www.pharos.com

PHAROS

Secure Release Technical Overview

PHAROS

Contents

Introduction

Pharos Secure Release enables a print workflow that enhances document security, reduces overall print costs, and lowers environmental impact by requiring users to authenticate at the device to release submitted print jobs.

With Pharos Secure Release, employees submit print jobs from a workstation or mobile device on any network (company, home, public, cellular, etc.) to a single cloud-based print queue and release the print jobs at any Pharos-secured print device on the company network by authenticating at the device. Users can authenticate using proximity card, mobile device, or keyboard login, and can delegate other users to release submitted print jobs on their behalf. A cloud-based secure print workflow reduces waste and data leakage through print by preventing documents from being left abandoned and forgotten at the printer after being printed, or being picked up before the user is able to retrieve them.

Pharos Secure Release is built on the Pharos Cloud platform, a cloud-native print management and optimization platform that replaces print servers and is proven to meet the scalability, security, and high-availability requirements of the largest corporate enterprises.

The purpose of this document is to provide a technical overview of how Pharos Secure Release works in its most common deployment method. Since organizations have different network topologies, leverage different identity providers, and have different needs, Pharos Secure Release provides multiple configuration options enabling it to fit practically any corporate environment and use case.

Pharos Secure Release is typically deployed on an organization's network with local services comprising of:

- Pharos Device Scout, a lightweight Windows app installed on a local server, and
- Pharos Print Scout, a client agent deployed on employee workstations

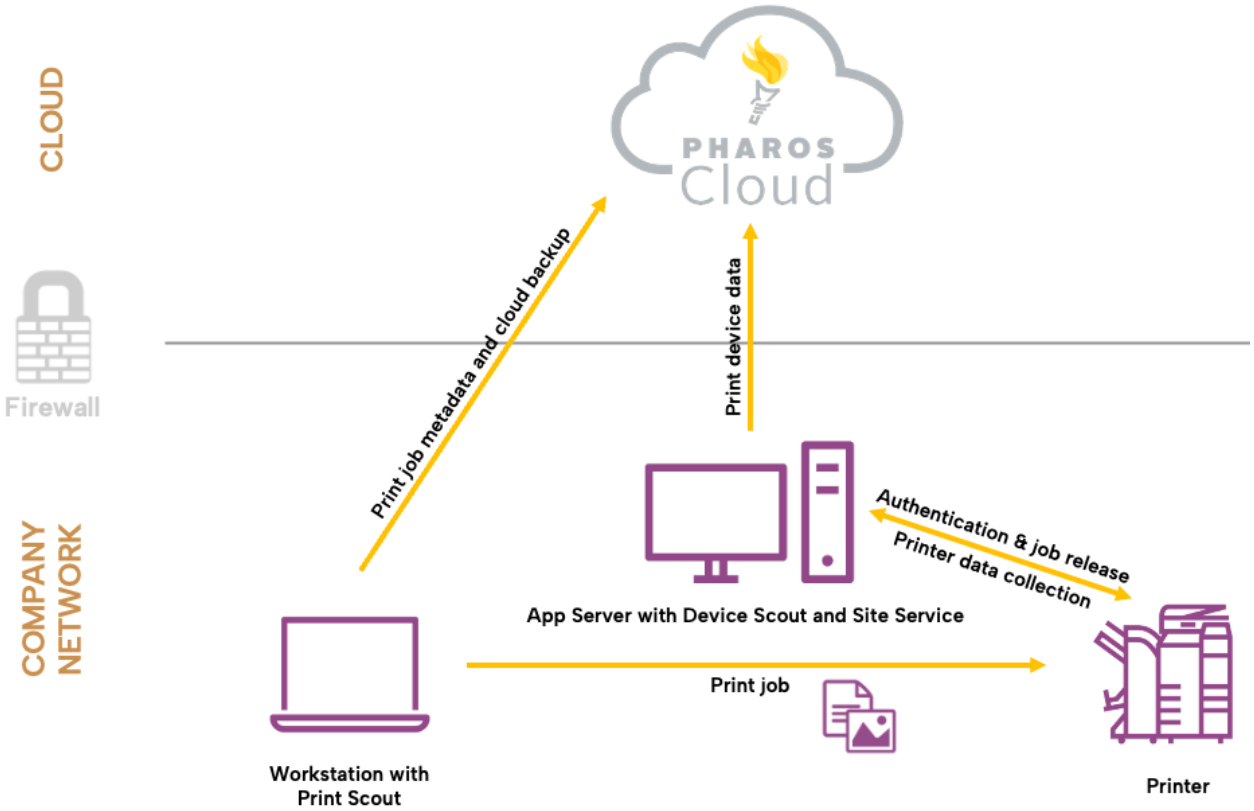
Depending on their configuration, companies may deploy additional Pharos technologies, such as:

- Pharos Mobile App, which enables users to submit print jobs from their iOS and Android devices and release them by scanning a QR code at a printer
- Pharos Card Connector system (SR-25), which enables proximity card release on non-supported multifunction printers (MFPs)

With Secure Release, employees print from their workstations as they normally do. The print job is encrypted and stored on the user's workstation by the Print Scout, and a copy is sent to Pharos Cloud if Cloud Storage is enabled. Employees release their submitted print jobs at any secured printer on the company network by authenticating. Secured printers connect to Pharos Cloud via Device Scout, which acts as a bridge to the cloud for printers unable to connect directly (among other functions, described in the next section).

This architecture enables Secure Release to work with practically any printer or MFP in an organization. Support for the user authentication option embedded on the printer's control panel will depend on the device in use. Non-supported print devices can be secured via Pharos Card Connector hardware for organizations wanting to authenticate via proximity card. All printers support Secure Release using the Pharos Secure Release mobile app available on iOS and Android devices.

System Components



Print Scout

Print Scout is a lightweight client application that monitors printing activity. Print Scout is deployed to employee workstations (Windows or MacOS) to enable secure printing workflows and capture printing data.

For Pharos Secure Release, Print Scout:

- Provides a simple setup wizard for each user to register with Secure Release and begin to print securely
- Submits print jobs, stores encrypted print jobs on the workstation, and uploads a copy to the cloud if Cloud Storage is enabled by the administrator
- Enforces corporate print policies and educates users on mindful printing practices at the point of print submission (requires Policy Print)
- Decrypts and sends print jobs to Pharos-secured print devices

Device Scout – Site Service

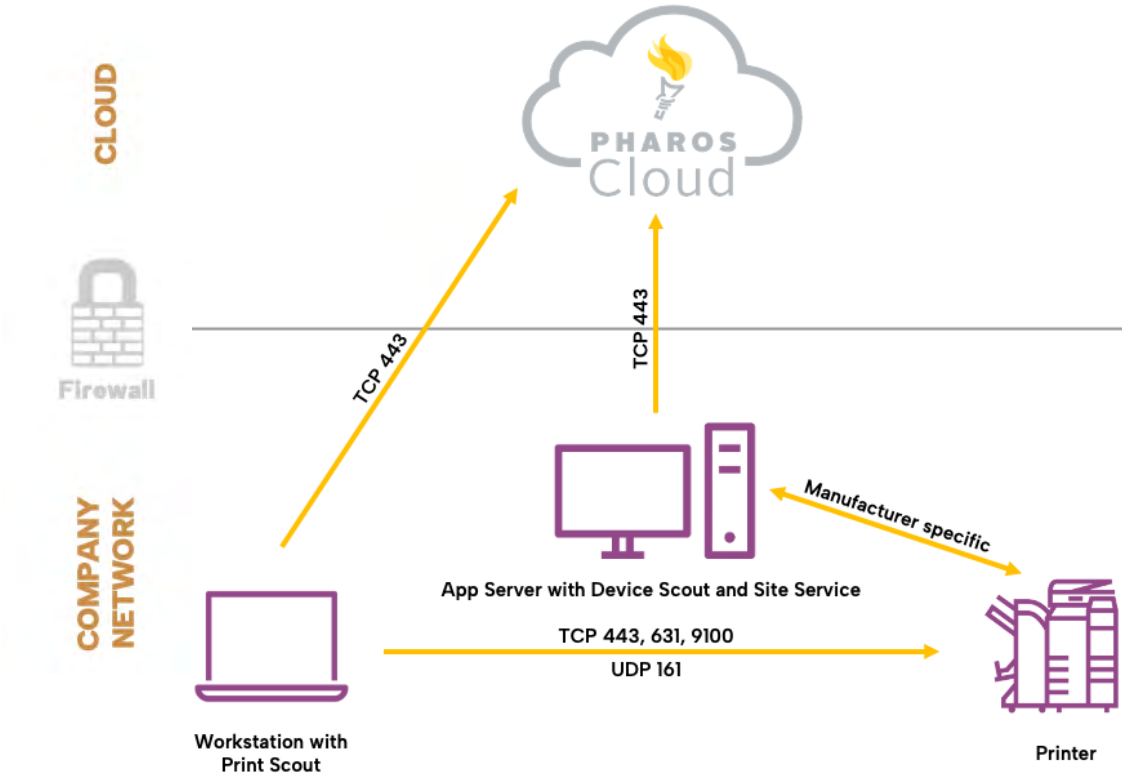
The Device Scout is an agent deployed on a Windows App Server within an organization's environment. For Pharos Secure Release, the Device Scout comes bundled with a Site Service that acts as a conduit between Pharos Cloud and networked printers that are unable to connect to Pharos Cloud directly and require authentication at the device panel.

The Site Service:

- Provides the interface for registering print users and authenticating users at the printers
- Acts as the device connector that bridges each networked printer being secured and unsecured to the cloud
- Captures secure release print, copy, and scan activity at secured printers

The figure below shows the architecture of a typical Pharos Secure Release deployment.

Deployment Architecture



- The Print Scout registers itself via an HTTPS (TLS) connection to Pharos Cloud and maintains a secure connection to the cloud service to enable print job submission and release.
- The Device Scout registers itself via an HTTPS (TLS) connection to Pharos Cloud and maintains a secure connection to the service to enable device configuration and secure managed printers.
- The secured printer communicates via an HTTPS (TLS) connection to Device Scout to authenticate users and release documents.
- Print Scout queries the printer for its status before delivering documents using SNMP.
- Print Scout delivers documents directly to the printer via an IPPS (TLS) connection. If the printer is not enabled for IPPS, the solution will fall back to using IPP. If IPP is also not supported, the solution will fall back to the RAW protocol. Since neither IPP nor RAW are encrypted, Pharos recommends enabling IPPS printing on printers.

Identity Providers

To print with Pharos Secure Release, users must register with Pharos Cloud using Print Scout. Secure Release supports three authentication provider types for user registration.

OpenID Connect

OpenID Connect is the recommended option by Pharos. This user authentication provider type uses token-based OpenID Connect technology to verify a print user's identity. This option is suitable for organizations with a supported OpenID Connect Identity Provider.

The OpenID Foundation defines OpenID Connect (OIDC) as a simple identity layer built on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an identity provider, as well as obtain basic profile information about the end-user.

Benefits of OpenID Connect include:

- Integration with well-known identity providers like Microsoft, Google, Okta, Ping Identity, etc.
- Elimination of the responsibility of storing and managing user credentials
- Separation of the user's print identity from the workstation's login identity—it does not matter what the user logs in as

More information regarding OpenID Connect can be found on its website.

Active Directory

This option is suitable for organizations that use Windows Active Directory (AD) for managing users. Print Scout uses the user's workstation ID to establish the identity of the user. This option does not require user registration.

Email

Email separates a user's print identity from their workstation's login identity. Users register their email address as their print identity. Email is a flexible option for organizations that do not have OpenID Connect or Active Directory.

Document Submission

Documents can be submitted for printing by a variety of methods.

Print Scout (Windows/MacOS)

Once Print Scout is installed, users simply select the Print command as they normally would when using an application. On PC or Mac workstations, this opens a standard Print dialog box that shows the Pharos Secure Printer queue.

Chrome OS

Pharos Secure release supports printing from Chromebooks and Chrome browsers using the Pharos Chrome Print extension, a Chrome Enterprise Recommended solution.

The Pharos Chrome Print extension creates a connection between the user workstation and Pharos Cloud. It establishes the user identity and provides the profile required for printing. Users can then submit print jobs with the Print menu from within the application being printed.

Mobile (iOS/Android)

Users can submit print jobs to Pharos Cloud from their mobile devices, from any location or network with internet access, using the Pharos Secure Release mobile app for iOS and Android devices.

The Secure Release mobile app creates a connection between the user and Pharos Cloud. It establishes the user identity and provides the profile required for printing. Users can then submit print jobs by using the native Print command on their mobile device.

Document Storage

Submitted print jobs are securely stored between print submission and print release.

Local Storage

Print jobs submitted from PC or Mac workstations are stored on the workstation, and sent directly to the printer when released. With local storage only, the workstation must remain online and within network line of sight to the printer.

Cloud Storage

If Cloud Storage is enabled, an encrypted copy of the print job is also sent to Pharos Cloud by the Print Scout and temporarily stored until the job is released or deleted by the job owner. If the originating workstation is not available, the print job is routed by Pharos Cloud through an available online Print Scout based on the organization's document handling configuration in the web console.

Print jobs submitted via mobile devices and the Pharos Chrome extension will always be stored in Pharos Cloud.

The default cloud storage location for Secure Release documents is in the United States. However, global organizations licensing the Data Privacy and Regional Document Storage feature have pre-defined geographic Regions correlating directly to secure AWS S3 repositories, and the ability to:

- Change the default Region
- Enable more than 20 different global Regions where users' Secure Release print jobs can be stored securely between print submission and print release based on each users' geography
- Determine the data privacy settings (what print job information is collected) in each Region for reporting purposes

For more information on how Pharos Cloud helps adhere to local data privacy and data sovereignty requirements, please refer to the Pharos Cloud Data Privacy and Regional Document Storage white paper.

Authentication and Release

After print submission, users may walk up and release their documents at any Pharos-secured print device on the company network by authenticating at the device of their choice. Pharos Secure Release supports document release through several methods:

- Swiping a proximity card (badge ID, access card, etc.)
- Scanning a QR code affixed to the device with the Pharos Secure Release mobile app
- Entering credentials on the printer's control panel

Proximity Card

With this configuration, employees use their proximity card to quickly authenticate at a chosen device to release their print jobs. Proximity cards are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication, and securely stored in the cloud as a one-way, non-reversible hash.

Mobile Release via QR Code Scan

Documents can also be released by scanning a QR code affixed to the print device with the Pharos Secure Release mobile app for iOS and Android devices. This option provides the following benefits:

- No printer installation or configuration required: Companies can enable secure print workflows without having to embed software on their print devices.
- Support for just about any networked printer: Leverage your existing printer fleet—virtually any network office printer can be enabled for mobile QR code release.
- Simple, touchless document release: There is no need to interact with the device control panel.

Keyboard Login

With this configuration, employees enter their credentials (passcode, username and password, email and PIN) at the print device's control panel to authenticate and release their print jobs.

Passcode

When OpenID Connect is set as the user authentication provider type, employees authenticate using their system-generated passcode. The passcodes are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication, and are securely stored in the cloud as a one-way, non-reversible hash.

Username and Password

When Active Directory is set as the user authentication provider type, employees authenticate using their AD credentials (username and password). User credentials are kept within the company's network and are never sent to the cloud. The authentication attempt is requested by the Site Service to the company's Active Directory domain controller.

Email and PIN

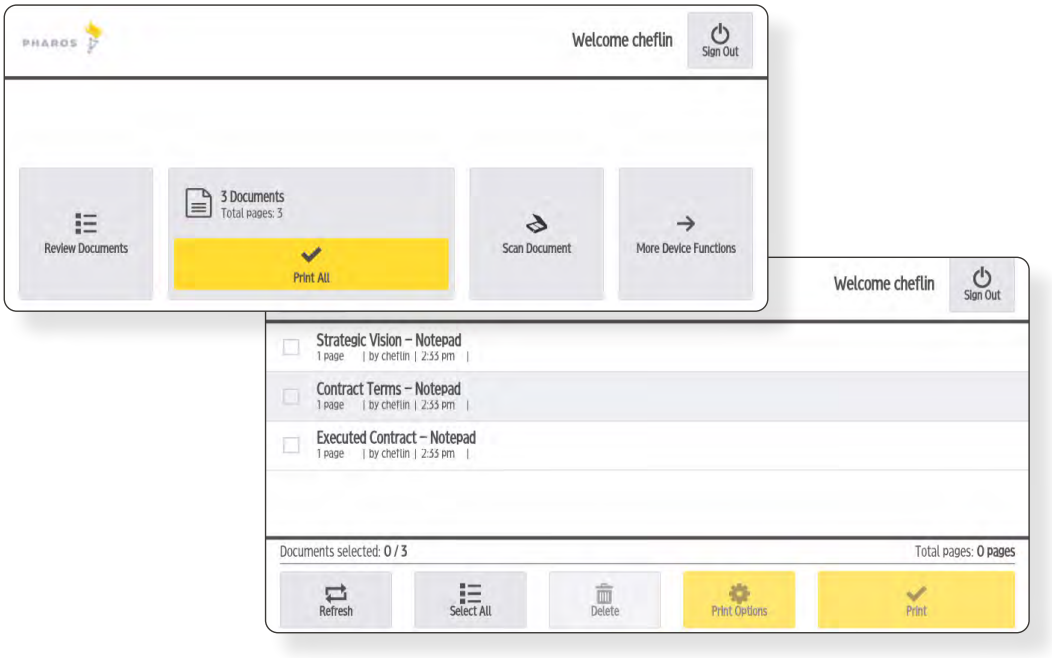
When email is set as the user authentication provider type, employees authenticate using their email address and user-generated, 4-digit PIN. The email and PIN are hashed using a one-way, non-reversible hash before being sent to the cloud for authentication, and are securely stored in the cloud as a one-way, non-reversible hash.

Document Release

Upon successful user authentication, users are presented with a simple screen that provides a one-touch method to review and print jobs in their queue.

Users can:

- Print all jobs in their queue with a single touch.
- View all jobs in their queue. The job list displays the document name, submission time, and page count—and users can select which job(s) they want to print, modify print settings, or delete.
- Access copy, scan, email, and other MFP functions/apps.



Job release requests are sent to Pharos Cloud, which requests the submitting workstation's Print Scout to deliver the selected print job(s) to the printer. If the originating workstation is not available, the print job is routed by Pharos Cloud through an available, online Print Scout based on the organization's document handling configuration.

Upon successful print output, the print device notifies Pharos Cloud to update the release state and orchestrate the cleanup of the document metadata and contents.

Secure Scanning

Pharos Secure Release also secures scanning from supported MFPs.

This allows:

- Administrators to manage enterprise printing and MFP scanning from a single web console
- Authenticated users to securely digitize and share documents

Users simply authenticate at an MFP via keyboard login or proximity card, click “Scan Document”, then select their desired settings and destination. After submission, the digitized document is sent from the MFP to the Site Service, to the Pharos Cloud, and then to the selected destination. Scanned documents are never stored at rest in Pharos Cloud and are encrypted in transit.

After secure scan settings have been set up by the company’s Pharos Cloud Administrator, users only need to authenticate at the device to pull up the Scan application.

Data Protection

Pharos Cloud supports end-to-end encryption to secure print job data. Print jobs can be sent encrypted from Print Scouts to IPPS-enabled printers over TLS 1.2.

To secure data at rest, there are two kinds of file encryption used in the system depending on the configuration in use. Documents stored on the client leverage zero knowledge encryption. For print jobs and print job information stored in the cloud, Amazon Simple Storage Service (S3) with Key Management Service (KMS) encryption is applied to the encrypted file.

Zero Knowledge Encryption

Pharos Cloud secures print jobs stored on the workstation or in the cloud whenever a Print Scout is used to send print jobs directly to a printer in the system with AES 256-bit zero knowledge encryption.

During installation, the Pharos Cloud Administrator is provided a system-generated site encryption password that is accessible only to the customer. This means that neither Pharos nor any other third party will ever know your site encryption password. The system does not retain a copy of this password; you must securely backup the password to enable future Scout installations and maintain the security of the print data.

The site encryption password is used to generate a 256-bit AES key, using the derivation function PBKDF2 with 1,000 iterations. This key is used to encrypt documents before they leave your local network, and to decrypt them prior to being sent to a printer. In addition, a PKI 2048-bit RSA key pair is generated for communication security with both the private key and AES key above being installed on the Scouts in your local network.

When documents are released from Pharos Cloud, they are decrypted when they arrive at a Print Scout on the company network. Therefore, even in the unlikely event that an attacker breaches the cloud security measures in Pharos Cloud, the attacker would be unable to access any document data.

AWS S3 with KMS Encryption

Print jobs and print job information stored in the cloud have multiple layers of encryption:

- The print job and print job information are first encrypted locally on the workstation using zero knowledge encryption into a single encrypted file
- A copy of the encrypted job is uploaded to Pharos Cloud over Transport Layer Security (TLS) 1.2

- Once uploaded to Pharos Cloud, Amazon S3 with Key Management Service (KMS) encryption is applied to the encrypted file

The following links provide more information on Amazon S3 and KMS encryption:

- https://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html
- https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

User Identity Hashing

When the user taps a proximity card, enters an email and PIN, or a passcode, the values are hashed using a one-way, non-reversible SHA-256 key and sent to the cloud for validation. The system looks at the hash value and authenticates the user accordingly.

Supporting Zero Trust Environments

Zero trust security has grown in popularity as more corporate enterprises abandon traditional strategies that rely on perimeter security. In today's world of remote workers and increasing cyberthreats, zero trust is emerging as the new standard for corporate security and infrastructure.

Zero trust is more than a singular technology or network topology—it's a comprehensive information security paradigm that initially distrusts all users and devices. The premise of zero trust is that no user, device, or application is inherently trusted—even inside the firewall. No user or device can gain access to other network resources without first proving the required level of identification and authentication. This controls lateral movement across the network and reduces the risk of a compromised endpoint providing a path to propagate a malicious payload to other endpoints. Zero trust involves the principle of least privilege and several technologies, including policy engines, encryption, endpoint security, and more.

Bad actors are assumed to be inside the network already. But the network remains secure, thanks to an array of technologies and best practices that make it more difficult for hackers to do the kind of damage they have done in the past to data centers and corporate networks.

Pharos Cloud delivers a robust and highly secure cloud service, with an architecture that can address NIST's zero trust security principles and permit employee printing to operate in a mature zero trust environment without having to disrupt your organization's printing workflows. For more information, please refer to the Pharos Cloud – Supporting Zero Trust Print Environments white paper.

Network Utilization

For many organizations, network traffic generated by print – especially large files – is non-trivial. Pharos Cloud is architected to minimize the impact on network traffic, particularly extranet traffic.

Print Scout Network Traffic

The Print Scout securely uploads print job information as it happens. The following table details the network traffic created by the Print Scout.

Task Type	Frequency	Network Traffic (bytes)
Status	1x24hrs	2K
AD lookups	Once per day, per user	Depends on size of average AD record
Cloud connection keep-alive	Every minute	< 0.1K
Print job metadata uploads	On print submission	3K
Print job content uploads	On print submission	Variable based on the size and complexity of the print job. This is conditional on Cloud Storage being enabled.
Incoming release requests and notifications	On print release	< 1K
Incoming job contents	On print release	Variable based on the size and complexity of the print job. Used only when a user's workstation is offline, and Cloud Storage is enabled.
Job delivery to printer	On print release	Variable based on the size and complexity of the job
Device SNMP lookup	On print release	2.5K

Print Scout Communication Patterns

- **Print Scout status checks:** Each Print Scout checks in once per day to upload its health report and check for new settings. This check is under 2 KB and will usually return an empty response if there have been no configuration changes. The Print Scout will also check for configuration changes when a print job is submitted.
- **Active Directory lookups:** When an employee submits a print job, the Print Scout will look up Active Directory information about that user. The AD lookup will occur only once per day. AD traffic is highly variable depending on the organization; however, the maximum traffic equates to the total number of unique AD users multiplied by the average AD record size.
- **Cloud connection:** The communication channel between Print Scouts and the cloud is kept alive by a server-initiated ping. This request occurs approximately once per minute and consists of a small packet of bytes.
- **Print job metadata uploads:** Data describing each print job is sent to the Pharos Cloud. This data is variable because of the strings involved (document name), but an approximation is 1 KB per print job.
- **Print job content uploads:** If enabled by the organization, a copy of submitted print jobs are uploaded to Pharos Cloud. The copy is used in the event the originating user's workstation is unavailable at the time of authentication. The size of this content is based on the size and complexity of the source document, but it is compressed prior to transfer. Typical one-page text documents are less than 100 KB.
- **Incoming release requests and notifications:** Pharos Cloud will issue requests to Print Scouts when a user selects their jobs to release at a printer. Notifications on the success or failure of the request are sent from the Print Scout back to Pharos Cloud. These requests and notifications comprise a small amount of text data, less than 1 KB in size.
- **Incoming print job content:** When necessary and configured to do so, a copy of the user's job contents may be delivered from the cloud service to the Print Scout. This can happen when the originating user's workstation becomes unavailable (goes into sleep mode, goes offline, etc.). In such an event, the server will select an available, online Print Scout to perform the print release.
- **Job delivery to printer:** The user's job contents are ultimately delivered from a Print Scout to their chosen printer. At this point, the data is uncompressed resulting in a file size equivalent to direct printing the file from Windows, without the Print Scout.

Device Scout Network Traffic

Pharos Secure Release requires access to your local area network to operate effectively. Device Scout will generate local network traffic when performing these operations:

- Scanning configured network ranges for printing devices
- Collecting meter data from discovered devices
- Collecting service alerts from discovered devices
- Configuring integrated printer
- Logging into a secure device

The Device Scout uses SNMP to communicate with local network devices and supports SNMPv1/v2 and/or SNMP v3. In some cases, the Device Scout will also try to connect to a device using HTTP port 80 if the device is a known model that cannot report serial number or meter reads via SNMP.

The Device Scout will generate Internet traffic when performing these operations:

- Device Scout Registration (one time occurrence during install)
- Polling Pharos Cloud for new configuration or instructions
- Uploading discovered device data
- Uploading device meter data
- Uploading Device Scout health check information
- Configuring integrated printers
- Logging into a secure device
- Interacting with a secure device (user activity)

The Device Scout uses secure HTTPS communication when connecting to Pharos Cloud. Additionally, all end-user access to the application is encrypted using TLS 1.2. Unencrypted SNMP traffic is restricted to the local subnets that the Device Scout is configured to monitor.

Here are the average payload sizes for the various Device Scout operations:

Task Type	Network Traffic (bytes)
Device discovery	15.8 K
Non-device usage	< 0.1K
Device status	16.6 K
Securing a device	2K
Printing from a secure device	< 100K

Excluding IP Ranges

Non-printing, SNMP-configured devices will let Device Scout know that they are not a print device with a 126-byte payload. While not harmful, this overhead may add up over large IP ranges. Therefore, Pharos recommends using "Exclude Ranges" in the Device Scout configuration to skip over any IP ranges that do not contain output devices.

Device Scout Communication Patterns

Registering a Device Scout: Customers create and configure a Device Scout record in the web application. During the installation of the Device Scout package, the Device Scout will open a secure connection to Pharos Cloud and identify itself using the registration information contained in the package. Once a package has been installed and registered, it cannot be used again.

Polling Pharos Cloud: Upon initial registration, and periodically during normal operation, the Device Scout will poll Pharos Cloud for updates to its configuration state. Updates might include new IP ranges to scan, a new version to download, or a new schedule for discovering or reading devices.

Uploading discovered device data: The Device Scout will upload discovered devices once per selected period (daily or weekly). More frequent uploads will result in more network traffic, but newly discovered devices will be displayed in the Pharos administrative web console sooner.

Uploading device meter data: The Device Scout will upload meter reads to Pharos Cloud on a scheduled basis. Administrators can configure this setting within the application.

Uploading toner data: Toner information will be collected along with meter data by default or configured to be collected as frequently as 15-minute intervals.

Uploading Device Scout health check information: The Device Scout Monitor runs as a scheduled Windows task to check the health of the Device Scout and its ability to communicate. It tracks the successful completion of Device Scout activities (i.e., discoveries, status collections, configuration updates) and uploads this information on a configured basis.

Cloud connection: The communication channel between the Device Scout and Pharos Cloud is kept alive by a Device Scout-initiated ping. This request occurs approximately once per minute and consists of a small packet of bytes.

Log in via username/password entry: The Device Scout controls the configuration settings on integrated printers. When a user logs into a secure printer via username/password entry, the solution will attempt to authenticate locally with Active Directory. The printer then retrieves and decrypts a document list from the cloud. Documents are then delivered to the device by a Print Scout.

SNMP device discovery: The Device Scout performs SNMP scans to discover new printing devices on a configured network segment. Some network monitoring tools may treat SNMP scans as sources of network congestion. Pharos recommends registering the Device Scout with your network security office so they are aware this network traffic is expected. Device Scout can be configured to exclude certain subnets or IP addresses, restrict its scans to certain times of the day, and reduce network utilization to a specific level.

Device Scout configuration data: Device Scout retrieves its configuration data by initiating an outgoing secure HTTPS connection to Pharos Cloud. When the configuration has been received, the Device Scout terminates the connection and operates without any outgoing connections until the next scheduled configuration check.

Internet Traffic

The following table provides details and guidance on the Internet traffic required by Pharos Secure Release. The number of documents per user per month is intended to be an example—actual traffic will vary by organization. Data consumption is also impacted by whether cloud-based document storage is enabled.

Monthly Internet Traffic Per User

SCENARIO	Cloud Storage Enabled? NO	YES
Number of secure documents[1]	3/day	3/day
Average document size[2]	0.5 MB	0.5 MB
PRINT DOCUMENT INFORMATION		
Transmission per document		
Document metadata	0.002 MB	0.002 MB
Document contents[3]	0.000 MB	0.550 MB
Job metadata for reporting	0.003 MB	0.003 MB
Transmission per document	0.005 MB	0.555 MB
Documents per user[4]	60/month	60/month
Data transmitted per month	**0.30 MB**	**33.3 MB**
WORKSTATION CONNECTION		
Keep-alive packet per minute	0.0001 MB	0.0001 MB
Connection data month[5]	**1.2 MB**	**1.2 MB**
OTHER DATA TRANSMISSION		
Print Scout daily status, AD lookups	0.004 MB	0.004 MB
Other data transmission / month[4]	**0.08 MB**	**0.08 MB**
Total Internet bandwidth	**1.58 MB**	**34.58 MB**

per user, per month

Assumptions

The guidance on traffic volume is based on the following:

1. An average of 3 secure documents printed per day, per user.
2. Document size can vary based on the nature of the documents printed. Calculations are based on an average document size of 500KB.
3. For cloud document storage, the solution will first attempt to retrieve the document from the user's workstation. Pharos estimates that 10% of the time, the user's workstation may not be available (e.g., in sleep mode or offline)—in this case, documents are retrieved from the cloud.
4. An average of 20 working days per month.
5. Workstation is online for an average of 10 hours/day for 20 working days/month

PHAROS

Pharos Systems International, Inc.
4545 East River Road Suite 210, West Henrietta, NY 14586, USA
888-864-7768 (Toll free US/Canada) | info@pharos.com | www.pharos.com