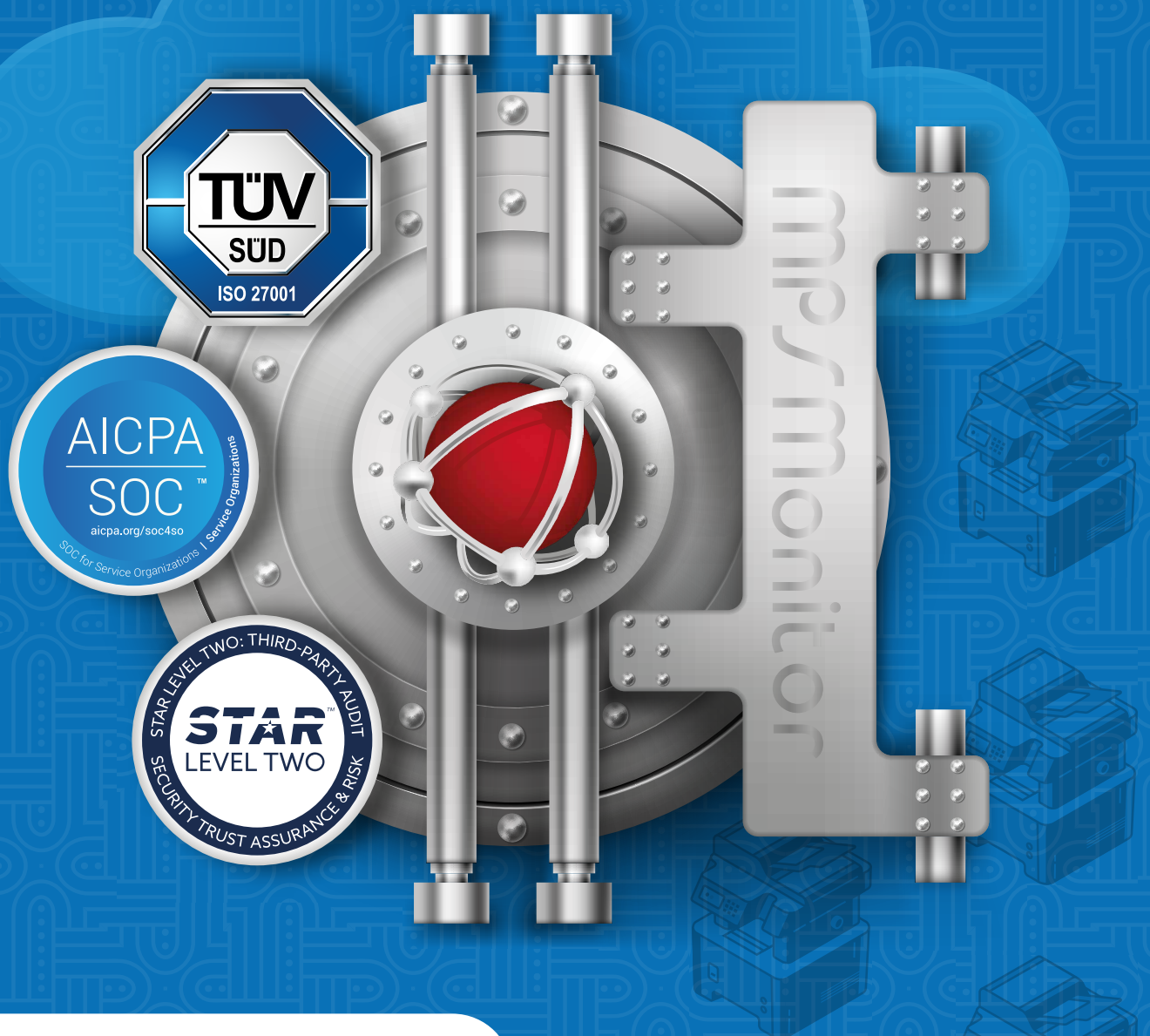


ABSICHERUNG IHRER MANAGED PRINT SERVICES



mpsMonitor
Printer Monitoring in the Cloud

01	Zweck und Aufbau dieses Whitepapers	pag. 03
02	Einführung in MPS Monitor > Ein umfassendes Sicherheitsframework > Einhaltung von Vorschriften und Standards > Datenschutz - Konformität mit der DSGVO	pag. 04
03	Sicherheit der Cloud-Komponente > Software-Integrität > Code-Reviews > Zugriffskontrolle - Benutzerauthentifizierung > Physische Sicherheit und Disaster Recovery	pag. 07
04	Anforderungen und Kommunikationsprotokolle des Data Collection Agent (DCA) > Data Collection Agent Version 4 > Device Web Access > DCA-Anforderungen • Lizenzanforderungen • Hardwareanforderungen • Netzwerkanforderungen • Betriebssystemanforderungen • Windows • MacOS • Linux • Eingebettete DCAs	pag. 10
05	Integration mit HP Smart Device Services (SDS) > Integration mit HP Smart Device Services (SDS) > HP SDS Cloud DCA > Einen Drucker als HP SDS Cloud-Connected einbinden > HP Smart Device Agent - für die Überwachung per USB angebundener HP-Geräte	pag. 18
06	Referenzdokumente	pag. 25

1 Zweck und Aufbau dieses Whitepapers

Dieses **technische Whitepaper** bietet einen Überblick über die SaaS-Plattform MPS Monitor und konzentriert sich auf verschiedene sicherheitsbezogene Aspekte. Die folgenden Abschnitte bieten eine detaillierte Betrachtung von Zertifizierungen, Sicherheitsrichtlinien, Eindämmung von Sicherheitsvorfällen, Software-Integrität und weiteren kritischen Komponenten der Plattform.

Einführung in MPS Monitor

In diesem Abschnitt werden die Kernfunktionen von MPS Monitor mit Schwerpunkt auf einer umfassenden Sicherheitsrichtlinie eingehend behandelt. Die Betrachtung erstreckt sich auf Strategien zum Datenschutz und zur Datensicherheit und schafft so ein solides Fundament für die Plattform.

Sicherheit der Cloud-Komponente

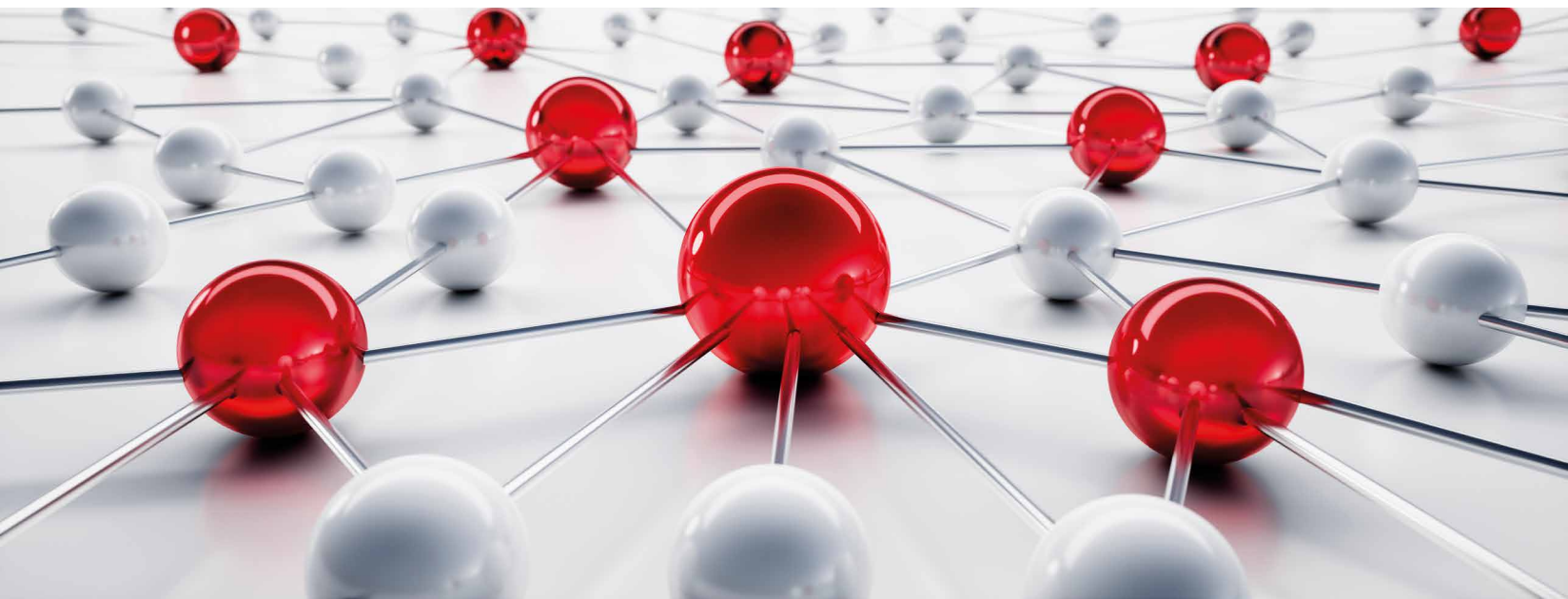
Dieser Abschnitt befasst sich mit der Sicherheitslage innerhalb der Software- und Cloud-Komponenten und legt den Schwerpunkt auf operative Sicherheitsmaßnahmen sowie auf Protokolle im Zusammenhang mit der Benutzerauthentifizierung.

Data Collection Agent (DCA) - netzwerkverbundene Geräte

Hier werden die Feinheiten der Data Collection Agents für netzwerkverbundene Geräte untersucht. Version 4 wird erörtert, mit besonderem Schwerpunkt auf verbesserter Kommunikationssicherheit und -geschwindigkeit. Die Anforderungen an DCAs, einschließlich Lizenz-, Hardware-, Netzwerk- und Betriebssystemspezifikationen, werden umfassend behandelt.

Integration mit HP Smart Device Services (SDS)

Das Whitepaper schließt mit einer Betrachtung der Integrationsmöglichkeiten mit HP Smart Device Services, die Connectors, Cloud-DCAs und Überwachungslösungen für USB-HP-Geräte umfassen.



2 Einführung in MPS Monitor

MPS Monitor bietet eine **herausragende cloudbasierte Software-as-a-Service-Lösung (SaaS), die von Händlern und Managed-Print-Services-Anbietern** weltweit eingesetzt wird. Ihre primäre Aufgabe besteht darin, eine Flotte von Druckgeräten aller wichtigen Druckermarken aufmerksam zu überwachen und zu verwalten.

Dieses Whitepaper legt dar, was MPS Monitor als führenden Anbieter bei der Bereitstellung **außerordentlich sicherer Managed-Print-Services-Lösungen (MPS)** sowohl für Händler als auch für deren anspruchsvolle Kundschaft auszeichnet. Die Plattform verfolgt einen ganzheitlichen Sicherheitsansatz, der von renommierten unabhängigen Drittorganisationen streng geprüft und bestätigt wird. Darüber hinaus wird sie kontinuierlich auditiert, um das Vertrauen in ihre Sicherheitsinfrastruktur und -praktiken dauerhaft zu erhalten und zu stärken.

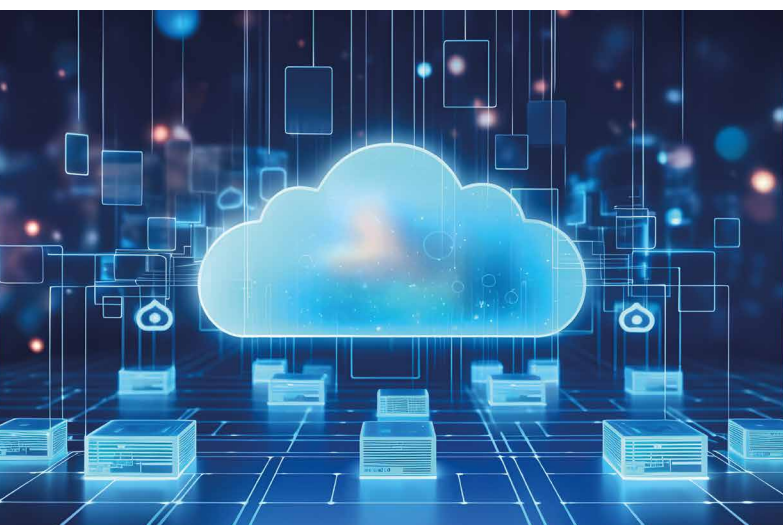
Die Plattform besteht aus zwei Hauptkomponenten:

- 1. Der Data Collection Agent (DCA) Konnektor:** Er wird im Local Area Network (LAN) des Kunden installiert und führt auf Grundlage der Anweisungen der Server-Komponente Operationen auf den Geräten aus. Die vielseitige Bereitstellung umfasst Windows-, Linux- oder macOS-Systeme oder die Integration in einen Multifunktionsdrucker (MFP). Eine cloudbasierte, agentenlose HP-Option (der **HP Cloud DCA**) überwacht und verwaltet HP FutureSmart-Geräte aus der Ferne, ohne dass ein lokaler Agent installiert werden muss.
- 2. Der Cloud-Server und das Web-Portal:** Der Cloud-Server enthält die wertvollen Gerätedaten, die vom DCA bereitgestellt werden. Endnutzer greifen über HTTPS sicher auf ein dediziertes Web-Portal zu und interagieren von jedem Ort und mit jedem Webbrowser mit der Plattform.



Ein umfassendes Sicherheitsframework

MPS Monitor hat ein **Informationssicherheits-Managementsystem (ISMS)** eingerichtet und implementiert, ein marktübliches Sicherheitsframework, das sich auf die wesentlichen Prinzipien der **Vertraulichkeit, Integrität und Verfügbarkeit** konzentriert und mit dem Ziel entwickelt wurde, seine Sicherheitsfunktionen zum Nutzen aller Händler und ihrer Kunden auszuweiten, bei denen die Plattform eingesetzt wird.





“ | *MPS Monitor hat sein Engagement für Sicherheit deutlich unter Beweis gestellt*



Einhaltung von Vorschriften und Standards

MPS Monitor hat sein Engagement für Sicherheit deutlich unter Beweis gestellt, indem das Unternehmen weltweit anerkannte sicherheitsorientierte Prüfungen und Zertifizierungen erfolgreich durchlaufen hat, darunter:



ISO/IEC 27001: steht für einen systematischen Ansatz zur Steuerung von Informationssicherheitsrisiken und gewährleistet maximale Vertraulichkeit, Integrität und Verfügbarkeit der Daten.



System and Organization Controls 2 (SOC 2): Erfüllung der Kriterien des AICPA Service Organization Control 2 Type 2 über einen Zeitraum von einem Jahr durch Überprüfung der Wirksamkeit der Sicherheitskontrollen.



CSA STAR Level 2 Attestation: gewährleistet die Konformität mit der Cloud Controls Matrix (CCM), einem Cybersicherheits-Kontrollframework für Cloud Computing.



Keypoint Intelligence: Zahlreiche Bewertungen bestätigen die Sicherheitsintegrität von MPS Monitor.



Datenschutz - Konformität mit der DSGVO



Jedes Unternehmen mit Kunden in Europa muss die **Datenschutz-Grundverordnung** 2016/679 (DSGVO) einhalten. Druckerhändler und Managed-Print-Service-Anbieter (MPS) bilden hier keine Ausnahme, da die DSGVO auch für die Verwaltung personenbezogener Daten in SaaS-Fernüberwachungssystemen gilt.

Artikel 4.1 der DSGVO definiert klar, was „personenbezogene Daten“ sind, und schließt Namen, Anschriften sowie Online-Kennungen wie eine E-Mail-Adresse, die mit einer physischen Identität in Verbindung steht, ein.



Die Konformität mit der DSGVO ist aus mehreren Gründen auch für amerikanische Kunden wichtig:



Globale Geschäftstätigkeit: Viele Unternehmen agieren global, indem sie entweder Kunden in der Europäischen Union (EU) haben oder personenbezogene Daten von EU-Bürgern verarbeiten. Die Konformität mit der DSGVO ist für jede Organisation, die personenbezogene Daten von EU-Bürgern verarbeitet, unerlässlich, unabhängig davon, wo das Unternehmen ansässig ist.



Kundenvertrauen und Reputation: Der Nachweis der DSGVO-Konformität spiegelt das Engagement für den Schutz der Privatsphäre und der Rechte von Einzelpersonen wider. In einer Zeit, in der Datenschutzverletzungen und Datenschutzbedenken weit verbreitet sind, werden Unternehmen, die dem Datenschutz Priorität einräumen, von Verbrauchern wahrscheinlich positiv wahrgenommen.



Rechtliche und regulatorische Anforderungen: Globale Unternehmen können Tochtergesellschaften, Niederlassungen oder Geschäftsbeziehungen in der EU haben, wodurch die Konformität mit der DSGVO zu einer gesetzlichen Anforderung wird. Nichteinhaltung kann erhebliche Bußgelder und rechtliche Konsequenzen nach sich ziehen.



Best Practices für die Datensicherheit: Die Konformität mit der DSGVO ermutigt Organisationen, robuste Datensicherheitspraktiken zu implementieren. Die Befolgung der DSGVO-Richtlinien steht im Einklang mit allgemeinen Best Practices für Datenschutz und Sicherheit. Selbst wenn dies gesetzlich nicht vorgeschrieben ist, kann die Einführung dieser Maßnahmen Unternehmen dabei helfen, ihre gesamte Cybersicherheitslage zu verbessern.

Zusammenfassend lässt sich sagen, dass die **Konformität mit der DSGVO** nicht ausschließlich ein Anliegen von Unternehmen mit Sitz in der EU ist; sie **hat Auswirkungen auf jede Organisation, die mit personenbezogenen Daten von EU-Bürgern** in Berührung kommt. Global tätige Unternehmen, die diese Aspekte erkennen und berücksichtigen, zeigen ihr Engagement für Datenschutz, rechtliche Verantwortung und globale Datenschutzstandards.



Weitere Einzelheiten dazu, wie MPS Monitor die Konformität mit DSGVO, ISO 27001, SOC 2 Type 2 und CSA STAR Level 2 sicherstellt,

finden Sie unter diesem [link](#)



3 Sicherheit der Cloud-Komponente

Die Backend-Cloud-Infrastruktur von MPS Monitor, die in Rechenzentren von British Telecom in Mailand, Italien, gehostet wird, befindet sich vollständig im Eigentum und in der Verwaltung des Unternehmens selbst. Ein internes Team hochqualifizierter IT- und Sicherheitsexperten überwacht alle vorhandenen Verfahren und Werkzeuge, um sicherzustellen, dass die strengsten Sicherheitsanforderungen erfüllt und die vollständige Konformität mit internationalen Standards stets gewährleistet ist. Zu den vom Unternehmen ergriffenen **Sicherheitsmaßnahmen** gehören:

- ➔ Systemüberwachung rund um die Uhr (24x7) mit einem umfassenden Satz an Werkzeugen zur Infrastruktur- und Anwendungsüberwachung;
- ➔ Umfangreiches Management von Log Analytics;
- ➔ Echtzeit-Alarmierung bei allen wesentlichen sicherheitsrelevanten Ereignissen;
- ➔ Kontinuierliches Vulnerability Assessment und Monitoring aller Assets;
- ➔ Jährliche Penetrationstests, durchgeführt von externen Cybersicherheitsunternehmen;
- ➔ Kontinuierliche Überwachung im Rahmen der jährlichen Assessments nach ISO 27001, SOC 2 Type 2 und CSA STAR Level 2.



Software-Integrität

Die Software von MPS Monitor folgt den Prinzipien „Sicherheit und Datenschutz durch Voreinstellung und durch Technikgestaltung“ (security and data protection by default and by design), indem sie eine große Anzahl von Maßnahmen und Sicherheitskontrollen implementiert, die höchste Sicherheit im Entwicklungs- und Freigabeprozess gewährleisten. Zu den Maßnahmen gehören:

- ➔ Versionskontrolle mithilfe von Versionsverwaltungssoftware;
- ➔ Überwachung der Dateintegrität, um nur autorisierte Änderungen zuzulassen;
- ➔ Getrennte Testumgebungen für Qualitätssicherung und Benutzerakzeptanztests;
- ➔ Digitale Signaturen für alle Komponenten innerhalb eines Release-Pakets;
- ➔ Code-Reviews bei jedem DCA-Code-Release;
- ➔ Sicherheitsaudits und -tests alle sechs Monate, unabhängig durchgeführt von spezialisierten Unternehmen.



Code-Reviews

Ein externes Sicherheitsunternehmen führt **vor jedem DCA-Code-Release** ein **Code-Review** durch. Die Code-Testaktivitäten werden mit einem hybriden Ansatz durchgeführt, der eine Phase der **statischen Codeanalyse** mit einer **dynamischen Anwendungsanalyse** kombiniert. Dieser Ansatz ermöglicht eine hohe Abdeckung der Angriffsfläche und die Aufdeckung sowohl oberflächlicher Schwachstellen als auch von Problemen, die tiefer in der Anwendungslogik liegen und daher nicht sofort erkennbar sind. Alle auf theoretischer Ebene gefundenen Probleme werden anschließend durch die Erstellung von **Proof-of-Concept-Software** (PoC) validiert, wodurch sich der tatsächliche Grad der Ausnutzbarkeit bewerten lässt, aus dem anschließend ein Schweregrad abgeleitet werden kann.

Die Code-Review-Aktivität umfasst auch das **Testen sowohl des Quellcodes als auch der kompilierten Komponenten anhand einer vordefinierten Sicherheits-Checkliste**, die sicherstellt, dass das freizugebende Paket den strengen Sicherheitsanforderungen entspricht, die für die DCA-Komponente festgelegt wurden. Eine neue Version des DCA-Codes kann erst dann an Kunden freigegeben werden, wenn der Code-Review-Prozess die Behebung der Sicherheitsprobleme und die Einhaltung aller Anforderungen formell bestätigt.



Zugriffskontrolle - Benutzerauthentifizierung

Der Zugriff auf das MPS Monitor Portal erfordert Benutzerkonten, die von einem sorgfältig strukturierten System von Benutzerrechten geregelt werden. Dieses System gewährleistet einen präzisen und kontrollierten Zugriff für Benutzer, abgestimmt auf ihre Rollen in der Organisation eines Händlers oder Endkunden.

Auch wenn Passwörter lang und komplex sein müssen, um als stark zu gelten, kann der Faktor Mensch die Wirksamkeit solch strenger Anforderungen häufig untergraben. Zudem erhöht die Notwendigkeit, mehrere Zugangsdatensätze für verschiedene Systeme zu verwalten, den Risikofaktor zusätzlich.

Um diesen Herausforderungen zu begegnen, hat **MPS Monitor zwei bemerkenswerte Funktionen integriert**, um die Sicherheit der Benutzerauthentifizierung zu erhöhen:



Unterstützung für Single-Sign-On-Lösungen (SSO):

MPS Monitor bietet Unterstützung für Single-Sign-On-Lösungen wie **Okta oder Azure AD**. Diese Integration ermöglicht es Benutzern, sich an den besten Passwortpraktiken zu orientieren, die von den Sicherheitsteams ihrer Organisation vorgegeben werden. Durch die Integration von Okta oder Azure AD können sich Benutzer über das Identity-Management-System (IDM) ihrer Organisation authentifizieren und erhalten so sicheren Zugriff auf die Cloud-Plattform von MPS Monitor. Dieser optimierte und vollständig sichere Single-Sign-On-Prozess vereinfacht nicht nur die Benutzererfahrung, sondern erhöht auch die Sicherheit, indem die Abhängigkeit von herkömmlichen Passwörtern für jedes einzelne System verringert wird. Benutzer können auf MPS Monitor zugreifen, ohne sich mehrere komplexe Passwörter merken zu müssen, was zu einem robusteren Sicherheitsökosystem beiträgt.



Unterstützung für Multi-Faktor-Authentifizierung

MPS Monitor räumt dem Schutz Ihrer Daten Priorität ein und setzt dazu robuste Sicherheitsmaßnahmen ein, darunter die Multi-Faktor-Authentifizierung. Benutzer profitieren von einer zusätzlichen Schutzebene für ihre sensiblen Informationen. Diese Funktion stellt sicher, dass der Zugriff auf die Anwendung nur autorisierten Personen gewährt wird, verbessert die allgemeine Sicherheitslage und verschafft den Benutzern ein beruhigendes Gefühl. Bei MPS Monitor ist uns die Bedeutung der Sicherheit Ihrer Daten bewusst, und unser Engagement für den Einsatz modernster Sicherheitsfunktionen wie der Multi-Faktor-Authentifizierung spiegelt dieses Bekenntnis wider.



Physische Sicherheit und Disaster Recovery

Der physische Zugang zum Rechenzentrum, in dem MPS Monitor gehostet wird, ist streng kontrolliert. Die Einrichtung wird von bewaffnetem Sicherheitspersonal geschützt, und alle Gäste müssen stets begleitet werden. Das Zentrum ist mit Videoüberwachung ausgestattet und gegen Brand und Überschwemmung gesichert.

Um die Kontinuität der Cloud-Dienste von MPS Monitor selbst im Falle eines vollständigen Verlusts der Infrastruktur, ob physisch oder digital, zu gewährleisten, ist ein **umfassender Plan zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung** (Disaster Recovery) in Kraft.

Dieser Plan umfasst die folgenden Maßnahmen:



Jährliche Erprobung des Plans anhand einer Reihe potenzieller Bedrohungsszenarien unter Berücksichtigung ihrer Eintrittswahrscheinlichkeit;



Fortlaufende Erprobung des Disaster-Recovery-Systems, um seine Funktionsfähigkeit im Notfall sicherzustellen;



Zusammenarbeit mit einem externen Cybersicherheits-Beratungsunternehmen für eine rasche Reaktion auf jeden Sicherheitsvorfall;



Jährliche Überprüfung der Richtlinien zur Reaktion auf Vorfälle.

4 Anforderungen und Kommunikationsprotokolle des Data Collection Agent (DCA)

Der **Data Collection Agent** (DCA) nutzt das **Simple Network Management Protocol** (SNMP) über **UDP-Port 161**, um nach netzwerkverbundenen MFPs, Kopierern und Druckern zu suchen. Nur Geräte, die die Mindestspezifikationen der Printer MIB v.2 gemäß dem Industriestandard RFC 3805 erfüllen, werden in MPS Monitor aufgenommen, während andere Geräte im Netzwerk vom Datenerfassungsprozess ausgeschlossen werden. Der DCA unterstützt SNMP v1, v2c und v3 des Standard-SNMP-Protokollstapels, wobei SNMP v3 aufgrund der integrierten Verschlüsselung am sichersten ist.

Für die lokale Netzwerkkommunikation zwischen dem DCA und den erfassten Geräten sind die erforderlichen Kommunikationsports wie folgt aufgeführt:

Interne Netzwerkanforderungen des DCA

Zielnetzwerk	Richtung	Protokoll	Port
Intern (Netzwerke mit Geräten) für die Geräteüberwachung (SNMP)	Ausgehend	UDP	UDP 161 (SNMP)
Intern (Netzwerke mit Geräten) für den Device Web Access und HP LFP	Ausgehend	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Intern (Netzwerke mit Geräten) für den Device Web Access und HP LFP	Ausgehend	TCP	TCP 9100 TCP 515 (LPR)



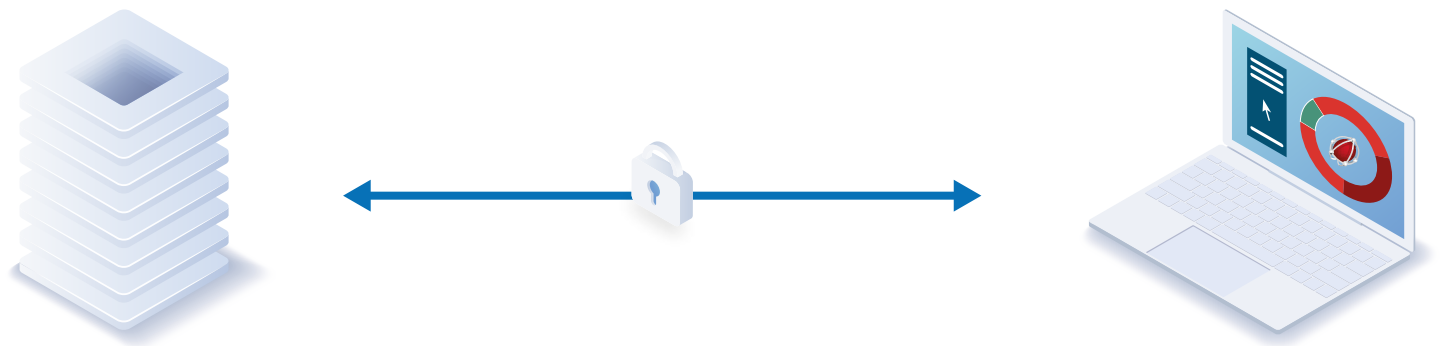


Data Collection Agent Version 4

DCA 4 ist für die Plattformen Windows, macOS und Linux verfügbar und führt **erweiterte Funktionen** ein, wie eine schnellere und sicherere Kommunikation, SNMP-v3-Unterstützung und die Ergänzung um Device Web Access (DWA). DWA ermöglicht es Benutzern der MPS Monitor Console, die Seiten des eingebetteten Webservers jedes Kundendruckers aufzurufen.

Verbesserte Kommunikationssicherheit und -geschwindigkeit

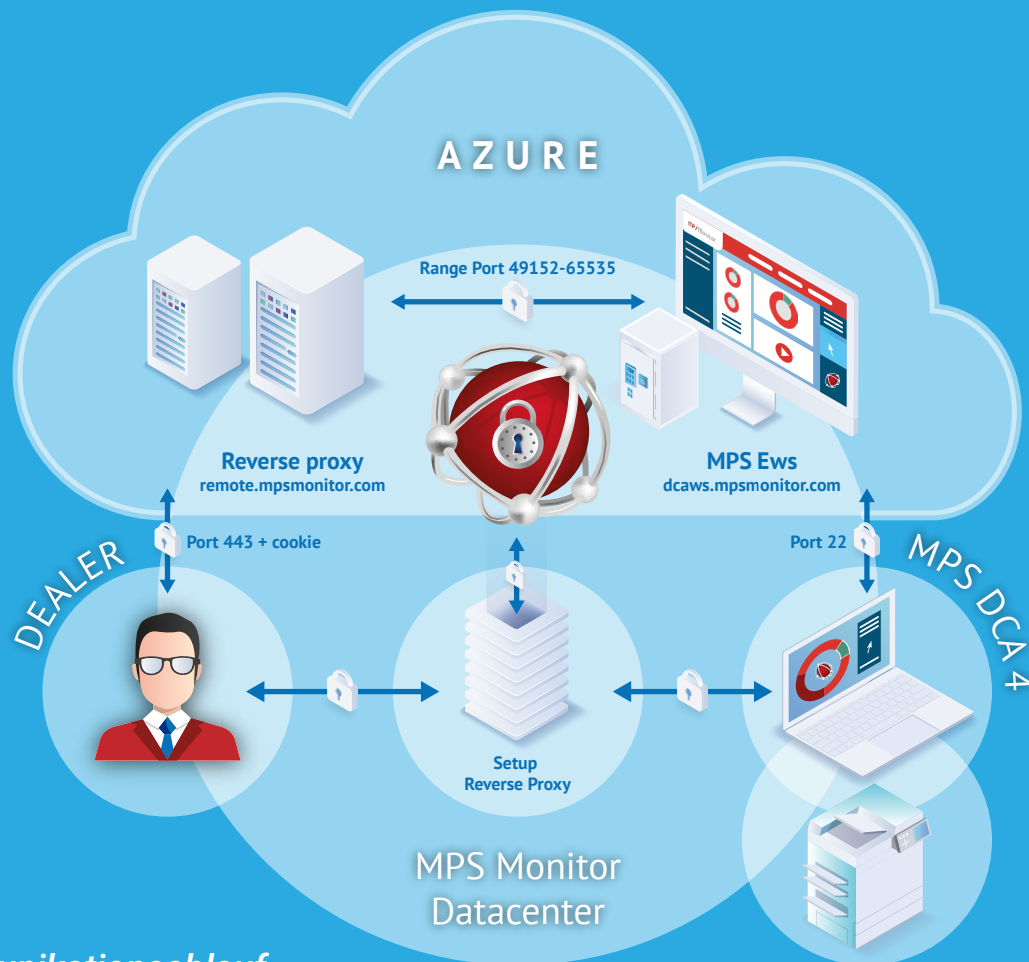
DCA 4 verbessert die Sicherheit und die Datenverkehrsoptimierung durch die Verwendung von HTTPS2/GRPC über Port 443. Darüber hinaus integriert DCA 4 MQTT, ein schlankes IoT-Kommunikationsprotokoll, und nutzt Azure IoT Hub als Message Broker. Dies steigert die Geschwindigkeit der Kommunikation zwischen dem DCA und den Geräten im lokalen Netzwerk sowie dem MPS Monitor Cloud-Dienst erheblich.



Device Web Access

Der **Device Web Access** (DWA) von DCA 4 ist eine robuste Funktion, die durch verschiedene Maßnahmen abgesichert ist, um einen eingeschränkten und sicheren HTTP-Zugriff auf Drucker zu gewährleisten:

- ➔ Der Zugriff ist auf Geräte beschränkt, die einem bestimmten Händler gehören;
- ➔ Die obligatorische Zwei-Faktor-Authentifizierung oder die Active-Directory-Integration stellt sicher, dass nur autorisierte Benutzer die DWA-Funktion nutzen können;
- ➔ Das DWA-System wird auf MS Azure gehostet, wodurch temporäre Firewall-Ausnahmen für den Zugriff auf den Dienst ermöglicht werden, die nach jeder Sitzung gelöscht werden;
- ➔ Bei jeder Verbindung wird eine Überprüfung der Attribute des Zielgeräts durchgeführt, um den Zugriff auf ungültige Geräte zu verhindern;
- ➔ Für jede Nutzung werden Zugriffsprotokolle erzeugt;
- ➔ Dateiübertragungen über DWA sind deaktiviert.



DWA-Kommunikationsablauf



DCA-Anforderungen

Lizenzanforderungen

Für die Installation von MPS Monitor sind keine zusätzlichen Lizenzen erforderlich.

Hardwareanforderungen

Empfohlene Hardware für den Rechner, der den DCA hostet:

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

Der PC muss nicht dediziert sein und kann gleichzeitig für andere Zwecke verwendet werden. Der DCA-Konnektor arbeitet im Hintergrund, ohne die PC-Benutzer zu beeinträchtigen. Für große Netzwerke mit hohen Scan-Anforderungen wird bessere Hardware empfohlen, um die Leistung zu verbessern.

Netzwerkanforderungen - DCA 4

Das System, auf dem DCA 4 installiert ist, muss dauerhaften Zugriff auf die folgenden Endpunkte und Protokolle haben:

EU STACK (portal.mpsmonitor.com)

Web-Endpunkte für die Regionen EMEA und APAC	Protokoll	Ports	CDN-Eintrag / IP-Adresse
https://dca4.mpsmonitor.com <i>für die Kommunikation zur Geräteüberwachung</i>	HTTP2, GRPC	443	213.92.56.75
https://cdn2.mpsmonitor.com <i>für DCA-Updates</i>	HTTP	443	Azure CDN
dcaws.mpsmonitor.com <i>für den Device Web Access</i>	SSH	22	13.80.42.210
eu01-broker-mpsmonitor.azure-devices.net <i>für die MQTT-Kommunikation des DCA</i>	MQTT over WSS	443	Azure IOT HUB

Web-Endpunkte für die Region Americas	Protokoll	Ports	CDN-Eintrag / IP-Adresse
https://us01-dca.mpsmonitor.com <i>für die Kommunikation zur Geräteüberwachung</i>	HTTP2, GRPC	443	20.106.185.115
https://cdn2.mpsmonitor.com <i>für DCA-Updates</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>für die anfänglichen Download-Setups</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.com <i>für den Device Web Access</i>	SSH	22	20.55.38.55
us01-broker-mpsmonitor.azure-devices.net <i>für die MQTT-Kommunikation des DCA</i>	MQTT over WSS	443	Azure IOT HUB

US STACK (portal.mpsmonitor.us)

Web-Endpunkte für die Region Americas	Protokoll	Ports	CDN-Eintrag / IP-Adresse
https://us01-dca4.mpsmonitor.us <i>für die Kommunikation zur Geräteüberwachung</i>	HTTP2, GRPC	443	20.81.25.170
https://cdn2.mpsmonitor.com <i>für DCA-Updates</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>für die anfänglichen Download-Setups des DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.us <i>für den Device Web Access</i>	SSH	22	104.211.20.116
us01-brk-prd-eus-iothub-01.azure-devices.net <i>für die MQTT-Kommunikation des DCA</i>	MQTT over WSS	443	Azure IOT HUB

**Betriebssystemanforderungen****Windows**

DCA 4 wird **für Clients ab der Version Windows 10 64-Bit Build 1607 (E)** und **für Serverinstallationen ab Windows Server 2016 64-Bit** unterstützt.

Das Setup von DCA 4 überprüft die Installation der .NET Core-Bibliotheken und lädt die erforderlichen Bibliotheken von der Microsoft-Website herunter.

DCA 4 installiert zwei Dienste, **MpsMonitor.Dca.Client** und **MpsMonitor.Dca.Monitor**, die jeweils die Systemkonten Network User bzw. Local User verwenden.

Falls besondere Einschränkungen oder Richtlinien bestehen, die die Aktivierung oder Ausführung der Dienste durch die oben genannten Konten verhindern, muss stattdessen ein spezifischer lokaler Benutzer verwendet werden.

Das DCA-Installationsverfahren weist diesem Benutzer die zur Ausführung des Dienstes erforderlichen Mindestrechte zu.

MacOS

DCA 4 kann ab **macOS 12 (Monterey)** installiert werden und lässt sich auf Intel- oder Arm-CPU's (M1, M2) installieren.

Linux und Raspberry

DCA 4 kann auf **Linux-Distributionen installiert werden, die .NET Core unterstützen.**
 Er kann installiert werden auf:

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

Für den Raspberry ist die Mindestanforderung ein Raspberry Pi 3 oder höher mit Bookworm (Arm 32-Bit oder Arm 64-Bit).

Eingebettete DCAs

Die eingebettete Version des DCA kann bei einigen Geräten bestimmter Hersteller direkt installiert werden, gemäß den Anforderungen und Anweisungen in den jeweiligen Installationsanleitungen.

Die unterstützten Geräte und ihre jeweiligen Endpunkte sind:

HP FutureSmart 3.5, 4, 5 (nur Plattform „L1 Classic“)

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
http://embeddedhp.mpsmonitor.com	Ausgehend	TCP	HTTP, port 80
http://embeddedfileshp.mpsmonitor.com	Ausgehend	TCP	HTTP, port 80

Samsung (mit XOA-Firmware 1.21+)

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
http://embedded.abassetmanagement.com	Ausgehend	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Ausgehend	TCP	HTTP, port 80

Kyocera HyPAS

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
http://embedded.abassetmanagement.com	Ausgehend	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Ausgehend	TCP	HTTP, port 80



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

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
http://embeddedlexmark.mpsmonitor.com	Ausgehend	TCP	HTTP, port 80
http://embeddedfileslexmark.mpsmonitor.com	Ausgehend	TCP	HTTP, port 80



5 Integration mit HP Smart Device Services (SDS)

Die Integration von MPS Monitor mit **HP Smart Device Services (SDS)** bietet eine nahtlose und effiziente Lösung zur Überwachung und Verwaltung von HP Druckgeräten. Durch die Nutzung der Fähigkeiten von MPS Monitor zusammen mit den fortschrittlichen Funktionen von HP SDS können Organisationen umfassende Einblicke in ihre Flotte von HP Druckern gewinnen. Diese Integration erleichtert die proaktive Wartung, die Echtzeitüberwachung und ein präzises Reporting und optimiert so die Gesamtleistung der Druckinfrastruktur.

Mit der kombinierten Leistungsfähigkeit von MPS Monitor und HP SDS können Unternehmen ihre **Produktivität steigern, Betriebskosten senken und das reibungslose Funktionieren ihres Druck-Ökosystems sicherstellen.**

Eine vollständige Liste kompatibler Geräte und verfügbarer Funktionen ist unter diesem [link](#) verfügbar



HP JetAdvantage Management Connector (JAMC)

Die **JAMC-Software**, ein von HP entwickelter DCA, ermöglicht die Ausführung von SDS-Funktionen in einer Windows-Installation. Die MPS Monitor Windows-DCAs sind vollständig in diese Technologie integriert und ermöglichen die Nutzung der SDS-Funktionen direkt aus dem MPS Monitor Portal.

Netzwerkkommunikationsanforderungen für die JAMC-Geräteüberwachung - interne Netzwerkanforderung für HP JAMC

Interne Netzwerkanforderungen für HP JAMC

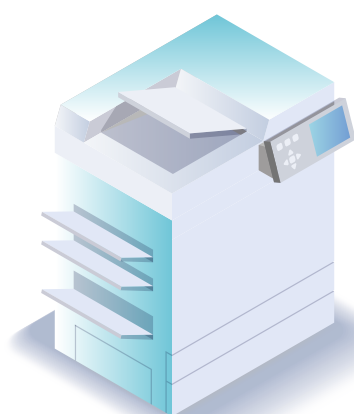
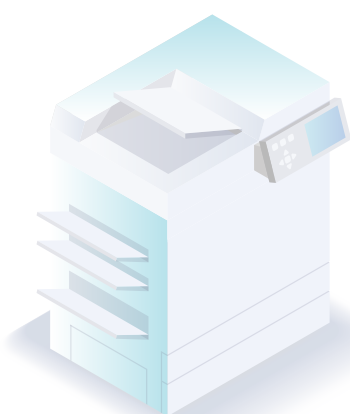
Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
Intern (Netzwerke mit Geräten) für die JAMC-Geräteüberwachung	Ausgehend	UDP	161, 427, 3702
Intern (Netzwerke mit Geräten) für die JAMC-Geräteüberwachung	Ausgehend	TCP	443, 3910, 3911, 7627, 8080



JAMC ist direkt mit der HP SDS Cloud-Infrastruktur verbunden, und die folgende Tabelle führt alle erforderlichen Kommunikationsports auf:

Web-Endpunkte für die Region Americas	Richtung	Protokoll	Port
https://jamanagement.hp.com	Ausgehend	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTPS, port 443
https://ews.hpjamservices.com	Ausgehend	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Ausgehend	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Ausgehend	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Ausgehend	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Ausgehend	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Ausgehend	TCP	HTTP, port 80

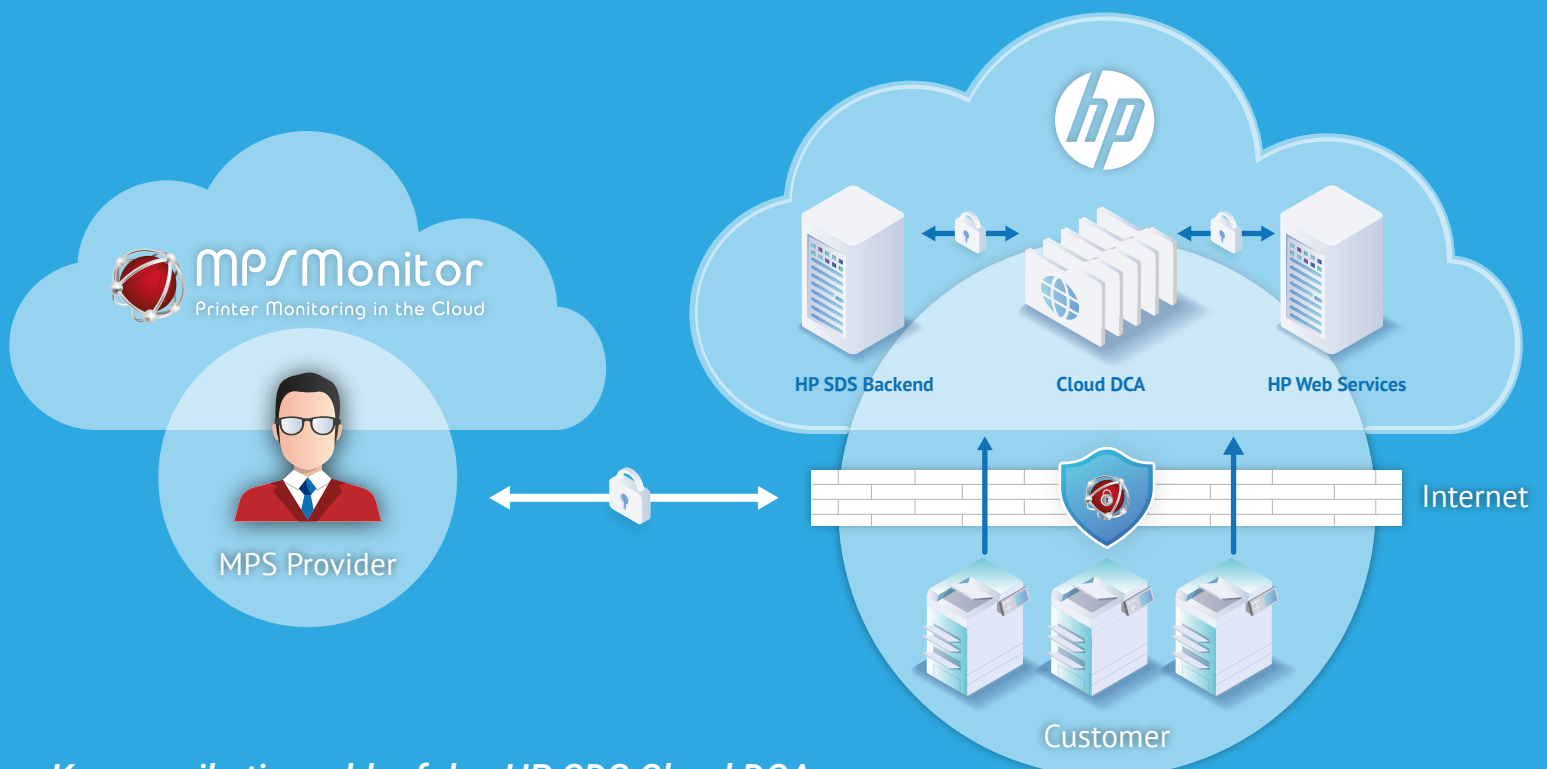
Web-Endpunkte für die Regionen EMEA und APAC	Richtung	Protokoll	Port
https://eu.jamanagerment.hp.com	Ausgehend	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTPS, port 443
https://eu.ews.hpjamservices.com	Ausgehend	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Ausgehend	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	Ausgehend	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	Ausgehend	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Ausgehend	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	Ausgehend	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	Ausgehend	TCP	HTTP, port 80





HP SDS Cloud

Der **HP Smart Device Services Cloud DCA** ermöglicht es MPS Monitor, HP FutureSmart-Geräte aus der Ferne zu überwachen und zu steuern, ohne dass eine DCA-Installation im Netzwerk erforderlich ist.



Kommunikationsablauf des HP SDS Cloud DCA

Kommunikation mit dem HP SDS Cloud DCA

Der HP SDS Cloud DCA ist für HP SDS-kompatible Geräte mit **HP FutureSmart Version 4.9.0.1** oder höher verfügbar.

Unterstützte Geräte müssen über eine stabile Verbindung zu den folgenden Web-Endpunkten verfügen:

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
https://*.avatar.ext.hp.com:443	Ausgehend	TCP	HTTPS, port 443
http://*.avatar.ext.hp.com:80	Ausgehend	TCP	HTTP, port 80
udp://*.avatar.ext.hp.com:9930	Ausgehend	UDP	UDP, port 9930
wss://*.avatar.ext.hp.com:443	Ausgehend	TCP	WSS, port 443
https://*.hpjamservices.com:443	Ausgehend	TCP	HTTPS, port 443
https://*.smartcloudprint.com:443	Ausgehend	TCP	HTTPS, port 443





Einen Drucker als HP SDS Cloud-Connected einbinden

Um den **HP SDS Cloud DCA** nutzen zu können, muss ein Drucker in die **HP SDS Cloud** eingebunden werden. Für die Durchführung dieses Vorgangs sind die folgenden Voraussetzungen erforderlich:



Der Drucker muss mit dem Internet verbunden sein;

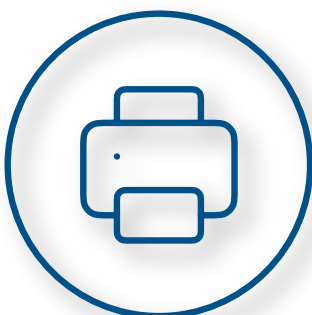


Ein Windows-PC, der mit demselben Netzwerk wie der Drucker verbunden ist und auf dem das HP MPS Onboarding Tool installiert wird;

Der Windows-PC muss auf die folgenden Endpunkte zugreifen können:

Web-Endpunkte für alle Regionen	Richtung	Protokoll	Port
https://dopplerservice.msit.hpcloud.hp.com	Ausgehend	TCP	HTTPS, port 443
https://dopplerservice.msit.hpcloud.hp.com	Ausgehend	TCP	HTTPS, port 443
https://directory.id.hp.com	Ausgehend	TCP	HTTPS, port 443
https://coresvcs.dp.smartcloudprint.com	Ausgehend	TCP	HTTPS, port 443
https://directory.stg.cd.id.hp.com	Ausgehend	TCP	HTTPS, port 443

Ausführliche Informationen zum HP MPS Onboarding Tool finden Sie im „**HP MPS Onboarding Tool User Guide**“ von HP, der im MPS Monitor Portal verfügbar ist.





HP Smart Device Agent - für die Überwachung per USB angebundener HP-Geräte

Der **HP Smart Device Agent (SDA) Local Agent** fungiert als Data Collection Agent für HP SDS-unterstützte Drucker, die über ein USB-Kabel mit einem Computer verbunden sind. Der Local Agent wird auf einem Windows-PC installiert, an den das physische Gerät angeschlossen ist, erfasst Daten vom Gerät und arbeitet mit einem im Netzwerk installierten JAMC zusammen.

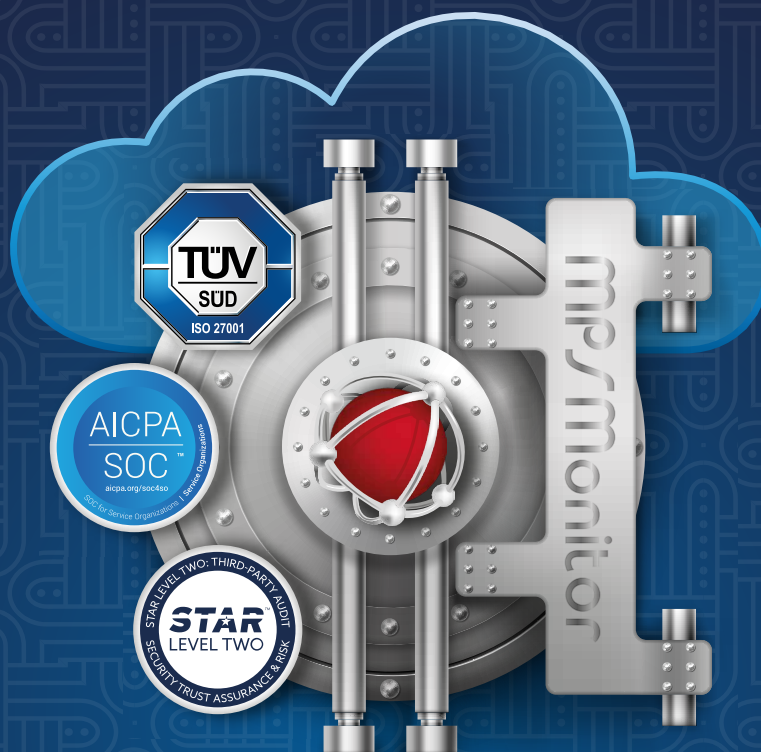
Der HP SDA nutzt Port 12351, um eine HTTPS-Kommunikation mit dem JetAdvantage Management Connector (JAMC) herzustellen.

Weitere Einzelheiten zum HP Smart Device Agent finden Sie im „**HP Smart Device Agent for USB Connected Printers User Guide**“, der im MPS Monitor Portal verfügbar ist.



6 Referenzdokumente

-  MPS Monitor 2.0 User Guide
-  ISO27001 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



***Bitte drucken Sie dieses Dokument nur,
wenn es notwendig ist. Vielen Dank.***



MPS Monitor unterstützt seit mehreren Jahren
das PrintReleaf-Programm und trägt so weltweit
zur Wiederaufforstung bei.



*MPS Monitor ist eine eingetragene Marke.
Alle gezeigten Marken gehören ihren rechtmäßigen Eigentümern.*





Kontaktieren Sie uns unter
info@mpsmonitor.com

Fordern Sie eine Testversion unter
www.mpsmonitor.com an

*Machen Sie sich bereit
für Ihre sichere Reise mit uns!*

