Using Ubiquiti UniFi Network Equipment With HDA

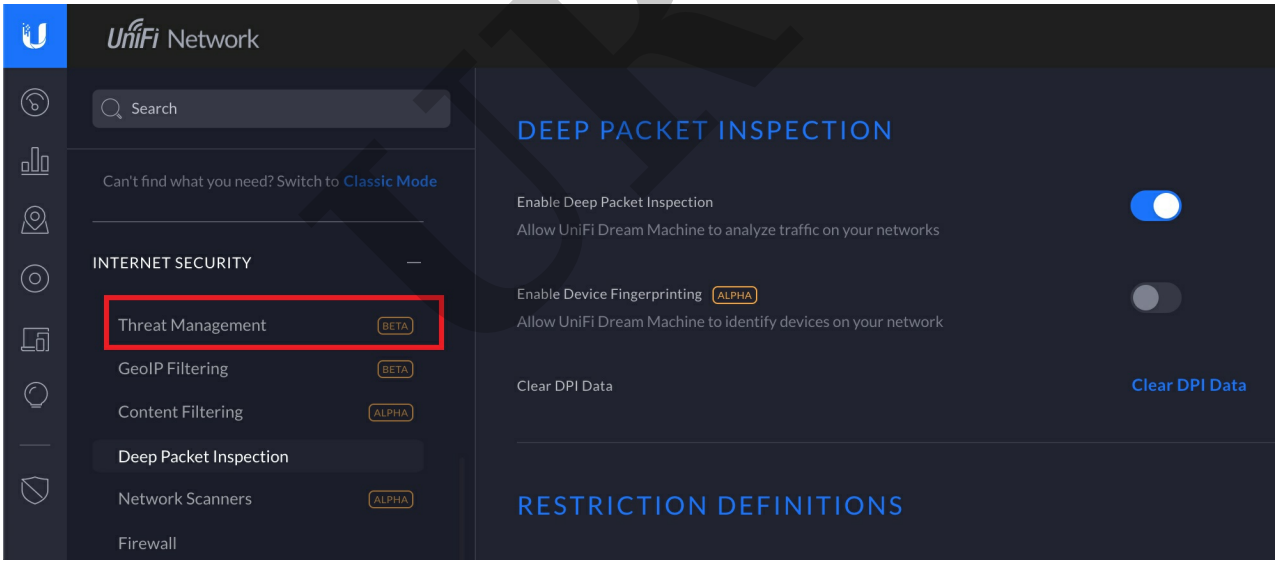
Last Modified on 08/09/2023 6:25 pm EDT

Ubiquiti UniFi **advanced security features** can cause issues when working with certain **HDA** products. Some of the advanced security functions can **create random reboots of HDA amplifiers**. URC recommends that you **disable** these functions when using HDA in both Accelerator 3 and TC Flex 2. This article details the procedure for configuring the settings.

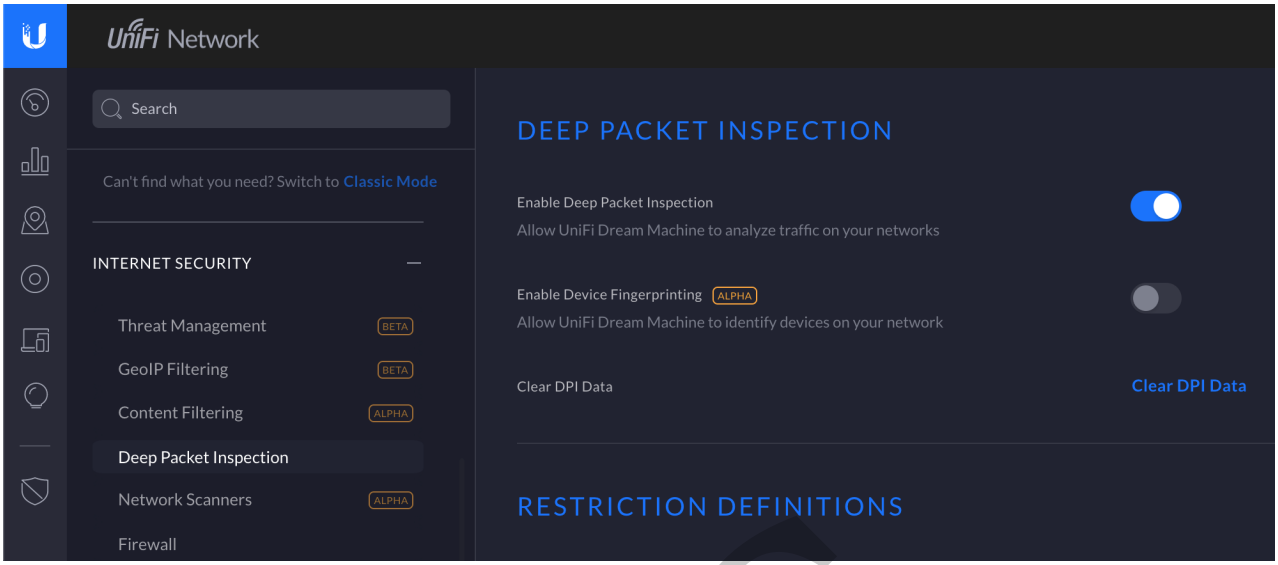
Any UniFi router including the USG and Dream Machine Pro that run on the UniFi controller software needs to have these functions disabled in order to avoid possible conflicts with HDA equipment.

At this time, these functions are released in the UniFi software and labeled as ALPHA/BETA and may be revisited once they have been updated and released without the testing labels and are ready for public use.

These functions can be found in the controller settings under Internet Security. For now, all aspects of Threat Management should be disabled.



Device Fingerprinting which can be found within Deep Packet Inspection should be disabled as well. Deep packet inspection itself can be used and appears to not cause any problems.



Additional Note: Other functions labeled ALPHA or BETA should be used with caution as they may create issues on the network that could cause unexpected reboots of the HDA equipment or may cause other issues within the Total Control System.

Additional Information & Resources:

To learn more about HDA products and programming, please see the HDA Programmers Guide or the Accelerator 3 online **Programming Guide.**