Blancco Drive Eraser WLAN Support

Blancco Drive Eraser (BDE) supports several wireless network encryption types, namely WPA-PSK, WPA-EAP, WEP and no encryption. WPA2 is also supported, the same configuration as for WPA is used and BDE does not make any difference, by default it tries to connect to WPA2 first. However, it is up to the access point to decide which one to use (WPA or WPA2).

Although WPA-EAP without authentication works fine, what BDE does not support is a WLAN using WPA-EAP with authentication (via a certificate and/or an authentication server) e.g. the 802.1X Authentication. There is a workaround if one needs to run BDE in an environment with such authentication (tested with Cisco ISE):

- When BDE (the client) makes its initial DHCP request (discovery message), it sends an information similar to "*Option: (60) Vendor class identifier: dhcpcd-5.5.6:Linux-4.1.3-0-BLANCCO:i686:GenuineIntel*". The customer can use it to set up a DHCP class identifier in Cisco ISE, such client profiling can be utilized as a common attribute for end points in the network for dynamic whitelisting.
- Once specific rules are set up in Cisco ISE, the client is able to authenticate.

Other workarounds include manual addition of mac addresses to the NAC system every time an erasure is run, or setting up specific ports that are 802.1x enabled.

There exist other possibilities to circumvent the 802.1X Authentication; they involve the creation of a dedicated "wireless network for erasure purposes":

- Configure a hidden WLAN network using one of the encryption types that BDE supports (e.g. WPA-PSK or WPA2-PSK) and set a strong password.
- Make sure that a local Blancco Management Console (or Blancco Cloud) can access this WLAN.
- Configure BDE to connect to this hidden WLAN and to the BMC: once you decide that a machine needs to be erased, boot BDE and the software will connect to the WLAN and to the BMC to get the erasure licenses and send the erasure report in the end.
- You can define other things like having your BMC in a LAN with one wireless access point only (for Wi-Fi machines to be able to establish a connection, but only in the vicinity of the access point) or adding rules in your WLAN firewall to allow connecting to only one IP address and port (both corresponding to your BMC).