How Device Classification Works

https://campus.barracuda.com/doc/99618369/

Device classification is used to classify users' devices as Personal, Managed, or Supervised. This is a powerful tool that IT administrators can use in order to better manage and secure corporate devices.

Your company's web security policies and the Tamperproof feature (see below for details) are enforced, optional, or always off, depending on the classification of your device:

Classification	Web Security	Tamperproof	Notes
Supervised	On, and company web policies are enforced.	On	
Managed	On, and company web policies are enforced, unless you opt-out.	Off	
Personal	Off	Off	Your organization CANNOT see the web traffic on your device, even if the CloudGen Access app is installed and running.

Tamperproof Feature

This feature provides your organization with the option to protect against unauthorized or accidental tampering with the app installation, security policy, and app settings on devices.   When Tamperproof is enabled, you will not see an option to quit, unenroll, or stop the CloudGen Access app on your device.

Information Logged by Your Organization

- The resource or application name, and when it was accessed.
- If the Web Security feature is enabled (for *Managed* or *Supervised* devices), list of domain names and applications you accessed on your device.