PRINTFLEET®

PrintFleet DCA Security Guide

This document discusses security-related issues related to the PrintFleet DCA. These include the measures PrintFleet takes to protect the data and code, as well as identifying network requests that may be made by the DCA in the course of diagnosing communication problems.

Protection Measures

PrintFleet recognizes the importance of protecting vendor MIB data. In order to safeguard this information, PrintFleet has implemented various types of security.

Protecting the DCA Data

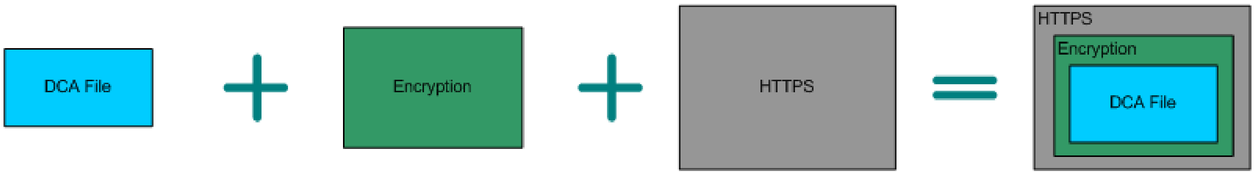
To protect the PrintFleet DCA data, PrintFleet uses encryption from end to end (both for DCA files and Semaphore commands). The data is never stored in plain text; the only time it is "in the clear" is when it has been processed and stored in the PrintFleet Optimizer database (security from there is up to MS SQL Server).

The purpose of encryption:

- To protect the data from interception and viewing/use without using PrintFleet Optimizer
- To authenticate the PrintFleet DCA and ensure integrity of the data (i.e. that it hasn't been tampered with).

Each PrintFleet DCA has its own encryption key, which must match the encryption key on the PrintFleet Optimizer server to verify the data is actually coming from that PrintFleet DCA. It makes it difficult to tamper with the data, because an attacker would need to know the encryption keys, algorithms used, and be able to re-create the checksums. Even so, if a key is ever compromised, it only affects that specific PrintFleet DCA, and re-activating the PrintFleetDCA will create a new key.

HTTPS adds an additional layer of encryption, but is not required. When using HTTP (not encrypted) to transmit Printer DCA data, the only difference is the message container is in plain text; the actual PrintFleet DCA data itself is still encrypted.



Encryption

The encryption provides key 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 PFO instance
- Ensures the data is not modified in-transit or any time after the DCA produced it
- Ensures to PrintFleet Optimizer (PFO) that the data was produced by the authorized DCA

It is important to note that each DCA also has its own encryption key, which must match the encryption key on the

PrintFleet Optimizer server to verify the data is actually coming from the DCA.

Printer DCA initiates all communication to the PrintFleet Optimizer server. No inbound ports need to be opened on the Printer DCA network.

Communications are initiated by both automatic and user-triggered actions, including:

- Activating DCA
- Testing communication
- Synchronizing configuration with server
- Sending scanned data to server
- Checking for software updates

Note that in addition to the PrintFleet Optimizer server address, DCA will also make requests to http://networktest.printfleet.com while testing for internet access.

Summary

We recognize the importance of protecting our clients' valuable MIB data, and have taken all reasonable steps to safeguard that information. It is in our own best interest to ensure that our clients feel confident that their information is safe and secure.