



Print Aware Powered by MPS Monitor

What is Print Aware?

Print Aware is a data collection tool specialized for copiers and printers. Print Aware scans and gathers Toner Levels and Meter Counts from copiers and printers on the network. Print Aware uses SNMP (Simple Network Management Protocol) to pull the MIB (Management Information Base) from the print devices on the network. The MIB contains information such as Serial Number, Make, Model, IP Address, Meter Counts, and Toner Levels for each print device.

What is the Data Path for MPS Monitor?

The MPS Monitor solution is a secure platform used to manage devices including A3, A4, thermal devices (Zebra) and scanners. Please see the following document to better understand the data path.

MPS Monitor Data Path

The MPS Monitor solution is a secure platform used to manage millions of devices around the world including A3, A4, thermal devices (zebra) and scanners.

Secure Solution



Admin Portal

Administrators of the MPS Monitor portal are able to authenticate and review the configurations of the MPS Monitor service, enact changes and download the DCA which will be installed within the customer environment.

Data sent

- "Printer metadata"
- "Printer Make"
- "Printer Model"
- "Printer's Serial number"
- "Printer's Mac address"
- "Printer's internal IP address"
- "Printer's Firmware version"
- "Encrypted Metadata"

Data NOT sent

- Who printed print job (username)
- What was printed (document type)
- Which printer the user printed to
- User's Full Name
- User's email address
- User password
- Credit card information
- Personal information

URLs, IPs, Ports

https://us01-dca.mpsmonitor.com <i>for DCA4 Device Monitoring Communication</i>	HTTPS2, GRPC - 443 <i>20.106.185.115</i>
us01-dcaws.mpsmonitor.com <i>for DCA4 Device Web Access</i>	SSH - 22 <i>20.55.38.55</i>
us01-broker-mpsmonitor.azure-devices.net <i>for DCA4 MQTT communication</i>	MQTTOverWSS - 443 <i>Azure IOT HUB</i>
https://cdn2.mpsmonitor.com <i>for DCA3 and DCA4 updates</i>	HTTP - 443 <i>Azure CDN</i>
https://usdca.mpsmonitor.com <i>for DCA3 device monitoring and communication</i>	HTTP - 443 <i>66.22.0.0/17</i>



British Telecom DC

Data is stored in the British Telecom data center which is:

- Secure by default
- Facility that has high availability and redundancy
- ISO27001 certification
- GDPR Compliant environment - as per US State legislation
- SOC2 Type 2
- Third party security audit

Secure communication to US connection point

Data on route to the cloud service communicates with the US data center through an encrypted & secure channel



DCA initiates communication from customer environment using a secure HTTPS over port 443 to the cloud service!