# KDFM eXplorer

## SECURITE DE LA PLATEFORME – DCA version 4

- Serveurs basés en Europe
- Editeur de Logiciel Indépendant (ISV) sans aucun lien avec un constructeur d'équipement OEM
- Cycle récurrent d'évaluations de la sécurité des applications DCA par des sociétés de conseil indépendantes en cybersécurité
- Plateforme certifiée ISO27001, SOC 2 Type 2 et CSA Star Niveau 2
- Ces certifications reconnaissent que l'infrastructure, les logiciels, les personnes, les données, les politiques, les procédures et les opérations ont été formellement examinés et sont conformes aux exigences de sécurité, de disponibilité et de confidentialité établies par l'AICPA (American Institute)
- SOC 2 Type 2 https://www.a-lign.com/articles/european-business-soc-2-assessment. Le certificat est disponible pour les revendeurs dans le portail KDFM eXplorer après avoir signé un accord de confidentialité.
- CSA Star 2 https://cloudsecurityalliance.org/star/registry/mps-monitor-srl/
- Conformité au règlement européen sur la protection des données (RGPD). Accord de traitement des données (DPA) via un processus de signature électronique automatisé.
- Afin d'échanger des données et de recevoir des informations sur les tâches à effectuer, le logiciel utilise des appels d'interrogation HTTP2 GRPC (généralement envoyés une fois toutes les 5 minutes) et une connexion MQTT à un serveur accessible via différentes URL de domaine appartenant au domaine racine https ://*.mpsmonitor.com. La connexion MQTT utilise par défaut MQTT sur WSS (port 443). Il peut également être configuré pour fonctionner comme une connexion MQTT standard (port 8883)
- Prise en charge des protocoles SNMPv1 /v2 et v3 et découverte des périphériques par nom d'hôte
- Tous les services Web sont protégés par le cryptage RSA SHA -2 256 bits TLS. 1.2
- Authentification utilisateur avancée : authentification à deux facteurs, authentification unique (SSO) pour les utilisateurs Active Directory (accès au portail via l'authentification Windows), autorisations utilisateur granulaires, désactivation de l'utilisateur après 5 tentatives infructueuses ou s'il n'y a pas de connexion dans les 90/180 jours, Fichier exécutable DCA désactivé après 5 essais

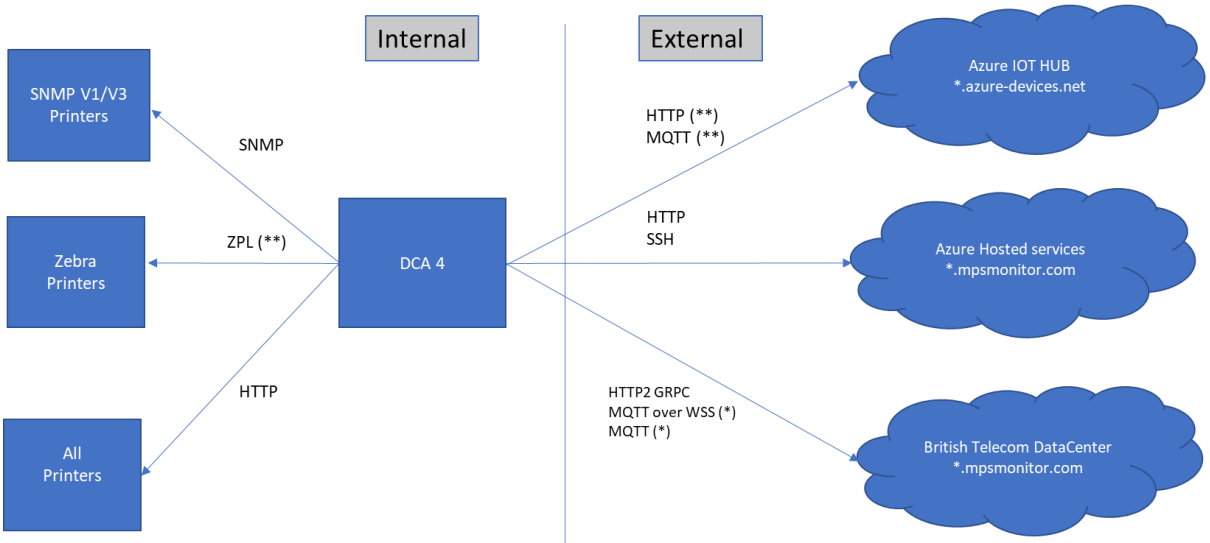
**Informations complémentaires :**

1. Le Cloud ne peut pas "appeler" le DCA installé sur le PC donc AUCUN port ou service n'est exposé à Internet par les réseaux clients.
2. C'est toujours le DCA qui démarre la communication via les protocoles GRPC et MQTT et vers un point de terminaison TCP (port 443) et la communication est cryptée à l'aide du certificat SSL.
3. Le port 22 est nécessaire pour exécuter Device Web Access à l'aide du protocole SSH
4. Le DCA utilise le protocole SNMP sur le port 161 pour lire les imprimantes MIB sur le réseau client et uniquement pour la plage d'adresses IP configurée. Le Device Web Access se connecte aux imprimantes via HTTP sur les ports 80, 433, 8000 ou autres spécifiquement configurés. Les ports 9100 et 631 peuvent également être utilisés pour accéder à l'imprimante.
5. 5. Le DCA peut également envoyer des paquets ICMP (il n'y a pas de spécification de port) (ceci est utilisé lors du dépannage)
6. Il n'y a pas d'autre port ou protocole.

## 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)<br>TCP 22 (SSH) |
| **External (*.azure-devices.net) for MQTT messaging** | Outbound | TCP | TCP 443 (MQTT over WSS)<br>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)<br>TCP 443 (HTTPS) * custom ports |
| **Internal (Networks with Devices) for Zebra commands** | Outbound | TCP | TCP 9100<br>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 |