1. BUG: Repaired a problem where the API call BASearchCustomers did not properly search if the parameters simuse or status were used.
2. BUG: Authorize Device whether used for DHCPv4 or DHCPv6 would allow an IP that was not tied to a client device to be used to authenticate. It would not actually be recorded, but would appear to be. This behavior has been corrected. It now correctly shows errors in this circumstance.
3. BUG: DHCPv6 (IPv6) -> Authorize Device would allow authentication of devices that were currently online. This was not the intended behavior and has been corrected. It will now find the current session and display when you can authenticate. This is the behavior that was intended and is long the way authenticated DHCPv4 has behaved.
4. BUG: The newly added Device Profile from 7.1.0 had a problem where an improperly formatted mac address could cause a crash. This has been fixed.
5. BUG: In DHCPv6 If there were no authenticated devices then the classes for authenticated/pre-auth devices were not created. This prevented any devices from authenticating since the classes didn't exit and no pre-auth IPs could be obtained. This catch-22 situation has been resolved.
6. BUG: There was a display issue where multiple instances of usernames sticky assigned to IP or prefix by RADIUS could appear in DHCPv6 (IPv6) -> Sticky Assignments. These entries appeared to be duplicates. They really weren't. They resulted from multiple DUIDs authenticated by the same username receiving the same sticky assignments via RADIUS. This list has been collapsed so that there no longer appear to be duplicate entries.
7. BUG: Under some circumstances some DHCPv6 sessions could be missed until their first renewal time or shown to end early due to a missed renewal only to start again at the next renewal. This did not affect the actual DHCPv6 sessions customers were using but rather is a problem that shows up only in the various reporting interfaces (such as 'DHCPv6 (IPv6) -> Search Sessions'). This missing data has been minimized as much as possible though some occasional misses are still possible.
8. BUG: Previously, 'DHCPv6 (IPv6) -> Search DHCP Logs' would not allow searches for longer than 24 hours even if a DUID or other search terms were entered. This problem has been corrected.
9. BUG: There was a problem with Authenticated, Standard and DHCPv6 view address usage reports. If the 'limit displayed entries' box was used, the string entered there was carried over to any popup windows resulting from clicking links on the same page. This has been corrected and the string no longer carries over.
10. BUG: When there is an IPv4 VRRP address configured, the DNS service would fail to listen on this IP address. This has been corrected and the DNS service now listens properly on all addresses.
11. BUG: AuthHostManager, if it needed to move to the primary device due to the secondary device being down, would pause for about 10 minutes in between loops of adding customers to the DHCP server. This caused delays in authenticated users getting a post-auth IP address after authenticating at the captive portal. This delay was intended to be a rest period between checks if the secondary was still running not between each loop. That has been corrected and there should be no more problems with these delays if the secondary fails.
12. BUG: Trimming the SSD based filesystems on boot up was not really feasible on certain DHCPatriot systems due to the length of time it takes. It was not possible to pre-determine which ones these were that took, at times, an hour and a half. This blocked bootup while the trim was completed. Therefore, trimming on bootup has been disabled. The SSD based filesystems will be trimmed only at the normal daily time from this version forward.
13. BUG: Some non-auto generated graph tables (like for CPU usage) could accidentally be deleted during the cleanup of empty tables. This has been fixed.
14. BUG: Multiple edits to admin notes in the function Auth DHCP Reports -> Users Using Multiple IPs would trigger CSRF protection logging the user out. This has been fixed.
15. BUG: Corrected a bug where DHCPv6 raw logs were not being recorded properly as pertained to prefix delegations so searches for IPs falling within a prefix delegation in DHCPv6 (IPv6) -> Search DHCP Logs would not return any results. Logs are now recorded correctly in the case of a DHCPv6 prefix delegation and are now properly searchable
16. BUG: The rate limiting on ssh for bad passwords previously was a global limit (ie: bad passwords from user A would also lock out user B for a short time). This has been corrected and now the wait period will only apply on a per user ssh basis.
17. BUG: The Captive Portal screen previously did not specify a destination IP in the action= line. The iPhone (and perhaps other devices) would default to submitting via IPv6 regardless if the initial form was obtained via IPv4. This caused the iPhone to fail to authenticate IPv4 if IPv6 was already authenticated. Now the form specifies

and IP destination of the answering DHCPatriot device of either IPv4 or IPv6 depending the source type of IP of the initial get. This should resolve the aforementioned problem.

18. BUG: Repaired a problem where if an admin user was restricted to any networks under System Configuration -> Administrators using 7) User Admin Restriction (Auth), 8) User Admin Restriction (Standard), or 9) User Admin Restriction (DHCPv6) it would work but it would potentially cause weird errors and occasionally strange data to leak through. It now all works as it should throughout the interface.
19. BUG: Repaired a problem where the various types of 'User Admin Restriction' under 'System Configuration -> Administrators' could step on each other if the names were the same (not possible between AUTH and STANDARD but completely possible between either of those and DHCPv6). This would make it impossible to check each one with the same name as one of them would disappear. Now they have their type after them as well so that the names, even if they are the same, will be visible.
20. NEW: Throughout the interface data rows are now highlighted on hover so you can easily tell what row you are about to interact with.
21. NEW: A new setting has appeared in 'System Configuration -> General Setup' called '31) DHCP Next Server Setting (TFTP)'. This setting is disabled by default. If enabled, it causes the DHCPv4 server to set the 'next-server' option for each shared-network that has a TFTP server specified. This is in addition to 'server-name' and 'tftp-server-name' options that were already being set on a per shared-network basis in the case of a configured TFTP server.
22. NEW: At the bottom left side of the web GUI, '▲' has appeared. Mousing over this will show an interface allowing a change to the relative font size throughout the interface. This can be adjusted to between 50% and 200% the original size.
23. NEW: Two Factor Authentication (2FA) has arrived on the DHCPatriot system. You can enable and disable this for your admin account under Main -> Two Factor Auth Setup. This should work with most any Authenticator that supports TOTP (Google Authenticator etc...). A new column has appeared in the list at the bottom under System Configuration -> Administrators also that will have a [Remove2FA] link for any administrator that has 2FA enabled on his account. This allows anyone with access to System Configuration -> Administrators to disable 2FA for anyone that has it enabled thusly preventing lockout.
24. NEW: A select menu called "Option 82 Encoding" has appeared in both "Auth DHCP Config -> Shared Network" and "Standard DHCP Config -> Shared Network". This setting allows a per subnet setting of how the Option 82 data is decoded from relay agent DHCP packets. If "DEFAULT" is chosen, then the per subnet setting is disabled here and the behavior will be influenced by whether "DHCP Decode Binary Option 82 Data" is checked in "System Configuration -> General Setup". If "ASCII" is chosen, then the option 82 data will be decoded in this shared network as if it is "ASCII" text. This is the typical encoding of option 82 from Calix equipment. If "BINARY" is selected, then option 82 data in this shared network will be decoded as binary encoded (base 16, 8 bit) hex. It will add a ":" separator between each octet. This is typical encoding in the case of Cisco Equipment. If you have no need of per shared network encoding differences, then leave this setting at "DEFAULT" for each shared network and the system will treat option 82 data the same as in previous software releases.
25. API: A new API call, DeviceProfiler, allows access via API to the data presented when clicking a DUID or MAC address throughout the GUI. Either a DUID or a MAC address can be used to access this data. By default, the data is returned in XML format. A JSON return can be enabled by adding &JSON=true Examples below: https://patriot.alpha.network1.net/cli/?function=DeviceProfiler&username=apiuser&password=apipass&MAC=14:91:82:b5:fb:4c&JSON=true https://patriot.alpha.network1.net/cli/?function=DeviceProfiler&username=apiuser&password=apipass&DUID=00:02:03:09:05:05:14:91:82:b5:fb:4c&JSON=true
26. API: All xml entities and values are now checked and any invalid characters are removed from the XML return to API calls that feature such a return. Most of these, this will also affect the JSON return. We did not see any entities that were actually changed in testing as none contained invalid characters. Allowed characters in entities are letters, numbers, underscores, dashes, and periods. Disallowed characters in values are less than signs, greater than signs, single quotes and double quotes. This is according to the current XML specification.
27. API: The call GetNetworkConfig has been updated. The DHCPv6 portion now properly includes Prefix in a sub structure that can contain multiple prefix delegations. It also now includes the Pre-Auth subnets and prefix

delegations. Also, there is an additional type of DHCPv6 network noted in the return of 'DHCPv6_Authenticated' if the network is in fact an authenticated network.

28. API: The call NewPass has been updated. This now, by default will operate as before and change the stored password for the DHCPv4 user. Now you can include an additional parameter &type=DHCPv4 or &type=DHCPv6 to specify which type you want to change the password storage for. If the stored password needs to be changed for both types then it will need to be run twice.
29. API: The call dhcplogs now supports returning dhcp6 logs by passing the parameter &type=DHCPv6. the type defaults to DHCPv4 if it is omitted. &ip= now supports passing an IPv6 address if &type=DHCPv6. &duid= has been added as well so that returns can be restricted to only a certain client..
30. API: The AuthorizeCustomer call now supports DHCPv6. Access this by sending &duid= for some DUID to authenticate a DHCPv6 device. Also, the &ip= field can contain a pre-auth DHCPv6 address and will find the DUID for a DHCPv6 device to authenticate.
31. API: The SuspendEnable API call now supports DHCPv6. Additional parameters are &type=DHCPv6 (defaults to DHCPv4 if not sent), &duid=. A user device may be suspended by username, mac, or DUID. A note may be sent, also, that will be shown to the customer on the Captive Portal. The &AuthTest= parameter has no meaning if &type=DHCPv6 is sent. Unsuspend can only be performed on a DUID so if &type=DHCPv6 is sent and &action=unsuspend is sent, then &duid= becomes required.
32. API: The SearchSessions call now supports &type=DHCPv6 (default is DHCPv4 if no type is submitted). There is one new parameter &duid= which allows the submission of a DHCPv6 DUID for searching. &CircuitID= and &RemoteID= can be used to submit option 18 and option 37 to search. $ip= can be used to search for a single IP, whether it was the assigned IP or part of a delegated prefix. &mac= can still be used as well!
33. API: A new call has been added: StickyAssignmentV6 This call grants access to DHCPv6 (IPv6) -> Sticky Assignments to the API. LIST, ADD and DELETE are the three supported actions. See below examples:
    LIST: https://patriot.example.com/cli/?username=apiuser&password=apipass&function=StickyAssignmentV6&action=LIST
    ADD: https://patriot.example.com/cli/?username=apiuser&password=apipass&function=StickyAssignmentV6&action=ADD&StickyIP=2620%3A0%3A2e50%3Ae8%3A%3A1339&Identifier=test4&MatchType=USERNAME&MatchString=someguy
    DELETE: https://patriot.example.com/cli/?username=apiuser&password=apipass&function=StickyAssignmentV6&action=DELETE&StickyIP=2620%3A0%3A2e50%3Ae8%3A%3A1337
    You can add &JSON=true to the LIST action to return the list in JSON format. The examples above have been URL encoded.
34. API: The call SearchAuthDevices has been updated to add access to DHCPv6 (IPv6) -> View Authenticated Users by passing &type=DHCPv6 An additional value of &duid= may be passed to limit the results to a certain DUID. &AddressType= has no meaning in the DHCPv6 type.
35. API: The call BASearchCustomers has been updated to include &staticipv6 and &delegatedprefix parameters that allow searching by static IPv6 and delegated prefix assignments.
36. API: The call KnownClient now supports &type=DHCPv6. An additional parameter of &duid= has been added. This call gives access to DHCPv6 (IPv6) -> Known Client via the API. The parameter &TFTPfile= has no meaning when &type=DHCPv6 is sent.
37. API: The call AuthMassSuspend now supports &type=DHCPv6. This works exactly the same as the DHCPv4 version.
38. All IPv6 addresses should now be forced lower case no matter how they were entered. This keeps a consistent look in the interface and also makes sure that the occasional case-sensitive searches will work no matter how the data was typed.
39. Database queries are now much more secure against tampering such as sql injection attacks as all queries are sanitized on both read and write.
40. A new sort algorithm has been implemented such that lists should be sorted in a more natural way (ie: 192.168.0.1 -> 192.168.0.2 -> 192.168.0.10 etc... instead of 192.168.0.1 -> 192.168.0.10 -> 192.168.0.2 etc...). This has been applied throughout the GUI.