Version 5.4.0 introduced the following:
Release Month-Year: September 2014

1. When unsuspending a user device in Auth DHCP Actions -> Suspend User, the limit displayed entries was not saved during the unsuspend process. This has been corrected and list limits are now remembered as user devices are unsuspended.
2. IPv6 logins to the web administration interface were impossible. This was traced to storage of the remote IP address being to small. The size has been increased so that it can store IPv6 addresses. The DHCPatriot system can now be administered from an IPv6 address.
3. Discovered that there was a problem where sometimes cron would no longer rotate logs or database files until it was restarted. Cron now restarts once per day to avoid this situation.
4. Both IPv4 and IPv6 versions of Firewall setup under System Configuration now support assigning several services to an IP address simultaneously. Previously you had to repeat the process several times to open the firewall for more than one service to a specific IP or subnet.
5. IPv6 Ping and Trace route are now supported in the web administration interface as well as the CLI admin menu. Options 12 and 13 are ping6 and trace6 respectively. Reboot and shutdown have moved to options 14 and 15 respectively.
6. API: Unsuspending via the API can now perform a RADIUS authentication check as the web administration interface does if the parameter AuthTest=true is passed to the API. Example: https://patriot.network1.net/cli/?function=SuspendEnable&username=apiuser&password=apipass&action=unsuspend&user=bobaaron&AuthTest=true
7. API: StickyIP ADD: It is now possible to add a sticky IP via the API by using a URL of the following format: https://patriot.network1.net/cli/?username=&password=&function=StickyIPs&action=ADD&Stickymac=&Stickyusername=&Stickyip=&Stickynote=
8. API: StickyIP DELETE: It is now possible to delete a sticky IP via the API by using a URL of the following format: https://patriot.network1.net/cli/?username=&password=&function=StickyIPs&action=DELETE&Stickymac=&Stickyusername=
9. API: StickyIP LIST: It is now possible to list sticky IP assignments via the API by using a URL of the following format: https://patriot.network1.net/cli/?username=&password=&function=StickyIPs&action=LIST An XML list is returned.
10. API: Its now possible to authenticate a user device using the current pre-auth IP address of the device by using the parameter ip= in place of the MAC= parameter as in this example: https://patriot.network1.net/cli/?username=&password=&function=AuthorizeCustomer&user=exampleuser&pass=examplepass&ip=exampleip
11. API: A new api call has been added to find authenticated devices. This is accessed in the same way as the rest of the API and returns results in XML format. All authenticated devices may be returned, or the search may be limited. The URL should have the following format: https://patriot.network1.net/cli/?function=SearchAuthDevices&username=&password=@&mac=&AdminNote=&user=&ShowOnlyOnline=(TRUE)&AddressType=(STATIC/DYNAMIC)
12. Default DNS servers (when a DHCPatriot has first been installed but not yet configured) have been changed to 8.8.8.8 and 8.8.4.4.

13 It is now possible to exclude a range of IP addresses in Auth DHCP Config -> Exclude IP Address in the GUI.

14 There is a new list that can be maintained in Auth DHCP Config -> Deny MAC Address as well as Standard DHCP Config -> Deny MAC Address. This list prevents mac addresses entered within from getting an IP address.

15 The DHCPatriot no longer prevents authentication if there is a current authenticated lease for the device. The reason it did this in the first place was to prevent sim-use violations. Logic dictates that the device is already suspend however, so there really wasn't a reason to prevent authentication. Authentication still isn't allowed if the device is a valid authenticated device that is not suspended.

16 It is now possible to delete suspended devices that do not currently have an IP address in View Authenticated Users.

17 Optional lease length overrides have been added to the dynamic subnets in standard and authenticated. This allows an administrator to set a different lease length for a certain dynamic subnet for maintenance purposes or whatever reason.

18 OpenSSL has been updated to fix the somewhat obscure security issue reported in: http://www.openssl.org/news/secadv_20140605.txt

19 A feature has been added that lets an admin add DHCP configs to the pool {} statement. This is needed by some customers to replicate custom ISC DHCP configs in specific environments.

20 A new feature called Built-in Authentication: User Import under Auth DHCP Actions allows the import of a list of users using a comma separated value (CSV) file upload in a specific format.

21 A new feature called Device Import under Auth DHCP Actions allows the import of a list of authenticated devices using a comma separated value (CSV) file upload in a specific format.

22 Repaired a problem where the Request Assistance under Main linked to a non-existant page.

23 Captive portal protection has gained the ability for the administrator to supply their own page to be used to protect the DHCPatriot from automated programs that use web. A new setting box appears in System Configuration -> General Setup allowing an administrator to supply their own HTML for the protection page if they don't want to use the math problem.

24 It was discovered that Internet Explorer was not following the 404 redirect on the DHCPatriot. Instead of showing the login page, it would show an Internet Explorer specific "Webpage not found" error page. This meant that if the home page of the user was set to something like http://www.sony.com/ps4 that instead of redirecting back to the login page, the user would get an Internet Explorer generated error page that looked similar to the "page cannot be displayed" error page. We have taken steps to rectify this and Internet Explorer is now being properly redirected to the login page.

25 Keepalive with one second timeout has been enabled on the DHCPatriot system web server. This affects the login page as well as the admin interface.

26 It was discovered that DHCPRELEASE log entries were not being recorded in the logs. This wasn't so much a bug as an oversite. These log entries would not have appeared in the logs at any time with version 5 as no routines for parsing them ever existed. This has been rectified and log messages about DHCPRELEASE now appear in the logs.