



PrintFleet Software Security

PrintFleet Data Collector Agent

Overview

The PrintFleet Data Collector Agent (DCA) is a software application that is installed on a networked computer running Windows 2000/XP or higher to collect printer and copier metrics to be used in the PrintFleet Optimizer application. It does not require a dedicated computer.

Windows Service

The PrintFleet DCA runs as a Windows service, allowing it to operate 24 hours a day, 7 days a week. You can customize the transmission interval to determine how often the DCA will perform a device discovery. After each discovery, the collected data will be sent to the hosting web server.

Data Collection Protocols

The PrintFleet DCA collects device data using SNMP (Simple Network Management Protocol), ICMP (Internet Control Message Protocol), and optionally PDL (Printer Job Language). The DCA gathers printer metric data with SNMP and ICMP at regular intervals from printer/multi-function peripheral devices on the customer's network.

Transmission Options

There are 3 methods by which you can transmit the data collected from the PrintFleet DCA, as listed below:

FTP, Port 21

File Transfer Protocol. The standard protocol used to transfer files over the internet between computers.

HTTP, Port 80

HyperText Transfer Protocol. A protocol used to transfer information over the World Wide Web.

HTTPS, Port 443

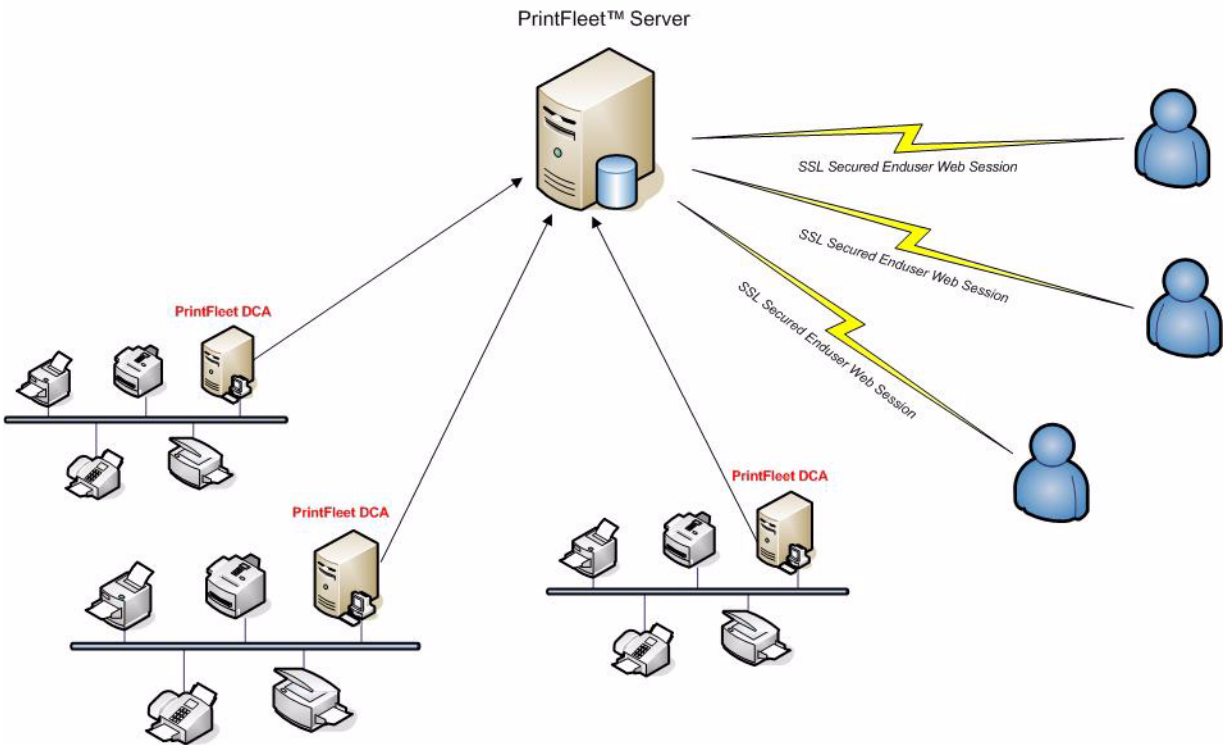
Secure HyperText Transfer Protocol. Data is transferred using the HTTP protocol, but instead of using plain text socket communication, the data is 128-bit encrypted using Secure Socket Layer (SSL) protocol during transit between the user's computer and the server itself. To prepare a web server for accepting https connections the administrator is required to create a public key certificate for the web server. This certificate must be signed by a certificate authority of one form or another, ensuring the user that the certificate holder is who they say they are.

One Way Communication Only

The PrintFleet DCA uses one-way communication only. This means that the collected data can be transmitted from the user's computer to the web server, but the web server cannot transmit information to the user's computer.

No User Data Collected

No personal or user data is collected with the DCA. Only information that is stored in the memory of the devices is collected, such as page counts, device description, device status, and so on.



PrintFleet Optimizer Web Portal

The web server, secure.printfleet.com, is physically stored in a Class-A data center. This data center has over eight fiber optic backbones feeding into it to ensure year-round 24/7 uninterrupted availability. Security background checks and iris scan access are required to gain physical access to the server. When physical access to the server is required, security personnel accompany the individual at all times.

The data center has a triple redundancy energy system preventing power loss of any kind. The web server farm is protected by an ISA software firewall that is completely locked down to only allow required communication.

Data is mirrored and backed up daily. Should the primary server go down for any reason, the feed is switched over to the secondary mirrored server.

PrintFleet Suite

Overview

PrintFleet Suite is a secure program that in itself cannot harm a computer system or network, or endanger any private information.

No software to install

PrintFleet Suite resides on a USB key that is plugged into an available USB port on the network, and does not need to be installed on the host computer.

Standard network protocols.

PrintFleet Suite uses the following network protocols: SNMP, PDL, and ICMP.

Communicates with internal network only

All scan activities take place within the client's network. There is no communication with the internet, except under the following circumstances:

- The option to email network scan results to desired recipients. This can be done by using the Email Report button or by setting up a task schedule to automatically scan and email results.
- All options under the Help menu connect to the internet so users can receive product updates and online help.

Collected information is confidential

PrintFleet Suite does not transmit information back to PrintFleet. The collected information is completely confidential unless the user shares the data with their dealer or other parties, using the PrintFleet Suite emailing feature, or by other means.

Discovery process

PrintFleet Auditor sends a request out to the network, and applicable printing devices send the requested information back to the program. The amount of bandwidth that this scan takes is approximately equal to that used when viewing a single website.

PrintFleet Suite does not send information out to the network or to any devices except under the following circumstances:

- The Send Print Job function within Auditor will send a requested print job to a specified device.
- PrintFleet Restarter can remotely restart a device, but requires the appropriate Community String if applicable.
- PrintFleet Asset Tracker can write the department, location, serial number, and asset number to the non-volatile memory of a device but requires the appropriate Community String if applicable.

PrintFleet Dashboard

Overview

PrintFleet Dashboard is a secure program that in itself cannot harm a computer system or network, or endanger any private information.

Installed, maintained, and operated on site

PrintFleet Dashboard is installed from a CD at the location that it will be monitoring. This gives the end user control over the program.

Standard network protocols.

PrintFleet Dashboard uses the following network protocols: SNMP, PJJ, and ICMP.

Communicates with internal network only

All scan activities take place within the client's network. There is no communication with the internet, except under the following circumstances:

- The option to email network scan results to desired recipients. This can be done by using the Email Report button or by setting up a task schedule to automatically scan and email results.
- All options under the Help menu connect to the internet so users can receive product updates and online help.

Collected information is confidential

PrintFleet Dashboard does not transmit information back to PrintFleet. The collected information is completely confidential unless the user shares the data with their dealer or other parties, using the PrintFleet Dashboard emailing feature, or by other means.

Discovery process

PrintFleet Auditor sends a request out to the network, and applicable printing devices send the requested information back to the program. The amount of bandwidth that this scan takes is approximately equal to that used when viewing a single website.

PrintFleet Dashboard does not send information out to the network or to any devices except under the following circumstances:

- The Send Print Job function within Auditor will send a requested print job to a specified device.
- PrintFleet Restarter can remotely restart a device, but requires the appropriate Community String if applicable.
- PrintFleet Asset Tracker can write the department, location, serial number, and asset number to the non-volatile memory of a device but requires the appropriate Community String if applicable.