Data sheet

Transfer print data with confidence

HP Universal Device Agent (UDA) provides a high degree of confidentiality and data security when exchanging device usage data over a network.

Introduction

HP Universal Device Agent (UDA) is a data collection tool critical to the service delivery of HP Managed Print Services (MPS). This document explores the technology in use, allowing HP UDA to gather data from your print devices and transfer the data to HP Servers, in a safe and secure manner.

Data transfer tools

HP uses Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS), for data transfer between HP UDA and the HP Server. The network activity that occurs during data transfer can be compared to browsing the web with an Internet browser on a standard PC. All data is compressed and encrypted prior to transfer via HTTPS port 443.

How it works

HP UDA extracts data from the Management Information Base (MIB) or similar data collection locations within each print device.

The MIB is an internal database that all network connected devices contain as part of their anatomy. The MIB hold data such as the model name, toner levels and the current status of the device.

The data transfer is initiated by a request from HP UDA. Data from the MIB is extracted, compressed, encrypted and securely transferred to the HP Server. Each data transfer requires very few network resources (~ 100 kb).

No other data is accessed by HP UDA, including: print jobs, stored documents, directory lists, or data held within the device relating to previous activity.

With the installation of HP UDA, HP can gather usage counts and supplies levels from the networked imaging and printing devices for billing and supplies replenishment purposes only. In the case of non-networked imaging and printing devices directly attached to a PC (e.g. via USB or Parallel cable), an additional software utility called the "PC Direct Connect SNMP Proxy" is required with the HP UDA to retrieve the usage counters and supplies levels.

Technology platform

The HP Server and UDA are building on the flexible and highly secure .NET platform that offers superior performance and scalability.

Requirements

- Microsoft Windows Communication Foundation (WCF)
- Microsoft .NET 4.6 Framework or higher -requires ~600MB
- SNMP version 1.0 enabled on network and devices
- Community default name: "Public"
  Note: It is possible to set the community name for each IP range
- Internet access
- Secure Network Management Protocol (SNMP)-enabled network

HP UDA requires few resources, can be installed on any networked PC and runs on hardware meeting .NET 4.6 or higher requirements.

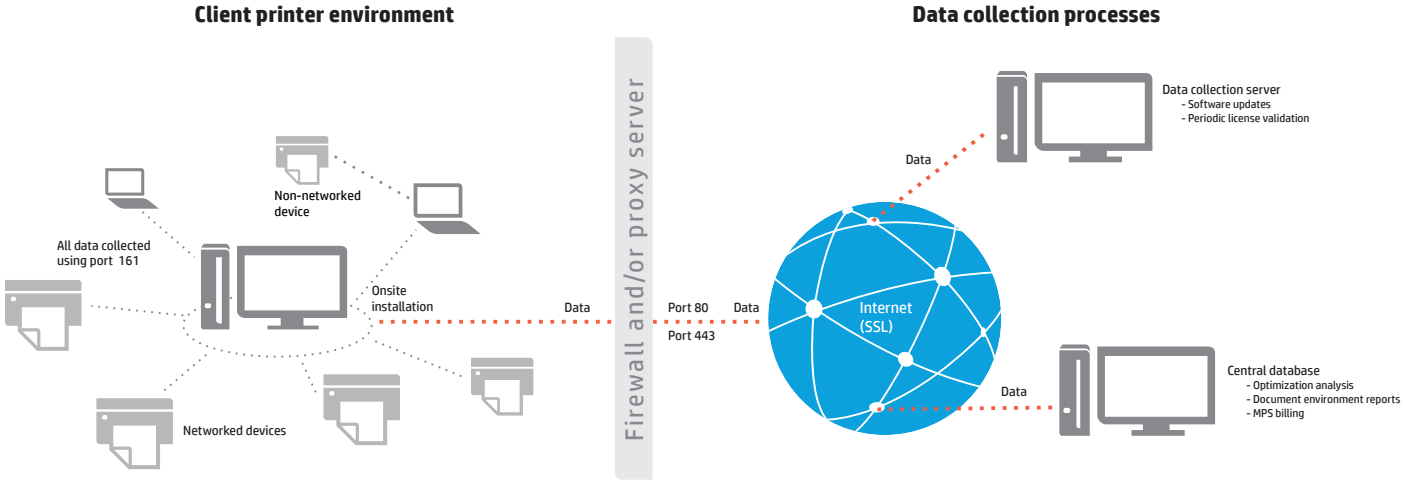

Fig 1
Firewall and/or proxy server.

Principal functions

HP UDA agent will contact the HP UDA server for:

- Authentication
- List of network ranges to search
- List of MIBs
- Discover and Collect phases

HP UDA will scan all defined network ranges searching for imaging devices (printers, MFPs, fax machines, etc.).

Network scans can be flexible, accessing a specific IP Address or a complete IP range - e.g., 192.168.99.1 to 192.168.99.254

HP UDA only performs SNMP reads and is not able to update or make any changes to the imaging device.

HP UDA uses two phases to collect data from an imaging device; Discover and Collect. Both phases use SNMP technology.

Discover phase

The Discover phase involves using SNMP to search specified IP Addresses and locate imaging devices. The first step includes sending one SNMP packet to all specified IP addresses, If a reply is received, a unique set of Object Identifiers (OIDs) is sent to identify the imaging device. The imaging device is "discovered" and data is stored in the database for the Collect phase. Discover interval occurs every 5 hours.

Collect phase

Depending on the imaging devices found in the Discover phase, the type of data requested can vary.

Small devices, such as mono printers, are asked for a small set of data, whereas a large multifunction printer (MFP) could have a wider data set to collect.

Not all data is collected each time a Collect phase is completed. Some data is collected at each query and other data is collected less often. A standard practice is to collect the IP address, MAC and Hostname of each image device scanned to ensure the accurate identity and location information of each imaging device.

During each scanning incident as data is collected, the data is matched to a specific MIB with queries for type and model as well. In this way, data is matched to devices, and vice versa. See sample data provided below. Collect interval occurs every 3 hours.

Name	OID	Result
Model_Name	1.3.6.1.4.1.11.	HP Color LaserJet CM4730
DeviceIdentifier	1.3.6.1.2.1.25.	HP Color LaserJet CM4730 MFP
Model_Number	1.3.6.1.4.1.11.	CB481Q
SerialNumber	1.3.6.1.4.1.11.	JPC1H11795
Firmware_Date_Code	1.3.6.1.4.1.11.	20110829
Firmware_Version	1.3.6.1.4.1.11.	50.021.0
HostName	1.3.6.1.2.1.1.5	NP1870A6C
Printer_Display	1.3.6.1.2.1.43.	Ready
Device_Location	1.3.6.1.4.1.11.	Reception
Device_AssetNumber	1.3.6.1.4.1.11	PRN-2011-A8743
Device_Total	1.3.6.1.4.1.11	698265
Copy_Total	1.3.6.1.4.1.11	12669
Print_Total	1.3.6.1.4.1.11	684331
Fax_Total	1.3.6.1.4.1.11	1265
Print_BW_Total	1.3.6.1.4.1.11	558744
Print_Color_Count	1.3.6.1.4.1.11	125587

Data Collector Ports, Firewall setting for URL of the UDA Server

When starting the data collector – The user credentials used on the server need to have internet access because the Data Collector will do the initial communication with the UDA Web Service on port 80.

- The user needs to have rights to access the internet using http port 80 and https port 443.

- If Proxy settings are required then the Proxy settings defined in the data collector are used.

- All data sent from data collector are encrypted and sent on port 443 TCP outbound.

No inbound UDP connection is needed.

- If the data collector can not be started please add the full link to the server in the customers Firewall:
https://jadcws.jetadvice.com/v2/service1.svc

- SNMP v1/v2 port 161/162 is used to discover and collect printers in LAN.

4AA4-6880ENW, July 2017

This is an HP Indigo digital print.