HP Device Connect Software Full v6.0.0- Security Technical Whitepaper

Document Version: V-1.0
Document Release Date: February 2019
Document last Update Date: March 2019
Software Release Date: March 2019

HP Inc, 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 Release Version number, which indicates the software version(s) for which this document is applicable.
- Document Last Update Date, which changes each time this document is updated.
- Software Release Date, which indicates the release date of the latest version of the software.

To ensure that you receive the updated or new editions, contact your local HP Device Connect representative.

Table of Contents

List of Figures

List of Tables

1 About this Whitepaper

This document describes:

- Security details of “HP Device Connect”.

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.

1.1 Intended Audience

This document is intended for administrators responsible for installing and managing “HP Device Connect”. 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”

1.2 Related Documentation

The following documents provide related information:

- HP Web JetAdmin (HP WJA) Security Whitepaper
- HP JetAdvantage Security Manager Documentation
- HP JetAdvantage Management (HP JAC) documentation

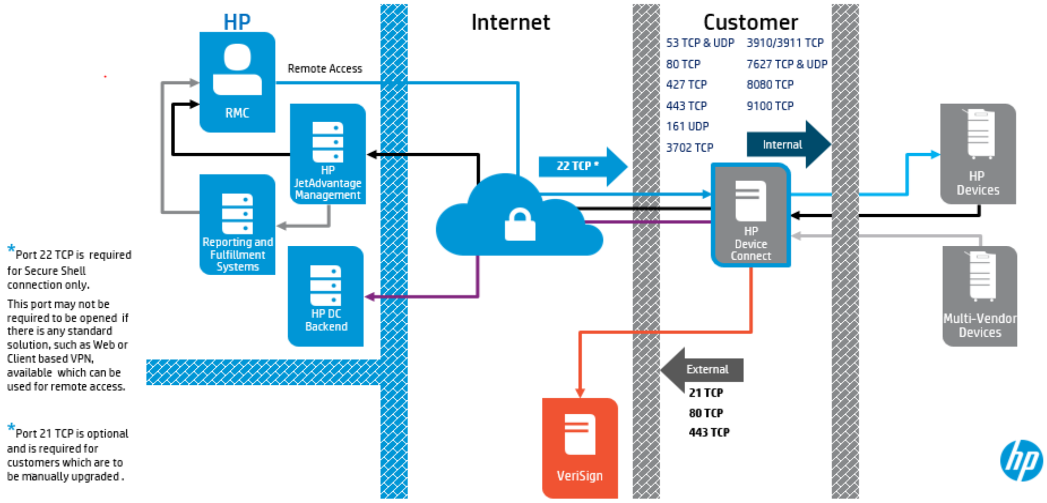
To obtain a copy of the above documents contact the local HP Device Connect representative.

2 Introduction: HP Device Connect - Software Full (HP DC-SF)

2.1.1 Overview

The HP Device Connect - Software Full (HP DC-SF) 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-SF 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-SF system overview:



*Port 22 TCP is required for Secure Shell connection only.

This port may not be required to be opened if there is any standard solution, such as Web or Client based VPN, available which can be used for remote access.

*Port 21 TCP is optional and is required for customers which are to be manually upgraded.

Figure 1 HP Device Connect System Concept

HP DC-SF provides three main functionalities as described below:

- Remote Monitoring: HP DC-SF enables remote monitoring as a secure means for collecting and reporting usage and device data for consumables replenishment and support. HP DC-SF utilizes the following tools to provide remote monitoring:
  - HP JetAdvantage Management for usage and supplies monitoring for HP and select Canon devices.
  - HP JetAdvantage Security Manager (Security Manager) is a security compliance tool. Use Security Manager to create policies that assess the security of your imaging and printing devices, configure the devices to comply with the policy, and monitor the devices for continued compliance.
- Remote Management: HP DC-SF enables remote management of devices in order to facilitate discovery, event troubleshooting, break-fix activities, updating of device configurations and firmware, and non-reporting device remediation.
  - HP DC-SF utilizes HP JetAdvantage Management Connector and HP Web JetAdmin (HP WJA) to provide remote management.
- Remote Access: Support Specialists use remote access to manage and support the customer fleet from the HP network. Remote access will require customer provided connection capabilities.

2.1.2 HP DC-SF Components

The table below outlines the HP DC-SF components.

Function	Enabling Software Component(s)	Description
Remote Monitoring and Management	HP JetAdvantage Management Connector	Provides a scalable and highly available platform for device discovery, entitlement, remote monitoring of usage and supplies, and management of network connected HP devices
	HP Web JetAdmin	Enables device management for configuration, diagnosis, and repair
	Device Configuration Tools (PJLs)	Utilities to that are used for printer configuration
Security Compliance Tool	HP JetAdvantage Security Manager	Easily and quickly create device security policies
System Maintenance	HP DC Updater Client	Update utility for components which do not have built-in update capabilities

Table 1 Components which make up HP DC-SF

3 HP DC-SF Security Overview

HP Device Connect - Software Full (HP DC-SF) security details are provided in the following sections:

3.1 Software Update Management Process

HP DC-SF updates are released broadly on a quarterly basis depending on the updates to the various underlying components. HP DC-SF 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 download and installed as per the convenience of the customer. Please contact your HP DC SME for the patch bundle download locations.

3.2 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-SF	Printer (WS)	HTTP Get
7627	TCP & UDP	Internal	Outbound	DC-SF	Printer (WS)	HTTP-Get
3910/3911	TCP	Internal	Outbound	DC-SF	Printer (WS)	HTTP
3702	TCP & UDP	Internal	Outbound	DC-SF	Printer	HTTP
8080	TCP	Internal	Outbound	DC-SF	Printer	HTTP-Alt
161	UDP	Internal	Outbound	DC-SF	Printer	SNMP Get/Set
9100	TCP	Internal	Outbound	DC-SF	Printer	JetDirect (PDL Data Stream)
53	TCP & UDP	Internal	Outbound	DC-SF	DNS Servers	DNS
427	TCP	Internal	Outbound	DC-SF	Printer	SLP
80	TCP	External	Outbound	DC-SF	http://crl3.digicert.com/ssca-sha2-g6.crl	JetAdvantage Management Connector to retrieve certificate

					http://crl4.digicert.com/ssca-sha2-g6.crl	revocation list (CRL) for the initial registration process
					http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6.crl	DC-SF Service retrieves a certificate revocation list (CRL) from the following URLs: http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6 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.
443	TCP	External	Outbound	DC-SF	https://management.hpjam.hp.com https://jamanagement.hp.com **Avatar URL**: http://acc.avatar.ext.hp.com **EWS URL:** http://ews.hpjamservices.com/SignalR	HP JetAdvantage Management backend for device usage, consumable, telemetry, and event log collection.

					https://connectivity.pod1.avatar.ext.hp.com:443/avatar/v1/entities/connectivityconfig/ https://registration.pod1.avatar.ext.hp.com:443/avatar/v1/entities/credentials/m/	
443	TCP	External	Outbound	DC-SF	https://dcmcservice.ext.hp.com	HP DC backend for automatic system updates
3389	TCP	Internal	Inbound	Internal Desktop network		(Optional), required to access HP DC SF within the Customer network.
80 and 8080	TCP	Internal	Inbound	HP SM Service	Printer	Used only when SSL is not supported on the device
443 and 8080	TCP	Internal	Inbound	HP SM Service	Printer	HTTP Web over SSL
N/A	TCP	Internal	Inbound	HP SM Service	Printer	Echo ping
161	TCP	Internal	Inbound	HP SM Service	Printer	Simple Network Management Protocol

8002	TCP	Internal	Inbound	HP SM Service	Printer	WCF with message encryption
1433	TCP	Internal	Inbound	HP SM Service	Printer	DB Communication
3329	TCP	Internal	Inbound	HP SM Service	Printer	HP Instant-On Security or hp-device-disc (IANA name) Uses SSL

Table 2 Internal / External Port Configuration and Firewall Rules

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

3.3 Communication Ports

3.3.1 HP JetAdvantage Security Manager

HP JetAdvantage Security Manager Service establishes connection to customer print fleet via HTTPS port 443 and 8080 and uses port 80 and 8080 only when SSL is NOT supported on the printer.

HP JetAdvantage Security Manager Service uses UDP port 161 for SNMP communication.

HP JetAdvantage Security Manager User Interface to Security Manager Service uses TCP port 8002 for WCF communication with message encryption.

HP JetAdvantage Security Manager connects to MS SQL over TCP Port 1433.

Print Fleet would communicate to Security Manager via SSL using port 3329.

HP JetAdvantage Security Manager Service and HP Print License Service would use port 8888.

3.3.2 HP JetAdmin

HP Web JetAdmin can be used to maintain the proper firmware on imaging and printing devices. To do so, it requires the ability to search for and download the correct firmware images from HP. These are then installed on the devices using port 9100.

Firewall Rules

Traffic numbers are

- HP Jetdirect firmware (firmware.glf index
    - http://ftp.hp.com/pub/networking/software/jetdirect/firmware/firmware.glf
        - 15.192.45.22

- Printer firmware (pfirmware.glf index file)
    - http://ftp.hp.com/pub/networking/software/pfirmware/pfirmware.glf
        - 15.192.45.22

3.3.3 HP JetAdvantage Management

HP JetAdvantage Management is a scalable, cloud-based printer management tool that HPI uses for the purpose of managing fleets of printers. HP Information Technology (IT) hosts HP JetAdvantage Management on server infrastructure known as Amazon Web Service Cloud (AWS). 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 HPI 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.

Firewall Rules

HP JAM	https://management.hpjam.hp.com https://jamanagement.hp.com Avatar URL: http://acc.avatar.ext.hp.com EWS URL: http://ews.hpjamservices.com/SignalR https://connectivity.pod1.avatar.ext.hp.com:443/avatar/v1/entities/connectivityconfig/ https://registration.pod1.avatar.ext.hp.com:443/avatar/v1/entities/credentials/m/ http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6.crl	JetAdvantage Management connector retrieves a certificate revocation list (CRL) from the URL: http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6.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.

Table 3 Communication Ports Firewall Rules

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

3.3.4 HP-DC- SF Backend

HP DC backend is a scalable, cloud-based DC server management tool that HPI uses for the purpose of managing DC Servers. 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 DC Server. 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 HPI 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://dcmcservice.ext.hp.com http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6.crl	DC Service retrieves a certificate revocation list (CRL) from the following URLs: http://crl3.digicert.com/ssca-sha2-g6.crl http://crl4.digicert.com/ssca-sha2-g6.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.

Table 4 HP DC Backend Firewall Rules

Note: All three components i.e. HP DC Backend, DC Service and DC Portal had undergone the HP Cyber Security reviews.

3.4 HP DC-SF Auto Update Duplex Communication

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

3.4.1 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

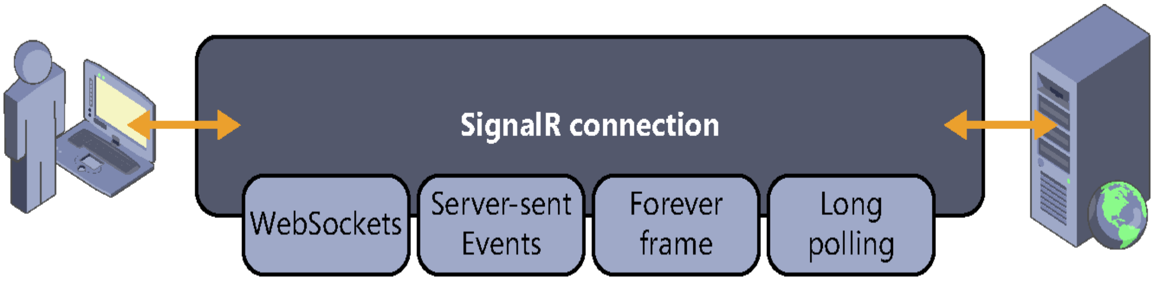


Figure 2 Signal R Connection

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 the either of these protocols: Server Send events, long polling SignalR handles the dispatching across machine boundaries as if by magic, allowing server to call methods on the client as easily as local methods, and vice versa.

3.4.2 HP DC-SF SignalR Components

HP DC-SF Backend SignalR Hub

HP DC-SF 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 the real time, whenever there is a trigger from Portal for an instance (client) ex. Schedule change, then HP DC-SF 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 persistent connection.

HP DC-SF SignalR Client

DC-SF SignalR Client initiates the connection with HP DC-SF 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-SF SignalR client will retry to reconnect with HP DC-SF 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 the end.

3.5 Data Centre Locations

Data security is paramount to HP. HP stores data in a few secure locations. These are located in the states of Virginia and Texas in the US. Exact locations and addresses will not be provided for security purposes

4 Appendix A: Network Traffic

Traffic numbers are available in documents of the individual application components

- Sample average SNMP traffic for 2000 devices (assuming HP WJA IP range discovery)
  - (HP RM + HP WJA (discovery) + HP SM) * 2000
  - (65KB + 3.7 KB + 150KB) * 2000 = 437400 KB = ~437 MB

Components	Traffic
HP Web JetAdmin (Device discovery)	SLP multicast - Network device • SLP multicast response = 2 packets, 768 bytes over 24.5 Sec • SNMP follow-up query/response = 6 packets, 1.9 Kbytes over 60 mSec IP broadcast - Network device • Each IP broadcast address = 3 SNMP packets, 255 bytes over 7 Sec IP broadcast response = 3 SNMP packets, 468 bytes over 7 Sec • SNMP follow-up query/response = 34 packets, 5.4 Kbytes over 109 mSec IP range - Network device • ICMP echo request send and receive = 2 packets, 148 bytes over 70 ms • SNMP follow-up query/response from printer = 28 packets, 3.6 Kbytes over 2.6 Sec Specified address - Network device • SNMP query/response from printer = 38 packets, 6.1 Kbytes over 1.1 Sec • Active Directory—Network device • SNMP follow-up query/response from printer = 34 packets, 4.2 Kbytes over 5 Sec IP broadcast - PC-connected device • SNMP query/response from printer = 23 packets, 3.6 Kbytes over 27.5 Sec
HP JetAdvantage Security Manager	Data is encrypted when transmitted if HTTP(s)/SNMP V3 is enforced on the devices. The data transmission (HTTP request) is usually below 150 KB per printer Network traffic is generated while discovering the devices and during the policy assessment & remediation

	HP JetAdvantage Security Manager does not poll data from devices
HP JetAdvantage Management	• Device Discovery - IP range discovery - ICMP echo request send and receive = 2 packets, 148 bytes over 70 ms - SNMP follow-up query/response from printer = 28 packets, 3.6 Kbytes over 2.6 Sec - 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 Data is encrypted and compressed when transmitted
HP DC Client Service	Data is encrypted and compressed when transmitted. The data transmission (HTTP request) is usually below 100 KB Heart beat data, by default, is scheduled to be transmitted every 60 min. to the HP DC backend server 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

Table 5 HP DC Communication Traffic

Disclaimer

© Copyright 2019 HP Inc. 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.