OBERON NEXTGEN

Print Tracker Pro
Technical Security Overview

Released: January 2024 | Revised August 2024

Data Collection Agents

Print Tracker Pro data collection agent (DCA) is a light-weight monitoring software for printer and copier devices. Each new release version of Print Tracker Pro is submitted to several major virus-protection companies for review prior to its public release. After downloading, Print Tracker Pro is installed by default within the C:\Program Files (x86)\Print Tracker Pro folder. The installation consists of the data collection agent (a Windows service and graphical interface) and configuration files.

Print Tracker Pro software can be installed to run from an end user’s workstation, virtual machine or server within a network.

Print Tracker Pro utilizes a network layer abstraction called gRPC (or Google Remote Procedure Call) that is powered by the new major revision of HTTP, called HTTP/2. Additional details about HTTP/2 can be found here. This article will be referenced throughout this whitepaper for explanations as to the advancements in HTTP/2 over HTTP, and how these new features affect the print tracking industry.

The technology used by Print Tracker and outlined in this whitepaper is used by top companies such as Netflix, Microsoft, Google, and more to provide a reliable and high-performance experience interacting with information. It is our goal at Print Tracker to take the technology that already impacts other aspects of our lives and bring it to the print tracking industry.

General Functionality

Network device discovery

Using SNMP version 1, 2 or 3 over port 161, Print Tracker Pro is designed to discover any network-connected and locally- attached print device (MFPs, copiers and printers, etc.) in the environment in which it is run or installed. Particular network segments or IPs can be specified along with limiting the scan to X number of hops from the original network segment where it is installed. If SNMP provided information is incomplete, Print Tracker Pro may request data from the device’s embedded web server over port 80 or other common HTTP ports as defined by the device manufacturer. Collected information includes the device’s network name, MAC address, model, serial number, various counters, and supply information. Print Tracker Pro cannot gather printed content.

Functionality of the Print Tracker Pro Data Collection Agent

Print Tracker Pro has a very small impact on network performance by running as a service in the background. Periodically it pulls meters to analyze data coming from existing devices for low-toner alerts and events. When and how often the software runs these scans throughout the day can be configured within the webadmin. For a typical network segment, Print Tracker Pro will send or receive about 80 KB of data per device when it pulls the meters.

Print Tracker Pro periodically performs a search of user-selected network segments to see if new devices have been added. Any new devices discovered will be added to a total list of devices and will automatically be tracked and managed from that point forward.

After meters are collected, they are securely uploaded to Print Tracker servers. All data is encrypted in-transit and at-rest.

In the event a DCA has issues that require assistance from the Print Tracker support team, log files will be uploaded to secure web servers for review. These files contain only information relating to the Print Tracker software, the host machine, and the device information gathered.

SNMP v1, v2 and v3 compliance

Print Tracker Pro discovers network devices that respond to Simple Network Management Protocol (SNMP) requests. A version of SNMP (either v1, v2 or v3) must be enabled for Print Tracker Pro to capture device information.

Working with Anti-Virus Software

Antivirus software is designed to detect and remove malicious software from a user's computer or network. However, in some cases, legitimate software can be falsely flagged as malicious by antivirus software. This can happen when the antivirus software detects behavior or code that is similar to that used by malware, or when it identifies a legitimate application as a potential threat due to a false positive in its signature-based detection algorithm.

Print Tracker uploads all releases to several antivirus providers so that they can update their definitions. However, ultimately the responsibility remains with the customer to make sure their environment is not uninstalling Print Tracker Pro. Most antivirus solutions allow for whitelisting of applications, and Print Tracker Pro can be added to the whitelist to prevent it from being uninstalled.

Print Tracker Pro Compliance

HIPAA compliance

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) [HIPAA] was enacted by the U.S. Congress in 1996. Title II of HIPAA, known as the Administrative Simplification provisions, required the establishment of national standards for electronic health care transactions while aiming to increase the efficiency of the health care system.

The Department of Health and Human Services drafted rules for the use and dissemination of health care information under Title II. The Administrative Simplification rules, including the HIPAA Privacy Rule, address the security and privacy of health data.

The HIPAA Privacy Rule regulates and establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information held by an entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. The HIPAA Privacy Rule also encourages the widespread use of electronic data interchange in the U.S. health care system.

Print Tracker Pro can only access an imaging device's meter information in the form of:

- Page counts
- Copy counts
- Scan counts
- Fax counts
- Supply levels
- Device service needs

Printed, copied, scanned or faxed content is inaccessible to Print Tracker Pro and therefore security of patient or business information is guaranteed.

Print Tracker Pro is HIPAA compliant because the software does not have the ability to capture PHI including health status, provision of health care, or payment for health care and cannot link to this information stored electronically or printed on a page.

GDPR compliance

Print Tracker Pro is General Data Protection Regulation compliant. All Print Tracker Pro data is stored on GDPR- compliant servers.

Sarbanes-Oxley compliance

Sometimes referred to as the Public Company Accounting Reform and Investor Protection Act of 2002, Sarbanes – Oxley is geared toward accountability. Compliance is not optional; all publicly traded corporations must comply with the mandates of the act.

Print Tracker Pro is Sarbanes - Oxley compliant because it does not store, process, transmit or come in contact with any financial documents or reports.

FISMA compliance

The Federal Information Security Management Act (FISMA) is a United States federal law as Title III of the EGovernment Act. The act recognizes the importance of information security to the economic and national security interests of the United States. The act requires agencies to develop, document, and implement programs that provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by a contractor or other source. The E-Government Act is a United States statute. Its stated purpose is to improve the management and promotion of electronic services and processes by establishing a framework of measures for Internet-based information technology. All government agencies must comply with the mandates of both acts.

Print Tracker Pro is Federal Information Security Management Act compliant because the software can be installed on any managed computer or system, does not increase risk vulnerability or allow changes to systems or security controls, and the information it gathers can be used to maintain cost objectives for any government agency.

Connectivity with the DCA

Print Tracker Pro brings cutting-edge technology to the print tracking industry by merging time tested, industry- standard principles with new ideas, creating the best possible printer tracking experience with the lowest overhead possible.

Service Mode vs Normal

Print Tracker Pro offers two forms of connection with the Web Admin. The first is the standard pull-connection where the DCA checks in with the server on a regular interval for new settings, instructions or jobs to complete. Print Tracker Pro checks in with the server about every 5 minutes allowing for a relatively quick time frame for new settings and instructions to be picked up by the DCA. While this solution is adequate for most needs, it takes a significant amount of time to troubleshoot, make remote changes, and update settings. In the past, solutions were presented to accomplish a more real-time connection between DCAs and remote servers by maintaining open ports where the two parties could push and pull data between each other. This, however, presents major network vulnerability risks that organization should not and are not willing to make.

Print Tracker Pro also offers a new industry-changing option called ServiceMode in which a real-time streaming connection is opened between the Web Admin and a single DCA. This allows the Web Admin to work with the DCA as if they were on the same machine, sending instructions and receiving responses immediately.

There are a number of security issues to consider when connecting the Web Admin to a remote DCA installed within a private network. Several new protocols that sit on top of existing networking layers have been developed and implemented that bridge the gap between security and real-time capabilities, allowing for a new generation of print tracking technology and near real- time connectivity.

HTTP/2

The primary goal of HTTP/2 is to reduce latency by enabling full request and response multiplexing, minimize protocol overhead via efficient compression of HTTP header fields, and add support for request prioritization and server push. HTTP/2 does not modify the application semantics of HTTP in any way. All core concepts, such as HTTP methods, status codes, URIs, and header fields, remain in place. Instead, HTTP/2 modifies how the data is framed (formatted) and transported between the client and server, both of which manage the entire process, and hides all the complexity from applications within the new framing layer.

The current paradigm that has driven DCA development to this point is the standard client to server request and response mechanism: a client makes a single request, a server responds with a single response. HTTP/2 allows the server to send multiple responses for a single client request. That is, in addition to the response to the original request, the server can push additional resources to the client, without the client having to request each one explicitly. This abstraction allows for what we call "server push".

Security

The ability for a remote party to push data and trigger remote actions can seem like a security vulnerability at first glance, however, there are several security mechanisms that minimize the risk to the same level as the risks that standard HTTP present. Under the hood, clients in an HTTP/2 stream always have the option to decline information pushed from a server, however, in a scenario where the remote server is a trusted party, there is usually no reason for a client to deny remote information.

In a web browser, malicious attacks are prevented by now allowing the remote execution of code based on the origin of the server that is providing it. Print Tracker Pro uses a similar concept where both the DCA and the server engage in a mutual TLS handshake when a DCA is registered. This handshake ensures communication can now only be done between that specific instance of a DCA, and the specific remote server with which the DCA requested a handshake. This prevents malicious third- party attacks because they were neither the requesting DCA nor the remote server.

Restricted scope of actions

Every DCA has a predefined set of abilities which can be remotely triggered, these abilities include (but are not limited to) updating local DCA settings, scanning the local network for devices that respond on port 161 (SNMP), etc. This is identical to how current DCA technology works, where a DCA will receive instructions to perform a specific task and will then execute that task based on predetermined logic that was installed with the DCA. Print Tracker Pro brings the ability to send these tasks to individual DCAs over the HTTP/2 stream with which the DCA established connectivity when it was started, allowing a near real- time interaction between dealers, and their customer's machines.

gRPC

Print Tracker Pro does not deal directly with the HTTP/2 transport, but instead utilizes an abstraction layer developed by Google called gRPC (Google Remote Procedure Call). The goal of gRPC is to provide a simple and secure way to initiate an action on another computer across a network. Within the first year of its launch, gRPC was adopted by CoreOS, Net ix, Square, and Cockroach Labs among others. Etcd by CoreOS, a distributed key/value store, uses gRPC for peer communication.

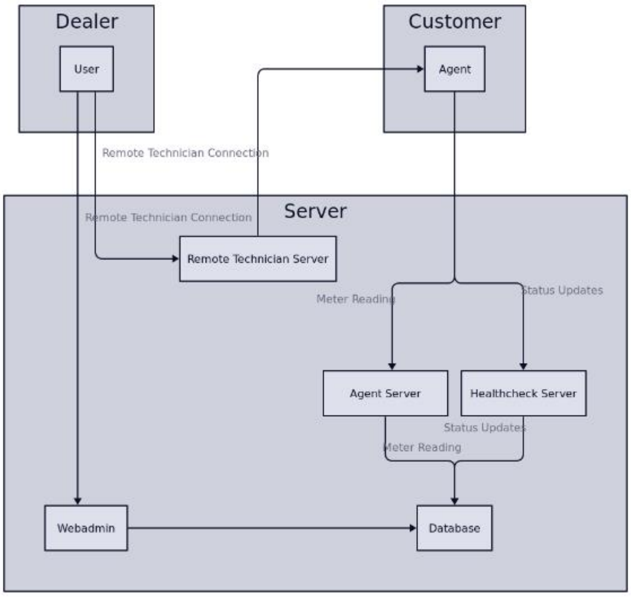
Telecom companies such as Cisco, Juniper, and Arista are using gRPC for streaming the telemetry data and network

configuration from their networking devices. gRPC has SSL/TLS integration and promotes the use of SSL/TLS to authenticate the server, and to encrypt all the data exchanged between the client and the server. Print Tracker Pro utilizes the mutual TLS authentication method to secure client to server (and vice versa) communication.

gRPC has SSL/TLS integration and promotes the use of SSL/TLS to authenticate the server, and to encrypt all the data exchanged between the client and the server. Print Tracker Pro utilizes the mutual TLS authentication method to secure client to server (and vice versa) communication.

Network Traffic

A core concern when facilitating this real-time communication was the amount of network traffic that HTTP/2 streams would bring to a customer's local network. gRPC uses an IDL (interface definition language) to prescribe the type of data that will be sent over the wire. This allows Print Tracker to send data faster and smaller than most other wire-format protocols would allow.



Network Ports, DNS and IPs

DNS	PORT	IP
dcam.printtrackerpro.com	443	34.82.142.242
csr.printtrackerpro.com	443	34.82.142.242
hc.printtrackerpro.com	443	34.82.142.242
api.printtrackerpro.com	443	34.82.142.242
www.cdn.printtrackerpro.com	443	34.102.200.41
www.googleapis.com	443	142.251.33.74, 142.251.211.234, 142.251.33.106, 142.250.69.202, 172.217.14.234, 142.251.215.234, 142.250.217.106, 142.250.217.74

Network Requirements

Data collection requires internet connectivity in order for meters and alerts to be uploaded to app.printtrackerpro.com. Our agents require access to the following domains which may need to be whitelisted in your network configuration:

Domain	Protocol	Port	Purpose
dcam.printtrackerpro.com	gRPC streaming (uses HTTP/2 as a transport)	443	Allows data collection agents to receive jobs, upload meters, and fire alerts.
csr.printtrackerpro.com	gRPC (uses HTTP/2 as a transport)	443	Allows data collection agents to register under entities that you configure.
hc.printtrackerpro.com	HTTPS	443	Allows data collection agents to report their health status.
api.printtrackerpro.com	HTTPS	443	Allows data collection agents to upload trouble reports.
www.cdn.printtrackerpro.com	HTTPS	443	Allows data collection agents to automatically upgrade themselves.
www.googleapis.com	HTTPS	443	Allows data collection agents to download Chromium, the browser used for web-based data collection.
remotetechnician.printtrackerpro.com	Proprietary	7000	Allows authenticated users to remotely access device embedded webservers if the feature is enabled.

System Requirements

Many of the following system requirements depend on the number of devices that are going to be tracked by this data collection agent. For networks with less than 100 devices, the minimum system requirements should be sufficient. For all other network sizes, we recommend that you install the data collection agent on a machine that meets the recommended system requirements.

	Minimum	**Recommended**
Operating System	Windows1, macOS, or Linux2	
CPU	1 GHz x 2 Cores	3 GHz x 4 Cores
Memory	2 GB	4 GB
Disk	2 GB HDD	10 GB SSD
Browser	Chrome, Firefox	Chrome, Firefox
Other Considerations	The data collection agent should not be installed on a laptop or any other machine that frequently shuts down, or the reliability may be affected.	