4.4.7.3

Features

- DMZ Mode
  - Optional configuration to use a signed CA bundle for TLS communication with authentication and telemetry servers. These CA bundles are then protected from tampering or deletion by Cyber Crucible’s proprietary anti-tampering capabilities.
  - OCSP and CRL checks are disabled to reduce the list of domains to allow through a firewall.

Fixes

- Reduced memory usage and CPU time spent on memory diff submission, especially after long offline periods.

MD5 Hashes

```
service.exe  = 536adc06bd5ac3d4caca53dd5b780759
CCRRSecMon.sys (Windows7)        = dc446d663e8c865b039de0eb585de1fb
CCRRSecMon.sys (Windows8)        = ea96fdf4b097ac9afb646e6a766431aa
CCRRSecMon.sys (Windows10)       = 434c9061390804e4e61f5299158aaa00
```

Revision #1
Created 2026-07-13 18:49:58 UTC by Dennis Underwood
Updated 2026-07-13 18:49:58 UTC by Dennis Underwood