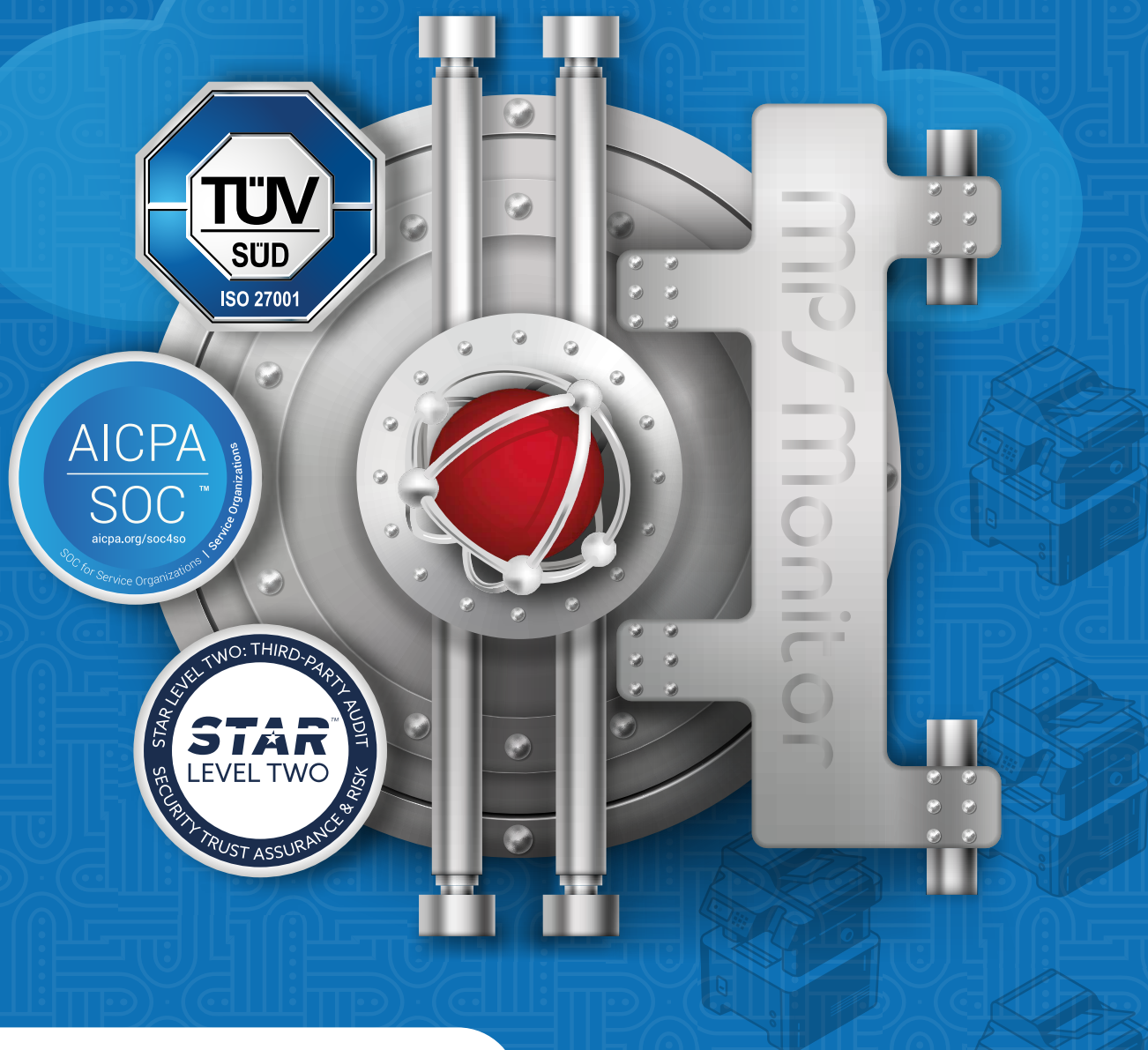


PROTEGGERE I TUOI MANAGED PRINT SERVICES



mpsMonitor
Printer Monitoring in the Cloud

01	Scopo e struttura di questo Whitepaper	pag. 03
-----------	---	----------------

02	Introduzione a MPS Monitor	pag. 04
	> Un framework di sicurezza completo	
	> Conformità a normative e standard	
	> Privacy dei dati: conformità al GDPR	

03	Sicurezza dei componenti cloud	pag. 07
	> Integrità del software	
	> Code review	
	> Controllo degli accessi: autenticazione degli utenti	
	> Sicurezza fisica e Disaster Recovery	

04	Requisiti e protocolli di comunicazione del Data Collection Agent (DCA)	pag. 10
	> Data Collection Agent versione 4	
	> Device Web Access	
	> Requisiti del DCA	
	• Requisiti di licenza	
	• Requisiti hardware	
	• Requisiti di rete	
	• Requisiti del sistema operativo	
	• Windows	
	• MacOS	
	• Linux	
	• DCA embedded	

05	Integrazione con HP Smart Device Services (SDS)	pag. 18
	> Integrazione con HP Smart Device Services (SDS)	
	> HP SDS Cloud DCA	
	> Onboarding di una stampante come HP SDS Cloud-Connected	
	> HP Smart Device Agent: per il monitoraggio dei dispositivi HP USB	

06	Documenti di riferimento	pag. 25
-----------	---------------------------------	----------------

1 Scopo e struttura di questo Whitepaper

Questo **Whitepaper tecnico** fornisce una panoramica della piattaforma SaaS di MPS Monitor, con particolare attenzione ai vari aspetti legati alla sicurezza. Le sezioni seguenti offrono un esame dettagliato delle certificazioni, delle policy di sicurezza, della mitigazione degli incidenti, dell'integrità del software e di altri componenti critici della piattaforma.

Introduzione a MPS Monitor

In questa sezione si approfondiscono le funzionalità principali di MPS Monitor, con particolare attenzione a una policy di sicurezza completa. La trattazione si estende alle strategie di privacy e sicurezza dei dati, garantendo una base solida per la piattaforma.

Sicurezza dei componenti cloud

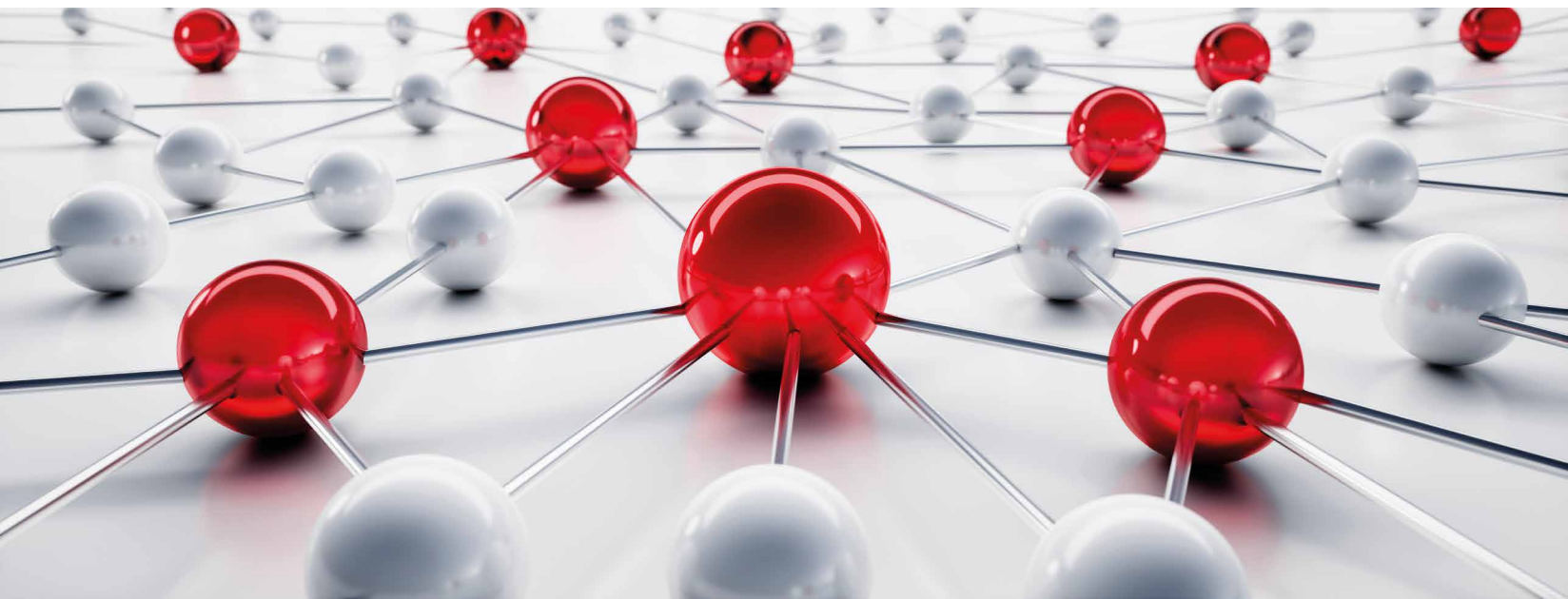
Questo segmento affronta il panorama della sicurezza all'interno dei componenti software e cloud, ponendo l'accento sulle misure di sicurezza operativa e sui protocolli relativi all'autenticazione degli utenti.

Data Collection Agent (DCA): dispositivi connessi in rete

In questa sezione si esaminano gli aspetti tecnici dei Data Collection Agent per i dispositivi connessi in rete. Viene trattata la versione 4, con particolare enfasi sul miglioramento della sicurezza e della velocità di comunicazione. Vengono trattati in modo esaustivo i requisiti dei DCA, comprese le specifiche di licenza, hardware, rete e sistema operativo.

Integrazione con HP Smart Device Services (SDS)

Il whitepaper si conclude con un'analisi delle capacità di integrazione con HP Smart Device Services, che comprendono connettori, cloud DCA e soluzioni di monitoraggio per i dispositivi HP USB.



2 Introduzione a MPS Monitor

MPS Monitor offre una **soluzione Software as a Service (SaaS) cloud di primo piano, adottata da dealer e provider di Managed Print Services** in tutto il mondo. La sua missione principale è supervisionare e amministrare con attenzione un parco di dispositivi di stampa prodotti da tutte le principali marche di stampanti.

Questo whitepaper illustra ciò che distingue MPS Monitor come leader di riferimento nella fornitura di **soluzioni di Managed Print Services (MPS) estremamente sicure**, sia per i dealer sia per la loro esigente clientela. La piattaforma adotta un approccio olistico alla sicurezza, rigorosamente esaminato e approvato da autorevoli organizzazioni indipendenti di terze parti. Inoltre, è soggetta ad audit continui per mantenere e rafforzare la fiducia nella propria infrastruttura e nelle proprie prassi di sicurezza.

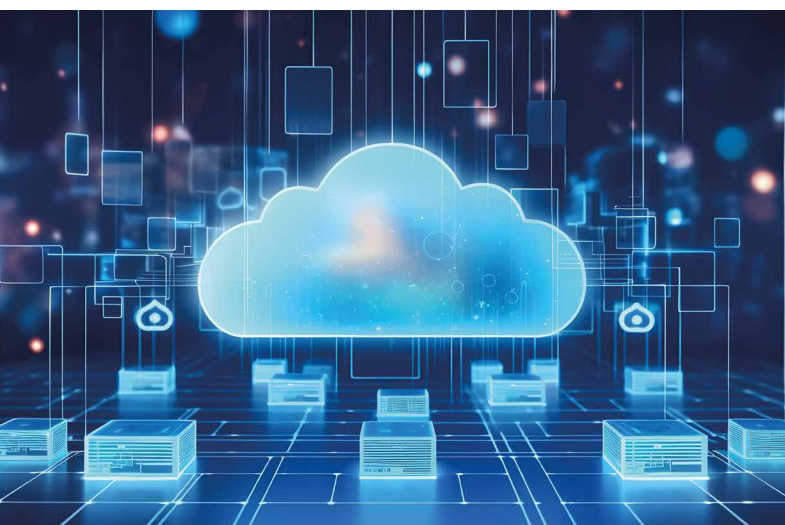
La piattaforma è composta da due componenti principali:

- 1. Il Connettore DCA (Data Collection Agent):** installato all'interno della rete locale (LAN) del cliente, esegue operazioni sui dispositivi in base alle istruzioni provenienti dal componente Server. Il deployment è versatile e comprende sistemi Windows, Linux o macOS, oppure l'integrazione in una stampante multifunzione (MFP). Un'opzione DCA-less basata sul cloud HP (l'HP Cloud DCA) consente di monitorare e gestire da remoto i dispositivi HP FutureSmart senza installare alcun Agent on-premise.
- 2. Il Cloud Server e il Web Portal:** il Cloud Server ospita i preziosi dati dei dispositivi forniti dal DCA. Gli utenti finali accedono a un portale web dedicato in modo sicuro tramite HTTPS, interagendo con la piattaforma da qualsiasi luogo e utilizzando qualsiasi browser web.



Un framework di sicurezza completo

MPS Monitor ha definito e implementato un **Sistema di gestione della sicurezza delle informazioni (ISMS)**, un framework di sicurezza standard di mercato che si concentra sui principi essenziali di **Riservatezza, Integrità e Disponibilità**, progettato con l'obiettivo di estendere le proprie funzionalità di sicurezza a beneficio di tutti i dealer e dei loro clienti che utilizzano la piattaforma.



“ *MPS Monitor ha dimostrato in modo evidente il proprio impegno per la sicurezza*



Conformità a normative e standard

MPS Monitor ha dimostrato in modo evidente il proprio impegno per la sicurezza superando con successo valutazioni e certificazioni incentrate sulla sicurezza riconosciute a livello globale, tra cui:



ISO/IEC 27001: attesta un approccio sistematico alla gestione dei rischi per la sicurezza delle informazioni, garantendo la massima Riservatezza, Integrità e Disponibilità dei dati.



System and Organization Controls 2 (SOC 2): raggiungimento della conformità ai criteri AICPA Service Organization Control 2 Type 2 nell'arco di un anno, verificando l'efficacia dei controlli di sicurezza.



CSA STAR Level 2 Attestation: garantisce la conformità alla Cloud Controls Matrix (CCM), un framework di controlli di cybersecurity per il cloud computing.



Keypoint Intelligence: numerose valutazioni confermano l'integrità della sicurezza di MPS Monitor.



Privacy dei dati: conformità al GDPR



Qualsiasi azienda con clienti in Europa deve rispettare il **Regolamento generale sulla protezione dei dati 2016/679** (GDPR). I dealer di stampanti e i provider di Managed Print Services (MPS) non fanno eccezione, poiché il GDPR si applica anche alla gestione dei dati personali all'interno dei sistemi SaaS di monitoraggio remoto.

L'articolo 4.1 del GDPR definisce chiaramente i «dati personali» e include nomi, indirizzi fisici e identificativi online come un indirizzo email collegato a un'identità fisica.



La conformità al GDPR è importante anche per i clienti americani per diverse ragioni:



Operatività aziendale globale: molte aziende operano su scala globale, avendo clienti nell'Unione Europea (UE) oppure trattando i dati personali di cittadini dell'UE. La conformità al GDPR è essenziale per qualsiasi organizzazione che tratta i dati personali di residenti dell'UE, indipendentemente da dove l'azienda abbia sede.



Fiducia e reputazione presso i clienti: dimostrare la conformità al GDPR riflette l'impegno a proteggere la privacy e i diritti delle persone. In un'epoca in cui le violazioni dei dati e le preoccupazioni per la privacy sono diffuse, le aziende che danno priorità alla protezione dei dati sono probabilmente viste in modo favorevole dai consumatori.



Requisiti legali e normativi: le aziende globali possono avere filiali, succursali o rapporti commerciali nell'UE, rendendo la conformità al GDPR un obbligo di legge. La non conformità può comportare sanzioni ingenti e conseguenze legali.



Best practice per la sicurezza dei dati: la conformità al GDPR incoraggia le organizzazioni a implementare solide prassi di sicurezza dei dati. Seguire le linee guida del GDPR è in linea con le best practice generali per la protezione e la sicurezza dei dati. Anche quando non richiesta per legge, l'adozione di queste misure può aiutare le aziende a migliorare la propria postura complessiva di cybersecurity.

In sintesi, la **conformità al GDPR** non riguarda esclusivamente le aziende con sede nell'UE: ha **implicazioni per qualsiasi organizzazione che interagisce con i dati personali dei cittadini dell'UE**. Le aziende globali che riconoscono e affrontano queste considerazioni dimostrano un impegno verso la privacy, la responsabilità legale e gli standard globali di protezione dei dati.



Per maggiori dettagli su come MPS Monitor garantisce la conformità al GDPR e agli standard ISO 27001, SOC 2 Type 2 e CSA STAR Level 2,

visita questo [link](#)



3 Sicurezza dei componenti cloud

L'infrastruttura cloud di backend di MPS Monitor, ospitata all'interno dei data center di British Telecom a Milano, in Italia, è di completa proprietà e amministrazione dell'azienda stessa. Un team interno di professionisti IT e della sicurezza altamente qualificati supervisiona tutte le procedure e gli strumenti in essere per garantire il rispetto dei **requisiti di sicurezza** più rigorosi e la piena conformità agli standard internazionali in ogni momento. Le misure di sicurezza adottate dall'azienda includono:

- ➔ Monitoraggio dei sistemi 24x7 tramite un set completo di strumenti di monitoraggio dell'infrastruttura e delle applicazioni;
- ➔ Gestione estesa di Log Analytics;
- ➔ Alerting in tempo reale su tutti i principali eventi legati alla sicurezza;
- ➔ Vulnerability Assessment e monitoraggio continui su tutti gli asset;
- ➔ Penetration test annuali eseguiti da aziende esterne di cybersecurity
- ➔ Sorveglianza continua nell'ambito delle valutazioni annuali ISO 27001, SOC 2 Type 2 e CSA STAR Level 2.



Integrità del software

Il software di MPS Monitor aderisce ai principi di «sicurezza e protezione dei dati by default e by design», implementando un elevato numero di misure e controlli di sicurezza che garantiscono la massima sicurezza nel processo di sviluppo e rilascio. Tali misure includono:

- ➔ Controllo delle versioni tramite software di version control;
- ➔ Monitoraggio dell'integrità dei file per consentire solo le modifiche autorizzate;
- ➔ Ambienti di test separati per il quality assurance e lo user acceptance testing;
- ➔ Firme digitali per tutti i componenti all'interno di un pacchetto di rilascio;
- ➔ Code review a ogni rilascio di codice del DCA;
- ➔ Auditing e testing di sicurezza ogni sei mesi, condotti in modo indipendente da aziende specializzate.



Code review

Un'azienda di sicurezza esterna esegue una **Code Review prima di ogni rilascio del codice del DCA**. Le attività di test del codice vengono svolte adottando un approccio ibrido che combina una fase di **analisi statica del codice** con un'**analisi dinamica dell'applicazione**. Questo approccio consente di offrire un'ampia copertura della superficie di attacco e di individuare sia le vulnerabilità superficiali sia i problemi che risiedono più in profondità nella logica applicativa e che pertanto non sono immediatamente identificabili. Tutte le criticità rilevate a livello teorico vengono poi validate attraverso la creazione di software **Proof of Concept (PoC)**, che consente di valutare l'effettivo livello di sfruttabilità sulla base del quale è possibile assegnare successivamente un punteggio di gravità.

L'attività di Code Review comprende anche il **test sia del codice sorgente sia dei componenti compilati rispetto a una checklist di sicurezza predefinita**, che garantisce che il pacchetto in fase di rilascio sia conforme ai rigorosi requisiti di sicurezza stabiliti per il componente DCA.

Una nuova versione del codice del DCA può essere rilasciata ai clienti solo quando il processo di Code Review certifica formalmente la risoluzione dei problemi di sicurezza e la conformità a tutti i requisiti.



Controllo degli accessi: autenticazione degli utenti

L'accesso al portale MPS Monitor richiede account utente, regolati da un sistema di privilegi utente strutturato in modo meticoloso. Questo sistema garantisce un accesso preciso e controllato agli utenti, in linea con i loro ruoli all'interno dell'organizzazione di un dealer o di un cliente finale.

Sebbene sia indispensabile che le password siano lunghe e complesse per essere considerate robuste, il fattore umano può spesso compromettere l'efficacia di requisiti così rigorosi. Inoltre, la necessità di gestire più set di credenziali per i vari sistemi accresce ulteriormente il fattore di rischio.

Per affrontare queste sfide, **MPS Monitor ha integrato due importanti funzionalità** per aumentare la sicurezza dell'autenticazione degli utenti:



Supporto per le soluzioni Single Sign-On (SSO):

MPS Monitor offre il supporto per soluzioni di Single Sign-On, come **Okta o Azure AD**. Questa integrazione consente agli utenti di allinearsi alle migliori prassi in materia di password prescritte dai team di sicurezza della loro organizzazione. Tramite l'integrazione con Okta o Azure AD, gli utenti possono autenticarsi attraverso il sistema di Identity Management (IDM) dell'organizzazione, ottenendo così un accesso sicuro alla piattaforma cloud di MPS Monitor. Questo processo di Single Sign-On ottimizzato e completamente sicuro non solo semplifica l'esperienza dell'utente, ma migliora anche la sicurezza riducendo la dipendenza dalle password tradizionali per ogni singolo sistema. Gli utenti possono accedere a MPS Monitor senza dover ricordare più password complesse, contribuendo a un ecosistema di sicurezza più robusto.



Supporto per la Multi-Factor Authentication

MPS Monitor dà priorità alla protezione dei tuoi dati con l'implementazione di solide misure di sicurezza, tra cui l'autenticazione a più fattori. Gli utenti possono beneficiare di un ulteriore livello di protezione per le loro informazioni sensibili. Questa funzionalità garantisce che l'accesso all'applicazione sia concesso solo alle persone autorizzate, migliorando la postura di sicurezza complessiva e offrendo agli utenti tranquillità. In MPS Monitor comprendiamo l'importanza di mantenere i tuoi dati al sicuro, e il nostro impegno nell'impiego di funzionalità di sicurezza all'avanguardia come l'autenticazione a più fattori riflette questa dedizione.



Sicurezza fisica e Disaster Recovery

L'accesso fisico al data center in cui è ospitato MPS Monitor è rigorosamente controllato. La struttura è protetta da personale di sicurezza armato e tutti gli ospiti devono essere sempre accompagnati. Il centro è dotato di videosorveglianza e protetto contro incendi e allagamenti.

Per garantire la continuità dei servizi cloud di MPS Monitor, anche in caso di perdita completa dell'infrastruttura, fisica o digitale, è in vigore un **piano completo di business continuity e disaster recovery**.

Questo piano comprende le seguenti misure:



Test annuale del piano rispetto a una serie di potenziali scenari di minaccia, tenendo conto della probabilità.



Test continui del sistema di disaster recovery per garantirne la funzionalità in caso di emergenza.



Collaborazione con una società di consulenza di cybersecurity di terze parti per una risposta rapida a qualsiasi incidente di sicurezza;



Revisioni annuali delle policy di risposta agli incidenti.

4 Requisiti e protocolli di comunicazione del Data Collection Agent (DCA)

Il **Data Collection Agent** (DCA) utilizza il **protocollo SNMP** (Simple Network Management Protocol) sulla **porta UDP 161** per rilevare MFP, fotocopiatrici e stampanti connessi in rete. Solo i dispositivi che soddisfano le specifiche minime della printer MIB v.2 secondo lo standard di settore RFC 3805 vengono integrati in MPS Monitor, mentre gli altri presenti in rete sono esclusi dal processo di raccolta dei dati. Il DCA supporta SNMP v1, v2c e v3 dello stack di protocollo standard SNMP, dove SNMP v3 è il più sicuro grazie all'inclusione della cifratura.

Per la comunicazione sulla rete locale tra il DCA e i dispositivi rilevati, le porte di comunicazione necessarie sono indicate come segue:

Requisiti di rete interna del DCA

Rete di destinazione	Direzione	Protocollo	Porta
Interna (reti con dispositivi) per il monitoraggio dei dispositivi (SNMP)	In uscita	UDP	UDP 161 (SNMP)
Interna (reti con dispositivi) per il Device Web Access e HP LFP	In uscita	TCP	TCP 80 (HTTP) TCP 443 (HTTPS) * custom ports
Interna (reti con dispositivi) per il Device Web Access e HP LFP	In uscita	TCP	TCP 9100 TCP 515 (LPR)



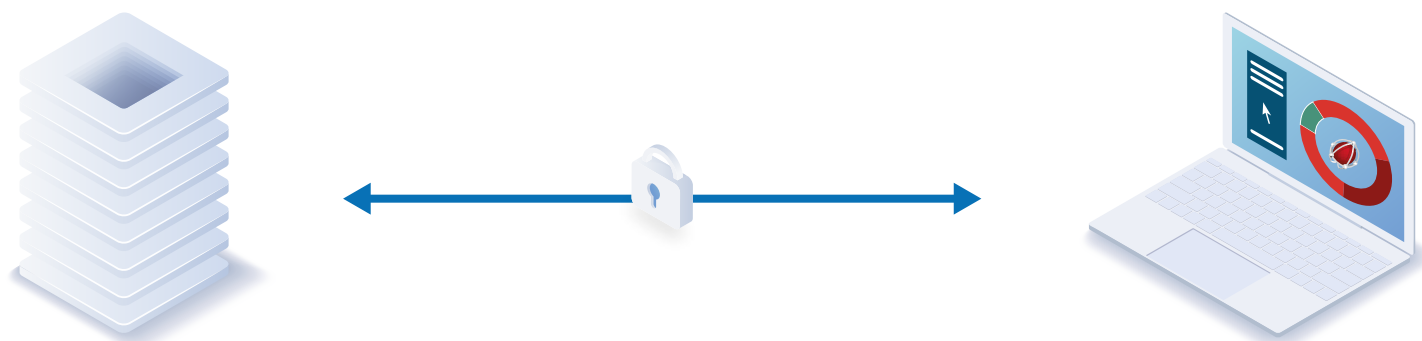


Data Collection Agent versione 4

Il **DCA 4** è disponibile per le piattaforme Windows, macOS e Linux e introduce **funzionalità migliorate** come una comunicazione più veloce e sicura, il supporto SNMP v3 e l'aggiunta del **Device Web Access** (DWA). Il DWA consente agli utenti della MPS Monitor Console di navigare tra le pagine del web server integrato di qualsiasi stampante del cliente.

Maggiore sicurezza e velocità di comunicazione

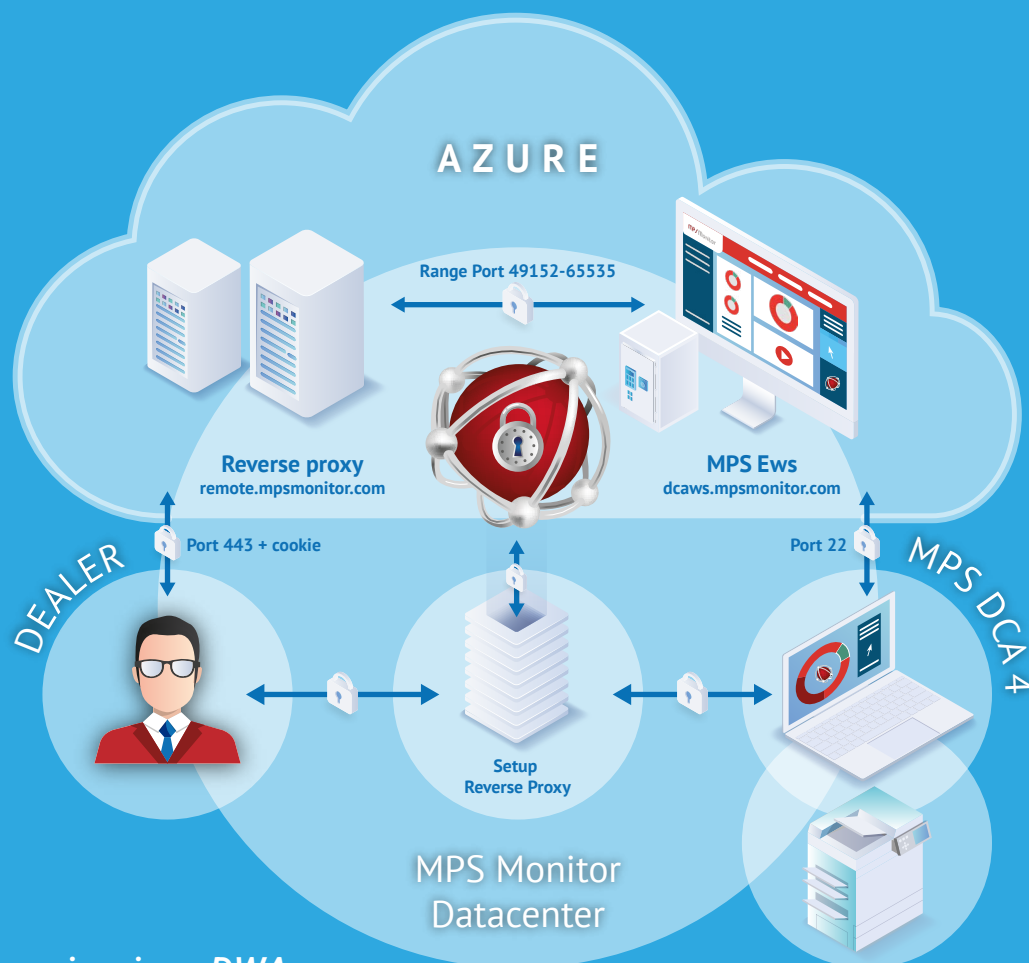
Il DCA 4 migliora la sicurezza e l'ottimizzazione del traffico utilizzando HTTPS2/GRPC sulla porta 443. Inoltre, il DCA 4 integra MQTT, un protocollo di comunicazione IoT leggero, utilizzando Azure IoT Hub come message broker. Questo aumenta in modo significativo la velocità di comunicazione tra il DCA e i dispositivi sulla rete locale e il servizio cloud di MPS Monitor.



Device Web Access

Il Device Web Access (DWA) del DCA 4 è una funzionalità robusta, protetta per garantire un accesso HTTP alle stampanti limitato e sicuro attraverso varie misure:

-  L'accesso è limitato ai dispositivi di proprietà di un determinato dealer;
-  L'autenticazione a due fattori obbligatoria o l'integrazione con Active Directory garantisce che solo gli utenti autorizzati possano utilizzare la funzionalità DWA;
-  Il sistema DWA è ospitato su MS Azure e consente eccezioni firewall temporanee per accedere al servizio, che vengono eliminate dopo ogni sessione;
-  A ogni connessione viene eseguita la verifica degli attributi del dispositivo di destinazione per impedire l'accesso a dispositivi non validi;
-  Per ogni utilizzo vengono generati log di accesso;
-  I trasferimenti di file tramite DWA sono disabilitati.



Flusso di comunicazione DWA



Requisiti del DCA

Requisiti di licenza

Per l'installazione di MPS Monitor non sono necessarie licenze aggiuntive.

Requisiti hardware

Hardware consigliato per la macchina che ospita il DCA:

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

Il PC non deve essere dedicato e può essere utilizzato contemporaneamente per altri scopi. Il connettore DCA funziona in background senza influire sugli utenti del PC. Per reti di grandi dimensioni con elevati requisiti di scansione, si consiglia un hardware migliore per prestazioni superiori.

Requisiti di rete: DCA 4

Il sistema su cui è installato il DCA 4 deve avere accesso permanente ai seguenti endpoint e protocolli:

EU STACK (portal.mpsmonitor.com)

Endpoint web per le regioni EMEA e APAC	Protocollo	Porte	Nodo CDN / indirizzo IP
https://dca4.mpsmonitor.com <i>per la comunicazione di monitoraggio dei dispositivi</i>	HTTP2, GRPC	443	213.92.56.75
https://cdn2.mpsmonitor.com <i>per gli aggiornamenti del DCA</i>	HTTP	443	Azure CDN
dcaws.mpsmonitor.com <i>per il Device Web Access</i>	SSH	22	13.80.42.210
eu01-broker-mpsmonitor.azure-devices.net <i>per la comunicazione MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB

Endpoint web per la regione Americas	Protocollo	Porte	Nodo CDN / indirizzo IP
https://us01-dca.mpsmonitor.com <i>per la comunicazione di monitoraggio dei dispositivi</i>	HTTP2, GRPC	443	20.106.185.115
https://cdn2.mpsmonitor.com <i>per gli aggiornamenti del DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>per i pacchetti di installazione iniziale del DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.com <i>per il Device Web Access</i>	SSH	22	20.55.38.55
us01-broker-mpsmonitor.azure-devices.net <i>per la comunicazione MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB

US STACK (portal.mpsmonitor.us)

Endpoint web per la regione Americas	Protocollo	Porte	Nodo CDN / indirizzo IP
https://us01-dca4.mpsmonitor.us <i>per la comunicazione di monitoraggio dei dispositivi</i>	HTTP2, GRPC	443	20.81.25.170
https://cdn2.mpsmonitor.com <i>per gli aggiornamenti del DCA</i>	HTTP	443	Azure CDN
https://cdn1.mpsmonitor.com <i>per i pacchetti di installazione iniziale del DCA</i>	HTTP	443	Azure CDN
us01-dcaws.mpsmonitor.us <i>per il Device Web Access</i>	SSH	22	104.211.20.116
us01-brk-prd-eus-iothub-01.azure-devices.net <i>per la comunicazione MQTT del DCA</i>	MQTT over WSS	443	Azure IOT HUB

**Requisiti del sistema operativo****Windows**

Il DCA 4 è supportato a partire dalla versione **Windows 10 64-bit build 1607 (E) per i clienti** e **Windows Server 2016 64-bit per le installazioni server**.

Il setup del DCA 4 verificherà l'installazione delle librerie .NET Core e scaricherà le librerie necessarie dal sito web Microsoft.

Il DCA 4 installa due servizi, **MpsMonitor.Dca.Client** e **MpsMonitor.Dca.Monitor**, che utilizzano rispettivamente gli account di sistema Network User e Local User.

Se sono presenti restrizioni o policy particolari che impediscono l'attivazione o l'esecuzione del servizio da parte degli account sopra indicati, sarà necessario utilizzare invece uno specifico utente locale.

La procedura di installazione del DCA assegnerà a questo utente i diritti minimi necessari per l'esecuzione del servizio.

MacOS

Il DCA 4 può essere installato a partire da **macOS 12 (Monterey)** o versioni successive, sia su CPU Intel sia su CPU Arm (M1, M2).

Linux e Raspberry

Il DCA 4 può essere installato su **distribuzioni Linux che supportano .NET Core**.
Può essere installato su:

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

Per il Raspberry, il requisito minimo è Raspberry Pi 3 o superiore con Bookworm (Arm 32-bit o Arm 64-bit).

DCA embedded

La versione embedded del DCA può essere installata direttamente su alcuni dispositivi di determinati produttori, secondo i requisiti e le istruzioni contenuti nelle rispettive guide di installazione.

I dispositivi supportati e i rispettivi endpoint sono:

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

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
http://embeddedhp.mpsmonitor.com	In uscita	TCP	HTTP, port 80
http://embeddedfileshp.mpsmonitor.com	In uscita	TCP	HTTP, port 80

Samsung (con firmware XOA 1.21+)

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
http://embedded.abassetmanagement.com	In uscita	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	In uscita	TCP	HTTP, port 80

Kyocera HyPAS

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
http://embedded.abassetmanagement.com	In uscita	TCP	HTTP, port 80
http://embeddedfiles.abassetmanagement.com	In uscita	TCP	HTTP, port 80



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

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
http://embeddedlexmark.mpsmonitor.com	In uscita	TCP	HTTP, port 80
http://embeddedfileslexmark.mpsmonitor.com	In uscita	TCP	HTTP, port 80



5 Integrazione con HP Smart Device Services (SDS)

L'integrazione di MPS Monitor con **HP Smart Device Services (SDS)** offre una soluzione fluida ed efficiente per monitorare e gestire i dispositivi di stampa HP. Sfruttando le capacità di MPS Monitor insieme alle funzionalità avanzate di HP SDS, le organizzazioni possono ottenere informazioni complete sul proprio parco di stampanti HP. Questa integrazione facilita la manutenzione proattiva, il monitoraggio in tempo reale e una reportistica precisa, ottimizzando le prestazioni complessive dell'infrastruttura di stampa.

Con la potenza combinata di MPS Monitor e HP SDS, le aziende possono **aumentare la produttività, ridurre i costi operativi e garantire il regolare funzionamento del proprio ecosistema di stampa.**

Un elenco completo dei dispositivi compatibili e delle funzionalità disponibili è consultabile a questo [link](#)



HP JetAdvantage Management Connector (JAMC)

Il **software JAMC**, un DCA sviluppato da HP, consente l'esecuzione delle funzionalità SDS su un'installazione Windows. I DCA Windows di MPS Monitor sono completamente integrati con questa tecnologia e consentono l'utilizzo delle funzionalità SDS direttamente dal portale MPS Monitor.

Requisiti di comunicazione di rete per il monitoraggio dei dispositivi JAMC

Requisito di rete interna HP JAMC

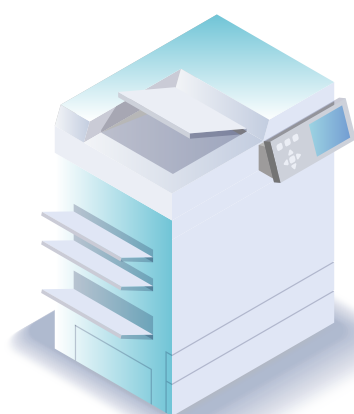
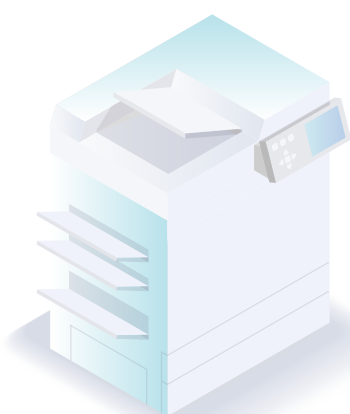
Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
Interna (reti con dispositivi) per il monitoraggio dei dispositivi JAMC	In uscita	UDP	161, 427, 3702
Interna (reti con dispositivi) per il monitoraggio dei dispositivi JAMC	In uscita	TCP	443, 3910, 3911, 7627, 8080



JAMC è connesso direttamente all'infrastruttura HP SDS Cloud e la tabella seguente indica tutte le porte di comunicazione necessarie:

Endpoint web per la regione Americas	Direzione	Protocollo	Porta
https://jamanagement.hp.com	In uscita	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	In uscita	TCP	HTTPS, port 443
https://ews.hpjamservices.com	In uscita	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	In uscita	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	In uscita	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	In uscita	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1.crl	In uscita	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	In uscita	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	In uscita	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-2.crl	In uscita	TCP	HTTP, port 80

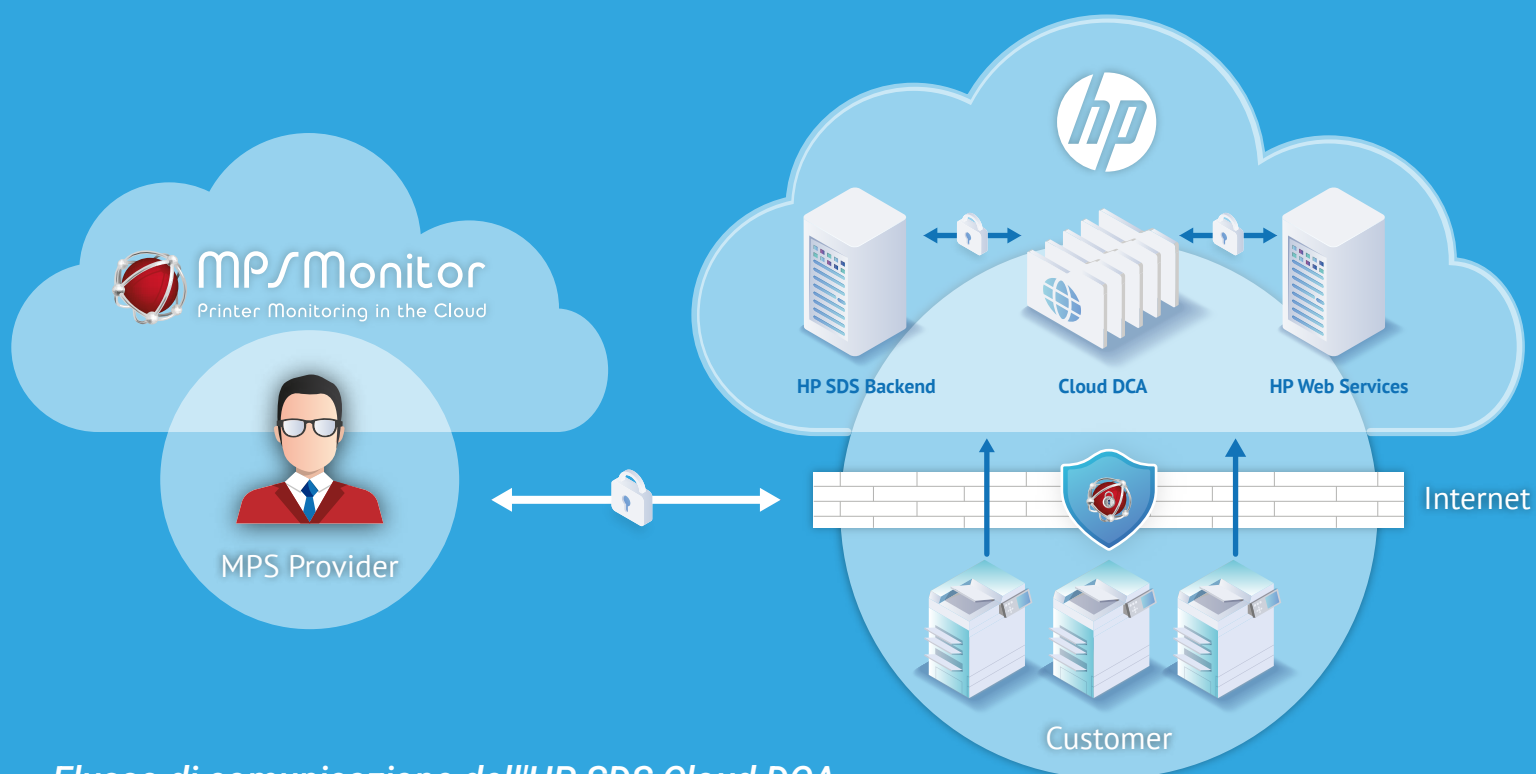
Endpoint web per le regioni EMEA e APAC	Direzione	Protocollo	Porta
https://eu.jamanagerment.hp.com	In uscita	TCP	HTTPS, port 443
https://connectivity.pod1.avatar.ext.hp.com	In uscita	TCP	HTTPS, port 443
https://eu.ews.hpjamservices.com	In uscita	TCP	HTTPS, port 443
http://crl.sca1b.amazontrust.com/sca1b.crl	In uscita	TCP	HTTP, port 80
https://registration.pod1.avatar.ext.hp.com	In uscita	TCP	HTTPS, port 443
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	In uscita	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1.crl	In uscita	TCP	HTTP, port 80
http://signal.pod1.avatar.ext.hp.com	In uscita	TCP	HTTP, port 80
http://crl3.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	In uscita	TCP	HTTP, port 80
http://crl4.digicert.com/DigiCertGlobalG2TLRSASHA2562020CA1-2.crl	In uscita	TCP	HTTP, port 80





HP SDS Cloud

L'**HP Smart Device Services Cloud DCA** consente a MPS Monitor di supervisionare e controllare da remoto i dispositivi HP FutureSmart senza richiedere l'installazione di un DCA in rete.



Flusso di comunicazione dell'HP SDS Cloud DCA

Comunicazione con l'HP SDS Cloud DCA

L'HP SDS Cloud DCA è disponibile per i dispositivi compatibili con HP SDS dotati di **HP FutureSmart versione 4.9.0.1** o successiva.

dispositivi supportati devono avere una connessione stabile ai seguenti endpoint web:

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
https://*.avatar.ext.hp.com:443	In uscita	TCP	HTTPS, port 443
http://*.avatar.ext.hp.com:80	In uscita	TCP	HTTP, port 80
udp://*.avatar.ext.hp.com:9930	In uscita	UDP	UDP, port 9930
wss://*.avatar.ext.hp.com:443	In uscita	TCP	WSS, port 443
https://*.hpjamservices.com:443	In uscita	TCP	HTTPS, port 443
https://*.smartcloudprint.com:443	In uscita	TCP	HTTPS, port 443





Onboarding di una stampante come HP SDS cloud-connected

Per utilizzare l'**HP SDS Cloud DCA**, una stampante deve essere sottoposta a onboarding nell'**HP SDS Cloud**. Per eseguire questa operazione sono necessari i seguenti requisiti:



la stampante deve essere connessa a internet;

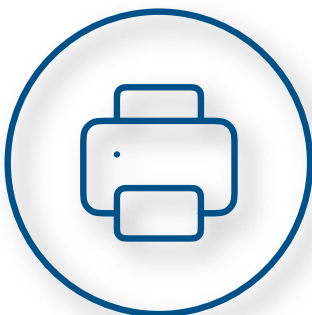


un PC Windows connesso alla stessa rete della stampante, su cui installare l'HP MPS Onboarding Tool.

il PC Windows deve accedere ai seguenti endpoint:

Endpoint web per tutte le aree geografiche	Direzione	Protocollo	Porta
https://dopplerservice.msit.hpcloud.hp.com	In uscita	TCP	HTTPS, port 443
https://dopplerservice.msit.hpcloud.hp.com	In uscita	TCP	HTTPS, port 443
https://directory.id.hp.com	In uscita	TCP	HTTPS, port 443
https://coresvcs.dp.smartcloudprint.com	In uscita	TCP	HTTPS, port 443
https://directory.stg.cd.id.hp.com	In uscita	TCP	HTTPS, port 443

Per informazioni dettagliate sull'HP MPS Onboarding Tool, consulta la «**HP MPS Onboarding Tool User Guide**» di HP, disponibile nel portale MPS Monitor.



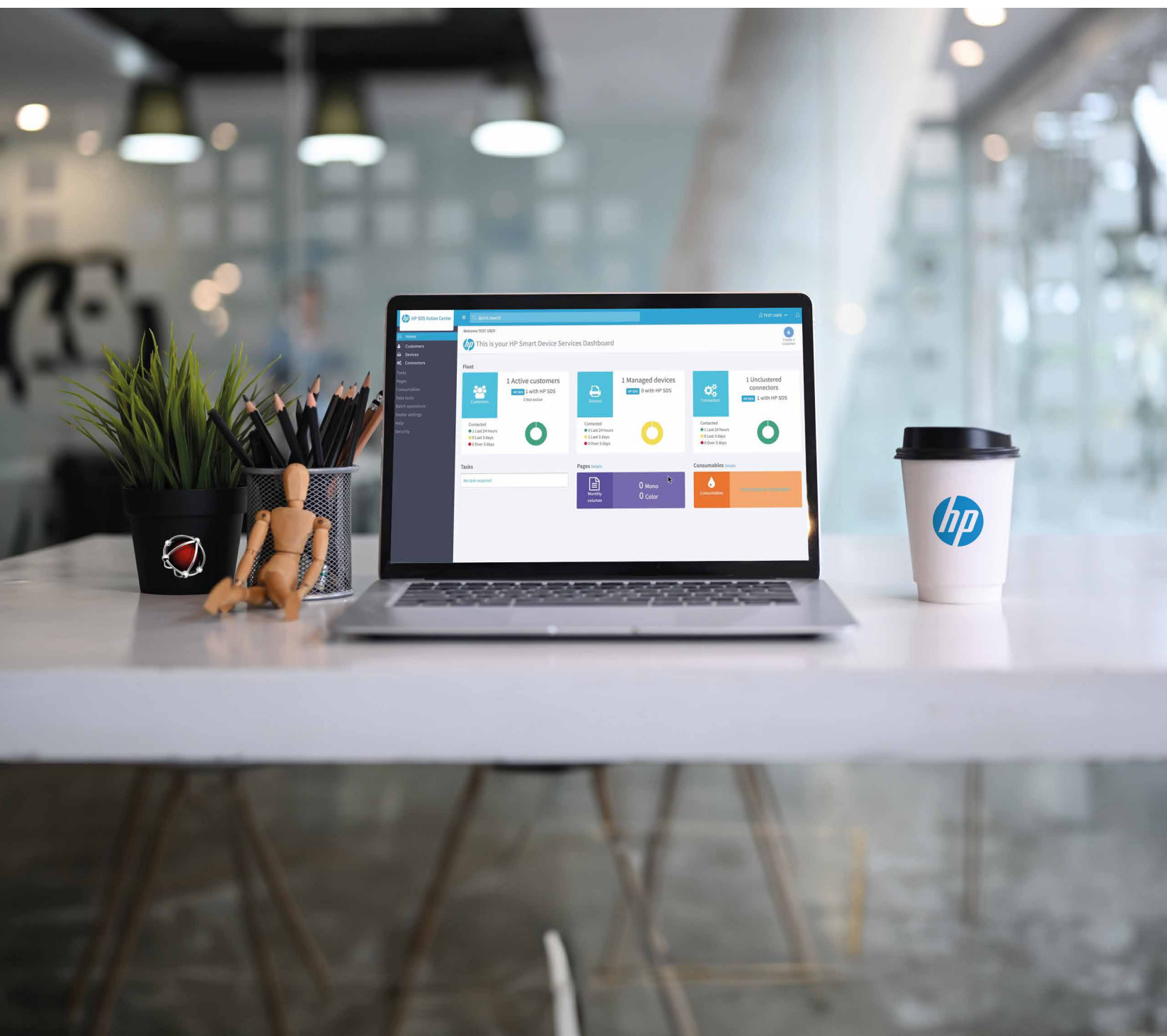


HP Smart Device Agent: per il monitoraggio dei dispositivi HP USB

L'**HP Smart Device Agent (SDA) Local Agent** funziona come agente di raccolta dati per le stampanti supportate da HP SDS connesse a un computer tramite cavo USB. Installato su un PC Windows a cui è connesso il dispositivo fisico, il Local Agent raccoglie i dati dal dispositivo e opera insieme a un JAMC installato in rete.

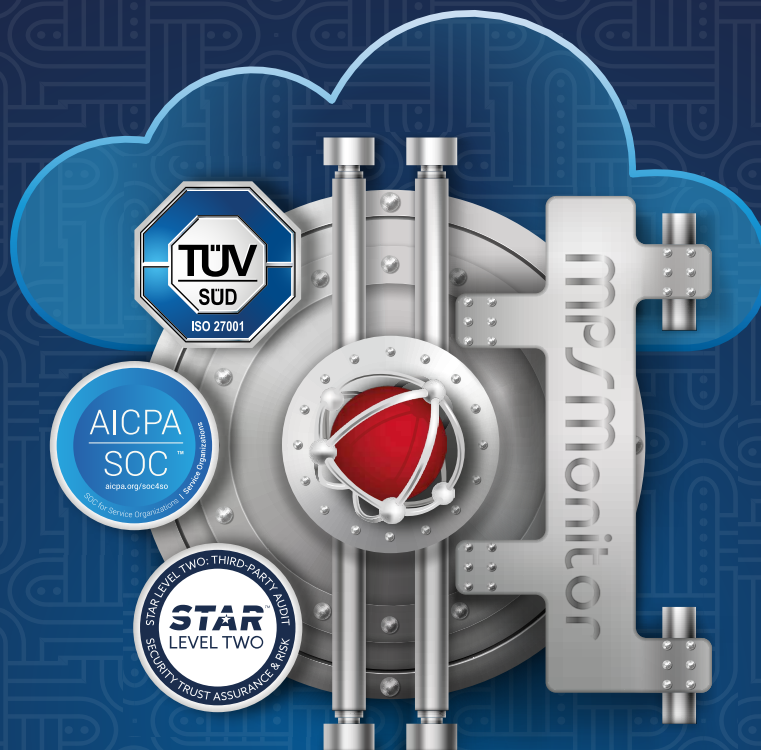
L'HP SDA utilizza la porta 12351 per stabilire una comunicazione HTTPS con il JetAdvantage Management Connector (JAMC).

Per maggiori dettagli sull'HP Smart Device Agent, consulta la «**HP Smart Device Agent for USB Connected Printers User Guide**» disponibile nel portale MPS Monitor.



6 Documenti di riferimento

-  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



***Stampa questo documento
solo se necessario, grazie.***



MPS Monitor supporta da diversi anni il programma
PrintReleaf, contribuendo alla riforestazione
a livello globale.



*MPS Monitor è un marchio registrato.
Tutti i marchi mostrati appartengono ai rispettivi legittimi proprietari.*





Contattaci all'indirizzo
info@mpsmonitor.com

Richiedi una prova su
www.mpsmonitor.com

*Preparati al tuo viaggio in totale
sicurezza con noi!*

