HP Device Connect Software Full v6.0.0- Technical Quick Specs

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

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

1 About the document 8
1.1 Intended Audience 8
1.2 Related Documentation 8

2 Introduction: HP Device Connect - Software Full 8
2.1 Overview 8
2.2 HP DC- SF Components 9
2.3 Deployment Models 10
2.4 Remote Access 11

3 Installation Details 11
3.1 General Requirements 11
3.2 . Host System Requirements 12
3.3 User and Roles 12
3.3.1 Administrator 12
3.3.2 DC-SF AutoUpdate Client Service Account 12
3.3.3 Operator(non-admin) 13
3.3.4 Roles, Responsibilities and HP DC Tools 13
3.4 Network Requirements 14
3.4.1 HP JetAdvantage Device Connection Requirements 18
3.4.2 DC Illustration 18

4 HP-DC-SF Security 19
4.1 Security Model 19
4.1.1 LogMeIn 19
4.1.2 HP Web JetAdmin 19
4.2 Communication Protocols 19
4.2.1 HP JetAdvantage Management 19
4.2.2 HP JetAdvantage Security Manager 20

4.2.3 HP AutoUpdate Client 20
4.3 Network Traffic 21

List of Figures

Figure 1 HP Device Connect System Concept 9
Figure 2 SSH Direct connection to the server 18

List of Tables

Table 1 HP DC-SF Components 10
Table 2 Host System Requirements 12
Table 3 User Roles, Responsibilities and MS Tools 14
Table 4 Internal / External Port Configuration and Firewall Rules 18
Table 5 HP DC Communication Traffic 22

List of Acronyms

HP DC -SF - HP Device Connect Software Full

LMI - LogMeIn

UI - User Interface

JAMC - JetAdvantage Management Connector

MPS - Managed Print Services

HP WJA - HP Web JetAdmin

HP JAM - HP JetAdvantage Management

1 About the document

This document describes:

- Details of HP Device Connect - Software Full

Document updates may be issued between editions to correct errors or to document product/process changes. To ensure that you receive the updated or new editions, contact your local HP Device Connect Contact for more information.

1.1 Intended Audience

This document is intended for administrators responsible for installing and managing HP Device Connect - Software Full. 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 Full.

1.2 Related Documentation

The following documents provide related information:

- HP JetAdvantage Management documentation
- HP Web JetAdmin documentation
- HP JetAdvantage Security Manager

To obtain a copy of the above documents contact your local HP Managed Services account representative.

2 Introduction: HP Device Connect - Software Full

2.1 Overview

The HP Device Connect - Software Full (HP DC-SF) is an integrated management platform containing a suite of capabilities that provides a secure and scalable platform for enabling efficient management of an enterprise 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:

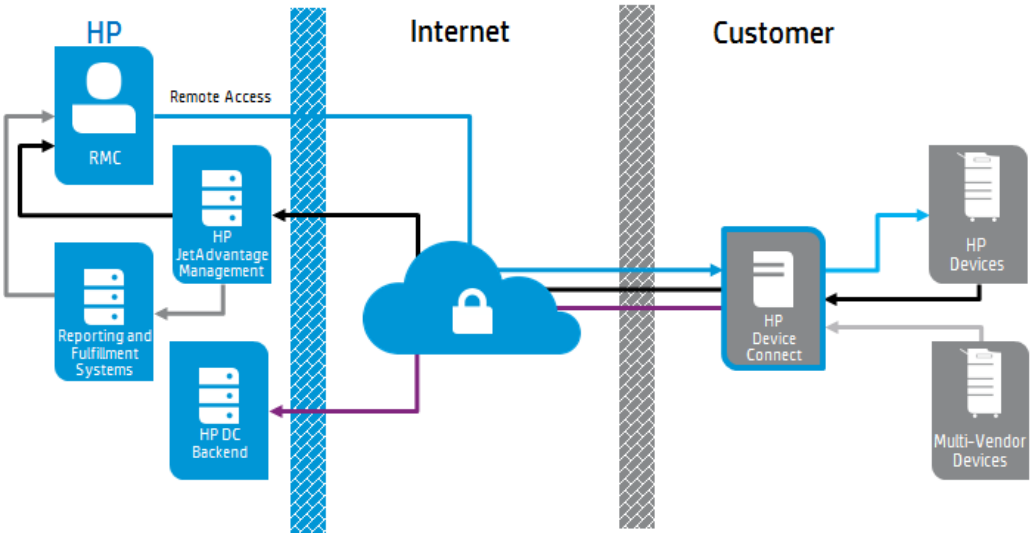

Figure 1 HP Device Connect System Concept

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.

2.2 HP DC- SF Components

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

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 HP DC-SF Components

2.3 Deployment Models

HP DC-SF is delivered as an installable .exe file that can be installed on a customer provided physical or virtual machine running on one of the following 64-bit operating systems:

- Windows Sever 2016
- Windows Sever 2008 R2
- Windows Sever 2012
- Windows Sever 2012 R2
- Windows 7
- Windows 8.1
- Windows 10

HP DC-SF comes in two versions - FULL and LITE. HP DC-SF FULL comes with the full suite of DC-SF applications and is used where remote monitoring and remote management are desired. HP DC-SF LITE is used for accounts where remote monitoring, limited device management, and limited proactive services are desired.

- HP DC-SF
    - HP JetAdvantage Management Connector
    - HP Device Connect AutoUpdate Client
    - HP Web JetAdmin
    - HP JetAdvantage Security Manager
    - Miscellaneous Utilities
- HP DC-SF
    - HP JetAdvantage Management Connector
    - HP Device Connect AutoUpdate Client

2.4 Remote Access

One of the key needs for an efficient service delivery using HP DC-SF, is to have remote access for the HP Support Specialists to monitor and manage the fleet.

HP DC-SF has the option of utilizing either an HP or customer provided remote access solution:

- HP provided HP Remote Device Access (HP RDA):
  HP RDA is a support solution that enables the delivery of HP remote support services over the Internet, or other connectivity methods, with enhanced security features like encryption, authentication, audit, and target authorization which address stringent customer compliance regulations.
- Customer provided remote access solution: If desired, HP will utilize a customer provided remote access solution for remote access activity. Compatibility testing will be required prior to full implementation.

Refer to HP provided solution section in this document for more information on Remote Access.
For more information and support regarding remote access implementation, please contact local HP Device Connect Contact support.

3 Installation Details

This chapter describes the installation pre-requisites required for HP DC-SF.

Contents

- Host system prerequisites
- Networking configuration information

3.1 General Requirements

Customer will need to provide the following:

- Host system setup and configuration on which HP DC-SF can be installed
- Anti-virus or other security software configured to allow DC-SF installation and operation
- Network and firewall configurations to allow communications between HP DC-SF and all imaging and printing devices under contract, as well as between HP DC-SF and HP;
- If desired, remote access connection point such as an SSH server;
- Customer IT resource to assist HP in resolving network issues that would impact HP DC-SF solution functionality; TCP\IP network; and
- Validate that there are no SNMP traffic blocks for the “Gets” (get commands)
- JAM does not currently support devices not connected to the network. Devices connected to PC’s will need to be connected to the network to be managed through JAM
- All devices managed under a customer in JAM must have a unique IP address. MPS partners who have multiple customers managed under a single customer name in JAM need ensure that all their various customers’ devices have distinct IP addresses compared to the devices of the other customers

3.2 . Host System Requirements

Perquisites (minimum)	Supported Environments	Opiating System	Other Requirements	Max # of Supported devices/Server
• Processor: Quad Core, 2.0 GHz • RAM: 10 GB Minimum, 12GB Recommended • Free Disk Space: 50 GB on C:\ - system drive Recommended • .NET: 4.5.50709 or above	• Physical • Virtual	• Windows Server 2016 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows 7 • Windows 8.1 • Windows 10	• .NET 3.5 and .NET 4.5 installed • PowerShell script execution allowed • Three user types – Administrator, Service Account and Operator (details in below section) • Anti-virus or other security software configured to allow DC-SF installation and operation • Recommended screen resolution 1024x768	• 2000 for HP WJA and HP SM • 4000 for JAMC

Table 2 Host System Requirements

Note: If HP WJA, HP SM and JAMC are configured in combination, then 3000 to 4000 devices are supported.

3.3 User and Roles

Two user roles need to be configured on the DC. These include Administrator and Operator. Each one has distinctive functions and responsibilities.

3.3.1 Administrator

This is a user with Administrator group privileges.

Administrator users are responsible for installing, updating, configuring and maintaining the various tools on HP DC- HP Web JetAdmin, HP JetAdvantage Security Manager etc. Configuration tasks include tool configuration, administration, and regular maintenance.

Administrator users are required to guarantee the continuous operation of the management environment and ensure timely adaptation of management systems to the latest versions.

3.3.2 DC-SF AutoUpdate Client Service Account

This is a service user with two types of privileges.

The DC-SF autoupdate client (HPDeviceConnectExecuterService) is responsible for keeping the DC-SF software up-to-date by automatically updating the software as and when newer versions become available and if configured to do so – similar to "Windows Update" - which keeps the Windows OS up-to-date.

Local System User: The software DC autoupdate client (HPDCExecuterService) runs the install as default Windows 'Local System User'.

Admin Credentials: User has an option to provide 'Admin Credentials' by enabling the check box 'Enable Admin Credentials'. When the user clicks the checkbox, install prompts the user for 'Admin Credentials' at a later phase during installation. Refer section 8 for Login Credentials setup.

In order to automatically update the system, the DC-SF autoupdate client service needs to run as above-mentioned privileges to properly perform the following functions:

- Install software (with permissions to create/update registry, create/update folders under C:\Program Files\ etc.)
- Stop/Start services
- Reboot server

Note: It is required that this user credentials (passwords) be kept up-to-date so as to enable the DC-SF autoupdate client service to run uninterrupted. It is recommended that the password for this user be kept as "Never Expires".

3.3.3 Operator(non-admin)

This is a regular Windows user.

Operators are responsible for the operational status of the managed imaging and printing environment. They work on executing configuration actions, diagnosing and troubleshooting fleet issues and ensuring overall fleet availability and performance using the pre-installed tools on HP DC.

Operators are trained on the operational procedures of managing the print fleet environment utilizing the tools on HP DC-SF.

3.3.4 Roles, Responsibilities and HP DC Tools

The following table provides details about the users' roles along with the privileges granted to perform their respective functions.

User	Functions	MS Tools
Administrator	• Perform routine maintenance tasks • Configuration of all pre-configured DC-SF applications • Diagnosis, troubleshooting and break-fix of DC-SF • DC-SF tools administrator role	• HP DC-SF pre-installed tools for tool administration - HP Web JetAdmin - HP JetAdvantage Management Connector

	• Have access to all capabilities and manage/maintain the different tools installed in DC-SF • Create Device Security Policies.	- HP JetAdvantage Security Manager - HP DC-SF AutoUpdate Client
Administrator (service account)	• Service account for DC-SF autoupdate client (HPDeviceConnectExecuterService) • Installation and upgrade of DC-SF software • Stop/Start services • Reboot server	• HP DC-SF AutoUpdate Client
Operator	• Fleet Support Specialist performing HP MPS service delivery • Print fleet management • Mostly read-only privilege to MS system	All applications for fleet management purposes • HP Web JetAdmin • HP JetAdvantage Management Connector • PJL tools

Table 3 User Roles, Responsibilities and MS Tools

3.4 Network Requirements

Networking information which will allow HP to configure HP DC-SF:

- **Web Proxy Name**: If the customer requires the use of a Proxy to get outside their intranet. If so, the following will be required:
  - Web Proxy Port Number
  - Web Proxy User Name
  - Web Proxy Password
- **HP DC-SF autoupdate schedule:** Schedule (days/time) when the HP DC system can perform download and installation of DC updates and patches.
- **Passwords and credentials** to:
  - HP DC-SF host system for remote access; and
  - Devices under contract.
- **Ports**: Access to the following ports is required:

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 http://crl4.digicert.com/ssca-sha2-g6.crl	JetAdvantage Management Connector to retrieve certificate 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.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.
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 https://connectivity.pod1.avatar.ext.hp.com:443/avatar/v1/entities/connectivityconfig/	HP JetAdvantage Management backend for device usage, consumable, telemetry, and event log collection.

					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		
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	ICMP	Internal	Inbound	HP SM Service	Printer	Echo ping
161	UDP	Internal	Inbound	HP SM Service	Printer	Simple Network Management Protocol
8002	TCP	Internal	Inbound	HP SM UI	HP SM Service	WCF with message encryption
1433	TCP	Internal	Inbound	HP SM Service	MS SQL	DB Communication
3329	TCP	Internal	Inbound	Printer	HP SM Service	HP Instant-On Security or hp-

						device-disc (IANA name) Uses SSL

Table 4 Internal / External Port Configuration and Firewall Rules

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

3.4.1 HP JetAdvantage Device Connection Requirements

HP JetAdvantage Management does not currently support devices not connected to the network. Devices connected to PC's will need to be connected to the network in order to be managed.

All managed devices within a customer's fleet must have distinct IP addresses irrespective of location or network setup.

3.4.2 DC Illustration

A depiction of the HP DC sitting on a customer's internal network is shown below. The depiction is of an SSH Direct connection to the server and lists the port requirements.

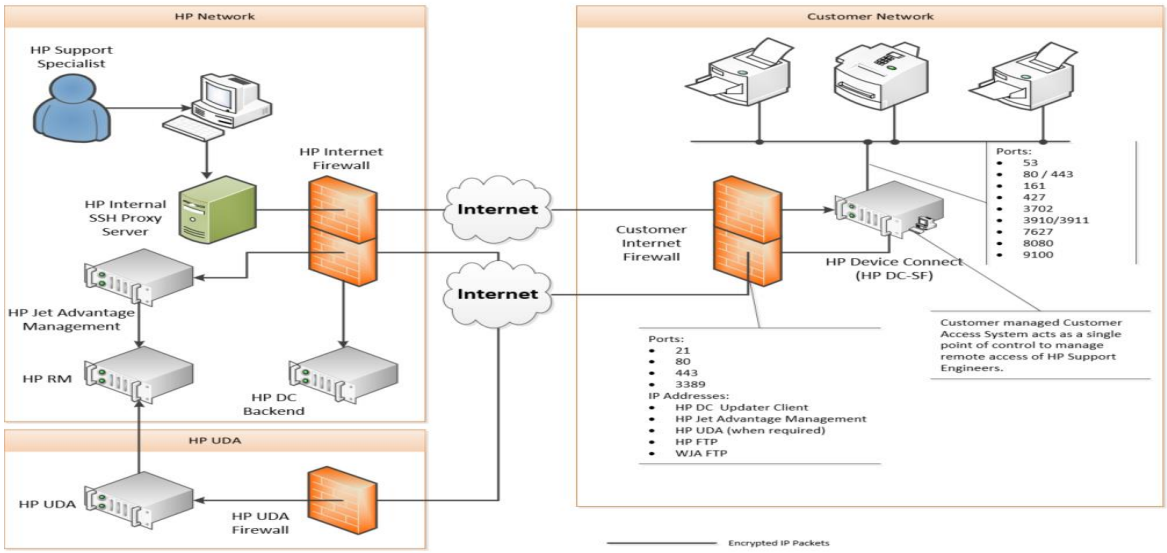

Figure 2 SSH Direct connection to the server

4 HP-DC-SF Security

4.1 Security Model

HP DC-SF utilizes the security of the individual components for all external communications.

4.1.1 LogMeIn

One of the key capabilities of HP DC is to provide remote access to the HP Support Specialists in order to monitor and manage the fleet. It is very important to ensure that this remote access is secure.

HP DC utilizes LogMeIn (LMI) Central to provide secure remote access.

LogMeIn allows secure remote access to critical resources over an untrusted network and security considerations always prevail over usability concerns.

4.1.2 HP Web JetAdmin

HP Web JetAdmin has several features that make it easy to secure the application and its features:

- **Single sign-on** – Users don't have to provide password and user details in order to access the application.
- **.NET Remoting** – The client displays through a local application that uses .NET Remoting as a secure means of communicating with the server.
- **Active Directory Integration –** Domain accounts are used to identify who has access to the application and its features.
- **Low privilege service –** HP Web JetAdmin does not run as a system and has no direct access to key OS components (the client application runs under user credentials).
- **Secure online downloads** – HP Web JetAdmin installer and update files that can be obtained from hp.com are digitally signed. This helps to ensure the integrity and authenticity of files as well as underlying components as they are installed.
- **Optional SSL/TLS –** Click Once client deployment can apply added security with certificates.

4.2 Communication Protocols

4.2.1 HP JetAdvantage Management

HP JetAdvantage Management is a scalable, cloud-based platform for managing customer printer and Multifunction Peripheral (MFP) fleets. HP Information Technology (IT) hosts HP JetAdvantage Management Platform. This cloud platform also makes use of an API gateway hosted by Apigee to provide access methods consistent with other HP Cloud APIs even beyond the scope of HP JetAdvantage Management.

The HP JetAdvantage Management Connector facilitates communication between the fleet of customer network devices and the HP JetAdvantage Management Platform. Internet load balancers manage traffic flow between both client and the HP JetAdvantage Management Connectors and the HP JetAdvantage Management Platform infrastructure. Dedicated team members in HP IT update the servers that support the infrastructure as well as the working and stored data.

HP JetAdvantage Management cloud logic (JAM) in turn communicates with a fleet of devices through a customer firewall using the HP JetAdvantage Management Connector (JAMC). This JetAdvantage Management Connector software can run on either a customer server or an HP appliance that also hosts other management applications.

HP JetAdvantage Management 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 JetAdvantage Management Platform servers, and database infrastructure. An HP controlled identity management system authenticates user identity access to the portal interface and a key registration process establishes secure communication between the data connectors and the application. Customer data is secured in a database infrastructure and sensitive details are encrypted using the standard practices.

Customer device details are transmitted to and from HP JetAdvantage Management Platform and are stored securely in the server infrastructure. This includes device serial numbers, hostnames, and IP addresses, although there is a feature to prevent IP addresses from leaving the customer environment.

Data is written to and retrieved from a few key HP JetAdvantage Management Platform databases in a tiered server infrastructure. HP JetAdvantage Management Platform uses provisioned database servers that include backup services. All sensitive data (account passwords and identities for both customer and connector are encrypted and stored in the database.

HP JetAdvantage Management Platform uses industry standard SSL/TLS to provide security when transmitting or receiving data. This is also known as HTTPS communication, which is simply HTTP over TLS (TLS 1.1 or higher) using an X. 509 certificate for authenticity and encryption. The certificate is used to establish a one-way trust between clients and the HP JetAdvantage Management Platform server. Clients trust the server if the server's certificate is valid. Once the HTTPS negotiation starts and communication to/from HP JetAdvantage Management Platform 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.

4.2.2 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.

4.2.3 HP AutoUpdate Client

HP DC AutoUpdate Client 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.

Note: Please refer the HP DC Security Whitepaper for more security related details.

4.3 Network Traffic

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

- Sample average SNMP traffic for 2000 devices (assuming HP WJA IP range discovery) with JAMC traffic for 8000 devices per day
  - (HP WJA (discovery) + HP SM) * 2000 + JAMC*8000
  - (3.7 KB + 150 KB) * 2000 + 500 KB * 8000 = ~ 4.31 GB

Components	Traffic
HP JetAdvantage Management	• 500KB of network traffic per device per day, can be less • Data is encrypted and compressed when transmitted
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 DC AutoUpdate 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

Table 5 HP DC Communication Traffic

Disclaimer