PHAROS

Beacon Analytics

Data security white paper

Learn about the architecture, policies, and safeguards that help keep your information secure when using Beacon Analytics

Pharos Systems International, Inc.
September 3, 2020

Table of Contents

INTRODUCTION

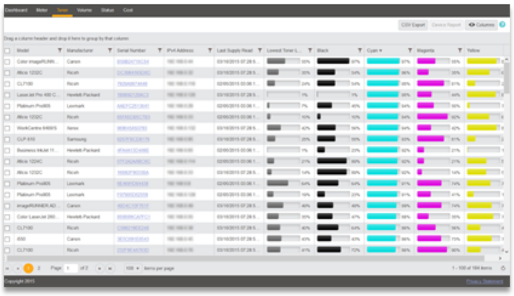
Pharos Beacon is a multivendor cloud print management platform that gives you a complete view of your organization's print environment, on demand. Beacon Analytics is a comprehensive print data management and insights tool that provides the clarity and control that businesses need to optimize their print environment. Beacon Analytics reveals the true cost of your printing and provides the decision support you need to reduce costs and improve end-user convenience.

Beacon Analytics is a true cloud service that runs on AWS. It comprises two elements:

- **Fleet Analytics:** Provides a comprehensive, multivendor view of print from your network devices and reveals volume, service, and operating cost information to help you build and maintain a more efficient fleet.
- **Print Analytics:** Reveals how print is created in your environment, including information about the user, the applications users print from, the output device, and comprehensive document parameters. It reveals opportunities to reduce costs and waste, and it helps you to discover the fleet design that best supports your people.

To perform its intended functions, Beacon will scan, collect, and store information about your print environment, your users, and the print jobs that users submit. The solution also gives you control over what data is collected and who can see it.

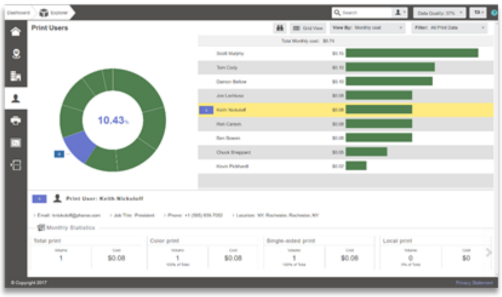
Fleet Analytics



- Device Status
- Device Meters
- Device Volume
- Device Toner Levels
- Cost of Print

Device Scout

Print Analytics



- Who is Printing
- What is Being Printed
- Targets and Trends
- Outliers
- Cost of Print

Print Scout

Solution Components

To take full advantage of Beacon Analytics, you will need to install two components in your local area network. Depending on your requirements and licensing, these components may include:

- **Device Scout**
- **Print Scout**

In some cases, multiple scouts of each type may be installed. No data (device data or user printing data) can be sent to Beacon until one or more scouts are installed and the scouts are activated with a registration key. If your registration key is ever invalidated or deleted, no further device or print data will be collected, even if the print/device scouts remain installed.

At any time, you may stop any scout from collecting information by uninstalling the scout. Instructions on how to uninstall the scouts can be found in the Beacon help documentation in the Pharos community (**community.pharos.com**).

Device Scout

The Device Scout is installed on a server as a best practice. It scans IP ranges that you define to locate all printers within your network. The Device Scout collects data on device status, meters, and consumables for use in Fleet Analytics views. The Device Scout will attempt to collect the following information from network devices that report themselves via SNMP as output devices:

- IP address
- Device description
- Maintenance kit levels
- Device serial number
- Non-toner supply levels
- Meter reads
- Asset number
- Monochrome or color identification
- Location
- Display reading
- MAC address
- Device status
- Manufacturer
- Model number
- Error codes
- Toner levels
- Firmware version/patch level

NOTE: Not all devices will report every attribute.

Print Scout

The Print Scout can be deployed to print servers and/or workstations (PC and Mac) to collect comprehensive information on how print is being created within the organization.

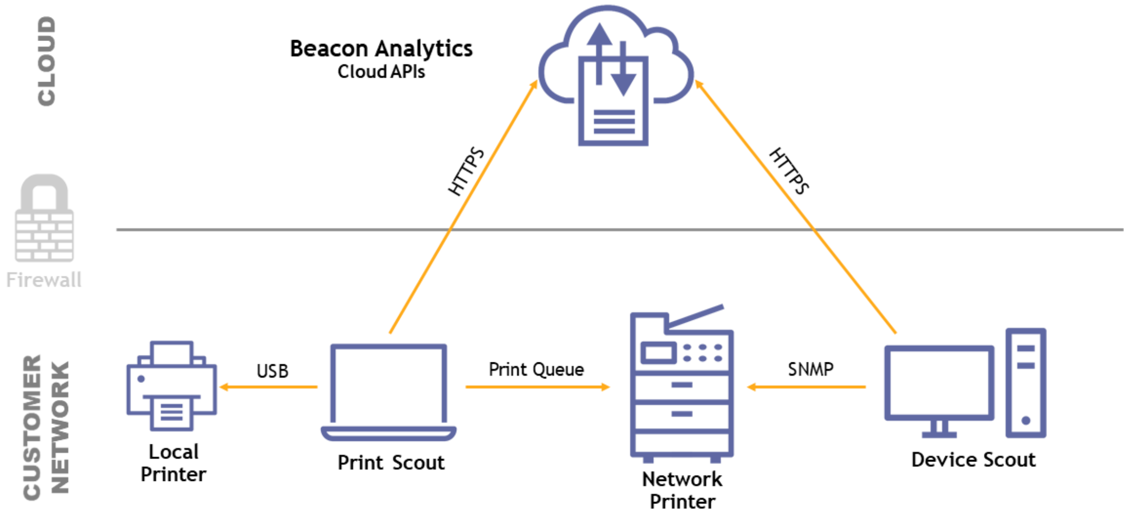
When installed on a print server, the Print Scout collects information on network printers and MFPs. Print Scouts deployed to employee workstations collect data on both network printing activity and any printing sent to locally attached devices. The Print Scout collects the following types of data:

- Information about the user from Active Directory
- Information from the printing device via SNMP
- Information about the print job via print stream analysis

You can control what data is collected and who can see it. You can configure the Print Scout's collection settings to disable the collection of certain types of data and obfuscate certain data if you need to maintain individual privacy. You can also apply role-based viewing restrictions, giving some users a limited view of the data.

Deployment Architecture

Depending on your network topology, requirements, and your print environment, you may deploy multiple print scouts and device scouts. An architectural overview is shown here for simplicity.



- The **Device Scout** registers itself via an HTTPS (TLS) connection to Beacon. Once the Device Scout has registered and obtained a copy of its configuration, it disconnects from Beacon and operates autonomously until the next configured check-in time.
- The **Print Scout** also registers itself via an HTTPS (TLS) connection to Beacon. The Print Scout behaves slightly differently than the Device Scout in that it will upload job data as it is captured.
- The integrity of customer data is critical. We use a combination of technological and procedural controls to restrict access to customer data.

Security Overview

Beacon addresses the following threat areas:

- **Machine or technical failure:** Such an event could include power loss, network connectivity loss, or data storage failure. Beacon uses a cloud-based infrastructure with a minimum of three geographic zones. The cloud infrastructure can detect a variety of fault conditions and remove or fix defective components on the fly with no interruption of service.
- **Malicious attack:** Such an event could include an attempt to intercept data in transmission, denial of service, or the attempted altering or disabling of established security measures such as logins or encrypted communication. Beacon encrypts all external connections using SSL or TLS at the highest level supported by the connecting browser. All application components are isolated by function; only necessary traffic can pass between components.
- **Passive data loss or corruption:** These losses could be caused by software defects, incompatibilities between software components, or data storage loss. The Beacon cloud infrastructure mitigates these risks through a formal software quality assurance methodology. In the event of a data corruption problem, Pharos maintains pre-state backups in order to roll back any data-altering changes. We also use segregation of duties and least privilege principles to restrict the level of access employees have, to include only that which is required to perform their job function. Access levels are periodically reviewed and adjusted as business needs or job roles change.

Securing Data is a Shared Responsibility

As a Pharos Beacon customer, you share the responsibility to protect your data. As your organization continually refines its security strategy to stay current with evolving threats, make certain that securing your print environment is a priority.

Add these security items to your standard processes to help you address the diverse and ever evolving threats out there.

1. Ensure that all scouts are accessible to authorized users only.

2. Ensure that servers and/or workstations hosting scouts are fully patched and meet all other security requirements of your organization.

   - Ensure that servers and/or workstations are regularly maintained according to the policies of your organization.

   - Ensure that the minimum necessary credentials are granted to individuals within your organization.

3. If the Print/Device Scout will be installed on a shared server (i.e. a server that performs multiple functions or that will be running software from another vendor), be sure to verify compatibility with Pharos technical support before installing.

CUSTOMER READINESS

This section details the environmental requirements and recommendations necessary to successfully deploy Beacon Analytics, and lists the ports and protocols required for Fleet Analytics and Print Analytics.

Platform communication

Your email security software must be set to trust the following email address to help prevent your organization from quarantining or blocking the message or sending the email to the Junk or Spam folder:

Beacon Admin **no-reply@beacon.pharos.com**

Cloud API endpoints

Sentry Print cloud API endpoints process collected data and print jobs, push application updates and configuration settings, and broker communication between systems components.

The software components, such as the Print Scout and cloud-aware printer, must be able to securely communicate to the cloud API endpoints. If permitted by your organization, Pharos recommends whitelisting the domain ***.beacon.pharos.com** to ensure that communication with current and future cloud API endpoints is permitted. Below is a list of cloud API endpoints if your organization requires the list of permitted URLs.

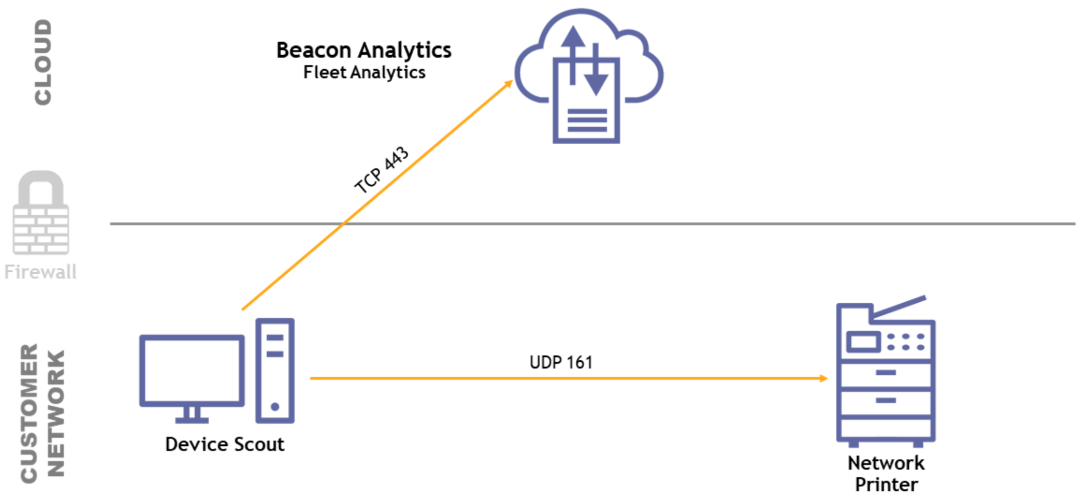
- https://api.beacon.pharos.com
- https://devicescout.beacon.pharos.com
- https://files.beacon.pharos.com
- https://login.beacon.pharos.com
- https://mfp-api.beacon.pharos.com
- https://printscout.beacon.pharos.com

Network ports and protocols

The following diagrams show the ports and protocols used to enable Beacon Analytics in your network environment.

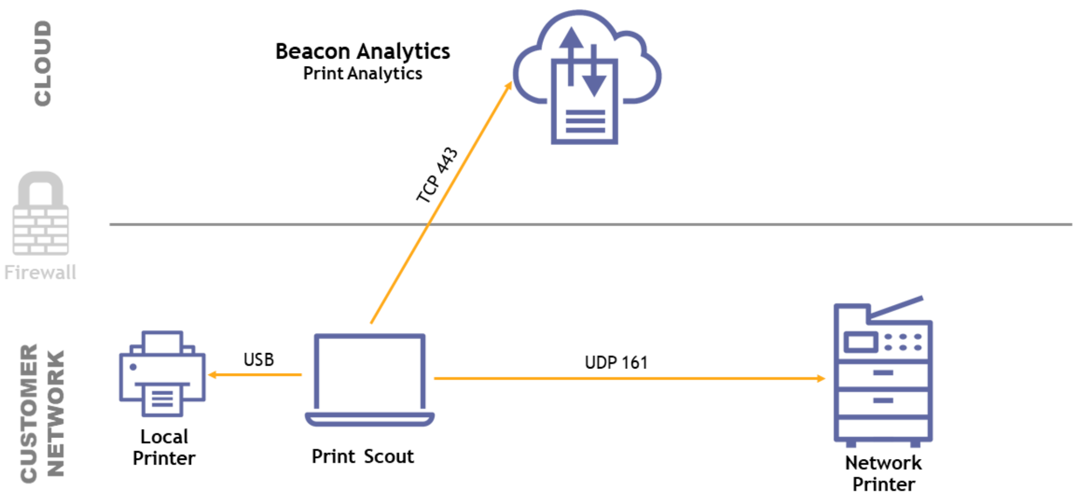
Fleet Analytics

The following diagram shows the basic structure, ports, and protocols required to deploy Beacon Fleet Analytics.



Print Analytics

The following diagram shows the basic structure, ports, and protocols required to deploy Beacon Print Analytics.



Deployment Requirements

Device Scout

The Device Scout discovers network devices and collects device-related data (status, meters, and consumables) and uploads it to Beacon for reporting and analysis.

Requirements

1. Supported operating systems:
   - Windows Server: 2008 R2 SP1, 2012, 2012 R2, 2016, and 2019
   - Windows: 7 SP1, 8, 8.1, and 10
2. Microsoft .NET Framework 4.6.1 (or newer) must be installed.
3. The Device Scout must be able to communicate with the cloud APIs to (1) upload collected device data and (2) download application updates and configuration settings.
4. The Web proxy server configuration (server, port, user credentials) is known, if required to access the Internet (cloud).
5. For Windows systems, end point protection (antivirus) software must trust the Device Scout and Local Connector executable (exe) files and dynamic link library (dll) files within this directory path and all its subfolders:

   C:\Program Files (x86)\PharosSystems\DeviceScout

   C:\Program Files (x86)\PharosSystems\Sentry Print Service
6. End point protection (antivirus) software must trust the Windows services for the Device Scout and Local Connector:

   Pharos Device Scout Service

   Pharos Systems Sentry Print Service
7. The Device Scout must be able to communicate with network printers to collect device data.
8. The following network ports must be open:
   - Outbound (Device Scout connecting to the cloud API endpoint):
     - 443 TCP (TLS v1.2)
   - Outbound (Device Scout connecting to the network printer):
     - 161 UDP (SNMP v1/v2 or SNMP v3)

Print Scout

The Print Scout is lightweight client software that is deployed to employee workstations to capture comprehensive printing data (and enable secure printing if Sentry Print is deployed). It also allows organizations to capture printing data for remote (home office) workers and their locally attached personal printers. This has become increasingly relevant in our Covid-19 environment and the strong trend toward a distributed workforce.

Requirements

1. Supported operating systems:
    - Windows: 7 SP1, 8, 8.1, and 10
    - macOS: 10.13, 10.14, and 10.15
    - Windows Server: 2008 R2 SP1, 2012, 2012 R2, 2016, and 2019
2. For Windows systems, Microsoft .NET Framework 4.6.1 (or newer) must be installed.
3. The Print Scout can be installed on print user workstations and Windows print servers.
4. The Print Scout must be able to communicate with network printers to collect device data.
5. The Print Scout must be able to communicate with the cloud APIs to (1) upload collected device data, print user information, and print job details, and (2) download application updates and configuration settings.
6. The Web proxy server configuration (server, port, user credentials) is known, if required to access the Internet (cloud).
7. For Windows systems, end point protection (antivirus) software must trust the Print Scout executable (exe) files and dynamic link library (dll) files within this directory path and all its subfolders:

    C:\Program Files (x86)\PharosSystems\PrintScout

8. End point protection (antivirus) software must trust the Windows services for the Print Scout:

    Pharos Systems Print Scout Service

    Pharos Systems Print Scout Spooler Service

9. The following network ports must be open:
    - Outbound (Print Scout connecting to the cloud API endpoint):
        - 443 TCP (TLS v1.2)
    - Outbound (Print Scout connecting to the network printer):
        - 161 UDP (SNMP v1/v2 or SNMP v3)

Network printer

A printer that is accessible by network connection, making it usable by other computers connected to the network.

Requirements

1. SNMP v1/v2 and/or SNMP v3 must be enabled
   - SNMP v1/v2: Read access is enabled and the Get Community Name string is known
   - SNMP v3: Username, Authentication Protocol and Passphrase, Privacy Protocol and Passphrase, and Context Name are known
     - Passphrase: 8 to 255 characters
     - Authentication Protocol: MD5 or SHA1
     - Privacy Protocol: DES or AES-128
2. The following network ports must be open:
   - Inbound (Device Scout connecting to the network printer):
     - 161 UDP (SNMP v1/v2 or SNMP v3)
   - Inbound (Print Scout connecting to the network printer):
     - 161 UDP (SNMP v1/v2 or SNMP v3)

NETWORK UTILIZATION

Print Scout

The Print Scout securely uploads print job information as it happens. The Print Scout does not perform network-wide discoveries; it is only aware of locally attached printers or network print queues. The following table details the network traffic created by the Print Scout.

TASK TYPE	FREQUENCY	NETWORK TRAFFIC (IN BYTES)
Status	1x24hrs	2K
AD lookups	Once per day, per user	Depends on size of average AD record
Print job metadata uploads	On print submission	3K
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 (AD) information about that user. The AD lookup occurs only once per day. AD traffic is difficult to estimate because the amount of data stored in AD is highly variable from one organization to the next. However, the maximum traffic equates to the total number of unique AD users multiplied by the average record size.
- **Print job metadata uploads:** Data describing each print job is sent to the cloud service. This data is variable because of the strings involved (document name), but a fair approximation is 1 KB per print job.
- **Automatic scout updates:** From time to time, a new version of the Print Scout will be released, with updated functionality and any bug fixes. The scout will check for new versions of itself whenever it checks for new configuration information. If a new version is available, the scout will automatically download and install the new version silently.

Device Scout

The Device Scout requires access to your local area network to operate effectively. The 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

The Device Scout uses SNMP to communicate with local network devices and supports SNMP v1, 2, and/or 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.

NOTE: The Device Scout does not record or track SNMP-enabled devices within its scanning range that do not report themselves as output devices.

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

- Registration
- Polling the Device Scout control server for new configuration or instructions
- Uploading discovered device data
- Uploading device meter data
- Uploading Device Scout health check information

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

Device Scout network traffic

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

TASK TYPE	NETWORK TRAFFIC (IN BYTES)
Device discovery	15.8 K
Non-device usage	< 0.1K
Device status	16.6 K
Integration	2K

Excluding IP ranges

Non-printing SNMP-configured devices respond with a 126-byte payload, which tells the Device Scout that the device is **not** a printing device. While not harmful, this overhead may add up over large IP ranges. Therefore, we recommend using “Exclude Ranges” in the Device Scout configuration to skip over any IP ranges that are not likely to contain output devices.

Device Scout communication patterns

- **Registering a Device Scout:** Customers create and configure a Device Scout record in the web application. To download the installation package, you must enter the site encryption key. A unique installation package per Device Scout record is created. During the installation of this package, the Device Scout will open a secure connection to Sentry Print 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 the scout control server:** Upon initial registration, and periodically during normal operation, the Device Scout will poll the control server 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 period, configured within the application. Discovery scans can be configured daily or weekly. More frequent uploads will result in more network traffic, but newly discovered devices will be displayed in the application more quickly.
- **Uploading device meter data:** The Device Scout will upload meter reads to the scout control server on a scheduled basis. Usage (meter) data can only be scheduled for a daily scan and upload. You configure this setting within the application.
- **Uploading toner data:** Toner information will be collected along with meter data by default. Or, you can configure it to be collected as frequently as 15-minute intervals.
- **Uploading 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 scout activities such as discoveries, status collections, and configuration updates. It uploads this information on a configured basis, once per day.
- **Cloud connection:** The communication channel between the Device Scout and the cloud is kept alive by means of a server-initiated ping. This request occurs approximately once per minute and consists of a small packet of bytes.
- **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. We recommend registering the Device Scout with your network security office so that they know to expect this network traffic. You can configure the Device Scout to exclude certain subnets or IP addresses, restrict its scans to certain times of the day, and reduce network utilization to a specific level.

- **Scout configuration data:** The Device Scout retrieves its configuration data by initiating an outgoing secure HTTPS connection to the scout control server. When the configuration has been received, the Device Scout terminates the connection and operates without any outgoing connections until the next scheduled configuration check. Additionally, the Device Scout will only communicate with output devices when configured to do so, and it does not hold open continuous data connections.
- **Automatic scout updates:** From time to time, a new version of the Device Scout will be released with updated functionality and any bug fixes. By default, the Device Scout will check for new versions of itself daily. If a new version is available, the scout will automatically download and install the new version. Based on your organization's preferences, you can easily control this setting; you can set it to Notify, Off, or Automatic (the default).

CLOUD ARCHITECTURE SECURITY

Pharos Beacon runs on a true cloud platform built on Amazon Web Services (AWS) to deliver a safe and scalable web application experience. The solution runs on a true cloud (cloud-native) platform built on Amazon Web Services (AWS). Pharos exclusively uses Infrastructure-as-a-Service (IaaS) providers that have achieved an SSAE 16 audit and ISO 27001 security certification covering all IaaS infrastructure and facilities. Additionally, Beacon uses a tiered application structure to isolate data within the cloud.

Infrastructure security

Pharos conducts periodic vulnerability assessments in all production environments. Access to production environments is restricted based on business need. Access roles are configured using Segregation of Duties (SOD) principles. System access levels are periodically reviewed and adjusted when necessary.

All production operating system and framework components are patched during predetermined maintenance windows. Pharos uses generally accepted guidelines for deploying new operating system and framework updates in a test environment before promoting to production.

Pharos monitors all vendor service bulletins for zero-day vulnerabilities and has processes in place for emergency patching should the need arise.

Privacy

Pharos does not collect, store, maintain, or transmit any information regarding the content of print jobs, and thus has no way of accessing, housing, or transmitting information, even if this information is printed or otherwise sent to print devices monitored by Beacon.

For more information regarding our privacy policy, please review our Privacy Statement at:

https://community.pharos.com/s/article/Pharos-Beacon-Privacy-Statement-764158147

Learn more:

https://pharos.com/cloud-print-management/