Print Aware Powered by MPS Monitor

What is Print Aware?

Print Aware is a data collection tool specialized for copiers and printers. Print Aware scans and gathers Toner Levels and Meter Counts from copiers and printers on the network. Print Aware uses SNMP (Simple Network Management Protocol) to pull the MIB (Management Information Base) from the print devices on the network. The MIB contains information such as Serial Number, Make, Model, IP Address, Meter Counts, and Toner Levels for each print device.

Why does Marco use Print Aware?

The Print Aware application allows Marco to automatically submit meter counts on print devices for billing, so you don't have to. It also allows for tracking of toner levels for devices. Marco uses Print Aware and predictive analysis to detect when your print devices are about to run out of toner, so we can ship it out to you before your device runs out.

Is Print Aware Safe?

Print Aware is powered by MPS Monitor. Please see the safety and security compliance document attached.

Subject: **MPS Monitor – DCA 4.x Software Safety and Compliance Certification**

We hereby certify that the MPS Monitor DCA 4 software, manufactured by our company, does not contain any viruses, malware, nor threats of any kind to the information security of the Customers running it, and that the installation of DCA 4 within the Customer's network does not pose or add any significant security risk to the network itself.

The DCA 4 software has been developed in compliance with the OWASP Top 10 international specifications and guidelines and is subject to continuous testing and verification by independent institutions that certify compliance with these guidelines.
The code of the DCA 4 software, before the release of each version, is subject to Code Review and static analysis by specialized cybersecurity firms, to verify that:

- the installation package contains only software modules digitally signed by MPS Monitor srl to guarantee its authenticity
- the software does not contain known vulnerabilities of high criticality, and that any vulnerability previously found has been eliminated before the release of each new version
- the software is not detected as malware by the most popular antivirus products on the market.

All access methods, API interfaces and web endpoints used for communication between DCA 4 and the MPS Monitor cloud systems are subject to Penetration Tests on a regular basis, usually every quarter, in order to verify the system's safety and compliance with international standards and guidelines. The process of automatic update of the software is subject to a specific Penetration Test process every year to verify the security against possible attacks in the update supply chain. The Device Web Access function, given its high criticality, is subject to specific and dedicated Penetration Testing and security review.

The information collected through the software is processed within an Information Security Management System that is certified in compliance with UNI CEI ISO/IEC 27001:2017; certificate no. 50 100 13777 Rev. 003 was issued by TÜV Italia srl on 06/03/2020 and is available at the following link: http://www.mpsmonitor.it/docs/iso-27001.pdf.

MPS Monitor srl adopts information security policies compliant with AICPA SOC 2, and undergoes an annual audit by A-LIGN to certify compliance with the defined Trust Services Criteria (**Security, Availability, Confidentiality).** The SOC 2 Audit Report issued by A-LIGN is available for download in the MPS Monitor Portal after e-signature of a specific Non Disclosure Agreement (NDA).

MPS Monitor srl adopts company policies aimed at adhering to regulatory requirements on privacy and information security, and processes data in full compliance with the provisions of Regulation (EU) 2016/679 of the **European Parliament and of the Council** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). With particular reference to the GDPR, the MPS Monitor software is produced and operated in compliance with the principles laid out in said European regulation and, in particular, with the principles of "*data protection by default and by design*". The protection of personal data is pursued as early as the design stage.

DCA 4 is developed to collect and process data relating to printing devices connected to the Customer's network, and to enable a real-time connection between users and devices, in order to manage them in a correct and effective way. The operations carried out are directly connected to this specific purpose. In particular, the software does not collect any data relating to the content of documents printed, nor to natural or legal persons whose data is processed through said devices and/or documents.

Technical specification and Data Collection process description
The DCA 4 software module has the following technical specifications and security features:

1. It is installed on a hardware device (PC, Server, MAC, or Raspberry) running a supported Operating System (Windows, Linux, Mac OS or Linux for Raspberry). The device needs to be connected to the Customer's network and needs to have Internet access (port 443 / HTTPS).
2. In order to exchange data and receive information about tasks to be performed, the software uses HTTP2 GRPC polling calls (usually sent once every 5 minutes) and MQTT connection to a Server that can be reached through different domain URLs belonging to the root domain https://*.mpsmonitor.com. The MQTT connection uses as default MQTT over WSS (port 443). It can be configured also to work as a standard MQTT connection (port 8883)
3. At configured intervals and based on the information made available by the Server, the DCA 4 performs UDP scans of the subnetworks, IP addresses, or hostnames where the printers can be reached; the times and subnets or IP addresses or hostnames to be scanned are defined in a special administration function on the configuration pages of the MPS Monitor Portal.

4. It identifies all printer-type devices, while completely omitting all other network devices of any other nature.
5. Data collection is performed using UDP (port 161), and generally takes a few seconds or minutes, depending on the complexity of the network and number of devices.
6. By using UDP, the traffic is minimum, and it does not have any noticeable impact on the network and devices.
7. The data collected by the printers are stored locally in a database. Changes in the stored data are sent using HTTPS to the MPS Monitor Server. Both the data at rest and the data sent over the Internet are encrypted.

Device Web Access process description

DCA 4 allows a user with adequate permissions to connect to the Printers' internal Web Server using the feature called "Device Web Access", which has the following technical specifications and security features:

1. DCA4 receives a Device Web Access connection command from the MPS Monitor Portal and verifies that the request is for a managed printer, then creates a Reverse SSH Tunneling.
2. The Reverse SSH Tunneling is based on SSH protocol and it is created from the Web Service Printer Port (typically 80 or 443, or other that can be configured) to a remote SSH server (port 22 / SSH) that can be reached through different domain URLs belonging to the root domain https://*.mpsmonitor.com.
3. Using the SSH protocol the system implements a public-key based authentication and encrypts connections between the printer and the MPS Monitor SSH server endpoints.
4. The server-side connection is created as a new tunnel at every connection request, and terminated after every session, with a maximum duration of 10 minutes. The security keys are unique for each installation, and every new tunnel uses a different session ID to avoid session reusing.
5. A complex authentication methodology is implemented to ensure that all the parties involved into each SSH tunnel are legitimate and have the authority to open and maintain the connection.
6. A number of verifications on the device are performed before opening the tunnel to ensure that the target device corresponds to the one on which the connection has been requested. If any of these verification fails, the tunnel is not open.
7. Device Web Access connection is restricted only to selected user profiles and can be activated only by users with strong authentication to the MPS Monitor Portal (Two-Factor Authentication or Single Sign-On via Active Directory). This prevents unauthorized or malicious usage of the Device Web Access feature in case of credentials theft.
8. All the web activities performed within Device Web Access are logged on the SSH Server. Customers can access the logs to check the usage of this function by other users.
9. Device Web Access can be disabled on each customer by the user in the MPS Monitor Portal, or directly from the DCA 4 local User Interface, by the customer itself. If the function is disabled in the DCA User Interface, it cannot be re-enabled from the Portal, thus ensuring that each customer has the ability to disable this function locally from the system where the DCA 4 is installed.

Print Management system integration

DCA 4 also allows, if used on a network where a Print Management system is present (like PaperCut MF/NG or similar systems), to be configured in order to collect and process data related to print jobs and users who print, with the goal of providing Business Intelligence and Analytics on said data. This is performed through the following process:

1. DCA 4 can be configured to access a folder on the Customer's network where the Print Management system exports text/CSV files containing print jobs data
2. When data files are created, DCA 4 collects them and sends them to the MPS Monitor cloud system, for processing
3. Data present in files are added to the central MPS Monitor Database and become available to the user in the Analytics section of MPS Monitor, to allow the creation of specific BI reports and dashboards
4. If the files contain data related to the content of the document (like file names or other potentially confidential information), those data are eliminated before being imported in the database, to make sure that no personal or confidential information is stored in the MPS Monitor system.

Milano, 24 March 2022

MPS Monitor srl
Chief Executive Officer
Nicola De Blasi

Subject: **MPS Monitor - eXplorer 3.9 Software Safety and Compliance Certification**

We hereby certify that the MPS Monitor eXplorer 3.9 software, manufactured by our company, does not contain any viruses, malware, nor threats of any kind to the information security of the Customers.

The eXplorer 3 software has been developed in compliance with the OWASP Top 10 international specifications and guidelines and is subject to continuous testing and verification by independent institutions that certify compliance with these guidelines.
The code of the eXplorer 3 software, before the release of each version, is subject to Code Review and static analysis by specialized cybersecurity firms, to verify that:

- the installation package contains only software modules digitally signed by MPS Monitor srl to guarantee its authenticity
- the software does not contain known vulnerabilities of high criticality, and that any vulnerability previously found has been eliminated before the release of each new version
- The software is not detected as malware by the most popular antivirus products on the market.

All access methods, API interfaces and web endpoints used for communication between eXplorer 3 and the MPS Monitor cloud systems are subjected to Penetration Tests on a regular basis, usually every quarter, in order to verify the system's safety and compliance with international standards and guidelines. The process of automatic update of the software is subject to a specific Penetration Test process every year to verify the security against possible attacks in the update supply chain.

The information collected through the software is processed within an Information Security Management System that is certified in compliance with UNI CEI ISO/IEC 27001:2017; certificate no. 50 100 13777 Rev. 003 was issued by TÜV Italia srl on 06/03/2020 and is available at the following link: http://www.mpsmonitor.it/docs/iso-27001.pdf.
MPS Monitor srl adopts information security policies compliant with AICPA SOC 2, and undergoes an annual audit by A-LIGN to certify compliance with the defined Trust Services Criteria (**Security, Availability, Confidentiality).** The SOC 2 Audit Report issued by A-LIGN is available for download in the MPS Monitor Portal after e-signature of a specific Non Disclosure Agreement (NDA).

MPS Monitor srl adopts company policies aimed at adhering to regulatory requirements on privacy and information security, and processes data in full compliance with the provisions of Regulation (EU) 2016/679 of the **European Parliament and of the Council** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). With particular reference to the GDPR, the MPS Monitor software is produced and operated in compliance with the principles laid out in said European regulation and, in particular, with the principles of "*data protection by default and by design*". The protection of personal data is pursued as early as the design stage.
eXplorer 3 is developed to collect and process data relating to printing devices connected to the Customer's network, in order to manage them in a correct and effective way. The operations carried out are directly connected to this specific purpose. In particular, the software does not collect any data relating to the type or content of documents printed, to users who print them, nor to natural or legal persons whose data is processed through said devices and/or documents.
The data is collected from the printers using the eXplorer 3.x software module, which has the following technical specifications and features:

1. It is installed on a hardware device (PC or printer) within the Customer's network and with Internet access (port 443 / HTTPS). The device should connect to the printers on the network using the SNMP protocol (port 161 / UDP).
2. In order to exchange data and receive information about tasks to be performed, the software connects (usually sending a ping once every 5 minutes) to a Server that can be reached through different domain URLs https://*.abassetmanagement.com or https://*.mpsmonitor.com.
3. At set and configurable times (generally three or more times a day) and based on the information made available by the Server, eXplorer 3 performs a UDP scan of the subnetworks or IP addresses where the printers can be installed; the times and subnets or IP addresses to be scanned are defined in a special administration function on the configuration pages of the MPS Monitor Portal.
4. It identifies all printer-type devices, while completely omitting all other network devices of any other nature.
5. Data collection generally takes a few seconds or minutes, depending on the complexity of the network and number of devices.
6. By using UDP, the traffic is minimum and it does not have any noticeable impact on the network and devices.
7. The data collected by the printers are stored in CSV and XML format in the \Agent\send folder of eXplorer 3 installation path, so that the customer can have access to the files and check what information is collected every time the scan is performed.
8. In case problems are found when reading data from a printer model, the system uses the

SNMPWalk command to generate additional files with information on the entire MIB of the printer; these files have .WLK extension and allow us to identify and solve problems when reading data. This function can be disabled when configuring the eXplorer from the MPS Monitor Portal.

9. CSV and WLK files are transferred via HTTPS to MPS Monitor servers on cloud. All communications between the eXplorer 3 software and the MPS Monitor Portal take place exclusively using the HTTPS protocol.
10. The data in the files is used to update the Database that manages the Client's printers.

Under no circumstances will the Customer's network be accessible from the outside. Therefore, the installation of the eXplorer 3 within the Client's network does not pose any security risk to the network itself.

Milan, 23 March 2022

MPS Monitor srl
Chief Executive Officer
Nicola De Blasi