HP Insights and HP Secure Print

HP Insights and Secure Print 4.2 Release Notes – May 2025

This release represents the latest version of HP Insights. This update includes several important new features including:

- Print Scout Updates
  - Support for Microsoft Windows on Arm devices
  - Support for Windows Protected Print (WPP)
  - Support for Ubuntu 24.04
- Secure Print Updates
  - Added folder search capability for OneDrive, SharePoint and Network Folder Scan Destinations (Secure Scan)
  - IPv6 Support for HP devices (Secure Print)
- Secure Print Mobile App Update
  - Fixed a Secure Print mobile app issue on iOS devices
  - Updated the Secure Print mobile app on Android devices to use the latest MAUI platform

Print Scout Updates

The Print Scout component (v8.0.1.103) has been updated with the following new features:

- Support for Microsoft Windows on Arm devices
- Support for Windows Protected Print Mode (WPP)
- Support for Ubuntu 24.04

Support for Windows on Arm devices

Starting with HP Insights 4.2, Print Scout has been updated to support ARM64 machines. However, in this release, only the following HP Insights features are supported. Other features may be made available in future updates.

- Secure Print
- Print Analytics

Note: Installing Print Scout on an Arm-based PC is the same as installing on an Intel-based PC.

Support For Windows Protected Print

Windows Protected Print (WPP) is a secure printing mode introduced by Microsoft in October 2024. It enhances print security by using the Microsoft IPP Class Driver and is designed to work with Mopria-certified printers. WPP modernizes the print infrastructure by eliminating the need for traditional print servers and vendor-specific drivers, offering simplified, secure, and driverless printing experience.

Windows Protected Print mode is supported on Windows 11 24H2 or newer.

Windows on Arm-based devices

For Arm-based PCs, enabling or disabling WPP does not have effect on the Print Scout installation. HP Insights will always use the **Microsoft IPP driver.**

Windows on Intel-based devices

If WPP is enabled, HP Insights uses the **Microsoft IPP driver**. If WPP is disabled, it defaults to the **HP Secure Printer**.

Below are known issues related to WPP mode on Windows 11 2H42 Intel machines.

- **Make sure to enable WPP first before installing Print Scout 8.0 on Intel machines**
  Enabling WPP after Print Scout 8.0 is installed creates two instances of the **HP Secure Printer** because Windows restores the old **HP Secure Printer.** Users will end up with HP Secure Printer with the HP Universal Print Driver as well as the new HP Secure Printer with Microsoft Class IPP Driver. This may confuse users.

HP recommends enabling WPP first before installing Print Scout 8.0 to prevent this issue from occurring.

HP recommends the following steps in Windows 11 when recreating the HP Secure Printer after WPP is turned on.

1. Uninstall Print Scout.
2. Reboot the workstation.
3. Setup Windows Protected Print (WPP) mode.
4. Install the latest Print Scout.

Note: We are partnering with Microsoft to address the issue. Stay tuned for updates.

- Upgrading to Print Scout 8.0 is not recommended if WPP is enabled
  Upgrading from older versions of Print Scout to Print Scout 8.0 or later is discouraged when WPP is enabled. We recommend a fresh installation of the Print Scout 8.0 to avoid potential issues.

Known Issues and Limitations

- Fresh install: It’s advisable to start with a fresh install of Windows 11 24H2 machines. Enabling WPP first before installing Print Scout can help avoid issues such as the reappearance of the 'HP Secure Printer' queue
- Multi-Tenant Package Setup: Queue removal and re-adding of queues may not work when switching regions on Arm-based devices or on machines with Windows Protected Print mode enabled.

Support for Ubuntu 24.04

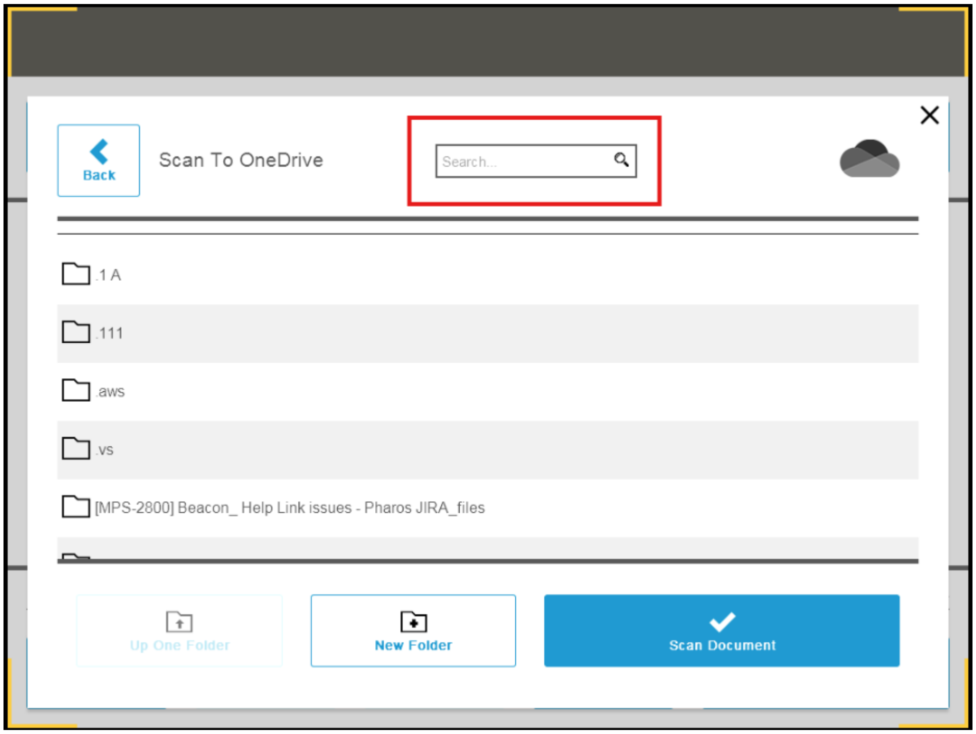
A new version (v2.2.0) of the Linux Print Scout is now available. This adds support for Ubuntu 24.04.

Secure Print Service Updates

This section includes the updates to the HP Secure Print Service.

Added search capability for OneDrive, SharePoint and Network Folder Scan Destinations (Secure Scan)

Users can now search for specific folders by name when selecting **OneDrive**, **SharePoint,** or **Network Folder** as a scan destination. This feature is useful for users with many folders, making the selection process faster and more efficient.



The **Up One Folder** option found at the bottom of the screen allows users to navigate through folders.

Notes:

- The initial screen of Scan to SharePoint is case-sensitive.
- Searches using the search icon are based on the first letter or word of the folder or file name.
- When searching within a folder, results are limited to that folder and its contents.
- If no matches are found, a blank screen is shown, meaning no folders or files are listed.
- Clicking the search icon again reloads the default list of folders and files.
- Special characters are supported in search queries, meaning you can include them when searching for folders or file names that contain these characters.

IPv6 Support for HP Devices (for Secure Print)

HP Insights 3.5 introduced IPv6 support for Insights and Direct Print, providing an expanded IP address space. With HP Insights 4.2, Secure Print now supports HP devices. This enables secure print job releases on IPv6 networks.

Bugfix

Addressed an issue with the "Oops! secure print is currently unavailable" message persisting on printers even after toggling offline print settings.

Secure Print Mobile App Updates

Bugfix: Resolved unresponsive screen issue on iOS devices

The latest version of the Secure Print mobile app (iOS) resolved an issue on certain models where the screen became unresponsive, preventing users from proceeding.

Update: Secure Print mobile app on Android devices

Updated the Secure Print mobile app Android app to use the latest MAUI platform.

Component Release Versions

This release includes the following software components and release versions.

*Note: Secure Print mobile apps and the Chrome extension are published after the Cloud Services are updated.

Software Component	Release Version	Build Date
Device Scout	1.23.9.103 (Not updated)	July 2024
Print Scout (Windows)	8.0.1.103	May 2025
Print Scout (Mac)	2.29.1.101	May 2025
Print Scout (Linux)	2.2.0	May 2025
Secure Print Site Service – Local Connector	2504.2210.4259 (tagged version) 25.4.32322.0 (MSI version)	May 2025
Secure Print Site Service – Cloud Connector	2504.2210.4259	May 2025
Device Discovery and Deployment Utility (DDU)	1.61.0	May 2025
Chrome extension	4.8.0	July 2024

Secure Print mobile app (Android)	2.11.0.282	March 2025
Secure Print mobile app (iOS)	2.11.0.6	March 2025

Notes:

- Secure Print mobile apps and the Chrome extension are published after the Cloud Services are updated.
- The HP Secure Print Service (Local Connector) shows two different version numbers in different locations for the same download. The MSI version (25.2.24935.0)appears in the Control Panel during installation or upgrade, while the tagged version (2504.2210.4259) is displayed on the **Secure Printers** screen and in the Secure Print Service Deployment and Runtime Logs.

HP Insights and Secure Print 4.1 Release Notes – March 2025

This release represents the latest version of HP Insights. This update includes several important new features including:

- Support for SAML as a User Authentication Provider
- New APIs
  - Users
  - Device Toner Data
  - Device Status Data
- External Card Integration (Preview Mode)
- Device Profiles Updates
  - Cloud Release setting added to Device Profiles
  - Added the ability to hide **Print Options** and **Print and Retain** Settings
- User Management: Add the View Guests only option
- Print Scout Updates
- Secure Print Service Updates

Support for SAML as a User Authentication Provider

HP Insights now supports SAML for end-user authentication, providing seamless and secure login experiences across all HP Insights applications.

SAML support, previously available for system users logging into the web console, is now expanded to end-user authentication. SAML has been added as a **User Authentication Provider** for Secure Print and Direct Print, facilitating user registration for HP Insights applications, such as Print Scout, User Portal, Chrome Print, and the mobile app.

With SAML support for SSO, end users can access HP Insights applications using their identity provider (IdP) credentials. During their first login, users are redirected to the IdP's login page to authenticate. Once successfully authenticated, they are seamlessly redirected back to HP Insights and logged into their account.

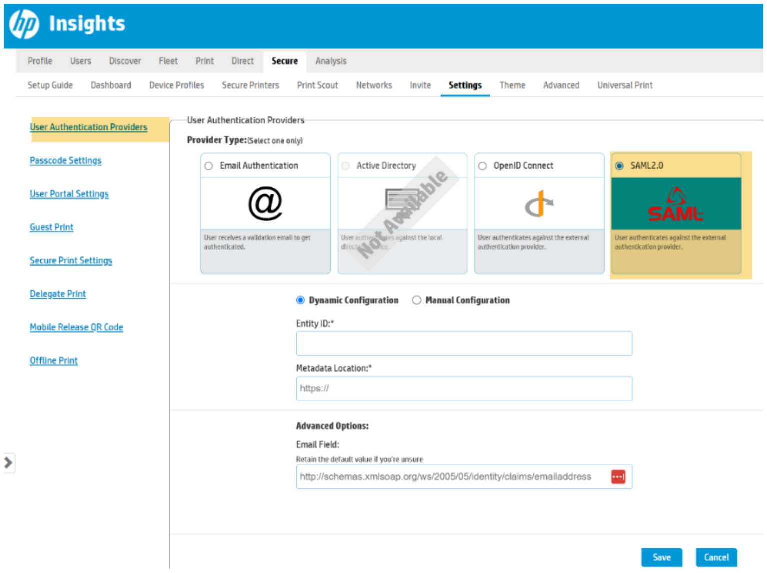
Key Benefits:

- **Improves user experience** - Users can log in using their existing company credentials. Users do not have to remember another set of credentials.
- **Helps lower IT costs** - Eliminates the responsibility of storing and managing user credentials.

Web Console Update

To support SAML, a new SAML2.0 option has been added to the following tabs in the HP Insights web console. These tabs are used to enable and configure SAML.

- Secure > Settings > User Authentication Providers
- Direct > Settings > User Authentication Providers



User Authentication Providers

Provider Type: (Select one only)

○ Email Authentication — User receives a validation email to get authenticated.

○ Active Directory — User authenticates against the local directory service.

○ OpenID Connect — User authenticates against the external authentication provider.

● SAML2.0 — User authenticates against the external authentication provider.

● **Dynamic Configuration** ○ **Manual Configuration**

Entity ID:*

Metadata Location:* https://

Advanced Options:

Email Field:

Retain the default value if you're unsure

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Refer to the HP Insights Help for more information on how to configure SAML Authentication Provider.

New APIs

Administrators can use the **Analysis** > **API** screen in the web console to connect to specific API endpoints. These endpoints enable the extraction of data from the HP Insights providing access to valuable information such as meter data and print transaction data. Once extracted, administrators can use a variety of tools, such as Power BI to manipulate and analyze the data.

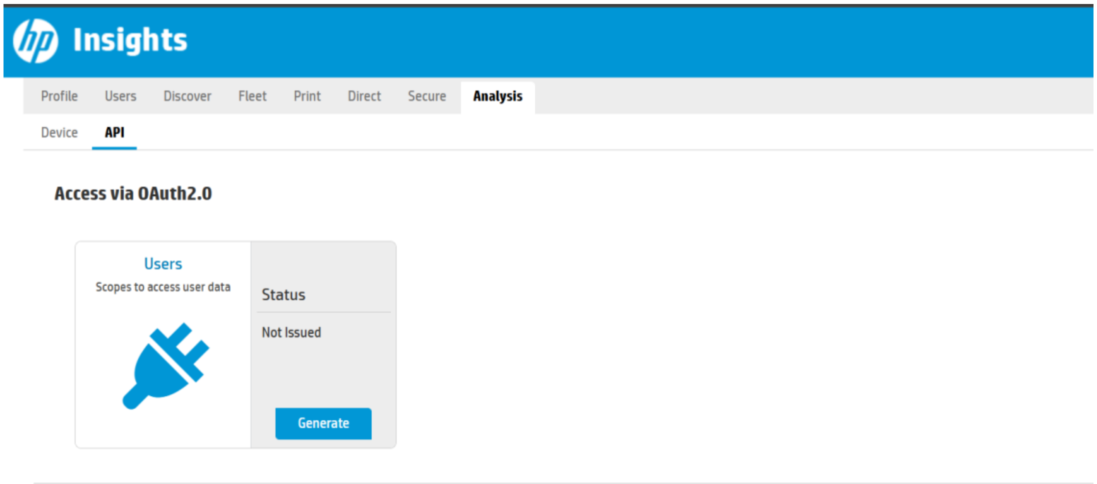
In this update, three new APIs have been introduced to expand data access and support various organizational requirements. The new APIs with this release are:

- Users
- Device Toner Data
- Device Status Data

Note: Device Toner and Device Status APIs require a Device Meter Data license.

Users API

The **Users API** allows administrators to create, manage, and access user accounts, including guest accounts, programmatically. It provides endpoints to handle tasks such as creating new users (including guest users), updating user details, and deleting users.



Access via OAuth2.0

Users

Scopes to access user data

Status

Not Issued

Refer to the API documentation to explore endpoints, view request and response details, and test API functionality.

- HP- US: API Documentation
- HP-EU: API Documentation

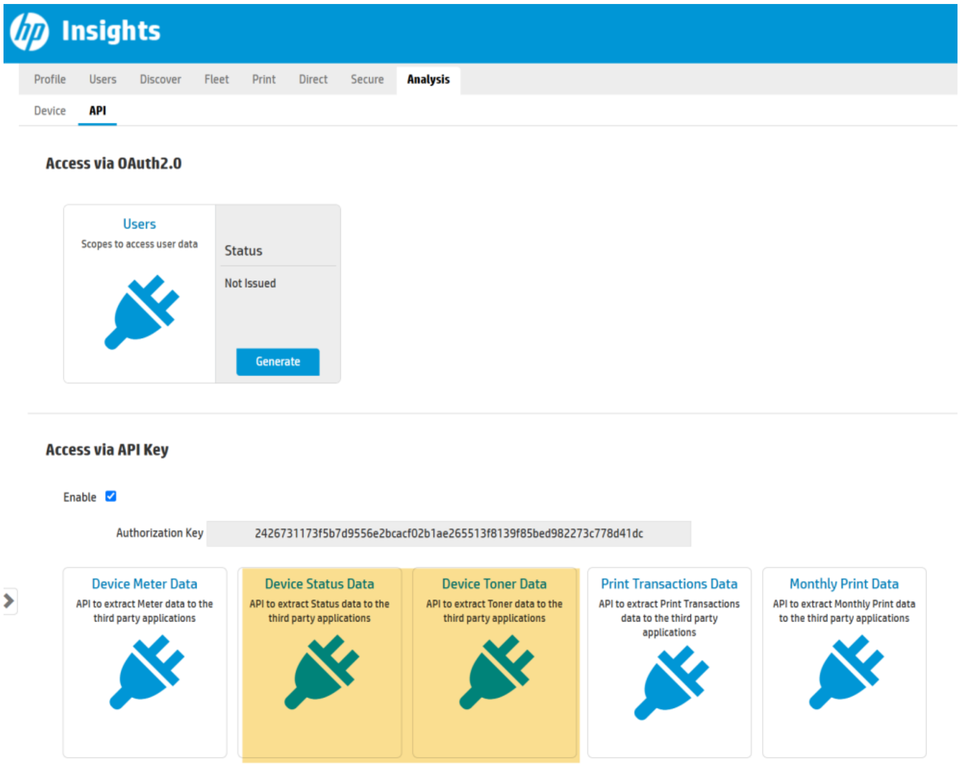
Refer to the HP Insights Documentation for more information on how to generate the Client ID and Client Secret required to connect to the API.

Device Toner Data

The **Device Toner Data** API allows administrators to extract data from the **Fleet** > **Toner** tab. The data contains information about toner levels and usage. It allows administrators to connect to endpoints and monitor toner consumption, track current toner levels, and identify when replacements are needed.

Device Status Data

The **Device Status Data API** enables administrators to extract device metrics from the **Fleet** > **Status** tab. The data contains specific information about the status of your print devices and other metrics that reflect device health and performance.



Access via OAuth2.0

Users
Scopes to access user data

Status

Not Issued

Access via API Key

Enable ☑

Authorization Key 2426731173f5b7d9556e2bcacf02b1ae265513f8139f85bed982273c778d41dc

Device Meter Data
API to extract Meter data to the third party applications

Device Status Data
API to extract Status data to the third party applications

Device Toner Data
API to extract Toner data to the third party applications

Print Transactions Data
API to extract Print Transactions data to the third party applications

Monthly Print Data
API to extract Monthly Print data to the third party applications

For more details about the APIs, refer to Connecting to the API to Extract Data in the HP Insights documentation.

External Card integration (Preview Mode)

Note: The External Card integration feature is in "Preview Mode" only. You can request access to this feature by emailing HP.

HP Insights now integrates with third-party card systems, allowing organizations to connect external web services to query card information. Printers can retrieve card details directly from external sources, offering a more flexible, secure, and scalable solution that meets modern workplace security requirements.

With this integration, card management is handled by your organization, reducing reliance on HP Insights. HP Insights performs real-time queries to third-party APIs whenever card information is needed. In addition, administrators can test card IDs directly within the HP Insights web console to help verify that the integration works and ensures smooth operations for end users.

Important Notes:

- This feature works for OpenID or SAML authentication providers only. It does not support Email Authentication or Active Directory authentication.

- When you enable and configure External Card Integration, any previously stored card data within HP Insights will no longer be used.
- Only one card system can be active at a time. You can either use the card system within HP Insights or use the external card integration feature. You cannot use both at the same time.

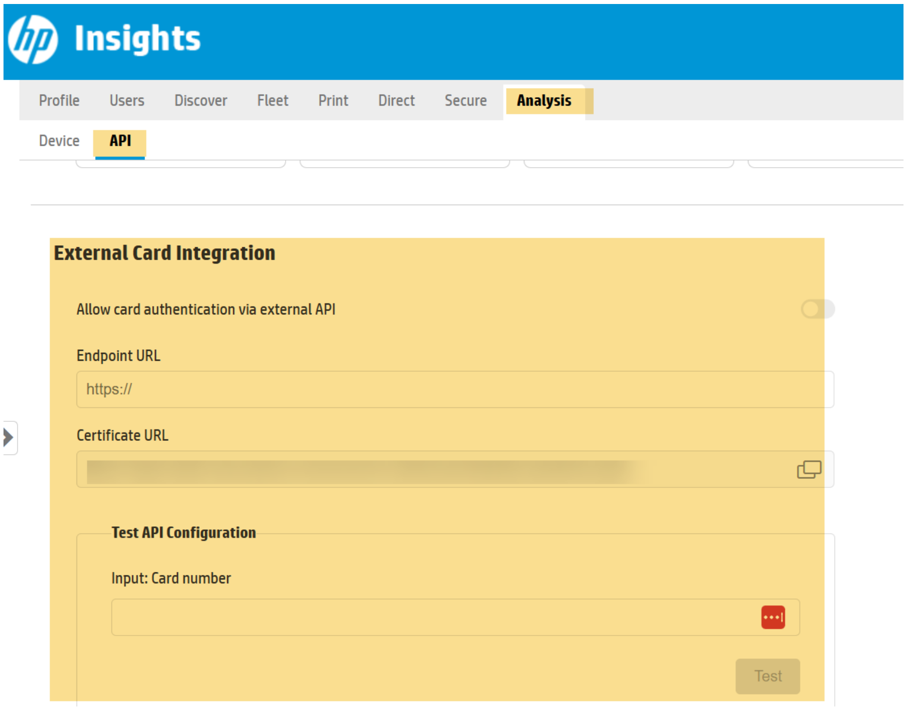
Web Console Update

To support this feature, a new External Card Integration section has been added to the Analysis > API tab in the web console. Administrators can use this section to configure and manage the connection between HP Insights and third-party identity providers.

Administrators configure the integration by entering details like the endpoint URL and authentication credentials. HP Insights then queries the third-party identity provider to retrieve or validate card details when a card is used at a secure printer.

The External Card Integration settings screen include

- Allow card authentication via external API - Toggle this switch to enable the feature. This can only be enabled when an Endpoint URL is provided.
- Endpoint URL – Add the API endpoint URL for the third-party card system.
- Certificate URL – Enter the URL of the digital certificate hosted on a server to establish secure communication between HP Insights and the third-party card system, ensuring the data exchanged is signed or encrypted for security.
- Test API Configuration - Test card IDs to ensure the integration is working correctly.



External Card Integration

Allow card authentication via external API

Endpoint URL

https://

Certificate URL

[redacted]

Test API Configuration

Input: Card number

How it Works

Configure Card Integration in the web console

1. The administrator configures the **External Card Integration** in the web console.
2. The administrator tests a card ID to verify that the card integration works.

User Workflow

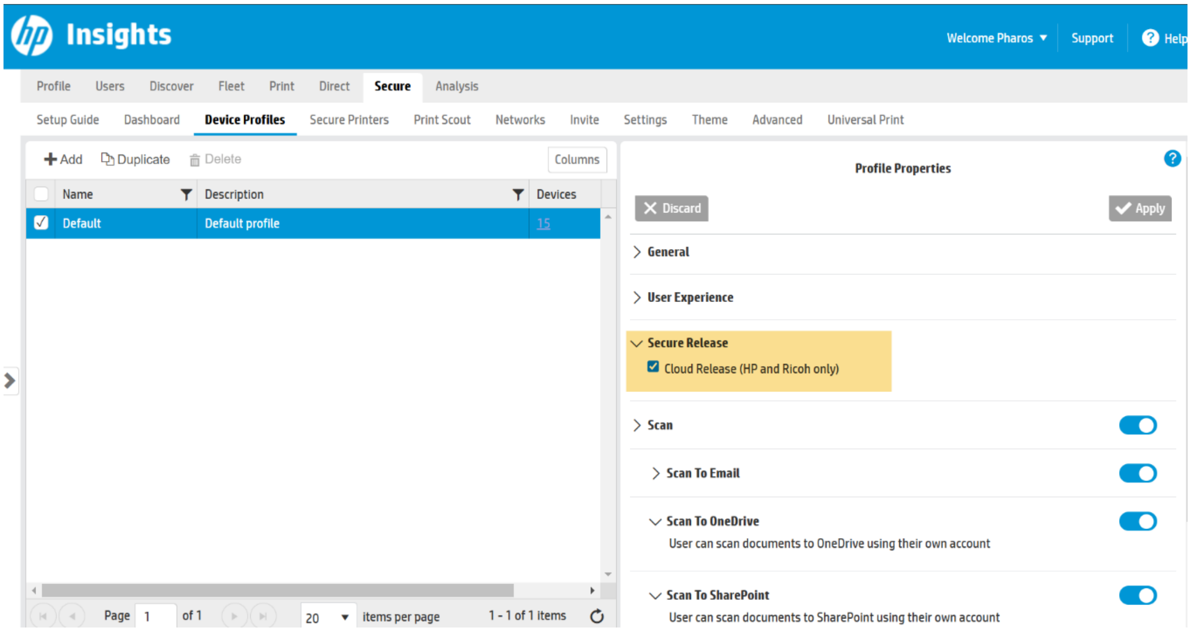
1. A user swipes their card at a secure printer or enters their card details, the contents of which are encrypted.
2. The encrypted data is sent to HP Insights for verification to generate a temporary access token.
3. HP Insights sends an authentication request to the third-party user identification provider.
4. The third-party provider decrypts, verifies, and identifies the user.

Device Profiles Updates

Added Cloud Release toggle in Device Profiles

This update introduces a new **Cloud Release** option within **Secure > Device Profiles**. The new setting allows administrators to override the global **Cloud Release** option available on the **Secure** Print Settings page. This update gives organizations more control over device configurations, making Secure Print setup simpler and more flexible.

The **Cloud Release** setting will remain in the **Secure Settings** tab, with a new toggle added to **Device Profiles**.



☐	Name	Description	Devices
☑	Default	Default profile	15

- General
- User Experience
- Secure Release
  - ☑ Cloud Release (HP and Ricoh only)
- Scan ●
  - Scan To Email ●
  - Scan To OneDrive ●
    User can scan documents to OneDrive using their own account
  - Scan To SharePoint ●
    User can scan documents to SharePoint using their own account

Notes:

- The Cloud Release checkbox in **Device Profiles** appears only if the global **Cloud Release** setting is enabled. If the global setting is OFF, **Cloud Release** will not be available in **Device Profiles**.
- **Cloud Release** setting applies to HP and Ricoh devices only.

Disabling the Cloud Release enables documents to be released via the Print Scout (instead of going through the cloud).

Added the ability to hide Print Options and Print and Retain

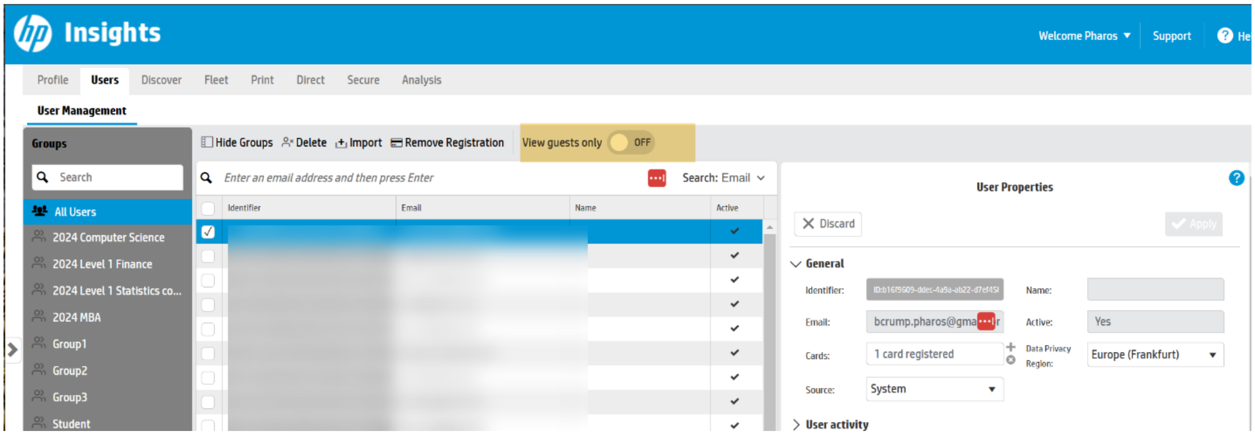
In the previous version, the **Print Options** and **Print and Retain** settings in the **Device Profiles** tab of the web console could only be set to "Shown". With this update, they can now be set to “Hidden” if needed. This allows administrators to allow or restrict users to use these options.

- **Print Options** – When set to “Hidden”, users are prevented from changing print options after the job has been submitted. When set to “Shown”, users can change document options at the secure printer before the job is released.
- **Print and Retain** – When set to "Hidden," users cannot retain print jobs in the queue after release. When set to "Shown," users can reprint documents as needed.

Note: These settings are set to “Shown” by default.

User Management: View Guests only

A new **View guests only** toggle has been added to the **Users** > **User Management** tab of the web console. This allows administrators to filter and view only guest users within the user grid. This feature makes it easier to quickly identify guest users within HP Insights.



View guests only OFF

[redacted]

User Properties

General

Identifier: ID:b16f9609-ddec-4a9a-ab22-d7ef45

Email: bcrump.pharos@gma r

Cards: 1 card registered

Source: System

Name:

Active: Yes

Data Privacy Region: Europe (Frankfurt)

Secure Print Service Updates

This section outlines the improvements and bug fixes for the latest version of the Secure Print Service.

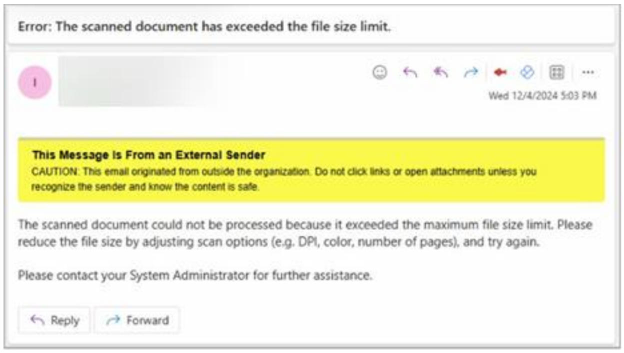
Improvements

- Enhanced Control over Secure Print Settings

  Updated the Secure Print Service to support the ability to disable **Print Options** and **Print and Retain** in the **Secure** > **Device Profiles** tab of the web console. Previously, these options were always visible on secure printers. In this update, these options can now be hidden if required.

- Email notification when scan file size is exceeded

  The file size limit for scanned documents in the Secure Scan app is 80 MB. When a user's file exceeds this limit, an email notification is now sent to users. This minimizes confusion by making users aware that they have exceeded the limit.



Error: The scanned document has exceeded the file size limit.

[redacted]

Wed 12/4/2024 5:03 PM

This Message Is From an External Sender
CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

The scanned document could not be processed because it exceeded the maximum file size limit. Please reduce the file size by adjusting scan options (e.g. DPI, color, number of pages), and try again.

Please contact your System Administrator for further assistance.

Bugfixes

- HP devices - Secure Scan quality attribute mapping on HP devices now functions correctly, ensuring full utilization of the scan functionality.
- Canon devices - Job upload and accounting for Copy/Scan now function correctly when a user logs out immediately after job completion. Previously, logging out too quickly caused failures when uploading to all destinations (OneDrive, SharePoint, Email, Network Folder).

Print Scout Updates

The Print Scout has been updated with the following changes:

- Added support for the latest HP Universal Print Driver 7.3.0 (released in November 2024).
- Implemented security patches to address known vulnerabilities and mitigate potential exploits.

Component Release Versions

This release includes the following software components and release versions.

*Note: Secure Print mobile apps and the Chrome extension are published after the Cloud Services are updated.

Software Component	Release Version	Build Date
Device Scout	1.23.9.103 (Not updated)	July 2024
Print Scout (Windows)	7.37.7.103	February 2025
Print Scout (Mac)	2.28.4.101	February 2025
Print Scout (Linux)	(Not Updated) 2.1.0	September 2022
Secure Print Site Service – Local Connector	2502.1707.3521 (tagged version) 25.2.24935.0 (MSI version)	February 2025
Secure Print Site Service – Cloud Connector	2502.1707.3521	February 2025
Device Discovery and Deployment Utility (DDU)	1.59.0	February 2025
Chrome extension	4.8.0	July 2024
Secure Print mobile app (Android)	2.10.4	October 2024
Secure Print mobile app (iOS)	2.10.4	October 2024

Notes:

- Secure Print mobile apps and the Chrome extension are published after the Cloud Services are updated.
- The Secure Print Service (Local Connector) shows two different version numbers in different locations for the same download. The MSI version (25.2.24935.0) appears in the Control Panel

during installation or upgrade, while the tagged version (2502.1707.3521) is displayed on the Secure Printers screen and in the Secure Print Service Deployment and Runtime Logs.

HP Insights and HP Secure Print

HP Insights and Secure Print 4.0 Release Notes – November 2024

This release represents the latest version of the HP Secure Print Site Service including significant new features, improvements, and bugfixes

- Secure Print Direct Enhancements
  - Off-network Direct IP Printing through the cloud
  - Support for Type 4 Drivers (Preview Mode)
- Secure Print: Device Profiles
- Secure Scan New Features and Improvements
  - Customizable Scan Options
  - Support for Microsoft 365 in Scan to Email
  - Scan to One Drive Scan to SharePoint Improvements
- Secure Print: Added the setting for Cloud Connector to the web console
- Secure Print: Encryption Improvements
  - Added option to disable job name encryption for jobs submitted by Print Scout
- Print Scout Improvements
  - Off-network Direct IP Printing through the cloud
  - Support for Type 4 Drivers (Preview Mode)
  - Microsoft Universal Print: Added Paper Tray Selection
  - Changed the default driver to Manufacturer Driver (from IPP driver)

Secure Print Direct Enhancements

This release includes improvements to Secure Print Direct that drive efficiency and improve user experience.

- Off-network Direct IP Printing via the cloud
- Support for Type 4 Drivers

Off-network Direct IP Printing through the cloud

Secure Print Direct was only suitable for environments where printers and users are on the same network segment or have line-of-sight connectivity. However, this approach is not suitable for geographically separated sites or environments where users and printers are on different network segments, where direct communication with printers isn't possible.

HP Insights' new off-network direct IP printing capability now allows users to send print jobs to printers across disparate networks via the cloud.

Off-network direct IP printing enables seamless printing across the organization, regardless of physical or network boundaries, ensuring that users can reliably print to any HP Insights-managed direct printer, even without a direct network path.

Prerequisites

- Off-network direct IP printing leverages the same cloud-based delivery pathway used by Secure Print and requires both the Secure Print Direct license and Secure Print License. Organizations with only a Direct Print license will not have access to the off-network IP printing capability.
- Latest Print Scout v 7.37.x.x installed on user workstations and/or App Servers installed on the printers' network.
- **Cloud-based delivery** is enabled on the HP Insights Web Console.

Key Benefits

Off-network direct IP printing provides the following benefits:

- **Seamless Printing Across Networks** - Users can print to any company printer, regardless of geographic location or network boundaries. This is especially useful for remote workers or employees who move between locations or enterprises where printers are hosted in a separate or isolated network segment for security reasons.
- **Enhanced Security** - Print jobs are securely handled using temporary cloud storage, where they are automatically deleted after printing to minimize data exposure. To ensure maximum confidentiality, Zero Knowledge Encryption (ZKE) is applied, safeguarding the content of print jobs while they are briefly stored in the cloud.

Supported Clients

Secure Print Direct Cloud supports the following clients.

- Windows Print Scout
- macOS Print Scout

Note: Off-network direct IP printing is not supported on Chrome Print.

Limitation

Off-network direct IP printing is limited to the Print Scout Release (or Push Print) delivery method. Cloud Release (or Pull Print) is not supported.

How Off-network Direct IP Printing through the Cloud Works

1. The user sends a print job from a workstation with Print Scout installed.
2. The Print Scout checks for a direct connection ("line of sight") to the target printer. If this connection is available, the print job is sent directly to the printer.
3. If a direct connection to the printer is not available, HP Insights switches to cloud delivery.
    a. The user's workstation Print Scout uploads the print job to the cloud for temporary storage, where it is encrypted with Zero Knowledge Encryption (ZKE) for enhanced security.
    b. HP Insights sends job release instructions to one of the Print Scouts within the same network as the target printer.
    c. When a Print Scout (workstation or Print Server) receives the release instructions, it will verify the connection to the target printer and either accept or reject the release request.
    d. Once the Print Scout accepts the release instructions, it will download the job data from the cloud and send the job to the target printer.
    e. The releasing Print Scout will update the cloud with the progress status of the print job release.
    f. The user is notified whether the print job was completed or failed to release.
    g. The print job is immediately deleted from the job store once it is released. Failed or canceled jobs are removed according to the specified purge rules.

For existing Secure Print customers, the following settings play a key role in how print jobs are delivered to printers. Understanding how these settings impact the routing of print jobs is essential when using Secure Print Direct Cloud with Secure Print.

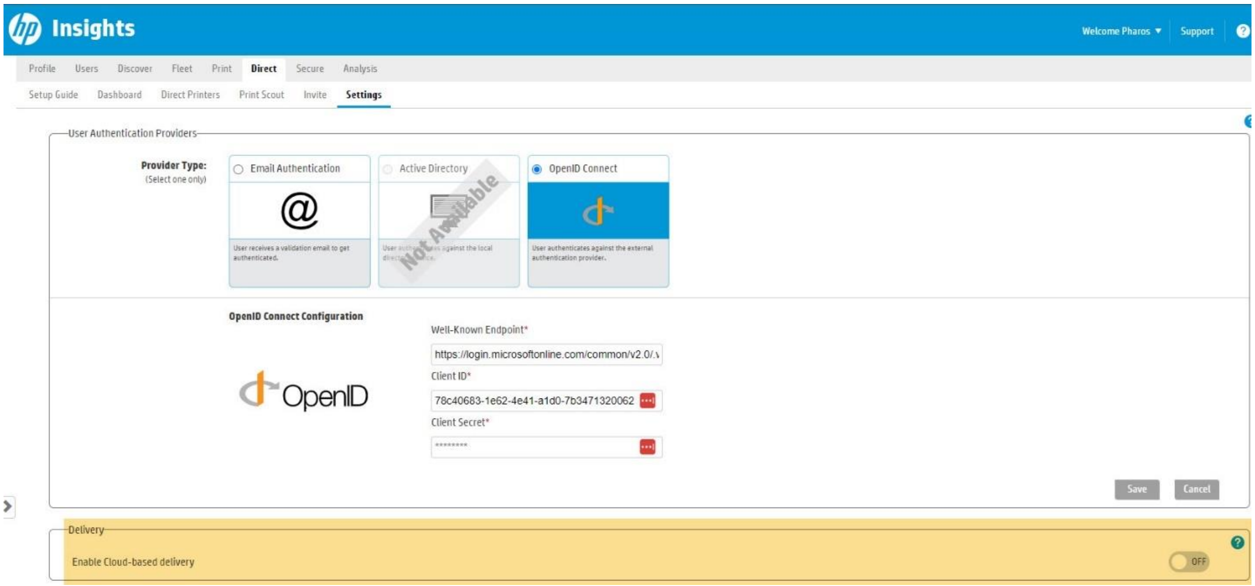
- If the **Restrict Print Scout Release** is enabled, direct print jobs via the cloud will be handled by the App Server Print Scout or the user's originating Print Scout. Jobs will never be handled by other users' Print Scout.

- If the **Force delivery through Print Servers** is enabled, direct print jobs via the cloud can only be handled by App Server Print Scout.

HP Insights Web Console Update

A new **Delivery** section has been added to the **Direct** > **Settings** tab of the HP Insights Web Console.

To enable Cloud-based delivery, toggle the option **Enable Cloud-based delivery** setting in the **Delivery** section. When Cloud-based delivery is enabled, print jobs will be routed through the cloud if there is no direct connection to the target printer and will be immediately sent to the designated printer.



User Authentication Providers

Provider Type: (Select one only)

○ Email Authentication — User receives a validation email to get authenticated.

○ Active Directory — User authenticates against the local directory service.

● OpenID Connect — User authenticates against the external authentication provider.

OpenID Connect Configuration

Well-Known Endpoint*: https://login.microsoftonline.com/common/v2.0/.\

Client ID*: 78c40683-1e62-4e41-a1d0-7b3471320062

Client Secret*: ********

Delivery

Enable Cloud-based delivery: OFF

Support for Type 4 Print Drivers (Preview Mode)

Secure Print Direct has been updated to support Type 4 print drivers. Type 4 drivers are a newer class of printer drivers introduced in Windows Server 2012 and are designed to enhance security, simplify installation, and improve overall performance.

Previously, the Driver Capture Tool (installed by the Print Scout) only worked with Type 3 print drivers, so the list of available manufacturer drivers for Secure Print Direct queues was limited to Type 3 print drivers.

With this update, the Driver Capture Tool's functionality has been updated to include the ability to configure and upload Type 4 print drivers, providing the same level of support as currently available for Type 3 drivers. Support for type 4 print drivers ensures compatibility with the latest printer features and technologies.

For details on the updates in the Driver Capture Tool to support Type 4 Print, refer to the **Print Scout Improvements and Bugfixes** section of this document.

Web Console Update

When creating Secure Print Direct queues in the **Direct > Secure Print** tab, all Type 4 print drivers that were uploaded using the Driver Capture Tool will be displayed as available options in the HP Insights Web Console.

Secure Print: Device Profiles

In the previous version, Secure Print settings were applied uniformly to all devices. This update introduces the **Device Profiles** feature, giving administrators greater control over device-level configurations.

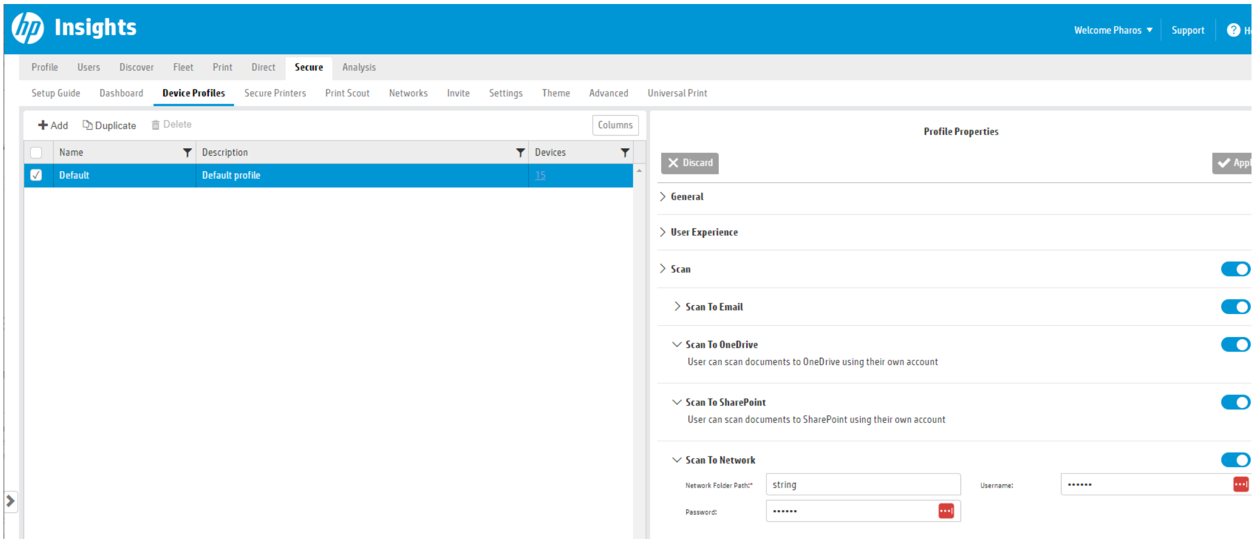
With Device Profiles, Secure Print settings can now be customized for each printer, allowing for tailored configurations rather than applying the same settings across all printers. For instance, administrators can now set different default paper sizes for scanning, such as Letter for devices in the US and A4 for devices in Europe.

Web Console Update

The following updates have been made to the web console with the introduction of the Device Profiles feature.

New Device Profiles sub-tab

A new **Device Profiles** sub-tab has been introduced under the **Secure** tab.



□	Name	Description	Devices
☑	Default	Default profile	15

> General

> User Experience

> Scan ●

> Scan To Email ●

∨ Scan To OneDrive ●
User can scan documents to OneDrive using their own account

∨ Scan To SharePoint ●
User can scan documents to SharePoint using their own account

∨ Scan To Network ●
Network Folder Path:* string
Username: ••••••
Password: ••••••

The **Device Profiles** tab includes the following action buttons:

- **Add:** Create a new profile.
- **Duplicate:** Copy an existing profile to create a duplicate.
- **Delete:** Remove an existing profile.

Default Profile

By default, a single **Default Profile** is created, which includes default Secure Print and Secure Scan options. Administrators cannot rename or delete this system-generated profile but can modify its settings.

All printers listed in the Secure Printers tab are assigned the Default Profile by default. Administrators can reassign printers to different profiles through the Secure Printers tab if specific configurations are needed. Any new devices that get added will get the Default Profile assigned to them automatically. Administrators can also edit the Default Profile.

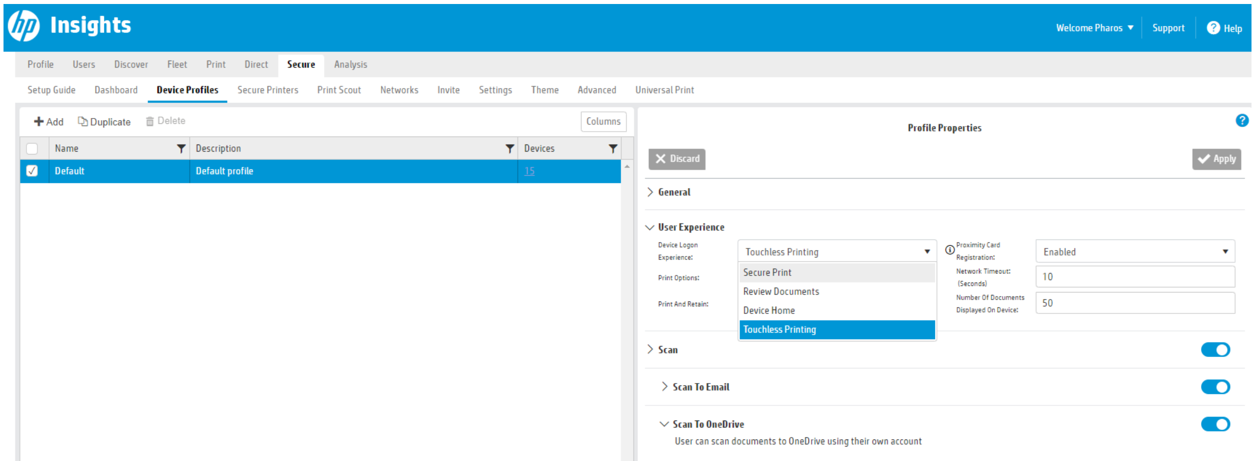
Secure Print Settings moved to Device Profiles

The following settings have been moved from the **Settings > Secure Print Settings** tab to the new **Device Profile Settings > User Experience** for improved management.

- Device logon experience
- Enable Proximity card registration
- Network Timeout (Seconds)
- Number of documents displayed on device
- The **Secure Scan Settings** have been migrated to the **Device Profiles** section

Device Logon Experience Update

- The **Device Logon Experience** setting includes a new **Review Documents** option in addition to **Secure Print**, **Device Home**, and **Touchless Printing**. When enabled, users will be directed to the Review Documents (showing the list of documents submitted) screen immediately after logging in.
- The **Device Logon Experience** setting defines the printer's user interface behavior during the login process on a device. This setting allows administrators to configure and customize how users authenticate themselves when logging into a device, including:
    - Secure Print
    - Review Documents
    - Device Home
    - Touchless Printing



☐	Name	Description	Devices
☑	Default	Default profile	15

Device Logon Experience: Touchless Printing ▾ (Secure Print, Review Documents, Device Home, Touchless Printing)

Print Options:

Print And Retain:

Proximity Card Registration: Enabled ▾

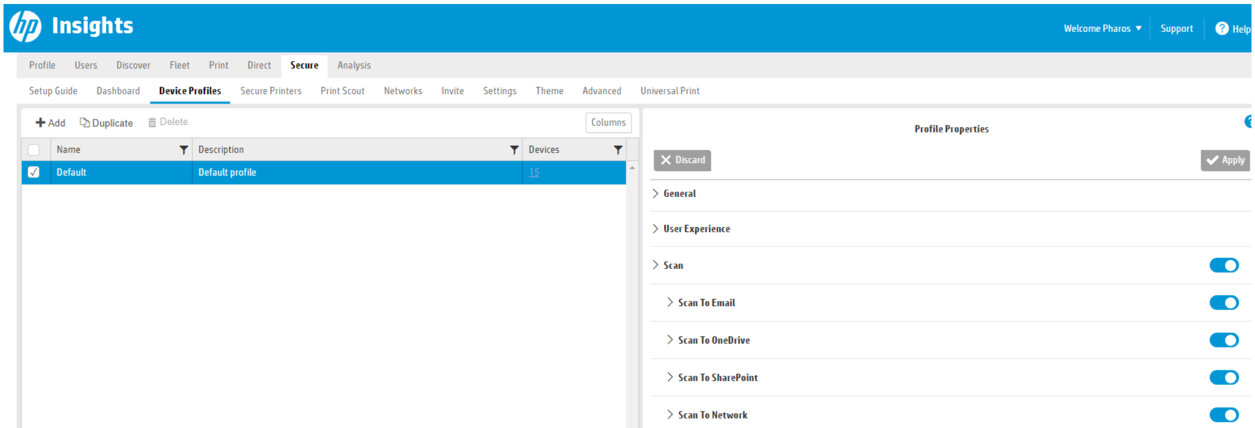
Network Timeout: (Seconds) 10

Number Of Documents Displayed On Device: 50

User can scan documents to OneDrive using their own account

Moved Secure Scan Settings to Device Profiles

The **Secure Scan Settings** tab previously located in the **Secure** tab has been moved to the **new Device Profiles** tab.



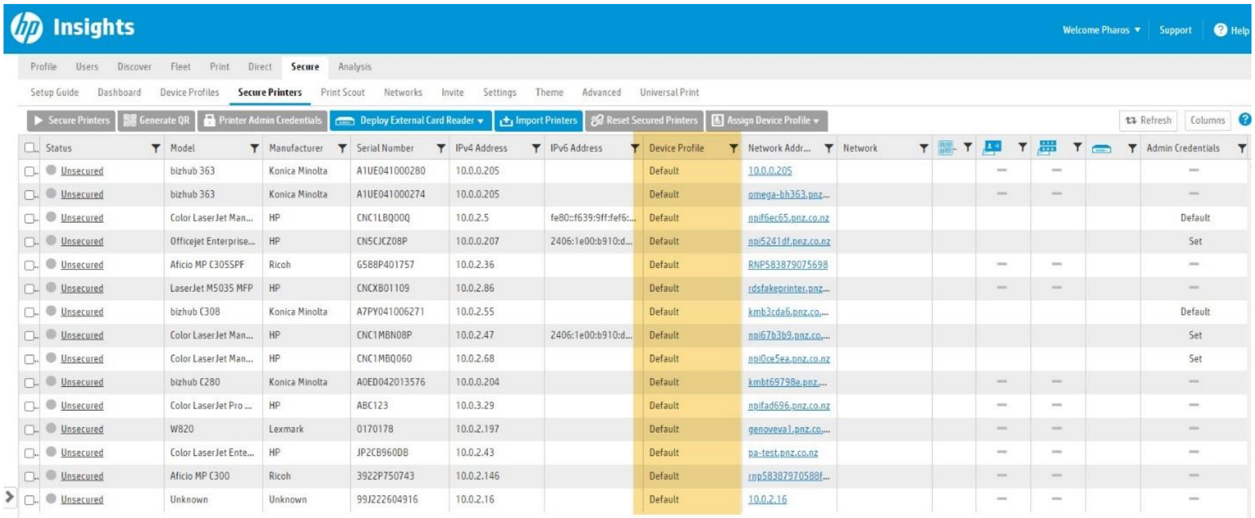
☐	Name	Description	Devices
☑	Default	Default profile	15

- General
- User Experience
- Scan ●
  - Scan To Email ●
  - Scan To OneDrive ●
  - Scan To SharePoint ●
  - Scan To Network ●

Note: If Secure Scan was previously enabled in the Secure Scan Settings screen, the scan settings will be migrated to the default device profile. This ensures that secure printers will continue to function with the Secure Scan feature enabled. However, if Secure Scan was not enabled, the scanning feature in the default device profile will be set to "off," meaning scanning will remain disabled by default until manually activated.

Updated Secure Printers tab

- The **Secure Printers** tab now includes a new **Assign Device Profile** option, allowing administrators to assign Device Profiles to devices. Once a Device Profile is assigned to one or more devices, the administrator can edit or delete the profile, with a warning message displayed.
- A new **Device Profile** column has been added to the **Secure Printers** tab that shows which Device Profile is assigned to each device. This allows administrators to easily see and manage the profiles associated with each device.



☐	Status	Model	Manufacturer	Serial Number	IPv4 Address	IPv6 Address	Device Profile	Network Addr...	Network					Admin Credentials
☐	Unsecured	bizhub 363	Konica Minolta	A1UE041000280	10.0.0.205		Default	10.0.0.205			—	—		—
☐	Unsecured	bizhub 363	Konica Minolta	A1UE041000274	10.0.0.205		Default	omega-bh363.pnz...			—	—		—
☐	Unsecured	Color LaserJet Man...	HP	CNC1LBQ00Q	10.0.2.5	fe80::f639:9ff:fef6:...	Default	npif6ec65.pnz.co.nz						Default
☐	Unsecured	Officejet Enterprise...	HP	CN5CJCZ08P	10.0.0.207	2406:1e00:b910:d...	Default	npi5241df.pnz.co.nz						Set
☐	Unsecured	Aficio MP C305SPF	Ricoh	G588P401757	10.0.2.36		Default	RNP583879075698			—	—		—
☐	Unsecured	LaserJet M5035 MFP	HP	CNCXB01109	10.0.2.86		Default	rdsfakeprinter.pnz...			—	—		—
☐	Unsecured	bizhub C308	Konica Minolta	A7PY041006271	10.0.2.55		Default	kmb3cda6.pnz.co....						Default
☐	Unsecured	Color LaserJet Man...	HP	CNC1MBN08P	10.0.2.47	2406:1e00:b910:d...	Default	npi67b3b9.pnz.co....						Set
☐	Unsecured	Color LaserJet Man...	HP	CNC1MBQ060	10.0.2.68		Default	npi0ce5ea.pnz.co.nz						Set
☐	Unsecured	bizhub C280	Konica Minolta	A0ED042013576	10.0.0.204		Default	kmbt69798e.pnz....			—	—		—
☐	Unsecured	Color LaserJet Pro ...	HP	ABC123	10.0.3.29		Default	npifad696.pnz.co.nz			—	—		—
☐	Unsecured	W820	Lexmark	0170178	10.0.2.197		Default	genoveva1.pnz.co....			—	—		—
☐	Unsecured	Color LaserJet Ente...	HP	JP2CB960DB	10.0.2.43		Default	pa-test.pnz.co.nz			—	—		—
☐	Unsecured	Aficio MP C300	Ricoh	3922P750743	10.0.2.146		Default	rnp58387970588f...			—	—		—
☐	Unsecured	Unknown	Unknown	99J222604916	10.0.2.16		Default	10.0.2.16			—	—		—

Notes:

- For existing sites, the settings from the **Secure > Settings** tab will automatically be migrated to the **Default Profile** in the **Device Profiles** tab. This ensures that any previously configured settings are retained and applied to the default profile.
- Administrators do not need to re-secure the device after the update; simply refreshing the screen on the device will apply the updated settings.

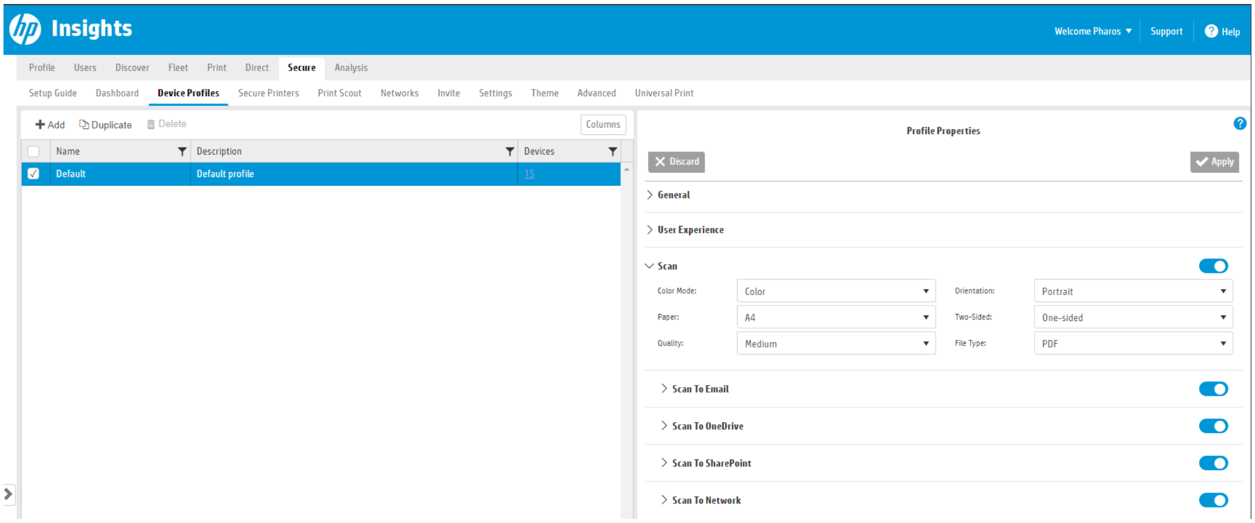
Secure Scan New Features and Improvements

Customizable Scan Options

With this update, administrators now have the flexibility to set up default scan options to match your organization's specific preferences.

The new **Device Profiles** tab includes a **Default Profile** with its own default scan options. By default, all printers are assigned to this Default Profile, and the scan options set within it will be applied universally to all the printers. To use different scan options for specific printers, administrators will need to create and apply a separate Device Profile for those printers.

Note: In the previous version of HP Insights, Secure Scan included a predefined set of default scan options for HP and Toshiba printers. With the introduction of Device Profiles, these predefined scan settings are now overridden. You will need to set up new scan options within Device Profiles, as any previous configurations will no longer apply.



☐	Name	Description	Devices
☑	Default	Default profile	15

Scan

Color Mode:	Color	Orientation:	Portrait
Paper:	A4	Two-Sided:	One-sided
Quality:	Medium	File Type:	PDF

Scan To Email

Scan To OneDrive

Scan To SharePoint

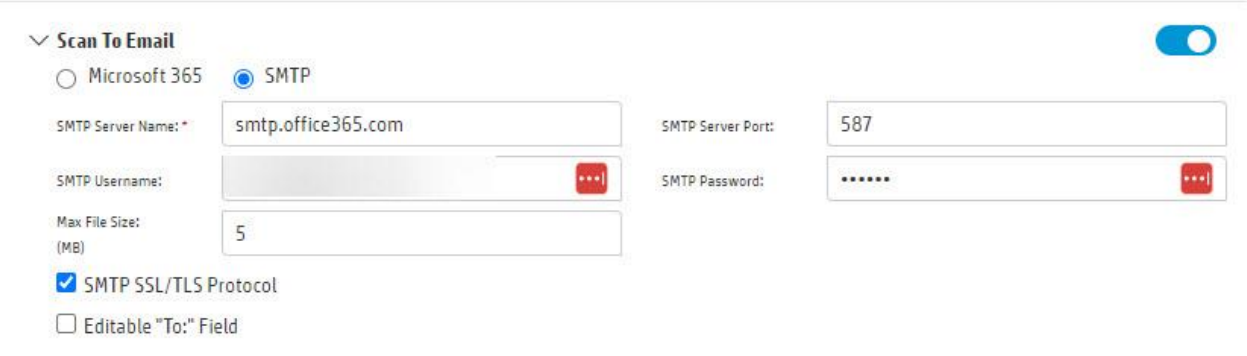
Scan To Network

Support for Microsoft 365 in Scan to Email

HP Insights integrated scanning capability has been enhanced with the ability to send emails using Microsoft 365, in addition to the previously supported SMTP. When configuring the "Scan to Email" feature, Administrators can now choose between Microsoft 365 or SMTP for sending scanned documents.

The new **Secure** > **Device Profiles** tab in the web console offers a Scan to Email feature with the following options.

- **Microsoft 365** - This option integrates with Microsoft's cloud-based email service, allowing users to use their existing Microsoft 365 account to send scanned documents. It's a convenient choice for organizations using Microsoft 365, as it leverages the same email infrastructure.
- **SMTP (Simple Mail Transfer Protocol)** - This is a standard method for sending emails and can be used with any email provider. Administrators can configure the SMTP settings with details like the server address, port, and authentication information. SMTP is a flexible option that works with a wide range of email services.



Scan To Email

○ Microsoft 365 ● SMTP

SMTP Server Name:* smtp.office365.com

SMTP Server Port: 587

SMTP Username: [redacted]

SMTP Password: ••••••

Max File Size: (MB) 5

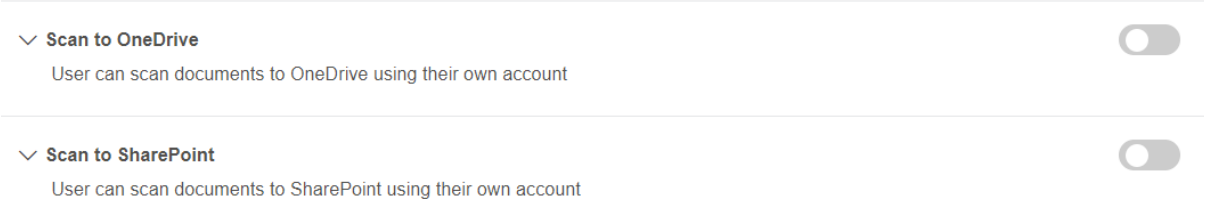
☑ SMTP SSL/TLS Protocol

☐ Editable "To:" Field

When the Microsoft 365 option is selected, all Email SMTP settings are hidden, leaving only the "Enable Editable To: Field" and "Max File Size" settings visible.

Scan to OneDrive and Scan to SharePoint Improvements

Scan to SharePoint and **Scan to OneDrive** are now separate options in the new Device Profiles screen. Previously, enabling the Scan to Office 365: Enable User Authentication setting activated both, but now administrators can enable or disable them individually.



Scan to OneDrive

User can scan documents to OneDrive using their own account

Scan to SharePoint

User can scan documents to SharePoint using their own account

Secure Scan Usability Improvements

- **Editable File Name for Scans**
  Users can now edit the file name of a scan file directly within the printer panel.
- **Enhanced Navigation for OneDrive and SharePoint**

When scanning to OneDrive or SharePoint, users will now see breadcrumb trails of the folders they've navigated through. These breadcrumbs are interactive, allowing users to click on any folder in the path to quickly jump back to a specific location. This improvement provides easier and more intuitive navigation.

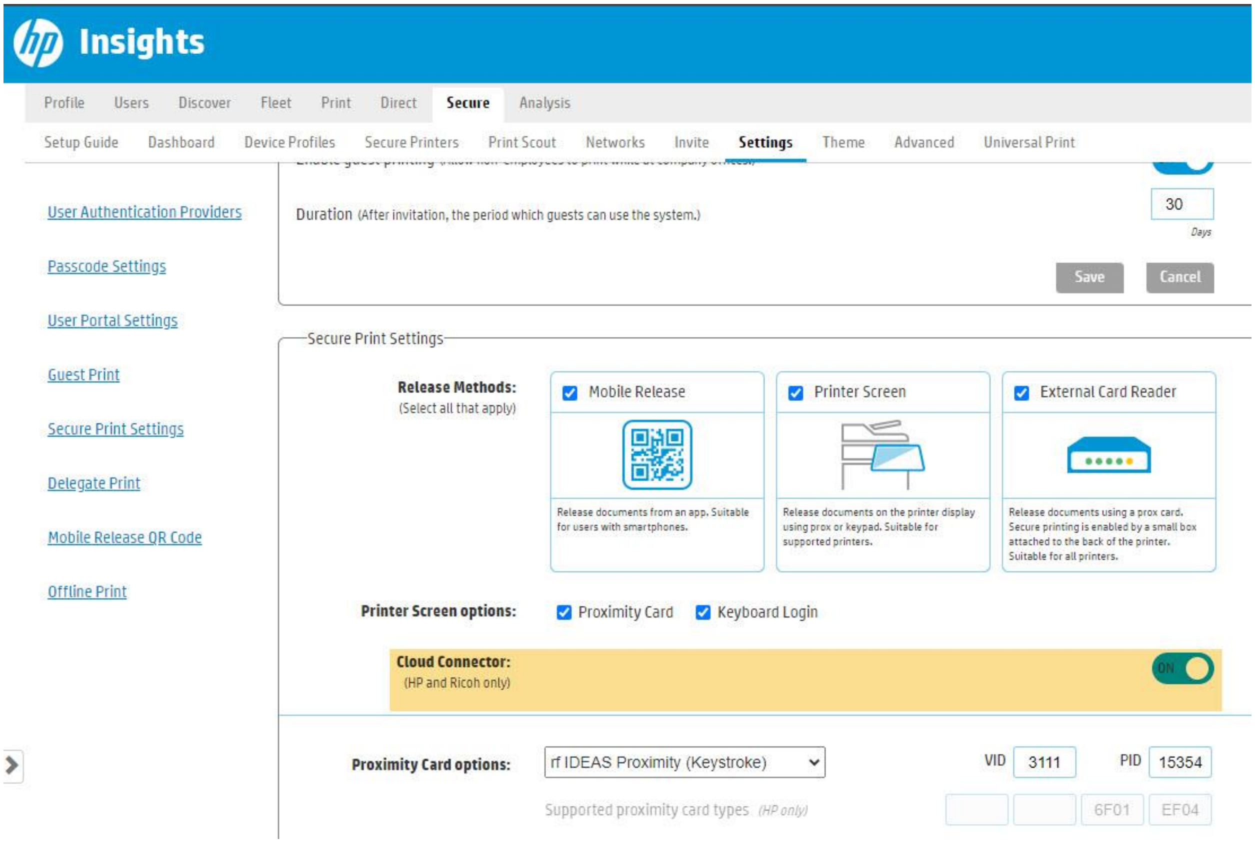
- Improved Back and Cancel Button Functionality
  The Back and Cancel buttons have been updated to function reliably, ensuring a smoother user experience.

Secure Print: Added the Cloud Connector Setting to the Web Console

The **Secure Print Settings** section of the HP Insights Web Console now includes a **Cloud Connector** toggle, allowing administrators to easily enable or disable it. This change lets organizations manage their Cloud Connector setting independently, reducing reliance on HP Support. Previously, this option was hidden and required HP to activate it, but now it is directly accessible in the console.

HP Insights Web Console Update

The new **Cloud Connector** toggle switch in the **Secure** > **Settings** > **Secure Print Settings** screen allows administrators to enable or disable Cloud Connector.



Duration (After invitation, the period which guests can use the system.) 30 Days

Secure Print Settings

Release Methods: (Select all that apply)

☑ Mobile Release
Release documents from an app. Suitable for users with smartphones.

☑ Printer Screen
Release documents on the printer display using prox or keypad. Suitable for supported printers.

☑ External Card Reader
Release documents using a prox card. Secure printing is enabled by a small box attached to the back of the printer. Suitable for all printers.

Printer Screen options: ☑ Proximity Card ☑ Keyboard Login

Cloud Connector: (HP and Ricoh only) ON

Proximity Card options: rf IDEAS Proximity (Keystroke) VID 3111 PID 15354

Supported proximity card types *(HP only)* 6F01 EF04

- When **Cloud Connector** is turned **ON**, devices can be secured against the Cloud Connector. Administrators will need to use the **Device Deployment Utility (DDU)** to secure printers against the **Cloud Connector** and make those printers "cloud-connected".

  Note: Only HP and Ricoh printers are currently supported by the **Cloud Connector**. For other printer manufacturers that don't support the Cloud Connector, the **Local Connector** will need to be used.

- When **Cloud Connector** is turned **OFF**, devices won't be able to be secured against the Cloud Connector. Devices can be secured with the Local Connector to secure devices.

For information on how to configure Cloud Connected Devices, refer to the Configuring Cloud Connected Devices document.

Cloud Connector behavior for new and existing sites

- For sites with the Cloud Connector enabled, the new **Cloud Connector** toggle switch in the Secure Print Settings will be **ON** by default.
- If a site either doesn't have the Cloud Connector enabled or is a new site, the **Cloud Connector** toggle switch in the Secure Print Settings will be set to **OFF** by default. Administrators will need to manually enable it if they want to use the Cloud Connector.

Secure Print: Encryption Improvements

Added option to disable job name encryption for Print Scout job submissions

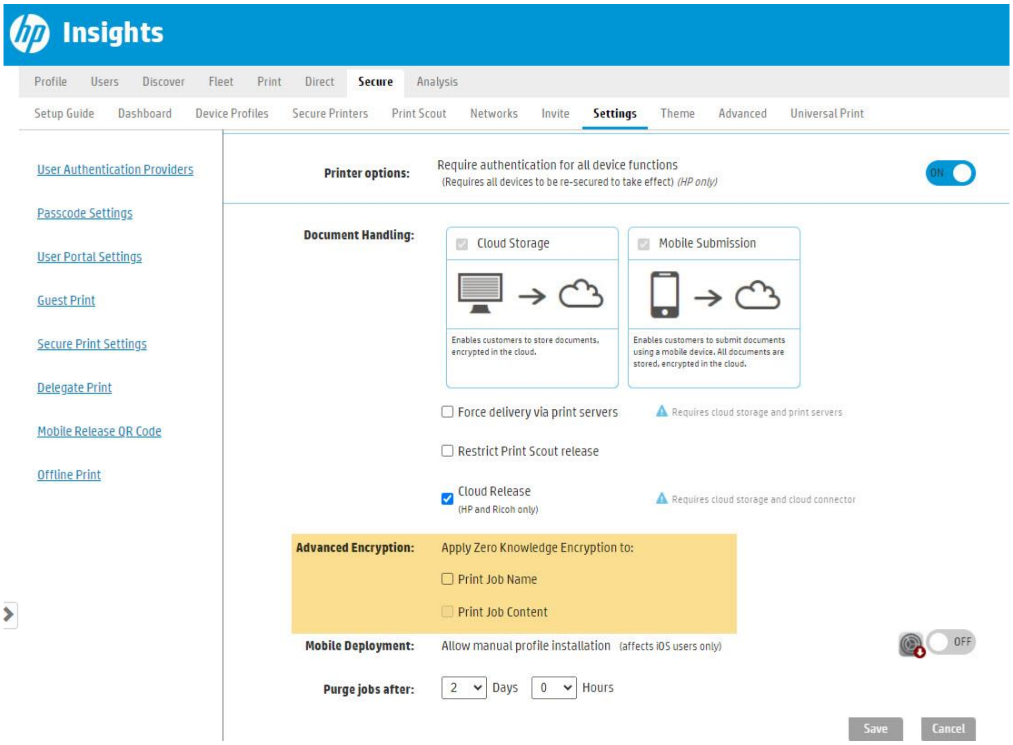
Encryption settings are now visible and manageable through the HP Insights web console. Previously, these settings were controlled by HP Insights and not accessible to administrators. Additionally, job name encryption has been de-coupled from the Cloud Connector feature. Job name encryption now functions independently without depending on whether the Cloud Connector is enabled or not.

Administrators can now view and modify encryption settings through the web console, giving them the option to enable or disable zero-knowledge encryption for the job name. For instance, for existing customers where Cloud Connector is disabled, print jobs sent through Print Scout show encrypted job names in HP Insights, making it harder for users to identify their print jobs in the User Portal, Mobile App, or cloud-connected devices. With this update, administrators have the flexibility to turn off job name encryption if desired, making it easier to identify print jobs.

HP Insights Web Console Update

A new **Advanced Encryption** section in **Secure > Settings > Secure Print Settings > Document Handling** on the HP Insights Web Console has been added. This includes settings that allow administrators to decide if they want to apply Zero Knowledge Encryption (ZKE) for print job names.

Additionally, it includes a setting that show how the content of the print jobs is encrypted. This encryption is based on a combination of settings, which are outlined in the "Print Job Content" section of the document.



Printer options: Require authentication for all device functions (Requires all devices to be re-secured to take effect) *(HP only)* ON

Document Handling:

☑ Cloud Storage – Enables customers to store documents, encrypted in the cloud.

☑ Mobile Submission – Enables customers to submit documents using a mobile device. All documents are stored, encrypted in the cloud.

☐ Force delivery via print servers – Requires cloud storage and print servers

☐ Restrict Print Scout release

☑ Cloud Release (HP and Ricoh only) – Requires cloud storage and cloud connector

Advanced Encryption: Apply Zero Knowledge Encryption to:

☐ Print Job Name

☐ Print Job Content

Mobile Deployment: Allow manual profile installation (affects iOS users only) OFF

Purge jobs after: 2 Days 0 Hours

Apply Zero Knowledge Encryption (ZKE) to:

- Print Job Name – This setting allows you to choose whether to encrypt print job names (document names) or leave them visible on the User Portal or Mobile App in plain text.
    - When enabled, job names will be encrypted meaning they will be shown in an encrypted format on the User Portal and Mobile App for jobs submitted by a Print Scout.
    - When disabled, the job names will not be encrypted meaning they will appear in clear, readable text on the User Portal and Mobile App for jobs submitted by a Print Scout.

  Note: This setting applies to print jobs submitted via Print Scouts only.

- Print Job Content – This read-only setting controls whether the content of a print job (the actual document) will receive advanced encryption.
    - When Print Job Content encryption is enabled, the document content is encrypted using the ZKE within the Print Scout before being uploaded to cloud storage. The document will also be encrypted with an AWS managed S3 KMS key while at rest within cloud storage.
    - When Print Job Content encryption is disabled, the document content will not be encrypted using the ZKE within the Print Scout before being uploaded to cloud storage. The document will, however, be encrypted with an AWS managed S3 KMS key while at rest within cloud storage.

Note: The **Print Job Content** setting is read-only and cannot be modified. The status of this setting — whether it is enabled or disabled, depends on the following conditions related to the **Cloud Connector** and **Cloud Release**.

- When the **Cloud Connector** is **OFF** (for on-premises setup via Local Connector) or when the **Cloud Connector** is **ON,** but **Cloud Release** is **OFF**, print job content encryption is automatically enabled and cannot be disabled in both cases.
- When **Cloud Release** is ON (indicating that Cloud Connector is also ON), the print job content encryption is automatically disabled. This means that job data sent to the cloud by Print Scouts will not use ZKE (Zero-Knowledge Encryption). However, these jobs will still be encrypted at rest with S3 KMS (Key Management Service).

Note: Cloud Release requires the Cloud Connector to be ON, so you cannot enable Cloud Release without first enabling Cloud Connector.

Print Scout New Features and Improvements

Off-network Direct IP Printing through the Cloud

This release introduces Off-network Direct IP Printing which enables seamless printing across an organization, allowing users to print to any HP Insights managed direct printer, regardless of physical location or network connection, without needing a direct network path to the printer.

The Print Scout component of the HP Insights has been updated to support Off-network Direct IP Printing through the Cloud.

Support for Type 4 Drivers (Preview Mode)

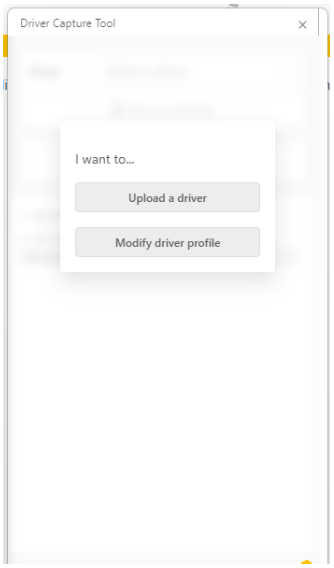
The Print Scout has been updated to support installation of Type 4 Print Drivers.

Driver Capture Tool Update

The Print Scout installs the Driver Capture Tool, which is used to upload drivers as well as set up related finishing options to the cloud so they can be used for print queue deployment.

The user interface of the Driver Capture Tool has been enhanced for improved usability. Key updates to the Driver Capture Tool include

- Administrators are now presented with the option to either **Upload a Driver** or **Modify a Driver Profile** when launching the Driver Capture Tool. Additionally, the tool no longer pre-selects a driver; instead, it allows an Admin to manually choose a driver from the list.



- The Driver Capture Tool now displays a cloud icon next to drivers that have already been uploaded to HP Insights.
- A new **Group View** button has been added to help administrators easily differentiate between drivers stored in the cloud and those that can be uploaded to the cloud. While drivers are initially listed alphabetically, admins can now use the Group View button to organize them into two categories:
  - **Drivers can be uploaded to the cloud** - Drivers installed on the workstation and ready to be uploaded to the cloud.
  - **Drivers available in the cloud** - Drivers already uploaded to the cloud, including pre-defined drivers and those already uploaded to the cloud

Supported Type 4-Drivers

Not all Type 4 drivers follow the Windows recommended standard, and as such they may not currently work with our Type 4 driver support. If a driver does not behave as expected when trying to upload or install queues with that driver, HP Insights can work with you try to expand the implementation to cover the particular driver.

HP has tested with the Canon, Lexmark and Ricoh Universal Type 4 drivers, and with a variety of HP and Xerox device-specific drivers.

- Canon Generic PCL6 V4
- HP OfficeJet Pro 9020 series PCL-3
- HP PageWide Color MFP 780-785 PCL6 (V4)
- HP Smart Universal Print
- Lexmark Generic v4 XPS
- Lexmark Universal v4 XL
- (Ricoh) PCL6 V4 Driver for Universal Print
- Xerox VersaLink C500 V4 PCL6

Type 4 Driver Limitations and Known Issues

- Print Scout Compatibility

  Print Scout version 7.37 or later is needed to successfully upload or install Type 4 drivers. Older versions of Print Scout won't install any print queues that are configured with a Type 4 driver and won't show an error message to indicate the failure.

- Retention of presets, shortcuts, and favorites are not supported for Canon, Ricoh, Lexmark, and Konica Minolta Type 4 Drivers. These need to be manually recreated. However, with HP and Xerox print drivers, these presets, shortcuts, and favorites can be copied or transferred along with user preferences.

- Supported Manufacturer Print Drivers

  HP Insights has tested print drivers, primarily universal or generic ones, from the manufacturers listed below, and we anticipate that most other drivers from the same manufacturers should work if they follow the same Type 4 standards and specifications. However, HP Insights cannot guarantee that all other drivers will work seamlessly and suggest performing your own testing to ensure compatibility and proper functionality for Type 4 drivers. If a driver doesn't function as expected, HP Support can work with you to adjust the implementation to support the driver.

  - Canon
  - Lexmark
  - Ricoh
  - HP
  - Xerox
- Xerox and Canon User Preferences UI

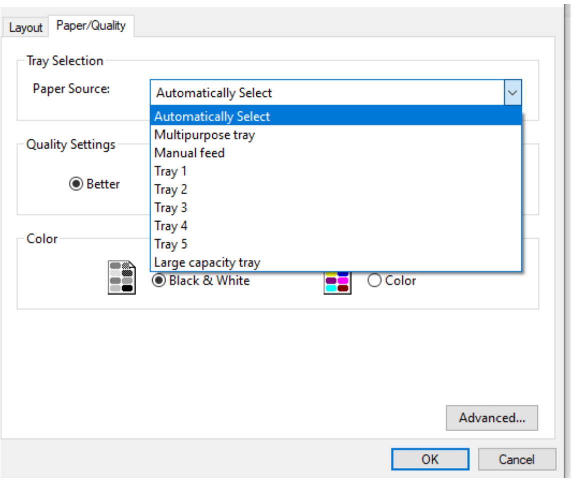
  When a Canon or Xerox Type 4 driver is initially installed, it only includes the basic user interface. To install the custom user interface (such as the User Preferences UI), administrators must complete additional steps. For example, Xerox drivers require admin users to run a separate MSI installer to add the User Preferences UI after the driver is installed.

  If a driver is uploaded or captured before completing these extra steps, only the basic UI will be captured, and you won't have access to the custom options (e.g. User Preferences UI). To avoid this, ensure the custom UI is installed before capturing or uploading the driver. If you have already uploaded the driver before installing the custom UI, you'll need HP Insights Support to help fix this issue.

Microsoft Universal Print Integration: Add Paper Tray Selection

The Universal Print secure queue has been enhanced to include additional finishing options.

Paper Source: A new drop-down called **Paper Source** has been added to the **Paper Quality** > **Tray Selection** option. This allows users to select a specific paper tray from which their document will be printed.


Tray Selection

Paper Source: Automatically Select

Quality Settings

● Better

Color

● Black & White ○ Color

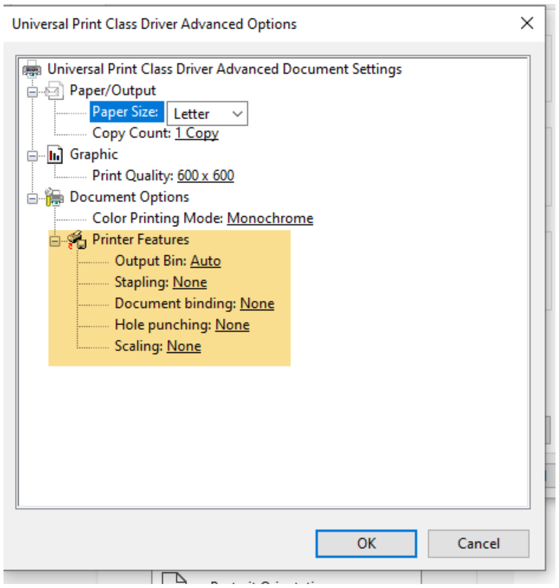
The following new options have been added under **Printer Features**, accessible via the **Advanced** button:

Output Bin: Users can now choose their preferred output tray for printing.

Stapling: Users can now choose their preferred stapling option:

- None (default)
- Top left
- Top right
- Bottom left
- Bottom right
- Left edge (2 staples)
- Top edge (2 staples)
- Right edge (2 staples)
- Bottom edge (2 staples)
- Saddle stitching
- Document Binding
- None (default)
- Bind (auto)
- Left edge (stitching)
- Top edge (stitching))
- Right edge (stitching)
- Bottom edge (stitching)
- Hole Punching
- None (default)
- Hole punch (auto)

Note: If users do not explicitly select paper source and output tray options, the system will default to either a standard configuration or the printer's default settings.



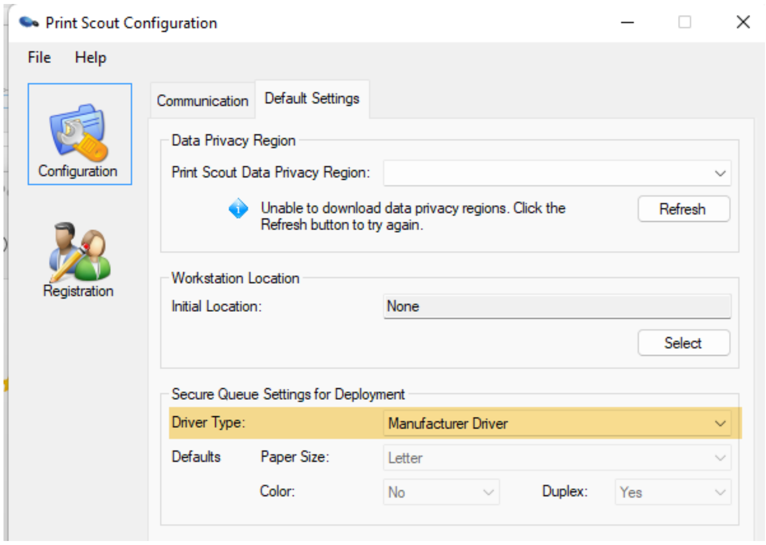
Universal Print Class Driver Advanced Options

Universal Print Class Driver Advanced Document Settings

- Paper/Output
  - Paper Size: Letter
  - Copy Count: 1 Copy
- Graphic
  - Print Quality: 600 x 600
- Document Options
  - Color Printing Mode: Monochrome
  - Printer Features
    - Output Bin: Auto
    - Stapling: None
    - Document binding: None
    - Hole punching: None
    - Scaling: None

Changed the default driver to manufacturer driver

In this update, the Print Scout installation defaults to the manufacturer driver instead of the IPP Class driver, as in the previous version. When an administrator creates a deployment package, the **Manufacturer Driver** is selected by default, but they can choose to switch to the IPP Class driver if preferred.



Print Scout Configuration

Data Privacy Region

Print Scout Data Privacy Region:

Unable to download data privacy regions. Click the Refresh button to try again.

Workstation Location

Initial Location: None

Secure Queue Settings for Deployment

Driver Type: Manufacturer Driver

Defaults Paper Size: Letter

Color: No Duplex: Yes

Component Release Versions

This release includes the following software components and release versions.

Software Component	Release Version	Build Date
Device Scout	1.23.9.103 (Not updated)	July 2023
Print Scout (Windows)	7.37.5.103	November 2024
Print Scout (Mac)	2.28.3.101	November 2024
Print Scout (Linux)	(Not Updated) 2.1.0	September 2022
Secure Print Site Service – Local Connector	2411.318.3346	November 2024
Secure Print Site Service – Cloud Connector	2411.318.3346	November 2024
Device Discovery and Deployment Utility (DDU)	1.57.0	November 2024
Chrome extension	4.8.0	July 2024
Secure Print mobile app (Android)*	2.10.4	October 2024
Secure Print mobile app (iOS)*	2.10.4	October 2024

*Note: Secure Print mobile apps and the Chrome extension are published after the Cloud Services are updated.

Secure Print Mobile App Release Notes – October 2024

This release represents the latest version of the HP Secure Print Mobile App.

SSO Support for the Secure Print Mobile App

The HP Secure Print mobile app now supports Single Sign-On (SSO). For sites using OpenID authentication, Print Scouts are no longer necessary for registering user's mobile devices with Secure Print. This allows users to log in to the mobile app using their existing SSO credentials, providing a more convenient and secure experience.

However, for sites using Email Authentication or Active Directory, Print Scouts are still required to be installed on user workstations. Users will need to scan a QR code to sign in and register their mobile devices for Secure Print.

Key benefits

- Increased security: SSO improves mobile app security by centralizing login and access. Moreover, combining SSO with Multi-Factor Authentication (MFA) strengthens security.
- Improved user experience: SSO simplifies the login process for users significantly reducing the time and effort required to log in to the Secure Print mobile app.

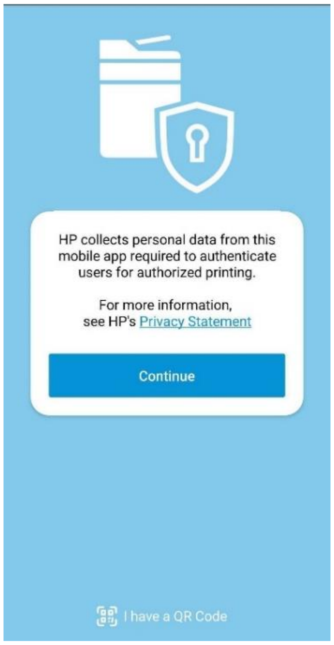
Important Notes:

- This feature is available only for sites using OpenID authentication. If your site uses Email Authentication or Active Directory, use the QR Code method to register your mobile device.
- User accounts must already exist in the HP Insights, whether through user registration, user import, or SCIM import.
- Logging out of the mobile app will require users to re-register their device with HP Secure Print.

SSO Workflow: Registering a Mobile Device for Secure Print

To use the Secure Print mobile app for releasing documents, users must first register their device. Here is the workflow for registering a mobile device for Secure Print using SSO, assuming the mobile app is already downloaded from the Google Play Store or Apple App Store

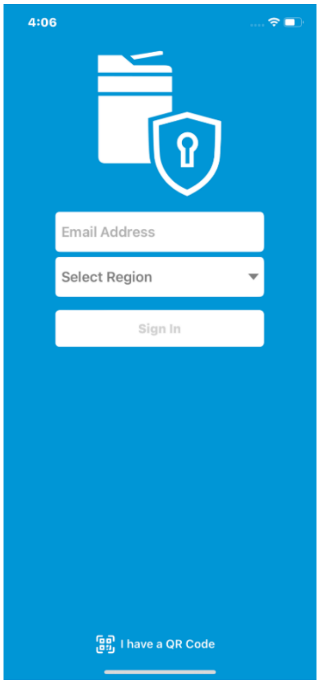
1. The user opens the Secure Print mobile app and is prompted to enter their email address.
2. In the mobile app, after reviewing the Privacy Statement, the user clicks Continue.



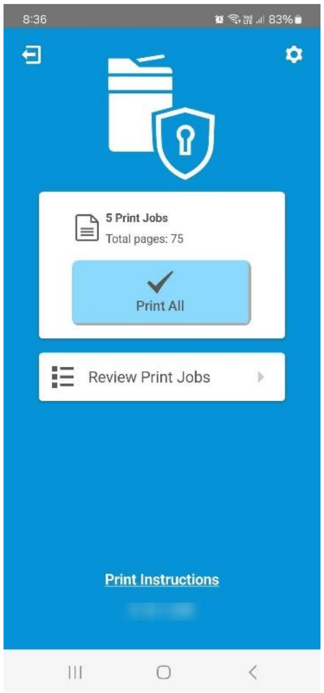
HP collects personal data from this mobile app required to authenticate users for authorized printing.

For more information, see HP's Privacy Statement

3. After entering their email address and clicking Sign In, the user is redirected to their organization's login page.

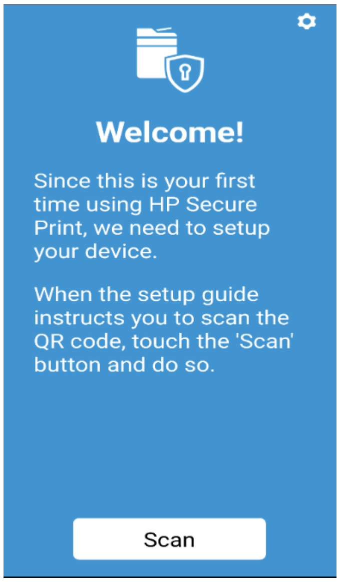


After a successful authentication, the user will be redirected to the mobile app and should now have access to the app's features and functions.



Changes to the Mobile Device Registration Process using a QR Code

If your organization uses Email Authentication or Active Directory Authentication, you can use the existing QR Code registration. The old method of registering a mobile device via QR Code has been updated to include the "I have a QR Code" option on the user interface, replacing the Scan option in the older version as shown in the images below.

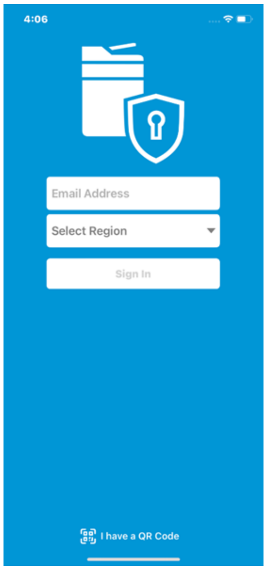


Welcome!

Since this is your first time using HP Secure Print, we need to setup your device.

When the setup guide instructs you to scan the QR code, touch the 'Scan' button and do so.

Old user interface with the Scan button

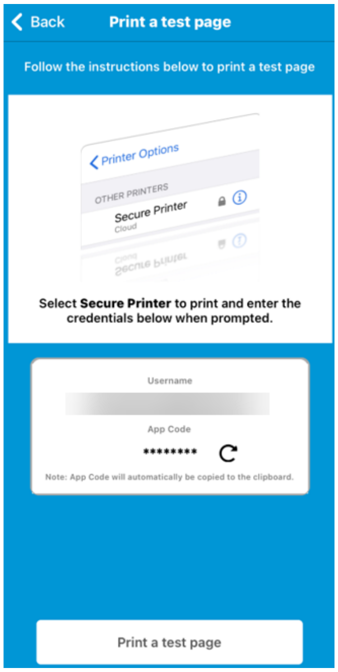


New user interface with the **I have a QR Code** button

Note: This workflow requires the installation of Print Scouts on users' workstations.

Updated Mobile Submission

The Mobile Submission feature of the Secure Print mobile app has been updated to enhance security. App codes are now encoded (not in cleartext). Users will receive an email with their app code when it is initially created or reset.



Follow the instructions below to print a test page

Select **Secure Printer** to print and enter the credentials below when prompted.

Username

[redacted]

App Code

****

Note: App Code will automatically be copied to the clipboard.

Component Release Versions

This release includes the following software components and release versions.

Software Component	Release Version
HP Secure Print Mobile app (Android)	2.10.4
HP Secure Print Mobile app (iOS)	2.10.4