TECHNICAL WHITEPAPER

2025

SECURING YOUR MANAGED PRINT SERVICES

MPS Monitor
Printer Monitoring in the Cloud

marco

1 Purpose and structure of this Whitepaper

This **Technical Whitepaper** provides an overview of the Print Aware powered by MPS Monitor, focusing on various aspects related to security. The following sections offer a detailed examination of certifications, security policies, disaster mitigation, software integrity, and other critical components of the platform.

Introduction to Print Aware powered by MPS Monitor

In this section, we delve into the core features of Print Aware powered by MPS Monitor, emphasizing a comprehensive security policy. The discussion extends to data privacy and security strategies, ensuring a robust foundation for the platform.

Cloud Component Security

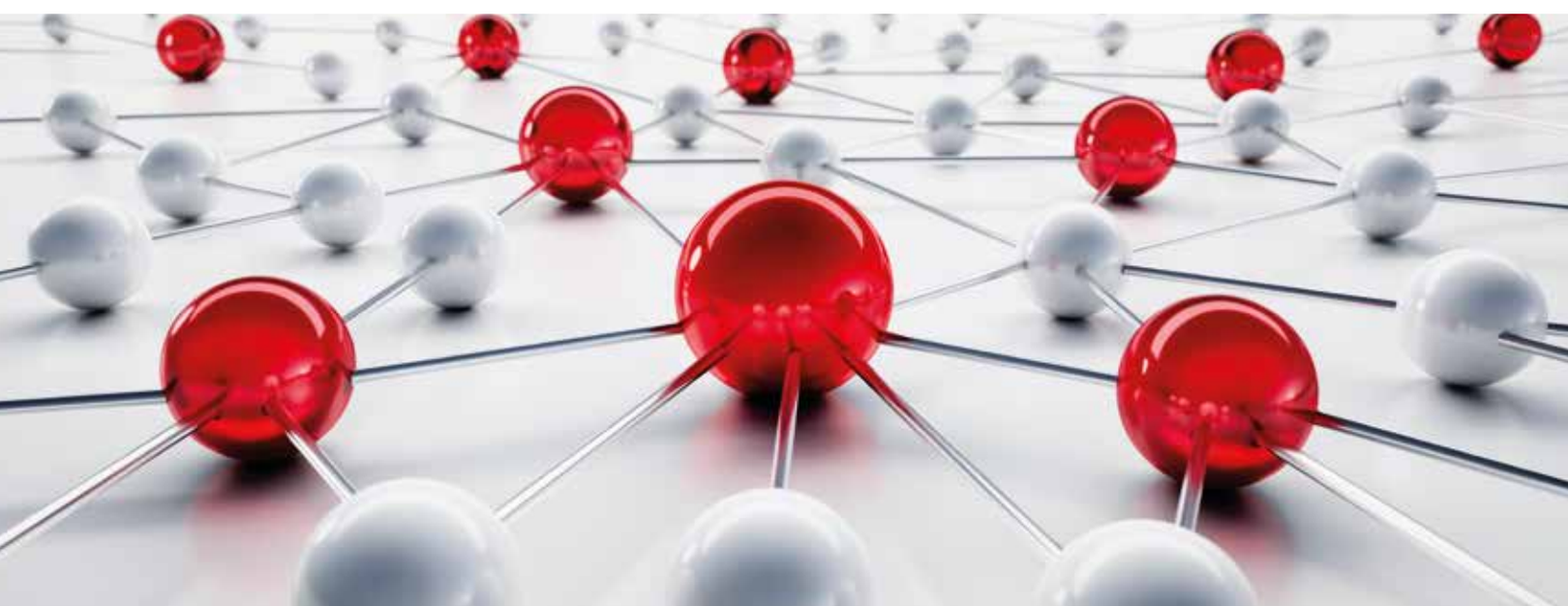
This segment addresses the security landscape within the software and cloud components, emphasizing operational security measures, and protocols related to user authentication.

Data Collection Agent (DCA) – Network-connected Devices

Here, we explore the intricacies of Data Collection Agents for network-connected devices. Versions 3 and 4 are discussed, with a particular emphasis on enhanced communication security and speed. The requirements for DCAs, including licensing, hardware, network, and operating system specifications, are comprehensively covered.

Integration with HP Smart Device Services (SDS)

The whitepaper concludes with an exploration of the integration capabilities with HP Smart Device Services, encompassing connectors, cloud DCAs, and monitoring features.



2 Introduction to Print Aware powered by MPS Monitor

Print Aware powered by MPS Monitor offers a **preeminent cloud-based Software as a Service (SaaS) solution deployed by Dealers and Managed Print Services** providers globally. Its primary mission is to vigilantly oversee and administer a fleet of printing devices manufactured by all main printer brands.

This whitepaper delineates what sets Print Aware powered by MPS Monitor apart as the premier leader in delivering **exceptionally secure Managed Print Services (MPS) solutions** for both dealers and their discerning clientele. The platform adopts a holistic approach to security, rigorously scrutinized and endorsed by reputable independent third-party organizations. Moreover, it undergoes continual audits to perpetuate and reinforce confidence in its security infrastructure and practices.

The platform comprises two principal components:

The Data Collection Agent (DCA) Connector: installed within the customer's Local Area Network (LAN), it executes operations on devices based on directives from the Server component. Versatile deployment includes Windows, Linux, or MAC OS systems, or integration into an MFP. An HP cloud-based DCA-less option (the **HP Cloud DCA**) monitors and manages HP FutureSmart devices remotely without installing any on-premises Agent.

The Cloud Server and Web Portal: the Cloud Server houses valuable device data furnished by the DCA. End-users access a dedicated web portal securely over HTTPS, interacting with the platform from any location and using any web browser.

A Comprehensive Security Framework

Print Aware powered by MPS Monitor has established and implemented an **Information Security Management System** (ISMS), a market-standard security framework which focuses on essential principles of **Confidentiality**, **Integrity**, and **Availability**, designed with the goal of extending its security features to the benefit of all dealers and their clients where the platform is used.

Compliance to regulations and standards

Print Aware powered by MPS Monitor has conspicuously demonstrated its commitment to security by successfully traversing globally recognized security-centric evaluations and certifications, including:

ISO/IEC 27001: signifying a systematic approach to managing information security risks, ensuring maximum Confidentiality, Integrity, and Availability of data.

System and Organization Controls 2 (SOC 2): achieving compliance with AICPA SOC 2 Type 2 Trust Service Criteria, by verifying the effectiveness of security controls over a period of one year.

CSA Star Level 2 Attestation: ensuring compliance with Cloud Control Matrix (CCM), a cybersecurity control framework for cloud computing.

Keypoint Intelligence: numerous evaluations corroborate the security integrity of Print Aware powered by Print Aware powered by MPS Monitor.

Data Privacy - GDPR Compliance

Any company with customers in Europe must comply with the **General Data Protection Regulation** 2016/679 (GDPR). Printer Dealers and Managed Print Service Providers (MPS) are no exception, as GDPR also applies to the management of personal data within SaaS remote monitoring systems.

Article 4.1 of the GDPR clearly defines “personal data” and includes names, physical addresses, and online identifiers such as an email address related to a physical identity.

GDPR compliance is important also for American customers for several reasons:

- **Global Business Operations**: many businesses operate on a global scale, either by having customers and clients in the European Union (EU) or by processing the personal data of EU citizens. GDPR compliance is essential for any organization that handles the personal data of EU residents, regardless of where the company is located.
- **Customer Trust and Reputation:** demonstrating GDPR compliance reflects a commitment to protecting the privacy and rights of individuals. In an era where data breaches and privacy concerns are prevalent, businesses that prioritize data protection are likely to be viewed favorably by consumers.
- **Legal and Regulatory Requirements**: global companies may have subsidiaries, branches, or business dealings in the EU, making GDPR compliance a legal requirement. Non-compliance can result in substantial fines and legal consequences.
- **Data Security Best Practices**: GDPR compliance encourages organizations to implement robust data security practices. Following GDPR guidelines aligns with general best practices for data protection and security. Even if not legally required, adopting these measures can help companies enhance their overall cybersecurity posture.

In summary, **GDPR compliance** is not solely a concern for EU-based businesses; it **has implications for any organization that interacts with the personal data of EU citizens**. Global businesses that recognize and address these considerations demonstrate a commitment to privacy, legal responsibility, and global data protection standards.

For more details on how Print Aware powered by MPS Monitor ensures compliance with GDPR, ISO27001, SOC2 Type 2 and CSA STAR Level 2,

visit this link

3 Cloud Component Security

Print Aware powered by MPS Monitor's backend cloud infrastructure, hosted within British Telecom data centers in Milan, Italy, is under complete ownership and administration of the technology provider, MPS Monitor. An internal team of highly skilled IT and security professionals oversees all the procedures and tools in place to ensure that the most stringent security requirements are met, and that full compliance with international standards is always guaranteed. **Security measures** adopted by the company include:

- 24x7 system monitoring using a comprehensive set of infrastructure and application monitoring tools;
- Extensive Log Analytics management;
- Real-time alerting on all main security-related events;
- Continuous Vulnerability Assessment and Monitoring on all assets;
- Bi-annual penetration testing performed by external cybersecurity companies;
- Continuous surveillance within annual ISO 27001, SOC 2 Type 2 and CSA STAR Level 2 assessments.

Software Integrity

Print Aware powered by MPS Monitor's software adheres to principles of "**security and data protection by default and by design**", by implementing a high number of measures and security control which ensure the utmost security in the development and release process. Measures include:

- Version control using version control software;
- File integrity monitoring to permit only authorized changes;
- Separate testing environments for quality assurance and user acceptance testing;
- Digital signatures for all components within a release package;
- Code reviews at every DCA code release;
- Security auditing and testing every six months, independently conducted by specialized firms.

Code Reviews

An external security firm carries out a **Code Review before every DCA code release**. The code testing activities are performed by adopting a hybrid approach that combines a **static code analysis** phase with a **dynamic application analysis**. This approach allows to deliver a high coverage over the attack surface and to discover both superficial vulnerabilities as well as problems that reside deeper in the application logic and therefore not immediately identifiable. All the issues found at a theoretical level are then validated through the creation of a **Proof of Concept** (PoC) software that allows to evaluate the actual level of exploitability from which it's subsequently possible to assign a severity score.

The Code Review activity also includes **testing both the source code and the compiled components against a pre-defined security checklist** which ensures that the package being released complies with the stringent security requirements set for the DCA component.
A new version of the DCA code can be released to customers only when the Code Review process formally certifies the resolution of security issues and the compliance with all requirements.

Access Control – User authentication

Accessing the Print Aware powered by MPS Monitor portal requires user accounts, governed by a meticulously structured system of user privileges. This system ensures precise and controlled access for users, aligned with their roles in a dealership or end customer's organization.

While it is imperative for passwords to be lengthy and complex to be considered strong, the human element can often undermine the effectiveness of such stringent requirements. Moreover, the necessity of maintaining multiple sets of credentials for various systems further compounds the risk factor.

Addressing these challenges, **Print Aware powered by MPS Monitor has incorporated two noteworthy features** to increase the security of user authentication:

Support for Single Sign-On (SSO) Solutions:

Print Aware powered by MPS Monitor offers support for Single Sign-On solutions, such as **Okta or Azure AD**. This integration empowers users to align with the best password practices prescribed by their organization's security teams. Through Okta or Azure AD integration, users can authenticate themselves via the organization's Identity Management (IDM) system, thereby gaining secure access to the Print Aware powered by MPS Monitor cloud platform. This streamlined and fully secure Single Sign-On process not only simplifies the user experience but also enhances security by reducing the reliance on traditional passwords passwords for each specific system. Users can access Print Aware powered by MPS Monitor without the need to remember multiple complex passwords, contributing to a more robust security ecosystem.

Support for Multi-Factor Authentication

Print Aware powered by MPS Monitor prioritizes the safeguarding of your data with the implementation of robust security measures, including multi-factor authentication. Users can enjoy an extra layer of protection for their sensitive information. This feature ensures that access to the application is granted only to authorized individuals, enhancing the overall security posture and providing peace of mind to users. At Print Aware powered by MPS Monitor, we understand the importance of keeping your data secure, and our commitment to employing cutting-edge security features like two-factor authentication reflects that dedication.

Physical security and Disaster Recovery

Physical access to the data center where Print Aware powered by MPS Monitor is hosted is strictly controlled. The facility is safeguarded by armed security personnel, and all guests are required to always have an escort. The center is equipped with video surveillance and fortified against fire and flooding.

To ensure the continuity of Print Aware powered by MPS Monitor's cloud services, even in the event of a complete infrastructure loss, whether physical or digital, a **comprehensive business continuity and disaster recovery plan** is in effect.

This plan includes the following measures:

- Annual testing of the plan against a range of potential threat scenarios, taking likelihood into account.
- Ongoing testing of the disaster recovery system to ensure its functionality in case of an emergency.
- Engagement with a third-party cybersecurity consulting firm for a rapid response to any security incident.
- Annual reviews of incident response policies.

4 Data Collection Agent (DCA) requirements and communication protocols

The **Data Collection Agent** (DCA) utilizes the **Simple Network Management Protocol** (SNMP) over **UDP port 161** to scan for network-connected MFPs, copiers, and printers. Only devices meeting the minimum printer MIB v.2 specifications as per the industry standard RFC3805 are incorporated into Print Aware powered by MPS Monitor, while others on the network are excluded from the data-gathering process. The DCA supports SNMP v1, v2c, and v3 of the standard SNMP protocol stack, with SNMP v3 being the most secure due to the inclusion of encryption.

For local network communication between the DCA and the enumerated devices, the necessary communication ports are outlined as follows:

DCA Internal Network Requirements

Destination Network	Direction	Protocol	Port
Internal (Networks with Devices) for Device Monitoring	Outbound	UDP	UDP 161 (SNMP)
Internal (Networks with Devices) for Device Web Access and HP LFP	Outbound	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Internal (Networks with Devices) for Device Web Access and HP LFP	Outbound	TCP	TCP 9100 TCP 515 (LPR)

Windows Data Collection Agent (eXplorer 3 version)

The **eXplorer 3** version of the DCA, installed on a Windows OS computer, uses port 443 for Secure Hypertext Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS 1.2) encrypted communications with the Print Aware powered by MPS Monitor cloud services. All communication between the Print Aware powered by MPS Monitor DCA and the Print Aware powered by MPS Monitor cloud is initiated by the DCA, periodically polling the Print Aware powered by MPS Monitor cloud for tasks to perform.

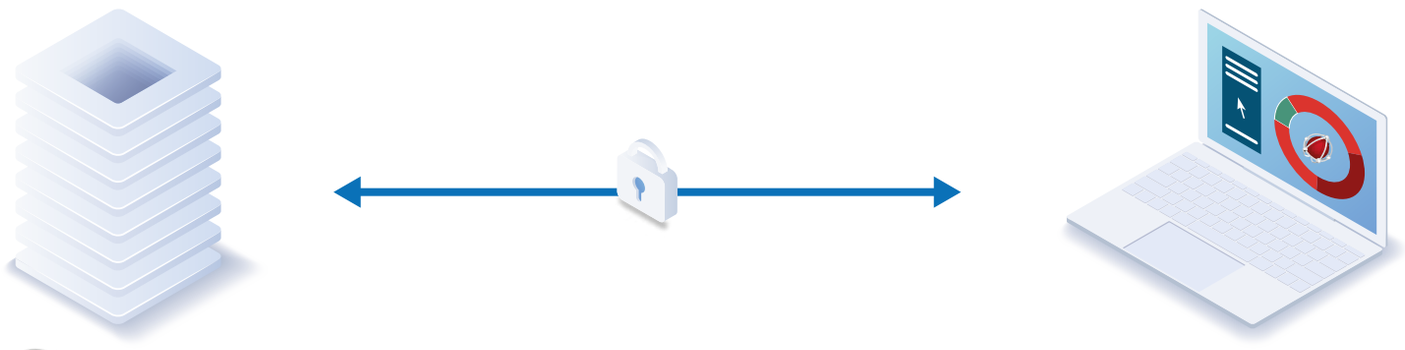
Appropriate firewall settings may be required on the computer running the DCA component and any network-based firewall to permit this data exchange. The DCA can be configured to work with the organization's proxy.

Data Collection Agent Version 4

DCA 4 is available for Windows Server 2016 or later and Windows 10 or later, introducing **enhanced functionalities** such as expedited and more secure communication, SNMP v3 support, and the addition of Device Web Access (DWA). DWA allows Print Aware powered by MPS Monitor Console users to browse the embedded web server pages of any customer's printer.

Improved Communication Security & Speed

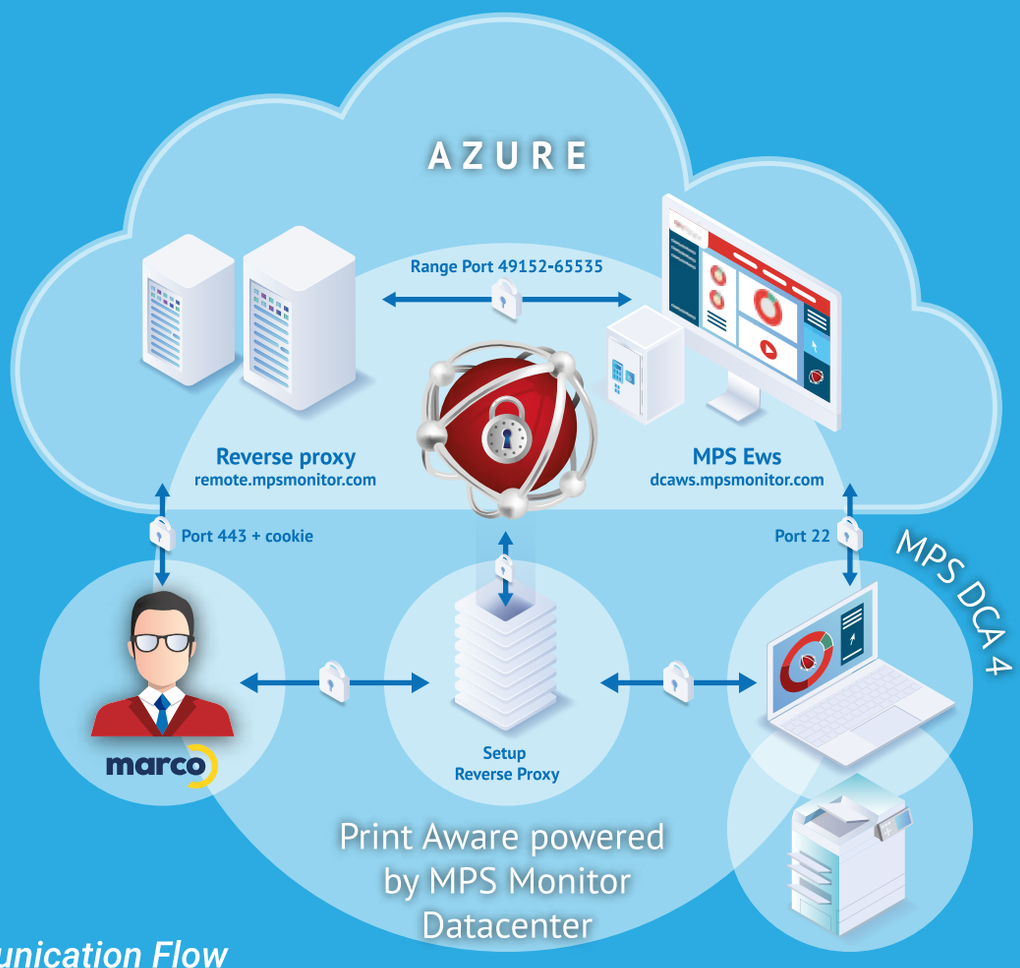
DCA 4 enhances security and traffic optimization by using HTTPS2/GRPC over port 443. Furthermore, DCA 4 incorporates MQTT, a lightweight IoT communication protocol, utilizing Azure IOT Hub as a message broker. This significantly boosts the speed of communication between the DCA and devices on the local network and the Print Aware powered by MPS Monitor Cloud service.



Device Web Access

DCA 4's **Device Web Access** (DWA) is a robust feature, safeguarded to ensure limited and secure printer HTTP access through various measures:

- Access is restricted to devices owned by a given dealer;
- Mandatory 2-factor authentication or Active Directory integration ensures that only authorized users may use the DWA feature;
- The DWA system is hosted on MS Azure, enabling temporary firewall exceptions to access the service, which are deleted after each session;
- Target device attribute verification is performed with each connection to prevent access to invalid devices;
- Access logs are generated for each use;
- File transfers using DWA are disabled.



DWA Communication Flow

DCA Requirements

Licensing Requirements
No extra licenses are needed for installing Print Aware powered by MPS Monitor.

Hardware Requirements
Recommended hardware for the machine hosting the DCA:

- CPU: Intel Core i3+
- RAM: 2 GB+ (4 GB+ recommended)
- HD Space: 100MB+ (1GB+ recommended)

The PC does not need to be dedicated and can be used simultaneously for other uses. The DCA connector works in the background without affecting PC users. For large networks with high scanning requirements, better hardware is recommended for improved performance.

Network Requirements - DCA 4

The system where DCA 4 is installed must have permanent access to the following endpoints and protocols:

Web endpoints for Americas Region	Protocol	Ports	IP Address CDN entry
https://us01-dca.mpsmonitor.com for Device Monitoring communication	HTTP2, GRPC	443	20.106.185.115
https://cdn2.mpsmonitor.com for DCA Updates	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.com for Device Web Access	SSH	22	20.55.38.55
us01-broker-mpsmonitor.azure-devices.net for DCA MQTT communication	MQTT over WSS	443	Azure IOT HUB

OS Requirements

Windows

DCA4 is supported starting from **Windows 10 version for clients** and **Windows Server 2016 for server** installation. For older operating systems, only DCA3 is supported.

DCA4 setup will verify the .NET core libraries installation and will download the necessary libraries from the Microsoft website.
DCA3 setup will verify the .Net Framework 4.5 (full module) installation and download the necessary libraries from the Microsoft website.
(Note: Installation of the .Net Framework may require a system restart.)

On a Windows computer, eXplorer 3 DCA 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.

Embedded DCAs

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 (only "L1 Classic" platform)

Web endpoints for all Regions	Direction	Protocol	Port
http://embeddedhp.mpsmonitor.com	Outbound	TCP	HTTP, port 80
http://embeddedfileshp.mpsmonitor.com	Outbound	TCP	HTTP, port 80

Samsung (with XOA firmware 1.21+)

Web endpoints for all Regions	Direction	Protocol	Port
http://embedded.abassetmanagement.com	Outbound	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Outbound	TCP	HTTP, port 80

Kyocera Hypas

Web endpoints for all Regions	Direction	Protocol	Port
http://embedded.abassetmanagement.com	Outbound	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Outbound	TCP	HTTP, port 80

Lexmark (with Framework eSF 4.x, eSF 7.x)

Web endpoints for all Regions	Direction	Protocol	Port
http://embeddedlexmark.mpsmonitor.com	Outbound	TCP	HTTP, port 80
http://embeddedfileslexmark.mpsmonitor.com	Outbound	TCP	HTTP, port 80

5 Integration with HP Smart Device Services (SDS)

Print Aware powered by MPS Monitor's integration with **HP Smart Device Services** (SDS) offers a seamless and efficient solution for monitoring and managing HP printing devices. By leveraging the capabilities of Print Aware powered by MPS Monitor alongside the advanced features of HP SDS, organizations can gain comprehensive insights into their fleet of HP printers. This integration facilitates proactive maintenance, real-time monitoring, and precise reporting, optimizing the overall performance of the printing infrastructure.

With the combined power of Print Aware powered by MPS Monitor and HP SDS, businesses can **enhance productivity, reduce operational costs, and ensure the smooth functioning of their print ecosystem**.

A full list of compatible devices and available features is available at this link

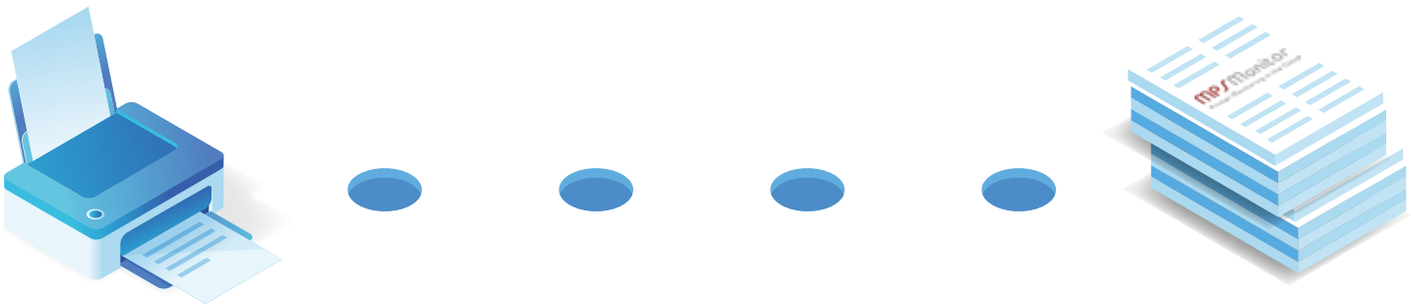
HP JetAdvantage Management Connector (JAMC)

The **JAMC software**, a DCA built by HP, allows executing SDS features on Windows installation. Print Aware powered by MPS Monitor Windows DCAs are fully integrated with this technology and allow the use of SDS features directly from the Print Aware powered by MPS Monitor portal.

Network Communication requirements for JAMC Device Monitoring

HP JAMC Internal network requirement

Web endpoints for all Regions	Direction	Protocol	Port
Internal (Networks with Devices) for JAMC Device Monitoring	Outbound	UDP	161, 427, 3702
Internal (Networks with Devices) for JAMC Device Monitoring	Outbound	TCP	443, 3910, 3911, 7627, 8080

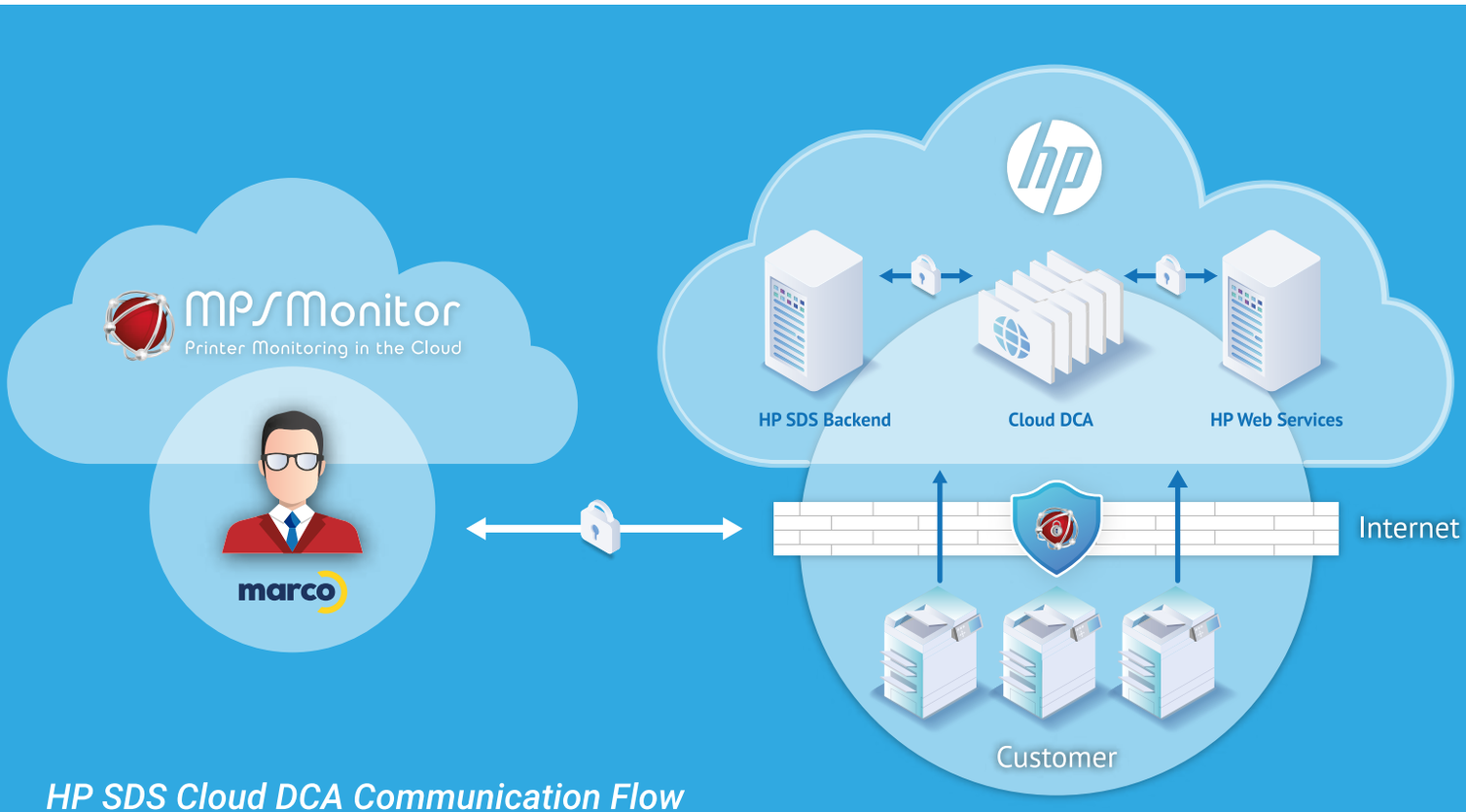


JAMC is directly connected to the HP SDS Cloud infrastructure and the table below outlines all necessary communication ports:

Web endpoints for Americas Regions	Direction	Protocol	Port
https://jamanagement.hp.com	Outbound	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Outbound	TCP	HTTPS, port 443
https://ews.hpjamservices.com	Outbound	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Outbound	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Outbound	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobal G2TLSRSASHA2562020CA1.crl	Outbound	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobal G2TLSRSASHA2562020CA1.crl	Outbound	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Outbound	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobal G2TLSRSASHA2562020CA1-2.crl	Outbound	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobal G2TLSRSASHA2562020CA1-2.crl	Outbound	TCP	HTTP, port 80

HP SDS Cloud

The **HP Smart Device Services Cloud DCA** enables Print Aware powered by MPS Monitor to remotely oversee and control HP Future Smart devices without requiring a DCA installation on the network.



HP SDS Cloud DCA Communication Flow

Communication with HP SDS Cloud DCA

HP SDS Cloud DCA is available for HP SDS compatible devices with **HP Future Smart version 4.9.0.1** or later.

Supported devices must need to have a stable connection to the following web endpoints:

Web endpoints for all Regions	Direction	Protocol	Port
https://*.avatar.ext.hp.com:443	Outbound	TCP	HTTPS, port 443
http://*.avatar.ext.hp.com:80	Outbound	TCP	HTTP, port 80
udp://*.avatar.ext.hp.com:9930	Outbound	UDP	UDP, port 9930
wss://*.avatar.ext.hp.com:443	Outbound	TCP	WSS, port 443
https://*.hpjamservices.com:443	Outbound	TCP	HTTPS, port 443
https://*.smartcloudprint.com:443	Outbound	TCP	HTTPS, port 443

Onboard a printer as HP SDS cloud-connected

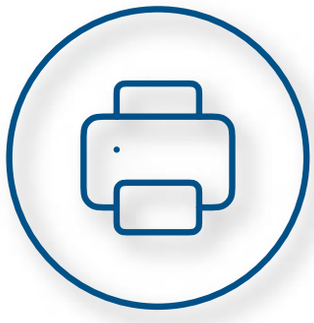
In order to use the **HP SDS cloud DCA** a printer needs to be onboard into the **HP SDS Cloud**.
To perform this operation the following requirements are needed:

- The printer needs to be connected to the internet;
- A Windows PC connected to the same network as the printer where to install the HP MPS Onboarding Tool;

The Windows PC needs to access the following endpoints:

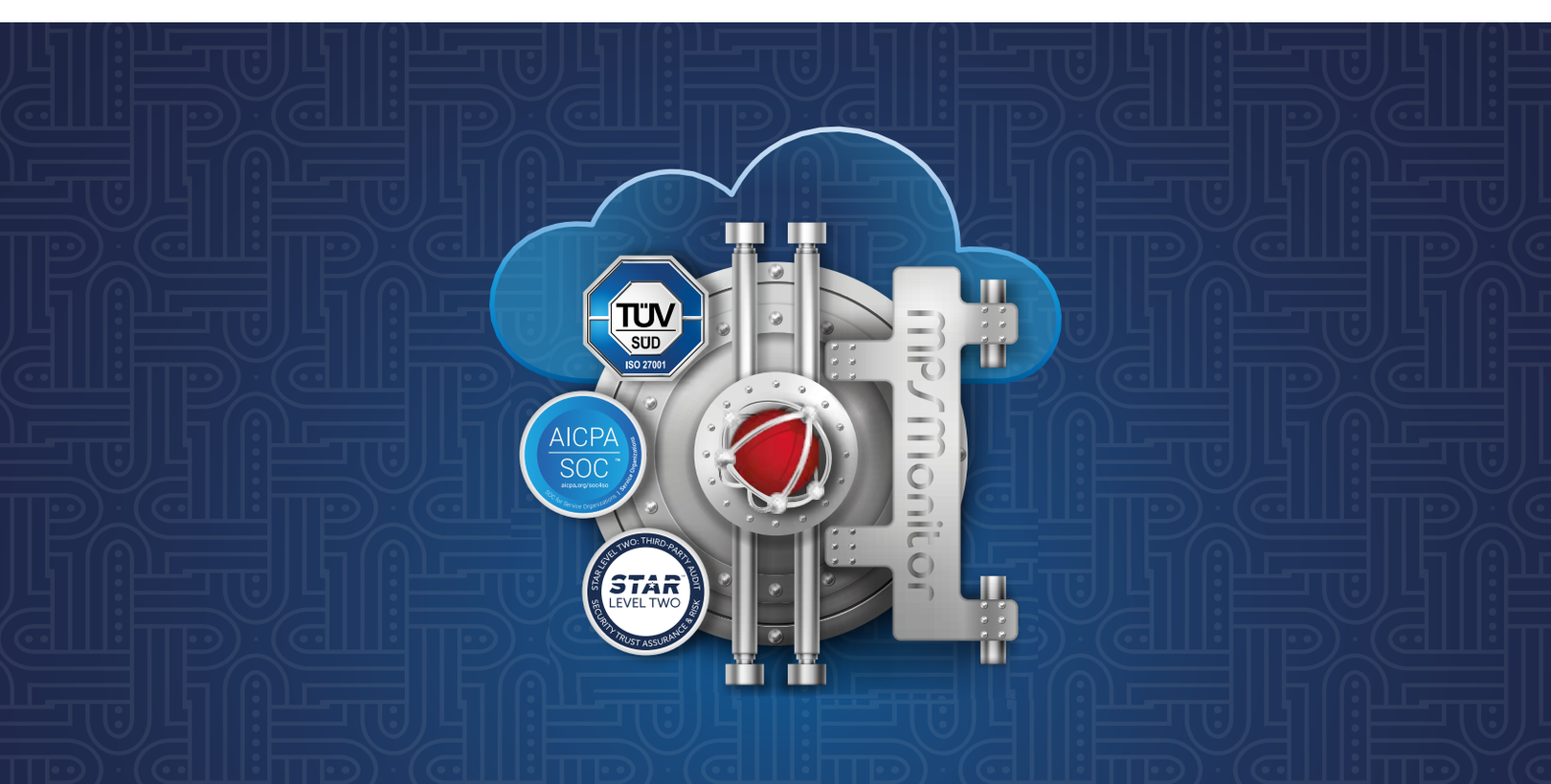
Web endpoints for all Regions	Direction	Protocol	Port
https://dopplerservice.msit.hpcloud.hp.com	Outbound	TCP	HTTPS, port 443
https://dopplerservice.msit.hpcloud.hp.com	Outbound	TCP	HTTPS, port 443
https://directory.id.hp.com	Outbound	TCP	HTTPS, port 443
https://coresvcs.dp.smartcloudprint.com	Outbound	TCP	HTTPS, port 443
https://directory.stg.cd.id.hp.com	Outbound	TCP	HTTPS, port 443

For detailed information about the HP MPS Onboarding tool, refer to HP's "**HP MPS Onboarding Tool User Guide**" available in the Print Aware powered by MPS Monitor Portal.



6 Reference Documents

- FAQ for Print Aware
- ISO 27001 Certificate for Print Aware
- Print Aware Data Path
- Print Aware Installation Guide for Clients
- Print Aware Security Due Diligence Question and Answer
- Print Aware Security Technical Whitepaper
- Safety and Security Compliance Certificate for Print Aware
- Keypoint Intelligence Solution Report - MPS Monitor
- Keypoint Intelligence Brochure - MPS Monitor
- CSA STAR CAIQ
- IDC Security Spotlight - MPS Monitor



MPS Monitor
Printer Monitoring in the Cloud

marco

For more information,
visit: