HP Workpath Apps - Security Features
# Table of contents

1 Introduction ............................................................................................................................................................................................... 1

2 HP Workpath overview ............................................................................................................................................................................. 3

3 HP Workpath ecosystem ........................................................................................................................................................................... 5

4 HP Workpath platform architecture ....................................................................................................................................................... 7

5 App security ............................................................................................................................................................................................... 9
   App Whitelisting, Monitoring, and Revocation ......................................................................................................................................................................................... 9
   App Validation and Verification .............................................................................................................................................................................. 11

6 Data security ............................................................................................................................................................................................. 13
   Authentication and Authorization ................................................................................................................................................................................. 14
   User authentication ................................................................................................................................................................................................. 14
   HP App Center authentication .................................................................................................................................................................................... 14
   HP Command Center authentication .................................................................................................................................................................................. 14
   HP App authentication ............................................................................................................................................................................................. 15
   Printer authentication ............................................................................................................................................................................................. 15
   HP Sign In Once (SIO) authentication ................................................................................................................................................................. 16
   Data collection ................................................................................................................................................................................................. 17
   LDB auditing ................................................................................................................................................................................................. 17
   Private certificate store .................................................................................................................................................................................... 17
   Regional data transfer .................................................................................................................................................................................... 17

7 Printer security .......................................................................................................................................................................................... 19

8 Manage printer security ............................................................................................................................................................................... 21
   HP URLs to access HP Command Center ................................................................................................................................................................. 21
   HP URLs needed to access cloud services ................................................................................................................................................................. 21
1 Introduction

While network security is a priority for IT and leaders, many organizations neglect security of endpoints on the network, such as HP Multifunction Printers (MFPs). HP offers the most secure printers, and that focus on security extends to the app ecosystem and the HP Workpath Apps that run on HP printers. These apps are developed through the HP Workpath platform.

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, and those making printer purchasing decisions who need to ensure their accounts, data, documents, and printers are protected.
HP Workpath, formerly HP JetAdvantage Link, is a new open developer platform from HP that enables software applications (apps) to be installed on compatible HP Multifunction Printers (MFPs) running HP FutureSmart 4. This platform includes Software Development Kits (SDKs) in industry standard development technologies that will be used by HP and independent software vendors to develop apps that extend the firmware capability of more than 1.8M HP printers in service, the world’s largest install base of office printing technology.

The HP Workpath Apps provide a direct connection to cloud services or on-premise servers and network folders, etc. to which documents can be sent and printed by authenticated users.

HP Command Center is a web interface used to purchase and deploy the apps on HP printers. HP Command Center 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 using HP Command Center.
3 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.

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 (VAV) 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 3-1 Developer components workflow
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.

An HP controlled identity management system authenticates user identity access to the HP Command Center web interface. Service provider and customer data are secured in a database infrastructure and encrypted using standard practices.

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

**Figure 4-1** HP Workpath secure infrastructure
App security

Apps must undergo HP’s stringent Validation and Verification (VAV) 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 be actively monitored, and any issues are remediated.

Along with app-specific security measures, HP Workpath Apps are also protected by HP SureStart, 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.
Active App Monitoring

Printers must stay connected to HP’s cloud-based security web services, which monitors app installations and renews every installed app’s whitelisted status on the printer regularly. 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 VAV 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 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 (HPCC) 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.
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.

**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.

**Security Screening and Signing**  
All apps are screened by HP's in-house Global Cyber Security team for known security vulnerabilities. Only apps that have passed these VAV 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 LDB for testing. The VAV security review includes, but is not limited to:

- Threat surface analysis, including new features and products
- Static and dynamic code scanning tools, such as Fortify, WebInspect, and/or Coverity
- Penetration testing by industry-leading vulnerability assessment scanners, such as Qualys and/or Nessus by Tenable
- Adherence to Open Web Application Security Project (OWASP) secure coding practices

**Ongoing Security Screening**  
Because new security vulnerabilities are continually discovered, HP's Global Cyber Security team is constantly 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.
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 tenants 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**. This is an industry standard protocol used by Internet browsers.

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**.

In order 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 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 6-1  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 Single Sign On integration with the app.

**HP Workpath Apps never have access to their client secrets**, which are never hard-coded in the app and 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 used to attest device and app data such as unique app identifiers used to attest 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

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) or enabling the HP Workpath platform, and installing apps – can be performed by authenticated users via HP Command Center. HP printers authorize 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 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, crypto-sandbox 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).

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’s 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
- 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 + AES-256 hybrid cryptosystem or AES-256 encryption.

Figure 6-2  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.

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 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 Command Center** is hosted in AWS Frankfurt and complies with GDPR Privacy requirements.
- **HP Web Services** is hosted in AWS US.
Printers are protected by embedded security features such as Firmware Whitelisting and HP SureStart, etc. that ensure the printer BIOS and/or network is protected before, during, and after the installation of HP Workpath Apps.

Figure 7-1 Printer security features

**Connection Inspector**

Unique HP technology is used to inspect outgoing network connections to stop 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.

**Downloaded Executable Protection**

Link for Device 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 JetAdvantage Security Manager 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 or HP JetAdvantage Link 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

Run-time intrusion detection detects potential malware intrusions in system memory by running in the background to validate the memory space, then rebooting the printer if a possible intrusion is detected. 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 the printer is 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.

SureStart

HP SureStart is a feature that 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.
Manage printer security

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’s EULA
- HP Command Center’s Data Use Statement
- 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 Proxy
  - https://core.api.hp.com
- HP App Center
  - https://coresvcs.dp.smartcloudprint.com
- HP Cloud Sign In Once (SiO)
  - https://mymfpprogram.com
- HP Command Center
  - https://sdp-onboarding.smartcloudprint.com
- HP EULA and Privacy Statement
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 Web Services
  - https://entitydiscovery.avatar.ext.hp.com
  - https://registration.pod1.avatar.ext.hp.com:443/avatar/v1/entities

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.

- 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

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

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