Version 6.3.0 introduced the following:
Release Month-Year: March 2019

1. Repaired a problem where Auth DHCP Config -> View Authenticated Users would show statically assigned user devices that were offline when "IP Address Type" was set to "Dynamic".
2. API: Repaired a problem with the function SuspendEnable where, when enabling a user or device, and not wanting an AuthTest to be performed, one would be performed if you did something like &AuthTest=false. This is because it isn't a true Boolean when coming from the web and we were evaluating it as if it was. We now look specifically for the word 'true' before performing an AuthTest.
3. Added the hostname to the title on the Administration web login page. This is to better facilitate password managers where the user has access to multiple DHCPatriot systems.
4. Previously it was possible to edit or delete a standard static subnet even if there were assigned IP addresses in the subnet. This left orphaned static assignments that showed up in no reports. This has been corrected. It is no longer possible to edit or delete a standard static subnet if addresses are assigned within the subnet.
5. Support for RFC 7710 has been implemented on DHCPv4 and DHCPv6. RFC 7710 (https://tools.ietf.org/html/rfc7710) provides a method for DHCP to provide a hint to the DHCP client, in the case of a Captive Portal, about the location (URL) of the captive portal. This is supposed to facilitate quicker access to the captive portal. There may be some clients out there that support this, but we at FNGi are unaware of any at this time.
6. Log messages for the various types of authentication have been cleaned up. Previously, it would only say that the device had been authenticated at the Captive Portal. Now it notes Captive Portal/Authenticate Device/CLI depending on which method was used.
7. It was discovered that directly connected USB keyboards did not function on the 2016-1 hardware models after the DHCPatriot software was running. This has been corrected and USB keyboards will now work with the DHCPatriot software on the 2016-1 hardware models.
8. It is now possible to show the option 82 data in-line in Auth DHCP Reports -> Search Sessions by selecting box '6) Show option 82 inline' before searching.
9. It is now possible to show the option 82 data in-line in Standard DHCP Reports -> Search Sessions by selecting box '6) Show option 82 inline' before searching.
10. Option 18 and 37 data may now be shown in-line when using DHCPv6 (IPv6) -> Search Sessions by selecting box '8) Show option 18/37 inline' before searching.
11. Current average cpu core temperature is now available via SNMP with the following OID: .1.3.6.1.4.1.2021.50.3.101.1
12. Current CPU Temperature has been added to Server Status complete with historical graphs.
13. Sticky IP address assignment will now warn you if you try to assign a sticky IP address that is currently in use dynamically by some device other than the one you are assigning it to.
14. The Captive Portal login page has received HTML5 pre-submit validation. It will now force lowercase in the username box (if configured) as well as enforce the other configured options like no '@' and no special characters. This is known to work in Windows/Mac/Linux: Safari, Chrome, Firefox, Internet Explorer and Microsoft Edge. This also works on the iPhone8 with Safari.
15. Added 3 second delay on authentication failure to the Captive Portal authentication. Previously, there was no delay.
16. Variables from the edit form of Auth DHCP Config -> Captive Portal were being displayed incorrectly at the bottom. This was not noticeable unless there was a field that contained HTML. These variables are no longer being incorrectly displayed beyond the bottom of the form.
17. It is now possible to set passwords containing spaces in Auth DHCP Actions -> Built-in Authentication: User Maintenance. This allows for the newer philosophy of long word based passwords containing random words of varying length. These types of passwords are easy to remember but due to the large amount of possible combinations, quite hard to guess or brute force. The jury is out if these types of passwords are better or worse. Here is a short bit of information: https://www.schneier.com/blog/archives/2012/03/the_security_of_5.html The short answer is that nonsense phrases like: 'correct horse battery staple' are

more secure than a normal random 8 character password while a known phrase like 'Harry Potter' is less secure.

18. The DUID field has been hidden when using the Authorize device form for DHCPv4 (Auth DHCP Actions -> Authorize Customer). People were accidentally putting values such as IP addresses and usernames in the DUID box for DHCPv4.
19. A cache system has been implemented for the GUI. This allows the caching of data retrieved for display in the GUI. The data will be pulled from cache when paging through it or reordering the sort or when limiting displayed entries. This should speed up certain operations on the DHCPatriot GUI. This has been implemented for Auth DHCP Reports -> Search DHCP Logs, Auth DHCP Reports -> Search Sessions, Standard DHCP Reports -> Search DHCP Logs, Standard DHCP Reports -> Search Sessions, DHCPv6 (IPv6) -> Search DHCP Logs and DHCPv6 (IPv6) -> Search Sessions.
20. A timeout has been implemented with the background process that adds and removes user devices from the DHCPv4 server. Previously, this process would sometimes get hung up for a time if the DHCP server failed to respond appropriately.
21. When a new DHCPatriot device is added to the system, we have to add the authenticated user devices to that device. This process has been changed such that the authenticated user devices are added from a different queue so as not to cause a long interruption in ongoing additions. The regular queued removals (and any subsequent adds for the same authenticated user device) still must wait until this process is complete, however.
22. The captive portal name server configuration has been adjusted such that if any DNS entry is requested via IPv4 then only an 'A' record can be returned, and if IPv6, then only a 'AAAA' record. Client web browsers were asking for the opposite type of record (mainly 'A' when connected via IPv6) and were therefore not able to access the captive portal page.
23. The model and serial number of the DHCPatriot devices (if known) are now shown in System Configuration -> Server Status at the bottom.
24. An alert now appears inside the GUI if there is a service down on either DHCPatriot device and the user is allowed to view System Configuration -> Server Status. This alert can be ignored (which starts a 15 minute timer of not showing outage alerts) or "View Outage" can be clicked which takes you to System Configuration -> Server Status.
25. A problem was discovered where the RADIUS attribute Acct-Session-Time (46) was not present in the accounting stop packets. This attribute is required by some RADIUS servers to extrapolate the start of the session. The attribute now appears in the RADIUS packet properly.
26. The RADIUS RFC requires some attributes, such as Class (25), to possibly be attached to the packet multiple times (ie, there could be several class attributes with different content). The Class attribute is also special in that if it is received in access-response, then it must be attached to accounting-start. The DHCPatriot previously did not support multiple Class attributes in a single packet. That problem has been solved. It is now possible to use multiple Class attributes.
27. Throughout the web GUI, submit buttons now disable (wherever possible) after clicking in order to prevent double form submission.
28. The web GUI interface now gives better feedback when the page is loading.
29. Data is now fully generated and laid out before transmission occurs to prevent partial page loads that may not be aesthetically pleasing.
30. There is now a 3 second delay on invalid login to the Web Admin GUI to prevent brute force attacks.
31. System Configuration -> Ping or Trace Host now (mostly) only pings or traces hosts from the correct address family so as to avoid confusion if an IPv6 address is found but ping (IPv4) was selected.
32. Mac address links now show a tooltip that has the manufacturer of the device wherever they appear.
33. A problem was repaired where IPv6 pre-auth clients were not being redirected to the customer login page when connecting via secure. What normally happens, in IPv4, was that the client would be automatically redirected to the customer login page. The DHCPatriot system was not looking for IPv6 pre-auth visitors and was not properly redirecting. It now does look for them and does the redirection properly.

34. Main -> Change Your Password received enhanced error messages. Previously, the error messages were often confusing as to what the real problem was when trying to change your password.
35. Alterations were made to DHCPv6 (IPv6) -> Authorize Device to remove the MAC address form field. That field should never have appeared there as it is not usable for authentication under DHCPv6.
36. API: Remote Search now includes Option 82 in the return data if requested. Set &82=true to receive the option 82 data in the XML return (see the manual for full details of this API function).
37. A new category of "auto suspend" has been added. This category will suspend devices that have been authenticated since the selected time period (default - 1 year) but have never had an online session.
38. It is now possible to assign a /31 IP address on the DHCPatriot devices. Please note that it will not be possible to use a VRRP address in this configuration as each DHCPatriot device would then be in a different subnet.
39. Further protections have been taken to secure the web GUI against attack using key / value pairings in a post message.
40. It is now possible to add a Custom Web Secure Certificate to the DHCPatriot system using: System Configuration -> Custom Web Certificate. This allows the addition of a certificate issued by a trusted certificate authority.
41. The count of available IPs was previously wrong in the case of subnets larger than /24 in both the graphs and view address usage. It included IPs ending in both .0 and .255 which are not allocated by the DHCPatriot system. These addresses are not allocated as some clients are not able to route properly when allocated these addresses. These IPs are now withheld from the count of total IP addresses.
42. Static subnets in Authenticated DHCP can now be configured with lease length overrides just like the authenticated dynamic subnets.
43. Static subnets in Standard DHCP can now be configured with lease length overrides just like the standard dynamic subnets.
44. All static and sticky assigned addresses in both authenticated and standard DHCP will follow the configured lease lengths in either the shared network configuration or the applicable lease length overrides. Previously they were all 12 hours in length regardless of the configured lengths.
45. API: It is now possible to access ping of both IPv4 and IPv6 ip addresses via the API. Example URL: https://patriot.network1.net/cli/?function=Ping&username=apiuser&password=apipass&ip=74.115.180.1 (IPv4) and https://patriot.network1.net/cli/?function=Ping&username=apiuser&password=apipass&ip=2620:0:2e50:fe::a (IPv6)
46. API: It is now possible to access trace route of both IPv4 and IPv6 ip addresses via the API. Example URL: https://patriot.network1.net/cli/?function=Trace&username=apiuser&password=apipass&ip=74.115.180.1 (IPv4) and https://patriot.network1.net/cli/?function=Trace&username=apiuser&password=apipass&ip=2620:0:2e50:fe::a (IPv6)
47. API: DHCP logs are now accessible via the API. Example URL: https://patriot.alpha.network1.net/cli/?function=dhcplogs&username=apiuser&password=apipass&start=1541376000&stop=1541462399&SearchText=DHCPREQUEST&ip=74.115.180.93&mac=52:54:00:27:04:0
48. Administrator password complexity restrictions have been added. These allow things like minimum characters, requiring symbols and the like to be set. These functions are available at the bottom of System Configuration -> Administrators if the logged on administrator's admin level is at least 6.
49. View Address Usage for both standard and authenticated style reports have been re-written for performance enhancement. Some larger DHCPatriot systems were taking several minutes to display these reports. This was due to the numbers being calculated in real time. These numbers are now gathered from the graph data that is already computed every five minutes. The side effects of this are that if a new subnet is added, it could be up to ten minutes before numbers appear in this report. Also, the numbers shown could be up to five minutes old. However, the report should be more accessible on the larger systems.
50. Repaired a problem where a certain event in DHCPv6 was being interpreted incorrectly leading to a crash and failure to process further events. This event is now recognized and is safely ignored.

51. Repaired a problem where it was possible to commit edits to Standard DHCP Actions -> Static IP Assignment that were invalid. For example, it was possible to match on mac address with no mac address entered. An error would be shown followed by a success message. This has been corrected. Now an error causes no commit to happen.
52. Repaired a problem where the MAC address did not show with DHCPv6 sessions when gathered in any other way than DHCPv6 option 79. The MAC address will now correctly show with the session no matter how it was gathered.
53. Repaired a problem where notes did not show when adding a user via cli function AuthorizeCustomer including a note. This has been repaired.