicitly select DFS channels in a device template to use them.
- **AP325 Support** — Support added for the AP325, an 802.11ac 2x2 MU-MIMO Wave 2 access point with a third scanning radio ideal for low to medium density deployments.
- **Pre-configured Country Codes for Israel and Egypt** — AP325 and AP420 devices sold into the Israel and Egypt markets can now be configured with their respective country codes during the manufacturing process. The country code is preserved during factory reset.
- **Google+ Support Deprecated** — Google+ authentication for portal splash pages is no longer available because Google+ has been deprecated by Google.

Resolved Issues

- The AP420 now supports device template configurations for Kazakhstan.
- An issue with the number of RADIUS accounting packets sent is resolved.
- The application bandwidth limit event notification to a client is no longer generated after a client has disconnected from an AP.
- AP420 devices configured in non-root mesh mode no longer reboot intermittently when there is no SSID profile configured on the mesh radio.
- Sub-applications of an application (for example, Skype File Transfer or Facebook Video) are now correctly detected and displayed by Application Visibility.
- Kernel panic with cookie allocation failure error is now resolved on AP320 devices.
- The client connectivity test on the third radio of an AP420 is now supported when 802.11r is enabled on the target AP.
- Data rates for clients are now correctly displayed with distinctions between unicast packet data and multicast/broadcast packets.
- APs now correctly send NAS IP addresses for additional clients after the first client in the interim accounting update for RADIUS portal authentication.
- RSSI values for certain clients are now correctly displayed.

WatchGuard Wi-Fi Cloud Version 8.3.0-657 — KRACK WPA/WPA2 Vulnerability Update: 15 October 2017

This release is a security update to address the recent WPA/WPA2 key reinstall vulnerabilities reported by researchers. Vulnerabilities have been discovered in how clients and APs implement state machines in software for WPA/WPA2 temporal key generation and transportation handshakes. The vulnerabilities can be exploited by manipulating certain handshake messages over the air. The exploit results in the reuse of some packet numbers when handshakes are performed.

These vulnerabilities occur in both AP software and client software implementations. WatchGuard has addressed these vulnerabilities for Wi-Fi Cloud and AP software in version 8.3.0-657. Vulnerabilities for clients must be addressed by updating the client OS software to a version that includes fixes to address these vulnerabilities.

Until all clients are updated, WatchGuard Wi-Fi Cloud APs can mitigate these client vulnerabilities by blocking handshake messages that can potentially exploit clients, and force clients to reauthenticate. In version 8.3.0-657 and higher, you can enable the **Mitigate WPA/WPA2 key reinstallation vulnerabilities** option for WPA2 and WPA/WPA2 mixed mode security settings in an SSID Profile to activate this handshake blocking and force clients to reauthenticate. This option is disabled by default.

This mitigation logic can trigger for other similar dropped packet symptoms, for example, natural frame errors during a handshake, or dropped packets when a client roams from one AP to another or roams beyond the range of the current AP connection. This can result in some client authentication connections to fail and be reestablished. WatchGuard recommends you enable this mitigation feature until you have updated all your client software to address the client vulnerabilities.

WatchGuard Wi-Fi Cloud WIPS (Wireless Intrusion Prevention System) with dedicated WIPS sensors provide zero-day protection against these vulnerabilities if the **MAC Spoofing** option is enabled in your Intrusion Prevention configuration and prevention is enabled. WIPS will block the exploit until you upgrade APs and clients.

WatchGuard Wi-Fi Cloud Update: 4 August 2017

- Resolved issue where Dashboard charts did not correctly display data after the Wi-Fi Cloud 8.3 upgrade.

WatchGuard Wi-Fi Cloud Version 8.3.0-648: 30 July 2017

New Features

- Role Based Control – Use role profiles to enforce restrictions (VLAN assignments, Bandwidth controls, Firewall rules, redirection URLs) on users and clients.
- Google Integration and Device Authentication – Integrate with Google for user authentication, device authorization, and role profile assignment.
- RADIUS MAC Authentication – Use RADIUS for client authorization and role profile assignment.
- Unified Client Steering – Enhancements to smart steering, band steering, 802.11k/v roaming support, and load balancing to optimize client load and band utilization across APs.
- Application Firewall – Create rules to allow or block specific applications on an SSID.
- MAC Address Blacklist / Whitelist – Create a list of whitelist/blacklist MAC addresses for an SSID.
- Enhanced Auto Channel Selection – Minimize interference from other APs and from non-Wi-Fi sources to optimize your wireless radio environment.
- Improved Smart Device detection – Improved detection of smart devices and operating systems of clients.
- Automatic VLAN Monitoring – Automatically monitor VLANs added by an SSID or your own user-configured VLANs.
- Broadcast / Multicast Control – Block broadcast/multicast packets on your wireless network and create exemptions for specific applications (Video, Bonjour, etc.)
- IGMP Snooping – Optimize multicast video streaming traffic.
- Engage / Analyze Enhancements – Marketing opt-in and opt-out options for portal plug-in settings. Track Twitter Follows and Facebook Likes for your portal.
- AP420 Support – High performance enterprise 4x4:4 MU-MIMO 802.11ac Wave 2 access point with dedicated third radio for scanning and over-the-air attack prevention.

Enhancements

- Application Visibility has been disabled on AP120, AP320, and AP322 platforms. You can now only enable Application Visibility on AP420 devices.
- A new option is added to allow the transmission of Inter AP coordination packets through an EoGRE tunnel when remote bridging is enabled.
- Added support for the new vendor OUI prefixes. Wi-Cloud AP devices now use prefix 88:B1:E1.
- Improved and faster detection of Internet connectivity loss.
- Enhanced stability to detect and resolve SSID issues such as client unable to see an SSID, and internal application level issues.
- Auto channel selection is enhanced to ensure that AP devices do not start auto channel selection at the same time.
- You can now view power status indication (including PoE, PoE+, and DC power) for AP420 devices.
- You can now disconnect multiple clients simultaneously in Manage.
- There is no longer a character restriction on a Walled Garden site entry in an SSID Profile.
- Failsafe mode enables problematic and unresponsive AP devices to remain connected to the cloud with limited connectivity to allow troubleshooting by WatchGuard Technical Support.

- On the Events page, you can now use the Delete Filtered Events option to delete all filtered event results.
- All Events in the Performance category are now deprecated.
- LLDP support is added.
  - To ensure Cisco Enterprise switches provide appropriate power to AP420 devices, you must enable LLDP on the switch.
  - Disable static allocation of maximum power of 30W if this was previously enabled.

Resolved Issues

- Resolved several issues with the loading of the Manage UI.
- AP120 devices no longer incorrectly transmit at low power on the 2.4 GHz band in Europe, China and India regions.
- Incorrect MAC spoofing alerts are no longer generated when AP devices are in AP/Sensor combo mode.
- AP classification and MAC address corruption no longer occur when background scanning is enabled.
- The vulnerability described in CVE-2016-5195 (Dirty COW) is resolved.
- Legacy insecure cipher suites in 3DES used in Manage are removed.
- A captive portal RADIUS user name entered when an AP device was in offline mode is now correctly updated after the AP device goes online.
- Several issues with the HTTP content analytics feature are resolved.
- Clients no longer experience connectivity issues with externally hosted splash pages and RADIUS authentication.
- Connection log issues no longer occur for inactive clients.
- You can now correctly disable the remote bridging option in an SSID profile configured with both remote bridging and Inter AP coordination.
- Connectivity tests that incorrectly interpret the gateway MAC address no longer cause AP devices to be classified as Rogue.
- Policy-based routing is now implemented for VLANs configured on all SSIDs to prevent incorrect VLAN tagging and connectivity issues.
- The device upgrade procure has been optimized to provide faster device upgrades.
- The move location procedure has been optimized to improve the time it takes to move an AP device to a different location.
- Slow Wi-Fi Cloud server response during a simultaneous upgrade of a large number of APs no longer occurs.
- Intermittent SSID unavailability that resulted in client connectivity issues no longer occurs.
- Clients now correctly authenticate with a RADIUS server and receive an IP address when dynamic VLANs are configured on an SSID profile.
- Incorrect VLAN tagging observed on an AP wired interface for ICMP error messages no longer results in incorrect information about valid network configurations.
- In certain cases, AP vendor names were not recognized by Wi-Fi Cloud.
- Manage UI responsiveness is improved when viewing a large number of clients.
- Client MAC address 00:03:7F:00:00:00 is a special client that was visible to a large number of APs that consumed resources for visibility analytics. This special MAC address is no longer part of visibility analytics data.

Historical performance data for APs will be reset after the upgrade to Wi-Fi Cloud 8.3.

WatchGuard Go Update: 8 June 2017

- Added support for new AP device models in the default device template created by WatchGuard Go.

WatchGuard Analyze Update: 21 May 2017

- Resolves a data syncing issue that affected analytics data.

WatchGuard Wi-Fi Cloud Version 8.0.581: 29 April 2017

- Added support for the AP420 device.
- If an AP device is detected as operating from an unsupported region, the operating region for the AP device will be set to the USA (country code 841).
- AP device software upgrades can now happen over port 443 in addition to port 80.

After an AP device upgrades to version 8.0.581, the device will undergo an extra reboot in addition to the reboot that is part of the upgrade process.

WatchGuard Analyze Update: 25 March 2017

- Facebook APIs are updated to support the latest version for Facebook social media portal authentication

WatchGuard Go Update: 4 March 2017

- In Go, you can now click anywhere on the ON/OFF switch to enable and disable Wi-Fi networks
- Alarm notifications are removed from Go

WatchGuard Wi-Fi Cloud Version 8.0.566: 25 February 2017

- In certain cases, the WatchGuard Manage service UI did not correctly load, and sometimes displayed the error message "An error has occurred in getting managed SSIDs".

WatchGuard Wi-Fi Cloud Version 8.0.564: 11 February 2017

- You can now configure the default country code in Engage splash page plug-in settings
- Country names are now included with country codes in Engage splash page plug-in settings
- Stability enhancements in AP firmware
- Added support for the AP322 device model

Known Issues and Limitations

You can find known issues for WatchGuard Wi-Fi Cloud, including workarounds where available, on the Technical Search > Knowledge Base tab. To see known issues for Wi-Fi Cloud, from the **Product & Version** filters, select **Wi-Fi Cloud**.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at https://www.watchguard.com/wgrd-support/overview. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

	Phone Numbe
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375