Tamperproof

https://campus.barracuda.com/doc/99615906/

The *Tamperproof* feature provides the option to protect against unauthorized or accidental tampering with the app installation, security policy, and app settings on endpoints. When you enable *Tamperproof* on a device, it will hide the quit, unenroll and stop/start option on the CloudGen Access App. Note different behaviors depending on the OS as described in the *Operating System Specifics* section below.

- Existing customer devices don't have Tamperproof configured by default. If you want to enable Tamperproof for ALL end users, enable **Default Tamperproof Protection** (global). See below.
- When you enroll a device, the **Default Tamperproof Protection** setting is applied (see the **Devices > Settings** page, **Tamperproof** section).

To configure this feature at a global level, go to **Device > Settings** and scroll down to **Tamperproof** .

- **Default Tamperproof Protection** – Turning this setting on applies Tamperproof protection to all devices that have **Device Tamperproof Posture** set to *Default Tamperproof Setting*. You can override this setting for individual devices by going to the **Devices** page and clicking the padlock in the **Tamperproof** column. For **Device Tamperproof Posture**, configure:
  - *Default Tamperproof Setting* – Inherits the global setting (Default Tamperproof Protection, either on or off) configured on the **Devices > Settings** page.
  - *Enforce Off* – Disables Tamperproof on devices, overriding the global setting (Default Tamperproof Protection) configured on the **Devices > Settings** page.
  - *Enforce On* – Enables Tamperproof on devices, overriding the global setting (Default Tamperproof Protection) configured on the **Devices > Settings** page.
- **OS Platforms Exemption** – Turning this setting on enables you to exclude specific operating systems from the Tamperproof feature.

Operating System Specifics

- *Windows* – With Windows, the CloudGen Access app automatically starts on Windows start-up. To prevent uninstallation and stopping of the agent by the user, install the process as an administrator and assign user level access to the end user.
- *macOS* – Requires an MDM solution and deployment of the .mobilconfig and .plist files, which enable CloudGen Access to automatically start on the endpoint and prevents the agent from being stopped by the user. The *mobilecconfig* file is set to prevent uninstall of the VPN profile and to make sure that the user cannot bypass web filtering by recreating a connection on the VPN when a connection is initiated. The *plist* file is used to restart the CloudGen Access

app if it is closed.

- *iOS* – Requires an MDM solution and deployment of the .mobilconfig file, which enables CloudGen Access to automatically start on the endpoint and prevents the agent from being stopped by the user.
- *Android* – Limited support for this OS.
- *Linux* – Limited support for this OS.