

HP Roam security



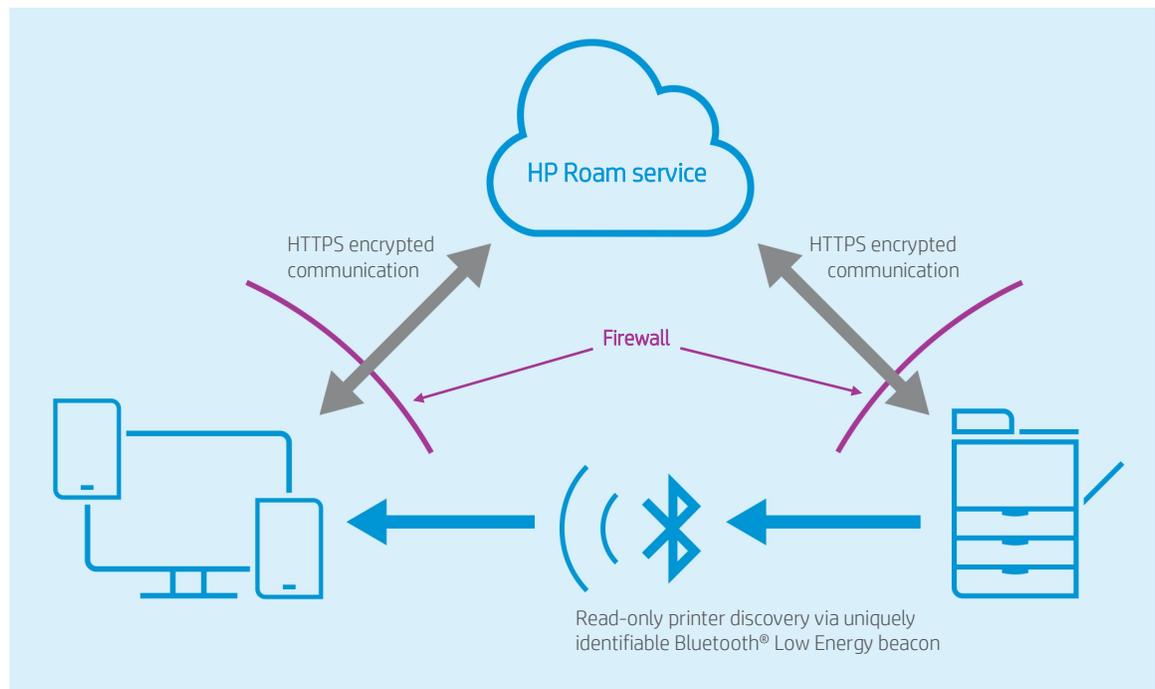
An experience-driven secure print solution

Table of contents

Data transfer architecture	2
Secure communication	2
Service instances	2
Client platforms	3
Data storage	3
Personally identifiable information (PII)	3
Scalability and reliability	3
Managed setup	4
Platform requirements	4
Supported discovery protocols	4
Password requirements	4
Firewall requirements	4
Customer information access	4
Logs	4
Facilities security	5
Privacy policy	5

HP Roam for Business (HP Roam) is an experience-driven secure print solution that allows users to print effortlessly from any device, virtually anywhere, to any HP Roam Bluetooth®-enabled printer,¹ securely through the cloud. HP Roam utilizes Bluetooth Low Energy (BLE) technology to create proximity events with mobile devices and printers. The solution is cloud-focused to support the most diverse print situations.

Data transfer architecture



Secure communication

All communication between components of HP Roam, including client-to-service and service-to-printer, are secured using transport layer security version 1.2 (TLS 1.2). TLS 1.2 uses 2048-bit level encryption and certificate validation to establish a secure channel.

Service instances

HP Roam is deployed in Amazon Web Services (AWS) on a platform of elastic compute (EC2) images. The EC2 images maintain current patching against evolving security threats. Penetration testing is also performed as part of threat review by HP Cyber Security Office (CSO).

Geographically, there is currently only a US-based instance servicing worldwide.

Client platforms

HP Roam clients for Android™ and Windows® each utilize a WebAuth token-based authentication exchange. HP Roam clients do not store users' password(s); instead, they leverage the secure credential storage mechanisms of each respective platform. Use of the secure credential storage requires elevation of access rights to the physical device using PINs, password, or other biometric access control.

For the mobility platforms (Android, iOS), the client software application (app) can only be obtained from the designated app store for each platform, i.e. Google Play and App Store. This controlled distribution route ensures integrity of the client package.

Supported platforms:

- Windows 10
- Android 5.0+
- iOS 10+: Due to the limitations of AirPrint® and its lack of support for WebAuth, iOS does a 'credentials proxy' flow. On iOS, the user's credentials are passed from AirPrint on the mobile device to the AirPrint interface within the HP Roam cloud and immediately routed to the IDM for access granting.

Data storage

HP Roam uses a hybrid combination of storage mechanisms to house data.

- For deep storage, HP Roam employs Amazon Simple Storage Service (S3). The data transferred to storage is encrypted service-side using AWS-managed advanced 256-bit AES encryption. Each object stored is encrypted with a unique key; the keys themselves are then encrypted with a rotating master key.
- S3 also provides an industry-leading level of data redundancy and durability with 99.99% availability. Allowing S3 to manage the data encryption creates a decoupled boundary among the data handling modules and a higher level of containerization.
- HP Roam also employs caching for rapid access to limited sets of data. The caching structures are housed in-memory and protected by the multifaceted security of their host instances comprised of elastic compute (EC2) images.
- HP Roam also utilizes databases to store information. The database storages are also encrypted on disk and access is limited by isolating the database in a secure environment accessible only by the abstraction layer.

A user's data is stored within the geographic instance closest to the user's defined location for service access. The geographic instances do link and share high-level cached details, such as basic account information, to provide better service latency. Print job content is stored for 72 hours. All other account information is stored indefinitely, contingent on service continuity.

Personally identifiable information (PII)

- First name
- Last name
- Email address

Scalability and reliability

HP Roam is designed from the ground up with a scalable architecture and deployment model capable of responding to increased traffic and usage spikes. Leveraging elastic compute capabilities, HP Roam can automatically and proactively deploy additional resources to meet rising demand.

Managed setup

The HP Roam setup tool is a client application capable of discovering printer resources existing inside of an environment and importing them into the managed printer section of the Roam administrative portal. The setup tool can be run once or as many times as necessary to capture printer devices. Simply run the utility on a supported platform, sign in to HP Roam with a valid account with administrative rights, and configure a discovery protocol.

Platform requirements

- Windows 10
- PC with network access

Supported discovery protocols

- Bonjour (mDNS); requires port 5353
- Active Directory
- Managed Printer Lists (MPLs)
- HP ePrint Enterprise export
- HP Web Jetadmin

Password requirements

User access credentials include a unique email address with validated owner control and a strong password adhering to the following requirements:

- Passwords must be at least 8 characters
- If passwords are less than 10 characters, they must fulfill 2 of these sub-requirements:
 - Contain at least 1 alphabetic character
 - Contain at least 1 numeric digit
 - Contain at least 1 special character
- If passwords are 10 or more characters, they must fulfill 2 or more of these sub-requirements:
 - Contain at least 2 alphabetic characters
 - Contain at least 2 numeric digits
 - Contain at least 2 special characters
- Passwords cannot contain numeric sequences, such as '1234Password'

Firewall requirements

- Port 631 IPP/IPPS
- Port 443 HTTP

Customer information access

Access to personally identifiable information (PII) and/or customer information is limited to HP Roam production team members comprised of HP and PrinterOn staff. Access is limited within a need-to-know basis.

Logs

Detailed system logs are kept on system usage, function, and access. The logs are reviewed as necessary when determined by issue reports, HP Roam service management, and/or automated service monitors.

Facilities security

HP Roam development, deployment, and management is orchestrated from HP offices worldwide as well as PrinterOn headquarters. All physical sites are access controlled with badge access.

Privacy policy

To learn more about the HP privacy policy, visit <http://www8.hp.com/us/en/privacy/privacy.html>.

Learn more

hp.com/go/roam

Product support

<https://support.hp.com/us-en/document/c06003325>

References

docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability

docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption

Notes

¹ HP Roam currently supports HP Enterprise printers and MFPs with FutureSmart 4 that are enabled with HP Roam Bluetooth® Low Energy.

Sign up for updates

hp.com/go/getupdated



Share with colleagues

© Copyright 2018 HP Development Company, L.P. 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.

AirPrint is a trademark of Apple Inc. Android is a trademark of Google Inc. Bluetooth is a trademark owned by its proprietor and used by HP Inc. under license. Windows is a U.S. registered trademark of the Microsoft group of companies.

4AA7-3388ENW, July 2018

