PrintFleet Security and Data Privacy Overview EMEA

Introduction

PrintFleet Inc. 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. As a result of changes in customer expectations and concerns about the way data is collected and stored, PrintFleet has altered security protocols and infrastructure to address these changes and 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:

- Data Collection Agent (DCA) 4.x and Local Print Agent
  - Activation and Submission Authentication
  - Types of Information Collected
  - Data Collection Methods
  - Data Transmission Methods
  - Data Transmission Formats
  - Network Traffic
  - Optional Remote Updates
  - Remote DCA 4.x Management
- DCA Pulse
  - Data Collected
  - Network Operations
  - Communications to Optimizer and PrintFleet Central
- PrintFleet Central
  - Data Transmitted and Held
- PrintFleet Optimizer application
  - Permissions Based User Management
  - HTTPS Access
- Data Privacy and Legislation
  - European Union (EU) Data Laws

Server Hardware and Software

Data Collection Agent 4.x and Local Print Agent

The PrintFleet Data Collection Agent 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. The DCA 4.x is capable of collecting data from imaging devices that have a network interface and are connected to the network the DCA 4.x is set up to monitor (Network Devices).

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

The DCA 4.x and the Local Print Agent run as Windows® services, allowing them to operate 24 hours a day, 7 days a week. Also, DCA can optionally run as a scheduled task.

Activation and Submission Authentication

DCA 4.x has to be activated on a PrintFleet Optimizer server prior to data submission to the server. DCA 4.x activation is managed by PrintFleet Optimizer Administrators.

When a DCA 4.x is created, a PIN code is issued which can be used to activate a DCA 4.x. The PIN code is one-time use, 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 the 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 accounts can have an expiration date that determines when their credentials to submit data to the PrintFleet Optimizer server are revoked automatically; a PrintFleet Optimizer 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 PrintFleet Optimizer server immediately after the DCA 4.x Expiration Date comes or the DCA 4.x is De-Activated.

PrintFleet Optimizer 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 Triple-DES, protected with the 128-bit shared key, including while stored on disk and in transport (in addition to any Transport Layer Security). This ensures end-to-end encryption.

The encryption provides a means of protection for the data:

- The data is protected from being read if intercepted by a 3rd party
- The data is protected from being read by a competitive or otherwise non-authorized PrintFleet Optimizer instance

It also provides protection for PrintFleet Optimizer:

- PrintFleet Optimizer will not read data (potentially using licenses for new devices) from DCAs that are accidentally routed to the wrong server
- Device data cannot be faked or modified

The Shared Key that is used to encrypt data exchange between a PrintFleet Optimizer server and a DCA 4.x is stored in the PrintFleet Optimizer 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 PrintFleet Optimizer nor other PrintFleet components expose Shared Keys to users.

DCA 4.x installation stores the shared key in encrypted local storage. The DCA 4.x can communicate to the server over HTTP and has support for SSL.

Types of Information Collected

DCA 4.x and DCA Pulse attempts 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, DCA 4.x with assistance of PrintFleet Local Print Agent attempts to collect the following information:

- 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.

Data Collection Methods

DCA 4.x collects networked imaging device metrics at a specified interval by polling networked devices using SNMP v1 or v3, ICMP, and HTTP.

DCA 4.x collects Local Device metrics at a specified interval by polling PrintFleet Local Print Agents using TCP and UDP requests at a predefined port (port 35). 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 – recommended) or HTTP (port 80).

It is recommended that users transmit data using HTTPS, because this provides SSL 128-bit encryption of the data during transmission. HTTP does not provide encryption in itself, but the underlying data is still encrypted (see Data Transmission Formats). To transmit using HTTPS, the machine receiving the transmitted data must be installed with an SSL security certificate.

Data Transmission Formats

DCA 4.x encrypts submission data with 128-bit TripleDES using the Shared Key. This adds an additional layer of data protection during transfer from the DCA 4.x to the PrintFleet Optimizer server, and 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 and even the message wrappers are encrypted. PrintFleet software uses encryption providers integrated into the Microsoft .Net Framework to encrypt data exchange between DCA 4.x and PrintFleet Optimizer.

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

The 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 a receive software updates and DCA 4.x configuration changes posted by an administrator on the PrintFleet Optimizer server. These features are enabled and disabled at the end user site, and are not required.

Remote DCA 4.x Management

PrintFleet Optimizer Administrators can remotely manage DCA 4.x's activated on the server through the use of 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 PrintFleet Optimizer server, to start submission to the PrintFleet Optimizer 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 PrintFleet Optimizer 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 leads to data collection beyond Types of Information Collected as described above. Data exchange between DCA 4.x and PrintFleet Optimizer 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 PrintFleet Optimizer Server.

When sending these commands to the DCAs, the PrintFleet Optimizer Server uses either HTTPS (port 443 – recommended) or HTTP (port 80).

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. Data collection agents 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 which is running in a separate location. As a result of this data transmission, there are

inherent concerns about security and data privacy. It is important to clearly understand these concerns in order 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. DCA Pulse enables customers 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 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.

DCA Pulse collects the same pieces of information that DCA 4.x did, please see **Types of Information Collected.**

Network Operations

The DCA Pulse service runs as local system in the Microsoft Windows security model. 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 Port 161 needs to be available for DCA Pulse to operate. DCA fully supports SNMP v3 for secure (credentialed) SNMP communications.

DCA Pulse may communicate with the device on Port 9100 to help determine if the active device is a printer. Additionally, there may be manufacturer-specific implementations 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.

Communications to Optimizer and PrintFleet Central

DCA Pulse has eliminated the use of unsecure hypertext transport protocol (HTTP), exclusively using hypertext transport protocol secure (HTTPS) and over transport layer security (TLS v1.2) to encrypt and protect information during transmission to PrintFleet Optimizer and PrintFleet Central.

All conversations with PrintFleet Optimizer and PrintFleet Central are initiated from DCA Pulse. At no point does either PrintFleet Optimizer or PrintFleet Central initiate communication or require any inbound openings. All communications are HTTPS over Port 443 other than the use of the DNS protocol for maintenance of a DCA Pulse 'heartbeat.'

DCA Pulse uses DNS protocol to register the new data collection with PrintFleet Central and to maintain a 'heartbeat' to PrintFleet Central, confirming that DCA Pulse is operating in the event that regular HTTPS communication to the relevant PrintFleet Optimizer fails or is blocked. The heartbeat communication is a DNS query with simple text to the DCA Registry DNS server that operates as a basic DCA Pulse identifying notification. No network or device information is transmitted to or received by the DCA Registry.

The HTTPS connection to PrintFleet Optimizer 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,

Data sent to PrintFleet Optimizer is device-specific information about device attributes, supply levels, meters and error codes. All data requested from devices and transmitted to PrintFleet Optimizer consists of information points extracted from device hardware components by the device firmware and then exposed through the SNMP service

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.

PrintFleet Central

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

Data Transmitted and Held

PrintFleet Central may collect the following fields for each device:

- Unique PrintFleet Optimizer internal deviceId, a globally unique generated string of characters with no identifying information
- 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 identifier
- Device 'name' or hrDeviceDescription, the name given to an imaging device on installation. The name identifies the device but is in no way related to any user of the device.
- Device serial number and MAC address
- Device entry creation and last active dates
- List of meters: name, last reported, last value, standardLabelId (if applicable)
- List of supplies: name, last reported, high percent, low percent, status, standardLabelId
- List of codes: code, type, count, group, groupIndex, location
- IsColor
- Engine firmware version
- Ccurrent license status

PrintFleet Central may also store the following aggregate data about the device:

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

Another measure taken to meet regulatory standards is that of data storage for customers who use PrintFleet hosted services. Data for European clients is stored in Europe at the Amazon Web Services (AWS) Dublin site and data for North American clients in stored at AWS' various North American locations.

PrintFleet Optimizer Application

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

Permissions based user management

Access to the PrintFleet Optimizer web console is controlled with permissions-based user management. Users must log in to PrintFleet Optimizer 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 an SSL security certificate. Optionally, PrintFleet Optimizer administrators can force users to access the website using HTTPS, by redirecting the HTTP version of the website. This is recommended, as it ensures encryption of data being transferred over the Internet.

Data Privacy and Legislation

European Union (EU) Data Laws

As of May 2016, European Union legislation was passed that gives individuals control over their personal data and simplifies the regulatory environment for businesses. PrintFleet took these regulations into account in the design of DCA Pulse to ensure that it complies with European Union Data Protection laws specifying the security, storage and transmission of client information.