eci™

DS Business Life Simplified

PrintFleet Security and Data Privacy Overview

V1.0

Table of Contents

Introduction

PrintFleet has always been committed to providing software solutions that are secure for use in all network environments. Data protection, digital security and privacy continue to be growing concerns for businesses and individuals as more and more processes are enabled by the Internet. Due to changes in customer expectations and concerns about the way data is collected and stored, PrintFleet has updated security protocols and infrastructure to address these updated industry standards.

It is important to note that PrintFleet software products only collect the critical imaging device metrics necessary to manage a printing environment and do not collect any personal or user information.

This security and data privacy overview examines the following:

- Server Hardware and Software
    - Self-Hosted
    - PrintFleet Hosted Solutions
- DCA Pulse
    - Data Collected
    - Types of Information Collected
    - Network Operations
    - Communications to Optimizer and PrintFleet Central
    - HP Smart Device Services
- Data Collection Agent (DCA) 4.x and Local Print Agent
    - Activation and Submission Authentication
    - Data Collection Methods
    - Data Transmission Methods
    - Data Transmission Formats
    - Network Traffic
    - Optional Remote Updates
    - Remote DCA 4.x Management
- PrintFleet Central
    - Data Transmitted and Held
- PrintFleet Optimizer application
    - Permissions Based User Management
    - HTTPS Access
- Version Management
    - Testing and Release Process
    - Source Code Security
- Data Privacy and Legislation
    - General Data Protection Regulations
    - 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)

DCA Pulse

DCA Pulse, our next generation data collection agent (DCA), has been fundamentally redesigned for a faster, more efficient and more accurate data collection process. DCAs are deployed remotely at customer sites to gather data about imaging devices and the network on which they operate and transmit that data to PrintFleet Optimizer (PFO) which is running in a separate location. With data transmission, there are inherent concerns about security and data privacy. It is important to clearly understand these concerns to explain any potential risks and impact of deploying a DCA and appropriately respond to customer concerns.

Data Collected

PrintFleet does not collect or process any personal data. The only way the system can collect this type of information is if you or your customers add them to a field or label such as a location or customer name.

DCA Pulse enables you to monitor network devices using Simple Network Management Protocol (SNMP). It exists inside the customer's network and from there, it communicates with devices to gather operational information about the device that is made available via the device firmware and an SNMP Management Information Base (MIB). The data exposed by the device varies by manufacturer and model, but it is always technical or operational in nature and specific to the device itself. At the most basic level the data exposed by a printer MIB is documented in the IETF RFC 3805 (https://tools.ietf.org/html/rfc3805). Additional device information may be exposed by the manufacturer through extensions and private MIBs, but the information is fundamentally technical and device-specific.

Types of Information Collected

DCA Pulse and DCA 4.x attempt to collect the following information from networked printing devices during a network scan:

- IP address
- 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)

DCA 4.x with assistance of the Local Print Agent (LPA) attempts to collect the following information from local devices:

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

No print job or user data is collected.

Network Operations

DCA Pulse performs a discovery scan of the target network by walking a range or ranges of IP addresses and attempting to communicate with each active device via SNMP on port 161/udp. DCA Pulse must be able to communicate to the local network using that port at a minimum. DCA Pulse fully supports SNMPv3 for secure (credentialed) SNMP communications.

DCA Pulse may communicate with some devices on other ports such as 9100/tcp (PDL), 80/tcp (HTTP) or 443/tcp (HTTPS). Additionally, there may be manufacturer-specific implementations, such as HP Smart Device Services (SDS), that require communication on other ports under certain circumstances. PrintFleet Technical Support can answer questions about specific port requirements for a particular manufacturer and device.

On Windows, the DCA Pulse service runs as a Local System in the Microsoft Windows security model. On Linux, by default, it runs as the user that installs it and on macOS it runs as the system user.

Communications to Optimizer and PrintFleet Central

DCA Pulse communicates to PFO using HTTPS (443/TCP) and will only use a TLS connection to the for secure communications, preferably TLS version 1.2 where possible. The HTTPS connection to PFO is kept open as long as the DCA is running. The connection is normally done using WebSockets but will fall back to using server-sent-events or long-polling if necessary. Data is only sent when changed.

DCA Pulse communicates with PrintFleet Central (PFC) for registration and to maintain a status heartbeat, and this communication is done using DNS (53/udp) with TXT lookups. Normally this communication happens via the local network DNS server, but if that fails, DCA Pulse will attempt to make a DNS query directly to PFC and well-known public DNS services. The registration and heartbeat communication include only a unique identifier, activation PIN, DCA version, and operating system name and version.

DCA Pulse will also connect to PFC using HTTPS (443/tcp) for both checking for and downloading software updates.

All conversations with PFO and PFC are initiated from DCA Pulse. At no point does either PFO or PFC initiate communication or require the DCA to accept any inbound connections.

Data sent to PFO is device-specific information about device attributes, supply levels, meters and error codes. All data requested from devices and transmitted to PFO consists of information points extracted from device hardware components by the device firmware and then exposed through the SNMP service or other proprietary protocols operating on the imaging device. No information about print jobs, content of any print job or information about the owner of a print job is requested from the device.

HP Smart Device Services

HP SDS is a set of tools and device capabilities designed to simplify device management.
When installing a DCA Pulse with HP SDS enabled, HP’s JetAdvantage Management Connector (JAMC) will also be installed then registered with HP JetAdvanatge Management Cloud. HP’s JAMC receives device information and performs operations on registered devices from PFO.

DCA 4.x and Local Print Agent

DCA 4.x is a software application that is installed and registered on a non-dedicated networked server at each location where imaging device metrics are to be collected. DCA 4.x can collect data from network imaging devices that have a network interface and are connected to the network the DCA is set up to monitor.

The PrintFleet Local Print Agent (LPA) is a software application that is installed on a non-dedicated networked server or on a networked workstation with one or many local, non-networked imaging devices connected to the server/workstation. The LPA acts as a proxy between a DCA 4.x and local devices, receiving requests from the DCA, transforming these requests into printer-compatible commands and sending device responses back to DCA 4.x.

DCA 4.x and the LPA run as Windows services, allowing them to operate 24 hours a day, 7 days a week. Optionally, DCA 4.x can run as a scheduled task.

It is important to note that DCA 4.x is our legacy collection agent and its capabilities, minus the LPA, are now available through DCA Pulse. The only reason you would need to install DCA 4.x is if you need to monitor locally connected devices.

Activation and Submission Authentication

DCA 4.x must be activated on a PFO server prior to data submission to the server. DCA 4.x activation is managed by PFO Administrators.

When a DCA 4.x is created, a PIN code is issued which can be used to activate the DCA. The PIN code can only be used once and is simply a lookup key to connect the physically installed DCA to a record on the server. During the activation process, the server looks up the PIN code and, if found, the server creates a new 128-bit shared key to be used to encrypt all future communication. The key is exchanged with DCA 4.x using temporary RSA public-private keys. This allows a secure exchange even when communicating over non-secure transport (HTTP). At no point is any part of the RSA keys persisted to storage on either the DCA 4.x or the server. After activation is successful, the PIN code is deleted and cannot be used to activate a DCA 4.x again, nor can it be used to determine which DCA 4.x it was used with. Although PIN codes may be re-used, the chances of a previously-used PIN code being able to activate are equal to guessing a valid PIN code (approximately 1 in 12.9 million).

DCA 4.x can have an expiration date that determines when their credentials to submit data to the PFO server are revoked automatically; a PFO Administrator also can revoke these credentials at any time by de-activating the DCA 4.x. Data submissions from a DCA start being rejected by the PFO server immediately after the DCA 4.x Expiration Date comes into effect or the DCA 4.x is de-activated.

PFO checks if the submitting DCA 4.x has an active account on the server prior to data acceptance. If the DCA 4.x account exists and is active, the data is saved in a database on the server for further processing; otherwise, the submission is ignored and no data is saved on the server.

All files are encrypted using TripleDES and protected with the 128-bit shared key while stored on disk and in transport (in addition to any Transport Layer Security). This ensures end-to-end encryption so data is protected from being read if intercepted by a third party, a competitive or otherwise non-authorized PFO instance. It also provides protection for

PFO in that PFO will not read data (potentially using licenses for new devices) from DCAs that are accidentally routed to the wrong server. Additionally, device data cannot be faked or modified.

The shared key that is used to encrypt data exchange between a PFO server and a DCA 4.x is stored in the PFO server database and is protected by means of MS Windows Server and MS SQL Server security. It is the responsibility of the MS Windows Server and MS SQL Server Administrator to implement security policies to exclude the possibility of unauthorized access to the shared key. Neither PFO nor other PrintFleet components expose shared keys to users. DCA 4.x installation stores the shared key in encrypted local storage.

Data Collection Methods

DCA 4.x collects networked imaging device metrics at a specified interval by polling networked devices using SNMPv1 or SNMPv3, and additional protocols including HTTP and proprietary manufacturer-specific ones.

DCA 4.x collects local device metrics at a specified interval by polling LPAs using ports 35/tcp and 35/udp. The LPA must allow inbound connections from the DCA on these ports. Request and response data is transferred using PrintFleet proprietary format.

Data Transmission Methods

DCA 4.x transmits the collected data to the centralized database via HTTPS (port 443/tcp recommended) or HTTP (port 80/tcp).

It is recommended that users transmit data using HTTPS because this provides the industry-standard security of TLS encryption. To transmit using HTTPS, the machine receiving the transmitted data must be installed with a valid SSL security certificate. When the DCA communicates over non-TLS HTTP connections, the device data is still encrypted and protected as described below.

Data Transmission Formats

DCA 4.x encrypts submission data with 128-bit TripleDES using the shared key. This provides on-disk protection and authenticity and adds an additional layer of data protection during transfer from the DCA 4.x to the PFO server. It also provides server validation during DCA 4.x submission. This additional encryption ensures that if SSL (HTTPS) is not being used, even though the message header/wrappers are not encrypted, the actual content containing any device data is encrypted. If SSL (HTTPS) is being used, it provides an additional layer of security so the message wrappers are encrypted as well. PrintFleet software uses encryption providers integrated into the Microsoft .NET Framework to encrypt data exchanged between DCA 4.x and PFO.

Network Traffic

The network traffic created by the DCA 4.x is minimal and will vary depending on the number of IP addresses being scanned. The table below outlines the network load associated with the DCA compared to the network load associated with loading a single standard webpage.

Network Byte Load Associated with the DCA 4.x

Event	Approximate Total Bytes
Loading a single standard webpage	60 KB

DCA scan, single empty IP address	5.2 KB
DCA scan, 1 device only	7.2 KB
DCA scan, 1 device, 254 total IPs	96 KB
DCA scan, 15 device, 254 total IPs	125 KB

Optional Remote Updates

DCA 4.x contains an optional remote update feature which is activated by enabling the Health Check and Intelligent Update options. Health Check will periodically ensure that the DCA 4.x service is operating and, if not, it will restart the DCA 4.x service. Intelligent Update allows the DCA 4.x to check for and receive software updates, and DCA 4.x configuration changes posted by an Administrator on the PFO server. These optional features are enabled and disabled at the end user site.

Remote DCA 4.x Management

PFO Administrators can remotely manage DCA 4.xs activated on the server using the following commands:

Deactivate	Forces the target DCA 4.x to de-activate itself
MIB Walk	Forces the target DCA 4.x to request all available OIDs from the device whose IP is specified in the command's parameter
Redirect	Forces the target DCA 4.x to stop files submission to its old PFO server, to start submission to the PFO server whose URL is specified in "ServerUrl" parameter of the command, and , if "DeActivate" parameter is set to "True", to de-activate itself on the old PFO server
Update	Forces the target DCA 4.x to check for updated available for its current version and, if there are updates available, to upgrade itself using the update
Uninstall	Forces the target DCA 4.x to uninstall itself

None of these commands lead to data collection beyond the types of information collected as described above. Data exchanged between DCA 4.x and PFO is encrypted using the same algorithm that is used for data submission and is based on a unique shared key. DCA 4.x receives software updates from its associated PFO server.

The DCA receives these commands at the end of its data transmission, using the same mechanism that the transmission uses (HTTP or HTTPS), and the DCA always initiates this communication to the server.

PrintFleet Central

PFC is a centralized system that manages all PFO installations and DCA Pulse deployments. It handles various tasks including PFO licensing and anonymous collection of device data as well as updates for operational components of the PFO system.

Data Transmitted and Help

PrintFleet Central may store the following anonymous device data collected by DCA Pulse:

- Manufacturer and model information, including hrDeviceDescription, hrDeviceId and SNMP Enterprise Numbers
- Manufacturer, model and ModelId, a generated string of characters that uniquely identifies models within the PrintFleet Model Database
- Model match type, an indicator of how a device was matched to a model description from the Model Database
- Device type, an internal device classification number
- Device-specific fields like SysName (user-configurable on some devices), hostname and location (user-configurable) Device serial number, MAC address and IP address
- Device entry creation and last active dates
- List of meters: name, last reported, last value, standadLabelID (if applicable)
- List of supplies: name, last reported, high percent, low percent, status, standardLabelId
- List of codes: code, type, count, group, groupIndex, location
- Engine firmware version

PrintFleet Central may also store the following data:

- Current license status
- License status changes
- DCA versions and timelines of DCAs that reported this device
- TotalCount by month

PrintFleet Optimizer Application

PrintFleet Optimizer functionality is accessible via a web-based user interface.

Permissions based user management

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

Users are assigned one or more roles which specify permissions and are granted access to one or more groups of devices. Administrators will full permissions can specify exactly which screens each user can view and/or interact with.

HTTPS access

The website can be accessed using HTTPS provided that the web server is installed with a valid SSL security certificate. Optionally, PFO Administrators can require users that access the website using HTTPS by redirecting the HTTP version of the website. We recommended this as it ensures encryption of data being transferred over the Internet.

Version Management

Testing and Release Process

Each major and minor release of the software goes through a quality control process, in which multiple PrintFleet personnel test altered portions of the system to ensure there has not been a downgrade in security or functionality of the system. Major releases go through a beta release process where select clients run the new and old systems in parallel.

Source Code Security

PrintFleet source code is kept in a secured revision control system, accessible only to authorized persons. Every change to the source code is tracked, which includes which developer made the change and why. Products are encrypted and digitally signed with a code-signing certificate before shipping.

Data Privacy and Legislation

General Data Protection Regulations

As of May 2018, the European Union's General Data Protection Regulations (GDPR) came into full effect. The GDPR replaces the Data Protection Directive 95/46/EC and is designed to strengthen and unify data privacy laws across Europe.

For more information on PrintFleet's data privacy policy, visit https://www.printfleet.com/company/data-privacy.php.

Health Insurance Portability & Accountability Act (HIPAA)

Health Insurance Portability & Accountability Act (HIPAA) compliance is not affected by usage of PrintFleet software applications
The use of PrintFleet software applications are not seen to have an impact on compliance with the Health Insurance Portability & Accountability Act (HIPAA) for covered entities. This is because PrintFleet software applications do not collect, house or transmit any information regarding the content of print jobs, so have no way of accessing, housing or transmitting electronic protected health information (ePHI) as defined by HIPAA.

For more information about HIPAA, visit http://www.hhs.gov/ocr/privacy/.

Sarbanes-Oxley

Sarbanes-Oxley compliance is not affected by usage of PrintFleet software applications
PrintFleet software is not intended to be used as part of an internal control structure as outlined in Section 404: Management Assessment of Internal Controls but will not interfere with these controls. Information Technology controls are an important part of complying with Sarbanes-Oxley. Under this Act, corporate executives become responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting. There are IT systems in the market that are designed specifically for meeting these objectives. PrintFleet software is not designed as an IT control system but will not interfere or put at risk other systems that are intended for that purpose.

For more information about Sarbanes-Oxley, visit http://www.sec.gov/about/laws/soa2002.pdf.

Gramm-Leach-Bliley Act (GLBA)

Gramm-Leach-Bliley Act (GLBA) compliance is not affected by usage of PrintFleet software applications
The use of PrintFleet software applications are not seen to have an impact on compliance with the Gramm-Leach-Bliley Act (GLBA) for covered entities. This is because PrintFleet software applications do not collect, house or transmit any information regarding the content of print jobs, so have no way of accessing, housing or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by PrintFleet software applications.

For more information about the Gramm-Leach-Bliley Act, visit http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

Federal Information Security Management Act (FISMA)

Federal Information Security Management Act (FISMA) compliance is not affected by usage of PrintFleet software applications
PrintFleet software applications are not intended to be part of an internal control system for FISMA but will not interfere with these controls. The use of PrintFleet software applications are not seen to have an impact on compliance with FISMA for covered entities. This is because PrintFleet software applications do not collect, house or transmit any information regarding the content of print jobs, so have no way of accessing, housing or transmitting high risk information, even if this information is printed or otherwise sent to print devices monitored by PrintFleet software applications.

For more information about the Federal Information Security Management Act,
visit http://csrc.nist.gov/groups/SMA/fisma/index.html.

PCI DSS (Payment Card Industry Data Security Standards)

PCI DSS (Payment Card Industry Data Security Standards) compliance is not required for PrintFleet software applications
The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI DSS standards apply to all organizations that store, process or transmit cardholder data. These organizations must be PCI DSS compliant.

The use of PrintFleet solutions does not have an impact on PCI DSS compliance. PrintFleet software applications do not store, process or transmit cardholder data or personal information. PrintFleet solutions also does not collect, house or transmit any information regarding the content of print jobs, so has no way of accessing, housing or transmitting customers' personal financial information, even if this information is printed or otherwise sent to print devices monitored by PrintFleet software.

For more information about PCI DSS compliance, visit
https://www.pcisecuritystandards.org/security_standards/index.php.

DS Business Life Simplified
COPIER TEAM

New Jersey Office (HQ)
151 Sumner Avenue
Kenilworth, NJ 07033
908.653.0600

New York Office
30 Wall Street
New York, NY 10005
212.468.5200

www.dsbls.com