HP Smart Device Services Security White Paper

Table of contents

Introduction

To enable service delivery cost savings via remote management and predictive services for HP managed device resellers, HP has introduced the HP Smart Device Services (SDS) platform. This whitepaper defines capabilities of the HP SDS platform and describes how it communicates, how HP stores data, and how HP SDS is integrated into MPS management software solutions. The overall security of an MPS management software solution is dependent upon the implementation by the solution provider. For more information on a given MPS management solution, please contact the solution provider.

HP Smart Device Services

The HP Smart Device Services (SDS) platform integrates with the HP JetAdvantage Management (JAM) platform to enable an extended set of capabilities for managed device fleets. For the purposes of this document, the combined capabilities and functionality of both platforms are referred to as HP Smart Device Services. In some cases, specific references to JAM are retained to prevent confusion.

The HP Smart Device Services platform enables remote device management capabilities such as remote reboot, firmware upgrade, diagnostics, and configuration to minimize the number of on-site service visits by HP managed product service technicians. Also, the HP SDS platform enables predictive service capabilities such as part replacement and training on demand which reduce the time required to perform a service. This enables HP managed product resellers to optimize their service visits and maximize their first-time fix rate.

HP SDS Platform Components

The HP SDS platform consists of four components:

1. HP JetAdvantage Management Connector (JAMC). The HP JetAdvantage Management Connector, HP's data collection agent (DCA), is installed on a machine at the customer's site and communicates with print devices and with the JetAdvantage Management platform.
2. HP Smart Device Services (SDS). The Smart Device Services platform is hosted on Amazon Web Services (AWS) servers and maintains the data, settings, and business logic of printer fleets, account configuration information, and can communicate with MPS management solutions
3. An MPS management software solution that has HP SDS functionality enabled.
4. HP Smart Device Agent (SDA), an optional component for managing USB-connected devices. The SDA runs on the PC where the device is attached.

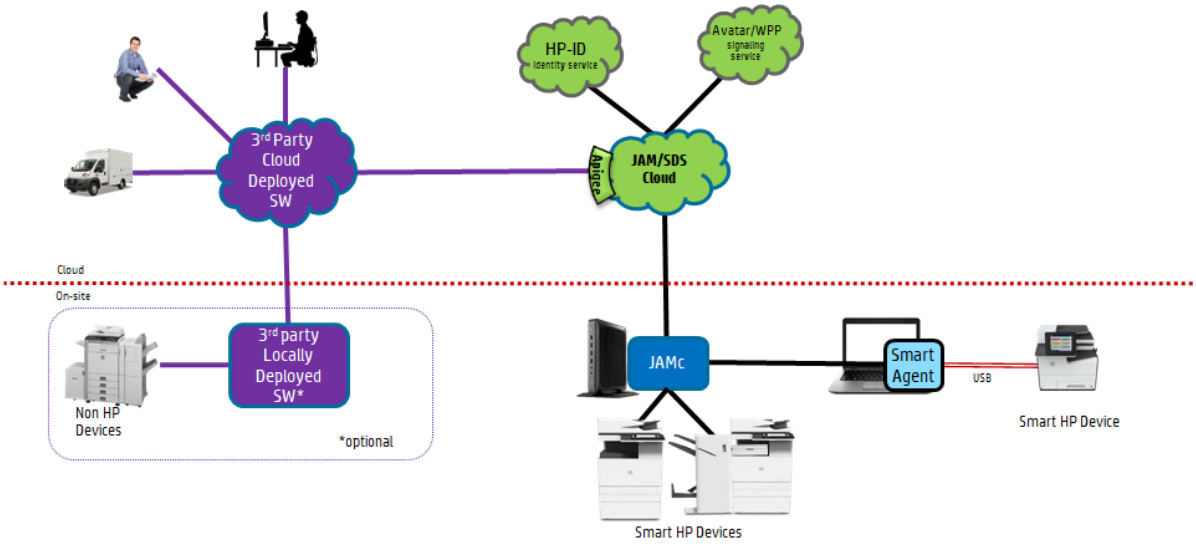
Platform Architecture

The HP Smart Device Services Platform is hosted on Amazon Web Services Cloud (AWS) servers. The full solution includes third party cloud and locally deployed software as well as the JetAdvantage Management Connector which communicate via the Internet. The diagram below shows how HP Smart Device Services and the MPS management software solutions communicate. Users of the MPS management solution rely on the user interface of the MPS software solution and do not interact with the HP Smart Device Services platform directly.

- The MPS management software interacts with HP Smart Device Services platform via a secure interface.
- HP Smart Device Services communicates with the HP JetAdvantage Management Connector which in turn communicates with a fleet of devices at the customer location.
- This JetAdvantage Management Connector software can run on either a customer server or an HP appliance that also hosts other management applications. The communication protocols used to facilitate cloud-based device management are discussed later in this document.

The HP Smart Device Services platform infrastructure consists of multiple servers (also known as a stack) that comprise working parts of the overall system. Examples of major components in the working system are load balancers, application servers, HP Smart Device Services platform servers, and database infrastructure. An HP controlled identity management system authenticates user identity access to the portal interface and a keyed registration process

establishes secure communication between the data connectors and the application. Customer data is secured in a database infrastructure and sensitive details are encrypted using standard practices.



Regional Support

HP Smart Device Services stacks are hosted on Amazon Web Services systems in both the US and EU. The EU-based stack is located in Frankfurt, Germany. Any personal data gathered is governed by the HP Privacy Statement. As a worldwide solution, some unique device identifiers are transferred between our European and Asian platforms to our centralized United States platform to ensure reliability and performance of our overall products and services.

Port Information

The HP JetAdvantage Management Connector requires access to various ports on both the Internet and the local intranet where it is installed. The following table describes each of these ports.

Ports Legend	
Legend	Description
I	Internet port The port with which HP JetAdvantage Management Connector communicates at HP.
i	intranet port This port is located usually inside your firewall, not Internet.
L	Local port The port at the HP JetAdvantage Management Connector host.
R	Remote port The port is outbound with respect to HP JetAdvantage Management Connector host, this host uses a Windows assigned source port

NOTE: Adding the application's path "%ProgramFiles(x86)%\HP JetAdvantage Management\HP JetAdvantage Management Connector\HP.Fms.Connector.Service.exe" to a local firewall list of allowed application rules might be necessary in order to communicate with an HP JetAdvantage Management Connector.

Ports used in HP JetAdvantage Management				
Port	i/I	L/R	UDP/TCP	Description
161	i	R	UDP	HP JetAdvantage Management and other management applications use SNMP to communicate with and manage devices. HP JetAdvantage Management uses this port on the printer to issue Set and Get commands to the SNMP agent.
427	i	L/R	UDP	Service Location Protocol (SLP) communication to and from the printing device go through this port for the purpose of Automatic discovery.
443	i	R	TCP	HP JetAdvantage Management uses this port to discover and manage LaserJet Pro Series and Business Ink (secure).
443	I	R	TCP	HTML communication using SSL/TLS communication are directed to this port on the Internet-facing JetAdvantage Management servers*
3329	i	R	TCP	HP JetAdvantage Management uses this port to support the Device Announcement Agent feature on devices.
3702	i	L/R	UDP	HP JetAdvantage Management uses this port to perform a Web Services discovery on newer HP devices.
3910	i	R	TCP	HP JetAdvantage Management uses this port during discovery and device management.
3911	i	R	TCP	HP JetAdvantage Management uses this port during discovery and device management.
7627	i	R	TCP	HP JetAdvantage Management uses this port to manage communications on some newer HP devices.
8080	i	R	TCP	HP JetAdvantage Management uses this port to discover and manage LaserJet Pro Series and Business Ink (non-secure).
12351	i	L/R	TCP	Smart Device Agent (SDA) clients and Real-time eventing over TLS

JAMC prefers TLS if available. The TLS version used is determined during the TLS negotiation with the device. JAMC will negotiate in this order: TLS 1.2, 1.1, 1.0, then, if the device only supports it, SSL2

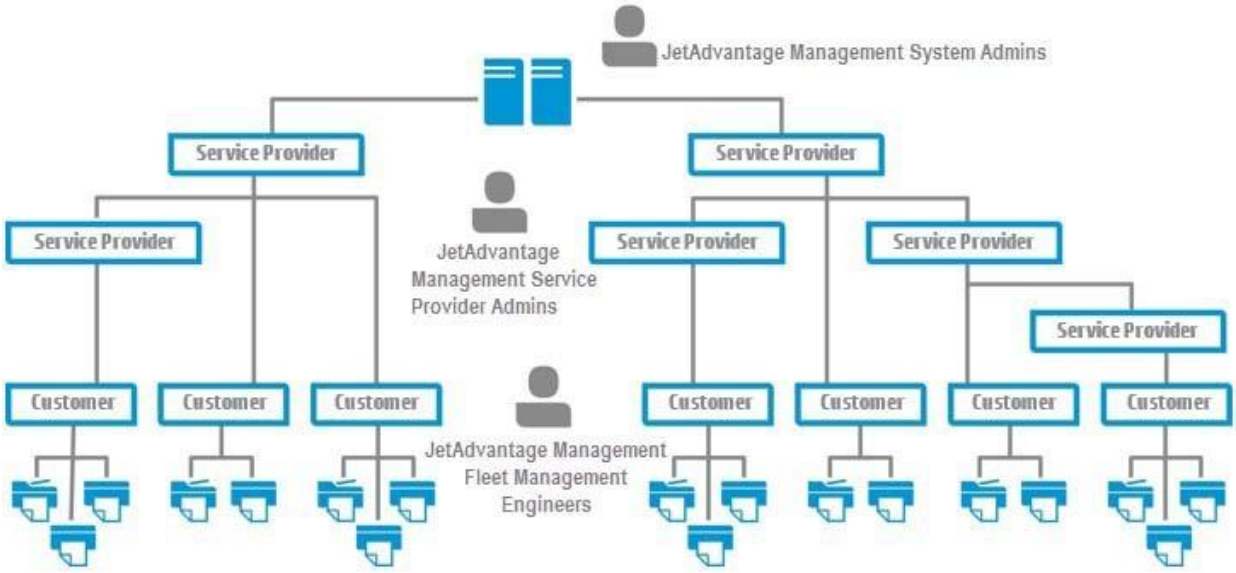
Between JAMC and JAM, a negotiation also occurs but it should always result in TLS 1.2 being used as both JAMC and JAM are configured to support it.

Note that JAM does not support SSL3; so, if a client only supports SSL3, the TLS connection will fail.

Customer Data Partitioning

HP JetAdvantage Management Platform is a multi-tenant system in that it can support multiple entities of both Service Providers and Customers. The customer name is not identifiable in HP JetAdvantage Management Platform. Customer is only identified in the system with information provided by the user of the platform (e.g. they may choose to only provide a globally unique identifier (GUID) as this identifier if desired).

The following diagram shows the hierarchical structure used to separate these entities. Only systems with the proper authentication can access service providers and customer data.



The HP JetAdvantage Management Platform assigns a unique identity to each device and links that identity to the HP JetAdvantage Management Platform customer element. This separation defines boundaries maintained between customer fleets and service provider hierarchies.

Data Security

The security of HP customers' devices, data and personal information is a top priority for HP. All communications between the HP JetAdvantage Management Connector and the HP SDS platform are initiated by the connector via the internet and are in a secure session via HTTPS/TLS over port 443. This is an industry standard protocol used by internet browsers and many 3rd party data collection systems. The HP Smart Device Services platform does not use persistent connections or the XMPP protocol. Instead the JetAdvantage Management Connector periodically polls the HP SDS platform for work it needs to perform. The SDS platform securely stores fleet data and settings, account data, and provides secure access via HTTPS/TLS over port 443.

To ensure the security of device data, HP uses secure AES-256 encryption for data at rest. Data in transit is secured through the use of secure encryption (HTTPS). Data is transmitted via TLS 1.1 or higher with an X.509 certificate for authenticity and encryption. HP uses a Class 3 Secure Server certificate signed by VeriSign with a 2048-bit RSA key.

All data gathered by HP is safeguarded per the tenants of the **Online HP Privacy Statement.**

For countries with personally identifiable information (PII) restriction requirements, HP provides regional hosting and does not let PII data leave a given region. For regional hosting information, please contact your HP representative or MPS software solution provider.

- HP Smart Device Services platform is used by HP and our partners to manage customer device fleets.
- Neither the HP JetAdvantage Management Connector nor the HP SDS platform collects customer names.
- HP SDS does not have access to the contents of printed, scanned or stored jobs.
- HP will not sell, rent, or lease any information without your company's express consent.

- HP retains customer data on the HP SDS platform for 10 years after the customer or HP has deactivated the account.
- After account deactivation, customer data is only held in the HP JetAdvantage Management Platform data stores and is not visible outside HP.
- SDS-enabled MPS management solutions must be authenticated with the HP SDS platform to access the data in the HP Smart Device Services system.
- Please contact the solution provider for security information regarding their MPS management solution.

How Managed Product Authorization Works

HP uses managed product authorization to reduce toner and ink cartridge fraud, counterfeiting and cloning. Both counterfeiting and cloning involve copying HP toner and ink cartridges and electronics to receive all the features and messaging as original HP cartridges when used in HP printers and MFPs. Certain key features of HP devices have only been qualified and tested using original HP toner and ink cartridges and can cause undesirable or inaccurate feature performance when used with unqualified counterfeit or cloned products. Counterfeiting also includes copying HP toner and ink cartridge packaging to attempt to market them as original HP products.

HP uses managed product authorization to address fraud similar to how Microsoft uses activation: **https://support.microsoft.com/en-us/kb/302806**. Microsoft is preventing piracy where a single licensed copy their software is shared and installed on multiple computers. HP managed product authorization prevents a single cartridge from being copied, cloned and installed in multiple printers or MFPs.

Managed product authorization is a simple and straightforward process that is completely software based. It requires no hardware add-ons to the printer. It requires the use of an MPS management software solution in conjunction with the HP Smart Device Services platform. The only information required to authorize managed products are product identifiers, toner or ink cartridge identifiers and usage – no print data or user data is collected. The information that is collected during managed product authorization cannot be used to personally identify a customer or their users.

Appendix A – Frequently Asked Questions

Q1: What data is gathered by HP SDS?

A1: The data gathered by HP SDS is outlined in the HP JetAdvantage Management Data Use Statement

Q2: Can I review the data collected by JAMc?

A2: To capture a sample of data collected by JAMC, edit the JAMC configuration file (Windows\ServiceProfiles\NetworkService\AppData\Local\HP\JAMC\config\HP.JAMC.Config.xml) and change the following value from False to True:

<property name="TraceOutgoingCommunications">

<type>String</type>

<value>true</value>

</property>

Then restart the HP JetAdvantage Management Connector service. Data collected from devices is saved in the log file C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP\JAMC\audit\HP.JAMC.Service.communicationAudit.log.

Note: This file can be very large. After collecting / reviewing the data, change value back to false and restart the service.

Q3: Which policies govern HP Data use and transport?

A3: All data gathered by HP is safeguarded per the tenants of the **Online HP Privacy Statement** and **HP JetAdvantage Management Data Use Statement**

Q4: Is HP SDS ISO 27001 certified?

A4: ISO 27001 is a standard created by the International Organization for Standardization (ISO) which deals with Information Security Management. It's a way of making sure that a company managing information is considering the security risks of managing this information effectively. It is not a new standard but one that can be traced back to the British Standard 7799, published in 1995. It essentially provides companies with guidelines to establish and maintain an effective Information Security Management System (ISMS), using a continual improvement approach. HP Inc. applied for this certification back in mid-2016 and after a thorough review received certification in February 2017.

Q5: Does HP SDS meet the EU's General Data Protection Regulation (GDPR) requirements?

A5: As HP, we have a strong program for privacy and data protection and are implementing additional controls to ensure that we have established the compliance framework to meet the GDPR requirements by May 2018. These include controls for managing third parties, enhancing the way we gather individual customer consents and implementing systemic procedures for the way we design our products, services and software.

Q6: Is any device data transmitted to the US from the SDS system in the EU?

A6: Device telemetry data, which includes both usage and device event information, is transmitted to the US. The telemetry services that perform the usage and performance analysis are not hosted in the EU. To ensure privacy, some elements are removed from the telemetry data collected from the device. If configured on the device, the following elements are removed from the data before being sent to the US telemetry service:

- Email addresses
- EWS ResourceURI
- Latitude
- Longitude
- GeoCoordinates

Q7: Within the HP Platform, how is the network connection initiated?

A7: All communications between the JetAdvantage Management Connector and the HP SDS and JetAdvantage platform are initiated by the JAM connector via the internet. The connector periodically polls the JAM platform for work it needs to perform.

Q8: Which network URLs are accessed by HP SDS?

A8: HP SDS accesses the following URLs:

US Production System

- https://jamanagement.hp.com (IPv4, port 443)

European Production System

- https://eu.jamanagement.hp.com (IPv4, port 443)

Certificate Revocation List (HTTP over port 80)

- http://crl3.digicert.com/ssca-sha2-g6.crl
- http://crl4.digicert.com/ssca-sha2-g6.crl

Avatar (An HP backend system that JAMC uses to efficiently check for work to be processed)

- https://connectivity.pod1.avatar.ext.hp.com:443/avatar/v1/entities/connectivityconfig
- https://registration.pod1.avatar.ext.hp.com:443/avatar/v1/entities/credentials

Q9: Which IP addresses are used HP SDS?

A9: The IP addresses used by HP SDS are allocated from a pool of IP addresses managed by Amazon Web Services. HP does not control which IP address is in use, and the IP address may change to accommodate system loads or for other needs.

The best way to determine the current IP address is by using the NSLOOKUP command. To use this NSLOOKUP open a command prompt window and type NSLOOKUP <hostname> and press enter. The NSLOOKUP command will return the IP addresses that correspond with the hostname.

Q10: Which certificates are used for network communication?

A10: The HP Smart Device Services host has the DigiCert CA Root (server) and CA Intermediate certificates installed to the local computer certificate stores. HP JetAdvantage Management Connector uses the same server certificate used by a browser accessing **https://jamanagement.hp.com or https://eu.jamanagement.hp.com**. The Certificate Authorities (CA) that currently meet this criteria are as follows

- DigiCert Global Root CA– G5 (within valid issue and expiration dates – see certificate details).
- DigiCert SHA2 Secure Server CA (within valid issue and expiration dates – see certificate details).

The customer Proxy/Firewall infrastructure must allow communication to/from these two DigiCert Certificate Revocation List URLs using standard HTTP communication over port 80: **http://crl3.digicert.com/ssca-sha2-g6.crl** and **http://crl4.digicert.com/ssca-sha2-g6.crl**.

HTTPS communication, which is simply HTTP over TLS (TLS 1.1 or higher) uses an X. 509 certificate for authenticity and encryption. The certificate is used to establish a one-way trust between clients and the HP Smart Device Services platform server. Clients trust the server if the server's certificate is valid. Once the HTTPS negotiation starts and communication to/from HP Smart Device Services platform begins, details traversing the network do so in an encrypted state. HP uses a secure server certificate signed by DigiCert with a 2048-bit RSA key.

Q11: Which network ports are used by Smart Device Agent (SDA)?

A11: The SDA Server on JAMC has an accessible Web Server on port 12351 that only supports HTTPS communications. By default, the Smart Device Agent will use **https://hp-print-mgmt:12351** to communicate with the SDA Server. For more information on HP SDA, please see the **HP Smart Device Agent for USB Connected Printers White Paper**

Q12: How is the remote Embedded Web Server (EWS) functionality enabled and protected?

A12: The Remote EWS feature was implemented securely to greatly diminish the possibility of compromises. To use this feature, it must be explicitly enabled via the management software solution as the feature is disabled by default.

The remote EWS feature is only available for HP devices that are connected to a JAM connector via a network connection. Specifically, a remote EWS connection can only be made to an HP device with genuine HP supplies and that is assigned a JAM device ID. Furthermore, device communication is verified prior to establishing a remote EWS connection.

The enablement of the remote EWS feature also requires a whitelist of one of more authorized users. Users not explicitly added to the whitelist will not have access.

Requests for a remote EWS connection have a limited time window before the request expires. Once a request is made and a user initiates a remote EWS browser session there is a limited window of time that the user can access the remote EWS before the session expires. After session expiration, the user must reauthenticate and make a new remote EWS request to continue using this feature.

Q13: Are there additional security considerations to evaluate when adopting HP Smart Device Services?

A13: Please contact your MPS management software solution provider to understand their integration of HP Smart Device Services, the HP JAM platform, and HP JAM connector into their overall solution.

hp.com/go/support

Current HP driver, support, and security alerts
delivered directly to your desktop

April 2018 v 2.0
HP and Channel Partner Viewable