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 data, 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, contact the solution provider.

HP Smart Device Services is ISO 27001 certified.[1] HP Inc. applied for this certification in mid-2016 and after a thorough review, received certification in February 2017.

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.

Key benefits

The HP Smart Device Services platform provides the following benefits:

- Enables remote device management capabilities such as remote reboot, firmware upgrade, diagnostics, and configuration to reduce the number of on-site service visits by HP managed product service technicians.
- Offers more optimized service capabilities, such as part replacement and training on demand which reduces the time required to perform a service. This enables HP managed product resellers to better optimize their service visits and maximize their first-time fix rate.
- Enables predictive part replacement alerts as HP is learning from the collected telemetry data.

HP SDS Platform Components

The HP Smart Device Services platform consists of four components:

- HP JetAdvantage Management Connector (JAMC): The HP JetAdvantage Management Connector, HP's data collection agent (DCA), is installed on a Windows operating system at the customer's site and communicates with print devices and with the JetAdvantage Management platform. Each physical or virtual machine Windows host can run one instance of JAMC and each customer site can support two or more Windows hosts each running JAMC.
- 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 managed device fleets, account configuration information, and can communicate with MPS management solutions.
- HP Smart Device Agent (SDA): SDA is an optional component for managing USB-connected devices. The SDA runs on the Windows PC where the device is attached.
- MPS management platform or other tools required to exercise SDS functionality.
    - HP ID account: The HP ID account is the login ID and password used for authentication into the HP SDS Platform. This account is required for creating a presence on the HP JetAdvantage Management platform.

1 ISO 27001 is a standard created by the International Organization for Standardization (ISO) which deals with Information Security Management.

- For the HP Smart Device Services platform to provide complete SDS capability requires a managed print service (MPS) software solution that has HP SDS functionality enabled. HP has partnered with several Independent Software Vendors (ISVs) that specialize in MPS software solutions. HP has also made available an HP Application Program Interface (API) for all MPS software developers that provides documentation and code examples on how to implement SDS functionality into their management software solutions.

Platform Architecture

The HP Smart Device Services Platform is hosted on Amazon Web Services Cloud (AWS) server stacks. Located both in the United States and Germany, JAMC connects to only one cloud server stack which can be a defined default of the ISV/MPS software or optionally selected during setup. The full solution may include third party cloud and locally deployed software as well as the JetAdvantage Management Connector which communicates via the Internet.

NOTE: Users of the MPS management solution rely on the user interface of the ISV/MPS software solution and do not interact with the HP Smart Device Services platform directly.

The following illustration (Figure 1) shows a common model of how HP Smart Device Services and the MPS management software solutions communicate.

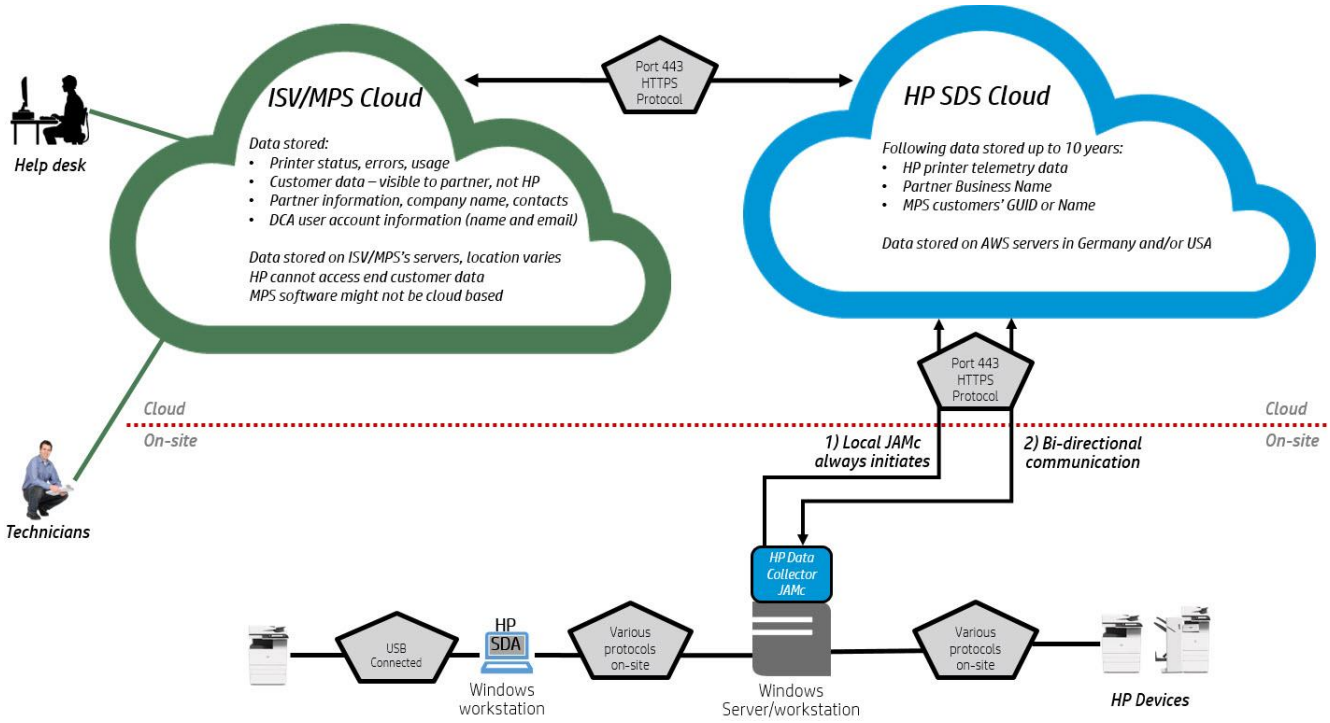

Figure 1: Communication between the HP SDS and MPS software solutions

- The ISV/MPS management software interacts with HP Smart Device Services platform via a secure connection as all communications are encrypted. The stored data is encrypted and HP-ID authentication is required when accessing the HP Smart Device Services platform.
- 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.

HP ID registration information is secured in a database infrastructure and sensitive details are encrypted using standard practices with the current encryption mechanism based on AES-256 encryption.

Data Collection Flow

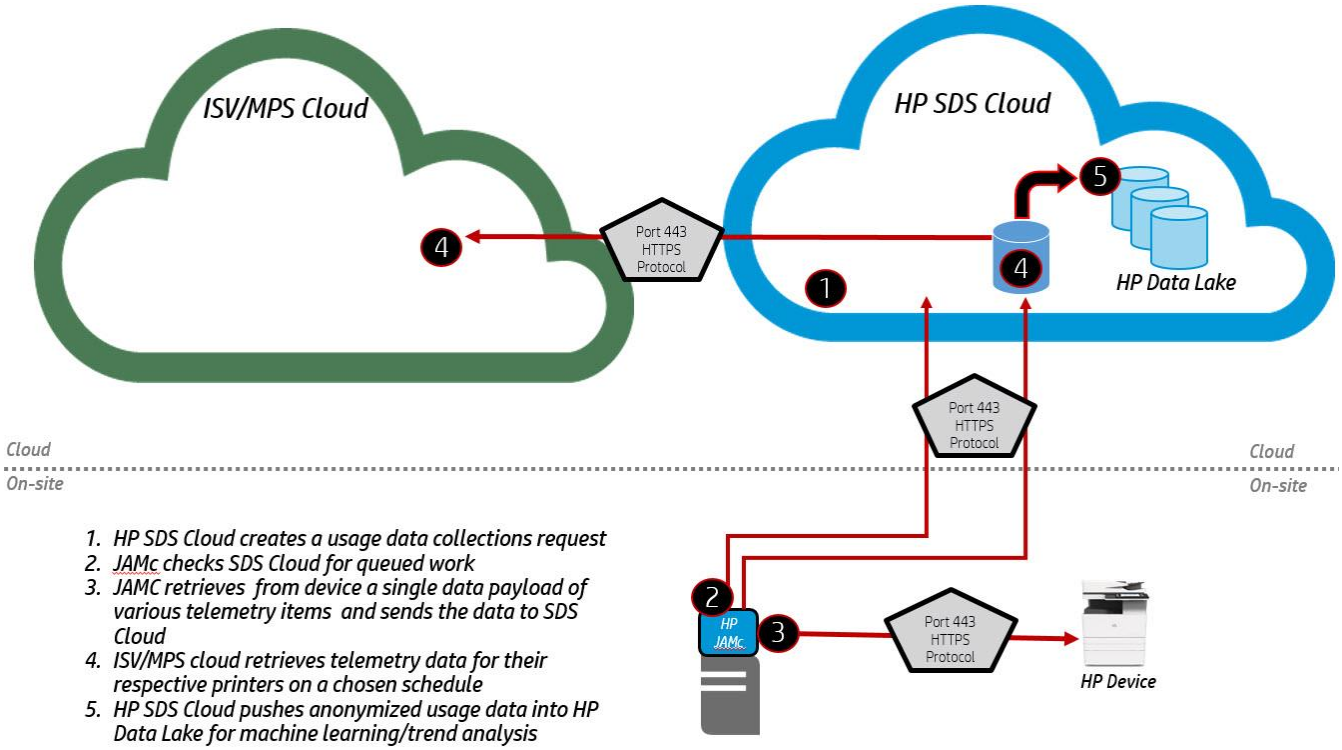

Figure 2: HP SDS Data Collection

To track device performance, HP collects telemetry data which includes device information, software registration, and user registration data. Device data is collected by JAMC connecting to the HP device which provides single file collection of all printer data that JAMC sends to the HP SDS Cloud. Any data gathered is governed by the HP Privacy Statement. Telemetry data collected by JAMC can be viewed by following the steps defined in the FAQ section. The HP Smart Device Services customer (Channel Partner) acknowledges and ensures that the end-user customer is aware of, and consents to, the following data collection parameters outlined in the HP JetAdvantage Management Data Use Statement, (effective as of May 2018) which includes:

- Information about devices such as model number, serial number including additional unique device identifiers, network connection information, administration information, firmware version, control panel language, date installed, number of pages printed, media used, ink or toner metrics and identifiers, and device configuration.
- Information about solutions that are installed on devices, such as solution name and version.

- Information about device events, such as errors and warnings.
- Information used to register and support the software installation, such as support contact information, and internet connection information.
- Information used to register and authenticate users, such as user contact information.

NOTE: No printed content from a print job is collected.

Firmware Update Flow

HP Smart Device Services enables for remote reflash and upgrade of HP released device firmware.

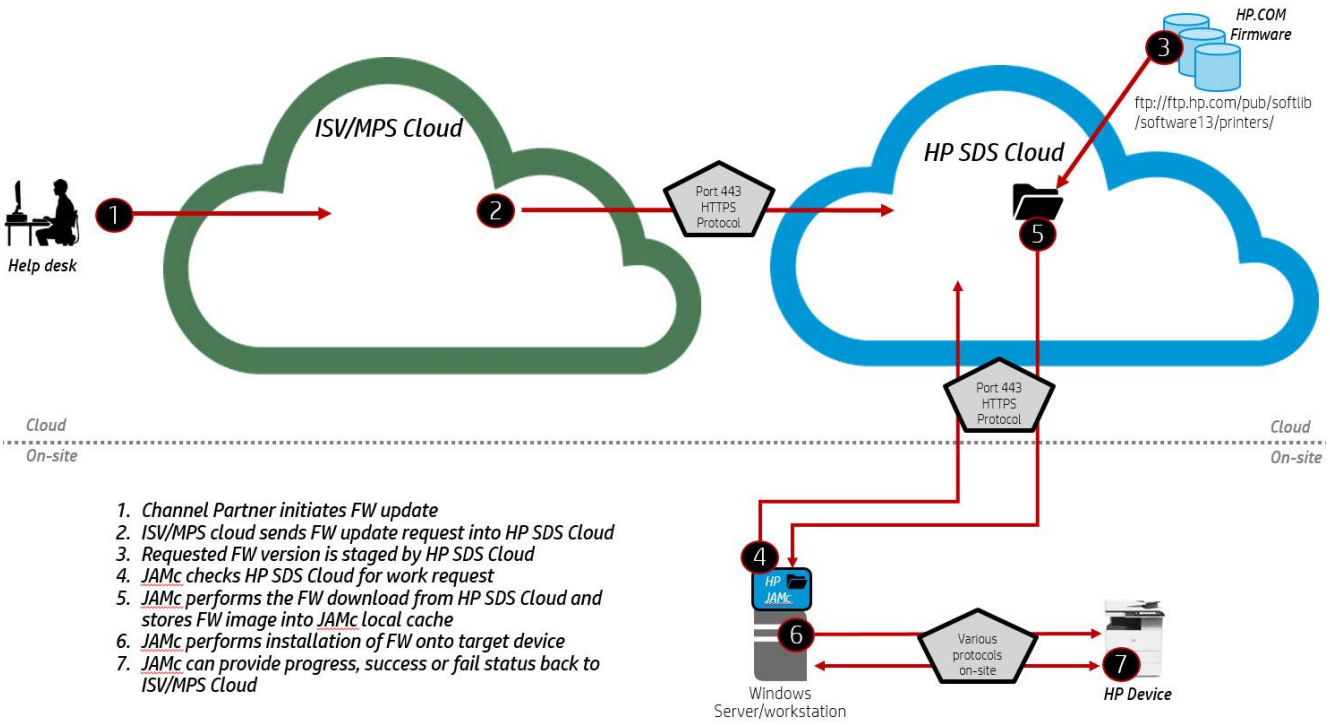

Figure 3: Firmware update flow

The ISV/MPS Cloud requests a list of supported firmware versions from the SDS Cloud. The ISV/MPS Cloud then requests a firmware update to the SDS Cloud for a specific firmware version. The SDS Cloud requests a firmware update to the JAMC (connector) and the connector downloads the firmware version from the SDS Cloud. When the firmware is downloaded, JAMC pushes the new firmware version to the device and polls the device until the device has been fully updated. After the firmware is updated, JAMC notifies the SDS Cloud of the firmware update success which the ISV/MPS Cloud can poll for status updates.

NOTE: All firmware packages applied by JAMC are secured and signed by HP.

Remote Embedded Web Server (EWS)

HP Smart Device Services enables remote access to the device's embedded web server. To use this feature, it must be explicitly enabled via the management software solution as the feature is disabled by default.

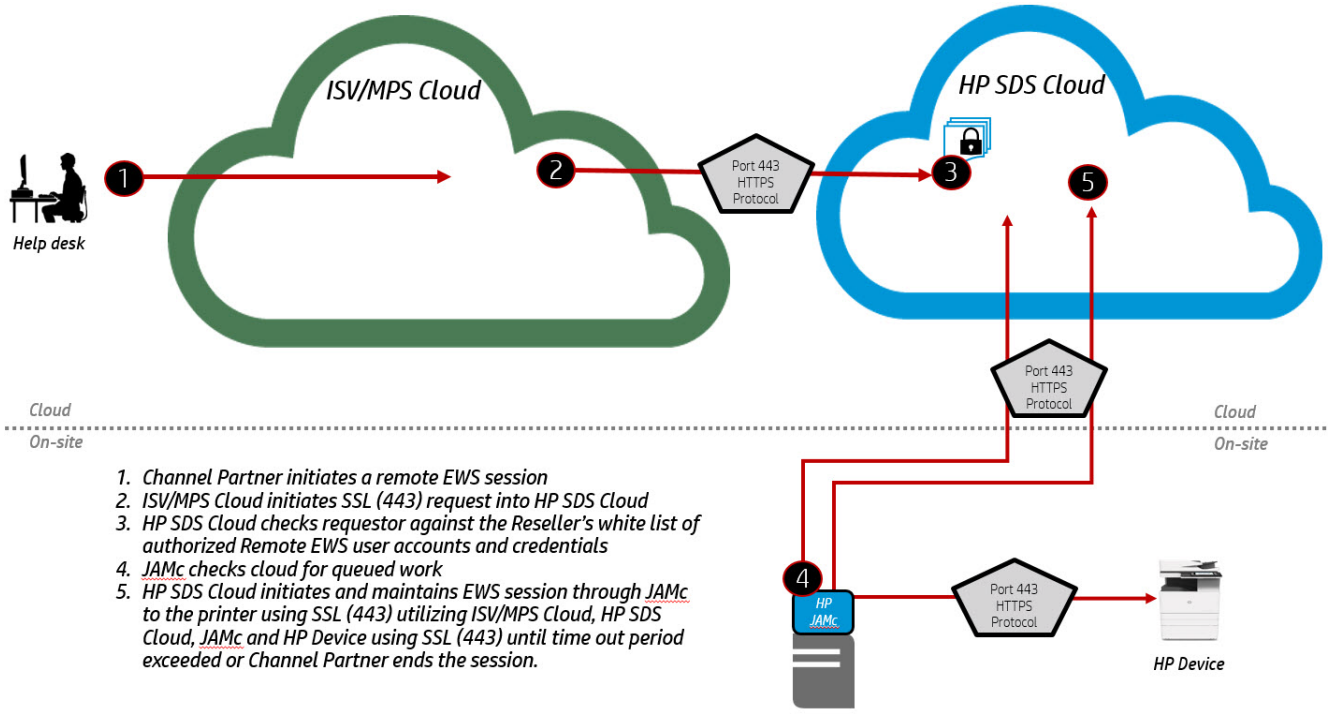

Figure 4: Remote EWS

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 HP SDS platform enablement of the remote device EWS feature defaults to disabled. If enabled, the option exists in the HP SDS platform to require a whitelist of one of the 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. When 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 the session expiration, the user must reauthenticate and make a new remote EWS request to continue using this feature.

The ISV/MPS Cloud initiates an Embedded Web Server (EWS) request to the SDS Cloud which then initiates a connection request to the device via the on-premise JAMC. When the connection is established, all further browser or ISV/MPS Cloud requests pass directly through the SDS Cloud to JAMC direct to the device.

Regional Data Transfer

HP Smart Device Services stacks are hosted on Amazon Web Services systems in both the United States and European Union. In the European Union, the SDS stack is hosted in Frankfurt, Germany. A third stack in Asia might be added in the future.

As a worldwide solution, some unique device identifiers are transferred between our European platform to our centralized United States platform. Ensuring high levels of reliability and performance of HP's overall products and services, this data transmission is required because the central HP SDS analytics engine that enables usage and performance analysis across the worldwide device population is hosted in the United States. JAMC collects from the device a single data payload which is sent to the SDS stack for data processing. Device data transmitted to the United States includes device identification, usage, supply level, and event information.

To protect privacy, some elements are removed from the data collected from the device. If the following data elements are configured on the device, they will be removed from the data before being sent to the US:

- Email addresses
- EWS ResourceURI
- Latitude
- Longitude
- Geographic Coordinates

Disabling IP Address Collection

Some customers might not want to share the IP addresses with HP.

To disable sharing of IP addresses with HP, follow these steps in the order presented:

1. Modify the JAMC configuration file (Windows\ServiceProfiles\NetworkService\AppData\Local\HP\JAMC\config\HP.JAMC.Config.xml).
2. Add the following property information:

   ```
   <property name="IPAddressIsNotExposed">
           <type>String</type>
           <value>true</value>
   </property>
   ```
3. Restart the HP JetAdvantage Management Connector service.

Port and Protocol Information

The HP JetAdvantage Management Connector requires access to various ports on both the Internet and the local intranet where it is installed. Review the ports listed in Table 1.

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.

The internet communication between JAMC and the cloud is always HTTPS using TLS 1.2.

Table 1: External ports used by HP JetAdvantage Management Connector

Port	Service	TCP	Protocol	Function	Benefit to customer
80	DigiCert certificate Verification	TCP	Hypertext Transport Protocol	Allows JAMC to download a certificate revocation list.	Configures agent to communicate securely using trusted encryption with HP Cloud.
443	HP Device Connect	TCP	Hypertext Transport Protocol (Secure)	Allows JAMC to retrieve instructions from the JetAdvantage Management Platform and report back device data.	Configures agent to communicate securely using trusted encryption with HP Cloud.

Service Provider Partitioning

HP JetAdvantage Management Platform is a multi-tenant system in that it can support multiple entities of both Service Providers and Customers.

The illustration below shows the hierarchical structure used to separate these entities. Only JetAdvantage Management Service Provider Admins with proper HP ID authentication can access their Service Provider and all nested Service Provider(s) and/or Customer(s).

NOTE: Using the same HP ID it is not possible for Service Provider Admins to access Service Providers at the same level or higher levels.

The SDS platform is designed to allow the customer name not to be identifiable in HP JetAdvantage Management Platform. The Customer name for ISV software implementations will be a globally unique identifier (GUID) created by the JetAdvantage Management platform's API is designed to prevent name identification at all levels of account privilege when viewed within the HP JetAdvantage Management Platform.

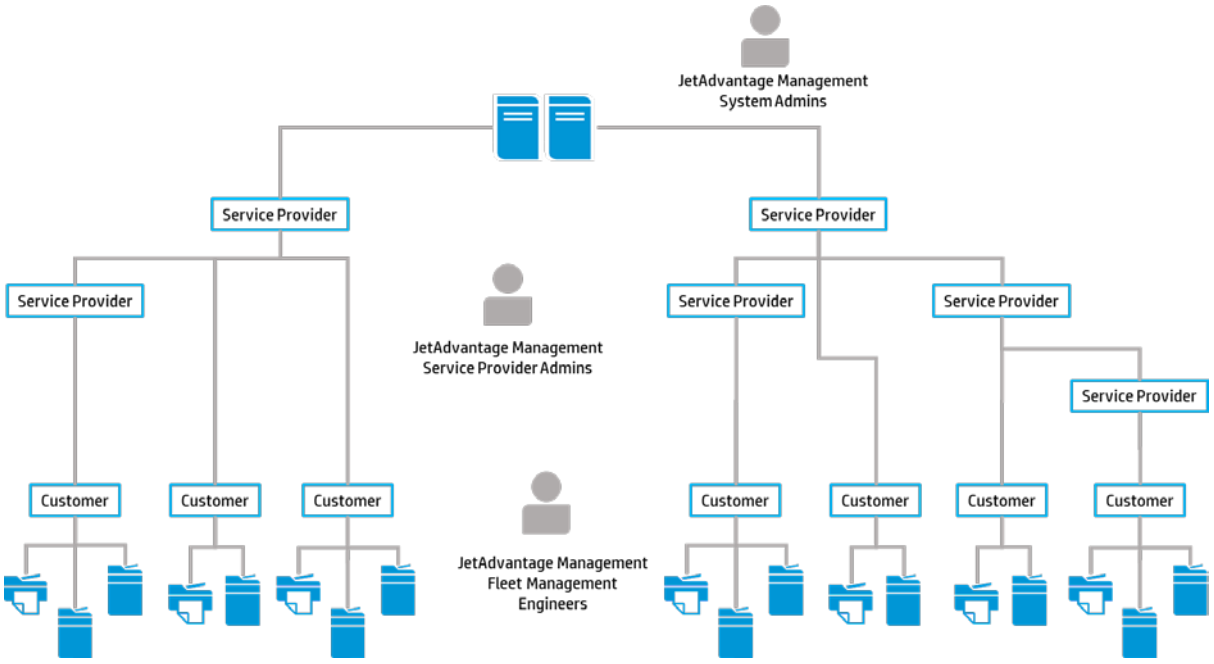

Figure 5: JetAdvantage Management tenant hierarchy

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 an additional boundary 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 third-party data collection systems. The HP Smart Device Services platform does not maintain 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 1.2 with an X.509 certificate for authenticity and encryption. HP uses a secure server certificate signed by DigiCert with a 2048- bit RSA key.

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

- HP Smart Device Services platform is used by HP and our partners to manage customer device fleets.
- When a Customer name entry is created in the HP SDS platform it is obfuscated utilizing a GUID in place of the customer's actual name.
- 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 and device telemetry data on the HP SDS platform for purpose of improving SDS machine learning accuracy for 10 years after the customer or HP has deactivated the account.

- After account deactivation, customer and device telemetry data is only held in the HP JetAdvantage Management Platform data stores and is not visible outside HP. To ensure the security of device data, HP uses secure AES-256 encryption for data at rest.
- 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 validate that the device under MPS management is utilizing original HP toner and ink cartridges. After validating, HP Smart Device Services features are enabled on the device.

Managed product authorization is a simple and straightforward process that is completely software based. It requires no hardware add-ons to the device. It occurs using 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.

An HP device receives authorization via the following steps:

1. JAMC connects to the HP device to collect data.
2. Jetadvantagement.com receives the data and performs the toner and ink cartridge verification process to generate an authorization license.
3. JAMC connects to Jetadvantage.com, receives the generated license, and delivers the authorized license to the device.
4. The above validation process repeats to maintain the device's authorization status.

Appendix A – Frequently Asked Questions

Q1: Can I review the data collected by JAMC?

A1: To capture a sample of data collected by JAMC, follow these steps

1. Edit the JAMC configuration file (Windows\ServiceProfiles\NetworkService\AppData\Local\HP\JAMC\config\HP.JAMC.Config.xml)
2. Change the following value from "False" to "True".

   <property name="TraceOutgoingCommunications">

   <type>String</type>

   <value>true</value>

   </property>
3. Restart the HP JetAdvantage Management Connector service.
4. Data collected from devices is saved in the log file:

   \Windows\ServiceProfiles\NetworkService\AppData\Local\HP\JAMC\audit\HP.JAMC.Service.communicationAu dit.log.

   NOTE: This file can be very large.

   After collecting or reviewing the data, make sure to change the value back to "False" and restart the service.

Q2: Which policies govern HP Data use and transport?

A2: All data gathered by HP is safeguarded per the tenants of the Online HP Privacy Statement and HP JetAdvantage Management Data Use Statement. Device data gathered by JAMC could include open text fields supplied by option of the device owner or maintainer (ie-printer's "Description" and "Contact").

Q3: Is HP SDS ISO 27001 certified?

A3: Yes. 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.

Q4: Does HP SDS meet the EU's General Data Protection Regulation (GDPR) requirements?

A4: Yes. At 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.

Q5: Within the HP Platform, how is the network connection initiated?

A5: All communications between the JetAdvantage Management Connector and the HP SDS and JetAdvantage platform are initiated by the JAM connector via the internet over an https connection on port 443 using TLS1.2. The connector periodically polls the JAM platform for work it needs to perform.

Q6: Which network URLs are accessed by HP SDS?

A6: 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

HP Signaling (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

Q7: Which IP addresses are used HP SDS?

A7: 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.

Q8: Which certificates are used for network communication?

A8: 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 1.2) 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.

Q9: Which network ports are used by Smart Device Agent (SDA)?

A9: 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

Q10: Does HP SDS require the EWS password?

A10: The EWS password is required for SDS use case functionality. If the managed print provider software has enabled HP JetAdvantage Management/HP SDS but has not provided each device's EWS password JAMC may only collect device data.

Q11: Are there additional security considerations to evaluate when adopting HP Smart Device Services?

A11: 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

© Copyright 2019 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed.

c05646238ENW/ c05783939ENW

Edited: October 2019 (v2.2)