

# KDFM eXplorer

## PLATFORM SICHERHEIT - DCA Version 4

- Server mit Standort in der EU
- Unabhängiger Software-Anbieter (ISV), der nicht an einen Hardware-Hersteller gebunden ist
- Wiederkehrender Zyklus von DCA Applicationen Security Assessments durch unabhängige Cybersecurity Beratungsunternehmen
- Zertifizierungen nach ISO/IEC27001, SOC 2 Typ 2 und CSA Star Level 2
- Mit diesen Zertifizierungen wird anerkannt, dass die Infrastruktur, die Software, die Mitarbeiter, die Daten, die Richtlinien, die Verfahren und die Abläufe formell überprüft wurden und den Anforderungen an Sicherheit, Verfügbarkeit und Vertraulichkeit entsprechen, die vom AICPA (American Institute)
- SOC2 Typ2 <https://www.a-lign.com/articles/european-business-soc-2-assessment>. Das Zertifikat ist für die Händler im KDFM eXplorer-Portal nach Unterzeichnung eines NDA verfügbar.
- CSA Star2 <https://cloudsecurityalliance.org/star/registry/mps-monitor-srl/>
- Konform mit der Europäischen Datenschutzverordnung (GDPR); Datenverarbeitungsvertrag (DPA) über automatisiertes e-Signing-Verfahren
- Um Daten auszutauschen und Informationen über auszuführende Aufgaben zu erhalten, verwendet die Software HTTP2 GRPC Polling-Aufrufe (in der Regel einmal alle 5 Minuten) und eine MQTT-Verbindung zu einem Server, der über verschiedene Domain-URLs erreicht werden kann, die zur Root-Domain [https://\\*.mpsmonitor.com](https://*.mpsmonitor.com) gehören. Die MQTT-Verbindung verwendet als Standard MQTT über WSS (Port 443). Sie kann auch so konfiguriert werden, dass sie als Standard-MQTT-Verbindung funktioniert (Port 8883).
- Unterstützung für SNMPv1/v2 und v3 und Geräteerkennung über Hostnamen
- Alle Webdienste sind durch RSA SHA -2 256 Bit TLS-Verschlüsselung geschützt. 1.2
- Erweiterte Benutzerauthentifizierung: Zwei-Faktor-Authentifizierung, Single Sign-On (SSO) für Active Directory-Benutzer (Portal-Zugang über Windows-Authentifizierung), granulare Benutzerberechtigungen, Deaktivierung des Benutzers nach 5 erfolglosen Versuchen oder wenn innerhalb von 90/180 Tagen keine Verbindung besteht, Deaktivierung der ausführbaren DCA-Datei nach 5 Versuchen.

### Zusätzliche Informationen:

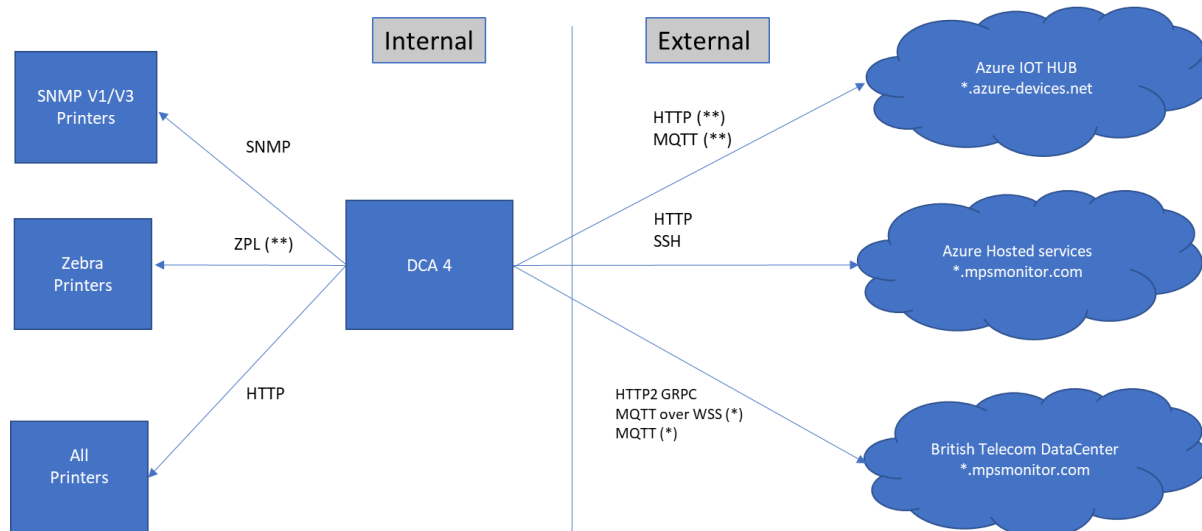
1. Die Cloud kann das auf dem PC installierte DCA nicht "anrufen", so dass KEIN Port oder Dienst von den Kundennetzen dem Internet ausgesetzt wird.
2. Es ist immer der DCA, der die Kommunikation über GRPC- und MQTT-Protokolle und einen TCP-Endpunkt (Port 443) startet, und die Kommunikation wird mit dem SSL-Zertifikat verschlüsselt.
3. Port 22 wird benötigt, um Device Web Access über das SSH-Protokoll auszuführen.
4. Der DCA verwendet das SNMP-Protokoll an Port 161, um die MIB von Druckern im Kundennetzwerk zu lesen, und zwar nur für den Bereich der konfigurierten IP-Adresse. Device Web Access stellt die Verbindung zu den Druckern über HTTP an den Ports 80, 433, 8000 oder anderen speziell konfigurierten Ports her. Port 9100 und 631 können ebenfalls für den Zugriff auf den Drucker verwendet werden.
5. Das DCA kann auch ICMP-Pakete senden (es gibt keine Port-Spezifikation) (dies wird bei der Fehlersuche verwendet).
6. Es gibt keinen anderen Port oder kein anderes Protokoll.



## DCA4 Network requirements:

Destination Network	Direction	Protocol	Port
External (*.mpsmonitor.com) for Device Monitoring communication	Outbound	TCP	TCP 443 (HTTP2 GRPC)
External (*.mpsmonitor.com) for Device Web Access and Updates	Outbound	TCP	TCP 443 (HTTPS) TCP 22 (SSH)
External (*.azure-devices.net) for MQTT messaging	Outbound	TCP	TCP 443 (MQTT over WSS) TCP port 8883 (MQTT)
Internal (Networks with Devices) for Device Monitoring	Outbound	UDP	UDP 161 (SNMP)
Internal (Networks with Devices) for Device Web Access and HP LFP	Outbound	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Internal (Networks with Devices) for Zebra commands	Outbound	TCP	TCP 9100 TCP 515 (LPR)

## Network Diagram:



(\*) current service that will be replaced in the next months. (\*\*) new endpoint/services that will be added in the next months

## Specific Endpoints and IP addresses:

Hostname	Protocol	Ports	Ip Address/ CDN entry
https://dca4.mpsmonitor.com	HTTP2, GRPC, MQTT, MQTToverWSS	443, 8883	213.92.56.75
https://cdn2.mpsmonitor.com	HTTP	443	Azure CDN
dcaws.mpsmonitor.com	SSH	22	13.80.42.210
eu01-broker-mpsmonitor.azure-devices.net	MQTT, MQTToverWSS	443, 8883	Azure IOT HUB