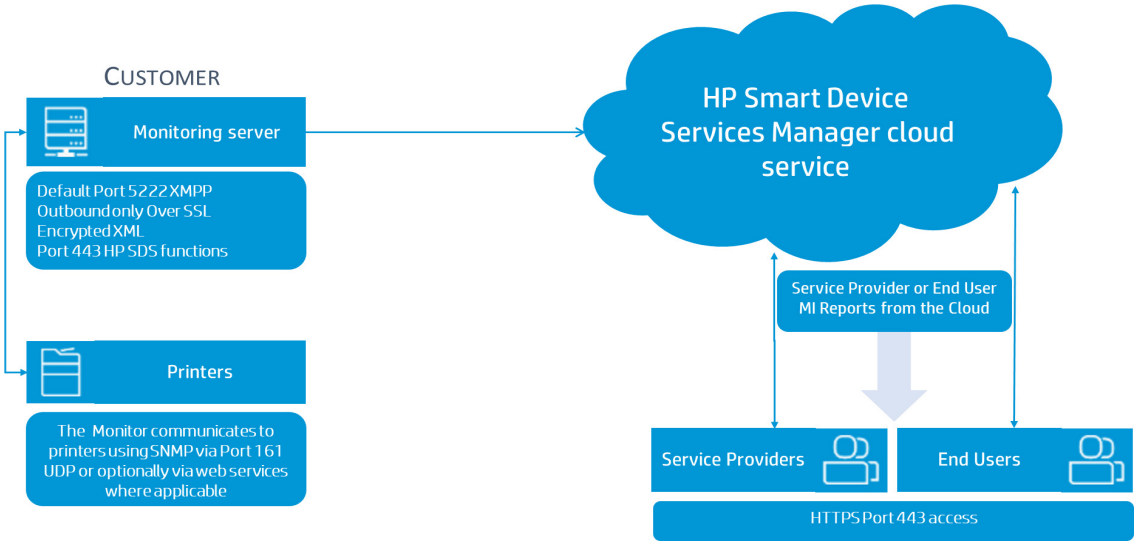
Security white paper

HP Smart Device Services Manager Data, security, and protocols

Table of contents

Ensuring safe, reliable remote print service delivery



Secure real-time print service management

HP Smart Device Services Manager is a real-time continuous service management solution that provides efficient and effective print service management from a central location. This is available to service providers over the Internet as a cloud service, reducing costs for their customers while maintaining exceptionally responsive service delivery and service quality.

To provide this highly responsive service, it is critical that information is sent securely and reliably to the central service management system in near-real-time. This ensures that customer print service management requirements are met, facilitating timely deliveries of consumables and associated services.

This white paper discusses the technologies used to provide secure and reliable data transmission and the steps taken to meet the most stringent security expectations of corporate customers in delivering a highly reliable and comprehensive print management service.

Specialized industry-standard protocol for real-time communication

To achieve the requirements of security and the provision of real-time service information for decision support, the system uses a specialized, highly secure, industry-standard data transmission protocol. This has been specifically designed for real-time data communication. It is called XMPP and it transmits encrypted XML information securely over SSL with extra encryption applied by the application to further enhance security.

Low overhead, fast and secure

Data messages are small, therefore extremely fast with very low overhead, ensuring effective scalability. The protocol is a point of presence protocol, meaning that both the transmitting server and the recipient server must be present and securely authenticated before data transmission can take place, maintaining both security and data integrity.

The presence requirement and the encryption virtually eliminate the possibility of a man-in-the-middle attack. As implemented within HP Smart Device Services Manager, all data transmission is outbound only from customers' servers, meaning *no connections* are made within your network that are initiated from outside of your controlled and secure environment.

This same technology is used by NATO for secure real-time communication between systems, applications, and people where required.

Industry-standard technology

XMPP is an industry standard defined by the Internet Engineering Task Force (IETF). In 2004, the IETF published RFC 3920 and 3921, officially adding XMPP to the list of Internet standards.

As part of this process, a default computer port was defined by the Internet Assigned Numbers Authority (IANA) for XMPP traffic. This default port is 5222 and is the recommended port to use. Being an IANA-defined port, this should be open by default within firewalls, routers, and switches.

The XMPP protocol is used in secure messaging, cloud printing, network management, and financial trading systems.

HP Smart Device Services Manager will, however, allow you to select an alternative port if required. By default, HP Smart Device Services Manager will attempt to use the defined XMPP port 5222; if this port is not open then HP Smart Device Services Manager can use alternative ports such as port 443. Should you wish to use a different port, please advise your service provider, and HP Smart Device Services Manager can be configured to accept transmissions on your selected port.

Port 5222 is the recommended port, since routers and firewalls expect to see encrypted XML data being sent. Should you wish to use an alternative port, you should ensure that your routers and firewalls will accept encrypted XML over that port.

To support HP Smart Device Services specialized features, port 443 is used for HTTPS traffic. Again, this is outbound-only communication from your network.

Information transmitted

The information sent is only the information required for remote printer service management. This information falls into three core categories: asset data, consumable status data, and service incident or alert data.

The asset data provides core details about each printer asset:

- What it is (make, model)
- Asset identifiers (anonymous database record ID, serial no, MAC address, hostname)
- Location identifiers, both electronic and physical if available within the device (IP address, hostname, physical location or zone name)
- Page counts or meter readings
- Identifier data is only sent once unless a change is detected, then the changed data is sent

The current consumable status information for each printer asset:

- What the consumable item is (toner, ink, drum, waste toner bottle, its color, its description, and an anonymous consumable record ID)
- The consumable(s) status (current level, maximum level, and status codes if applicable)
- Page counts at that status point
- Time and date stamps

The current service alert conditions reported by the printer:

- What the alert is (the description, an anonymous alert record ID)
- The alert details (the alert code, the error code if available, the alert class, the alert severity, the alert training level required to resolve the issue)
- Page counts at that status point
- Time and date stamps

Data collected for feature enhancements and service improvement

To provide further customer value and service improvement, anonymized performance information from printers is collected and analyzed by HP. This builds a knowledge base used to prioritize and develop new capabilities and functionality focused on improving the customer experience, the serviceability of new products, and therefore the value received by customers.

No user or print job data

No user data, no print job data, nor content is collected, recorded, or transmitted by the system.

Cloud server location and data protection

As standard, HP Smart Device Services Manager uses Microsoft Azure cloud computing services. This provides the ability to select the region or country in which your printer service data is stored. Microsoft Cloud computing services have met Europe's stringent data protection rules, one of few companies so far to receive such approval. Microsoft already operates data centers in Amsterdam, Dublin, Frankfurt, and London, allowing European customers to store their data locally. Additional locations may be added over time. The regionalized efforts are likely to become increasingly important, as European policy-makers finalize new data protection and privacy rules, which will come into force during 2018. Microsoft also provides multiple data centers in North America, South America, and Asia Pacific, which are used for our customers operating in those regions and to which we apply our strict data security policies.

Additional information used for service management

Other information that is not transmitted can be associated with the printer data in the central system to facilitate effective service management.

This might include consumable shipping information or key user contact details, device specifications, part numbers, and consumable yields.

In addition, the central system maintains histories of the assets, the consumables used, and service alert conditions raised. These are used in decision support, forecasting, asset management, supply chain, and service chain management information and reporting services.

System protocols and communication ports

The system uses the following protocols and ports:

Protocol	Port	Connection	Function
SNMP	161	Local	Local network print device discovery and monitoring.
HTTPS	443	Local and outbound	To access the HP SDS Manager Cloud Portal server systems and for local operations via web browser. Also used to pass some specific HP SDS data from the monitor to the HP SDS Portal.
HTTP	80	Local and outbound	To monitor some devices that provide their detailed data via web services as opposed to SNMP. To allow the monitor to access and check its license server.
XMPP	5222	Outbound	Passing data from local monitor to the HP SDS Portal servers.

In conclusion

HP Smart Device Services Manager delivers a highly efficient and secure remote print service management solution, enabling your service provider to have full visibility of the status of your printing assets in near-real-time without the need to have remote access into your network. The underlying technologies used for communication are industry standard, flexible, and extensible, making them the protocols of choice for real-time communications over the Internet.

The HP Smart Device Services Manager solution enables the reliable transport of structured XML data between systems. Numerous mission-critical business applications use the XMPP protocol used by HP Smart Device Services Manager, including cloud printing, network management, and financial trading.

Only the data required for efficient print service delivery is collected and transmitted to the central server. No user data or print job content is collected or transmitted.

All central servers are configured to be within the customer's region or country, eliminating risks associated with data protection legislation both now and in the future. With inherent security features, scalability, and support for multi-vendor print services, HP Smart Device Services Manager is more than able to meet the needs of the most demanding environments.

For more information, contact your HP Partner or hpsds@ekmglobal.com

4AA7-0878ENL, August 2017