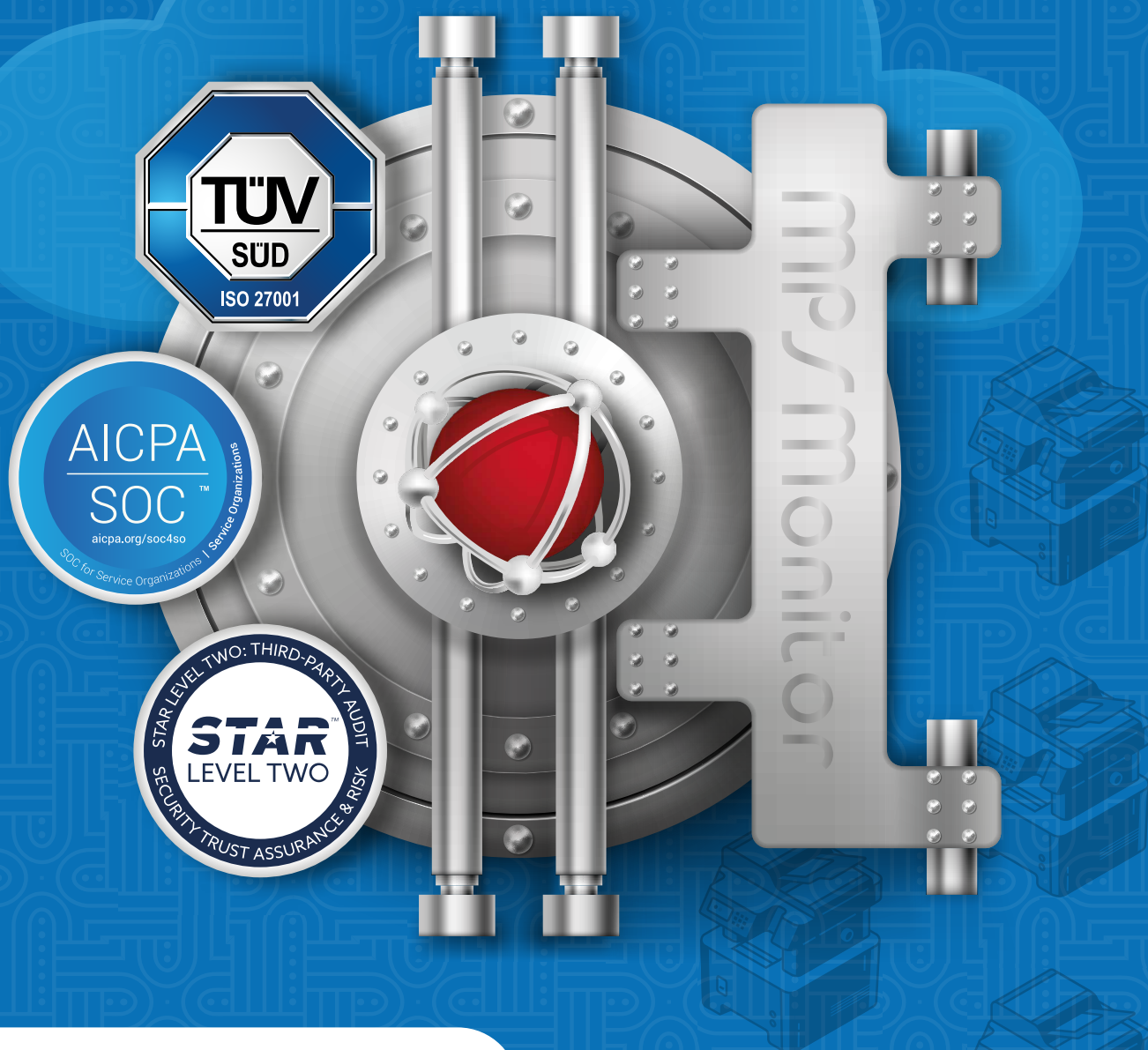


SÉCURISER VOS MANAGED PRINT SERVICES



mpsMonitor
Printer Monitoring in the Cloud

01	Objet et structure de ce whitepaper	pag. 03
-----------	--	----------------

02	Introduction à MPS Monitor	pag. 04
	> Un cadre de sécurité complet	
	> Conformité aux réglementations et aux normes	
	> Protection des données, conformité au RGPD	

03	Sécurité des composants cloud	pag. 07
	> Intégrité logicielle	
	> Revues de code	
	> Contrôle d'accès, authentification des utilisateurs	
	> Sécurité physique et reprise après sinistre	

04	Prérequis et protocoles de communication du Data Collection Agent (DCA)	pag. 10
	> Data Collection Agent version 4	
	> Device Web Access	
	> Prérequis du DCA	
	• Prérequis de licence	
	• Prérequis matériels	
	• Prérequis réseau	
	• Prérequis du système d'exploitation	
	• Windows	
	• macOS	
	• Linux	
	• DCA embarqués	

05	Intégration avec HP Smart Device Services (SDS)	pag. 18
	> Intégration avec HP Smart Device Services (SDS)	
	> HP SDS Cloud DCA	
	> Enrôler une imprimante en tant que périphérique HP SDS connecté au cloud	
	> HP Smart Device Agent, pour la surveillance des périphériques HP connectés en USB	

06	Documents de référence	pag. 25
-----------	-------------------------------	----------------

1 Objet et structure de ce whitepaper

Ce **whitepaper technique** offre une vue d'ensemble de la plateforme SaaS MPS Monitor, en se concentrant sur différents aspects liés à la sécurité. Les sections suivantes proposent un examen détaillé des certifications, des politiques de sécurité, de l'atténuation des incidents, de l'intégrité logicielle et d'autres composants essentiels de la plateforme.

Introduction à MPS Monitor

Dans cette section, nous approfondissons les fonctionnalités centrales de MPS Monitor, en mettant l'accent sur une politique de sécurité complète. La discussion s'étend aux stratégies de protection et de sécurité des données, garantissant une base solide pour la plateforme.

Sécurité des composants cloud

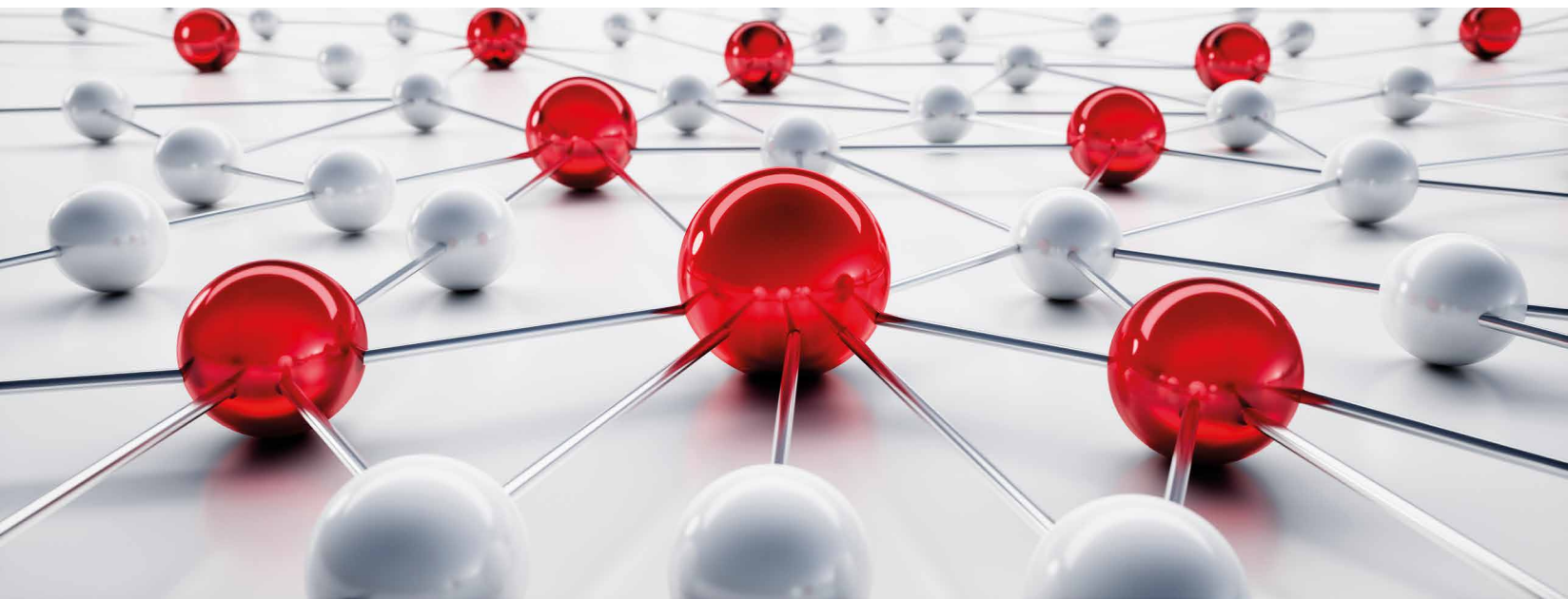
Ce segment traite du paysage de la sécurité au sein des composants logiciels et cloud, en mettant l'accent sur les mesures de sécurité opérationnelle et sur les protocoles liés à l'authentification des utilisateurs.

Data Collection Agent (DCA), périphériques connectés au réseau

Nous explorons ici les subtilités des Data Collection Agents pour les périphériques connectés au réseau. La version 4 est présentée, avec un accent particulier sur l'amélioration de la sécurité et de la rapidité des communications. Les prérequis des DCA, notamment les spécifications de licence, matérielles, réseau et de système d'exploitation, sont traités de manière exhaustive.

Intégration avec HP Smart Device Services (SDS)

Le whitepaper se conclut par une exploration des capacités d'intégration avec HP Smart Device Services, englobant les connecteurs, les DCA cloud et les solutions de surveillance des périphériques HP connectés en USB.



2 Introduction à MPS Monitor

MPS Monitor propose une **solution SaaS (Software as a Service) basée sur le cloud de premier plan, déployée par les revendeurs et les prestataires de Managed Print Services** dans le monde entier. Sa mission première est de superviser et d'administrer avec vigilance un parc de périphériques d'impression fabriqués par toutes les principales marques d'imprimantes.

Ce whitepaper décrit ce qui distingue MPS Monitor en tant que leader de référence dans la fourniture de **solutions de Managed Print Services (MPS) exceptionnellement sécurisées**, tant pour les revendeurs que pour leur clientèle exigeante. La plateforme adopte une approche globale de la sécurité, rigoureusement examinée et validée par des organismes tiers indépendants et réputés. De plus, elle fait l'objet d'audits continus visant à entretenir et à renforcer la confiance dans son infrastructure et ses pratiques de sécurité.

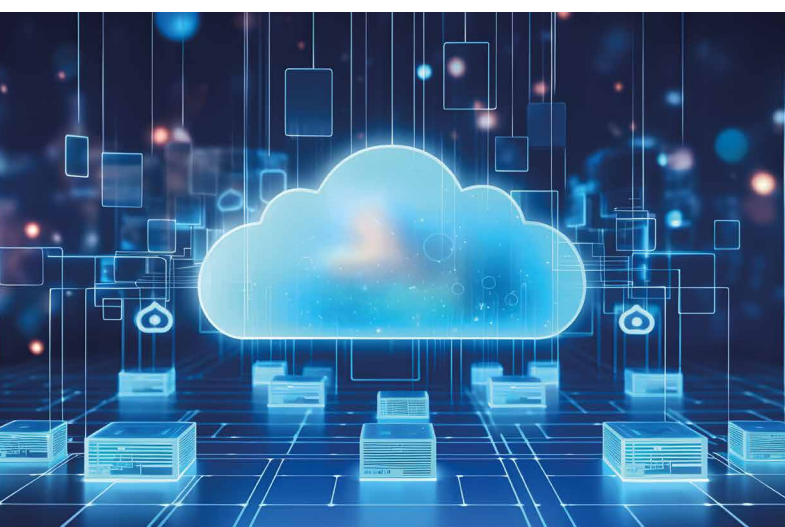
La plateforme se compose de deux composants principaux:

- 1. Le connecteur Data Collection Agent (DCA):** installé au sein du réseau local (LAN) du client, il exécute des opérations sur les périphériques d'après les directives du composant Serveur. Son déploiement polyvalent inclut les systèmes Windows, Linux ou macOS, ou l'intégration dans une imprimante multifonction (MFP). Une option HP sans DCA, basée sur le cloud (le **HP Cloud DCA**), surveille et gère à distance les périphériques HP FutureSmart sans installer aucun Agent sur site.
- 2. Le serveur cloud et le portail web:** le serveur cloud héberge de précieuses données sur les périphériques fournies par le DCA. Les utilisateurs finaux accèdent à un portail web dédié de manière sécurisée via HTTPS, en interagissant avec la plateforme depuis n'importe quel emplacement et à l'aide de n'importe quel navigateur web.



Un cadre de sécurité complet

MPS Monitor a établi et mis en œuvre un **système de management de la sécurité de l'information (ISMS)**, un cadre de sécurité standard du marché qui se concentre sur les principes essentiels de **Confidentialité**, d'**Intégrité** et de **Disponibilité**, conçu dans le but d'étendre ses fonctionnalités de sécurité au bénéfice de tous les revendeurs et de leurs clients là où la plateforme est utilisée.





“ *MPS Monitor a manifestement démontré son engagement en faveur de la sécurité*



Conformité aux réglementations et aux normes

MPS Monitor a manifestement démontré son engagement en faveur de la sécurité en franchissant avec succès des évaluations et certifications axées sur la sécurité et reconnues au niveau mondial, notamment:



ISO/IEC 27001: témoignant d'une approche systématique de la gestion des risques liés à la sécurité de l'information, garantissant une Confidentialité, une Intégrité et une Disponibilité maximales des données.



System and Organization Controls 2 (SOC 2): atteinte de la conformité aux critères AICPA Service Organization Control 2 Type 2 sur une période d'un an, ce qui atteste l'efficacité des contrôles de sécurité.



Attestation CSA STAR Level 2: garantie de la conformité à la Cloud Controls Matrix (CCM), un cadre de contrôles de cybersécurité pour le cloud computing.



Keypoint Intelligence: de nombreuses évaluations corroborent l'intégrité de la sécurité de MPS Monitor.

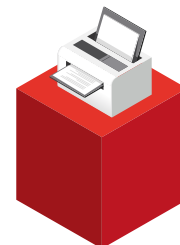


Protection des données, conformité au RGPD



Toute entreprise ayant des clients en Europe doit se conformer au **Règlement général sur la protection des données** 2016/679 (RGPD). Les revendeurs d'imprimantes et les prestataires de Managed Print Services (MPS) ne font pas exception, car le RGPD s'applique également à la gestion des données personnelles au sein des systèmes SaaS de surveillance à distance.

L'article 4.1 du RGPD définit clairement les « données à caractère personnel » et inclut les noms, les adresses postales et les identifiants en ligne tels qu'une adresse e-mail liée à une personne physique.



La conformité au RGPD est également importante pour les clients américains, et ce pour plusieurs raisons:



Activités commerciales mondiales: de nombreuses entreprises opèrent à l'échelle mondiale, soit en ayant des clients dans l'Union européenne (UE), soit en traitant les données personnelles de citoyens de l'UE. La conformité au RGPD est essentielle pour toute organisation qui traite les données personnelles de résidents de l'UE, quel que soit le lieu d'implantation de l'entreprise.



Confiance et réputation auprès des clients: démontrer la conformité au RGPD reflète un engagement à protéger la vie privée et les droits des personnes. À une époque où les violations de données et les préoccupations relatives à la vie privée sont fréquentes, les entreprises qui privilégient la protection des données sont susceptibles d'être perçues favorablement par les consommateurs.



Exigences légales et réglementaires: les entreprises mondiales peuvent avoir des filiales, des succursales ou des relations commerciales dans l'UE, ce qui fait de la conformité au RGPD une exigence légale. Le non-respect peut entraîner des amendes substantielles et des conséquences juridiques.



Bonnes pratiques de sécurité des données : la conformité au RGPD encourage les organisations à mettre en œuvre des pratiques robustes de sécurité des données. Le respect des lignes directrices du RGPD s'aligne sur les bonnes pratiques générales de protection et de sécurité des données. Même lorsqu'elles ne sont pas légalement requises, ces mesures peuvent aider les entreprises à améliorer leur posture globale de cybersécurité.

En résumé, la **conformité au RGPD** ne concerne pas uniquement les entreprises basées dans l'UE ; elle **a des implications pour toute organisation qui interagit avec les données personnelles de citoyens de l'UE**. Les entreprises mondiales qui reconnaissent et prennent en compte ces considérations démontrent un engagement envers la vie privée, la responsabilité juridique et les normes mondiales de protection des données.



Pour plus de détails sur la manière dont MPS Monitor assure la conformité au RGPD, à l'ISO 27001, au SOC 2 Type 2 et au CSA STAR Level 2,

consultez ce [lien](#)



3 Sécurité des composants cloud

L'infrastructure cloud backend de MPS Monitor, hébergée au sein des centres de données de British Telecom à Milan, en Italie, est sous la propriété et l'administration complètes de l'entreprise elle-même. Une équipe interne de professionnels de l'informatique et de la sécurité hautement qualifiés supervise l'ensemble des procédures et des outils en place afin de garantir que les exigences de sécurité les plus strictes sont satisfaites et qu'une pleine conformité aux normes internationales est toujours assurée. Les **mesures de sécurité** adoptées par l'entreprise comprennent:

-  Une surveillance des systèmes 24 h/24 et 7 j/7 à l'aide d'un ensemble complet d'outils de surveillance de l'infrastructure et des applications;
-  Une gestion approfondie de l'analyse des journaux (Log Analytics);
-  Des alertes en temps réel sur tous les principaux événements liés à la sécurité;
-  Une évaluation et une surveillance continues des vulnérabilités sur tous les actifs;
-  Des tests d'intrusion annuels réalisés par des sociétés externes de cybersécurité;
-  Une surveillance continue dans le cadre des évaluations annuelles ISO 27001, SOC 2 Type 2 et CSA STAR Level 2.



Intégrité logicielle

Le logiciel de MPS Monitor adhère aux principes de « sécurité et protection des données par défaut et dès la conception », en mettant en œuvre un grand nombre de mesures et de contrôles de sécurité qui garantissent la plus grande sécurité dans le processus de développement et de publication. Ces mesures comprennent:

-  La gestion des versions à l'aide d'un logiciel de gestion de versions;
-  La surveillance de l'intégrité des fichiers pour n'autoriser que les modifications autorisées;
-  Des environnements de test distincts pour l'assurance qualité et les tests d'acceptation par les utilisateurs;
-  Des signatures numériques pour tous les composants au sein d'un package de publication;
-  Des revues de code à chaque publication du code du DCA;
-  Un audit et des tests de sécurité tous les six mois, réalisés de manière indépendante par des sociétés spécialisées.



Revue de code

Une société de sécurité externe réalise une **revue de code avant chaque publication du code du DCA**. Les activités de test du code sont effectuées en adoptant une approche hybride qui combine une phase d'**analyse statique du code** avec une **analyse dynamique de l'application**. Cette approche permet d'assurer une couverture étendue de la surface d'attaque et de découvrir aussi bien les vulnérabilités superficielles que les problèmes qui résident plus profondément dans la logique applicative et qui ne sont donc pas immédiatement identifiables. Tous les problèmes détectés sur le plan théorique sont ensuite validés par la création de logiciels **Proof of Concept** (PoC), ce qui permet d'évaluer le niveau réel d'exploitabilité à partir duquel un score de gravité peut ensuite être attribué.

L'activité de revue de code comprend également le **test du code source et des composants compilés au regard d'une checklist de sécurité prédéfinie** qui garantit que le package en cours de publication respecte les exigences de sécurité strictes définies pour le composant DCA.

Une nouvelle version du code du DCA ne peut être publiée auprès des clients que lorsque le processus de revue de code certifie formellement la résolution des problèmes de sécurité et la conformité à toutes les exigences.



Contrôle d'accès, authentification des utilisateurs

L'accès au portail MPS Monitor requiert des comptes utilisateurs, régis par un système méticuleusement structuré de privilèges utilisateurs. Ce système garantit un accès précis et contrôlé pour les utilisateurs, en cohérence avec leurs rôles au sein d'une organisation revendeuse ou d'un client final.

S'il est impératif que les mots de passe soient longs et complexes pour être considérés comme robustes, le facteur humain peut souvent compromettre l'efficacité de telles exigences strictes. De plus, la nécessité de conserver plusieurs jeux d'identifiants pour différents systèmes accroît encore le facteur de risque.

Pour relever ces défis, **MPS Monitor a intégré deux fonctionnalités notables** afin de renforcer la sécurité de l'authentification des utilisateurs:



Prise en charge des solutions de Single Sign-On (SSO):

MPS Monitor offre une prise en charge des solutions de Single Sign-On, telles qu'**Okta ou Azure AD**. Cette intégration permet aux utilisateurs de s'aligner sur les bonnes pratiques en matière de mots de passe préconisées par les équipes de sécurité de leur organisation. Grâce à l'intégration d'Okta ou d'Azure AD, les utilisateurs peuvent s'authentifier via le système Identity Management (IDM) de l'organisation, obtenant ainsi un accès sécurisé à la plateforme cloud MPS Monitor. Ce processus de Single Sign-On rationalisé et entièrement sécurisé simplifie non seulement l'expérience utilisateur, mais renforce également la sécurité en réduisant la dépendance aux mots de passe traditionnels pour chaque système spécifique. Les utilisateurs peuvent accéder à MPS Monitor sans avoir besoin de mémoriser de multiples mots de passe complexes, contribuant ainsi à un écosystème de sécurité plus robuste.



Prise en charge de l'authentification multifacteur

MPS Monitor accorde la priorité à la protection de vos données grâce à la mise en œuvre de mesures de sécurité robustes, dont l'authentification multifacteur. Les utilisateurs peuvent bénéficier d'une couche de protection supplémentaire pour leurs informations sensibles. Cette fonctionnalité garantit que l'accès à l'application n'est accordé qu'aux personnes autorisées, renforçant la posture de sécurité globale et offrant une tranquillité d'esprit aux utilisateurs. Chez MPS Monitor, nous comprenons l'importance d'assurer la sécurité de vos données, et notre recours à des fonctionnalités de sécurité de pointe telles que l'authentification multifacteur reflète cet engagement.



Sécurité physique et reprise après sinistre

L'accès physique au centre de données où MPS Monitor est hébergé est strictement contrôlé. Le site est protégé par du personnel de sécurité armé, et tous les visiteurs doivent être accompagnés en permanence. Le centre est équipé d'une vidéosurveillance et protégé contre l'incendie et les inondations.

Afin d'assurer la continuité des services cloud de MPS Monitor, même en cas de perte totale de l'infrastructure, qu'elle soit physique ou numérique, un **plan complet de continuité d'activité et de reprise après sinistre** est en vigueur.

Ce plan comprend les mesures suivantes:



Des tests annuels du plan face à une gamme de scénarios de menaces potentielles, en tenant compte de leur probabilité.



Des tests continus du système de reprise après sinistre pour garantir son bon fonctionnement en cas d'urgence.



La collaboration avec une société de conseil en cybersécurité tierce pour une réponse rapide à tout incident de sécurité.



Des revues annuelles des politiques de réponse aux incidents.

4 Prérequis et protocoles de communication du Data Collection Agent (DCA)

Le **Data Collection Agent** (DCA) utilise le protocole SNMP (**Simple Network Management Protocol**) sur le **port UDP 161** pour rechercher les MFP, copieurs et imprimantes connectés au réseau. Seuls les périphériques répondant aux spécifications minimales du MIB imprimante v.2 conformément à la norme industrielle RFC 3805 sont intégrés à MPS Monitor, tandis que les autres périphériques présents sur le réseau sont exclus du processus de collecte de données. Le DCA prend en charge les versions SNMP v1, v2c et v3 de la pile de protocoles SNMP standard, la version SNMP v3 étant la plus sécurisée en raison de l'inclusion du chiffrement.

Pour la communication au sein du réseau local entre le DCA et les périphériques recensés, les ports de communication nécessaires sont décrits ci-dessous:

Prérequis réseau interne du DCA

Réseau de destination	Direction	Protocole	Port
Interne (réseaux avec périphériques) pour la surveillance des périphériques (SNMP)	Sortant	UDP	UDP 161 (SNMP)
Interne (réseaux avec périphériques) pour le Device Web Access et HP LFP	Sortant	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Interne (réseaux avec périphériques) pour le Device Web Access et HP LFP	Sortant	TCP	TCP 9100 TCP 515 (LPR)



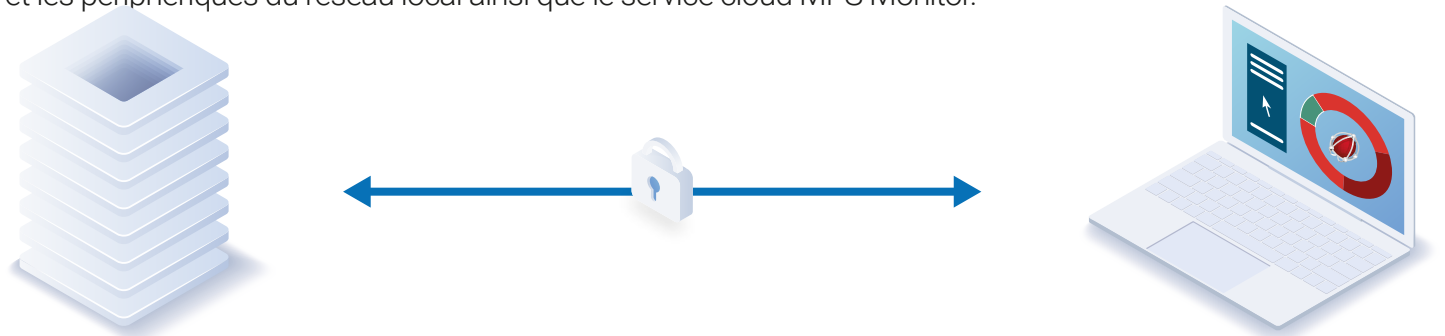


Data Collection Agent version 4

Le **DCA 4** est disponible pour les plateformes Windows, macOS et Linux, introduisant des **fonctionnalités améliorées** telles qu'une communication plus rapide et plus sécurisée, la prise en charge de SNMP v3 et l'ajout du **Device Web Access** (DWA). Le DWA permet aux utilisateurs de la Console MPS Monitor de parcourir les pages du serveur web embarqué de n'importe quelle imprimante d'un client.

Amélioration de la sécurité et de la rapidité des communications

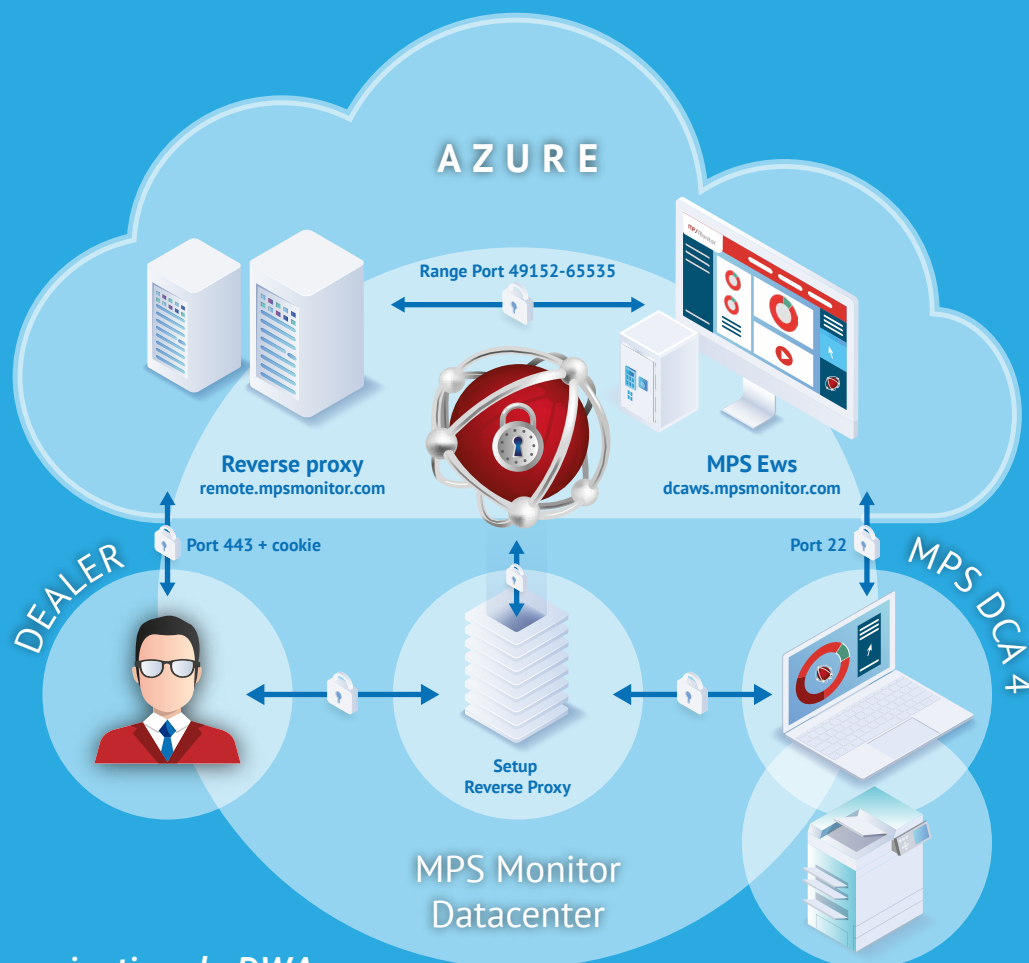
Le DCA 4 renforce la sécurité et l'optimisation du trafic en utilisant HTTPS2/GRPC sur le port 443. En outre, le DCA 4 intègre MQTT, un protocole de communication IoT léger, en utilisant Azure IoT Hub comme broker de messages. Cela accroît considérablement la rapidité de communication entre le DCA et les périphériques du réseau local ainsi que le service cloud MPS Monitor.



Device Web Access

Le Device Web Access (DWA) du DCA 4 est une fonctionnalité robuste, protégée pour garantir un accès HTTP limité et sécurisé aux imprimantes grâce à diverses mesures:

-  L'accès est restreint aux périphériques appartenant à un revendeur donné;
-  Une authentification à deux facteurs obligatoire ou une intégration à Active Directory garantit que seuls les utilisateurs autorisés peuvent utiliser la fonctionnalité DWA;
-  Le système DWA est hébergé sur MS Azure, permettant des exceptions temporaires de pare-feu pour accéder au service, qui sont supprimées après chaque session;
-  Une vérification des attributs du périphérique cible est effectuée à chaque connexion afin d'empêcher l'accès à des périphériques non valides;
-  Des journaux d'accès sont générés à chaque utilisation;
-  Les transferts de fichiers via le DWA sont désactivés.



Flux de communication du DWA



Prérequis du DCA

Prérequis de licence

Aucune licence supplémentaire n'est nécessaire pour installer MPS Monitor.

Prérequis matériels

Matériel recommandé pour la machine hébergeant le DCA:

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

Le PC n'a pas besoin d'être dédié et peut être utilisé simultanément à d'autres fins. Le connecteur DCA fonctionne en arrière-plan sans affecter les utilisateurs du PC. Pour les grands réseaux nécessitant une capacité de balayage élevée, un matériel plus performant est recommandé afin d'améliorer les performances.

Prérequis réseau, DCA 4

Le système sur lequel le DCA 4 est installé doit disposer d'un accès permanent aux endpoints et protocoles suivants:

EU STACK (portal.mpsmonitor.com)

Endpoints web pour les régions EMEA et APAC	Protocole	Ports	Entrée CDN / adresse IP
https://dca4.mpsmonitor.com <i>pour la communication de surveillance des périphériques</i>	HTTP2, GRPC	443	213.92.56.75
https://cdn2.mpsmonitor.com <i>pour les mises à jour du DCA</i>	HTTP	443	Azure CDN
dcaws.mpsmonitor.com <i>pour le Device Web Access</i>	SSH	22	13.80.42.210
eu01-broker-mpsmonitor.azure-devices.net <i>pour la communication MQTT du DCA</i>	MQTT over WSS	443	Azure IOT HUB

Endpoints web pour la région Amériques	Protocole	Ports	Entrée CDN / adresse IP
https://us01-dca.mpsmonitor.com <i>pour la communication de surveillance des périphériques</i>	HTTP2, GRPC	443	20.106.185.115
https://cdn2.mpsmonitor.com <i>pour les mises à jour du DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>pour les setups de téléchargement initial du DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.com <i>pour le Device Web Access</i>	SSH	22	20.55.38.55
us01-broker-mpsmonitor.azure-devices.net <i>pour la communication MQTT du DCA</i>	MQTT over WSS	443	Azure IOT HUB

US STACK (portal.mpsmonitor.us)

Endpoints web pour la région Amériques	Protocole	Ports	Entrée CDN / adresse IP
https://us01-dca4.mpsmonitor.us <i>pour la communication de surveillance des périphériques</i>	HTTP2, GRPC	443	20.81.25.170
https://cdn2.mpsmonitor.com <i>pour les mises à jour du DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>pour les setups de téléchargement</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.us <i>pour le Device Web Access</i>	SSH	22	104.211.20.116
us01-brk-prd-eus-iothub-01.azure-devices.net <i>pour la communication MQTT du DCA</i>	MQTT over WSS	443	Azure IOT HUB



Prérequis du système d'exploitation

Windows

Le DCA 4 est pris en charge à partir de la version **Windows 10 64 bits build 1607 (E) pour les postes clients** et de **Windows Server 2016 64 bits pour les installations serveur**.

Le programme d'installation du DCA 4 vérifiera l'installation des bibliothèques .NET Core et téléchargera les bibliothèques nécessaires depuis le site web de Microsoft.

Le DCA 4 installe deux services, **MpsMonitor.Dca.Client** et **MpsMonitor.Dca.Monitor**, qui utilisent respectivement les comptes système Network User et Local User.

En présence de restrictions ou de politiques particulières qui empêchent l'activation ou l'exécution du service par les comptes ci-dessus, il sera nécessaire d'utiliser à la place un utilisateur local spécifique.

La procédure d'installation du DCA attribuera à cet utilisateur les droits minimaux nécessaires à l'exécution du service.

MacOS

Le DCA 4 peut être installé à partir de **macOS 12 (Monterey)** ou d'une version ultérieure, et peut être installé sur des processeurs Intel ou Arm (M1, M2).

Linux et Raspberry

Le DCA 4 peut être installé sur les **distributions Linux qui prennent en charge .NET Core**. Il peut être installé sur:

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

Pour le Raspberry, le prérequis minimal est un Raspberry Pi 3 ou supérieur fonctionnant sous Bookworm (Arm 32 bits ou Arm 64 bits).

DCA embarqués

La version embarquée du DCA peut être installée directement sur certains périphériques de certains fabricants, conformément aux prérequis et aux instructions contenus dans leurs guides d'installation respectifs.

Les périphériques pris en charge et leurs endpoints respectifs sont :

HP FutureSmart 3.5, 4, 5 (uniquement la plateforme « L1 Classic »)

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
http://embeddedhp.mpsmonitor.com	Sortant	TCP	HTTP, port 80
http://embeddedfileshp.mpsmonitor.com	Sortant	TCP	HTTP, port 80

Samsung (avec le firmware XOA 1.21+)

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
http://embedded.abassetmanagement.com	Sortant	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Sortant	TCP	HTTP, port 80

Kyocera HyPAS

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
http://embedded.abassetmanagement.com	Sortant	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	Sortant	TCP	HTTP, port 80



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

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
http://embeddedlexmark.mpsmonitor.com	Sortant	TCP	HTTP, port 80
http://embeddedfileslexmark.mpsmonitor.com	Sortant	TCP	HTTP, port 80



5 Intégration avec HP Smart Device Services (SDS)

L'intégration de MPS Monitor avec **HP Smart Device Services (SDS)** offre une solution fluide et efficace pour la surveillance et la gestion des périphériques d'impression HP. En tirant parti des capacités de MPS Monitor conjointement avec les fonctionnalités avancées de HP SDS, les organisations peuvent obtenir des informations complètes sur leur parc d'imprimantes HP. Cette intégration facilite la maintenance proactive, la surveillance en temps réel et un reporting précis, optimisant les performances globales de l'infrastructure d'impression.

Grâce à la puissance combinée de MPS Monitor et de HP SDS, les entreprises peuvent **améliorer leur productivité, réduire leurs coûts opérationnels et assurer le bon fonctionnement de leur écosystème d'impression.**

Une liste complète des périphériques compatibles et des fonctionnalités disponibles est consultable via ce [lien](#)



HP JetAdvantage Management Connector (JAMC)

Le **logiciel JAMC**, un DCA développé par HP, permet l'exécution des fonctionnalités SDS sur une installation Windows. Les DCA Windows de MPS Monitor sont pleinement intégrés à cette technologie et permettent l'utilisation des fonctionnalités SDS directement depuis le portail MPS Monitor.

Prérequis de communication réseau pour la surveillance des périphériques via JAMC

Prérequis réseau interne HP JAMC

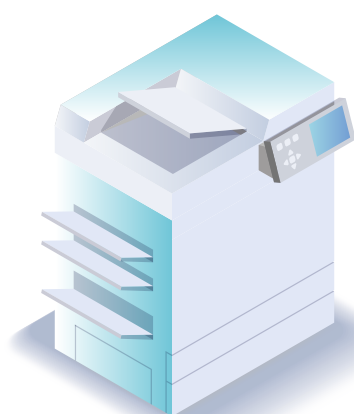
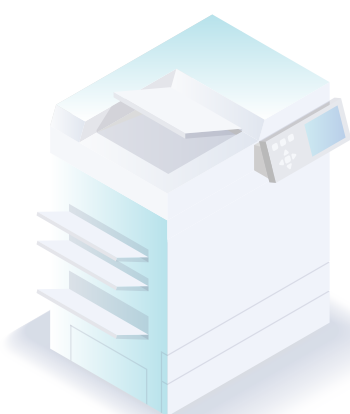
Points de terminaison web pour toutes les régions	Direction	Protocole	Port
Interne (réseaux avec périphériques) pour la surveillance des périphériques JAMC	Sortant	UDP	161, 427, 3702
Interne (réseaux avec périphériques) pour la surveillance des périphériques JAMC	Sortant	TCP	443, 3910, 3911, 7627, 8080



Le JAMC est directement connecté à l'infrastructure HP SDS Cloud, et le tableau ci-dessous décrit tous les ports de communication nécessaires:

Endpoints web pour la région Amériques	Direction	Protocole	Port
https://jamanagement.hp.com	Sortant	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Sortant	TCP	HTTPS, port 443
https://ews.hpjamservices.com	Sortant	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Sortant	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Sortant	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Sortant	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Sortant	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Sortant	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Sortant	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Sortant	TCP	HTTP, port 80

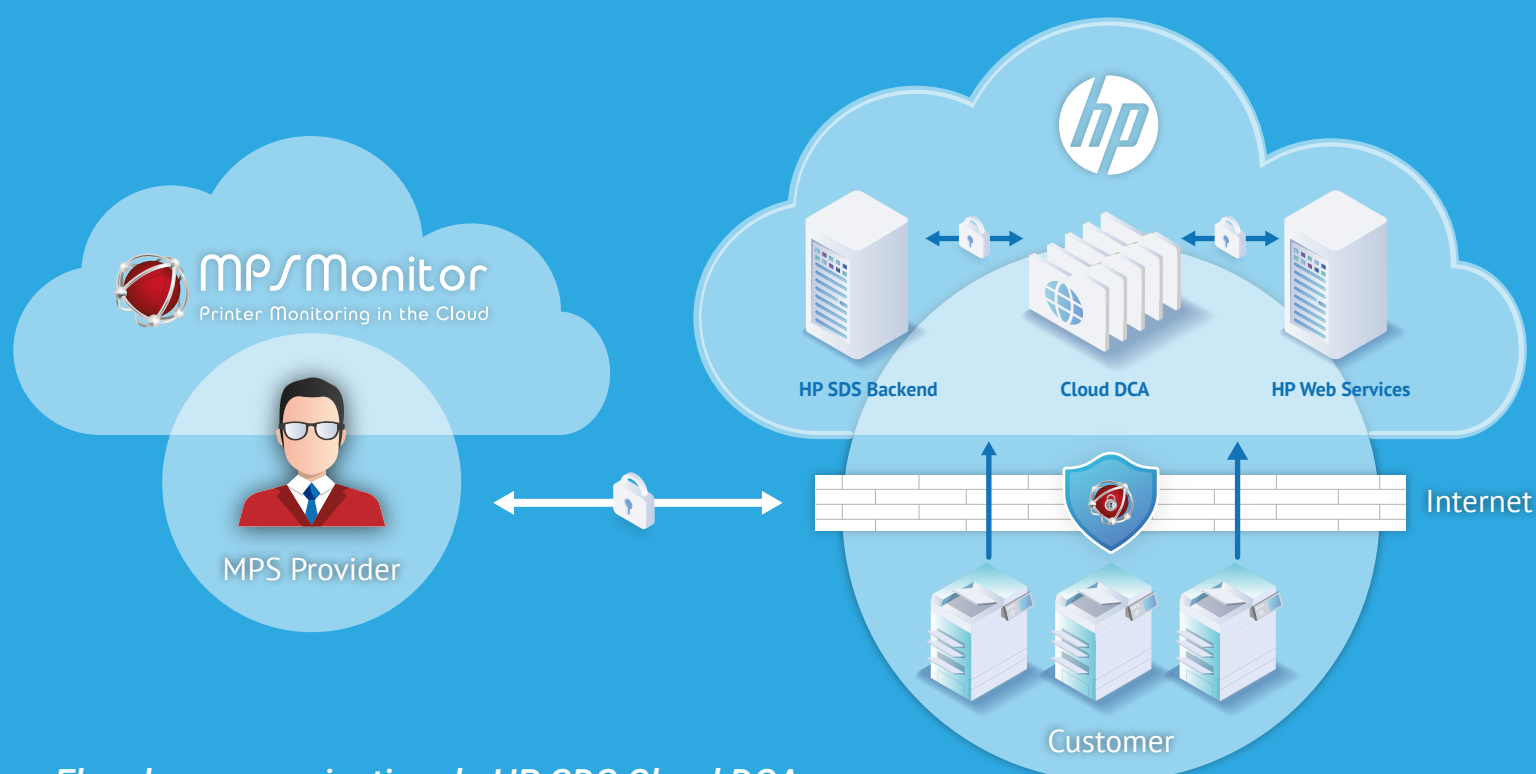
Endpoints web pour les régions EMEA et APAC	Direction	Protocole	Port
https://eu.jamangement.hp.com	Sortant	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	Sortant	TCP	HTTPS, port 443
https://eu.ews.hpjamservices.com	Sortant	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	Sortant	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	Sortant	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Sortant	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	Sortant	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	Sortant	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Sortant	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	Sortant	TCP	HTTP, port 80





HP SDS Cloud

Le **HP Smart Device Services Cloud DCA** permet à MPS Monitor de superviser et de contrôler à distance les périphériques HP FutureSmart sans nécessiter l'installation d'un DCA sur le réseau.



Flux de communication du HP SDS Cloud DCA

Communication avec le HP SDS Cloud DCA

Le HP SDS Cloud DCA est disponible pour les périphériques compatibles HP SDS dotés de la version **HP FutureSmart 4.9.0.1** ou ultérieure.

Les périphériques pris en charge doivent disposer d'une connexion stable aux endpoints web suivants:

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
https://*.avatar.ext.hp.com:443	Sortant	TCP	HTTPS, port 443
http://*.avatar.ext.hp.com:80	Sortant	TCP	HTTP, port 80
udp://*.avatar.ext.hp.com:9930	Sortant	UDP	UDP, port 9930
wss://*.avatar.ext.hp.com:443	Sortant	TCP	WSS, port 443
https://*.hpjamservices.com:443	Sortant	TCP	HTTPS, port 443
https://*.smartcloudprint.com:443	Sortant	TCP	HTTPS, port 443





Enrôler une imprimante en tant que périphérique HP SDS connecté au cloud

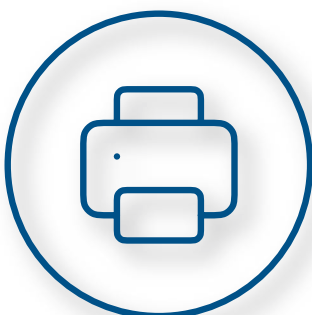
Afin d'utiliser le **HP SDS Cloud DCA**, une imprimante doit être enrôlée dans le **HP SDS Cloud**. Pour effectuer cette opération, les prérequis suivants sont nécessaires:

-  L'imprimante doit être connectée à Internet;
-  Un PC Windows connecté au même réseau que l'imprimante, sur lequel installer le HP MPS Onboarding Tool;

Le PC Windows doit accéder aux endpoints suivants:

Points de terminaison web pour toutes les régions	Direction	Protocole	Port
https://dopplerservice.msit.hpcloud.hp.com	Sortant	TCP	HTTPS, port 443
https://dopplerservice.msit.hpcloud.hp.com	Sortant	TCP	HTTPS, port 443
https://directory.id.hp.com	Sortant	TCP	HTTPS, port 443
https://coresvcs.dp.smartcloudprint.com	Sortant	TCP	HTTPS, port 443
https://directory.stg.cd.id.hp.com	Sortant	TCP	HTTPS, port 443

Pour des informations détaillées sur le HP MPS Onboarding Tool, reportez-vous au « **HP MPS Onboarding Tool User Guide** » de HP, disponible dans le portail MPS Monitor.





HP Smart Device Agent, pour la surveillance des périphériques HP connectés en USB

Le **HP Smart Device Agent (SDA) Local Agent** fonctionne comme un agent de collecte de données pour les imprimantes prises en charge par HP SDS et connectées à un ordinateur via un câble USB. Installé sur un PC Windows auquel le périphérique physique est connecté, le Local Agent recueille les données du périphérique et fonctionne avec un JAMC installé sur le réseau.

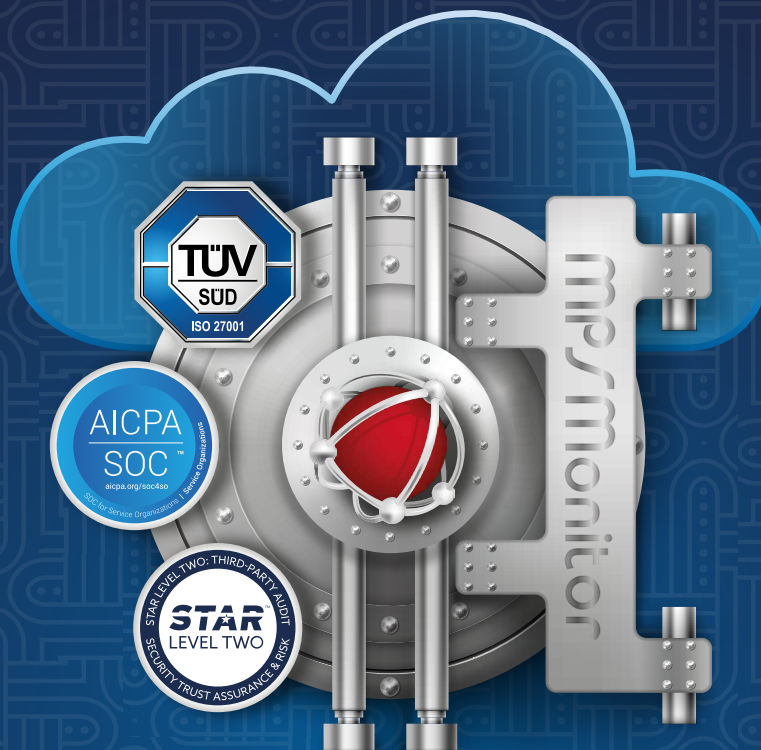
Le HP SDA utilise le port 12351 pour établir une communication HTTPS avec le JetAdvantage Management Connector (JAMC).

Pour plus de détails sur le HP Smart Device Agent, reportez-vous au « **HP Smart Device Agent for USB Connected Printers User Guide** » disponible dans le portail MPS Monitor.



6 Documents de référence

-  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



***N'imprimez ce document
que si nécessaire, merci.***



MPS Monitor soutient le programme PrintReleaf
depuis plusieurs années, contribuant
à la reforestation à l'échelle mondiale.



*MPS Monitor est une marque déposée.
Toutes les marques présentées appartiennent à leurs propriétaires légitimes.*





mpsMonitor

Printer Monitoring in the Cloud

Contactez-nous à l'adresse

info@mpsmonitor.com

Demandez un essai sur

www.mpsmonitor.com

*Préparez-vous à voyager en toute sécurité
avec nous !*

