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 Product dealers, HP has introduced the HP Smart Device Services (SDS) platform. This whitepaper defines capabilities of the HP Smart Device Services (SDS) platform and describes how it communicates, how HP stores data, and is being integrated into MPS management tools. The overall security of an MPS management tool will depend on the implementation by the software vendor. For more information on a given MPS management tool, please contact the vendor.

HP Smart Device Services

The HP Smart Device Services (SDS) platform integrates with the HP JetAdvantage Management platform to enable an extended set of capabilities for managed fleets. These capabilities range from device-based functionality such as remote reboot, firmware upgrade, diagnostics, and configuration to minimize the number of on-site service visits by HP Managed product service technicians to more advanced predictive services capabilities such as part replacements, training on demand, and time required to perform a service so HP Managed product dealers can optimize their service visits and maximize their first time fix rate. HP Smart Device Services (SDS) is available through MPS management tool vendors which have integrated the functionality.

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 does require the use of an MPS management tool with HP Smart Device Services enablement. 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.

Your managed product will be authorized via the internet. The HP Smart Device Services platform does all of the work.

How the HP Smart Device Services Platform works

The HP Smart Device Services platform consists of five components: 1. JetAdvantage Management Connector is installed on a machine at the customer's site and communicates with devices and with the JetAdvantage Management platform, 2. JetAdvantage Management platform is hosted on AWS servers, and maintains the data, settings, and business logic of your fleet, the data of your account, 3. HP Smart Device Services, 4. An MPS management tool that has HP Smart Device Services functionality enabled, and 5. HP Smart Device agent to allow monitoring of USB connected printers (optional). The HP Smart Device Services interact with the JetAdvantage Management platform to collect data and perform operations

Data Security

The security of HP customers' devices, data and personal information is a top priority for HP. All communications between the JetAdvantage Management Connector and the HP Smart Device Services platform are initiated by the Connector via the internet and are in a secure session via HTTPS/TLS over port 443. In addition, all communications between the MPS Management tool and the HP Smart Device Services Platform and are in a secure session via HTTPS/TLS. This is an industry standard protocol used by internet browsers and many 3rd parties in the 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 Smart Device Services platform for work it needs to perform. The Smart Device Services platform securely stores fleet data and settings, account data, and provides secure access via HTTPS/TLS over port 443. The implementation by each MPS Management tool will differ - customers will want to work with their ISV to understand the security of their overall solution.

All data gathered by HP is safeguarded per the tenets of the **Online HP Privacy Statement**.
For countries with PII restriction requirements, regional hosting is provided and does not let PII data leave a given region. For regional hosting information, please contact your MPS fleet management tool vendor.

- HP Smart Device Services platform is used by HP and our partners to help manage customer printer and multifunction device fleets.
- Neither the HP JetAdvantage Management Connector nor the HP Smart Device Services platform collects customer names keeping your customer's privacy.
- Smart Device Services enabled MPS management tools are required to authenticate in order to access the data in the HP Smart Device Services.
- HP Smart Device Services platform does not have access to the contents of what your company's employees print or to your company's stored documents.
- HP will not sell, rent, or lease any information without your company's express consent.
- HP retains HP Smart Device Services platform customer data for 10 years after the customer or HP has deactivated the account.
- After account deactivation, customer data is only held in HP JetAdvantage Management Platform data stores and is not visible outside HP. The data retention policies of an MPS management tool will depend upon the implementation by the software vendor. For data retention policies on a given MPS management tool, please contact the vendor.

The overall security of an MPS management tool will depend on the implementation by the software vendor. For security information on a given MPS management tool, please contact the vendor.

hp.com/go/support

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

August 2017 v 1.0
Public