KDFM eXplorer

PLATFORM SECURITY – Specific to New DCA version 4

- Servers located in the EU
- Independent Software Vendor (ISV) not tied to any manufacturer of hardware
- Recurring-cycle of DCA Application Security Assessments by independent cybersecurity consulting firms
- Platform certified with ISO27001 and complies with the European Data Protection Regulation (GDPR).
- GDPR compliance: a Data Processing Agreement (DPA) via automated e-signing process
- Developed in complicance with OWASP Top Ten Web Application Security Risks | OWASP
- In order to exchange data and receive information about tasks to be performed, the software uses HTTP2 GRPC polling calls (usually sent once every 5 minutes) and MQTT connection to a Server that can be reached through different domain URLs belonging to the root domain https://*.mpsmonitor.com. The MQTT connection uses as default MQTT over WSS (port 443). It can be configured also to work as a standard MQTT connection (port 8883)
- Support for SNMPv1/v2 and v3 and device discovery by hostnames
- All web services are protected by RSA SHA -2 256 Bit TLS encryption. 1.2
- Advanced User Authentication: Two-factor authentication, Single Sign-On (SSO) for Active Directory users (portal access via Windows authentication), granular user permissions, user deactivation after 5 unsuccessful attempts or if there is no connection within 90/180 days, DCA executable file disabled after 5 times.
- Certifications: SOC 2 Audit report Type 1 provided by A-LIGN, Okta, BLI Security validation test, ISO 27001 TUV
- SOC 2 Type 1 Security Audit Compliance: the practices and controls comply with the Security, Availability, Confidentiality requirements established by AICPA (American Institute).

Additional info:

1. The Cloud can't "call" the DCA installed on the PC so NO port or service is exposed to the internet by the customer networks.
2. It is always the DCA that starts the communication through GRPC and MQTT protocols and to a TCP endpoint (port 443) and the communication is encrypted using the SSL certificate.
3. Port 22 is needed to execute Device Web Access using SSH protocol
4. The DCA uses the SNMP protocol on port 161 to read printers MIB in the customer network and only for the range of IP Address configured. Device Web Access connects to printers using HTTP on port 80, 433, 8000 or others specifically configured. Port 9100 and 631 can also be used to access the printer.
5. The DCA can send ICMP packets (there is no port specification) as well (this is used during troubleshooting)
6. There aren't any other port or protocol.