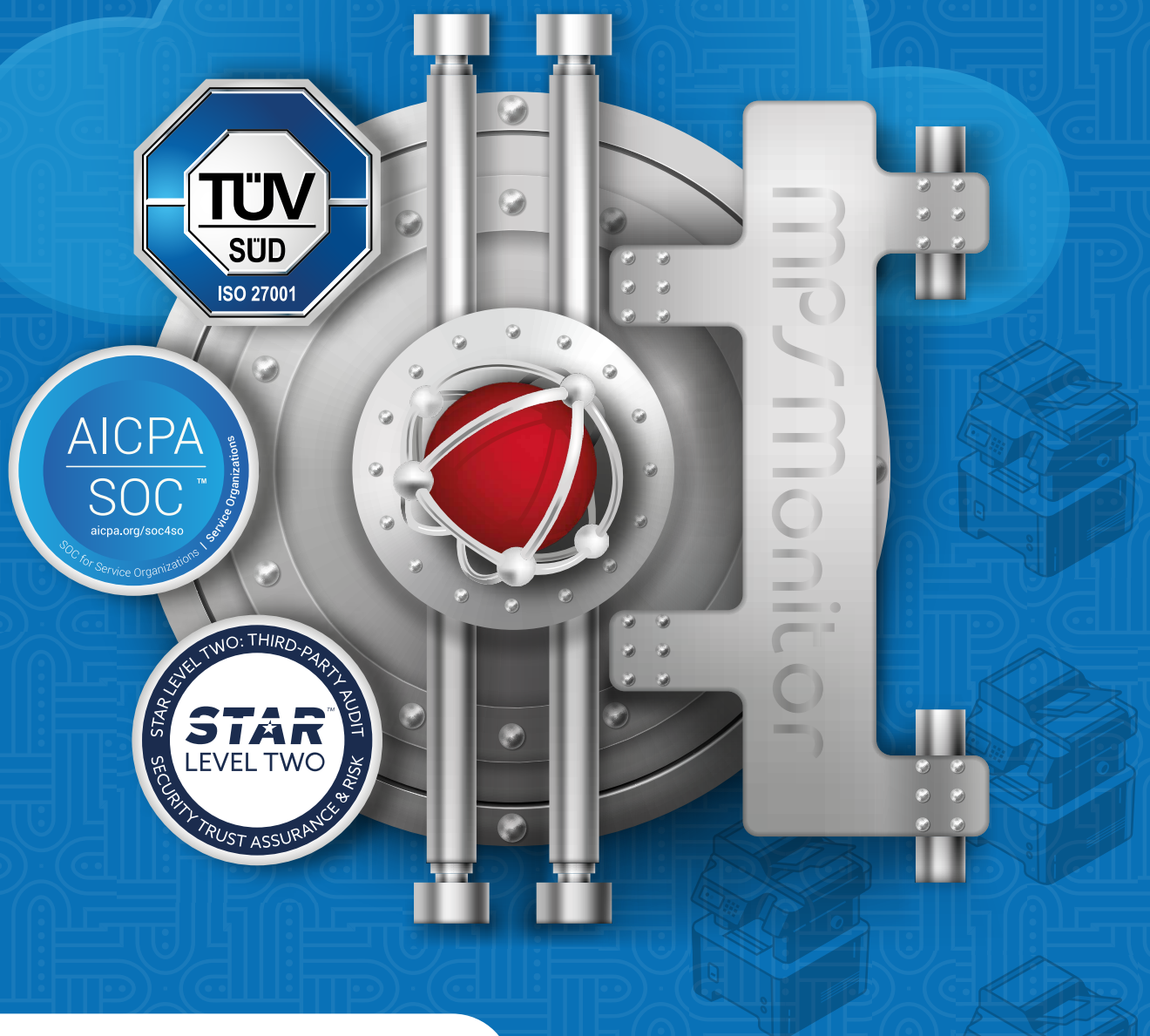


CÓMO PROTEGER SUS MANAGED PRINT SERVICES



mpsMonitor
Printer Monitoring in the Cloud

01	Finalidad y estructura de este Whitepaper	pág. 03
-----------	--	----------------

02	Introducción a MPS Monitor	pág. 04
-----------	-----------------------------------	----------------

- > Un marco de seguridad integral
- > Cumplimiento de normativas y estándares
- > Privacidad de los datos: cumplimiento del RGPD

03	Seguridad de los componentes en la nube	pág. 07
-----------	--	----------------

- > Integridad del software
- > Revisiones de código
- > Control de acceso: autenticación de usuarios
- > Seguridad física y recuperación ante desastres

04	Requisitos del Data Collection Agent (DCA)	pág. 10
-----------	---	----------------

y protocolos de comunicación

- > Data Collection Agent versión 4
- > Device Web Access
- > Requisitos del DCA
 - Requisitos de licencia
 - Requisitos de hardware
 - Requisitos de red
 - Requisitos del sistema operativo
 - Windows
 - MacOS
 - Linux
 - DCA embebidos

05	Integración con HP Smart Device Services (SDS)	pág. 18
-----------	---	----------------

- > Integración con HP Smart Device Services (SDS)
- > HP SDS Cloud DCA
- > Incorporar una impresora como dispositivo conectado a la nube de HP SDS
- > HP Smart Device Agent: para la monitorización de dispositivos HP por USB

06	Documentos de referencia	pág. 25
-----------	---------------------------------	----------------

1 Finalidad y estructura de este whitepaper

Este **whitepaper técnico** ofrece una visión general de la plataforma SaaS de MPS Monitor, centrándose en diversos aspectos relacionados con la seguridad. Las siguientes secciones ofrecen un examen detallado de las certificaciones, las políticas de seguridad, la mitigación de incidentes, la integridad del software y otros componentes críticos de la plataforma.

Introducción a MPS Monitor

En esta sección se profundiza en las funciones principales de MPS Monitor, poniendo el énfasis en una política de seguridad integral. El análisis se extiende a las estrategias de privacidad y seguridad de los datos, garantizando una base sólida para la plataforma.

Seguridad de los componentes en la nube

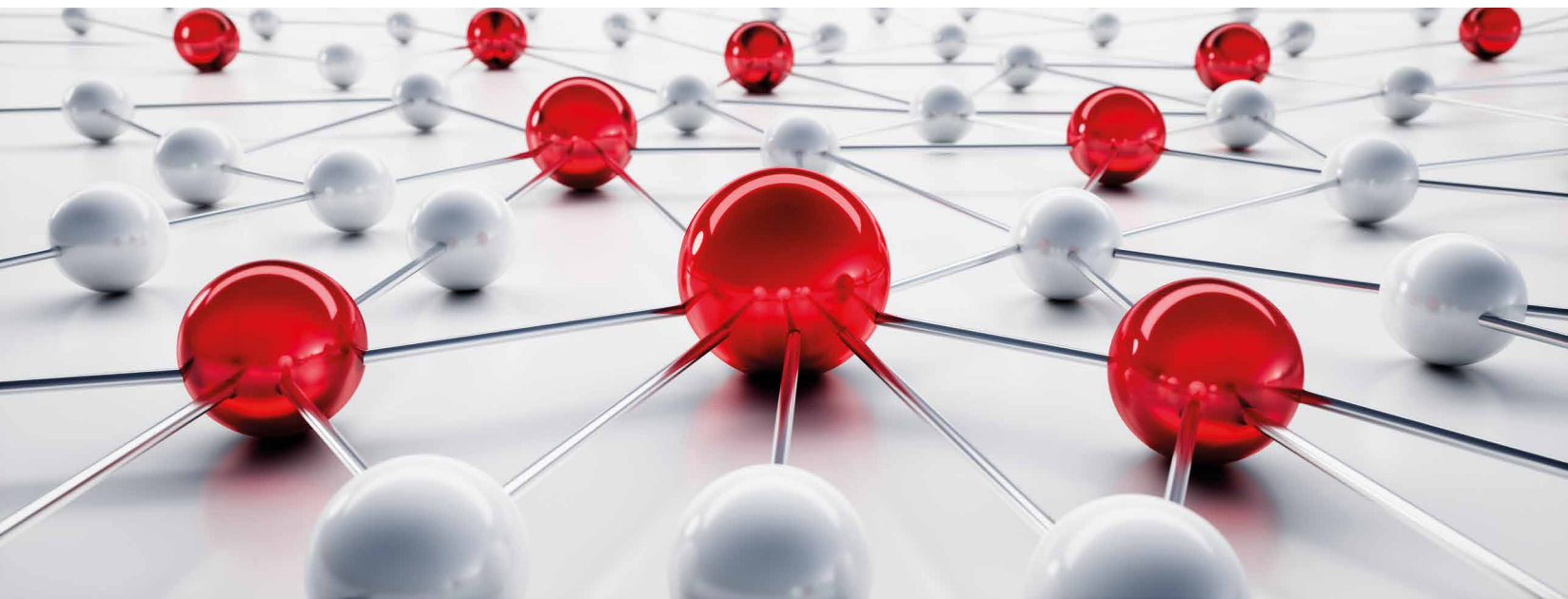
Este apartado aborda el panorama de la seguridad dentro del software y los componentes en la nube, destacando las medidas de seguridad operativa y los protocolos relacionados con la autenticación de usuarios.

Data Collection Agent (DCA): dispositivos conectados a la red

Aquí se exploran los aspectos más complejos de los Data Collection Agents para dispositivos conectados a la red. Se analiza la versión 4, con especial atención a la mayor seguridad y velocidad de las comunicaciones. Los requisitos de los DCA, incluidas las especificaciones de licencia, hardware, red y sistema operativo, se tratan de forma exhaustiva.

Integración con HP Smart Device Services (SDS)

El whitepaper concluye con una exploración de las capacidades de integración con HP Smart Device Services, que abarca conectores, DCA en la nube y soluciones de monitorización para dispositivos HP por USB.



2 Introducción a MPS Monitor

MPS Monitor ofrece una **solución preeminente de Software como Servicio (SaaS) basada en la nube**, implantada por **distribuidores y proveedores de Managed Print Services** de todo el mundo. Su misión principal es supervisar y administrar de forma rigurosa un parque de dispositivos de impresión fabricados por todas las principales marcas de impresoras.

Este whitepaper describe qué diferencia a MPS Monitor como líder de referencia a la hora de ofrecer **soluciones de Managed Print Services (MPS) excepcionalmente seguras**, tanto para los distribuidores como para su exigente clientela. La plataforma adopta un enfoque holístico de la seguridad, rigurosamente examinado y avalado por organizaciones independientes de reconocido prestigio. Además, se somete a auditorías continuas para mantener y reforzar la confianza en su infraestructura y sus prácticas de seguridad.

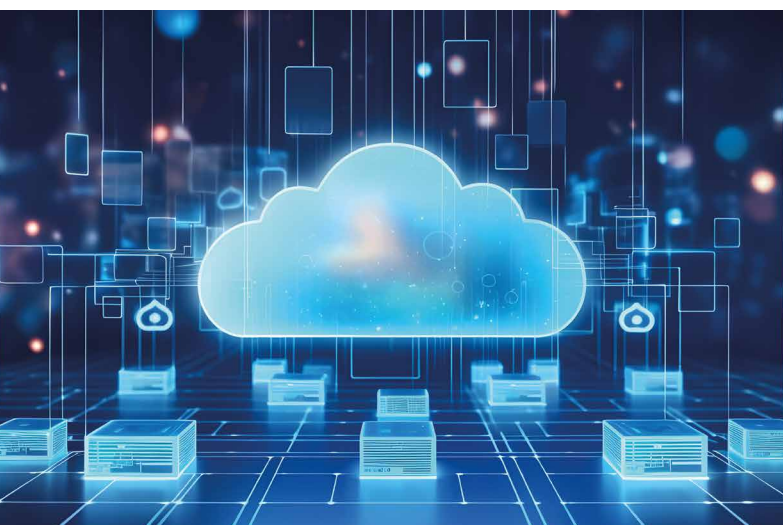
La plataforma se compone de dos componentes principales:

- 1. El conector Data Collection Agent (DCA):** instalado dentro de la red de área local (LAN) del cliente, ejecuta operaciones en los dispositivos según las directivas del componente Servidor. Su despliegue versátil incluye sistemas Windows, Linux o macOS, o la integración en una impresora multifunción (MFP). Una opción sin DCA basada en la nube de HP (el **HP Cloud DCA**) monitoriza y gestiona los dispositivos HP FutureSmart de forma remota, sin instalar ningún Agente en las instalaciones.
- 2. El servidor en la nube y el portal web:** el servidor en la nube alberga valiosos datos de los dispositivos proporcionados por el DCA. Los usuarios finales acceden a un portal web específico de forma segura a través de HTTPS, interactuando con la plataforma desde cualquier lugar y con cualquier navegador web.



Un marco de seguridad integral

MPS Monitor ha establecido e implantado un **Sistema de Gestión de Seguridad de la Información (ISMS)**, un marco de seguridad estándar del mercado que se centra en los principios esenciales de **Confidencialidad, Integridad y Disponibilidad**, diseñado con el objetivo de extender sus funciones de seguridad en beneficio de todos los distribuidores y sus clientes allí donde se utiliza la plataforma.





“ *MPS Monitor ha dimostrato de forma notoria su compromiso con la seguridad*



Cumplimiento de normativas y estándares

MPS Monitor ha demostrado de forma notoria su compromiso con la seguridad al superar con éxito evaluaciones y certificaciones de seguridad reconocidas a nivel mundial, entre las que se incluyen:



ISO/IEC 27001: que denota un enfoque sistemático para gestionar los riesgos de seguridad de la información, garantizando la máxima Confidencialidad, Integridad y Disponibilidad de los datos.



System and Organization Controls 2 (SOC 2): con el cumplimiento de los criterios AICPA Service Organization Control 2 Type 2 durante un periodo de un año, verificando la eficacia de los controles de seguridad.



Atestación CSA STAR Level 2: que garantiza el cumplimiento de la Cloud Controls Matrix (CCM), un marco de controles de ciberseguridad para la computación en la nube.



Keypoint Intelligence: numerosas evaluaciones corroboran la integridad de la seguridad de MPS Monitor.



Privacidad de los datos: cumplimiento del RGPD



Toda empresa con clientes en Europa debe cumplir el **Reglamento General de Protección de Datos** 2016/679 (RGPD). Los distribuidores de impresoras y los proveedores de Managed Print Services (MPS) no son una excepción, ya que el RGPD se aplica también a la gestión de datos personales dentro de los sistemas SaaS de monitorización remota.

El artículo 4.1 del RGPD define claramente los «datos personales» e incluye nombres, direcciones físicas e identificadores en línea, como una dirección de correo electrónico relacionada con una identidad física.



El cumplimiento del RGPD es importante también para los clientes estadounidenses por varias razones:



Operaciones comerciales globales: muchas empresas operan a escala global, ya sea porque tienen clientes en la Unión Europea (UE) o porque tratan datos personales de ciudadanos de la UE. El cumplimiento del RGPD es esencial para cualquier organización que maneje datos personales de residentes en la UE, con independencia de dónde esté ubicada la empresa.



Confianza y reputación de los clientes: demostrar el cumplimiento del RGPD refleja el compromiso de proteger la privacidad y los derechos de las personas. En una época en la que las brechas de datos y las preocupaciones por la privacidad son frecuentes, es probable que los consumidores valoren favorablemente a las empresas que priorizan la protección de datos.



Requisitos legales y reglamentarios: las empresas globales pueden tener filiales, sucursales o relaciones comerciales en la UE, lo que convierte el cumplimiento del RGPD en un requisito legal. El incumplimiento puede acarrear multas cuantiosas y consecuencias legales.



Buenas prácticas de seguridad de los datos: el cumplimiento del RGPD anima a las organizaciones a implantar prácticas sólidas de seguridad de los datos. Seguir las directrices del RGPD está en línea con las buenas prácticas generales de protección y seguridad de los datos. Aunque no sea legalmente obligatorio, adoptar estas medidas puede ayudar a las empresas a mejorar su postura general de ciberseguridad.

En resumen, el **cumplimiento del RGPD** no es una preocupación exclusiva de las empresas con sede en la UE: tiene **implicaciones para cualquier organización que interactúe con los datos personales de ciudadanos de la UE**. Las empresas globales que reconocen y abordan estas consideraciones demuestran un compromiso con la privacidad, la responsabilidad legal y los estándares globales de protección de datos.



Para obtener más detalles sobre cómo MPS Monitor garantiza el cumplimiento del RGPD, ISO 27001, SOC 2 Type 2 y CSA STAR Level 2,

visite este [enlace](#)



3 Seguridad de los componentes en la nube

La infraestructura de nube de backend de MPS Monitor, alojada en los centros de datos de British Telecom en Milán (Italia), es propiedad y está administrada por completo por la propia empresa. Un equipo interno de profesionales de TI y seguridad altamente cualificados supervisa todos los procedimientos y herramientas implantados para garantizar que se cumplen los **requisitos de seguridad** más estrictos y que se mantiene siempre el pleno cumplimiento de los estándares internacionales.

Entre las medidas de seguridad adoptadas por la empresa se incluyen:

- ➔ Monitorización del sistema 24x7 mediante un completo conjunto de herramientas de monitorización de infraestructura y aplicaciones;
- ➔ Amplia gestión de Log Analytics;
- ➔ Alertas en tiempo real sobre todos los principales eventos relacionados con la seguridad;
- ➔ Evaluación y monitorización continuas de vulnerabilidades en todos los activos;
- ➔ Pruebas de penetración anuales realizadas por empresas externas de ciberseguridad;
- ➔ Vigilancia continua dentro de las evaluaciones anuales de ISO 27001, SOC 2 Type 2 y CSA STAR Level 2.



Integridad del software

El software de MPS Monitor se adhiere a los principios de «seguridad y protección de datos por defecto y desde el diseño», mediante la implantación de un elevado número de medidas y controles de seguridad que garantizan la máxima seguridad en el proceso de desarrollo y publicación. Entre las medidas se incluyen:

- ➔ Control de versiones mediante software de control de versiones;
- ➔ Monitorización de la integridad de los archivos para permitir únicamente los cambios autorizados;
- ➔ Entornos de prueba independientes para el control de calidad y las pruebas de aceptación de usuario;
- ➔ Firmas digitales para todos los componentes dentro de un paquete de publicación;
- ➔ Revisiones de código en cada publicación de código del DCA;
- ➔ Auditorías y pruebas de seguridad cada seis meses, realizadas de forma independiente por empresas especializadas.



Revisiones de código

Una empresa externa de seguridad lleva a cabo una **revisión de código antes de cada publicación de código del DCA**. Las actividades de prueba del código se realizan adoptando un enfoque híbrido que combina una fase de **análisis estático de código** con un **análisis dinámico de la aplicación**. Este enfoque permite ofrecer una amplia cobertura de la superficie de ataque y descubrir tanto vulnerabilidades superficiales como problemas que residen a mayor profundidad en la lógica de la aplicación y que, por tanto, no son identificables de inmediato. Todos los problemas detectados en el plano teórico se validan después mediante la creación de software de **prueba de concepto** (Proof of Concept, PoC), lo que permite evaluar el nivel real de explotabilidad a partir del cual puede asignarse posteriormente una puntuación de gravedad.

La actividad de revisión de código incluye también **probar tanto el código fuente como los componentes compilados frente a una lista de comprobación de seguridad predefinida** que garantiza que el paquete que se va a publicar cumple los estrictos requisitos de seguridad establecidos para el componente DCA. Una nueva versión del código del DCA solo puede publicarse para los clientes cuando el proceso de revisión de código certifica formalmente la resolución de los problemas de seguridad y el cumplimiento de todos los requisitos.



Control de acceso: autenticación de usuarios

El acceso al portal de MPS Monitor requiere cuentas de usuario, regidas por un sistema de privilegios de usuario meticulosamente estructurado. Este sistema garantiza un acceso preciso y controlado para los usuarios, alineado con sus funciones en la organización de un distribuidor o de un cliente final.

Aunque es imprescindible que las contraseñas sean largas y complejas para que se consideren seguras, el factor humano puede menoscabar a menudo la eficacia de estos requisitos tan estrictos. Además, la necesidad de mantener varios juegos de credenciales para distintos sistemas agrava aún más el factor de riesgo.

Para hacer frente a estos retos, **MPS Monitor ha incorporado dos funciones destacables** para aumentar la seguridad de la autenticación de usuarios:



Compatibilidad con soluciones de Single Sign-On (SSO):

MPS Monitor ofrece compatibilidad con soluciones de Single Sign-On, como **Okta o Azure AD**. Esta integración permite a los usuarios alinearse con las mejores prácticas de contraseñas prescritas por los equipos de seguridad de su organización. Mediante la integración con Okta o Azure AD, los usuarios pueden autenticarse a través del sistema de Identity Management (IDM) de la organización, obteniendo así un acceso seguro a la plataforma en la nube de MPS Monitor. Este proceso de Single Sign-On optimizado y totalmente seguro no solo simplifica la experiencia del usuario, sino que también mejora la seguridad al reducir la dependencia de las contraseñas tradicionales para cada sistema concreto. Los usuarios pueden acceder a MPS Monitor sin necesidad de recordar múltiples contraseñas complejas, contribuyendo a un ecosistema de seguridad más sólido.



Compatibilidad con la autenticación multifactor

MPS Monitor da prioridad a la protección de sus datos con la implantación de sólidas medidas de seguridad, incluida la autenticación multifactor. Los usuarios pueden disfrutar de una capa adicional de protección para su información confidencial. Esta función garantiza que el acceso a la aplicación se conceda únicamente a las personas autorizadas, mejorando la postura general de seguridad y ofreciendo tranquilidad a los usuarios. En MPS Monitor entendemos la importancia de mantener sus datos seguros, y nuestro compromiso de emplear funciones de seguridad de vanguardia, como la autenticación multifactor, refleja esa dedicación.



Seguridad física y recuperación ante desastres

El acceso físico al centro de datos donde se aloja MPS Monitor está estrictamente controlado. Las instalaciones están protegidas por personal de seguridad armado y todos los visitantes deben ir siempre acompañados de un escolta. El centro está equipado con videovigilancia y protegido frente a incendios e inundaciones.

Para garantizar la continuidad de los servicios en la nube de MPS Monitor, incluso en caso de una pérdida total de la infraestructura, ya sea física o digital, existe un **plan integral de continuidad del negocio y recuperación ante desastres**.

Este plan incluye las siguientes medidas:



Pruebas anuales del plan frente a una serie de posibles escenarios de amenaza, teniendo en cuenta su probabilidad.



Pruebas continuas del sistema de recuperación ante desastres para garantizar su funcionalidad en caso de emergencia.



Colaboración con una consultora externa de ciberseguridad para dar una respuesta rápida a cualquier incidente de seguridad.



Revisiones anuales de las políticas de respuesta ante incidentes.

4 Requisitos del Data Collection Agent (DCA) y protocolos de comunicación

El **Data Collection Agent** (DCA) utiliza el protocolo **Simple Network Management Protocol** (SNMP) sobre el **puerto UDP 161** para buscar MFP, copiadoras e impresoras conectados a la red. Solo se incorporan a MPS Monitor los dispositivos que cumplen las especificaciones mínimas de la printer MIB v.2 según el estándar del sector RFC 3805, mientras que los demás dispositivos de la red quedan excluidos del proceso de recopilación de datos. El DCA es compatible con SNMP v1, v2c y v3 de la pila estándar del protocolo SNMP, siendo SNMP v3 el más seguro por incluir cifrado.

Para la comunicación en la red local entre el DCA y los dispositivos enumerados, los puertos de comunicación necesarios se detallan a continuación:

Requisitos de red interna del DCA

Red de destino	Dirección	Protocolo	Puerto
Interna (redes con dispositivos) para la monitorización de dispositivos (SNMP)	Saliente	UDP	UDP 161 (SNMP)
Interna (redes con dispositivos) para el Device Web Access y HP LFP	Saliente	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Interna (redes con dispositivos) para el Device Web Access y HP LFP	Saliente	TCP	TCP 9100 TCP 515 (LPR)



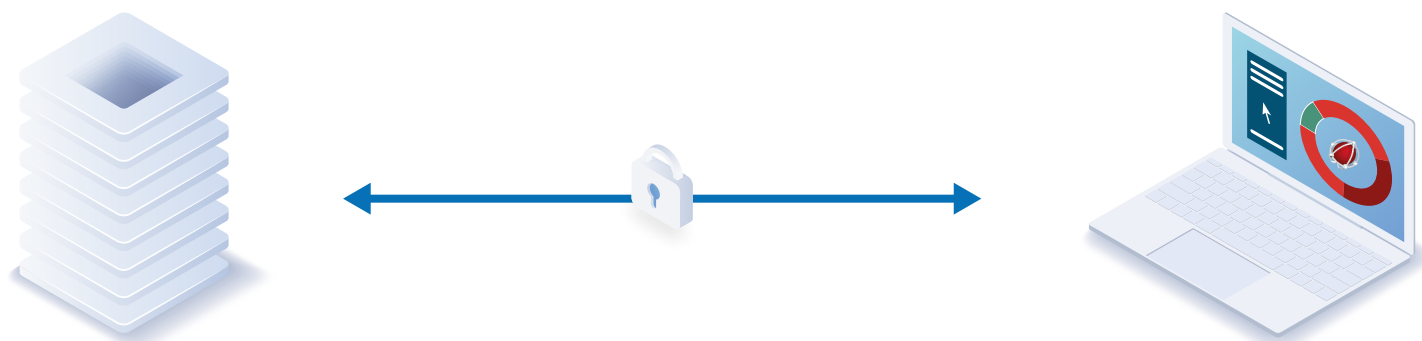


Data Collection Agent versión 4

El **DCA 4** está disponible para las plataformas Windows, macOS y Linux, e introduce **funcionalidades mejoradas** como una comunicación más rápida y segura, la compatibilidad con SNMP v3 y la incorporación de **Device Web Access** (DWA). DWA permite a los usuarios de la Consola de MPS Monitor navegar por las páginas del servidor web embebido de cualquier impresora del cliente.

Mayor seguridad y velocidad de las comunicaciones

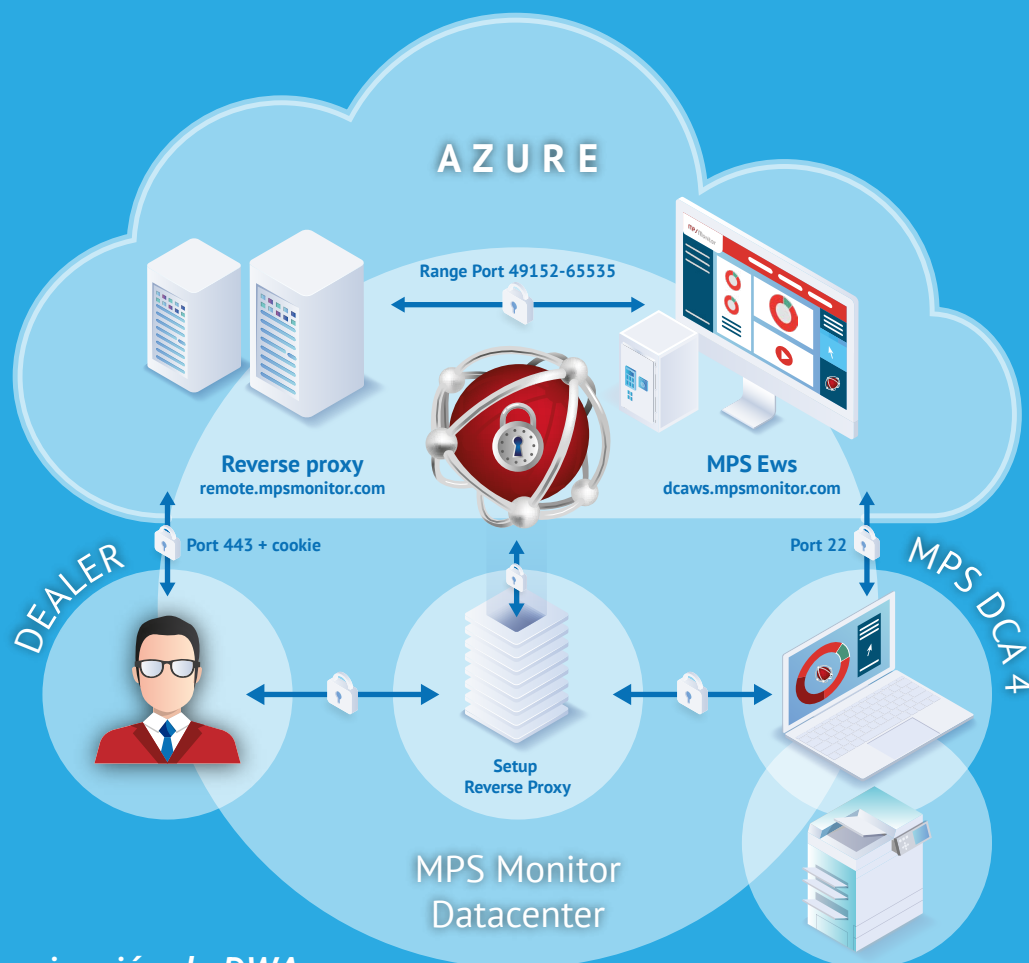
El DCA 4 mejora la seguridad y la optimización del tráfico utilizando HTTPS2/GRPC sobre el puerto 443. Además, el DCA 4 incorpora MQTT, un protocolo de comunicación IoT ligero, utilizando Azure IoT Hub como broker de mensajes. Esto aumenta significativamente la velocidad de comunicación entre el DCA y los dispositivos de la red local y el servicio en la nube de MPS Monitor.



Device Web Access

El Device Web Access (DWA) del DCA 4 es una función robusta, protegida para garantizar un acceso HTTP limitado y seguro a la impresora mediante diversas medidas:

-  El acceso está restringido a los dispositivos propiedad de un distribuidor determinado;
-  La autenticación de doble factor obligatoria o la integración con Active Directory garantizan que solo los usuarios autorizados puedan utilizar la función DWA;
-  El sistema DWA está alojado en MS Azure, lo que permite excepciones temporales de firewall para acceder al servicio, que se eliminan después de cada sesión;
-  La verificación de los atributos del dispositivo de destino se realiza con cada conexión para impedir el acceso a dispositivos no válidos;
-  Se generan registros de acceso en cada uso;
-  Las transferencias de archivos mediante DWA están deshabilitadas.



Flujo de comunicación de DWA



Requisitos del DCA

Requisitos de licencia

No se necesitan licencias adicionales para instalar MPS Monitor.

Requisitos de hardware

Hardware recomendado para la máquina que aloja el DCA:

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

El PC no tiene por qué ser dedicado y puede utilizarse simultáneamente para otros fines. El conector DCA funciona en segundo plano sin afectar a los usuarios del PC. Para redes grandes con altos requisitos de escaneo, se recomienda un hardware mejor para un mayor rendimiento.

Requisitos de red: DCA 4

El sistema donde se instala el DCA 4 debe tener acceso permanente a los siguientes endpoints y protocolos:

EU STACK (portal.mpsmonitor.com)

Endpoints web para las regiones EMEA y APAC	Protocolo	Puertos	Entrada CDN / dirección IP
https://dca4.mpsmonitor.com <i>para la comunicación de monitorización de dispositivos</i>	HTTP2, GRPC	443	213.92.56.75
https://cdn2.mpsmonitor.com <i>para las actualizaciones del DCA</i>	HTTP	443	Azure CDN
dcaws.mpsmonitor.com <i>para el Device Web Access</i>	SSH	22	13.80.42.210
eu01-broker-mpsmonitor.azure-devices.net <i>para la comunicación MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB

Endpoints web para la región de América	Protocolo	Puertos	Entrada CDN / dirección IP
https://us01-dca.mpsmonitor.com <i>para la comunicación de monitorización de dispositivos</i>	HTTP2, GRPC	443	20.106.185.115
https://cdn2.mpsmonitor.com <i>para las actualizaciones del DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>para los paquetes de descarga inicial del DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.com <i>para el Device Web Access</i>	SSH	22	20.55.38.55
us01-broker-mpsmonitor.azure-devices.net <i>para la comunicación MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB

US STACK (portal.mpsmonitor.us)

Endpoints web para la región de América	Protocolo	Puertos	Entrada CDN / dirección IP
https://us01-dca4.mpsmonitor.us <i>para la comunicación de monitorización de dispositivos</i>	HTTP2, GRPC	443	20.81.25.170
https://cdn2.mpsmonitor.com <i>para las actualizaciones del DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>para los paquetes de descarga inicial del DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.us <i>para el Device Web Access</i>	SSH	22	104.211.20.116
us01-brk-prd-eus-iothub-01.azure-devices.net <i>para la comunicación MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB



Requisitos del sistema operativo

Windows

El DCA 4 es compatible a partir de la versión **Windows 10 de 64 bits build 1607 (E) para clientes** y de **Windows Server 2016 de 64 bits para instalaciones de servidor**.

La instalación del DCA 4 verificará la instalación de las bibliotecas de .NET Core y descargará las bibliotecas necesarias desde el sitio web de Microsoft.

El DCA 4 instala dos servicios, **MpsMonitor.Dca.Client** y **MpsMonitor.Dca.Monitor**, que utilizan respectivamente las cuentas Network User y Local User del sistema.

Si existen restricciones o políticas especiales que impidan la activación o la ejecución del servicio por parte de las cuentas anteriores, será necesario utilizar en su lugar un usuario local específico.

El procedimiento de instalación del DCA asignará a este usuario los derechos mínimos necesarios para ejecutar el servicio.

MacOS

El DCA 4 puede instalarse a partir de **macOS 12 (Monterey)** o posterior, en CPU Intel o Arm (M1, M2).

Linux y Raspberry

El DCA 4 puede instalarse en **distribuciones de Linux compatibles con .NET Core**.

Puede instalarse en:

- ✓ Debian 12 or higher
- ✓ Ubuntu 22.04 or higher

Para la Raspberry, el requisito mínimo es una Raspberry Pi 3 o superior con Bookworm (Arm de 32 bits o Arm de 64 bits).

DCA embebidos

La versión embebida del DCA puede instalarse directamente en algunos dispositivos de determinados fabricantes, de acuerdo con los requisitos e instrucciones contenidos en sus respectivas guías de instalación.

Los dispositivos compatibles y sus respectivos endpoints son:

HP FutureSmart 3.5, 4, 5 (solo plataforma «L1 Classic»)

Endpoints web para todas las regiones	Dirección	Protocolo	Puertos
http://embeddedhp.mpsmonitor.com	Saliente	TCP	HTTP, port 80
http://embeddedfileshp.mpsmonitor.com	Saliente	TCP	HTTP, port 80

Samsung (con firmware XOA 1.21+)

Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
http://embedded.abassetmanagement.com	Saliente	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Saliente	TCP	HTTP, port 80

Kyocera HyPAS

Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
http://embedded.abassetmanagement.com	Saliente	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Saliente	TCP	HTTP, port 80



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

Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
http://embeddedlexmark.mpsmonitor.com	Saliente	TCP	HTTP, port 80
http://embeddedfileslexmark.mpsmonitor.com	Saliente	TCP	HTTP, port 80



5 Integración con HP Smart Device Services (SDS)

La integración de MPS Monitor con **HP Smart Device Services (SDS)** ofrece una solución fluida y eficiente para monitorizar y gestionar los dispositivos de impresión HP. Al aprovechar las capacidades de MPS Monitor junto con las funciones avanzadas de HP SDS, las organizaciones pueden obtener información completa sobre su parque de impresoras HP. Esta integración facilita el mantenimiento proactivo, la monitorización en tiempo real y unos informes precisos, optimizando el rendimiento general de la infraestructura de impresión.

Con la potencia combinada de MPS Monitor y HP SDS, las empresas pueden **aumentar la productividad, reducir los costes operativos y garantizar el buen funcionamiento de su ecosistema de impresión.**

En este [enlace](#) está disponible una lista completa de dispositivos compatibles y funciones disponibles



HP JetAdvantage Management Connector (JAMC)

El **software JAMC**, un DCA desarrollado por HP, permite ejecutar las funciones de SDS en una instalación de Windows. Los DCA de MPS Monitor para Windows están totalmente integrados con esta tecnología y permiten utilizar las funciones de SDS directamente desde el portal de MPS Monitor.

Requisitos de comunicación de red para la monitorización de dispositivos con JAMC

Requisito de red interna de HP JAMC

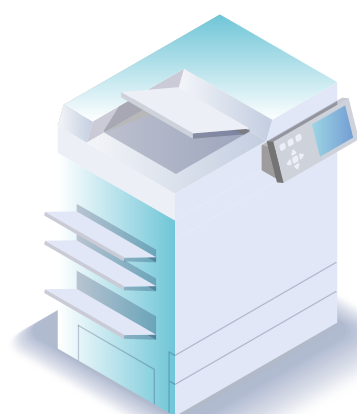
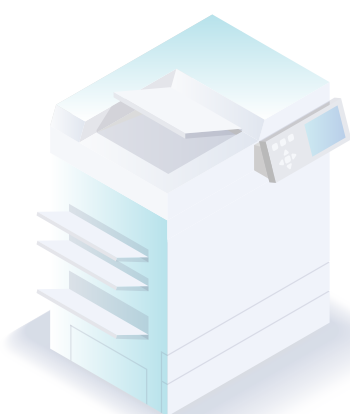
Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
Interna (redes con dispositivos) para la monitorización de dispositivos JAMC	Saliente	UDP	161, 427, 3702
Interna (redes con dispositivos) para la monitorización de dispositivos JAMC	Saliente	TCP	443, 3910, 3911, 7627, 8080



JAMC está conectado directamente a la infraestructura de HP SDS Cloud, y la siguiente tabla detalla todos los puertos de comunicación necesarios:

Endpoints web para la región de América	Dirección	Protocolo	Puerto
https://jamanagement.hp.com	Saliente	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Saliente	TCP	HTTPS, port 443
https://ews.hpjamservices.com	Saliente	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Saliente	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Saliente	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Saliente	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Saliente	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Saliente	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Saliente	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Saliente	TCP	HTTP, port 80

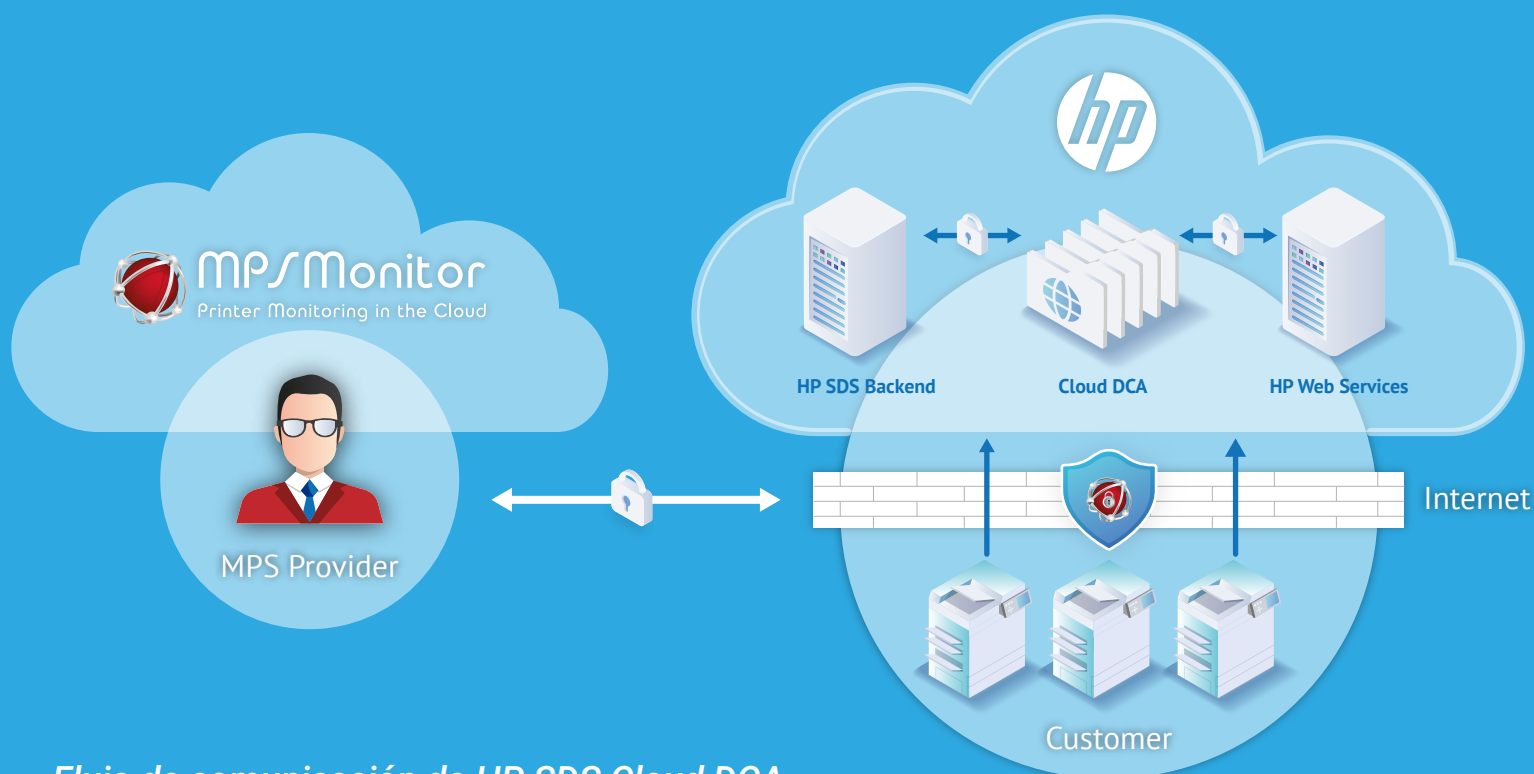
Endpoints web para las regiones EMEA y APAC	Dirección	Protocolo	Puerto
https://eu.jammanagement.hp.com	Saliente	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Saliente	TCP	HTTPS, port 443
https://eu.ews.hpjamservices.com	Saliente	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Saliente	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Saliente	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	Saliente	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	Saliente	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Saliente	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	Saliente	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	Saliente	TCP	HTTP, port 80





HP SDS Cloud

El **HP Smart Device Services Cloud DCA** permite a MPS Monitor supervisar y controlar de forma remota los dispositivos HP FutureSmart sin necesidad de instalar un DCA en la red.



Flujo de comunicación de HP SDS Cloud DCA

Comunicación con HP SDS Cloud DCA

HP SDS Cloud DCA está disponible para dispositivos compatibles con HP SDS que tengan la versión HP **FutureSmart 4.9.0.1** o posterior.

Los dispositivos compatibles deben tener una conexión estable con los siguientes endpoints web:

Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
https://*.avatar.ext.hp.com:443	Saliente	TCP	HTTPS, port 443
http://*.avatar.ext.hp.com:80	Saliente	TCP	HTTP, port 80
udp://*.avatar.ext.hp.com:9930	Saliente	UDP	UDP, port 9930
wss://*.avatar.ext.hp.com:443	Saliente	TCP	WSS, port 443
https://*.hpjamservices.com:443	Saliente	TCP	HTTPS, port 443
https://*.smartcloudprint.com:443	Saliente	TCP	HTTPS, port 443





Incorporar una impresora como dispositivo conectado a la nube de HP SDS

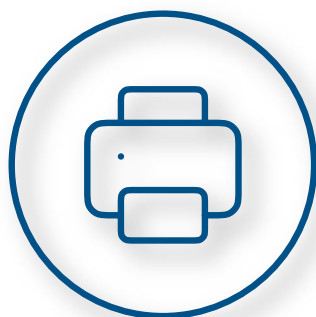
Para utilizar el **HP SDS Cloud DCA**, es necesario incorporar una impresora a **HP SDS Cloud**. Para realizar esta operación se necesitan los siguientes requisitos:

- ✓ La impresora debe estar conectada a internet;
- ✓ Un PC con Windows conectado a la misma red que la impresora, en el que instalar la HP MPS Onboarding Tool.

El PC con Windows debe tener acceso a los siguientes endpoints:

Endpoints web para todas las regiones	Dirección	Protocolo	Puerto
https://dopplerservice.msit.hpcloud.hp.com	Saliente	TCP	HTTPS, port 443
https://dopplerservice.msit.hpcloud.hp.com	Saliente	TCP	HTTPS, port 443
https://directory.id.hp.com	Saliente	TCP	HTTPS, port 443
https://coresvcs.dp.smartcloudprint.com	Saliente	TCP	HTTPS, port 443
https://directory.stg.cd.id.hp.com	Saliente	TCP	HTTPS, port 443

Para obtener información detallada sobre la HP MPS Onboarding Tool, consulte la «**HP MPS Onboarding Tool User Guide**» de HP, disponible en el portal de MPS Monitor.





HP Smart Device Agent: para la monitorización de dispositivos HP por USB

El **HP Smart Device Agent (SDA) Local Agent** funciona como agente de recopilación de datos para las impresoras compatibles con HP SDS conectadas a un ordenador mediante un cable USB. Instalado en un PC con Windows al que está conectado el dispositivo físico, el Local Agent recopila datos del dispositivo y funciona con un JAMC instalado en la red.

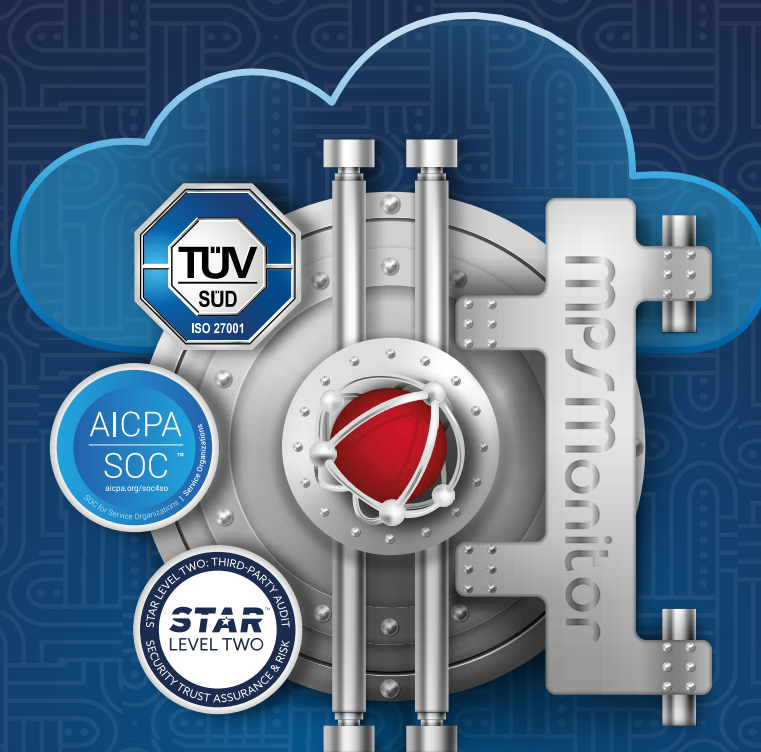
El HP SDA utiliza el puerto 12351 para establecer la comunicación HTTPS con el JetAdvantage Management Connector (JAMC).

Para obtener más detalles sobre el HP Smart Device Agent, consulte la «**HP Smart Device Agent for USB Connected Printers User Guide**», disponible en el portal de MPS Monitor.



6 Documentos de referencia

-  MPS Monitor 2.0 User Guide
-  ISO 27001 Certificate
-  CSA STAR Registry Listing & CSA STAR CAIQ
-  Keypoint Intelligence Security Whitepaper
-  DCA 4 Security Certificate
-  IDC Security Spotlight
-  Impact Networking / DOT Security Cybersecurity testing
-  HP SDS Security Whitepaper
-  HP SDS Cloud DCA Security Whitepaper



***Imprima este documento
solo si es necesario, gracias.***



MPS Monitor lleva varios años apoyando el programa
PrintReleaf, contribuyendo a la reforestación
a nivel mundial.



*MPS Monitor es una marca registrada.
Todas las marcas mostradas pertenecen a sus legítimos propietarios.*





Contacte con nosotros en
info@mpsmonitor.com

Solicite una prueba
www.mpsmonitor.com

*Prepárese para viajar seguro
con nosotros!*

