MPS Monitor Security Technical Whitepaper

AUGUST 2022

Contents

Introduction

This whitepaper examines how MPS Monitor stands out as the market leader in providing a secure MPS solution for all dealers and their customers, with a comprehensive approach to security that has been tested and verified by independent third-party organizations and is the subject of ongoing audits to maintain confidence in its security posture.

Certifications & Evaluations - Summary

MPS Monitor has passed a multitude of internationally recognized security-related evaluations and certifications:

- ISO/IEC 15408
- ISO/IEC 27001
- System and Organization Controls 2 (SOC 2)
- Buyers Laboratory / Keypoint Intelligence (various)
- Personal Data Protection laws (various, such as GDPR in Europe and California's Consumer Protection Act)

These achievements are referenced throughout this document. They represent the independent confirmation of MPS Monitor's position as a security leader.

Introduction to MPS Monitor

MPS Monitor is a cloud-based SaaS solution used by Managed Print Services providers worldwide to securely monitor and manage fleets of printing devices of any brand, including Zebra label printers.

To provide its services and functions, MPS Monitor relies on two main components:

1. **The Data Collection Agent (DCA) Connector**: This component, installed on the customer's LAN, performs all operations on devices based on the instructions provided by the Server component. The DCA can be installed at the customer's location on a Windows, Linux, or MAC OS system or embedded directly on an MFP/SFD. Optionally, an HP cloud-based DCA may be deployed to remotely monitor and manage HP FutureSmart devices without installing any DCA in the customer's network.

   The DCA communicates with the MPS Monitor Cloud Server to report collectible information about the devices within a customer's environment using a secure channel.

   In March 2022, DCA version 4 was introduced.

2. **The Cloud Server and Web Portal**: The Cloud Server component houses the device data (meters and consumable data) supplied by the DCA. To access the data for fleet monitoring and management, a user accesses a dedicated web portal securely authenticating over the HTTPS protocol.

A Comprehensive Security Policy

MPS Monitor has designed and implemented what is formally known as an Information Security Management System (ISMS), which conforms with the requirements of the *ISO 27001:2014* standard. The general objectives that MPS Monitor sets out in its security policy are to *guarantee each client that their information will be processed according to the fundamental requirements of confidentiality, integrity, and availability.* ISO 27001 covers not only digital security but also physical security and company policies and practices contributing to an overall security posture. All subscribing dealers and their customers are equally covered by the security policies described in this whitepaper.

Physical Security and Disaster Mitigation

Physical access to the ISO 27001-certified data center hosting MPS Monitor is restricted, and the facility is patrolled by armed guards. Guests must always be accompanied. The facility is under video surveillance and protected by anti-fire and anti-flood protection systems.

A business continuity and disaster recovery plan are in place to ensure that MPS Monitor cloud services can be restored within hours of even a total loss of its infrastructure, whether physical or digital. As part of this plan:

- The plan is tested annually against various threat scenarios based on likelihood.
- Continuous testing of the disaster recovery system is conducted by a third-party firm to ensure functionality in case of need.
- A third-party cybersecurity consulting firm is under contract to provide a rapid response to any kind of security breach.

- All incidents are logged along with the response, escalations, impact, root cause, and resolution. Resolution of incidents is communicated to affected users.
- Incident response policies are reviewed at least annually.

Software Integrity

The MPS Monitor software is produced and operated according to the GDPR principles of "data protection by default and by design." As a result, the integrity of the MPS Monitor software is ensured from the very start:

- Version control software maintains code and history of changes.
- File integrity monitoring software ensures that only authorized changes are deployed into the production environment.
- Quality Assurance and user acceptance testing are performed in an environment separated from production.
- All components of a release package are digitally signed using the MPS Monitor developer's code signing certificate, not just the executables (not an uncommon practice), which prevents anyone from making changes, other than the developer's team f. Unsigned components introduce the risk of manipulation which could then compromise all systems downloading and installing the new package.
- All the components of each distribution package are tested to ensure the integrity of the digital signature before general release.
- MPS Monitor implements a reoccurring 6-month cycle of auditing and testing performed separately by two independent firms specializing in application security testing and cybersecurity. Testing is performed not only on the source code but also on all operational artifacts.
- Any identified vulnerabilities are addressed, and testing begins anew before release.

A review of these policies, procedures, testing methodology and results are part of the ISO 27001 documentation. This information is also included in the SCO2 compliance documentation, which reveals no critical vulnerabilities to any customer environment.

Cloud Component Security

MPS Monitor's back-end cloud systems are used to host the data from MPS service providers and their customers. This cloud infrastructure is fully owned and managed by MPS Monitor and hosted in the British Telecom data centers—one of the world's largest and most secure data centers service providers—in Milan, Italy. MPS Monitor customers include thousands of banks, insurance companies, government and public institutions, airlines, airports, health-related organizations, energy and utilities, manufacturing facilities, and many more.

While cloud-based services are a prime target for cybercriminals, MPS Monitor holds some of the most accredited security certifications available for cloud-services providers to ensure the safety of MPS Monitor service providers and their clients.

Monitored continuously (24 x 7 x 365), the MPS Monitor cloud platform is subject to several security audits, including:

- An annual evaluation by the ISO 27001 certification body to confirm the validity of the certificate.
- Quarterly web penetration testing of MPS Monitor's back-end cloud systems was conducted separately by two independent cybersecurity firms.
- Once a year, the worldwide HP Cyber-security team ensures the MPS Monitor infrastructure are compliant with HP's worldwide cyber-security standards for all HP partners worldwide.
- Compliance and regulation testing by a specialized privacy consulting firm to ensure compliance to the privacy regulations in the USA, Canada, EU (GDPR), and others.
- Those performed upon request by organizations, typically banks and financial institutions, who have above-average security requirements and wish to validate the level of security and compliance the MPS Monitor infrastructure has for their organization's strategic initiatives.

Security protocols of the MPS Monitor cloud systems are also examined as part of SOC2 certification.

Data Privacy

MPS Monitor conforms to one of the most restrictive personal information privacy laws in the world, Europe's General Data Protection Regulation (GDPR), as well as privacy laws in Canada, the United States, Mexico, and more.

MPS Monitor Srl, an independent, privately-held company, does not transmit, share, store, or process any personally-identifiable information, health information, or other kinds of personally identifiable information as part of MPS Monitor’s operation. The MPS Monitor portal user account information is also protected (see additional information below under User Accounts).

Operational Security

User Accounts

User accounts are required to access the MPS Monitor portal. To ensure security, MPS Monitor features a comprehensive list of user privileges so that a user’s access to features, Power Bi reports, dashboards, and modules can be exactly tailored and limited to the user’s role within the dealership or end-customer’s organization.

For ease of management and use, these “capabilities” are gathered into sets. Default sets are provided based on typical roles, and custom capability sets can also be created to match an organization’s specific requirements.

While maintaining the security of the MPS Monitor platform, the sharing of reports, alerts, and notifications with internal or end-customer users are all managed within the platform, therefore there is no need for exported files to be sent by less secure mediums (eg: email or cloud storage solutions, etc.).

Password Protocols

Passwords are an essential part of any security system but present their own security challenges. While length and complexity are features of a good password, the human factor can render such requirements less effective. In addition, the need to have multiple sets of credentials for different systems can also add to the risk factor.

MPS Monitor has two features to help mitigate this security risk:

- Support for single-sign-on (SSO) solutions like Okta or Azure allows people to adhere to password best practices implemented by the security teams within the organization. Okta or Azure integration allows the user to authenticate with the organization's IDM (Identity Management) system to access the MPS Monitor cloud platform through a fully secure Single Sign-On process.

Communication Protocols

Data Collection Agent (DCA) – Network-connected Devices

A Windows DCA scans for network-connected MFPs, copiers, and printers using the Simple Network Management Protocol (SNMP) over UDP port 161. Devices that meet the minimum printer MIB v.2 specifications according to the industry-standard RFC3805 are added to MPS Monitor, while all other devices on the network are omitted from the data gathering process.

While the DCA supports SNMP v1, v2c, and v3 of the standard SNMP protocol stack, SNMP v3 is the most secure due to the addition of encryption.

The table below details all required communication ports for local network communication between the DCA and the devices itemized within the DCA:

Port	Protocol	Port	Protocol
161	UDP	**3910**	TCP
427	UDP	**3911**	TCP
443	TCP	**7627**	TCP
3702	UDP	**8080**	TCP

Data Collection Agent – MPS Monitor Cloud

A DCA installed on a Windows OS computer (see Software Requirements, below) uses port 443 using Secure Hypertext Transfer Protocol Secure (HTTPS) for Transport Layer Security (TLS 1.2) encrypted communications with the MPS Monitor cloud services at these addresses only:

- https://*.mpsmonitor.com
- https://*.abassetmanagement.com

All communication between the MPS Monitor DCA and the MPS Monitor cloud is initiated by the locally-installed DCA. The DCA periodically polls the MPS Monitor cloud for tasks to perform.

Notes:

- Appropriate firewall settings may be required on the computer running the DCA component as well as any network-based firewall to permit this data exchange.
- MPS Monitor can be configured to work with the organization's proxy server. If the proxy requires authentication credentials, enter the username, password, and port of the proxy server on the configuration page during or after the installation of the DCA. These credentials are saved by DCA, in encrypted form, exclusively on the customer's system; they are never transmitted to the MPS Monitor Cloud Server or other sites outside of the customer's network and are never visible to staff which has access to the customer's system.

The DCA can be installed on MFPs and other devices and operating systems. A full list of supported configurations and related security details can be found below in the section, DCA Operating System Requirements & Security Details.

Data Collection Agent Version 4

Released in March 2022, the optional DCA 4 added new capabilities, including faster and more secure communications, as well as Device Web Access (DWA) which allows MPS Monitor Console users to browse any customer's printer's embedded web server pages.

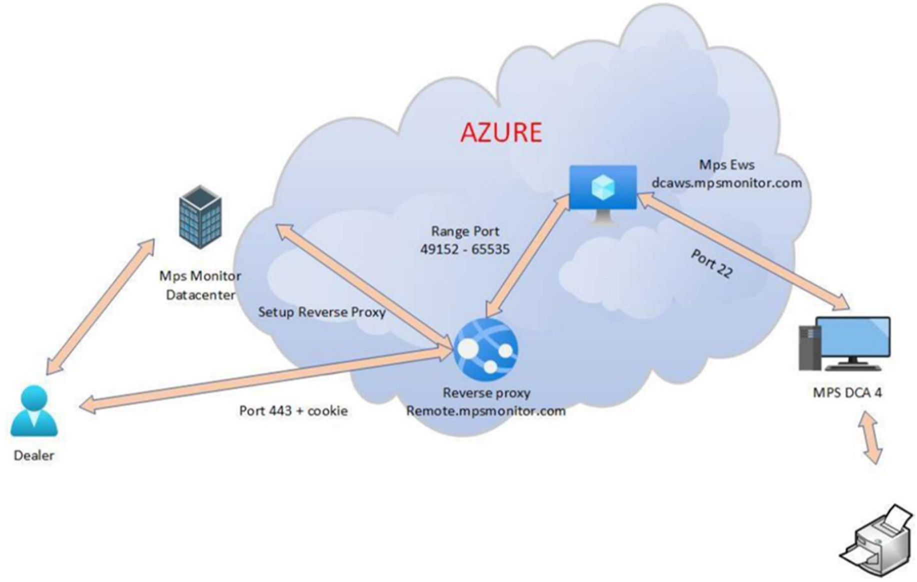
Improved Communication Security & Speed

DCA 4 improves security by defaulting to HTTPS2/GRPC over port 443 where possible, falling back to HTTPS when necessary. In addition, DCA 4 uses MQTT, a lightweight IoT communication protocol, over port 8883 or 443 (using WSS), as an optional way to greatly increasing the speed with which the DCA communicates with devices on the local network and the MPS Monitor Cloud service.

Device Web Access

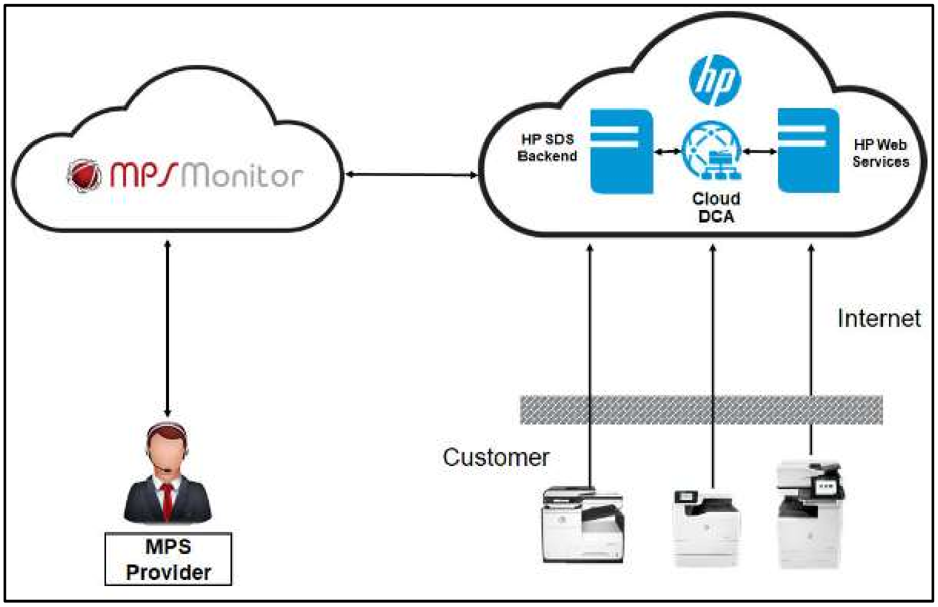
DCA 4's DWA is a powerful feature protected to ensure restricted and secure access via the following features:

- Access to DWA is generally restricted to devices directly 'owned' by a given dealer, with specific permissions required for top-level support operators to access the devices belonging to sub-dealers.
- Mandatory 2-factor authentication or Active Directory integration ensures only authorized users may use the DWA feature.
- The use of OpenSSH with Azure-based SSH gateway and reverse proxy provides a secure connection that prevents man-in-the-middle attacks.
- DWA requires HTTPS2/GRPC to provide appropriate communication security.
- DWA uses temporary firewall exceptions that are deleted after each session.
- Target device attribute verification is performed with each connection to prevent cross-device access.
- An access log is generated for each use.
- File transfers using OpenSSH are disabled.



HP SDS Cloud DCA

The HP Smart Device Services Cloud DCA allows MPS Monitor to remotely monitor and manage HP FutureSmart devices without a DCA being installed on a network.



Compatible devices with an internet connection use HTTPS over port 443 to communicate with the Cloud DCA using the following endpoints:

- https://dopplerservice.msit.hpcloud.hp.com
- https://dopplerapp.msit.hpcloud.hp.com
- https://directory.id.hp.com
- https://coresvcs.dp.smartcloudprint.com
- https://directory.stg.cd.id.hp.com

See the Requirements section below for additional details about HP SDS Cloud DCA, including those of specific HP SDS features.

Local Agent/HP SDA – USB Devices

The Local Agent acts as a data collection agent for a printer or MFP connected to a computer via USB cable. Installed on the PC to which the physical device is attached, the Local Agent collects the data from the device and communicates with the MPS Monitor cloud service in the same manner as the DCA.

The HP Smart Device Agent (SDA) serves the same function, but exclusively for HP devices. The PC-based HP SDA will use port 12351 to communicate using HTTPS with the JetAdvantage Management Connector (JAMC) [https://hp-print-mgmt:12351].

More information about the Local Agent and HP Smart Device Agent can be found in the MPS Monitor Component Quick Reference section below.

For more information about the HP SDA, please read HP's "HP Smart Device Agent for USB Connected Printers White Paper" (see References, below).

Requirements

Licensing Requirements

No additional security-related subscription or licensing fees for MPS Monitor are required.

Hardware Requirements

The recommended hardware for the machine hosting the DCA are as follows:

CPU: Intel Core i3+

RAM: 2 GB+ (4 GB+ recommended)

HD Space: 100MB+ (1GB+ recommended)

The Microsoft Windows machine hosting the DCA does not have to be a dedicated desktop PC or server, but it does have to be a stable machine that will always remain online while the DCA runs in the background as a service to collect the information from the printing devices within the environment.

DCA Operating System Requirements & Security Details

Windows

Supported OS

- Windows 10 (v1709 +)*
- Windows Server 2016*
- Windows Server 2019*

* .Net Framework 4.5 (full module) is also required. (Note: Installation of the .Net Framework may require a system restart.)

Service Account

On a Windows computer, DCA 3 installs as a Windows system service (MpsMonitor.eXplorer.Service) that is configured with Automatic Activation, and by default, uses the Local System User for the execution of all its activities.

DCA 4 installs two services, MpsMonitor.Dca.Client and MpsMonitor.Dca.Monitor, that use the system Network User and Local User accounts respectively.

If there are special restrictions or policies that prevent the activation or the service execution by the above accounts, it will be necessary to use a specific local user instead. The DCA installation procedure will assign to this user the minimum rights needed to perform the service.

Ports

A list of ports used by a Windows installation of the DCA can be found above.

Windows Endpoints

The following URLs and ports are used to communicate with the MPS Monitor cloud services:

- https://*.abassetmanagement.com (port: 443)
- https://*.mpsmonitor.com (port: 443, and 8883 for DCA 4)

In addition, a configuration involving one or more HP SDS devices will use the following endpoints and ports:

- https://jamanagement.hp.com (port: 443)
- https://eu.jamanagement.hp.com (port: 443 - European production system)
- https://ews.hpjamservices.com (port: 443)
- https://connectivity.pod1.avatar.ext.hp.com:443/avatar/v1/entities/connectivityconfig (port: 443)
- https://registration.pod1.avatar.ext.hp.com:443/avatar/v1/entities/credentials (port: 443)
- Certificate Revocation List
    - http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl (port: 80)
    - http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl (port: 80)

Please see HP's SDS Security Whitepaper for more information. (A copy is available from the Help > Documentation section of the MPS Monitor console.)

MacOS

Supported OS

- Mac OS 10.8 – 10.12 (eXplorer MacOS v2)*
- Mac OS 10.10 + (eXplorer MacOS v3)*

  * Requires: Java for OS X 2015-001

  * Installation requires machine administrator's credentials

Ports

Besides the earlier-mentioned ports used for communication with devices, the MacOS DCA also uses ports 30006 and 30007 for communication between the graphic interface and the service.

Endpoints

- https://embedded.abassetmanagement.com (port: 443)
- https://embeddedfiles.abassetmanagement.com (port: 443)

Linux Debian-Ubuntu

Supported OS

- DCA 3: Ubuntu 17.04 LTS (64-bit)*
- DCA 3 and DCA 4: Ubuntu 18.04 LTS (64-bit)*
- DCA 3: Debian 9 Stretch (64-bit)* / DCA 4: Debian 11
- Other Linux OSes may be supported if the .NET CORE condition below can be met.

* Requires: “net-tools” package be installed, and Gnome used as desktop manager.

Installation of DCA 4 also requires .NET CORE 6.0 Runtime and ASP.NET CORE 6.0 Runtime be pre-installed.

Installation requires that the logged-in user have administrator rights (belongs to SUDO group). A user that interacts with Linux DCA (”EElinux”) application must belong to the "SUDO" and "EELINUX" groups. The user that is performing the installation is automatically added to “EELINUX” group.

Ports

Besides the earlier-mentioned ports used for communication with devices, the application uses ports 30006 and 30007 for communication between the graphic interface and the service.

Endpoints

- http://embeddedlinux.mpsmonitor.com (port: 80)
- http://embeddedfileslinux.mpsmonitor.com (port: 80)

Raspberry PI 3 board (Model B) / Raspbian GNU/Linux 9

Supported Configuration

- Raspberry PI 3 board (Model B) equipped with an 8Gb Micro SD card with at least 150MB free space.
- DCA 3: Raspbian GNU/Linux 9 OS with default LXDE desktop manager.
- DCA 4: See Linux section above for OS support.

  * Installation requires that the logged-in user have administrator rights (belongs to SUDO group). The user that interacts with Linux DCA ("EElinux") application must belong to the "SUDO" and "EELINUX" groups. A user that is performing the installation is automatically added to "EELINUX" group.

Ports

Besides the earlier-mentioned ports used for communication with devices, the application uses ports 30006 and 30007 for communication between the graphic interface and the service.

Endpoints

- http://embeddedraspberry.mpsmonitor.com (port: 80)
- http://embeddedfilesraspberry.mpsmonitor.com (port: 80)

HP Cloud DCA

Device Requirements

- HP FutureSmart devices with firmware version 4.9.0.1 or later
- Internet connection

Software Requirements

The HP MPS Onboarding Tool is the software used to enable Web Services at the printer level and obtain the device credentials that the SDS Cloud DCA will use to connect to the devices.

Supported OSes

- Windows 10 (x64)
- Windows 8.1 and 8.0 (x64)

Device Endpoints

The HP devices will use the following URLs and ports to communicate with the HP Cloud DCA:

- https://dopplerservice.msit.hpcloud.hp.com (port 443)[1]
- https://dopplerapp.msit.hpcloud.hp.com (port 443)[1]
- https://directory.id.hp.com (port 443)[1]
- https://coresvcs.dp.smartcloudprint.com (port 443)
- https://directory.stg.cd.id.hp.com (port 443)
- SDS On Device Services (e.g., Report a Problem)
  - https://ondeviceservicesprod.smartcloudprint.com/*
- SDS Remote Firmware Update
  - https://prod.firmwareupdate.hpjamservices.com/*
- HP Web Services
  - https://*.avatar.ext.hp.com/*
  - wss://*.avatar.ext.hp.com:443/*

[1] The HP MPS Onboarding Tool must also be able to reach these endpoints.

Embedded Device DCAs

Also, the embedded version of the DCA may be installed directly on some devices from some manufacturers as per the requirements and instructions contained in their respective installation guides. The supported devices and their respective endpoints are:

HP Future Smart 3.5, 4, 5

- https://embeddedhp.mpsmonitor.com (port: 80)
- https://embeddedfileshp.mpsmonitor.com (port: 443)
- (See the Windows Endpoints section, above, for additional communication channels used by HP SDS.)

Samsung (with XOA firmware 1.21+)

- http://embedded.abassetmanagement.com (port: 80)
- http://embeddedfiles.abassetmanagement.com (port: 80)

Kyocera Hypas

- http://embedded.abassetmanagement.com (port: 80)
- http://embeddedfiles.abassetmanagement.com (port: 80)

Lexmark (with Framework 4.x)

- http://embeddedlexmark.mpsmonitor.com (port: 80)
- http://embeddedfileslexmark.mpsmonitor.com (port: 80)

Konica Minolta (IWS version 2.x*, OpenAPI, and web browser option)

- http://embeddedkonica.mpsmonitor.com (port: 80)
- http://embeddedfileskonica.mpsmonitor.com (port: 80)

* Note: also uses ports 8090 and 8091 for internal, device/service communications.

References

Other Reference Materials

1. FBI Internet Crime Complaint Center (IC3) 2021 Report.pdf
2. HP Wolf Security Report: “Blurred Lines & Blind Spots” - May 2021
3. Quocirca Report: “The Print Security Landscape, 2022” – January 2022
4. Cybernews.com: "We hijacked 28,000 unsecured printers to raise awareness of printer security issues" - August 2020
5. MPS Monitor announces SOC2 compliance
6. MPS Monitor earns BLI Security Validation Testing seal for Policy Compliance from Keypoint Intelligence-Buyers Lab
7. MPS Monitor partners with Okta to provide Single Sign-On access
8. HP Smart Device Agent for USB Connected Printers White Paper
9. MPS Monitor announces integration with Universal Print in Microsoft 365