CPM WHITEPAPER

Introduction: What is CPM?

CPM is the software designed to capture information from printers, package it and transmit it correctly to the main data processing server (CPS).

CPM is designed to work with network printers or USB/LPT connected devices that comply with the DOT4 (IEEE 1284.4) standard. For other devices, it will be possible to use intermediate tools or specific solutions from the printer manufacturer.

CPM Features

CPM has been designed under three fundamental pillars:

- Non-invasive. Its execution is transparent to printers or copiers, to the PC/VM where it is executed and to the network electronics that control it.
- Security. A wide range of security policies are followed and source code is distributed for auditing by network security officers.
- Flexibility. The application's behavior can be strictly determined through a configuration file (xml) that can be manipulated by the implementer. There are no limitations regarding networks, concurrent applications, ranges or segments.

Depending on the type of network and the guidelines set by project managers, it will be possible to use the flexibility of CPM software to adapt to needs.

CPM Security:

- Completely respectful of the network and its equipment, meeting the most demanding communications and security criteria and the most important international regulations:
  - Communications and Security RFCs
  - HIPAA: Health Insurance Portability and Accountability Act
  - Sarbanes-Oxley Act
  - Gramm-Leach-Bliley Act
  - Federal Information Security Management Act
  - ENISA Advising Directives
  - GDPR (EC General Data Protection Regulation)
    - Nubeprint DCA (CPM) does not store reading information in situ, avoiding the generation of new attack vectors.
    - Nubeprint DCA (CPM) never uses extra or non-standard ports to operate. For example, to receive updates (manual or automatic), compromising the network structure.
    - Nubeprint DCA (CPM) is not installed as a service, so it is not kept resident in memory. Its execution is 100% controlled by the installer.
    - The Nubeprint Server (CPS) uses Hosting services that meet extreme security requirements.
    - Transmissions between CPM and CPS use public encryption layers, allowing the user to know with complete certainty what data is being transmitted at all times and at the same time, use a secure transmission channel.
  - Others

- It does not capture any sensitive data (jobs, names, package types etc.).

- Only the data existing in the printer or copier MIB that is necessary for MPS management: serial number, MAC, model, error stack, page counters, cartridge and/or parts levels, display (note: when a given model does not have this information field, CPM does not even try to capture it in order to minimize network traffic).

- Supports encryption layers and communications over SSL (1024-bit HTTPS).

- No access to the Print Server is required. Data transmitted from the client to the CPS server is fully auditable by the client and the service provider.

CPM Security Concepts

CPM is a software installed on the network client and therefore, in addition to its high security performance by default, it is adaptable to any demand in terms of internal security policies or particularities of the networks on which it works. Compliance with security requirements can be established in different complementary categories.

Security layers

Security by design Due to SDD (Security Driven Development), CPM complies with the strictest security policies (Banking, Health Services, Agencies).

- 100% auditable, open source: CPM is delivered with its sources (PAR toolkit) in order to be easily examined by the security team.
- Core admitted and public release on CPAN
- Interpreted language: with direct access to the code being executed.
- Implementation with strict compliance with standards and rules: RFCs for communications and network security, IETF, HIAPP, etc.
- Security in data transmissions: At all levels, the CPM allows the processing of the collected data to be defined by the security team to carry out its own security policies (HIAPP, etc.).
- Data collection: Strict collection of page counters, consumable levels, and operation alerts (e.g. damaged drum).
- Collection frequency: This is defined by the IT team using the standard operating system scheduler rather than an internal or ad hoc application timer.
- HTTP Channel: Ability to stream over HTTP with strong SSL layer (256-bit), with support for authenticated or anonymous proxies.
- SMTP Channel: Ability to connect through the client's SMTP server with SSL layer (256-bit) with the possibility of copies from the source (without the use of forwarding rules) of each message for auditing purposes.
- Network Security: CPM is fully adaptable to network security policies and procedures due to its flexible deployment architectures and extensible configuration.
- Unlimited CPMs per network, multiple networks of a single CPM, and/or multiple ranges per network – IT decides the number and logical placement of CPMs to meet their needs.
- Firewall, segmented networks, and dynamic routes support: Supports blocking of ports and routes also during the discovery process using escalations.
- IP Address Read List: Operating in "list mode", the CPM scans the specific group of IPs.
- Latency and Timeout: Supports internal definition of timeout and latency with soft values to adjust and not be intrusive.
- Security by isolation: CPM operates as a transparent layer that does not disrupt any client's network element. It is a completely portable software that can be connected without any system modification.
- No installation required: allows IT and Security staff to define their own usage policies.

- No network changes required – routes and specific network architecture are managed through CPM's extensible configuration. Multiple networks, subnets, VLANs, etc.
- No printer/copier changes are needed - it only uses SNMP (v1, v2c and v3) and is used in strictly read-only mode in all cases.

CPM: from the IT perspective

Security

1 What about CPM and privacy?

CPM will not query the printer and therefore will not collect sensitive information (users, jobs sent to the printer or settings). It collects data related to the printer status (page counters, consumable levels, errors).

2 Can CPM be audited?

Absolutely yes.

3 Does the CPM need write access via SNMP?

Of course not. The CPM only reads counters and status information.

Non Invasive

- **What about CPM and bandwidth?**CPM does not broadcast the network. In case the software does not include a list of printers to monitor, it will follow a process to discover them on the network with an extremely low resource usage rate (from the network, the PC and the printer).

- **Does CPM need external libraries and frameworks (.NET, Java, SQL, etc)?**Absolutely not. CPM is portable and has no software requirements.

- **Does CPM require any specific operating system?**There are CPM versions for Windows XP/2000/2003/Vista/2008/7, Mac OS X, Unix/Linux, FreeBSD and Solaris.

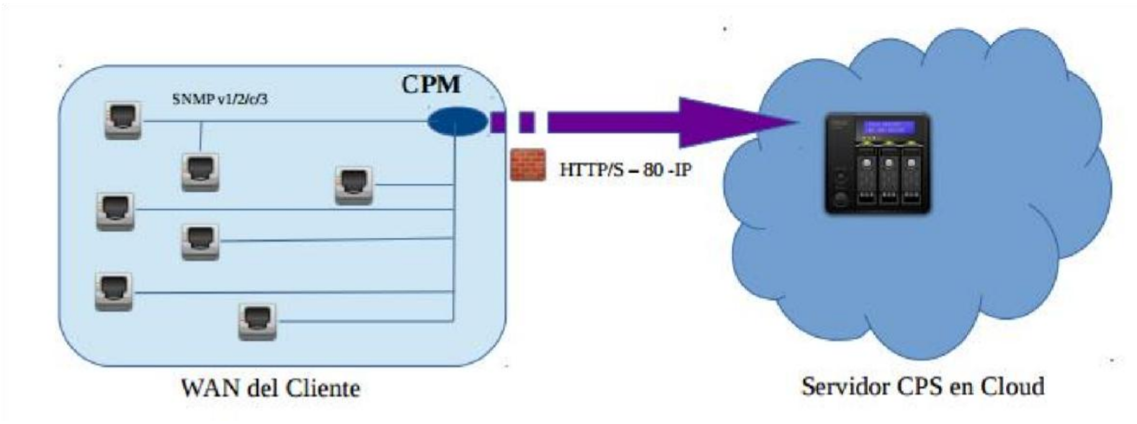
- **How many times does the CPM read the printers?**? CPM is controlled by the Task Scheduler utility. It is the client, responsible for the network, who decides when and how many times the printers should be read. It can also be configured to run in the background.

- **Should the printers' port ping and/or 9100 be accessible when CPM?**Absolutely not. Even during the discovery process, the CPM only uses the SNMP service (161/UPD) to detect and read printers. Both echo (ping) and port 9100 facilitate the discovery process but are not strictly necessary at all.

Deployment and Activation in WAN type networks

This document details the requirements necessary to successfully implement the implementation on WAN (wide area) networks.

It should be noted that the deployment of the solution only requires the implementation of the monitoring tools (CPM) as these are responsible for capturing and sending data that will be transformed into information through a server already operational and made available in the Cloud.



The usual implementation architectures in WAN networks correspond to:

- Installing a CPM at a central point with general network access (e.g. data center)
- Installing a backup CPM to start on demand
- Execution of a daily equipment discovery process for the generation and updating of the physical inventory of machines
- Running CPM in list mode (reading only IP addresses from inventory) in conjunction with the discovery process

NOTE: More information about WAN networks can be found in the appendix.

Frequently Asked Questions:

1. **What is CPM software?**It is an application that allows you to discover and collect data from printers on a TCP/IP network, and then send the information to the Cloud.
2. What data does it collect? Although it depends on the printer model, the CPM is capable of capturing basic data from the equipment such as its serial number, values of its page counters, the status of the consumables, and the messages that appear on the printer display.
3. **What can be said about CPM and privacy**? Under no circumstances does the CPM collect sensitive information (users, printed jobs or configurations).

In addition, the CPM code can be studied, evaluated and modified for any need, distributed and of course audited.

4. **Where is the source code??** The CPM program is packaged using PAR (Perl Archiving Toolkit). The executable can be directly unzipped to extract all the source code.
5. **What can be said about CPM and security?**It is important to note that no sensitive data is collected, only the printer status itself. CPM applies security criteria by design.
6. **What can be said about CPM and bandwidth consumption?**By design, the CPM never broadcasts over the network. If it does not have a list of devices to monitor, it performs a discovery process over the local network, where low resource consumption (network, CPU and printer) is the most important requirement.
7. **What can be said about CPM and external connection?**Once a printer has been monitored, the CPM will attempt to send the data to the Cloud server, which will require Internet access via HTTPs.
8. **How do you upload data to the Cloud??** Through a simple connectionless protocol over HTTPs. This protocol is public and will soon be published on the web. Currently it can be easily extracted from the CPM code itself.
9. **Why does it take so long to execute the discovery?**If the CPM does not contain a predefined list of printer locations to monitor, it will attempt to perform an automatic discovery, trying in no case to overload the network or the connected devices, and will carry out the process slowly and safely.

ANNEX: Deployment and Activation in WAN type networks

Recommended Base Architecture for Installation

In the case of architecturally complex networks with unknown or mobile printing fleets, the use of at least two CPMs is recommended.

1. Inventory Control CPM: This is a tool configuration that will scan the network typology for printers. It runs weekly so that any new device is automatically integrated into inventory.

2. Read CPM: This is an efficient configuration where only the inventoried printing equipment is monitored. It is run frequently (2-4 times daily).

It is recommended to install CPM on a dedicated server (physical/virtual). This is to provide the greatest flexibility in terms of architecture and to prevent a configuration forced by another application from diminishing its performance.

As long as the client's network architecture allows it, the installation of redundant CPMs or auxiliary service is not necessary.

In the event that the WAN network is highly compartmentalized (several independent subnets), then the CPM installation process would be applied to each of them individually.

Once activated, the maintenance required by CPM is low (changing or updating its configuration). In standard operation, no incremental activity logs are stored (the application “does not grow”).

IT requirements for implementing CPM in WAN networks

1.- Installing the application on a computer connected to the WAN network

- CPM can be run on the following operating systems.
- GNU/Linux (recommended for large networks)
- Microsoft Windows 7/8/8.1/10
- Microsoft Windows Server 2003/2008/2012
- Mac OS X
- UNIX FreeBSD, NetBSD, OpenBSD, AIX
- CPM can be run on a low-resource computer and its requirements will depend on the operating system and the number of networks to be discovered concurrently. The following parameters can be taken as reference:
- CPU: 1 ECU
- RAM: 4G
- Storage: 100M
- Ethernet: 1Gbps

2.- Visibility of the SNMP service (port 161/tcp/udp) from the computer running CPM to all printers on the network

- This is the default printer settings. If they have been changed (community, version, port) it will be necessary to notify us.

- Only SNMP read access is required and from the IP from where CPM is running.

3.- Visibility of the HTTP/S service on the Internet

- CPM must connect to the CPS server and to do so it will use a layer over the HTTP (80) and/or HTTPS (443) protocol.
- Once installed, possibility to restrict output to a single output IP (or domain): the CPS location.
- Possibility of using a proxy with username and password authentication. It must be a standard proxy (proprietary authentication solutions such as NTLM are not supported).

4.- (Optional) Visibility of the ping service from the computer running CPM to all printers on the network

- This is an optional parameter that, if enabled, increases the efficiency of the printer discovery process.

5.- (Optional) Visibility of the printing service (port 9100/tcp) from the computer running CPM to all printers on the network

- This is an optional parameter that, if enabled, increases the efficiency of the printer discovery process.