HP Device Connect – Software Lite:

Security Technical Whitepaper

Software Release Version: 4.4

Document Version: 1.3
Document Release Date: January, 2016
Document Last Update Date: November, 2016
Software Release Date: November, 2016

HP Development Company PROPRIETARY INFORMATION

The information contained in this document constitutes information that is commercial or financial and confidential or privileged and should be considered HP confidential.

The information contained in this document is proprietary to HP, Inc. and is tendered for purposes of review and evaluation only. This document shall not be reproduced, copied or stored in any retrieval system, in whole or in part, nor shall the information contained herein be used by or disclosed to others except as expressly authorized by HP, Inc.

DOCUMENTATION UPDATES

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time this document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To ensure that this is the latest edition, contact the local HP Device Connect representative.

Table of Contents

About this whitepaper

This document describes:

- Security details of “HP Device Connect - Software Lite”.

Document updates may be issued between editions to correct errors or to document product/process changes. To ensure that this is the most recent edition, contact the local HP Device Connect representative.

Intended Audience

This document is intended for administrators responsible for installing and managing “HP Device Connect - Software Lite”. This document is also intended for Operators working on the “Print Fleet Management”. Administrators and Operators are expected to have knowledge of operating systems, networking concepts, and their data center.

This document is also intended for customers who may be interested in understanding the security aspects of “HP Device Connect - Software Lite”

Related Documentation

The following documents provide related information:

- HP JetAdvantage Management documentation

To obtain a copy of the above documents contact the local HP Device Connect representative.

1 Introduction

1.1 Overview

The HP Device Connect - Software Lite (HP DC-SL) is an integrated management platform containing a suite of capabilities that provide a secure and scalable platform for enabling efficient management of an enterprise's printing ecosystem. HP DC-SL will be installed on a customer provided system. Various components will be installed and configured enabling HP to provide previously agreed to services.

The following diagram depicts the HP DC-SL system overview:

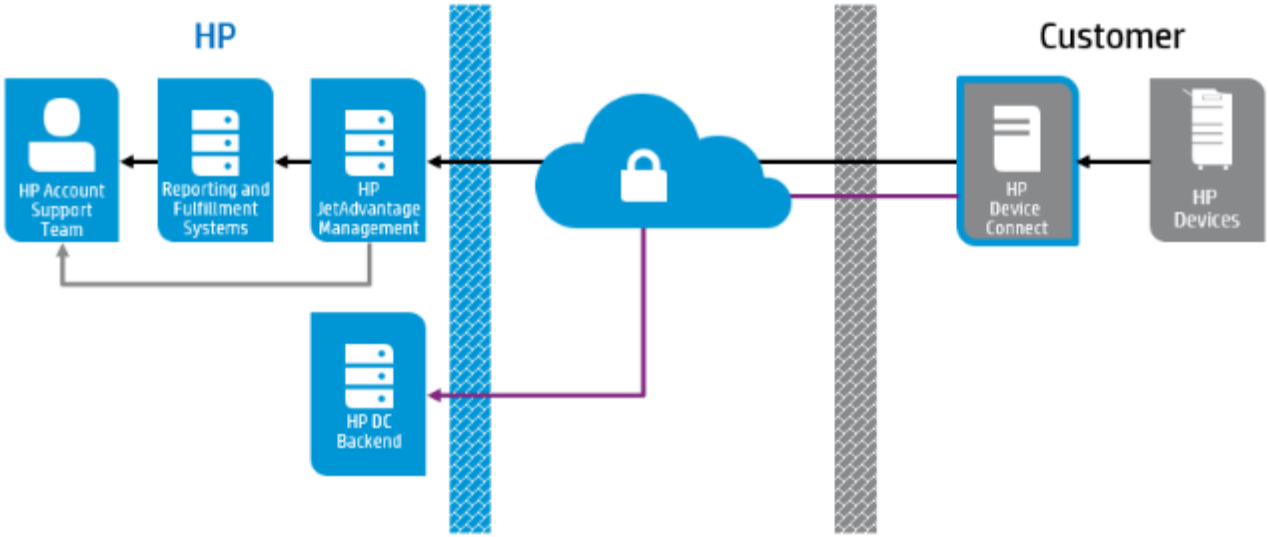


Fig.1: HP Device Connect - Software Lite System Concept

HP DC-SL provides Remote Monitoring and Remote Management functionalities as described below:

1. Remote Monitoring: HP DC-SL enables remote monitoring as a secure means for collecting and reporting usage and device data for consumables replenishment and support.

2. Remote Management: HP DC-SL enables remote management of devices in order to facilitate event troubleshooting, managing limited device configurations, and non-reporting device remediation.

1.2 HP DC-SL Components

The table below outlines the components which make up HP DC-SL.

Function	Enabling Software Component(s)	Version	Description
Remote Monitoring and Management	HP JetAdvantage Management Connector	V1.x	Provides a scalable and highly available platform for device entitlement, remote monitoring of usage and supplies, and management of network connected HP devices.
System Maintenance	HP DC Updater Client	N/A	Update utility for components which do not have built-in update capabilities

2 Security Overview

HP DC-SL security details are provided in the following sections:

2.1 Software Update Management Process

HP DC-SL updates are released broadly on a quarterly basis depending on the updates to the various underlying components. HP DC-SL provides a flexible approach to install the software updates and supports both an automated as well as manual update process.

- Automatic Updates: If automatic updates are enabled, the update installation to the server follows an automated process. Once the auto-update system is registered with the HP backend, the system will automatically check at periodic intervals for availability of updates/patches and install them as and when they become available. The time to check for updates can be determined as per customer convenience and this can be configured in the HP backend.
- Manual Updates: The patch bundles will be made available at HP DC download locations and these can be manually downloaded and installed as per the convenience of the customer. Please contact your HP DC representative for the patch bundle download locations.

2.2 Ports

Internal / External Port Configuration and Firewall Rules

Remote Port	TCP/ UDP	Internal/ External	Inbound/ Outbound	Source	Destination	Description
80/443	TCP	Internal	Outbound	DC-SL	Printer (WS)	HTTP Get
7627	TCP & UDP	Internal	Outbound	DC-SL	Printer (WS)	HTTP-Get
3910/3911	TCP	Internal	Outbound	DC-SL	Printer (WS)	HTTP
3702	TCP & UDP	Internal	Outbound	DC-SL	Printer	HTTP
8080	TCP	Internal	Outbound	DC-SL	Printer	HTTP-Alt
161	UDP	Internal	Outbound	DC-SL	Printer	SNMP Get/Set
9100	TCP	Internal	Outbound	DC-SL	Printer	JetDirect (PDL Data Stream)
53	TCP & UDP	Internal	Outbound	DC-SL	DNS Servers	DNS
427	TCP	Internal	Outbound	DC-SL	Printer	SLP
21	TCP	External	Outbound	DC-SL	ftp.usa.hp.com (15.73.40.56, 15.73.244.52)	HP FTP site for downloading patches.

Remote Port	TCP/ UDP	Internal/ External	Inbound/ Outbound	Source	Destination	Description
80	TCP	External	Outbound	DC-SL	http://svrsecure-g3-crl.verisign.com http://ss.symcb.com/ss.crl	JetAdvantage Management Connector to retrieve certificate revocation list (CRL) for the initial registration process
					http://ss.symcb.com/ss.crl	DC-SL Service retrieves a certificate revocation list (CRL) from the URL: *http://ss.symcb.com/ss.crl* which is embedded in the HTTP certificate downloaded from HP DC Backend. The certificate name and the associated IP address are not HP controlled attributes.

Remote Port	TCP/ UDP	Internal/ External	Inbound/ Outbound	Source	Destination	Description
443	TCP	External	Outbound	DC-SL	www.hpjac.com (15.48.64.209, 15.50.64.106) www.xmpp-hpjac.com (15.48.64.208, 15.50.64.105)	HP JetAdvantage Management backend for device usage, consumable, telemetry, and event log collection. NOTE: JetAdvantage Management XMPP service requires a persistent TCP/IP connection from JetAdvantage Management Connector software. IP ports - 5222, 5223,443 or 80 - are used to establish this connection directly to HP's XMPP service or, in the case where HTTP proxy is used, JetAdvantage Management connector sends an HTTP CONNECT request. Once established, the connection communicates using TLS protocol and becomes the JetAdvantage Management control communication channel.
					https://mgtsmcservice.hp.com (15.48.65.22)	HP DC backend for automatic system updates
3389	TCP	Internal	Inbound	Internal Desktop network		

Note: ICMP Echo response from printer needs to be allowed to reach DC.

2.3 Communication Protocols

2.3.1 HP JetAdvantage Management

HP JetAdvantage Management is a scalable, cloud-based printer management tool that HP uses for the purpose of managing fleets of printers. HP Information Technology (IT) hosts HP JetAdvantage Management on server infrastructure known as Next Generation Data Center (NGDC). The application is

made available to users through an Internet-hosted portal so there is no client software to download or upgrade. The portal is a browser-based interface and can be accessed from Chrome, Firefox, or Internet Explorer 9 or 10. There is also no server software for the customer to load aside from a lightweight application named JetAdvantage Management connector that facilitates communication between fleets of customer networked devices (printing and multifunction printing) and the JetAdvantage Management application. Internet load balancers are used to manage traffic between both client browsers and the JetAdvantage Management connectors and the application infrastructure. Dedicated team members in HP IT update the servers that support the infrastructure as well as the working/stored data. No customer upgrades are needed aside from maintenance on desktop hosts running the browser and systems where JetAdvantage Management connector is installed. The remainder of this document describes JetAdvantage Management security.

HP IT and development teams work together to protect confidentiality, integrity, trust, and availability of all HP JetAdvantage Management resources. HP JetAdvantage Management development includes a software security strategy that adheres to an overall HP development security policy and encompasses these key security practices: training, design, development, test/audit, and deploy.

JetAdvantage Management uses SSL/TLS to provide security when transmitting or receiving data. This is also known as HTTPS communication, which is simply HTTP over SSL/TLS using an X.509 certificate for authenticity and encryption. Once the HTTPS negotiation starts and communication to/from JetAdvantage Management begins, details traversing the network do so in an encrypted state. HP uses a Class 3 Secure Server certificate signed by VeriSign with a 2048-bit RSA key. Both JetAdvantage Management client communication and JetAdvantage Management connector communication traverse the Internet using SSL/TLS communication, meaning the communication is authenticated and encrypted.

NOTE: JetAdvantage Management XMPP service requires a persistent TCP/IP connection from JetAdvantage Management connector software. IP ports - 5222, 5223,443 or 80 - are used to establish this connection directly to HP's XMPP service or, in the case where HTTP proxy is used, JetAdvantage Management connector sends an HTTP CONNECT request. Once established, the connection communicates using TLS protocol and becomes the JetAdvantage Management control communication channel.

- Firewall Rules

HP JAM	www.hpjac.com	15.48.64.209 15.50.64.106
HP JAM	www.xmpp-hpjac.com	15.48.64.208 15.50.64.105

HP JAM	http://svrsecure-g3-crl.verisign.com http://ss.symcb.com/ss.crl	JetAdvantage Management connector retrieves a certificate revocation list (CRL) from the URL: *http://svrsecure-g3-crl.verisign.com* / *http://ss.symcb.com/ss.crl* which is embedded in the HTTP certificate downloaded from JetAdvantage Management. The certificate name and the associated IP address are not HP controlled attributes.

Note: Please contact your DC representative to obtain a copy of HP JetAdvantage Management security whitepaper for more detailed security information

2.3.2 HP DC Backend

HP DC backend is a scalable, cloud-based management tool that HP uses for the purpose of managing instances of DC. HP Information Technology (IT) hosts HP DC backend on server infrastructure known as "HP IT Cloud Services". There is also no server software for the customer to load aside from a lightweight application named "HP DC Client Service" which communicates with the HP DC backend to manage the instance of HP DC-SL. Internet load balancers are used to manage traffic between DC Service and the application infrastructure. DC support team updates the servers that support the infrastructure as well as the working/stored data in HP IT Cloud. No customer upgrades are needed aside from systems where DC Service is installed. The remainder of this document describes HP DC backend security.

HP IT and development team work together to protect confidentiality, integrity, trust, and availability of all HP DC backend resources. HP DC backend development includes a software security strategy that adheres to an overall HP development security policy and encompasses these key security practices: training, design, development, test/audit, and deploy.

HP DC backend uses SSL/TLS to provide security when transmitting or receiving data. This is also known as HTTPS communication, which is simply HTTP over SSL/TLS using an X.509 certificate for authenticity and encryption. Once the HTTPS negotiation starts and communication to/from HP DC backend begins, details traversing the network do so in an encrypted state. HP uses a Class 3 Secure Server certificate signed by VeriSign with a 2048-bit RSA key. HP DC Client Service communication traverse the Internet using SSL/TLS communication, meaning the communication is authenticated and encrypted.

- Firewall Rules

HP DC backend	https://mgtsmcservice.hp.com	15.48.65.22

HP DC backend	http://ss.symcb.com/ss.crl	DC Service retrieves a certificate revocation list (CRL) from the URL: http://ss.symcb.com/ss.crl which is embedded in the HTTP certificate downloaded from HP DC backend. The certificate name and the associated IP address are not HP controlled attributes.

Note: All three components i.e HP DC Backend, DC Service and DC Portal have undergone HP security reviews such as CATA and ASTA.

2.4 HP DC-SL Auto Update Duplex Communication

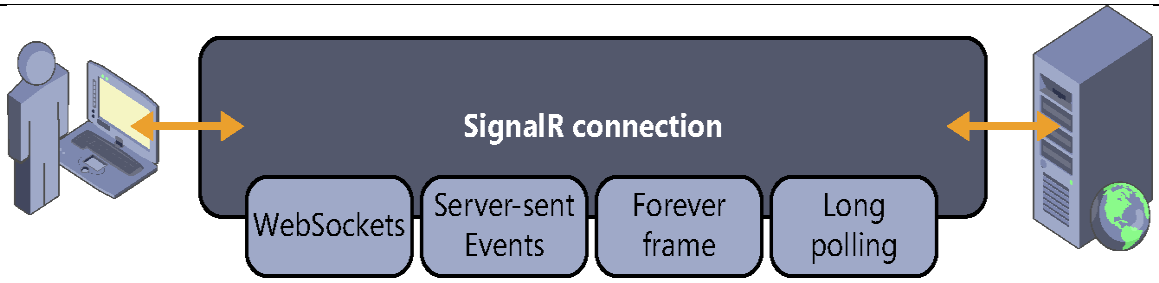
HP DC Auto Update system enables the HP DC-SL to be updated automatically without any human intervention. As part of auto update system, HP DC Client Service establishes a duplex communication with HP DC Backend. This duplex communication enables the HP DC Backend to communicate to the HP DC Client Service any time when there is a change in configuration or any message to be notified immediately. This communication is using SignalR framework.

2.4.1 SignalR Overview

SignalR is an abstraction over some of the transports that are required to do real-time work between client and server. SignalR provides a simple API for creating server-to-client remote procedure calls (RPC) that call Client functions from server-side .NET code. SignalR handles connection management automatically, and lets Server broadcast messages to all connected clients simultaneously. Also Server can send messages to specific clients. SignalR supports "server push" functionality, in which server code can call out to client code using Remote Procedure Calls (RPC), rather than the request-response model common on the web today.

Transports

SignalR includes components specific to both ends of communication, which will facilitate message delivery and reception in real time between the two. SignalR is in charge of determining which is the best technique available both at the client and at the server (long polling, forever frame, WebSockets, and so on) and uses it to create an underlying connection and keep it continuously open, also automatically managing disconnections and reconnections when necessary as shown in the figure below



SignalR includes an "out-of-the-box" set of transports—or techniques to keep the underlying connection to the server open—and it determines which one it should use based on certain factors, such as the availability of the technology at both ends. SignalR will always try to use the most efficient transport and will keep falling back until selecting the best one that is compatible with the context. This decision is made automatically during an initial stage in the communication between the client and the server, known as negotiation.

A SignalR connection starts as HTTP, and is then promoted to a WebSocket connection if it is available. Otherwise it uses either of these protocols: Server Send events, long polling SignalR handles the dispatching across machine boundaries, allowing server to call methods on the client as easily as local methods, and vice versa.

2.4.2 HP DC SignalR Components

HP DC Backend SignalR Hub

HP DC Backend SignalR Hub waits to accept the connection from client instance. Once a client is connected, it can send any message to that client. So in real time, whenever there is a trigger from the Portal for an instance (client), ex. Schedule change, then HP DC Backend SignalR Hub will publish that command or message to that instance immediately.

The default transport it chooses is Server-Sent Events which proposes the creation of a one-directional channel from the server to the client, but opened by the client. That is, the client "subscribes" to an event source available at the server and receives notifications when data are sent through the channel. All communication is performed on HTTP. The only difference with respect to a more traditional connection is the use of the content-type text/event-stream in the response, which indicates that the connection is to be kept open because it will be used to send a continuous stream of events—or messages—from the server.

Next fall back transport is long-polling in which a client maintains a long-held HTTP request, where the server can use to push data to the client without the client specifically requesting it. It is not a persistent connection.

HP DC SignalR Client

HP DC SignalR Client initiates the connection with HP DC Backend SignalR Hub on load. This connection is via HTTPS protocol, which is simply HTTP over SSL/TLS using an X.509 certificate for authenticity and encryption and it is secured. If the connection interrupted the DC SignalR client will retry to reconnect with HP DC Backend SignalR Hub on its own. There is no special port to be opened in the client side as the communication is over HTTPS. There are no inbound and outbound rules to be created in the firewall for this connection. As explained in the 'Transports' section, choosing the underlying protocol is the functionality of the SignalR framework based on the resources available at both ends.

3 Appendix A: Network Traffic

Traffic numbers are available in the documents of the individual application components

Sample average SNMP traffic for 2000 devices

- (HP JetAdvantage Management) * 2000
- (65KB) * 2,000 = 130,000 KB = ~130 MB

Component	Traffic

HP JetAdvantage Management	Data is encrypted and compressed when transmitted
	• Device Discovery
	  ○ Specified address discovery
	  ▪ SNMP query/response from printer = 38 packets, 6.1 Kbytes over 1.1 Sec
	• Data Collection
	  ○ FW/Solutions Data Collection FutureSmart Single Device = 18K Bytes
	  ○ FW/Solutions Data Collection non-FutureSmart Single Device = 10K Bytes
	  ○ Telemetry Data Collection FutureSmart Single Device = 24K Bytes
	  ○ Telemetry Data Collection non-FutureSmart Single Device = 37K Bytes
	The average daily traffic generated per device in the fleet to do a data collection and send the information to HP is:
	  ○ Business InkJet printers: 34KB of internal (SNMP) and 41KB of external (HTTPS)
	  ○ Monochrome LaserJet printers: 33KB of internal (SNMP) and 39KB of external (HTTPS)
	  ○ Monochrome multifunction printer: 33KB of internal (SNMP) and 40KB of external (HTTPS)
	  ○ All-in-one printers: 4KB of internal (SNMP) and 4KB of external (HTTPS)
	  ○ Color LaserJet printers: 65KB of internal (SNMP) and 78KB of external (HTTPS)
	  ○ Color multifunction printer: 91KB of internal (SNMP) and 109KB of external (HTTPS)
	  ○ Edgeline Technology devices: 126KB of internal (SNMP) and 142KB of external (HTTPS)
	  ○ Personal monochrome LaserJet printers: 2KB of internal (SNMP) and 2KB of external (HTTPS)
	  ○ HTTP printers: approximately 80KB of internal (HTTP) and approximately 90KB of external (HTTPS)

Component	Traffic
HP DC Updater Client	Data is encrypted and compressed when transmitted. The data transmission (HTTP request) is usually below 100 KB. Heartbeat data, by default, is scheduled to be transmitted every 60 min. to the HP DC backend. Task schedule request occurs based on the schedule configured in HP DC Portal for the DC Server. On the response it will bring back the configuration data (less than 100KB) and then it will download the 'DC update bundle', if there is any, using BITS technology.

Disclaimer

4AA7-1052ENA, September 2017