Technical white paper

HP Workpath apps—Security features

Table of contents

HP Workpath overview 2
HP Workpath ecosystem 2
HP Workpath platform architecture 3
App security 4
App whitelisting, monitoring, and revocation 4
App validation and verification 6
Data security 6
Authentication and authorization 7
Data collection 9
Link Debug Bridge (LDB) auditing 9
Private certificate store 9
Regional data transfer 9
Printer security—features 10
Printer security—management 11
HP URLs to access HP Command Center 11
HP URLs needed to access cloud services 11
Non-HP URLs needed to access cloud services 12
URLs needed to access on-premise servers 13
Glossary 14

Click here to verify the latest version of this document

Introduction

The cyber threat landscape is getting more sophisticated. Security threats are increasing at alarming rates and IoT devices—including printers—are a new attack vector for hackers. These devices pose a security risk not only to the network infrastructure, but also to private information, as hackers target the weakest link on the network. HP offers the world's most secure printers,[1] and that focus on security extends to the application (app) ecosystem, which includes the HP Workpath apps that run on HP printers.

Because IoT devices include printers, HP has been working to bring state of the art computer security to modern printers. Today, HP Enterprise LaserJet and PageWide products running FutureSmart firmware have the industry's strongest security.[1] HP takes an end-to-end security architecture approach, from the design of printers themselves, to the design of management and monitoring infrastructure, mechanisms for supply authenticity verification, and secure development assurance across our supply chain.

This document is intended for app developers or service providers who need a deeper understanding of the security measures that protect the HP Workpath platform, the HP Workpath apps, and the printers they run on.

HP Workpath overview

HP Workpath, formerly HP JetAdvantage Link, is an open developer platform from HP that enables software applications to be installed on compatible HP multifunction printers (MFPs) running HP FutureSmart 4, release 4.9 or later. This platform includes Software Development Kits (SDKs) using industry standard development technologies that provides HP and independent software vendors the ability to develop apps that extend the firmware capability on more than 1.8 million HP printers in service.

The HP Workpath apps connect directly to cloud services or on-premise servers and Microsoft® SharePoint®, etc., to which documents can be sent and printed by authenticated users.

HP Command Center (HPCC) is a web interface used to purchase and deploy the apps on HP printers. HPCC provides HP service providers the ability to manage users, enable HP Cloud Sign In Once (SIO), manage app portfolios, and install apps on HP printers. For information on how to deploy apps, refer to the HP Workpath apps—Deployment Guide, which you can find in HP Command Center.

HP Workpath ecosystem

The development ecosystem offers open, industry-standard Application Program Interfaces (APIs) and robust forum support, as well as remote testing, deployment, and app management.

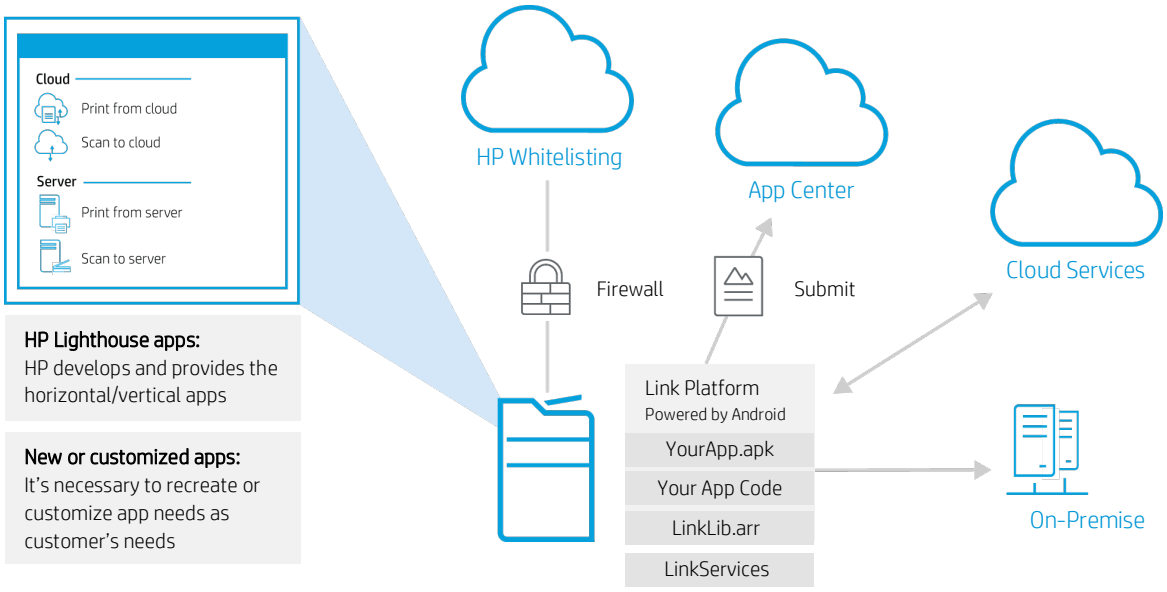
The HP Workpath platform allows independent developers to create and submit apps for use on HP printers. Developers can either create new apps or use open-sourced apps to customize an app using the capabilities of the device provided in the HP Workpath library. The ecosystem supplies all of the processes highlighted in Figure 1.

Figure 1. App development process

Apps, including executable files and metadata, are submitted by registered HP Workpath developers to the HP App Center. The apps are then vetted by HP's stringent Validation and Verification (V&V) security assessment process. All apps must be signed and whitelisted by HP before they can be offered in the Solutions Catalog in HP Command Center.

The Solutions Catalog makes it easy for service providers to find and deploy their chosen apps on printers. After the app is deployed, users can scan to or print using cloud services or on-premise servers.

Figure 2. Developer components workflow



HP Workpath platform architecture

The development ecosystem is protected by strong security features to guard the printers and any network communications that involve apps.

The HP Workpath cloud services are hosted on Amazon Web Services Cloud (AWS) servers.

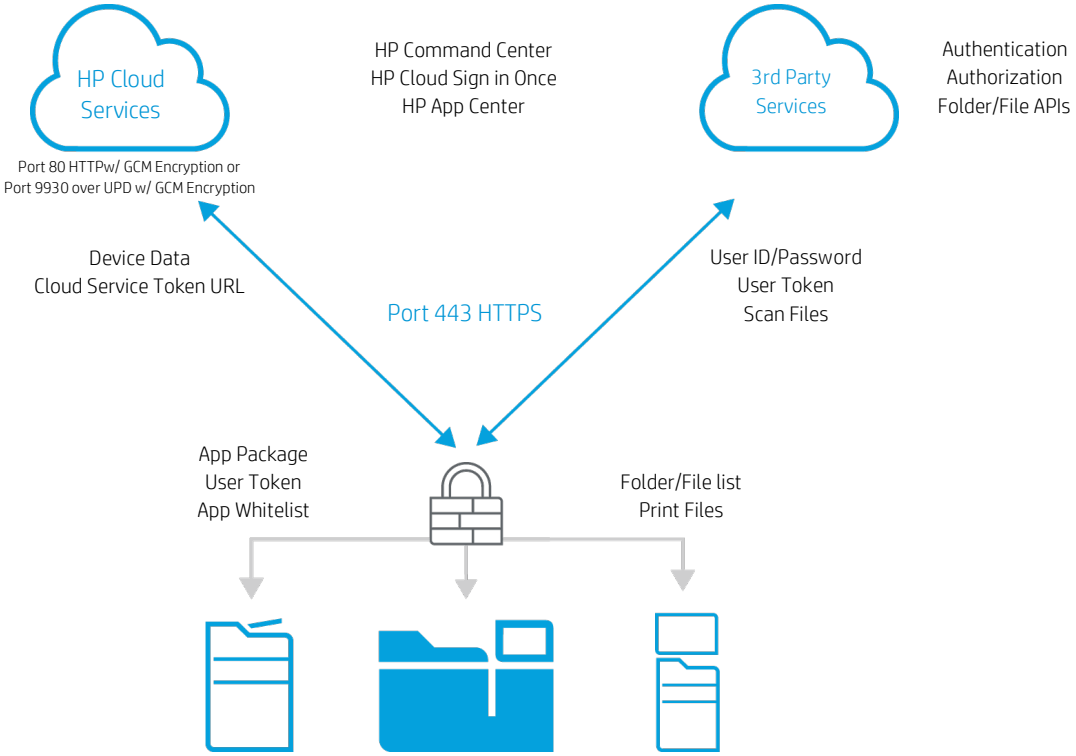
The HP cloud services infrastructure consists of multiple servers (also known as stacks) that comprise working parts of the overall system. Examples of major components in the working system are load balancers, application servers, cloud services servers, and database infrastructure.

HP's controlled identity management system (HP ID) authenticates user identity access to the HP Command Center web interface. The service provider data and customer data are secured in a database infrastructure and encrypted using industry best practices.

The diagram on the next page shows how HP printers and the HP Workpath apps securely communicate with HP and third-party cloud services.

NOTE
HTTP/port 80 and UDP/9930 are used for the signaling (frequent short polling), the use case is encrypted with GCM encryption.

Figure 3. HP Workpath secure infrastructure



App security

Apps must undergo HP's stringent Validation and Verification screening process to ensure that they are safe for use before they can be offered in the Solutions Catalog. App security is also managed using Active App Monitoring and Revocation. Even after installation, apps are actively monitored, and any issues are remediated.

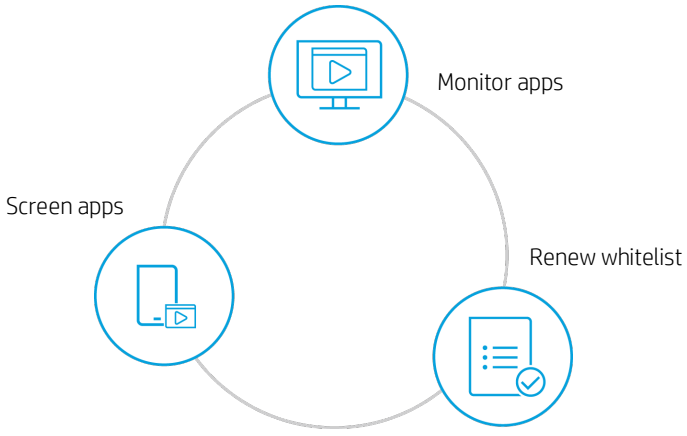
Along with app-specific security measures, HP Workpath apps are also protected by HP Sure Start, a security feature embedded in the printer that responds to any potential compromise of the BIOS by restarting with a safe "golden copy" of its BIOS. For more information, see HP Enterprise printers—Embedded security features.

App whitelisting, monitoring, and revocation

App settings

HP Workpath app settings can only be modified by authenticated Admin users.

Figure 4. HP Workpath app settings



Active app monitoring

Printers must stay connected to HP's cloud-based security web services, which monitors app installations and regularly renews every installed app's whitelisted status on the printer. If the printer is not continuously connected to HP's security web services, the whitelisted status of an installed app will not be renewed and one of the following error messages will be received every time the app is opened:

- If the whitelisted status is not renewed for more than 14 days, "`This app will be disabled in X days`" displays but the app will be allowed to operate as usual.
- If the whitelisted status is not renewed for more than 30 days, "`This app has been disabled`" displays and the app will not be allowed to launch.

These warnings and errors can be avoided by keeping the printer constantly connected to HP's cloud-based security web services.

Device data such as unique device identifiers and timestamps, and app data such as unique app identifiers, are used for active app monitoring and to maintain a whitelist.

App whitelisting and revocation

All apps that pass V&V are added to a cloud-based whitelist. Every app's whitelisted status is verified before allowing installation onto an HP printer, except when loaded through the Link Debug Bridge (LDB) for testing.

In extreme cases, an app can be removed from the whitelist at HP's sole discretion. When an app is removed from the whitelist, HP security web services will automatically revoke the app's whitelisted status on all connected printers. After the whitelist status is revoked, the printer will display an error any time an attempt to launch the app is made and the app will not be allowed to open. Its revoked whitelist status will also be displayed in the HP Command Center Solutions Catalog. If a printer has been disconnected from HP security web services, the error will ultimately result in the app being disabled within 30 days or less.

Bug bounty

By using a bug bounty program, HP integrates and leverages highly trained, geographically diverse ethical hackers with deep, hard-to-find technical skills and unleashes them to find obscure, previously unidentified vulnerabilities. A bug bounty program provides an incentive to ethical hackers by rewarding them for each vulnerability they discover in our product.

Our goal is to find obscure product vulnerabilities that are missed during product development and penetration testing processes. In today's cybersecurity environment, there are white hat hackers and black hat hackers.

White hat hackers are considered ethical hackers who use their skills for overall security improvement. They work with manufacturers to inform them about a potential vulnerability and allow the standard quiet period of 90 days before public disclosure to allow the manufacturer time to develop patches for the vulnerabilities. On the other hand, black hat hackers are highly sophisticated hackers seeking to penetrate challenging targets, such as government bodies and large businesses. Often, these black hat hackers are looking to cause destruction, steal valuable data, or develop new methods and means of cyberattacks.

The bug bounty program allows HP to take security to the next level by leveraging community-based testing using white hat hackers. Workpath utilized HP's bug bounty program during the beta testing phase prior to release of the product.

Penetration testing

HP has been performing penetration testing of our products for over 10 years. Our testing is based on automated scans and manual testing of application and printer interfaces to effectively identify vulnerabilities. Workpath went through extensive penetration testing by HP cyber security experts.

Software Development LifeCycle

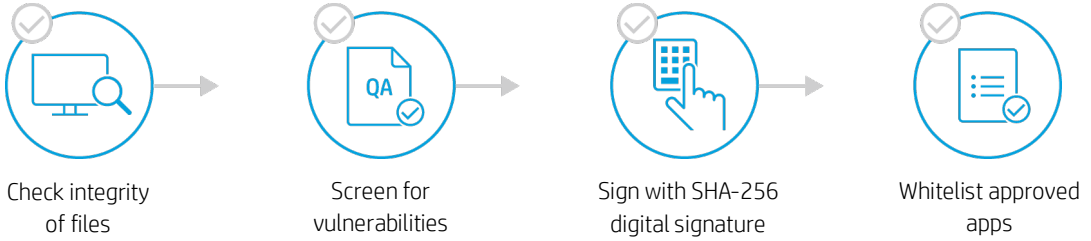
HP recognizes the importance of not only the security mechanisms and solutions designed from the ground up into our products, but also how we design, deliver, and support those offerings throughout their entire lifecycle. For this reason, HP has made it a priority to develop and maintain a company-wide Secure Development LifeCycle (SDLC) program which includes all aspects of a product's deliverables, including firmware, to guide and oversee our development teams' use of industry-accepted best practices, from design through product end-of-life. In today's R&D ecosystem and because our pace of innovation requires it, our SDLC program extends across our vast supply chain ecosystem, including secure development requirements for our suppliers and partners. We continuously work to improve our SDLC processes and methodology, both for internally developed technologies and to improve our ability to collaboratively address security issues in technology components provided by our partners and suppliers.

To validate that HP's development teams and our partners and suppliers are incorporating security best practices into their development processes, HP has partnered with Security Innovations to provide SD-PAC certifications. Security Innovation's Secure Development Process Assessment Certification (SD-PAC) is a rigorous security validation and certification program for software/firmware vendors to validate their use of security development best practices in the development of products. This independent certification helps assure users of HP commercial print and MFP devices that robust software development practices were incorporated into the development processes. The certification is based on industry-leading SDLC methodologies proven to reduce overall risk.

App validation and verification

To validate and verify that an app is whitelist approved, the printer uses App Integrity Checking, Security Screening, and Digital Signature verification in addition to ongoing security screening.

Figure 5. App validation and verification process



App integrity checking

The printer validates the digital signature and the integrity of app files during the installation, except when loaded through the Link Debug Bridge (LDB) for testing on a printer set to developer mode. In this setting, the device cannot have any live whitelisted apps installed.

Ongoing security screening

Because new security vulnerabilities are continually discovered, HP's Cyber Security team is continuously updating its test suite to screen for those new vulnerabilities. As the test suite changes, all HP Workpath apps are re-screened. If a major threat is discovered in a whitelisted app, the app developer will be notified, and is expected to publish a fixed version in a reasonable amount of time. In extreme cases, an app can be removed from the whitelist at HP's sole discretion.

Security screening and signing

All apps are screened by HP's Cyber Security team for known security vulnerabilities. Only apps that have passed these Verification and Validation (V&V) tests, and have subsequently been signed by HP using a SHA-256 HP digital signature, will be offered for installation onto HP printers, except when loaded through the Link Debug Bridge (LDB) for testing. The V&V security review includes, but is not limited to:

- Threat surface analysis of the app
- Running a customized tool looking for known vulnerabilities and ensuring compliance with the Open Web Application Security Project (OWASP) and mobile app security best practices launch

Data security

The security of HP customers' printers, accounts, data, and personal information is top priority for HP.

Data in transit is secured with secure encryption (HTTPS/TLS). Data at rest is secured via an RSA + AES-256 hybrid cryptosystem or AES-256 encryption, e.g. cloud service tokens.

HP Workpath apps use an RSA + AES-256 hybrid cryptosystem or AES-256 encryption, e.g. cloud service tokens, to secure user and app information.

All data gathered by HP is safeguarded per the principles of the HP Privacy Statement.

All communications between HP printers, HP cloud services, and third-party cloud services (Microsoft, Google™, etc.) are initiated by the HP printer and are in a secure session via HTTPS/TLS over port 443, which is an industry-standard protocol used by internet browsers. The use of Port 80 for signaling with GCM encryption via HTTP is required and may also require Port 9930 over UDP using GCM Encryption if Port 80 is blocked in the firewall environment.

NOTE
The printer will attempt to use both HTTP/80 and UDP/9930 during onboarding. It will periodically attempt to use UDP even if HTTP is permitting communications across the firewall. UDP/9930 is not a mandatory requirement, but one of the two ports (HTTP/80 and/or UDP/9930) is required and is expected behavior when configuring your firewall.

The HP Workpath apps also communicate with HP cloud services and third-party cloud services in a secure session via HTTPS/TLS over port 443.

To use the HP Workpath apps platform, HP printers and HP apps must have access to internet port 443.

Authentication and authorization

HP verifies the identity of users, printers, apps, and third-party service providers using secure authentication processes.

User authentication

HP Command Center and HP Cloud Sign In Once (SIO) use HP's controlled identity management system, HP ID, to authenticate user credentials.

HP ID requires users to provide their first name, last name, email address, and country as part of account creation. HP Command Center allows a user to individually or bulk onboard end users for Sign In Once (SIO) where this information is provided for a list of end users.

HP App Center authentication

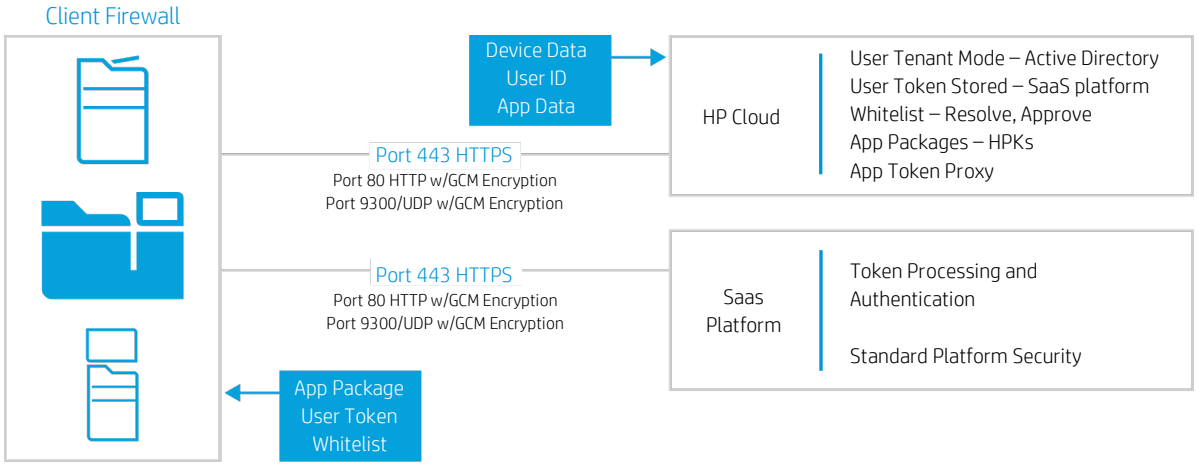
App data such as the app file (hpk) are used to publish the app in the catalog and install the app.

HP Command Center authentication

Device data such as unique device identifiers, network connection information, firmware version, and device configuration are used to onboard the device, configure the device, upgrade firmware, and install apps.

HP Command Center is a multi-tenant system that can support multiple entities of both service providers and customers to which HP printers are linked. The following diagram shows the hierarchical structure used to separate these entities. Only users with proper authentication can access HP printers or service provider and customer data.

Figure 6. HP Command Center architecture



HP app authentication

Some HP Workpath apps use a web view to display an authentication page hosted by a third-party. The authentication page provides Sign In Once (SIO) integration with the app.

HP Workpath apps never have access to their client secrets, which are never hard coded in the app and are only managed via HP App Center and accessed via the cloud by token proxy.

HP app attestation and token proxy validates an app's identity via the app's ID, signature, and secure hash. After HP App Attestation verifies the app's identity, an app token is returned. The app supplies this app token along with the Client ID and information about the service's token endpoint to the token proxy.

Device data, such as unique device identifiers, are used to attest the device and app data, such as unique app identifiers, are used to attest the app.

The token proxy retrieves the client secret for this token from App Center and calls the service's token endpoint to obtain tokens. The returned tokens are returned to the app. This ensures that a malicious app cannot masquerade as an authentic app and gain access to the client secrets.

The following HP Workpath apps use a web view authentication hosted by the third-party service (not HP) that applies OAuth2:

- HP for Box
- HP for Clio
- HP for Google Drive
- HP for OneDrive
- HP for OneDrive Business
- HP for SharePoint Online
- HP for Dropbox
- HP for SAP Concur

The following HP Workpath apps use an app authentication via third-party services that apply proprietary authorization protocols to accept credentials and authenticate:

- HP for iManage
- HP for Sage Intacct

For more information on app authentication security, see Third-party service authentication.

Printer authentication

HP printer operations—such as enabling Cloud Sign In Once (SIO), enabling the HP Workpath platform, and installing apps—can be performed by authenticated users via HP Command Center. HP printers verify that these commands are coming from HP Command Center using a unique cryptographic identity provided by the web interface.

HP printers are onboarded by an authenticated user from the printer control panel and a mobile or PC Internet browser. To ensure the security of the printer during this process, HP Command Center and HP Sign In Once (SIO) verify that the printer is an HP-manufactured printer via the unique cryptographic identity provided by the HP printer.

HP Sign In Once (SIO) authentication

Device data such as unique device identifiers, app data such as unique app identifiers, and user authentication data such as email address and HP Cloud password are used to authenticate the user and crypto-sandbox the app and user data.

Similar to HP Command Center, HP Sign In Once (SIO) is a multi-tenant system that can support multiple entities of both service providers and customers to which HP printers are linked. Only users with proper authentication can access HP printers or service provider and customer data because these entities are separated (see HP Command Center authentication on page 7.

When a user links their local authentication account with their HP Cloud account they will be asked to read and agree to the following statements:

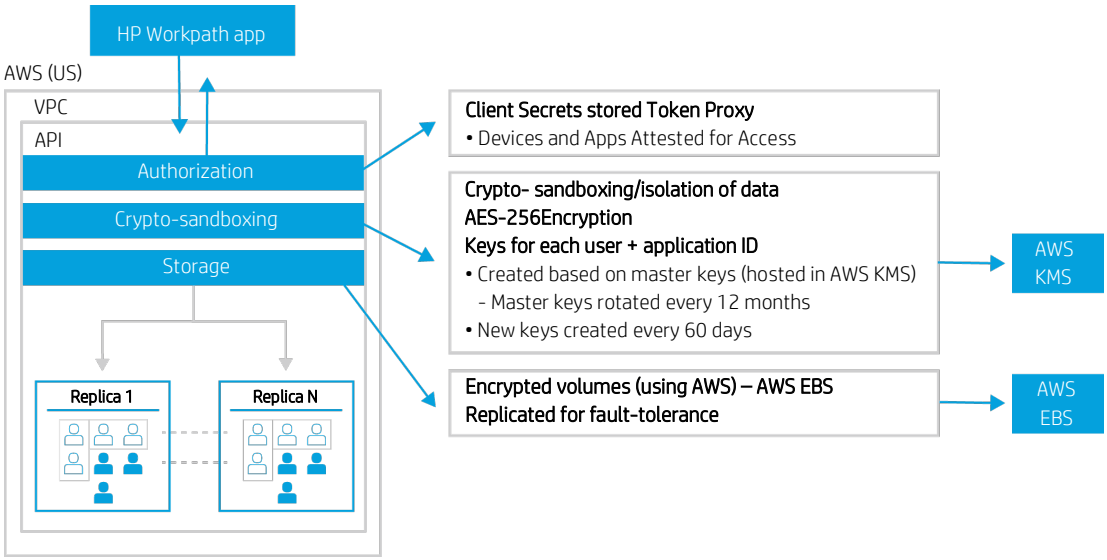
- HP Cloud EULA
- HP Privacy Statement

After successful HP ID authentication, the user is prompted for a PIN required to access HP Sign In Once (SIO). The PIN must meet the following requirements:

- PIN must be 6 numeric digits
- PIN must meet randomness rules—no consecutive 3 digits with the same value, no +1/-1 progression members
- On PIN changes, any new PIN cannot match the current PIN

HP Workpath apps have the capability to store user tokens in the app's sandbox. The key to these tokens is a combination of Authentication Agent provider, domain, and user ID. The tokens are stored encrypted with the RSA + GCM hybrid cryptosystem or AES-256 encryption.

Figure 7. HP Workpath apps Cloud SIO security protection



After the account is linked to the printer, an HP Workpath app can be authorized to use cloud SIO on behalf of the authenticated HP Cloud user and the app. During this process, App Attestation validates the app's identity. After the app's identity is verified, the app requests access to the user's Cloud SIO storage for this app via the Token Proxy to retrieve a cloud SIO token.

The app will use the cloud SIO token to store user tokens in the cloud SIO. Cloud SIO crypto-sandboxes these tokens by encrypting them with AES-256 encryption using a unique key per user and an application ID. These encrypted tokens are stored in encrypted volumes in the AWS Elastic Block Store (EBS).

Data collection

HP does not track customer names, even during report generation. HP Cloud Services refer to customers with untraceable IDs. While reports do have customer names, HP personnel have no access to a service provider's customer usage data.

Link Debug Bridge (LDB) auditing

Device data such as unique device identifiers and user authentication data such as email address and HP Cloud password are used to enable Link Debug Bridge (LDB).

Private certificate store

Some HP Workpath apps support a private certificate store to store trusted CA public certificates. Administrators can install public certificates for these apps directly in the app using the private certificate store.

This store is protected with a random 256-bit password encrypted with the RSA + AES-256 hybrid cryptosystem. The following apps can use certificate signing to create a secure connection:

- HP for iManage
- Secure Access

Regional data transfer

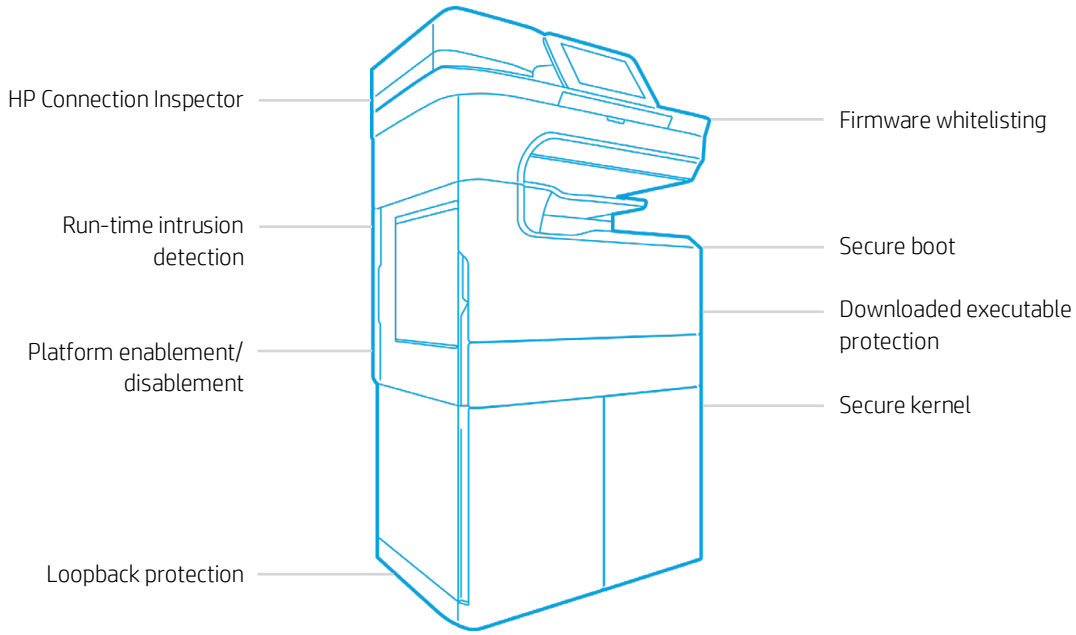
Data is protected within the confines of a certain region. The HP Workpath ecosystem elements are hosted in the following locations:

- HP App Center is hosted in AWS US
- HP Cloud Sign In Once (SIO) is hosted in AWS US
- HP ID is hosted in AWS US
- HP Command Center is hosted in AWS Frankfurt and complies with GDPR Privacy requirements
- HP Web Services is hosted in AWS US

Printer security—features

HP Enterprise and Managed printers and MFPs are protected by embedded security feature HP Sure Start to protect the printer BIOS. In addition, run-time intrusion detection continuously monitors memory for any abnormal behavior on the printer. These security features and others are described in the following sections.

Figure 8. Printer security features



HP Connection Inspector—In HP Enterprise and Managed devices, unique HP technology is used to inspect outgoing network connections to detect potential malware attacks and prevent that malware from "calling home" to malicious servers, stealing data, and compromising the network. Network activity is monitored for suspicious activity. Unfamiliar or distrusted requests are halted, and a warning is sent to IT administrators. When a potential malware attack is suspected, the printer goes through a self-healing process by rebooting the device and returning it to the pre-malware-attack state.

Downloadable executable protection—HP Workpath apps are not allowed to download executable code after installation. This prevents any attacks that could harm the printer BIOS or network.

Firmware whitelisting—Firmware whitelisting validates the integrity of firmware system files (including the Link for Device system files) during the load process using a SHA-256 hash signed with HP's digital signature. If the validation fails, the printer reboots to the pre-boot menu to prevent a potential malware exploitation from executing.

Link Debug Bridge (LDB) auditing protection –The Link Debug Bridge (LDB) facility can only be enabled by app developers registered with printer administrator authority. The developer's identity is verified with the HP cloud-based security web services. LDB audit logs include the device serial number, model number, and firmware version. The LDB allows registered app developers to install, test, and debug their unverified app code on HP printers.

When LDB is enabled, a warning is displayed in the Message Center on the printer control panel, alerting users to this potential security issue. HP Security Manager[2] can also detect devices where LDB is enabled, and alert customers to this potential security issue. If LDB is disabled, all installed apps are automatically removed.

Loopback protection—HP Workpath apps are not able to bypass network security by making network requests over loopback connections.

Platform enablement—The HP Workpath platform is disabled by default and apps cannot be loaded onto printers unless the platform is enabled for each printer by an authorized printer administrator.

Run-time intrusion detection—In HP Enterprise and Managed devices, run-time intrusion detection detects potential malware intrusions in system memory by running in the background to validate the memory space. In the event that the device detects memory anomalies, the device goes through a self-healing process by rebooting the printer. If the auto-recover feature is disabled, or a possible intrusion occurs twice within 30 minutes, the printer reboots to the pre-boot menu to prevent a potential malware exploitation from executing. The printer will attempt to wait until in-process print jobs have been cancelled before rebooting.

Secure boot—Each time HP Pro devices are powered on, the Link for Device kernel is scanned for unexpected modifications. In addition, the root and system mass storage partitions are verified using device-mapper-verity (dm-verity). The boot sequence will be stopped if any unexpected modifications are found.

Secure kernel—The HP Workpath platform uses the most secure kernel available.

HP Sure Start—This feature on HP Enterprise and Managed devices automatically validates the printer's BIOS and responds to any potential compromise of the BIOS by restarting with a safe "golden copy" of its BIOS.

Printer security—management

Use the following information to manage security on HP printers and enable HP Workpath apps to access the internet from a local network.

HP URLs to access HP Command Center

When a user activates their account for HP Command Center they will be asked to read and agree to the following statements:

- HP Command Center EULA
- HP Command CenterTerms of Service
- HP Privacy Statement

As part of the onboarding process, users will also be prompted to enable HP Web Services (if not already enabled), and to read and agree to the HP Web Services EULA.

HP URLs needed to access cloud services

HP Workpath apps access HP Cloud Services via multiple HP owned URLs in order to use the HP Workpath platform.

HP URLs that must be accessible to the printer

The following URLs must be accessible to the HP printer. This may include the printer trusted sites list as well as firewall exceptions:

- HP App Attestation and Token
  https://*.api.hp.com
- HP App Center
  https://*.smartcloudprint.com
- HP Cloud Sign In Once (SIO)
  https://*.mymfpprogram.com
- HP Command Center
  https://*.smartcloudprint.com
- HP EULA and Privacy Statement
  https://*.smartcloudprint.com
- HP Web Services
  https://*.avatar.ext.hp.com
  http://*.avatar.ext.hp.com
  UDP://*.avatar.ext.hp.com:9930

NOTE
All communications between HP printers, HP cloud services, and third-party cloud services (Microsoft, Google, etc.) are initiated by the HP printer and are in a secure session via HTTPS/TLS over port 443 and Port 80 for signaling with GCS encryption. This is an industry-standard protocol used by Internet browsers.

HP URLs that must be available from a web browser

The following URLs must be accessible from a web browser. These sites might also need to be added as firewall exceptions:

- HP App Center
  - https://*.smartcloudprint.com
- HP Command Center
  - https://*.smartcloudprint.com
  - https://*api.hp.com

Non-HP URLs needed to access cloud services

HP Workpath apps also access third-party cloud service URLs and local URLs. The following URLs must be accessible to the HP printer. This may include firewall exceptions and/or adding these URLs to the printer's Trusted Sites List.

Figure 8. Client ID list for selected apps

App Name	Client ID
HP for Box	t6dvrexqc80ks448bndp3qnuewzqcma4
HP for DropBox	25ytu7s3v6h45j0
HP for Google Drive	829638088362-dpjpclmpa1vfj3sucumm2nrqac1mtgfi.apps.googleusercontent.com
HP for OneDrive	84033ce7-f809-43e1-a7f0-1c2469c9e230
HP for OneDrive Business	84033ce7-f809-43e1-a7f0-1c2469c9e230
HP for SharePoint Online	c766abae-c90b-4ef0-bbca-536371018c3f

- Microsoft Services (MSFT)
  - https://localhost/callback
- HP for Box
  - https://*.box.com
  - https://*.linkbox.com
- HP for Clio
  - https://*.clio.com
- HP for Google Drive
  - https://www.googleapis.com
  - https://account.google.*
- HP for OneDrive
  - https://graph.microsoft.com
  - https://*.live.com
- HP for OneDrive Business
  - https://graph.microsoft.com
  - https://*.microsoftonline.com
  - https://*.live.com
- HP for Sage Intacct
  - https://api.intacct.com

- HP for SharePoint

  https://graph.microsoft.com

  https://*.microsoftonline.com

Below you may find additional references for the following cloud services and how to configure the HP Apps within your Admin Console and whitelist their Client IDs:

- Get started with Office 365 Management APIs
- Box Application Settings for Your Enterprise
- Box Managing Custom Apps
- How to manage apps for your Dropbox Business team
- Integrate Drive with Third-party Apps
- Allow Third-party Apps for Drive files

URLs needed to access on-premise servers

The following apps rely on URLs configured to connect to the on-premise servers:

- Scan to Email—Must be configured to access the SMTP server
- Scan to FTP—Must be configured to access the FTP server
- Scan to SMB—Must be configured to access the SMB server folder
- Secure Access—Must be configured to access the LDAP server

Support

For support or more information, contact your HP representative or service provider.

Glossary

Term	Description	**Function**
Active App Monitoring	Apps are continually monitored to verifythat whitelisting is current	Active App Monitoring and Revocation
App Integrity Checking	Validates the digital signature and files of the app during installation	App Validation and Verification
App Whitelist Revocation	Revokes the whitelist status of the app and prevents the app from launching	Active App Monitoring and Revocation
App Whitelisting	Only HP whitelisted apps can be installed on HP printers	App Validation and Verification
Connection Inspector	Detects suspicious network communications	Device Ecosystem Security
Downloaded Executable Protection	Blocks executable code from being downloaded after installation	Device Ecosystem Security
Firmware Whitelisting	Validates the integrity of firmware system files	Device Ecosystem Security
Link Debug Bridge Auditing (LDB)	Creates audit logs for the Link Debug Bridge (LDB) used for testing and debugging apps.	Device Ecosystem Security
Loopback Protection	Blocks loopback connections	Device Ecosystem Security
Ongoing Security Screening	Apps are continually re-screened to guard against newly discovered security threats	Active App Monitoring and Revocation
Platform Enablement	The platform is disabled by default and can only be enabled by an authorized printer administrator	Device Ecosystem Security
Run-time Intrusion Detection	Validates firmware while the printer is running	Device Ecosystem Security
Secure Boot	Scans the printer for unexpected modifications when the printer is powered on	Device Ecosystem Security
Secure Kernel	Controls access to system resources	Device Ecosystem Security
Security Screening and Signing	Apps are reviewed and signed by the HP Cyber Security team	App Validation and Verification

[1] Based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/printersecurityclaims.
[2] HP Security Manager must be purchased separately. To learn more, please visit hp.com/go/securitymanager.

4AA7-9734ENW, May 2021, Rev. 1