Configuring Open-Audit with HTTPS/SSL

UPDATE - The below applies to Open-AudIT versions **prior** to 5.0.0 As at 5.0.0, Open-AudIT is "just another website" in terms of HTTP / HTTPS. There is no configuration of Open-AudIT required for HTTPS.

Open-AudIT works perfectly fine using HTTPS. But - there's always a but... We do **require** http traffic be allowed from localhost / 127.0.0.1. This is for Open-AudIT to spawn more processes when discovery runs and for task execution (well, task checking for execution). As the traffic is localhost only, it never actually hits the network interface, so is never at risk of being eavesdropped upon. We also do not use these connections to send any sensitive information. They are purely to tell Open-AudIT "check if any tasks need running" or "start another discovery thread".

If your security group insists that http be disabled from absolutely everywhere (including localhost), Opmantek is always will to assist a supported customer achieve this. Having said that:

- The onus and burden of maintaining the required changes after each upgrade will fall to you.
- This work may be chargeable.
- There is **no** security benefit to disabling localhost http.

Configuring https is an exercise left to your System Administrator as no code or configuration changes are required in the Open-AudIT application itself.

If you are usign a self-signed certificate, edit the file -

Windows c:\omk\conf\opCommon.json

Linux - /usr/local/omk/conf/opCommon.json

In the omkd section find (or add if it's not there) **omk_ua_insecure** and set it to **1**.

Restart the daemon for it to take effect -

Windows - restart the task in the task scheduler.

Linux - sudo systemctl restart omkd