WatchGuard Wi-Fi Cloud Release Notes

Latest Wi-Fi Cloud Update	7 April 2023
Release Notes Revision Date	7 April 2023
Current Wi-Fi Cloud Version	13.0.0-67

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 a full list of the enhancements and resolved issues in each update, see the Enhancements and Resolved Issues section, or review the *What's New* presentations for each release on the Wi-Fi Cloud documentation page.

Enhancements and Resolved Issues

For more information about new features, go to the What's New in Wi-Fi Cloud 13.0 PowerPoint.

Latest Release

Wi-Fi Cloud 13.0.0-67: 7 April 2023

New Features and Enhancements in v13.0

- The legacy Manage application is now deprecated and no longer appears in the Launchpad. You must perform all Wi-Fi network management, configuration, and monitoring in Discover. If you still require access to Manage, click the WatchGuard Logo in the top-left corner of the page in Discover, then select the **UI** link in the *Service Build* section. Manage is also still available from the direct URL to your regional server (*mwm-wgxxxxx.watchguard.cloudwifi.com*)
- The Device Settings configuration is now located in the **Configure > Device** menu. Previously, Device Settings were located in the **Configure > WiFi** menu. The Device settings page now include:
  - Device (General device settings)
  - Security (VLAN monitoring, WIPS settings)
  - Wi-Fi Radios (Wireless radio settings)
  - IoT Radios (Bluetooth settings)

  - LAN Ports (AP interface settings)
- RADIUS, Tunnel, and Role Profile configurations are now located in the **Configure > Network Profiles** menu.
- You can now monitor network switches that connect your APs to the network from the **Monitor > Switch** menu. This feature uses LLDP to monitor details such as the switch vendor name, number of APs connected to the switch, and number of clients connected to the switch through a connected AP.
- You can now scan and detect nearby Bluetooth devices on the AP225W, AP325, and AP327X. To enable Bluetooth Scanning, go to **Configure > Device > Access Points** and select the **IoT Radios** tab. Detected Bluetooth devices are available on the **Monitor > WIPS > Clients** page in the **Bluetooth Clients** drop-down list.
- You can now configure a VXLAN over IPSec tunnel for an AP on the **Configure > Network Profiles > Tunnel** page. This adds an extra layer of security to the VXLAN packets to protect client's data from interception or modification.
- Spectrum analysis now includes additional charts for Signal Strength, Duty Cycle, and Spectrum Density. You can run Spectrum Analysis from **Monitor > WiFi > Access Points** in the actions for an AP with a third radio (AP225W, AP325, and AP420). Spectrum Analysis is no longer available from the **Troubleshoot** menu.
- You can now use DHCP Fingerprinting-based access control on the AP420 to allow or deny client connections to an SSID based on the OS type of the device. To configure DHCP fingerprinting, go to **Configure > WiFi > SSID**, select the **Access Control** tab, then select **DHCP Fingerprinting based Access Control**.
- The Access Point logs now show the factors that cause an AP to change its channel based on ACS, DCS, and DFS events.
- The baseline charts on the **Monitor > WiFi > Clients > Client Details** page now include charts for Retry Rate and RSSI.
- Wi-Fi Cloud now detects high DHCP/AAA/DNS server latency for client root cause analysis.
- You can now view a Channel Map chart that shows the number of APs and clients seen by the AP on each channel. To view the Channel Map, select **Monitor > WiFi > Access Points > AP details**, then select **Channel Map** from the drop-down menu in the **Spectrum Occupancy** chart.
- The **Monitor > WiFi > Access Points** page now includes an Access Point Explorer that helps you view the distribution of APs by attributes such as model, software version, and status.
- The **Monitor > WiFi > Clients** page now includes an Client Explorer that helps you view the distribution of clients by attributes such as associated SSID, OS version, and status.
- Enhanced Managed WiFi Device Inventory, WiFi Access Point Details, and Client Connectivity reports are available on the **Reports** page.
- 802.11r settings are moved from the **Security** tab to the **RF Optimization** tab in the SSID settings.
- In the Captive Portal settings of an SSID, you can now select a new SAML authentication plug-in to authenticate clients with an identity provider (IdP).
- You can now use Scheduled mode with Automatic Channel Selection (ACS) that enables you to schedule ACS scans up to two times a day.
- In the 5 GHz radio device settings, you can now select the **Use DFS history in channel selection** option to optimize automatic channel selection based on the DFS detection history.
- You can now import a list of Authorized APs, Rogue APs, Authorized Clients , Guest Clients, Rogue Clients, and Managed Devices in **System > Advanced Settings > Import Devices**.

- You can now add additional CoA server IP addresses and a shared secret when you configure Enterprise RADIUS authentication. This enables organizations with load balancer deployments to add additional CoA server IP addresses to directly send CoA requests from RADIUS servers to APs. APs accept the authentication and authorization messages coming from a load-balancer server and CoA requests from RADIUS servers.
- Role Profiles now support redirection of clients to a URL returned by a RADIUS server.

Resolved Issues in v13.0

- Client connectivity VoIP and throughput tests fail if client isolation is enabled on an SSID. *[AP-433]*
- AP125 and AP325 no longer reboot after an out of memory kernel panic message. *[AP-811]*
- AP125 and AP325 no longer reboot due to an ARP flood. *[AP-1114]*
- The Authentication column in the Active SSIDs page in Discover now correctly shows the authentication type for an SSID. *[AP-1148]*
- APs no longer lose connectivity and reboot with an "Ethernet Stuck. Rebooting device" log message. *[AP-1171]*
- APs in a mesh network no longer frequently reboot. *[AP-1180]*
- Users no longer have to reauthenticate with a Captive Portal when roaming. *[AP-1193]*
- Link aggregation now works correctly on the AP420. *[AP-1243, AP-1356]*
- Wi-Fi clients can now correctly redirect to a Captive Portal for authentication. *[AP-1244]*
- The AP web server on TCP port 8080 now requires TLS 1.2 or higher. *[AP-1370]*
- Users are now correctly redirected after successful Guestbook self-registration to a Captive Portal. *[AP-1352]*
- The transmit power of the AP225W is now correctly set in the UNII-3 band.
- L2TIF functionality now works correctly on the AP125, AP225W, and AP325.
- VoIP tests no longer fail when dynamic VLAN configuration is enabled on an SSID.
- The RADIUS Accounting Stop Delay timer now works correctly.
- The Proximity View page for a Wi-Fi client now correctly includes access points that operate in WIPS sensor-only mode and are tagged at different locations.
- Packet captures now correctly handle missing packets due to interference.
- An AP now correctly discovers the Path MTU to a configured tunnel endpoint when the configuration changes on the secondary endpoint.
- An authenticated wireless client is no longer redirected back to a Captive Portal page if the client's IP address changes.
- The use of special characters in a device name no longer causes a device reboot.
- Application monitoring now correctly generates data for Zoom and Teams calls initiated with a web browser.
- Visibility analytics data upload in JSON format to a third-party server no longer fails when you configure a high Send Interval.
- RADIUS accounting is now correctly restarted for Captive Portal clients when the clients reconnect to an AP.
- The DHCP server service for an SSID no longer incorrectly restarts.
- Delays no longer occur when APs send third-party analytics data.
- DHCP lease data now correctly synchronizes between neighboring APs.
- Captive Portal redirection now works correctly if you update the SSID configuration.
- Zendesk application tests for client connectivity now work consistently.
- The live client debugging logs for roaming clients now have the correct AP name.
- Bluetooth scanning now correctly detects Apple Watch devices.
- Application data is now correctly generated for YouTube.
- Windows 11 clients are no longer misreported as Windows 10 clients.

- LLDP packet errors no longer occur if more than 80 VLANs are configured on an AP.
- The downstream QoS option now works correctly when the priority flag is set to Fixed.
- Auto transmit power control events no longer appear in the AP event logs when there is no SSID enabled.
- Client data traffic is no longer blocked when client isolation is enabled and the client is assigned a Dynamic VLAN.
- Client information for the Poor Application Experience baseline chart is now correctly displayed.
- Discover is no longer unresponsive when you delete a large number of reports.
- On-demand reports now show the correct data and time.
- The horizontal scroll bar now correctly appears for the client connection logs widget.
- The application usage time, number of sessions, and number of clients are now correctly displayed in the Application Dashboard and Application details pages.
- The RF Heatmap is now accessible to a user with the operator role.
- The Authentication column now shows the correct data in the **Monitor > WiFi > Active SSID** page.
- The Last Booted At column in a list of APs now correctly shows both the date and time of the last reboot.
- A custom splash page hosted by Analyze is now correctly viewable in Discover.
- The auto-populated passphrase in a Client Connectivity Test profile is now correctly retained when you select an SSID.
- The device properties panel for APs imported with WLC integration now opens correctly on the AP details page.
- Automatic channel selection now correctly selects a channel based on neighbor WatchGuard AP visibility and RSSI detection.
- APs no longer reboot if the link of the primary Ethernet interface goes down or is reconnected, even when link aggregation is enabled.
- AP125, AP225W, and AP325 devices no longer reboot after low memory conditions.
- The regulatory domain for 802.11ac Wave1 APs is now correctly displayed in Discover.
- Beacons are no longer transmitted at 6 Mbps when you set the data rate for multicast, broadcast, and management traffic to values greater than 36 Mbps.
- Discover no longer shows an authentication failure when a new client successfully completes RADIUS-based MAC Authentication onboarding through a Captive Portal.
- An AP now correctly discovers the Path MTU to a configured tunnel endpoint after you change a Network Profile configuration.
- AP reboots due to a kernel panic in "ieee80211_complete_wbuf_sensor" are resolved.
- Incorrect subnet masks are no longer reported for certain VLANs in Discover.
- APs now correctly detect the client OS for the Samsung Galaxy S10 and for iOS devices version 15 and higher.
- APs can now successfully resolve a RADIUS server FQDN if the length is more than 200 characters.
- Wi-Fi clients are no longer disconnected if a VLAN is assigned through a Role Profile with RADIUS-based authentication and the assigned VLAN is different from the SSID VLAN.
- In rare cases, the channel width of an AP did not change after you saved the configuration.
- Channel change events due to radar detection now correctly show the current event data instead of the previous change.
- An AP now correctly changes the secondary 80 MHz channel if radar is detected.
- Speed tests are now deprecated in Client Connectivity Tests and the AP CLI.
- The OS for a MacOS client is now correctly identified in the Client Details page.
- A Windows 11 client is now correctly reported in the Client Details page.
- Bandwidth limits for uploads and downloads received from a CoA-Request are now correctly applied in a Role Profile.

- An AP now correctly selects a DFS operating channel after a timeout when radar is detected on all available candidate channels.
- Transmit power change events are now correctly reported.
- An AP no longer loses network connectivity when all radios are disabled.
- Japanese characters are now supported in the encoding of a URL in a Captive Portal.
- An AP no longer selects a previously saved DFS channel that is not part of the ACS channel candidate list after a DFS timeout.
- APs no longer go into failsafe mode after a cloud agent crash.
- WIPS sensor communication now recovers faster after an AP reboots with the negotiated power source lower than required.
- Channel change events are now correctly generated when radar is detected on a DFS channel.
- The cloud agent on an AP no longer crashes due to invalid memory access.
- In rare cases, an AP might constantly reboot due to a "kernel panic atn_apc_buffer_ handler+0x4c/0x454 [umac]".
- Pub key failures no longer occur when you correctly create a Secondary IPSec tunnel.
- The RF Utilization in the radio list now correctly matches the actual channel utilization.
- Clients no longer terminate an EAP session with an EAPOL log off message after a successful authentication.
- High CPU utilization no longer occurs when multiple streaming telemetry sessions are in progress.
- APs no longer reboot with many clients in a video call.
- SSID now correctly broadcast after a radio configuration change when a high number of clients are connected to the radio.
- A data range no longer appears for instantaneous reports.
- You can now correctly enable radios when an AP has no active SSIDs.
- Client event logs now correctly display client role details if the role contains special characters.
- You can now correctly download a packet trace pcap file in the Safari browser.
- Device customization is no longer disabled for displayed inactive devices.
- The AP details page no longer displays "Fetching data..." for Clients by Avg. Data Rate and Channel Utilization if a device's tagged location does not have active SSIDs.
- The system now correctly checks for duplicate VLAN names for a Named VLAN and Location-based VLANs.
- The insights for ACS event logs now correctly appear.
- The RF explorer channel occupancy chart now correctly displays the channel width for BSSIDs.
- The client count in the global counter now correctly matches the number of clients that appear in other parts of Discover.
- You can now save a secondary RADIUS profile for the RADIUS plug-in an SSID Captive Portal.
- You can now correctly save an ArcSight Server configuration with a valid primary CIP.
- The Retry Rate, RF Utilization, and Channel Width now show correct values for inactive radios.
- An SSID can now be correctly enabled if unicast data rates are saved in combination of 6/9 Mbps for the 2.4 GHz band.

Previous Updates

Analyze Update: 25 March 2022

New Features and Enhancements

- You can now use Okta for social media plug-in authentication for captive portal users. For more information, see Create Social Media Plug-in Apps in the Wi-Fi Cloud help.
- The Analyze server database is upgraded for improved performance.
- Engage web application services are integrated with Analyze for improved security.

Resolved Issues

- In Discover, you can now correctly copy an SSID with Captive Portal enabled.

Wi-Fi Cloud 11.0.0-36: 17 December 2021

New Features and Enhancements

- Wi-Fi Cloud now provides improved visibility for scheduled device updates:
  - New Scheduled Update icon that shows the version for the next scheduled update.
  - Additional columns in **Monitor > WiFi > Access Points** indicate the last successful update and the next scheduled update window.
  - Scheduled Update Notification in the network counters at the top of the page.
  - You can now specify firmware update schedules in 12-hour format.

In Wi-Fi Cloud v11.0 and higher, the AP120, AP320, and AP322 no longer appear in the firmware update model list because the latest firmware version they can use is v8.8.3.

- The Capability column in **Monitor > WiFi > Clients** now indicates if a client is 802.11ac Wave 1 or Wave 2.
- You can now flash the AP LEDs from the **Monitor > WiFi > Access Points** page when you select an AP action.
- You can now configure custom applications for the Application Experience widget on the Applications Dashboard.
- You can now apply AP Offline mode settings for WIPS Device Classification and Intrusion Prevention Policy in **Configure > WiFi > Device Settings > Security**.
- You can now use set a custom password in RADIUS MAC authentication for an SSID.
- You can now define RADIUS servers by a hostname in addition to an IP address.
- You can now define up to 3 additional backup RADIUS servers in addition to the primary RADIUS server when you configure RADIUS authentication.
- You can now download a device list inventory from the **Monitor > WiFi > Clients**, **Monitor > WIPS > Access Points**, and **Monitor > WIPS > Clients** pages.
- You can now place unmanaged authorized devices on a floor plan so you can view the heat map for these devices.
- Real-time visualization is now available in Discover for AP and client troubleshooting, with enhanced support to identify root causes for wireless client connectivity issues and troubleshoot new clients not yet seen by Wi-Fi Cloud.
- The Dynamic VLAN limit on an AP has been raised from 64 to 128.

Resolved Issues

- The FragAttacks vulnerabilities for the AP125, AP225W, AP325, AP327X, and AP420 are resolved in AP firmware 11.0.0-36. For more information, see WatchGuard Wi-Fi products and the FragAttacks vulnerabilities.
- A remote code execution vulnerability in the Apache Log4j2 utility (CVE-2021-44228) is resolved.
- Clients no longer experience association issues on SSIDs with NAT or a Captive Portal enabled. DNS replies are now correctly passed from the AP to the client. *[AP-757]*
- Clients now correctly obtain a DHCP IP address on an SSID with 802.1x authentication and Dynamic VLANs enabled. *[AP-996]*
- AP LED indicators now correctly indicate when WIPS sensors are powered with lower 802.3af PoE power instead of 802.3at PoE+.
- Discover now correctly shows a successful RADIUS-based MAC Authentication onboarding event.
- In some cases, the use of Application Visibility caused rare AP reboots.
- The tunnel status and event logs are now available in Discover when the tunnel profile name is greater than 32 characters.
- Dual-radio APs with VoIP-aware scanning are no longer reported as clients by Discover.
- The client OS for devices on iOS versions greater than 14 and the Samsung Galaxy S10 are now correctly detected.
- FaceTime calls with a host on a mobile network are no longer misclassified as WhatsApp Voice calls.
- The Hangout application is now correctly detected over TCP when the QUIC protocol is used.
- Client connectivity application tests for instagram.com now work correctly.
- The client event log now correctly displays the VLAN Name received from the RADIUS server.
- The AP no longer detects MS Teams traffic as Skype P2P traffic.
- The Internet throughput Client Connectivity Test now shows correct values.
- NAT now correctly works on an SSID when the AP is unable to obtain an IP on the configured VLAN.
- Captive portal authentication no longer fails if the portal is configured with RADIUS and the NAS identifier contains fields with a "\" character.
- Discover now correctly shows if there are no APs available that can become a root node in a mesh network.
- Incorrect values for a third-party hosted captive portal configuration in Discover are no longer applied if you navigate to another SSID configuration tab.
- Client packet captures are now correctly captured by APs that do not have a multi-function radio.
- Accessing the SSID configuration tabs in Discover no longer results in configuration change entries in the user action logs.
- Channel width information is now displayed correctly in RF Explorer for a specific BSSID.
- A highlighted band in RF explorer for a 5 GHz radio is now correctly displayed when auto-channel selection is configured.
- 80 + 80 MHz non-contiguous channels are no longer displayed as a contiguous channel in RF Explorer.
- The AP action drop-down menu no longer persists in Discover after an AP is deselected automatically after two minutes.
- The Access Point Debug Logs in the Troubleshoot menu are now visible when the location is changed in the location navigator.
- AP groups now correctly display the access points assigned to the group.

- The correct Candidate Channels now appear when the regulatory domain is set to a country other than the United States.
- You can now correctly save Access Control settings when Role Based Control is enabled and an external RADIUS server is enabled on a Captive Portal.

Wi-Fi Cloud 10.0.0-124: 9 July 2021

New Features and Enhancements

- From the **Monitor > WiFi > Access Points** page in Discover, you can now view additional AP health and performance widgets when you select a specific AP:
  - Spectrum Occupancy and RF Explorer
  - Channel Utilization
  - CPU and Memory Utilization
  - Average Data Rate Baseline Chart
- You can now use VLAN names to map a VLAN name to one or more VLAN IDs. This enables you to use different VLAN IDs at multiple locations for the same SSID.
- You can now monitor the application experience for web-based enterprise applications, such as cloud services, web-based email and office applications, online drives, and custom applications that you define.
- You can now add floor plan images to location folders, add notes to floor plans, and drag and drop subfolder locations on to a floor plan.
- You can define new auto deletion settings for alerts, including the number of system and security alerts that you can retain on the server, and the total number of days that you can retain alerts.
- You can now define auto deletion settings for APs, clients, and networks in the **Monitor > WIPS** pages. This enables you to delete inactive devices or networks based on their classification.
- The Root Cause Analysis widget is now more prominently displayed in the **Dashboard > Performance** page when issues occur, and includes information on poor application experience for single wireless clients.
- To minimize downtime when an AP reboots, Auto Channel Selection (ACS) now uses the last best channel and does not wait to scan the radio spectrum.
- The time it takes to update an AP with a configuration change in the device or radio settings has been reduced by approximately 15 seconds. The radio downtime has been reduced to approximately 1 second, except for operating channel changes.
- You can now download an inventory list of data from the Access Points, Tunnels, WIPS, and Alerts monitor pages.
- Configuration changes to SSIDs, WIPS, and radio changes (except for operating channel changes) no longer result in wireless client disconnections.
- APs now support multicast DNS (mDNS) packet tagging. This feature is configured in the network settings of an SSID and also requires a location tag.
- You can now configure the Dead Time (the time delay before fallback to a primary server) when you enable the **Prefer Primary RADIUS Server** option.
- From Discover, you can now configure ArcSight Enterprise Security Management (ESM) server integration.
- From Discover, you can now open an SSH web shell for command line interface access to a specific AP. This is intended for use in conjunction with WatchGuard Technical Support for troubleshooting.
- You can now set a default language for system notifications and email notifications.

- Third-party analytics data now includes RSSI and channel data for APs and clients.
- Configuration changes to RADIUS, Role Profiles, and Tunnel Profiles now indicate the number of devices that are affected by the change.
- Channel 144 is now supported in Japan.

Resolved Issues

- You can now correctly add an AP to the banned device list. *[AP-908]*
- Discover now correctly shows a scheduled Client Connectivity Test as executed when the configured time zone and the browser time zone are different.
- RADIUS servers now correctly fail over when the number of retry attempts is set to 9 or 10.
- This release resolves a rare kernel panic that occurs after long periods of uptime in AP325 devices.
- APs with link aggregation in failsafe mode can now communicate correctly with any wired host.
- APs now correctly process upgrade operations in failsafe mode.
- Client failures no longer appear in the connection logs when the captive portal session timeout expires.
- APs now correctly obtain an IP address in WIPS sensor mode when link aggregation is enabled and only the eth1 network is active.
- Auto transmit power now correctly sets the maximum power based on the regulatory limit instead of the full EIRP limit.
- Changes to the AP device name or location no longer cause the RADIUS called-station-id parameter to be incorrectly sent as a ":" separated value instead of a "-" separated value when you use the %m variable.
- Duplicate "smart-logging-disabled" messages no longer occur in the AP logs.
- The deletion of an RF neighbor no longer results in a kernel panic on an AP.
- Clients are no longer redirected to an incorrect portal if there are multiple SSID profiles with a captive portal enabled and one of these SSID profiles is disabled or is not scheduled as active.
- Increased resource usage no longer occurs when you stop a client connectivity test.
- VoIP and throughput client connectivity tests no longer fail on the target AP if the AP is already running client connectivity tests as a client.
- Mesh links are now visible in location tracking results.
- The alert type is now correctly included when you search for devices.
- Root cause analysis no longer incorrectly identifies 802.11ax clients as not supporting the latest 2.4 GHz band.
- Channel width information in Discover now correctly appears in the Access Point properties widget.
- Moved location folders now correctly reset to an "unplaced" state.
- A scheduled report email attachment is now correctly encoded when the report name contains non-English characters.
- You can now return to the previous page when you view contending clients in full screen mode on the interference details page.
- The device context menu now correctly closes when you switch to another location on a floor plan.
- IGMP snooping options are now correctly validated when you save an SSID profile.
- The Go application now correctly allows you to enable up to 8 SSIDs instead of 4 SSIDs.
- You can now correctly rename an AP when the device note is undefined.

Wi-Fi Cloud 9.0.1-14.3: 12 March 2021

New Features and Enhancements

- You can now configure a WatchGuard AP as a Remote Access Point that enables a remote worker or branch office to tunnel traffic from the AP over an IPSec VPN to a corporate enterprise network.

Remote AP functionality is only supported on the AP225W, AP327X, and AP420.

- You can now tunnel RADIUS messages to a RADIUS server that is located on a network behind a remote endpoint of a VPN tunnel. This enables you to authenticate Wi-Fi clients with a remote RADIUS server when SSID traffic is tunneled.
- You now receive a warning notification message if an AP configuration change might impact end user connectivity, such as when an SSID resets or an AP reboots.
- You can now individually disable or enable the 2.4 GHz and 5 GHz radios on an AP. This helps with AP deployments where you need to disable the 2.4 GHz radio on specific APs to prevent interference on the 2.4 GHz band in a high-density deployment.
- The Spectrum Analysis troubleshooting tool is now available again in Discover.
- From the Monitor pages in Discover, you can now view access point properties directly from the **Access Point**, **Client**, and **Radio** lists.
- Root cause analysis now includes a list of contending clients or BSSIDs in the **Recommendations** panel if a client experiences high contention issues.
- You can now download audit logs and set the audit log retention policy from the **System > Logs** page in Discover.
- You can now download visibility and association analytics reports from the **Reports** menu in Discover.
- You can now download a full list of possible alert events in tab-separated value format from the **Configure > Alerts** page in Discover.
- Alerts are now generated when an AP connected to Wi-Fi Cloud reboots.
- You can now configure the communication key or passphrase used for authentication and encryption between Wi-Fi Cloud and managed APs from the **System > Advanced Settings** page in Discover.

Resolved Issues

- The **Allowed AP Vendor** list now correctly appears in an Authorized WiFi Policy in Discover. *[AP-737]*
- The correct VLAN is now applied to a scheduled SSID if the configuration changes during the SSID downtime.
- A wireless client now receives an IP address from the correct VLAN if multiple DHCP servers respond from different VLANs.
- A captive portal now works correctly for wired clients connected to a secondary LAN port on an AP.
- The correct transmit power is now applied to the new AP operating channel after DFS radar detection.
- AP features such as Application Visibility, the Application Firewall, and Captive Portals now work correctly when the AP transmit power is set higher than 30.

- You can now edit a client connectivity test profile after the corresponding SSID profile is deleted. This enables you to edit the client connectivity test to run with a different SSID profile.

After the upgrade to Wi-Fi Cloud v9.0, the lowest firmware version an AP can downgrade to is v8.8.

Engage Update: 31 October 2020

- Instagram has been removed from the social media plug-in configuration. If you have previously enabled and configured the Instagram plug-in, the option will not be removed until you disable the plug-in and update the configuration. For more information, see Impact of Instagram privacy and security changes on WatchGuard Wi-Fi Cloud.
- Improved notification when the maximum number of captive portals is reached.

Discover and Analyze Update: 25 September 2020

- The client location tracking view now shows association information.
- The AP location tracking view now highlights the last searched and placed managed device.
- The Show Associations and User/Device Name options are enabled by default in the location tracking view.
- Performance issues for AP floor map placement are resolved.
- A broken help link in the Discover mesh network configuration has been removed.
- Added support for a forward proxy configuration for outbound HTTP requests. HTTP endpoints configured for custom SMS and third-party integration must have a valid SSL certificate for integration with Analyze.
- Updated AWS email services API on Analyze servers.
- Instagram plug-in statistics are removed from Analyze charts.

Instagram has recently changed their privacy and security policies. As a result of these changes, the Instagram plug-in cannot authenticate captive portal logins, and guest users that attempt to log in with their Instagram credentials will receive an error. For more information, see Impact of Instagram privacy and security changes on WatchGuard Wi-Fi Cloud.

Analyze Update: 4 September 2020

- The Wi-Fi Users and New vs Repeat Users widgets on the Analyze dashboard now correctly display data. *[AP-741]*

WatchGuard Wi-Fi Cloud Version 8.9.0-063: 7 August 2020

New Features and Enhancements in Discover

- The Zoom and Microsoft Teams applications are now available on the Application Dashboard. In addition, you can now select which applications appear on your Applications Dashboard from a drop-down list on the Application Health widget. You can view a maximum of five applications.

- Customized filters and the sort order of access point and client lists are now preserved when you navigate between pages.
- You can now configure scheduled firmware upgrades and options for new device upgrades in Discover.
- You can now configure mesh networks in Discover. You must configure mesh network profiles for APs in an AP Group.
- You can now view the root cause analysis of issues that affect one or more client devices and the recommendations for how to resolve these issues. This includes clients affected by low data rates, low RSSI, and high retry rate.
- You can now locate APs and clients on a floor map in Discover. On the Access Points or Clients Monitor page, right-click the device, then click the **Locate** action. You can also perform a locate action from the Floor Plans page.
- Cloud Integration Point (CIP) now supports a high availability configuration that enables you to select a primary and secondary CIP-enabled AP for syslog and SNMP servers, and WLAN integration.
- AP monitoring pages and AP properties include new AP health statistics and wired network properties:
  - AP Health — Shows CPU and memory utilization.
  - Configuration — Indicates the AP location, operating mode, SSID, and channel information.
  - Wired Properties — Indicates the wired side properties of an AP. This includes the switch details, the link speed, and the VLANs detected by the AP. The IP address network properties of the AP include the DHCP and DNS servers the AP uses, and the DHCP lease time.
- Client connectivity tests now support SSIDs with captive portals. You can enable a Portal Authentication Test that attempts to connect to the Internet through the specified portal URL and bypasses the captive portal authentication.
- You can now view IPv6 addresses for APs and wireless clients. You can also configure IPv6 addresses for some features, such as a RADIUS server, NTP server, and third-party servers.
- You can now configure location-specific properties for a location folder, such as the Location Tag and Venue ID for an AP from **System > Navigator** in Discover.
- You can now configure the Additional VLAN Monitoring settings for each AP in Discover. This includes the ability to set a static IP address for the AP on the communication VLAN.

General Enhancements

- Wi-Fi Cloud now supports WPA3 (Personal and Enterprise) and the enhanced Open security protocol based on Opportunistic Wireless Encryption (OWE). These features are only supported on Wi-Fi 6 (802.11ax) APs.
- If an AP reboots, the reason for the reboot now appears in the event logs for an AP.
- Configuration changes to the channel scanning list or SSID VLAN/Auto VLAN monitoring no longer require an AP reboot.
- Added support for AP325 revision B hardware with improved antenna design.

AP firmware versions 8.9.0-063 and higher are only available for 802.11ac Wave 2 access points. Wave 1 access points (AP120, AP320, and AP322) will remain on 8.8.x firmware versions for maintenance releases only.

Resolved Issues

- Broken help file links no longer appear in event notification email messages.
- The channel scan/defend list is now updated correctly when the country of operation changes.
- The prefix for captured packet trace files is now auto-populated based on the device MAC address.
- Certificate-based authentication is now logged correctly.
- XSS vulnerabilities in the UI are resolved.
- When you upload a list of banned devices or allowed/blocked devices, you must now upload a CSV file.
- You can now correctly configure BYOD (Redirection), Captive Portal, and Firewall settings with Dynamic VLANs when RADIUS MAC Authentication is enabled in an SSID profile.
- If you search for an IP address in the global search, the AP list is now limited to five items and the See More option no longer appears.
- In Discover, the Captive Portal external RADIUS authentication configuration now supports the Change of Authorization (CoA) flag.
- Discover now correctly displays a new uploaded floor location layout.
- The Refresh, Help, and Logout buttons now render correctly in Internet Explorer 11.

Known Issues

- The Spectrum Analysis feature has been temporarily removed from Discover starting in Wi-Fi Cloud v8.9. This feature will be reintroduced in a future version to improve the quality of results based on new AP chipset capabilities.

Analyze and Engage Update: 26 June 2020

- Floor Map Analytics details now open correctly in Analyze. *[AP-704]*
- Engage server maintenance.

WatchGuard Wi-Fi Cloud Version 8.8.3-12: 5 June 2020

New Features and Enhancements

- You can now configure tri-radio AP models so that the AP operates in full WIPS sensor mode on radio 1 (2.4 GHz) and radio 2 (5 GHz), while the third radio is disabled.
- The AP325 is now PoE 802.3af compliant. The AP now operates with full capabilities in both 802.3af (PoE) and 802.3at (PoE+) power modes.
- You can now enable Cloud Integration Point (CIP) mode for the AP420 in Discover. To enable CIP mode, select **Monitor > WiFi > Access Points**, right-click the AP, then select **Enable CIP Mode**.
- Added hardware-based encryption support for IPSec tunnels to increase the throughput and performance on AP420 devices.
- Added support for TCP MSS (maximum segment size) clamping in the EoGRE, IPSec, and VxLAN tunnel configuration. APs clamp the MSS to a value lower than the tunnel maximum transmission unit (MTU) value to make sure that packets that flow through the tunnel do not exceed the tunnel MTU size.
- Some changes have been made to the LED behavior for the radio and LAN indicators on an AP:
  - A radio LED indicator is on when the radio is operational with an enabled SSID or if WIPS scanning is in progress on the radio.

    - The primary LAN LED indicator is on when the interface is connected and up. Any additional LAN ports on the AP will be indicated as on when a VLAN extension, wired extension, or link aggregation is enabled on the interface.
    - For more information, see Troubleshoot WatchGuard AP LED Status or the Hardware Guide for your AP model.
- The automatic channel selection algorithm is enhanced to improve optimum channel distribution in high density deployments.
- Added support to restrict AP operation on the 5 GHz band in the Israel regulatory domain.
- APs now support the RADIUS authentication NAS-IP-Address and NAS-IPv6-Address attributes. The AP uses these attributes and the existing NAS-ID attribute to uniquely identify the NAS (Network Access Server) in Disconnect-Request and CoA-Request packets. These attributes simplify integrations with servers such as Cisco ISE, Forescout, and Aruba ClearPass because the NAS ID is no longer mandatory. The AP gives preference to a NAS ID, if specified, then the NAS-IP-Address and NAS-IPv6-Address attributes.

Resolved Issues

- An AP now correctly performs a DFS channel availability check (CAC) for radar detection before it selects a DFS channel.
- An 802.11ac Wave2 AP now correctly accepts client connections after a channel change operation.
- Deprecated events are no longer generated in the Events list.
- APs with a high number of RF neighbors no longer show an incorrect high value of transmit power.
- APs no longer show an incorrect power LED status after a communication VLAN change.
- VxLAN interfaces for SSID VLANs are now correctly enabled after an SSID configuration change.
- An AP now correctly deletes VLAN interfaces for SSID profiles mapped on a VxLAN tunnel.
- Secondary VxLAN interface creation now works correctly when a configuration change operation is performed after a tunnel failover.
- Accounting packet registration now works correctly with a RADIUS server when an AP is configured with a captive portal.
- An SSID network is now correctly reported when SSID scheduling is enabled.
- LLDP power allocation from a switch is now ignored if the received power value from the network switch is 0. This prevents the AP from switching to lower PoE power if it is connected through a PoE+ injector and receives LLDP messages from a PoE switch. *[AP-625]*
- AP connections to Wi-Fi Cloud are no longer disrupted after you configure a VLAN extension in the device settings for the AP225W and the communications VLAN (for example, 0) is set to the LAN1 or LAN2 interface. *[AP-627]*

Analyze, Engage, and Customer Provisioning Portal (CPP) Update: 24 April 2020

- Required Analyze server security maintenance.
- AP activation and provisioning times are improved.
- In some cases, the ability to enable the Clickthrough plug-in did not work correctly in Engage.

Analyze and Engage Update: 3 February 2020

- Required Analyze server database maintenance.
- A guest user's valid SMS authentication code now works correctly for re-authentication to a captive portal. *[AP-548]*

WatchGuard Wi-Fi Cloud Version 8.8.1-101: 22 November 2019

Enhancements

- Enhanced role-based access control for RADIUS MAC authentication — You can now configure RADIUS MAC authentication to assign role profiles to clients both before and after authentication. This enhances Wi-Fi Cloud integration with third-party RADIUS servers and deployment scenarios that use external RADIUS portal authentication. For more information, see RADIUS MAC Authentication.
- Uniform LED patterns for all 802.11ac Wave 1 and Wave 2 APs. For more information, see Troubleshoot WatchGuard AP LED Status or the Hardware Guide for your AP model.
- Support added for the upcoming AP225W wall-plate access point.

Resolved Issues

- You are now able to delete a location from the location tree if a scheduled device firmware update is configured or if client connection test results exist for the location. *[AP-562]*
- Blacklist and whitelist client configuration now works correctly in Discover.
- A captive portal RADIUS configuration on an AP now correctly fails over to a secondary accounting server if the primary is unavailable.
- Role redirection issues no longer occur for APs configured with more than one SSID.
- A device name configured with special characters in Manage is now correctly displayed in the hostname sent by LLDP.
- IP failure events are no longer reported for a client if a dynamic VLAN or role-based VLAN is enabled on the AP.
- The Client Steering Common Parameters and Client RSSI Update Interval options now appear in the Radio Settings tab in the Discover Wi-Fi profile settings. Previously, these options were location in the Device Settings tab.
- The "Top Applications by Traffic" graph on the Applications Dashboard in Discover now correctly shows data for time filters of 4 hours and lower.

WatchGuard Wi-Fi Cloud Hotfix Version 8.8.0-192: 18 October 2019

- APs can now correctly connect to Wi-Fi Cloud if they receive a DNS suffix from DHCP.
- AP125 and AP325 devices configured in a mesh network no longer reboot when high downlink traffic occurs.
- Offline APs that are placed on a floor map in Discover no longer remain on the user interface when you navigate to a different page.
- Role redirection issues no longer occur on APs configured with more than one SSID.
- Cloud Integration Point (CIP) mode now works correctly when used with a static VLAN setting.

Analyze and Engage Update: 6 September 2019

- TCP SACK panic kernel vulnerabilities (CVE-2019-11477, CVE-2019-11478, CVE-2019-11479) are resolved.
- Updated API for the LinkedIn social media plug-in.
- Updated default splash page bundles to resolve page rendering issues in Chrome web browser version 73.0.3683.86 and higher.

WatchGuard Wi-Fi Cloud Version 8.8.0-179: 23 August 2019

Discover Enhancements

You can now perform these tasks in Discover:

- Configure SSIDs and AP device and radio settings.
- Configure WIPS settings, including AP and client classifications, Authorized WiFi Policies, and Intrusion Prevention.
- Monitor WIPS classifications and security alerts.
- Configure, schedule, and view Wi-Fi Cloud reports.

Additional Discover enhancements:

- AP Groups enable you to organize and manage your APs across your location tree. For example, you can apply the same configuration to APs even though the APs are in different location folders and floors.
- Support for the Slack application in the Applications Dashboard.
- Ability to monitor any configured tunnels from a new Tunnel tab on the Monitor > WiFi page.
- New device template migration tool to help you convert legacy model-specific device templates to universal templates.
- New widgets are available on the Monitor > WiFi > Access Points page that show the devices that can see the AP, and VLANs visible to the AP.
- HTTP and VoIP connectivity tests in Discover are now supported in cases where the target site blocks ICMP traffic or the web service is stopped. Note that many connectivity tests cannot run successfully on SSIDs that have a Captive Portal enabled.
- Application tests now use HTTP Get requests instead of ping for better reliability.
- Client connectivity test results now support partial success based on the results of the test categories.

Wi-Fi Cloud New Features and Enhancements

- Hitless Device Firmware Update — Minimizes the downtime for wireless clients during AP upgrades. APs are not upgraded at the same time as nearby APs so that wireless clients in that vicinity can remain connected to the Wi-Fi network.
- Use SSID Profile Configuration for Authorized WiFi Policy — You can now use the settings of your SSID Profiles to validate the configuration of your APs for the Authorized WiFi Policy. This simplifies the security settings of your Wi-Fi deployment when you use only WatchGuard APs. Disable this option if you want to create custom Authorized WiFi Policies for deployments such as WIPS overlay for third-party APs, or specific security configurations.
- SNMP Trap Support — Adds support for sending SNMP trap messages to network monitoring tools with an AP configured as a Cloud Integration Point (CIP).
- VXLAN Support — You can now configure and monitor VXLAN tunnels.
- Staging Area Folder — The folder for newly deployed APs is now called "Staging Area". Previously, this folder was called the "Unknown" folder.
- Improved HTML Reports — HTML reports in Manage have been improved for better readability and interactivity. XML and PDF formats have been removed.
- AP327X Support — Adds support for the AP327X outdoor access point.

Monitoring Enhancements

- New 802.11ac Wave 2 AP firmware updates for performance and monitoring enhancements.
- AP transmit power is now displayed as the Equivalent Isotropic Radiated Power (EIRP) that includes the transmit power with the antenna gain for the AP.
- The "Up/Down Since" column is renamed to "Connected/Disconnected Since"
- A new "Last Booted At" column indicates the time of the last device reboot.

Resolved Issues

- TCP SACK panic kernel vulnerabilities (CVE-2019-11477, CVE-2019-11478, CVE-2019-11479) are resolved.
- An AP125 or AP325 can now correctly create a mesh link on the 5 GHz radio as a "non-root" AP in dense AP deployments.
- The AP320 no longer occasionally auto-selects an incorrect channel of operation.
- The use of 802.11r on the AP325 and AP420 no longer causes slow speeds after roaming.
- APs no longer randomly reboot when they connect to switches with 802.3az enabled. 802.3az has been disabled on all APs to prevent connectivity issues.
- AP utilization and data rate charts for 802.11ac Wave 2 APs now correctly display data for the 5 GHz band.
- This release adds the ability to change the user role when a RADIUS CoA (Change of Authorization) is requested from an external service.
- MacBook client connectivity issues are resolved.
- An issue where high memory utilization for the AP325 appeared in the UI is resolved.
- APs now correctly add the DNS suffix in DNS query packets.
- VoIP and Wi-Fi client connectivity tests no longer fail when client isolation is enabled on the target AP.
- Client packets are no longer dropped for an SSID when content analytics are enabled on the SSID.
- Networks now correctly appear in the parent location when the current location is deleted.
- SSID Profile configuration and other similar pages no longer allow auto-fill of previously stored passwords.
- You can now save an SSID name that includes UTF-8 characters.
- You can now correctly restore SSH Whitelisting to default settings in a device template.
- In Manage, an audit Log is now correctly generated when the 802.11n/ac radio setting is enabled or disabled.
- The location of a Managed Device and its corresponding BSSID is now correctly reported.
- In some cases, you could not load AP details from the Visible Clients or Visible APs page.
- Channel information is now correctly displayed for clients in the Monitoring > Security > Clients page in Manage.
- Cross Site Scripting vulnerabilities in Discover have been resolved.
- The device password is now correctly set if the password contains non-English characters.
- The Dashboard now correctly loads when there are a large number of location folders defined.
- Users with administrator privileges for a location subfolder are now able to put APs on the floor map in their subfolder.
- 802.11ac Wave 1 devices (AP120, AP320, and AP322) no longer make repeated requests for a country code.
- Received data reported for an SSID for 802.11ac Wave2 devices is now accurately reported.

Engage Update: July 25 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.

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.

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.

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.

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