PRINTFLEET SECURITY AT A GLANCE

PrintFleet is committed to providing secure software solutions for use in all network environments. Data security and privacy continue to be growing concerns for businesses and individuals as more processes are enabled by the internet. In response to these changes, PrintFleet has ensured its security protocols and infrastructure meet updated industry standards.

Data Collection Agent

PrintFleet's data collection agent (DCA 4.x and DCA Pulse) is a software application installed in a print environment to collect device metrics such as meters, supplies, error codes and device attributes. The data is securely transmitted to the PrintFleet Optimizer (PFO) web interface so MPS providers can access this information to remotely monitor and manage devices.

Types of Data Collected

PrintFleet software solutions only collect critical device metrics necessary to manage print environments. No personal or user information is collected by either DCA 4.x and DCA Pulse. DCAs will attempt to collect the following information from networked printing devices during a network scan:

- IP address (can be masked)
- Toner cartridge serial number
- Device description
- Maintenance kit levels
- Serial number
- Non-toner supply levels
- Meter reads
- Asset number
- Monochrome or color identification
- Location
- LCD reading
- MAC address
- Device status
- Manufacturer
- Error codes
- Firmware
- Toner levels
- Miscellaneous (machine specific)

For local devices, the Local Print Agent (LPA) attempts to collect the following information:

- Manufacturer
- Asset number
- Device description
- Location
- Serial number
- Meter reads
- IP address of the machine the LPA is installed on (LPA Host)
- OS version of LPA Host
- Name of the account used to run LPA service
- Miscellaneous (machine specific)

PRINTFLEET SECURITY AT A GLANCE

Data Security Measures

PrintFleet software solutions use the following security measures to encrypt and protect data during transmission and prevent unauthorized access:

	Hypertext Transport Protocol (HTTP)	Hypertext Transport Protocol Secure (HTTPS)
DCA 4.x	Encrypts submission data with 128-bit TripleDES using the Shared Key. Device data is encrypted, message header/wrappers are not.	Encrypts submission data using the Public Key (SSL certificate). Device data and message header/wrappers are encrypted.
DCA Pulse	DCA Pulse not available with HTTP.	Encrypts submission data using the Public Key (SSL certificate). Device data and message header/wrappers are encrypted.

SNMP

All data collected by the DCA and transmitted to PFO consists of data points extracted from hardware components by the device firmware and exposed through the Simple Network Management Protocol (SNMP) service operating on the print device. Both DCA 4.x and DCA Pulse fully support SNMP v3 for secure, credentialed SNMP communications.

User Management

Access to PFO is controlled via permissions-based user management. Users must log in to PFO using a designated username and password.

Data Privacy and Legislation

Due to the nature of PrintFleet's software, compliance with the following security protocols is not affected by the use of PrintFleet software applications:

- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)
- Payment Card Industry Data Security Standards (PCI DSS)

For information on the EU General Data Protection Regulation (GDPR), please see PrintFleet's data privacy policy. For the complete PrintFleet Security and Data Privacy Overview, please contact your MPS provider.