Technical white paper

HP JetAdvantage Secure Print

Security

Table of Contents

HP JetAdvantage Secure Print Overview

HP JetAdvantage Secure Print provides a secure mechanism to print business information. The solution removes the possibility of privacy breaches by removing uncontrolled access to sensitive documents at printers.

Security is enforced by authenticating users at the printer using a mobile device, proximity card, or keypad login. Documents are then released only to the intended recipient.

In addition to security, Secure Print offers additional workflows not supported by traditional printing. Users can easily release documents at any enabled printer. Also being cloud-based, the solution supports mobile staff to print at any business location without having to configure print queues on their workstation.

When used with HP JetAdvantage Insights, customers can both implement the Secure Print workflow and have clarity on the state of the print environment through data visualization in Print Analytics and Fleet Manager. These products share some of the same infrastructure in order to simplify deployment and provide comprehensive capabilities.

Basic Workflow

Security is essential to everything we do. Secure Print also gives you control over what data is collected and who can see it. This document outlines the architecture, policies, and safeguards in place to keep your information secure.

No device or print information can be transmitted to Secure Print until Scouts are installed and are activated with a registration key. If your registration key is invalidated or deleted from the system, no further device or print information will be collected, even if the Print/Device Scouts remain installed.

Figure 1 shows the Secure Print workflow. A user submits a document from their workstation. The document is stored encrypted on their machine and optionally in the cloud. The user identifies themselves at a device using a mobile device, proximity card, or keypad login. The document is then securely released to the printer.

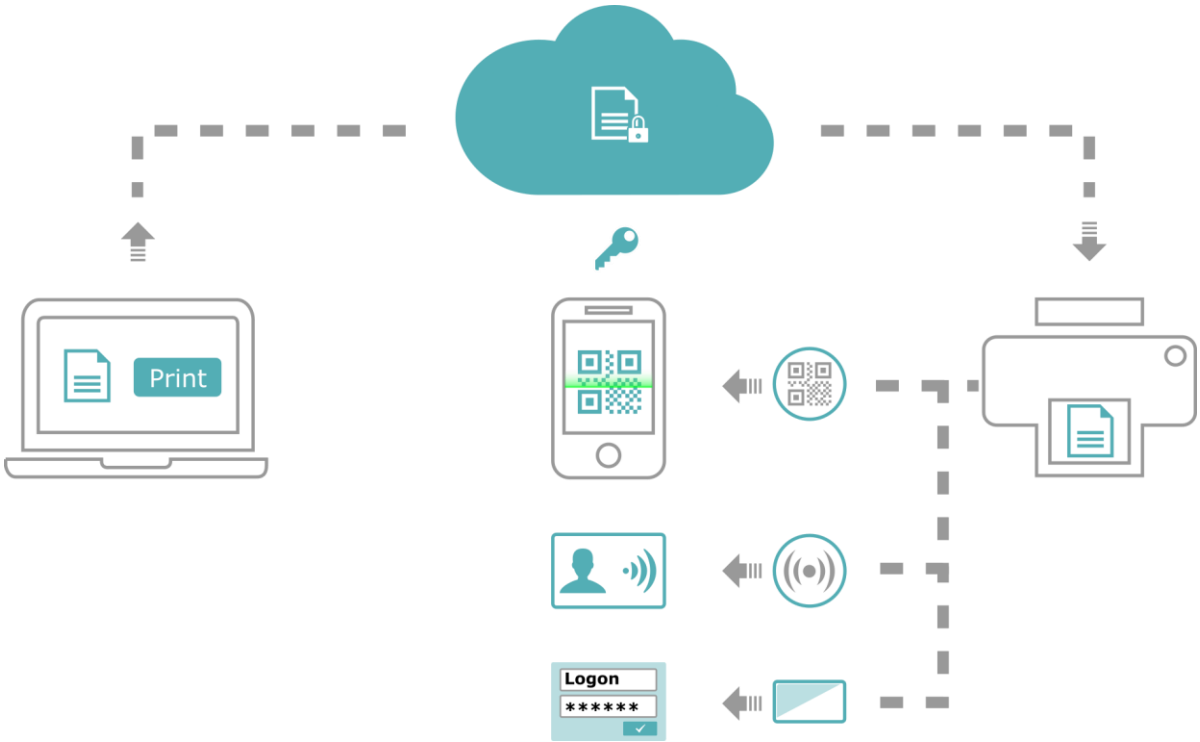


Figure 1: HP JetAdvantage Secure Print Workflow

Your Network

To make use of HP JetAdvantage Secure Print, you will need to install certain components in your local area network. The components to be installed are:

- Print Scout (PC workstations)
- Device Scout (non-dedicated server)
- Either
  - Secure Print Mobile App (mobile release), or
  - Secure Printer App for HP FutureSmart devices (prox/keypad release)

Data Control Overview

The integrity of customer data is critical. HP JetAdvantage Secure Print uses a combination of technological and procedural controls to restrict access to customer data.

At any time, you may stop any Scout from collecting information by uninstalling it. You can find instructions on how to uninstall the Scouts in the application installation document.

Secure Print employs a **Zero knowledge encryption scheme** to encrypt print data using a key held only on the customer network. See the Data Protection section for more details.

Device Scout

For Secure Print, the Device Scout has two roles: device data collection and device management.

Device Data Collection

The Scout finds all printers within your network and collects data on device status, meters, and consumables. The Device Scout attempts to collect the following information from network devices that respond via SNMP as output devices:

- IP address
- Device description
- Maintenance kit levels
- Device serial number
- Toner and non-toner supply levels
- Meter reads
- Asset number
- Monochrome or color identification
- Display reading
- MAC address
- Device status
- Manufacturer
- Model number
- Error codes
- Firmware Version/Patch Level
- Location

Enabling Printers
With Secure Print, the Device Scout controls the Secure Print app on enabled printers. During setup, the Scout also deploys the app to compatible printers.

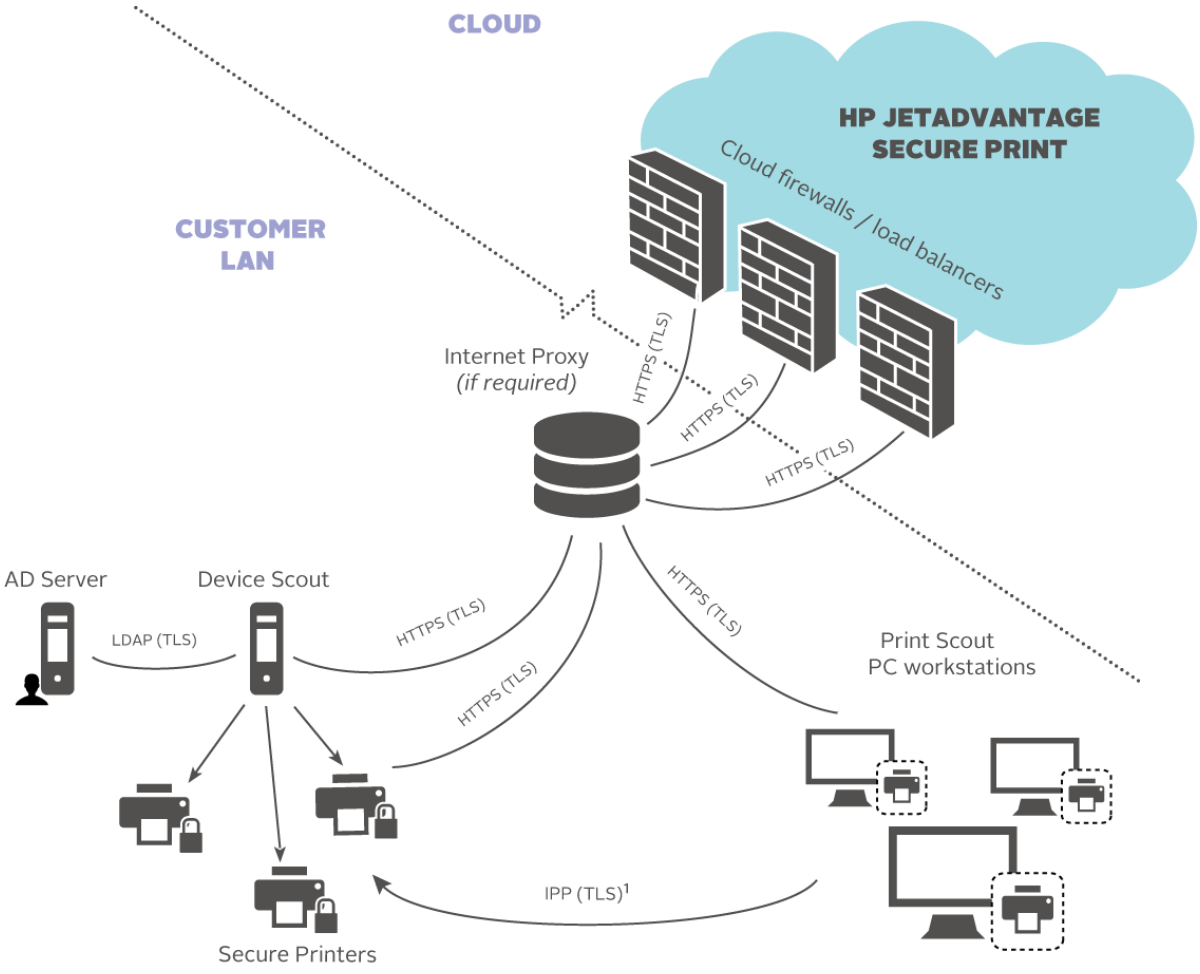
Print Scout

Before using Secure Print, the Print Scout must be deployed to workstations. The Print Scout includes functionality to:

- Assist the user to print their first document securely
- Submit, hold, and release documents securely
- Collect print activity for reporting purposes including:
  - Information about the user from Active Directory
  - Information from the printing device via SNMP
  - Information about the print job via print stream analysis

You can control what data is collected and who can see it by configuring the Print Scout collection settings. You can also apply role-based viewing restrictions, giving some system users a limited view of the data.

DEPLOYMENT ARCHITECTURE



12

Figure 2: Deployment Architecture

[1] If Internet Printing Protocol (IPP) is not enabled on the printer, the raw delivery protocol is used.
[2] Standard TLS negotiation is used to support TLSv1, TLSv1.1, TLSv1.2

The Print Scout registers itself via an HTTPS (TLS) connection to HP JetAdvantage cloud. The Print Scout communicates with the cloud when the user prints documents. It maintains a connection with the cloud to receive document delivery requests. Workstations are used deliver documents to printers.

The Device Scout also registers itself via an HTTPS (TLS) connection to HP JetAdvantage cloud. The Device Scout maintains a secure connection to the cloud to enable configuration of devices.

The Device Scout communicates with Active Directory using LDAP (TLS) to authenticate user credentials.

The Secure Printer communicates via an HTTPS (TLS) connection to HP JetAdvantage cloud to release print documents. This only applies if an app is installed on the printer.

The Print Scout delivers documents to the printer via an IPP (TLS) connection. If the printer is not enabled for IPP, the solution will use the Raw protocol which is not encrypted. To ensure that encryption is used to deliver documents, enable IPP printing on the printer.

AUTHENTICATION OPTIONS

Mobile Authentication

Mobile authentication utilizes a user's smartphone (iOS or Android) to enable secure printing.

Configuring Mobile Authentication

1. **Secure the Printer:** During this process, the system user attaches QR code tags to enabled printers. The code contains a GUID that identifies the printer for document release.
2. **Activating Mobile Devices:** The print user installs the Secure Print App and activates it by scanning an onscreen QR code, thereby linking the workstation creating print jobs to the mobile device that will release them. The smartphone validates the code with the HP JetAdvantage cloud and authorizes the mobile device to release only this user's documents.

Releasing Documents

Having submitted a document from their workstation, the user walks to any enabled device. Using the mobile app, they scan the printer's QR code. The code is sent to the HP JetAdvantage cloud for validation. Once validated, the system instructs the user's Print Scout to deliver the documents to the selected device.

Note: If cloud storage is enabled, the system may utilize another Print Scout if the user's machine is unavailable.

Proximity Card Authentication

Configuration

The System User (Administrator) secures the printer through the Secure Print Setup Guide or the Secure Printers grid in the web application. The request to secure the device is passed to the Device Scout. The Scout then connects to the printer and installs the Secure Print app. The Site Encryption Key[3] is passed to the app to allow the printer to decrypt documents.

Releasing Documents

The first time a user accesses the system, they must register their proximity card by swiping their card at a printer and authenticating with their domain credentials. The authentication request is passed to the local Device Scout which validates the user against Active Directory, and activates the card.

After card activation, the user authenticates by swiping their card at an enabled printer.

[3] For more information about the Site Encryption Key, refer to the Zero Knowledge Encryption Scheme section later in this document.

Note: To maintain security, user credentials are kept within the company's network and are never transported to the cloud.

Device Communication

The Device Scout generates 2048-bit AES certificates which are used to secure the channel between the MFP and the four services hosted on premises: authentication, authorization, accessories, and statistics. All communication with the four services use port 4321.

Additionally, the deployment service pushes a public certificate to the MFP that it uses to securely access the Secure Print app using port 443.

Keypad Login

Keypad login authentication is identical to proximity card authentication with the following exceptions:

Configuration

The setup workflow is identical but does not require a proximity card reader on the printer.

Releasing Documents

In the username/password release, print users can register a PIN as an alternative to their password. Once registered, the PIN is hashed using SHA-256 (Secure Hashing Algorithm - 256bit) and stored in the cloud.

DATA PROTECTION

Types of threats we address:

1. GENERAL MALICIOUS ATTACK

   Such an event could include an attempt to intercept data in transmission, denial of service, or the attempted altering or disabling of established security measures such as logins or encrypted communication. HP JetAdvantage Secure Print encrypts all external connections using TLS at the highest level supported by the connecting browser or service. All application components are isolated by function; only necessary traffic can pass between components.
2. MALICIOUS ATTACK OF PRINT DATA
   Such an event could include an attempt for a third party to intercept a customer's print data. JetAdvantage Secure Print employs a Zero Knowledge Encryption scheme described on the next page.
3. MACHINE OR TECHNOLOGICAL FAILURE
   Such an event could include power loss, network connectivity loss, or data storage failure. JetAdvantage Secure Print uses a cloud-based infrastructure with a minimum of three geographic zones. The JetAdvantage Secure Print cloud infrastructure can detect a variety of fault conditions and remove or fix defective components on the go with no interruption of service.
4. PASSIVE DATA LOSS OR CORRUPTION
   These losses could be caused by software defects, incompatibilities between software components, or data storage loss. The HP JetAdvantage cloud infrastructure mitigates these risks through a formal software quality assurance methodology. In the event of a data corruption problem, JetAdvantage Secure Print maintains pre-state backups in order to roll back any data-altering changes. JetAdvantage Secure Print also uses segregation of duties and least privilege principles to restrict the level of access employees have to include only that which is required to perform their job function. Access levels are periodically reviewed and adjusted as business needs or job roles change.

Zero Knowledge Encryption Scheme

As well as full encryption of transport, Secure Print takes the additional step of employing a Zero Knowledge Encryption scheme. The scheme ensures that core cloud components do not hold the information required to access customer's documents or metadata.

During installation, customers designate a password. This password is used to create an encryption key and is used to encrypt documents before they leave the customer local network. When documents are released, the encrypted documents are decrypted when they arrive on the network.

This ensures that even if an attacker were to breach Secure Print cloud security measures, they would be unable to access customer document data.

Security Details

Item	Encryption Used
Encryption of data transport	TLS Versions: 1.0/1.1/2.0 Ciphers ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256
Document Encryption	AES 128bit
QR Code	128 bit GUID
MFP Certificates	2048 bit AES

Security is a Shared Responsibility

As an HP JetAdvantage Secure Print customer, you also share the responsibility to protect your data.

1. Ensure that Device Scouts are accessible to authorized users only.
2. Ensure that the server is fully patched and meets all other security requirements of your organization.
   A. Ensure that the server is regularly maintained according to the policies of your organization.
   B. Ensure that the minimum necessary credentials are granted to individuals within your organization who require access to the server(s) to perform their job functions.

NETWORK UTILIZATION

Print Scout

The Print Scout uploads secure print job information as it occurs. The Print Scout does not perform network-wide discoveries.

Print Scout Network Traffic

PRINT SCOUT NETWORK TRAFFIC SUMMARY		
TASK TYPE	FREQUENCY	NETWORK TRAFFIC (in bytes)
Status	1x24hrs	2kB
AD lookups	Once per day, per print user	Depends on size of average AD record
Cloud connection keep-alive	Every minute	< 0.1KB
Print job metadata uploads	On print submission	< 1kB

Print job content uploads	On print submission	Variable based on the size and complexity of the job. Conditional on customer setting, off by default.
Incoming release requests and notifications	On print release	< 1kb
Incoming job contents	On print release	Variable based on the size and complexity of the job. Only used when user's workstation is offline and cloud holds a copy of their job contents.
Job delivery to printer	On print release	Variable based on the size and complexity of the job.
Device SNMP lookup	On print release	2.5kB

Print Scout Communication Patterns

PRINT SCOUT STATUS CHECKS
The Print Scout checks in once per day to upload its health report and check for new settings. This check is under 2kB and in most cases will return an empty response if there have been no configuration changes. The Print Scout will also check for configuration changes when each job is uploaded.

ACTIVE DIRECTORY LOOKUPS
When a user prints, the Print Scout will query Active Directory (AD) for that user only. This occurs only once per day. AD traffic is difficult to estimate because the amount of data stored in AD is highly variable. However, the maximum traffic equates to the total number of unique AD users multiplied by the average AD record size.

CLOUD CONNECTION
The communication channel between the Print Scout and the cloud is kept alive by means of a server-initiated ping. This request occurs approximately once a minute.

PRINT JOB METADATA UPLOADS
Data describing the job is sent to the cloud. This data is variable because of the strings involved (document name). A good approximation is 1kB per job.

PRINT JOB CONTENT UPLOADS
The printed document can be optionally uploaded to the cloud when configured to do so. This copy is used as a backup if the user's workstation is not reachable at the time of print release. The size of the content is variable based on the source document, but it is compressed prior to transfer.

INCOMING RELEASE REQUESTS AND NOTIFICATIONS
The Device Scout will issue requests to Print Scouts when a user releases a print job. Notifications on the success or failure of the request are sent from the Print Scout back to the Device Scout. These requests and notifications are a small amount of text data, less than 1kb in size.

JOB DELIVERY TO PRINTER
Print job contents are ultimately delivered from a Print Scout to the target printer. The data at this point is uncompressed.

AUTOMATIC SCOUT UPDATES
In order to provide the most up to date features and security, new versions of the Print Scout will download and install automatically unless disabled.

Device Scout

HP JetAdvantage Secure Print requires access to your local area network to operate. The following section describes how the Device Scout interacts with your environment.

- Scanning configured network ranges for printing devices
- Collecting meter data from discovered devices
- Collecting service alerts from discovered devices
- Configuring Secure Print apps on secure printers
- Logging in to a secure device

The Device Scout uses SNMPv1 and SNMPv2 to communicate with network devices. The Device Scout will also collect the same information from SNMPv3-compatible devices as long as they provide support for SNMPv1 and SNMPv2. In some cases, the Device Scout will also try to connect to a device using HTTP port 80 if the device is a known model that cannot report serial number or meter reads via SNMP.

The Device Scout will generate internet network traffic when performing the following operations:

- Registering a new Scout
- Polling the Scout control server for new configuration or instructions
- Uploading discovered device data
- Uploading device meter data
- Uploading Scout health check information
- Configuring apps on secure devices
- When users interact with a secure device
- Logging in to a secure device

The Device Scout uses secure HTTPS communication when connecting to the HP JetAdvantage cloud. Additionally, all end-user access to the application is encrypted using TLS. Unencrypted SNMP traffic is restricted to the local subnets that the scout is configured to monitor.

Device Scout Network Traffic

Here are average payload sizes for the various scout operations:

DEVICE SCOUT NETWORK TRAFFIC SUMMARY		
TASK TYPE	DEVICE TYPE	NETWORK TRAFFIC (in bytes)
Discovery	Device	15.8KB
Usage	Non-Device	0.1KB
Status	Device	16.6KB
Integration	Device	2.0KB
Printing a document from a Secure Device	Secure Device	<100KB

Note that non-printing SNMP-configured devices respond with a 126-byte payload, which tells the Device Scout that the device is not a printing device. While not harmful, this overhead may add up

over large IP ranges. Therefore, **we recommend using *Exclude Ranges* in the Device Scout configuration to skip over IP ranges that are not likely to contain output devices.**

Device Scout Communication Patterns

REGISTERING A SCOUT
When the Scout is first installed, it will include a unique registration code that identifies the Scout to HP JetAdvantage Secure Print. This registration code is unique to every Device Scout install; do not re-use or share the registration code. The Scout will attempt to open a secure HTTPS connection to identify itself using the registration code. If the code is valid, the Scout will receive a set of configuration instructions.

POLLING THE SCOUT CONTROL SERVER
Upon initial registration, and periodically during normal operation, the Scout will poll the control server for updates to its configuration state. Updates might include new IP ranges to scan, a new version to download, or a new schedule for discovering or reading devices.

UPLOADING DISCOVERED DEVICE DATA
The Device Scout will upload discovered devices once per period, configured within the application. This period can be as frequent as once per hour or once every 48 hours. More frequent uploads will result in newly discovered devices showing up within the application more quickly, but will result in more network traffic.

UPLOADING DEVICE METER DATA
The Device Scout will upload meter reads to the Scout control server on a scheduled basis, which can be as frequent as once per hour or once every 48 hours. This setting is configurable within the HP JetAdvantage Secure Print application. More frequent uploading of meter reads will result in more up-to-date information available within the HP JetAdvantage Secure Print application, but will result in more network traffic.

UPLOADING SCOUT HEALTH CHECK INFORMATION
The Device Scout Monitor runs as a scheduled Windows task to check the health of the Scout and its ability to communicate. It tracks the successful completion of Scout activities such as discoveries, status collections, and configuration updates. It uploads information about the health of the Scout on a configured basis (as frequently as once every 12 hours or as infrequently as once every 48 hours). More frequent updates will allow problems with the Scout to be detected earlier, while less frequent updates will result in less network activity.

CLOUD CONNECTION
The communication channel between the Device Scout and the cloud is kept alive by means of a server initiated ping. This request occurs approximately once a minute and consists of a small packet of bytes.

USER SIGNING IN TO A SECURE DEVICE
The Device Scout controls the behavior of apps on secure devices. When a user signs in to a device, the solution will generate network traffic attempting to authenticate locally with Active Directory. The device will then retrieve and decrypt a secure document list from the cloud. Print documents are then delivered to the device from Print Scouts.

SNMP DEVICE DISCOVERY
The Device Scout uses SNMP scanning to discover new printing devices on a configured network segment. Some network monitoring tools may treat SNMP scans as sources of network congestion. HP recommends registering the Device Scout with your network security office so that they know to expect certain traffic from the Scout.

The Scout can be configured to exclude certain subnets or IP addresses, restrict its discovery activities to certain times of the day, or reduce network utilization to a specified level.

SCOUT CONFIGURATION DATA
Device Scout retrieves its configuration data by initiating an outgoing secure HTTPS connection to the Scout control server. When the configuration has been received, the Device Scout terminates the connection and operates without any outgoing connections until the next scheduled configuration check.

AUTOMATIC SCOUT UPDATES

From time to time, a new version of the Device Scout will be released containing updated functionality and any bug fixes. By default, the Scout will check for new versions of itself on a daily basis. If a new version is available, the Scout will download the newer version and install it. Based on customer preferences, this setting can be easily be configured to notify, off or automatic.

INTERNET TRAFFIC

This section deals with internet communication with the HP JetAdvantage cloud. The data consumption can be tailored depending on whether cloud-based document storage is required.

The table below provides guidance on the internet traffic required by the solution.

MONTHLY INTERNET TRAFFIC PER USER

	Cloud storage		
Scenario	**No**	**Yes**	
Number of secure documents[1]	5	5	per day
Average document size[2]	0.5	0.5	MB
Cloud document storage	No	Yes	
Print Document information			
Transmission per document			
Document metadata	0.002	0.002	MB
Document contents[3]	0.000	0.550	MB
Job metadata for reporting	0.003	0.003	MB
Transmission per document	0.005	0.555	MB
Documents	152	152	per month
Data transmitted per month	**0.760**	**84.406**	**MB**
Workstation connection			
Keep-alive packet per minute	0.0001	0.0001	MB
Connection data month	**3.241**	**3.241**	**MB**
Other data transmission			
Print Scout daily use: Status/AD look-ups	0.004	0.004	MB
Device Scout daily use: Device meters	0.005	0.005	MB
Other data transmission daily total	0.009	0.009	MB
Other data transmission per month	**0.274**	**0.274**	**MB**
Total Internet bandwidth	**4.28**	**87.92**	**MB per user per month**

Assumptions

The guidance on traffic volume is based on the following:

1. An average 5 secure documents per day printed per user.
2. Document size can vary based on the nature of the documents printed. The calculations are based on an average document size of 500KB.
3. For cloud document storage, the Secure Print solution will first attempt to retrieve the document from the submitter's workstation. It is assumed that 10% of time the submitter's workstation may not be available. In this case, documents are retrieved from the cloud.

Worked Examples

Scenario 1. Customer with 500 users storing documents in the cloud

Traffic per user: 87.92 MB per Month

Total traffic: 500 x 87.92MB = 43.96 GB per month

Scenario 2. Customer with 1000 users not storing documents in the cloud

Traffic per user: 4.28 MB per Month

Total traffic: 1,000 x 4.28MB = 4.28 GB per month

4AA6-8661ENW, November 2016