Technical white paper

HP Roam security

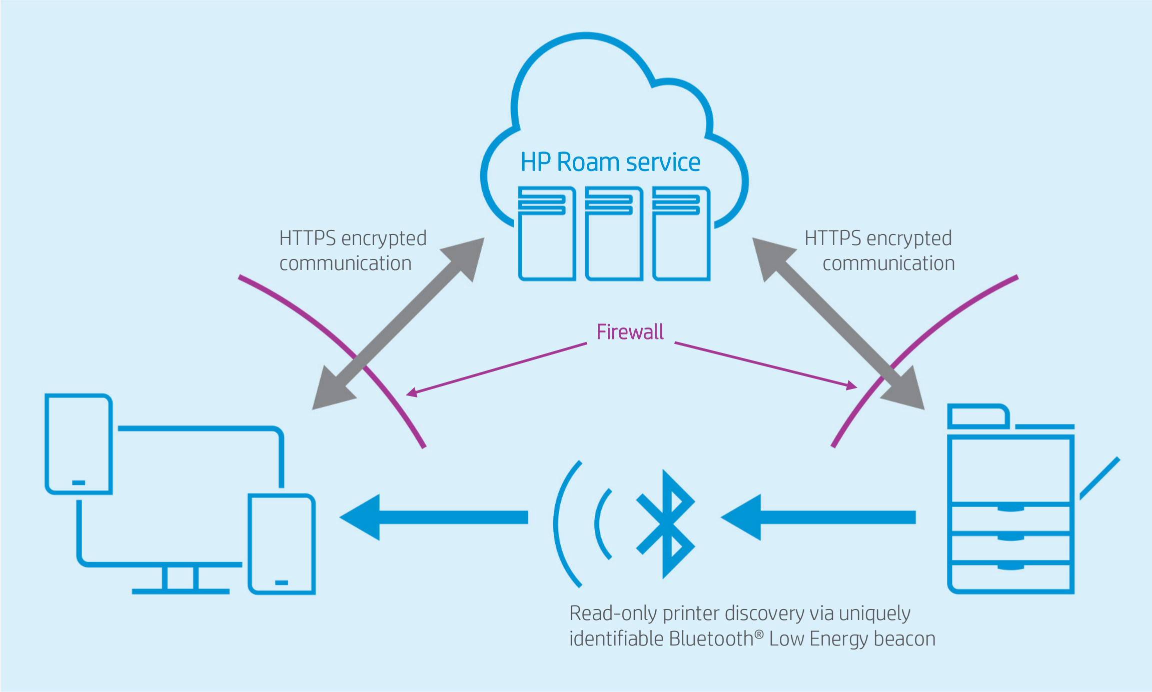
An experience-driven secure print solution

Table of contents

Click here to verify the latest version of this document

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

Data transfer architecture


HP Roam service
HTTPS encrypted communication
HTTPS encrypted communication
Firewall
Read-only printer discovery via uniquely identifiable Bluetooth® Low Energy beacon

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 RSA encryption and certificate validation to establish a subsequent 256-bit 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). EC2 cloud compute instances also constantly run intrusion detection services and scanning agents to detect vulnerable or out-of-date packages. Any issues detected are remedied immediately.

Geographically, there is currently a US-based instance located in the US-East region and a European-based instance in Frankfurt, Germany or the EU-Central region.

Client platforms

HP Roam clients for Android™ and Windows® each utilize a WebAuth token-based authentication exchange. The HP Roam clients do not store the user's password(s); instead leveraging 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 PIN, passwords, or other biometric access controls.

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 7 & 10, Android 6.0+, iOS 11+

iOS 11+: Due to the limitations of AirPrint® and the lack of support for WebAuth, HP Roam utilizes a 'transient trust' flow. With an iOS client, the user is first authenticated to the HP Roam app. As part of the iOS HP Roam app authentication process, the user's iOS device is registered with the HP Roam service. The user can then choose to install the iOS profile configuration for HP Roam. The profile configuration adds the HP Roam endpoint as a choice print destination. The first time the user sends a print job to the HP Roam destination they will see an authentication challenge requesting username and password. The user has been instructed to enter a new set of credentials in this prompt. Upon the user's submission the server identifies the user and directs a confirmation notice to the user's registered client. After the user confirms the action, the new set of credentials are stored in the iOS secure keychain and used henceforth on print submissions to HP Roam. The HP Roam service trusts the new credential set as it would a standard WebAuth flow because the new credentials were associated with an associated and authenticated WebAuth client.

Both mobile platforms (Android & iOS) support dual modes to submit print jobs to the cloud: 1) in-app or app-based print submission via the "File +" selection, and 2) native print (host OS print flow) submission.

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 are then themselves 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 by only the abstraction layer.

A user's data is housed within the geographic instance in which the user declares home. The geographic instances do link and share high-level cached details such as basic account information to provide better service latency when crossing geographic service boundaries. The point of truth for a user's data is still within their home relative HP Roam instance. Print job files are 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. HP Roam utilizes Kubernetes to configure and manage scaling triggers and events in real-time.

Managed setup

The HP Roam setup tool (Horizon) 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. Horizon 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. Passwords must include characters from at least 3 of the 4 following categories:

- Uppercase letters
- Lowercase letters
- Numerals
- Symbols

These requirements are standardized by HP’s identity management service, HP ID.

Network ports/Firewall requirements

- Outbound/Inbound IPP Print-associated requests/responses
  - Port 631 IPP/IPPS TCP (TLSv1.2)
- Outbound/Inbound IPP Print-associated requests/responses
  - Port 443 TCP (TLSv1.2)
- Port 80 HTTP

Customer information access

Access to personally identifiable information (PII) and/or customer information is limited to select HP Roam production team members comprised of HP staff. Access is limited with 2-person controls.

Logs

Detailed system logs are kept on system usage and function, as well as access. They are reviewed during processes of intervention as determined by management and automated safeguards on access and system usage.

Facilities security

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

Privacy policy

To learn more about the HP privacy policy, see HP Privacy policy.

GDPR

Adherence to HP global compliance.

Learn more

hp.com/go/roam

Product support

hp.com/go/RoamHelp

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.